

An Investigation into a Digital Forensic Model to Distinguish between "Insider" and "Outsider"

PhD Thesis

Abdulrazaq Abdulaziz Al-Morjan

This thesis is submitted in partial fulfilment of the requirement for the
Doctor of Philosophy, awarded by

Software Technology Research Laboratory

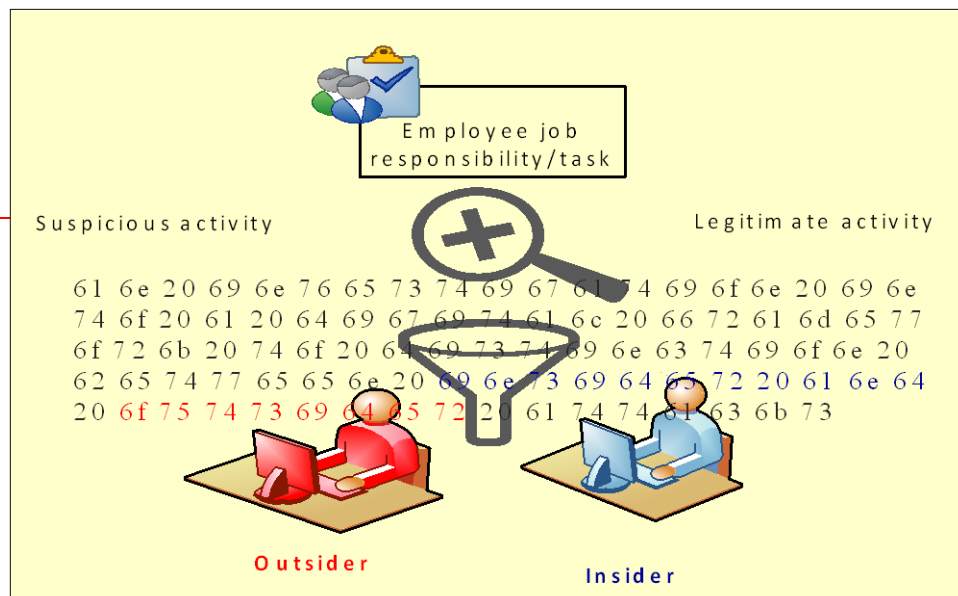
Faculty of Technology

De Montfort University

United Kingdom, England

— 2010

An Investigation into a Digital Model Forensic to Distinguish between "Insider" and "Outsider"



Abstract

IT systems are attacked using computers and networks to facilitate their crimes and hide their identities, creating new challenges for corporate security investigations. There are two main types of attacker: insiders and outsiders. Insiders are trusted users who have gained authorised access to an organisation's IT resources in order to execute their job responsibilities. However, they deliberately abuse their authorised (i.e. insider) access in order to contravene an organisation's policies or to commit computer crimes. Outsiders gain insider access to an organisation's IT objects through their ability to bypass security mechanisms without prior knowledge of the insider's job responsibilities, an advanced method of attacking an organisation's resources in such a way as to prevent the abnormal behaviour typical of an outsider attack from being detected, and to hide the attacker's identity.

For a number of reasons, corporate security investigators face a major challenge in distinguishing between the two types of attack. Not only is there no definitive model of digital analysis for making such a distinction, but there has to date been no intensive research into methods of doing so. Identification of these differences is attempted by flawed investigative approaches to three aspects: location from which an attack is launched, attack from within the organisation's area of control, and authorised access. The results of such unsound investigations could render organisations subject to legal action and negative publicity.

To address the issue of the distinction between insider and outsider attacks, this research improves upon the first academic forensic analysis model, Digital Forensic Research Workshop (DFRWS) [63]. The outcome of this improvement is the creation of a Digital Analysis Model for Distinction between Insider and Outsider Attacks (DAMDIOA), a model that results in an improvement in the analysis investigation process, as well as the process of decision. This improvement is effected by two types of proposed decision: fixed and tailored. The first is based on a predetermined logical condition, the second on

the proportion of suspicious activity. The advantage of the latter is that an organisation can adjust its threshold of tolerance for such activity based on its level of concern for the type of attack involved.

This research supports the possibility of distinguishing between insider and outsider attacks by running a network simulation which carried out a number of email attack experiments to test DAMDIOA. It found that, when DAMDIOA used predetermined decisions based on legitimate activities, it was able to differentiate the type of attack in seven of the eight experiments conducted. It was the tailored decisions with threshold levels $Th=0.2$ and 0.3 that conferred the ability to make such distinctions.

When the researcher compared legitimate activities, including users' job responsibilities, with the current methods of distinguishing between insider and outsider attacks, the criterion of authorised access failed three times to make that distinctions. This method of distinction is useless when there is a blank or shared password. He also discovered that both the location from which an attack was launched and attacks from areas within an organisation's control failed five times to differentiate between such attacks. There are no substantive differences between these methods. The single instance in which the proposed method failed to make these distinctions was because the number of legitimate activities equalled the number of suspicious ones.

DAMDIOA has been used by two organisations for dealing with the misuse of their computers, in both cases located in open areas and weakly protected by easily guessed passwords. IT policy was breached and two accounts moved from the restricted to the unlimited Internet policy group. This model was able to identify the insiders concerned by reviewing recorded activities and linking them with the insiders' job responsibilities.

This model also highlights users' job responsibilities as a valuable source of forensic evidence that may be used to distinguish between insider and outsider attacks. DAMDIOA may help corporate security investigators identify suspects accurately and avoid incurring financial loss for their organisations. This research also recommends many improvements to the process by which user activities are collected before the attack takes place, thereby enabling distinctions to be better drawn. It also proposes the

creation of a physical and logical log management system, a centralised database for all employee activities that will reduce organisations' financial expenditures. Suggestions are also proposed for future research to classify legitimate and suspicious activities, evaluate them, identify the important ones and standardise the process of identifying and collecting users' job responsibilities. This work will remove some of the limitations of the proposed model.

Acknowledgment

I would like to express my sincere gratitude to my first supervisor Dr. Francois Siewe for his support, ideas, guidance and encouragements through my research study. I would also like to express my thankful to Professor Hussain Zedan and Peter Norris for their support.

I would also like to express my deep gratitude to my mother and father for their endless love and support all the way through. Special thanks to my older sister for her prayers and everlasting sympathy.

My big thanks go to my wife for her love, full support, encouragement and cooperation without which I was not going to be able to do this research. Her support was made doubly significant by her pregnancy at this trying time.

Table of Contents

Abstract	ii
Acknowledgment	v
1. Introduction	2
1.1 Background.....	2
1.2 Hypothesis.....	6
1.3 Aim and objectivities	7
1.4 Research methodology.....	7
1.5 Contribution to knowledge	8
1.6 Measure of success	10
1.7 Thesis outline.....	11
2 Insider and Outsider Attacks and Digital Incident Investigations	13
2.1 Network infrastructures	13
2.1.1 <i>Public networks (Internet)</i>	13
2.1.2 <i>Local Area Networks (LANs)</i>	15
2.2 Security threats	24
2.2.1 <i>Internet threats</i>	24
2.2.2 <i>Threats to a LAN</i>	26
2.3 Computer-related attacks	27
2.3.1 <i>Insider</i>	28
2.3.2 <i>Outsiders</i>	32
2.4 The Issue of insider and outsider attacks.....	33
2.4.1 <i>Advanced methods of attack (outsiders gaining insider access)</i>	35
2.4.2 <i>Current methods of distinguishing between insider and outsider attacks</i>	36
2.5 Computer forensics	39
2.5.1 <i>The principles of computer forensics</i>	40
2.5.2 <i>The process of investigation into a relevant computer crime/incident</i>	41
2.5.3 <i>The analysis of computer investigations</i>	41
2.5.4 <i>Types of computer investigation model</i>	43
2.5.5 <i>Corporate security investigations</i>	47
2.6 Summary.....	51
3 User Activities and Assumptions	53

3.1	Job responsibilities/roles	53
3.2	Legitimate user activities.....	54
3.3	Suspicious activity/taxonomy of attacks	57
3.3.1	<i>Client-side attacks</i>	57
3.3.2	<i>Malicious software</i>	58
3.3.3	<i>Spoofing</i>	60
3.3.4	<i>Impersonation</i>	61
3.3.5	<i>Denial of Service (DoS) attack</i>	61
3.3.6	<i>Physical attacks</i>	63
3.3.7	<i>Password attacks</i>	63
3.3.8	<i>Social engineering</i>	63
3.3.9	<i>Information-gathering attacks</i>	64
3.3.10	<i>Theft of an organisation's devices and information</i>	64
3.3.11	<i>Computer and Internet abuse</i>	65
3.3.12	<i>Email attacks</i>	66
3.4	Location of user activities.....	71
3.4.1	<i>Legitimate activity logs</i>	71
3.4.2	<i>Security logs</i>	71
3.4.3	<i>Personal devices</i>	72
3.5	Assumptions	72
3.5.1	<i>Conditions attached to assumptions</i>	73
3.5.2	<i>Information and technology requirements</i>	74
3.6	Summary.....	79
4	Digital Analysis Model for distinguishing between Insider and Outsider Attacks (DAMDIOA)	82
4.1	Limitations of DFRWS	82
4.2	DAMDIOA	83
4.2.1	<i>Collection/identification process</i>	84
4.2.2	<i>Examination process</i>	90
4.2.3	<i>Analysis process</i>	92
4.2.4	<i>Presentation process</i>	99
4.2.5	<i>Decision</i>	100
4.3	Summary.....	103
5	Experiments.....	104

5.1	Hypothesis.....	104
5.2	Experiment components.....	104
5.2.1	<i>Experiment design.....</i>	<i>105</i>
5.2.2	<i>Established parameters of the experiment.....</i>	<i>106</i>
5.2.3	<i>Network Infrastructure.....</i>	<i>108</i>
5.2.4	<i>Software.....</i>	<i>111</i>
5.3	Conduct of Experiments.....	114
5.3.1	<i>Experiment (Ex) 1.....</i>	<i>114</i>
5.3.2	<i>Experiment (Ex) 2.....</i>	<i>119</i>
5.3.3	<i>Experiment (Ex) 3.....</i>	<i>123</i>
5.3.4	<i>Experiment (Ex) 4.....</i>	<i>128</i>
5.3.5	<i>Experiment (Ex) 5.....</i>	<i>133</i>
5.3.6	<i>Experiment (Ex) 6.....</i>	<i>136</i>
5.3.7	<i>Experiment (Ex) 7.....</i>	<i>139</i>
5.3.8	<i>Experiment (Ex) 8.....</i>	<i>142</i>
5.4	Discussion.....	146
5.5	Tailored decisions.....	147
5.5.1	<i>Similarities and comparisons between fixed and the tailored decisions.....</i>	<i>148</i>
5.6	Summary.....	149
6	Test and Evaluation.....	150
6.1	Discussion.....	150
6.1.1	<i>Comparisons between current methods of distinguishing insider from outsider attacks.....</i>	<i>150</i>
6.1.2	<i>Comparison between the proposed model and existing models.....</i>	<i>155</i>
6.2	Case studies.....	157
6.2.1	<i>Case study 1.....</i>	<i>157</i>
6.2.2	<i>Case study 2.....</i>	<i>159</i>
6.3	Challenging the distinction between insider and outsider attacks.....	163
6.3.1	<i>The model's incapability of model to distinguish between co-workers.....</i>	<i>163</i>
6.3.2	<i>The model's inability to model to distinguish between insider and outsider attacks.....</i>	<i>163</i>
6.3.3	<i>Classification of activities.....</i>	<i>163</i>
6.3.4	<i>Relative weighing of activities.....</i>	<i>164</i>
6.3.5	<i>Mis-configured security components.....</i>	<i>164</i>
6.3.6	<i>Lack of implementation of full-content network monitoring.....</i>	<i>164</i>
6.3.7	<i>Lack of preservation of the log files.....</i>	<i>164</i>

6.3.8	<i>Lack of recording of legitimate activities</i>	164
6.3.9	<i>Lack of retention policy</i>	165
6.4	Summary.....	166
7	Recommendations	167
7.1	Recommendations for enhancing an organisation’s resource authentication	167
7.1.1	<i>User authentication</i>	167
7.1.2	<i>Enabling of different passwords for different applications</i>	169
7.2	Recommendations for enhancing an organisation’s log files	170
7.2.1	<i>Creating multiple event records</i>	170
7.2.2	<i>Enabling of communication records</i>	170
7.3	Implementation of physical access controls.....	170
7.4	Physical access control logs.....	171
7.5	Insider and outsider activities log management	172
7.5.1	<i>Log management</i>	173
7.5.2	<i>Components of logs management</i>	173
7.6	Interview insiders	175
7.7	Security incident report policy	175
7.8	Defining of user’s job responsibilities	176
7.9	Summary.....	177
8	Conclusion	178
8.1	Future Work	182
8.1.1	<i>Clustering of activities</i>	182
8.1.2	<i>Identification of the most important information</i>	182
8.1.3	<i>Assigning relative weightings to legitimate and suspicious activities</i>	182
8.1.4	<i>Develop DAMDIOA:</i>	183
8.1.5	<i>Applicability to various types of incident</i>	183
8.1.6	<i>Users’ job responsibilities/roles</i>	184
9	References	185
	Appendixes	193
	Appendix A: Build configuration of experiment	193
	A1. <i>Iptables</i>	193
	A2. <i>Ubuntu Requirement:</i>	193
	A3. <i>Netkit Requirements:</i>	194

<i>A4. Technical Configuration Description</i>	194
<i>A5. Setting the Network</i>	195
Appendix B: The Process of Analysis the Attack Experiments	206
<i>B1.Ex1:</i>	206
<i>3.Examination Data:</i>	210
<i>B1. Ex2:</i>	230
<i>B1.Ex3:</i>	237
<i>B1. Ex4:</i>	245
<i>B1. Ex5:</i>	260
<i>B1. Ex6:</i>	273
<i>B1: Ex8.</i>	279

Table of figures

Figure 1: Financial losses resulting from computer attacks.....	3
Figure 2: Proportionate occurrence.....	4
Figure 3: Components of the model.....	6
Figure 4: Issue of Insider and Outsider Attacks.....	50
Figure 5: An organisation's structure.....	56
Figure 6: Type of information.....	70
Figure 7: DAMDIOA Model.....	84
Figure 8: Diagram of IT infrastructure.....	86
Figure 9: Information sources of data collection.....	88
Figure 10: Data collection process.....	89
Figure 11: Examination process.....	91
Figure 12: Timeline analysis revealing attack session.....	93
Figure 13: Review attack period activity.....	94
Figure 14: Examine gap between sessions.....	95
Figure 15: Analysis of the gap between login activities.....	95
Figure 16: Relational analysis examination of the activities relation.....	97
Figure 17: Analysis process.....	99
Figure 18: Network infrastructure for Experiments.....	109
Figure 19: Components of the experiment's mail server.....	109
Figure 20: Timeline analysis for Experiment 1.....	115
Figure 21: Relational analysis for Experiment 1.....	117
Figure 22: Insider's business emails.....	118
Figure 23: Timeline analysis for Experiment 2.....	120
Figure 24: Relational analysis for Experiment 2.....	122
Figure 25: Timeline analysis for Experiment 3.....	124
Figure 26: User activities for collecting information.....	126
Figure 27: Relational analysis for Experiment 3.....	127
Figure 28: Content of the abusive message.....	129
Figure 29: Full header of an abusive email.....	130
Figure 30: Timeline analysis for Experiment 4.....	131
Figure 31: Relational analysis for Experiment 4.....	132
Figure 32: Timeline analysis for Experiment 5.....	134
Figure 33: Relational analysis for Experiment 5.....	135
Figure 34: Timeline analysis for Experiment 6.....	137
Figure 35: Relational analysis for Experiment 6.....	138
Figure 36: Timeline Analysis for Experiment 7.....	140
Figure 37: Relational analysis for Experiment 7.....	141
Figure 38: Timeline analysis for Experiment 8.....	143
Figure 39: Relational analysis for Experiment8.....	144
Figure 40: Number of false and correct decision.....	154
Figure 41 Evidence of modification Internet Policy.....	160
Figure 42: Advantages of enhancing the collection process.....	172
Figure 43: Using Ping for testing Experiment network connection.....	196
Figure 44: Configuration of MUA for insider's client.....	199
Figure 45: Creation of new five accounts in MX.....	200
Figure 46: Configuration of Experiment's server (NS).....	203
Figure 47: Review Experiment's network.....	207

Figure 48: Examine the insider's activity	208
Figure 49: IMAP insider's activity	209
Figure 50: SMTP insider's activity	210
Figure 51: Examine insider's authentication login	211
Figure 52: Examine insider's email activity	212
Figure 53: Examine insider's email activity	213
Figure 54: Examine an abusive email	214
Figure 55: Examine insider's logout activity	215
Figure 56: Examine insider's authentication login	215
Figure 57: Examine insider's email activity	216
Figure 58: Examine insider's email activity	217
Figure 59: Examine insider's email activity	218
Figure 60: Examine insider's logout activity	218
Figure 61: Examine insider's login activity	219
Figure 62: Examine insider's email activity	220
Figure 63: Examine insider's email activity	221
Figure 64: Examine insider's email activity	222
Figure 65: Examine insider's authentication login activity	223
Figure 66: Examine insider's email activity	224
Figure 67: Examine insider's logout activity	225
Figure 68: Examine insider's authentication activity	226
Figure 69: Examine insider's email activity	227
Figure 70: Examine insider's logout activity	228
Figure 71: Examine insider's computer analysis	229
Figure 72: Authentication login activity	231
Figure 73: Examine insider's email activity	232
Figure 74: Examine insider's email activity	233
Figure 75: Examine insider's email activity	234
Figure 76: Examine abuse email	235
Figure 77: Examine insider's email activity	236
Figure 78: Examine insider's computer activity	237
Figure 79: Examine authentication login	238
Figure 80: Examine email activity	239
Figure 81 : Examine email activity	240
Figure 82: Examine email activity	241
Figure 83: Examine email activity	242
Figure 84: Examine abusive email	243
Figure 85: Examine insider's computer activity	244
Figure 86: Examine insider's computer activity	245
Figure 87: Examine full abusive email header address	246
Figure 88: Firewall activity log	247
Figure 89: Insider's authentication login activity	248
Figure 90: Examine email activity	249
Figure 91: Examine SMTP email activity	251
Figure 92: Examine SMTP email activity	252
Figure 93: Examine SMTP activity for the first step of creating a fake email	253
Figure 94: Examine SMTP activity for the second step of creating a fake email	254
Figure 95: Examine SMTP activity for the third step of creating a fake email	255
Figure 96: Examine SMTP activity for the fourth step of creating a fake email	255
Figure 97: Examine SMTP activity for the fifth step of creating a fake email	256
Figure 98: Examine SMTP activity for sixth step of creating a fake email	257

Figure 99: Examine SMTP activity for the seventh step of creating a fake email	257
Figure 100: Examine SMTP activity for the eighth step of creating a fake email.....	258
Figure 101: Examine SMTP activity for the ninth step of creating a fake email	259
Figure 102: Examine insider's computer activity	260
Figure 103: Examine email abusive.....	261
Figure 104: Examine firewall activity log	262
Figure 105: Examine email activity	265
Figure 106: Examine email activity	268
Figure 107: Examine email activity	269
Figure 108: Examine email activity	272
Figure 109: Authentication login activity	274
Figure 110: Authentication login activity	275
Figure 111: Authentication login activity	276
Figure 112: Examine login activity.....	277
Figure 113: Examine login activity.....	278
Figure 114: Examine abusive email.....	279
Figure 115: Examine insider's login activity	280
Figure 116: Examine email activity	281
Figure 117: Examine abuse email	282
Figure 118: Examine the insider's computer activity	283

List of tables

Table 1: A server's main services	17
Table 2: Differences between transport protocols	19
Table 3: Examples of well-known port numbers	19
Table 4: Examples of registered port numbers	20
Table 5: Examples of security threats	20
Table 6: IP address classes	21
Table 7: Private IP addresses	22
Table 8: Main methods of distinguishing between insider and outsider attacks	39
Table 9: Process of computer investigation for general and specific models	46
Table 10: Illustration of insider and outsider attacks	69
Table 11: Type of user activity	100
Table 12: Components of the Experiment's infrastructure	104
Table 13: User activity for Experiment 1	115
Table 14: Experiment 1 result	119
Table 15: User activity for Experiment 2	120
Table 16: Experiment 2 results	123
Table 17: User activity for Experiment 3	125
Table 18: Experiment 3 results	128
Table 19: User activity for Experiment 4	131
Table 20: Experiment 4 results	133
Table 21: User Activity for Experiment 5	134
Table 22: Experiment 5 results	136
Table 23: User activity for Experiment 6	137
Table 24: Experiment 6 Result	139
Table 25: User activity for Experiment 7	140
Table 26: Experiment 7 results	141
Table 27: User activity for Experiment 8	143
Table 28: Experiment 8 results	145
Table 29: Results of Experiments	146
Table 30: Results of experiments based on portion of suspicious activities	147
Table 31: Comparison between fixed and tailored decision	148
Table 32: Results of experiments to determine the best factor for distinguishing the type of attack	151
Table 33: Timeline of the insider's activities	162
Table 34: Relative weightings assigned to legitimate activities	183
Table 35: Filter Packet Chain Types	193
Table 36: Policy of IPtables Chains	193
Table 37: Minimum System Requirements of Ubuntu	193
Table 38: Minimum System Requirements of Netkit	194
Table 39: IP Address for Experiment's Client Machines	196

1. Introduction

1.1 Background

The majority of organisations rely greatly on computer systems and the Internet to operate and to enhance their businesses, relying on those systems' ability to process, transmit, store and retrieve data. Studies demonstrate that in 2005, 93 per cent of all documents created in U.S. organisations were created electronically, 70 per cent of which never migrated to paper [46]. Outside attackers can exploit the weaknesses of Internet infrastructures or the vulnerabilities of organisations' resources to gain insider access without detection and to carry out attacks. Gaining insider access prevents the abnormal behaviour of outsider attacks from being detected and hides attackers' identities. Wilson [104] finds that code obfuscation through various randomisation techniques becomes more complex if codes are made invisible to the pattern-matching/signature-based methods used by antivirus products. Organisations' computers, servers and laptops have therefore increasingly become targets of crime, tools for committing crimes or repositories of information used or generated in their commission [37; 15].

Computer attacks or threats to information technology may have a significant impact on organisations [23; 50; 51]. These threats usually lead to the disclosure of information, modification, denial of service (DoS), illegal use, identity theft or repudiation [31]. Threats against IT systems can be internal, stemming from insiders, or outsider threats initiated beyond an organisation's boundaries [51]. According to the British Department of Trade and Industry (DTI) in association with PriceWaterhouseCoopers, who published the *Information Security Breaches Survey 2006*, the number of malicious security incidents stemming from organisational insiders is almost double that of those originating from outsiders [66]. In 2006, the cost to the U.S. of computer crime was \$18,922,410 (£9,209,525) [18]. The CSI/FBI 2006 Computer Crime and Security Survey indicates that the financial losses resulting from computer crime were as follows [18]:

- Unauthorised access \$10,617,000
- Theft of property information \$6,043,000
- Insider Net Abuse \$2,262,410

Figure 1 shows financial losses resulting from computer attacks.

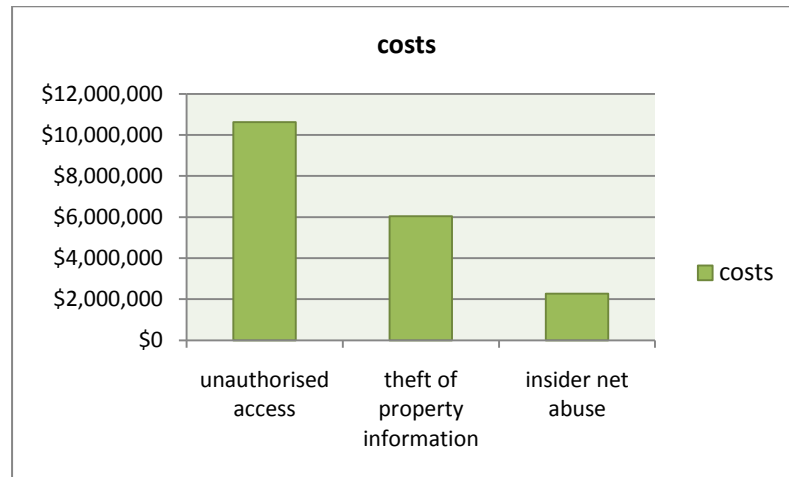


Figure 1: Financial losses resulting from computer attacks

The CSI/FBI 2008 report reveals that the four most common types of incident are viruses, insider abuse, laptop theft and unauthorised access to systems [19]. Theft of laptops can pose problems if they hold sensitive insider information such as usernames, passwords, personal information and e-mail messages. Figure 2 shows the common types of computer incident in 2008 and their rate.

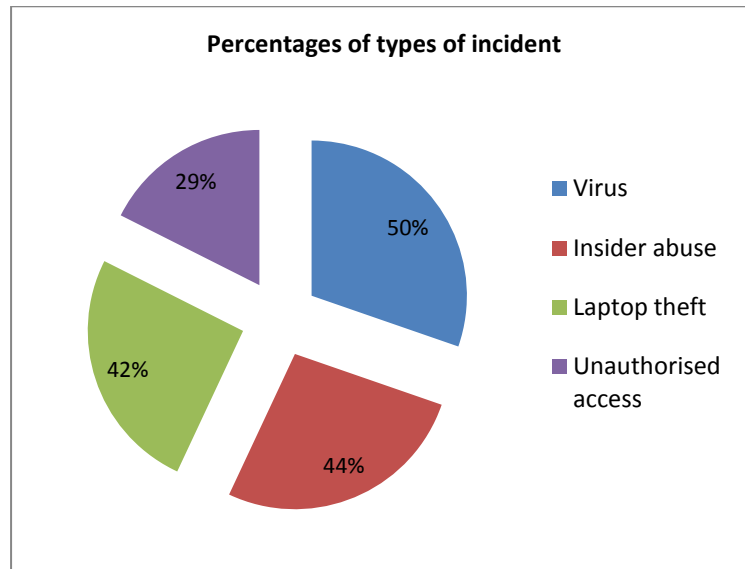


Figure 2: Proportionate occurrence

Haggerty and Taylor [37] believe that corporate security investigations are making increasing use of computer forensics in areas such as fraud, the accessing or distribution of pornography, and harassment. However, the increasing sophistication of methods of computer attack methods creates a new challenge for computer crime and corporate security investigators. Attacks occur when insider (i.e. authorised) access is gained without detection by outsiders who use such access to carry out attacks against organisations' IT resources.

Insider access can generally be gained in a number of ways. Stolen storage devices such as USBs or legitimate users' laptops can be obtained in order to use the settings stored on such devices to dial in. The vulnerabilities of insiders' computers or their lack of personal security can be exploited. Fake websites are a known method of obtaining insider access by attracting insiders to the site and deceiving them into downloading malicious software that is usually designed to steal usernames and passwords. The deployment of advanced hacking tools needs less technical knowledge on the part of outsiders who wish to launch password attacks to gain insider access [24]. If they were successful, they would be seen as

insiders, and evidence from investigations conducted according to current models would lead directly to those insiders rather than to the parties who launched the attack. The most important issue is how to distinguish between insider and outsider attacks. Advanced attacks therefore present corporate security investigators with two main challenges: they must confront the possibility of distinguishing between insider and outsider attacks, and their investigations must deal with insiders who deny carrying out attacks.

The present research addresses this issue via a proposed Digital Analysis Model for Distinction between Insider and Outsider Attacks (DAMDIOA), created by enhancing the Digital Forensic Research Workshop (DFRWS) method to enable the distinction between insider and outsider attacks to be made. DFRWS has many limitations, one of which is that its approach is usually that of a general model that does not consider the distinction between insider and outsider attacks, for example by providing a guideline of how to conduct an investigation into such attacks separately. Another drawback is that it does not include a method of relational analysis by which to identify the relationship between the activities performed during the period of an attack and an insider's job responsibilities. Neither does this model develop data collection processes such as deciding what data should be collected and why, and how they should be analysed. These limitations therefore result in insufficient data being made available to analyse in order to identify suspects, a deficiency with a detrimental impact on the decision-making process.

DAMDIOA is of material benefit when conducting digital investigations in cases where insider access is obtained by outsiders who then proceed to carry out attacks against an organisation's IT resources, or when insiders deny allegations of carrying out such attacks. Four conditions should be met in order for DAMDIOA to distinguish between the two types of attack. The first is that an outsider should have no prior knowledge of an insider's job responsibilities, the second is the log system's ability to record legitimate and suspicious activities for

a certain length of time, the third that a client/server environment should have been implemented and the last that users' job responsibilities and roles should be dependent on IT systems. DAMDIOA supports corporate security investigators in identifying suspects. The relationships between DAMDIOA's investigative use and the four conditions mentioned are shown in Figure 3.

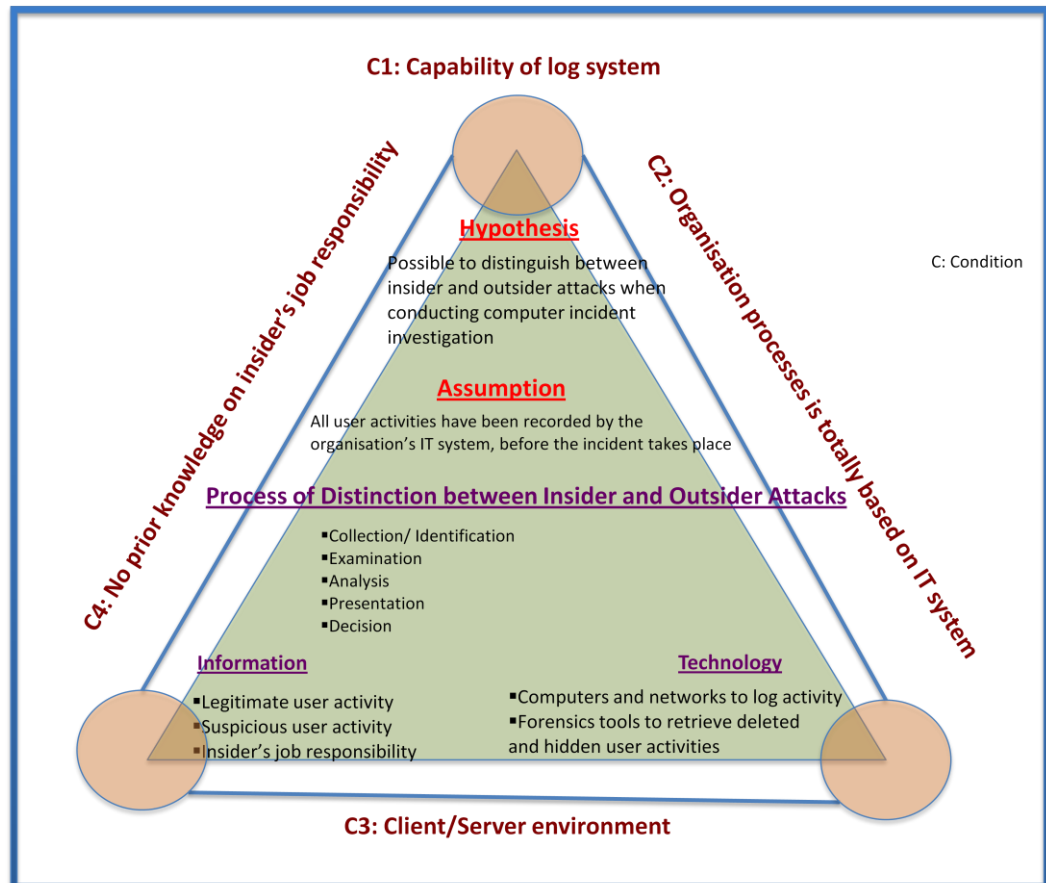


Figure 3: Components of the model

1.2 Hypothesis

This research proposes that, under certain circumstances, it is possible to distinguish between insider and outsider attacks when conducting computer incident investigations.

1.3 Aim and objectivities

The aim of this research is to determine the possibility of distinguishing between insider and outsider attacks. It will also create DAMDIOA in order to help corporate security investigators identify suspects.

The objectives of the research are as follows:

- to critically review the literature in order to identify the main problems in distinguishing between the two types of attack
- to investigate the various types of computer forensic investigation model. This analysis will help determine the shortcomings of existing models of computer investigation, as well as the requirements of DAMDIOA
- to determine the methods by which insider access is gained
- to improve the Digital Forensic Research Workshop (DFRWS) method
- to improve the collection and analysis of organisations' digital incident/crime investigations
- to evaluate the model using data gathered through network simulation
- to recommend improvements to the process by which insider and outsider attacks are distinguished.

1.4 Research methodology

An extensive search of the literature relating to the current state of the art, particularly with regard to digital incident/crime investigation models available to corporate security investigators, has been undertaken. A hypothesis has been created and ways of solving the problem have also been identified. The methodology of this research comprises three parts:

1. **Research**, which has used journals, conference proceedings, books and websites to understand the problem and provide a solution.

2. **Design**, which has improved DFRWS by creating DAMDIOA to address the issue of distinction between insider and outsider attacks.
3. **Implementation and evaluation**, which has been conducted as follows:
 - A network experimental test has been set up to carry out computer incidents such as the sending of abusive emails
 - **Netkit**: a software that is used to set-up a virtual network such as a Local Area Network (LAN), clients, servers and firewalls
 - **Computer incident**: this experiment used the following methods to carry out computer incidents:
 1. Password guessing, in which an outsider gains insider access by exploiting that insider's weak password
 2. Fake email header, where an insider and outsider use a fake email header to impersonate someone else's identity by using Simple Message Transfer Protocol (SMTP)
 3. Using an organisation's email, in which an outsider and insider use an organisation's email system to send an abusive email.
 - Tcpdump, a sniffing tool that is used to collect legitimate and suspicious activities carried out by insiders
 - Wireshark, an analysis tool used to analyse the resulting collection
- II. The hypothesis has been tested by using the DAMDIOA to gather and analyse data in order to ascertain whether the attack was carried out by an insider or an outsider

1.5 Contribution to knowledge

This research has produced the following results:

1. **Identification of the main issues involved in distinguishing between insider and outsider attacks.** It establishes that none of the current methods of making such distinctions, methods involving the location from which the attack was initiated, attacks within an organisation's control, and authorised access, address the problem. Furthermore, the lack of an organisation's authentication (for example, a single-sign on or a password policy) allows outsiders to gain insider access easily. The use of these current methods to make such distinctions therefore results in the collection and analysis of incorrect data. Such methods will not result in the correct identification of suspects, and will additionally incur financial loss for the organisation using them.
2. **Creation of DAMDIOA for solving the problem of distinguishing between insider and outsider attacks.** This model is effective when insider access is covertly gained by outsiders who use it to carry out attacks against organisations' IT resources, or when insiders deny allegations of having carried out such attacks. This is because most current computer attack investigation models are designed to deal with traditional attacks, such as breaking into networks or computer systems. These models focus on translating the requirements of legal systems into those of IT systems in order to conduct proper computer forensic investigations. However, they do not address the distinction between insider and outsider attacks. It is in these cases that DAMDIOA helps corporate security investigators correctly identify suspects and avoid financial penalties for their organisations.
 - **Identification of "insider's job responsibilities" as a method for distinguishing between insider and outsider attacks.** This model recognises that an insider's job responsibilities are a valuable source of information that can be used to make such a distinction. A particular job profile is requested from the holder's supervisor or the organisation's human resources department in order to identify a link between these responsibilities and the activities that

were carried out as part of an attack. If there is a link between them, it indicates that this is an insider attack, because an outsider could have had no prior knowledge of what the insider's job entails.

- **Implementation of full content data monitoring.** This is an efficient tool that can be used to distinguish between the two types of attack, because it intercepts the content of data transmitted between two parties. It includes not only packet headers but also payloads, which are required for collection and analysis for the purpose of identifying whether or not these data are consistent with the insider's discharge of their job responsibilities.
3. **Improvement of the process of distinction between insider and outsider attacks. by which insider and outsider attacks are distinguished.** This model identifies the information that should be collected in order to distinguish between attacks, thereby improving the process by which such distinctions are made. It also improves the analysis stage of the process by using timeline and relational analyses on the collected data.
- **Evidence of the correctness of the hypothesis that it is possible to distinguish between insider and outsider attacks.** The experimental results show that DAMDIOA correctly distinguished between insider and outsider attacks in seven experiments of eight.
 - **The consequent elimination of false positive decision.** Traditional methods of distinction, such as attacks within an organisation's control and locations from which attacks are initiated, misidentified five of the eight experiments. In the experiments involving DAMDIOA, however, only one false identification was made.

1.6 Measure of success

The success of thesis is measured in two ways:

- Evaluation: a number of digital attack experiments were conducted to test the hypothesis.
- Comparative analysis: this methodology was compared with other methods of computer forensic investigation.

1.7 Thesis outline

Chapter 2: Insider and outsider attacks and digital computer incident/crime investigation

This chapter reviews in detail the existing literature concerning insider and outsider attacks and how these occur in the real world; it provides insight into the kind of evidence that such attacks may leave for the computer forensic investigator. This evidence is not enough to distinguish between insider and outsider attacks. The primary aim is to outline the main problem involved in distinguishing between insider and outsider attacks and the research that has been conducted into this problem, and to outline the shortcomings of the current models of corporate computer forensic investigations.

Chapter 3: Assumptions and environment

Legitimate activity and organisational users' job responsibilities are discussed, as are suspicious activities, by means of extending Hansman and Hunt's classification of computer and network attacks. This chapter principally discusses outsider methods of gaining insider access by their exploitation of IT systems' vulnerabilities and users' lack of security awareness. It also demonstrates that employees' job responsibilities can be used as a main source of distinction between insider and outsider attacks.

Through its assumption that all user activities are recorded by an organisation's IT systems, this chapter enhances the analysis process of computer investigations to improve the process of distinction between insider and outsider attacks. It also

provides corporate security investigators with the necessary information and technology that can help them conduct their investigations.

Chapter 4: Digital Analysis Model for Distinction between Insider and Outsider Attacks (DAMDIOA)

This chapter discusses the limitation of the DFRWS method and the processes involved in the DAMDIOA model including collection, examination, analysis, presentation and decision. It also discusses timeline and relational analysis, used to examine these legitimate and suspicious activities and identify the relationship between activities performed during attacks and users' job responsibilities. This chapter proposes two types of decision.

Chapter 5: Experiments

This chapter aims to test the hypothesis by conducting eight experiments covering all possible attacks. The results of these experiments are based on fixed and tailored decisions are compared. This chapter supports the possibility that insider and outsider attacks can indeed be distinguished.

Chapter 6: Evaluation and case studies

The experiments results based on current methods of distinguishing between insider and outsider attacks (authorised access, attack within an organisation's control and location of initiation attack) and the proposed method of legitimate activities are compared as are DAMDIOA and the other models. This chapter outlines the real cases with which this model was used to deal, and discusses DAMDIOA's limitations.

Chapter 7: Recommendations

This chapter makes many recommendations that would enhance the process by which organisations' users are authenticated and the audit logs of security events. It also suggests that developing a physical and logical management log will

facilitate the process of distinction between insider and outsider attacks. These recommendations will lead to improvements in this process.

Chapter 8: Conclusion

This chapter presents this thesis findings and makes suggestions for future research, including classification and relative weighting of activities, developing DAMDIOA into an automated investigation tool and standardising ways of identifying and collecting user's job responsibilities.

2 Insider and Outsider Attacks and Digital Incident Investigations

Objectives:

-
- to introduce network infrastructure
 - to define insiders and outsiders
 - to identify the main distinguishing issues between insider and outsider attacks
 - to introduce the shortcomings of current digital investigation models
-

The chapter that follows aims to give a detailed review of the existing literature concerning insider and outsider attacks, and how they occur in the interconnected world, and to look at the kind of evidence that may be left behind for the computer investigator to find but which may not be enough to distinguish whether an insider or outsider attack has been made. The main aim is to present the research that has been conducted until now, and to introduce the shortcomings of current models of corporate computer investigations or digital investigations.

2.1 Network infrastructures

Corporate security investigators must familiarise themselves with the infrastructure of private and public networks as well as the threats to components of the Internet and Local Area Networks (LANs), in order to understand potential digital crime scenes. It is necessary for investigators to understand the advanced methods of attack used by outsiders to exploit the weaknesses of the Internet and thus gain insider access without detection from the organisation's security network.

2.1.1 Public networks (Internet)

The first type of network infrastructure to consider is the public network (Internet). In order to comprehend threats to the security of the Internet, it is essential that the investigator first gains a solid knowledge of the components of the Internet [53, 30].

2.1.1.1 *The components of the Internet*

The main components of the Internet are the backbone, Network Access Points (NAPs), Internet Service Providers (ISPs) and the Domain Name System (DNS).

- **The Backbone**

The first component of the Internet is the backbone. The Internet is defined as a packet-switched network that consists of a number of private networks, machines and users connected together [30]. It is not controlled by a single authority, country, government or organisation, but there are many groups involved in the infrastructure and management of the Internet, such as the Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA). The Internet is usually a very high-speed connection of networks and it has three main components, as listed below [30]:

- **Network Service Providers (NSPs):**

- an NSP provides national and international interconnecting Internet services to Regional Network Providers and large ISPs;

- **Long Distance Carriers (LDCs):**

- LDCs are responsible for the physical network of communication channels for the Internet and voice/data applications. The general method would be for an NAP to contract with an LDC to provide the channels for Backbone communication;

- **Network Access Points (NAPs):**

The second component of the Internet is the NAPs. These are the actual method by which ISPs and NSPs are connected.

- **Internet Service Providers (ISPs)**

The third component of the Internet is the ISP. An ISP is responsible for connecting actual users to the Internet.

- **Domain Name Systems (DNSs)**

The fourth component of the Internet is the DNS. This is responsible for translating Internet numbers (Internet Protocol (IP) addresses) to Web names. The organisation that keeps track of all the names and numbers associated with the DNS is IANA. In fact, IANA works as the main coordinator for the assignment of IP addresses, and manages the Root Domain Name System.

2.1.1.2 Applications (activities) of the Internet

The Internet has five main applications as follows [30]:

- **Email:** this application allows the composing, sending and receiving of electronic mail;
- **News:** newsgroups are specialised forums in which users with common interests can exchange messages;
- **Remote login:** users on the Internet can log on to any machine on which they have an account by using the ssh;
- **File transfer:** users can copy files from one machine on the Internet to another by using the SFTP program;
- **World Wide Web (WWW):** it allows a site to set up a number of pages of information containing text, pictures, sound and video, with embedded links to other pages;
- **Virtual Private Network (VPN):** it creates a secure communication between two or more computers over the Internet;
- **Voice over Internet Protocol (VoIP):** this application allows to make voice telephone calls and video-conference over the Internet such as Skype [71];
- **Bit torrent:** this peer- to- peer file sharing application allows to transfer large files [67].

2.1.2 Local Area Networks (LANs)

The second type of network infrastructure is the private network. Investment in IT infrastructure provides organisations with a number of significant advantages, such as high quality services, sharing of resources and reduced costs. Therefore, organisations create their own private networks, otherwise called Local Area Networks (LANs). A LAN is defined by Gojzman and Rawles [30:12] as “A combination of hardware and

software technology that allows computers to share a variety of resources such as printers, data, application programs, and storage devices”.

2.1.2.1 The components of a LAN

Basically, there are three main components of a LAN: network hardware, software and media. This section illustrates these components [30; 45; 54]:

- **Network hardware**

The first component of a LAN is network hardware. The hardware contains two main parts:

1. a **Network Interface Card (NIC)** which is installed for each server, client and device. An NIC is the primary requirement of every network device, such as the client workstation, the server hosting the resource and the router. The NIC’s job is to transfer data between a client or server and the shared network media. Moreover, an important function of the NIC is to listen to frames with their MAC address.
2. a **wire centre** which is a physical link by which all network devices, such as hubs and switches, connect with each other. A wire centre manages the network as segments, and as a result each organisational department has its own signal segment.
 - i. A **hub** device is a connection point for network devices which allows them to connect with each other physically on a LAN. Nowadays, it is rare for organisations to use a hub. Security issues may arise when using a hub device.
 - ii. A **network switch** is a networking device that connects network nodes as network segments. It is sometimes called an intelligent hub. A switch usually has a table that contains a MAC address for each node. Moreover, each port in a switch is independent as a virtual LAN. It appears that a switch is more secure than a hub because of reduced broadcast.
 - iii. A **router** is a network device that is responsible for moving data between different network segments and examining packet headers to determine the best routes for packets to travel. It recognises paths to all the

segments on the network by accessing information stored in the routing table.

- **Network software**

The second component of a LAN is network software. There are two types of software in a LAN: network protocols and operating system architectures. This software runs on a client computer used by the user to access the network's resources, and then on network devices to allow them to be shared.

- **Operating systems architectures**

There are actually two kinds of network operating system architecture (NOS) in a LAN: peer-to-peer and client/server. Today, most LANs use client/server NOS because of scalability, centralised management and security issues [54]. This research concentrates on client/server NOS because it has become a standard model for networking [54]. The computer in a LAN is either a client (requester) or a server (provider). A client is an authorised user's computer which can request data or services from an organisation's server. A server is the provider of services or data to the client, such as mail and directory service servers. Table 1 outlines the principal services that are provided by a server.

Table 1: A server's main services

Server	Service
FTP	Transferring data from one computer to another through a network
DHCP	Assigning a private IP to an organisation's clients
Network address translation (NAT)	Hiding a private IP address
Active directory	Database containing computer details, names and services
Mail	Transferring electronic mail messages from one computer to another
Web	Accepting HTTP requests from web clients (browser)

- **Network Protocols**

As a precondition for smooth communication between two computers, there must be agreed methods of communication. The protocol that all hosts on the network use is Transmission Control Protocol/ Internet Protocol (TCP/IP). TCP/IP has four layers, as illustrated below [53; 54]:

1- Application layer: this layer is responsible for providing services and utilities that allow applications to access network resources, such as Simple Mail Transfer Protocol (SMTP). SMTP will be discussed later because an email abuse will be selected for experiment in this thesis to represent a method of computer attack.

SMTP is a protocol which operates over Transmission Control Protocol (TCP) port 25, which transfers mail across the Internet. It comprises three main components [94]:

- 1- a Mail User Agent (MUA) which is an SMTP client that allows a user to send and receive email;
- 2- a Mail Transfer Agent (MTA) which is an SMTP server that allows emails to transfer from one MTA to another;
- 3- a Message Store (MS) which is a server that enables emails to reach their final destination and be dumped in a user's mailbox.

2- Transport layer: this layer is responsible for delivery and end-to-end communication. There are two kinds of transport layer protocol:

- Transmission Control Protocol (TCP) which provides the functions of connection-oriented communication using features such as three-way handshaking and sequence and acknowledgement numbers. Sequence numbers are used in TCP headers and allow hosts to identify packets sent and received. Acknowledgement numbers (ACK) are also used in TCP headers and allow two hosts to be given a receipt of delivery. Connections between two hosts are always in open status. There are two kinds of open status, i.e.:
 - passive open for a host ready to receive data
 - active open for a host ready to establish communication

An established connection is called a three-way handshake or three steps. The three-way handshake is between a source and a destination. The first step is when a source sends an initial packet called a synchronized packet (SYN) and a sequence number to a destination host to start to open a connection. The second step is a response from the destination that sends SYN/ACK (ACK is an initiating packet) to the source. The final step takes place when the source responds with ACK. The connection is then open and data is transferred until the communication is terminated.

- User Data Protocol (UDP) provides an unreliable connection and there is no guaranteed way of acknowledging the delivery data. It also provides connectionless communication, but it is a faster connection. Table 2 summarises the differences between the two protocols.

Table 2: Differences between transport protocols

TCP	UDP
Connection-oriented	Connectionless
Reliable	Unreliable
Slow	Fast

Port: is defined as a “*logical connection place, specifically using the Internet’s protocol, TCP/IP, as the way a client program specifies a particular server program on a computer in a network [15]*”. Port numbers are located in the TCP or UDP header. They can be assigned to specific functions or applications. There are three kinds of port number:

- 1- Well-known ports are assigned to specific applications. These ports are controlled, defined and maintained by IANA [39]. The range of these ports is from 1 to 1023. Table 3 gives several examples of common, well-known port numbers and services.

Table 3: Examples of well-known port numbers

Port number	Services
20 & 21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP
143	IMAP

2- Registered Ports can be registered to a specific function but are not controlled by any authority. The range of these ports is from 1024 to 49151. Table 4 summarises several registered port numbers and services [39]:

Table 4: Examples of registered port numbers

Port number	Services
1033	Local net info port
1036	Nebula secure sequence transfer protocol
1038	Message tracking query protocol
1155	Network file access

3- Private ports or dynamic ports: Any user can use them. They range from 49152 to 65536.

Corporate and public investigators should be aware that many ports can be security threats in networks. There are several Trojan horse programs that use specific ports. Table 5 shows several of the critical port numbers which can be exploited by outsiders or insiders.

Table 5: Examples of security threats

Port number	Type of Port	Trojan program
1243	Registered	Sub Seven
12345	Registered	NetBus
31337	Registered	Back Orifice
54320	Private	Back Orifice 2000

3- Internet layer: this layer is responsible for encapsulating transport layer data into packets, and then addressing and routing them. There are three main types of Internet layer protocol:

- Internet Protocol (IP) addresses and routes packets between hosts and networks;

- Address Resolution Protocol (ARP) resolves an IP address to an MAC address of a host located on the same physical network;
- Internet Control Message Protocol (ICMP) sends messages and reports errors regarding the delivery of a packet.

It is very important for digital investigators to understand fully the structure of an IP address in order to find a particular host on a private network. IPs are numerical identifications (logical addresses) that are assigned to a particular computer. They are divided into two parts: networks and hosts. The network part is what is used to identify the network that the host belongs to, whereas the host part is used to identify the specific host on the network.

There are two kinds of IP address: public and private. Public IP addresses are registered with the Network Information Centre (NIC) and are used on the Internet (public network). There are five classes of public IP address, as illustrated in Table 6 below:

Table 6: IP address classes

Class	Value	Explanation
A	01-126	First 8 bits define the network and 24 define the host
B	128-191	First 16 bits define the network and 16 define the host
C	192-223	First 24 bits define the network and 8 define the host
D	224-239	Used for multicasting
E	240-247	Used for experimental functions

On the other hand, private IP addresses are issued by IANA. They are never used on the Internet, but private addresses are used in a LAN to address the lack of public IP addresses. Private addresses have three classes, as illustrated in Table 7 below:

Table 7: Private IP addresses

Class	Value	Number of networks	Number of hosts per network
A	10.0.0.0	1	16,777,214
B	172.16.0.0	16	65,534
C	192.168.0.0	256	254

4- Link layer: this layer is responsible for sending data into the physical network and receiving data from the physical network.

- **Network media**

The third component of a LAN is network media. The media is responsible for the physical connection between network devices, and transmits data between nodes.

2.1.2.2 A LAN's security controls

Dhillon [22] and Melara and Sarriegui [50] explain that organisations have three types of internal security control: formal, technical and informal. However, when one of the three kinds of control measure is not correctly implemented, an insider can pose a major risk to an organisation's resources [22; 23].

1. **Formal controls:** the network security controls are responsible for establishing a proper security policy and procedure to ensure that data integrity, confidentiality and availability are maintained. The security policy should include steps to secure the network, the procedure for hiring and firing employees, equipment to be used and action to be taken in the event of incidents.
2. **Technical controls:** the technical security controls are the tools and techniques responsible for protecting the system from attacks and recording suspicious activities at the technical level, such as IDS antivirus software and access control [13; 21; 26; 62].
 - **Firewall:** computer software or hardware that enforces a boundary between two or more networks;

- **Remote authentication access server:** this is responsible for authenticating and allowing an organisation's users to gain access to that organisation's resources on the LAN from a remote location
- **Intrusion Detection Systems (IDS):** these systems employ different techniques to attempt the detection of intrusion into a computer or network by observation of actions, security logs or auditing data. While an IDS is used primarily to identify incidents and raise alerts, once an incident has occurred it can be used as an evidence-gathering and logging tool. There are several IDS techniques two examples of which are:
 - **Anomaly detection model:** a model whereby intrusion is detected by looking for activity that is different from the user's normal behaviour. An anomaly-based detection system is responsible for ascertaining a baseline of legitimate activity according to which different types of traffic go across the network as intended for access to a specific system and this therefore amounts to normal working conditions;
 - **Misuse detection model:** this model is responsible for detection of intrusions, by looking for an activity that corresponds to known intrusion techniques or system vulnerabilities (role based detection).
- **Network traffic:** a network sniffer tool that is able to record the header and content of network packets. It is responsible for capturing the full communication stream;
- **Access Control List (ACL):** ACL is a packet filter that compares a packet with a given set of rules;
- **Auditing:** systematic observation of the log files of network devices, scanning for details that can identify the use of network resources;
- **Network forensics:** the process of determining how an attack took place and the amount of damage caused, along with the process of gathering evidence to prove damage

3. **Informal controls:** these controls are responsible for educating and increasing the awareness of employees.

2.2 Security threats

It is fundamental that corporate security investigators are able to comprehend security threats against the Internet and LANs. These threats allow outsiders to gain inside access, with the possibility that they can bypass the security mechanisms put in place by organisations. In order to collect potential evidence, investigators must understand the methodology and techniques used by outsiders to exploit the weaknesses of a system. Graves [34] recognises security threats as situations that could lead to serious breaches of computer security. An exploit is needed in order to create a computer threat. This is a piece of software that takes advantage of a bug, or vulnerability, leading to unauthorised access, privilege escalation or Denial of Services (DoS) on a computer system [34].

There are two types of exploit: remote and local. A remote exploit runs over a network and exploits security vulnerabilities without any prior access to the vulnerable system, whereas a local exploit needs prior access to the vulnerable system to gain increased privileges. Furthermore, vulnerability is defined as the existence of a flaw in the software, logic design, or implementation that can bring about an undesirable event in the form of giving bad or damaging instructions to the system [34]. In general, security threats are categorized as being either intentional or accidental [85]. The aim of this research is to focus only on intentional threats. Intentional threats are deliberate actions with the intent of harming and damaging an organisation's information. They are divided into passive and active attacks. Based on the purpose of this research, security threats to an organisation's systems are divided between the Internet and LANs, as follows:

2.2.1 Internet threats

An Internet threat refers to any criminal method that takes advantage of online services, and examples include e-mail spam or harassment, illegal access to private networks, spoofed web pages, identity theft, and spoofed DNS and web banking. Research conducted in 2006 showed that 60 per cent of homes in the UK had Internet access [96]. In

2004, this figure was 49 per cent and in 1999 it was only 13 per cent. The same research showed that, in June 2006, 72.6 per cent of all Internet connections in Britain were broadband connections [96].

As the number of Internet users worldwide continues to grow, so too will the accounts of cyber-related criminal activity [79]

The wide use of broadband connections enables the user to be online during the whole day; in addition, it allows many users (outsiders) to perform the following tasks:

- locate a potential target (specific organisations and users)
- search the Web in order to discover tools that can be employed in an attempt to compromise an organisation's network
- exploit the lack of authentication services on the Internet, e.g. to create a fake website;
- target routers by injecting false routing data. Because backbone routers do not hold any default routing, a data border gateway protocol is used to learn new routes dynamically. A router can be attacked from a LAN. The outsider can inject data into routing tables, because the Routing Information Protocol (RIP) uses UDP packets for exchange of data and does not have any built-in authentication mechanism;
- target ISPs to reach the maximum number of potential targets in the shortest possible time. This attack will provide outsiders with the user data of an organisation, such as user names, passwords and IP addresses;
- target the DNS (this attack will be illustrated in Chapter 3) ;
- gain remote illegal access (such as insider access) to an organisation's resources by stealing a laptop belonging to that organisation.

Therefore, because no single body controls the Internet, outsiders can obtain insider information in a number of ways, such as by creating fake websites. This method prevents audit trails and log files from detecting their abnormal behaviour.

2.2.2 Threats to a LAN

These threats allow outsiders to gain insider information by, for example, updating a routing table with false information [76]. This false information redirects an insider's computer to an outsider's computer. Security threats on various LAN components may be manifested as follows:

- **at wireless network level**
 - easy to deploy unauthorised wireless access point
 - encrypted messages can be easily sniffed
 - private networks could be abused by any attackers
- **at cabling level**
 - information that can be read by an eavesdropper
 - cabling that can cause denial of service if disconnected
- **at NIC level**
 - an attacker who can modify the options of an NIC to listen for all frames regardless of the recipient's MAC address (use of sniffers)
- **at hub level**
 - anyone who can plug their computer into a physically unsecured hub to listen to the network
- **at switch level**
 - MAC flooding
 - table overflowing
 - ARP spoofing
- **at router level**
 - routing tables that can be falsely updated by an attacker
 - IP spoofing
 - replay of IP datagram
 - misconfigured access control decisions at the router level

After the infrastructure of private and public networks has been discussed and the threats of these networks identified, it is necessary to comprehend the differences be-

tween insiders and outsiders in order to identify potential e-evidence. The potential e-evidence is extracted from a sequence of an insider's activities.

2.3 Computer-related attacks

Computer attacks appear when a computer is compromised as a result of its vulnerability. Attackers usually employ special methods or tools to find a system that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the system to prevent an attack [34]. Additionally, Stallings [85] has classified security attacks into four main types, as follows:

- **interruption:** directed at making a computer system become unavailable, for example through destruction of a piece of hardware
- **interception:** levelled against the confidentiality of a computer system, such as when an unauthorised user gains access to a system by using wiretapping, for example, to capture data in a network
- **modification:** made against the integrity of a computer system, when an unauthorised user tampers with the system, for example by altering a program so that it performs differently
- **fabrication:** directed against authenticity, when an unauthorised user inserts counterfeit objects into the system, such as the addition of records to a file

These attacks are divided into two types: active and passive [85]. Active attacks involve the direct theft of information, software and hardware, and sabotage and destruction, whereas passive attacks are in the nature of eavesdropping on, or monitoring of, the transmission of data. Nowadays, computer-related attacks are being designed increasingly to obtain information silently without leaving any damage to be noticed by a user. The purpose of attacks of this kind is to escape detection so that they remain on host systems for long periods of time [104]. A malicious code hosted on websites is one of the main forms of advanced attack. Finjan Inc. analysed, from Internet traffic recorded in the UK in 2007, more than 10 million unique websites, and it found that [104]:

- advanced attack methods that employ code obfuscation through various randomisation techniques are becoming more sophisticated, making them invisible to pattern-matching/signature-based methods used by antivirus software;
- attackers are displaying a growing level of sophistication when embedding malicious codes within legitimate content.

Another form of advanced attack is identity theft. This method exploits organisations' inadequate computer security practices [104]. In 2005, personal and sensitive information for 310,000 U.S. citizens was stolen in a security data breach that involved 59 instances of unauthorised access to its corporate databases using stolen passwords [104].

Furthermore, threats to an organisation's systems or networks are posed by attackers who are referred to as 'threat agents'. These attackers are persons or groups who, with malicious intent, deliberately use their capability to disable or damage an organisation's systems. There are two types of attacker: "insiders" and "outsiders". Vidalis and Jones [99] maintain that insiders (employees) and outsiders (crackers) have the same hostile intention towards the system. They also state that outsiders are the more dangerous threat to a computer system, because they have the knowledge and motivation to perform active attacks and the capability to create the opportunities needed in order to carry out attacks. However, Magklaras and Furnell [49] believe that insiders represent the more dangerous threat to their own organisation, because they have authorised access, privileges to perform tasks and physical access to a target. This section therefore continues by providing overviews of insiders and outsiders.

2.3.1 Insider

An insider is defined by Vidalis and Jones [99] as "*a threat agent who is directly or indirectly employed by an organisation, and has access to the system or sensitive information not otherwise disclosed to him and to the general public*". Walton [101] notes that authorised access, enabling insiders to commit crimes or breach an organisation's policies, is also essential to enable them to perform their jobs. Moreover, insider attacks can be perpetrated by full-time and part-time employees alike, as well as by temporary employees, contractors and auditors.

Numerous attempts have been made to define an insider with malicious intent and to identify their distinguishing features. Schneier [77] recognises a malicious insider as being an employee who is an expert who designed the system against which he is now committing an attack. However, Schultz [78] defines an insider attack as the intentional misuse of a computer system by an individual who is authorised to access the organisation's computers and networks. It appears that the majority of definitions of insiders agree that their main distinguishing feature is their authorised access to an organisation's IT facilities, whereas there is debate about other features of insiders, such as their possession of technical computer skills.

According to Schneier [77], computer skills and knowledge of an organisation's IT facilities are the main features of insiders who commit crimes. In addition to skills, Rowlingson [74] extends the features of insiders to include knowledge of, and privileged access to, the resources under the control of an organisation. On the other hand, Schultz [78] and Randazzo *et al.* [68] report that technical skills are not always necessary to commit a crime. They claim that authorised access to an organisation's IT facilities and the intention to commit a crime are the main features of insiders. Furthermore, Randazzo *et al.* [68] support the view that computing skills are not always particularly important in this respect, by finding that 87 per cent of internal incidents in the banking sector used simple user commands and that technical skills were not required. Moreover, Rasmussen [69] states that many sophisticated password cracking tools have been created that can assist a technically unskilled person to increase their privileges and gain unauthorised access to a computer system.

Therefore, the current researcher defines insiders as trusted individuals who have been hired by an organisation and gained authorised access to their organisation's IT resources (facilities) in order to perform their particular job responsibilities/roles. However, their authorised access (insider access) can be deliberately abused to violate the policies of the organisation or commit computer crimes. These abuses could include information theft, modifying data, downloading pornographic images or sending harassing emails.

2.3.1.1 *Types of insider*

As mentioned previously, there is some debate about computer skills being the main feature that distinguishes insiders. This feature depends on the type of insider under consideration. Many types of insider are classified based only on their technical skills.

The first categorisation of insiders was attempted by Anderson [5] and concentrated on technical skills only. This comprised masqueraders and legitimate and clandestine users. A masquerader is an insider, with or without full privileged access to an organisation's IT resources, who wishes to exploit another authorised user's ID and password. Threats to IT by legitimate users involve the misuse of authorised access to the system and its data [5]. An example arises when an insider uses his legitimate privilege to gain access to information he is not normally authorised to access in the course of his day-to-day activities. A clandestine user is related to insiders by his ability to bypass audit and access control mechanisms in a specific system [5]. Anderson's categorisation is debatable because it was based only on the difficulty of detecting insiders' activities through audit trail data.

However, advanced categorisation techniques have been designed based on various features of insiders, such as knowledge and intention. Magklaras and Furnell [49] have developed the categorisation of insiders into three levels with regard to their sophistication as end users (based on insiders' capabilities and knowledge). The first level is advanced; these insiders have high levels of skill and privileges such as that of a network administrator. The second level is ordinary; these insiders have an intermediate level of knowledge of certain applications, such as that of a database administrator. The third level is novice; these insiders know only a little about computer software and hardware.

2.3.1.2 *Insider attacks/abuse*

Insider attacks, such as stealing information, embezzlement, email harassment and sabotage, are believed to be the main form of breaching and violating the IT policies of an organisation [60]. Nykodym *et al.* [62] assist organisations in understanding the types of insider who are likely to commit net abuse and/or cybercrime and the types of offence insiders may commit. These attacks can include espionage, theft, sabotage and personal abuse of the organisation's network. There is some debate here, because no distinction

is made between hardware theft and information theft. There are usually two forms of insider theft: information theft (e.g. stealing sensitive information) and hardware theft (e.g. theft of a laptop). This distinction is necessary for identifying the methodology of the attacks and establishing whether they have been carried out locally or remotely. Furthermore, Stanton *et al.* [86; 87] propose six categories of insider behaviour based on two dimensions: intention and technical skill. The six categories are as follows:

1. Intentional destruction: this requires both technical skill and a strong intention to harm the organisation's IT facilities. For instance, a user obtains an employer's protected files to steal a trade secret.
2. Detrimental misuse: this requires no technical skill, but nonetheless includes intention to harm through annoyance, harassment, rule breaking, etc.; for example, using a company email system for sending spam messages that market a private business.
3. Dangerous tinkering: this requires only technical skill and no intention to harm the organisation's IT facilities. For instance, an employee configures a wireless gateway that allows wireless access to the organisation's network by outsiders in cars passing by or parked in the vicinity.
4. Naïve mistakes: this requires neither technical skill nor intention to harm the organisation's IT facilities, e.g. choosing a weak password.
5. Awareness: this requires both technical skill and a strong intention to do good by preserving and protecting the organisation's resources. For instance, an employee discovers a backdoor on his PC by using the task list to investigate unusual hard drive activity.
6. Basic hygiene: this requires no technical skill and a clear intention to preserve and protect the organisation's IT facilities; for example, a skilled employee resisting an attempt at social engineering by refusing to reveal his password to an impersonating user.

It also appears that, at the present time, technical skill is not always necessary to commit insider crimes owing to the availability of complicated hacking software employed by unskilled insiders. Insider offences are also becoming increasingly

common because of the many features that allow the commission of such crimes. For example:

- insiders are authorised to access their organisation's IT facilities such as files and printers;
- they have physical access to a target;
- they are privileged to perform specific tasks (jobs);
- they have knowledge of where valuable resources are located[72].

The interesting point here is that many insider features are not limited to insiders, because the advancements of technology are rapidly changing the methods of outsider attacks. For instance, an outsider can bring the insider to his machine by luring him to it and downloading malicious software in order to gain insider access.

2.3.2 Outsiders

Blyth and Kovacich [11-:10] define an outsider as someone “*who gains unauthorised access to or breaks into computer-based information systems.*” This definition of an outsider is debatable, because it is believed that the main feature of outsiders is that they have no prior knowledge of the target. Walton [101] makes this claim. In fact, all outsiders have only a limited chance of carrying out their attacks against an organisation's IT facilities. They can gain access only by exploiting gaps or weaknesses in corporate protection systems [101]. Furthermore, advanced methods used by outside attackers focus on gaining unauthorised access rather than breaking into the organisation's network, this being in order to prevent the attacker's activities from being detected. A successful outsider attack requires at least three conditions [44]:

1. proper motivation
2. adequate technological skills
3. right opportunity

It appears that the changing methods of outsider attack have influenced the definition of an outsider significantly. Therefore, outsiders can be defined as users who gain unauthorised access (insider access) to an organisation's IT facilities, by having the ability to

bypass security mechanisms (no detection by a security mechanism) and with no prior knowledge of the facilities to be attacked.

2.3.2.1 Types of outsiders

There are three types of outsider [44]:

- curiosity seekers: motivation for attacks is to have fun or to show off;
- skilled hackers: outsiders targeting an organisation's IT for a specific reason. The attacks lead to data theft or corruption.
- elite attackers: outsiders who gain insider access and commit a crime, leaving no trace.

An outsider strives to gain insider access in order to use it to destroy data, deny service to authorised users and cause problems for the organisation [34].

2.4 The Issue of insider and outsider attacks

Since most security mechanisms focus on preventing outsider attacks from taking place, the only way of attacking an organisation's IT facilities would be through insider access [34]. Park and Giordano [64] state that *“Many security technologies have been invented to prevent threats from outsiders, but they have limited use in countering insiders' abnormal behaviour.”*

Because of the advancement of security mechanisms and defences for organisations, the old attack techniques, such as emails infected with malicious viruses and worms, are no longer effective. Ackerman [1] reported that, in the past, the main computer threats came from e-mails infected with worms and viruses. Nowadays, outsiders employ websites to carry codes designed to obtain information from an insider's computer [1]. Many codes are designed to download themselves automatically as soon as an insider accesses a Web page. Furthermore, other sites prompt the insider to accept what appears to be legal software but is in fact a malicious program [1]. For instance, insiders who browsed the MySpace and YouTube websites in 2005 and who had not patched their computers (i.e. their PCs were infected), found that, if they clicked on an advertisement or banner, that action silently installed Spyware on their computers to log keystrokes and capture usernames and passwords [1; 104]. The CRS Report for Congress found

that analysts at Google had reviewed a large number of web pages for the presence of malicious software, and identified 4.5 million web pages that were suspicious in this regard. More than a million were found to launch downloads of malicious software, collect sensitive data, and then email that data to a temporary email account.

Advanced methods of outsider attack focus on gaining insider access without leaving tracks. These methods lead to the involvement of insiders and may leave limited amounts of information (evidence) to distinguish between insiders and outsiders, this evidence being extremely hard to find. This is because the outsider aims to bring insiders to the outside of the organisation's security defences, or the outsider may initiate attacks that go behind the organisation's defences (inside the organisation) as follows:

1. **Local information theft** is a form of confidentiality attack (passive attack) but this kind of attack is hard to detect. Physical access to an organisation and use of suitable software or hardware is required to gain sensitive data, such as passwords, when the data travels in clear text across trusted networks. Therefore, outsiders can gain insider access by exploiting the following weaknesses [45]:
 - **Weak password:** sometimes a password configuration policy is lacking as part of an organisation's systems, resulting in an organisation selecting a weak password protocol or an insider being able to select a weak password (easy to guess) such as his wife's name;
 - **Weak access control to secret data:** poor access controls can create good opportunities for outsiders to gain privileged access to a target (file) and then delete, modify or read a file.
2. **Remote information theft** is launched by using malicious software such as a Trojan. This software is usually designed to steal sensitive data. It allows an outsider to control an insider's computer when the software is installed on that computer.

An interesting experiment took place in June 2006, when Stasiukonis was employed by a credit union to penetrate their network and confirm the threat of a social engineering attack. Twenty USB devices were placed in designated areas

frequently visited by the employees, such as smoking areas. The interesting content in each one of these USBs was a specially written Trojan program, planted in image files, which would email any employee's sensitive information, such as logins and passwords, to Stasiukonis. After three days, fifteen of the USB drives had been found by the company's employees, who tried to find out the contents of the USB devices by plugging them into their organisation's computers. Subsequently, the employees' user names and passwords were sent out to Stasiukonis. The actions of the employees, who were innocent users under no suspicion of any potential fraud, proves how easily social engineers can gain insider access [20].

3. **Spoofing** occurs over the Internet because organisations do not have control over the ISP, the public routers or the public domain name service (DNS) servers [76]. Outsider attacks can redirect a DNS server to lead an employee's computer to a false destination.
4. **The theft of hardware** such as laptops or disks may also present a good opportunity for outsiders to gain remote access to an insider's computer, once the organisation's devices are loaded with confidential information. The BBC reported that a memory stick with user names and passwords for a key government computer system had been lost and later found in a pub car park [10]. This proves that opportunities for an outsider to gain insider access can occur anywhere.

The main problem arises when an outsider has gained insider access or an insider denies carrying out an attack. This kind of attack needs special treatment, because it involves different parties (an insider and an outsider). The next section describes how corporate security investigators deal with different advanced methods of attack.

2.4.1 Advanced methods of attack (outsiders gaining insider access)

Once the attacker has gained insider access without detection and has employed an insider's computer to commit a crime against an organisation's IT facilities, they usually redirect the computer crime investigation to a different crime. Indeed, nowadays this type of attack is directly linked to money laundering, fraud, the accessing or distribution

of pornography, espionage or harassment [37]. A significant case of this type of attack is illustrated by Dataclinic [21]. A university professor was sacked after being accused of downloading pornographic images. The university's IT security found that 150 pornographic images had been downloaded by the professor. The professor's PC was examined by two computer forensic firms (third party). The first firm produced a report that supported the university's allegations. However, the second firm found that the professor was innocent and the incident had been committed by an outsider in order to incriminate him [21]. The university paid the professor £90,000 for unfair dismissal [21].

Furthermore, it is vital to know when an outsider might also be directly linked to terrorist groups, especially in countries that have been the victims of physical terrorist activities such as Saudi Arabia, India, the United Kingdom and the United States. A recent case of such an attack involving terrorism occurred in India in 2008 and was reported by the Guardian newspaper. Access belonging to an American user who worked as an expert in India was used by an outsider who was a member of a terrorist group in India. After the compromised computer was used to broadcast a large number of terrorist emails, these emails were tracked, leading to the American expert. Subsequently, an extensive computer forensic investigation was conducted which found that access to the American's computer had been gained by an outsider [100].

Such an attack is complicated. The reason for this complication is that no effort is put into identifying the features that can distinguish between insider and outsider activities.

2.4.2 Current methods of distinguishing between insider and outsider attacks

The revolution of the Internet and communication technology, and the extension of private networks, has led to constant changes in the methods of attack. In the past, outsiders found difficulties in identifying potential targets because of slow connection to the Internet and a different IP address being generated every time. However, with high speed, always-on Internet connections for the outsider, ISPs have created a new playing field for the outsiders, who just need time to be able to identify their potential targets. The ability of attackers to hide their identity can also create a difficult challenge for corporate security investigators.

Casey [12:9] stated that “*Criminals are using technology to facilitate their offences and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals*”. Gaining insider access is an advanced method of attacking the organisation’s facilities in order to prevent the abnormal behaviour of an outside attack from being detected and to hide the identity of the outsiders. As a result of sophisticated attacks, new challenges are arising for investigators in terms of distinguishing between insider and outsider activities. Owing to the rapid development of attack methods, making the distinction between insider and outsider attacks has become extremely difficult. As mentioned previously, the development of new attack methods influences insider features and those features are not only limited to insiders. Furthermore, the current methods of distinguishing between insider and outsider attacks are insufficient. These methods are described next.

2.4.2.1 Location from which attacks are initiated

One of the main aspects (or features) of distinction between insider and outsider attacks is the location of where the attack was initiated. Melara and Sarriegui [50] and Graves [34] claim that the difference between insider and outsider attacks is based on whether they were initiated from inside or outside the organisation. However, this statement is debatable because, as discussed previously, the revolution of the Internet and communication technology, and the extension of private networks, allow insiders to commit crimes against their own organisation from the outside, whereas the improvement of wireless networks and the advancement of hacking tools such as keystroke devices allow an outsider to commit a crime against an organisation from the inside. For instance, an organisation configures a wireless gateway that allows wireless access to the organisation’s network by outsiders passing by the organisation's premises.

Therefore, the outsider will be classified as an insider based on the location. However, from a computer forensics perspective, this is insufficient evidence and cannot support the assertion that it is possible to distinguish between insider and outsider attacks based solely on the location of the attack’s initiation.

2.4.2.2 Attacks within an organisation's control

Another way to distinguish between insider and outsider attacks is demonstrated by Walton [101]. He believes that insider attacks are within the organisation's control, whereas outsider attacks are not [101]. However, this distinction is inappropriate because when insider access is gained by an outsider, this attack is still within an organisation's control and he/she is classified as an insider. However, from the perspective of a corporate security investigation, the outsider's computer is not subject to forensic collection. Furthermore, the insider's personal computer is also not subject to forensic collection when the attacks are initiated from outside the organisation. Since the main aim of this research is to develop the process of computer incident analysis, gaining access to the log of interest is the first step in collecting appropriate evidence. Therefore, the insider's computer may be subject to collection, analysis and examination, whereas an outsider's computer is not.

2.4.2.3 Access

Authorised access is another aspect of distinguishing between insider and outsider attacks, as demonstrated by the majority of computer security experts [68; 74; 78]. They report that the most important difference between these attacks is that insiders have authorised access to an organisation's IT facilities whereas outsiders do not have such access. However, having authorised access is not always the best way of distinguishing between insider and outsider attacks, because insider access can be gained illicitly. As mentioned previously, as a result of the development of the Internet and communication technology, remote access to private networks is extended to be accessible to a company's employees from anywhere and at any time using, for example, a Virtual Private Network (VPN). However, when insider access is gained by outsiders, this access is shared between the insider and the outsider. As a result of having insider access, outsiders can easily access the organisation's IT resources without breaking into their private network. Therefore, security defences such as a firewall recognise an outsider as an insider. Consequently, the task of distinguishing between an insider and an outsider becomes extremely hard. Table 8 illustrates the main ways of distinguishing between insider and outsider attacks.

Therefore, an issue arises as to how to distinguish between insider and outsider activities when an insider denies carrying out an attack.

Table 8: Main methods of distinguishing between insider and outsider attacks

Current methods of distinction between insider and outsider attacks	Disadvantages	Example
Location of attack initiation	Classifies an outsider as an insider	Wireless networks and keystroke devices allow an outsider to commit a crime against an organisation from the inside.
Attack is within the organisation's control	Classifies an outsider as an insider	When insider access is gained remotely by an outsider, it is within the organisation's control.
Authorised access	Classifies an outsider as an insider	When an outsider gains insider access, with the capability to bypass the security mechanism, the outsider has authorised access.

Since this research focuses on identifying items that facilitate computer incident investigation for distinction between insider and outsider attacks, the next section of the literature review introduces state-of-the-art computer forensics and investigation, in particular, corporate computer investigation. It ends with a description of the shortcomings of current models of computer forensic investigation.

2.5 Computer forensics

Computer forensics is a new discipline based on both computer security technology and forensic science [59]. As mentioned previously in the section on a LAN's security control, computer security technologies are the tools and techniques that are responsible for preserving, detecting and gathering electronic evidence (e-evidence). On the other hand, forensic science is the application of science to the law. It involves the search for, and examination of, physical traces. The main principles of forensic science are as follows [59]:

- frozen crime scene in order to protect the integrity of the evidence
- chain of evidence

- record of all steps taken to reach the conclusion arrived at, in order to allow an independent party to review these steps.

Computer forensics concentrates on the investigation of computer-related crime and incidents of computer abuse [102]. Furthermore, the purpose of computer forensics is to discover, acquire, identify, analyze and preserve electronic evidence (e-evidence). Newman [59] recognizes e-evidence as information or data of some investigative value that is usually stored on, or transmitted by, a computer system such as emails, files, images and IP addresses. This e-evidence is as demonstrated below [59]:

- data are raw facts that can be processed by computing devices into relevant pieces of information such as a credit card statement;
- software is recognized as instructional coding that manipulates the hardware in a computer system such as Java;
- hardware is described as the physical equipment and attached devices used in a computer system, such as computers and printers.

However, the nature of e-evidence is fragile because the evidence is subject to alteration, damage or destruction under improper handling or examination [2]. For that reason, there are many conditions that apply to e-evidence before it can be rendered acceptable in court.

2.5.1 The principles of computer forensics

The principles are as follows [2]:

- no action taken by those undertaking computer forensic activities should change data held on a computer or other media, which may subsequently need to be relied upon in court
- an audit trail or other record of all processes applied to e-evidence should be created and preserved. A third party should be able to examine those processes and achieve the same result

2.5.2 The process of investigation into a relevant computer crime/incident

There are four main forensic procedures that should be followed in order to conduct the investigation, as indicated below [2]:

1. The collection process is responsible for the search, recognition, collection and documentation of computer based e-evidence. This phase involves both real-time and stored information which can be lost if the investigator does not take precautions at the scene.
2. the examination process is responsible for making the evidence visible and explaining its origin and significance. It should accomplish several things. It should document the content and the state of the evidence. This documentation allows investigators to discover what the evidence consists of. It includes the search for hidden information. Furthermore, physical computer evidence can be represented by physical items such as central processing units (CPU), chips, boards, media, monitors, printers, digital cameras and USBs. E-evidence, while stored on these physical items, is latent and exists only in an abstract electronic form. The result that is reported from an examination is the recovery of this latent information. Computer forensics requires adherence to certain methods to ensure the integrity of the data and information contained within those physical items.
3. The analysis process is a technical review that is within the area of expertise of the forensic professional. The analysis of evidence involves identifying the most appropriate software tools to be used. It might include a forensic toolkit, a file viewer for deleted and extant files, software for reading network logs, and hex editors.
4. The report outlines the examination process and the pertinent data recovered, and completes the examination.

2.5.3 The analysis of computer investigations

This section illustrates the different types of computer analysis, because this research aims to employ many types of analysis such as “timeline analysis” and “relational analysis” to distinguish between insider and outsider attacks. The analysis is the process

of observing the data and determining its relevance and significance to the specific case. There are several types of analysis, as shown below [43]:

2.5.3.1 Timeframe (timeline of activities) analysis

The timeframe or timestamp is the date/time stored or communicated by an electronic medium. Computer systems store timestamps in many different ways and according to different rules [103]. Timestamps are usually stored whenever a file is created, modified or accessed. Furthermore, most computer systems have logging functions that log activities on the computer with timestamps. The importance of timeframes or timestamps in digital forensics lies in establishing the correct sequence of events and associating a particular user to a time period. It is also a fundamental method of activity reconstruction during a case investigation [44; 103].

2.5.3.2 Data-hiding analysis

This analysis is used to search for data that may be hidden on the hard disk in order to hide the crime and the evidence. Files can be hidden in many ways on a computer system, such as hiding in plain view. This method of hiding allows the criminal user to give a file a name that makes it appear to be something it is not and something that an investigator would not be interested in.

2.5.3.3 Application and file analysis

This analysis is used to identify the kind of programs that the suspect is using, recognizing common file types used for specific purposes relevant to the investigation, and associating the files that have been located on the drive with particular software. A number of files can be associated with specific applications to identify the programs that are normally used. For instance, investigators could link files in a Temporary Internet Files directory to those used with Internet Explorer, whereas other files could be associated with email programs.

2.5.3.4 Functional analysis

This analysis is used to determine the capabilities of computers and users, and the proper working of the system during relevant time periods, and to understand an offender's motivation and intent [12].

2.5.3.5 Relational analysis

This analysis is used to identify relationships between suspects, victims and the crime scene. Relational analysis is useful in creating nodes that represent places those involved have been to, and email and IP addresses used by them, and to determine if there are connections between these nodes [12; 43].

2.5.3.6 Ownership and possession

This analysis is used to identify who has created, modified or accessed files on a computer in order to associate the existence of a file with the actions of users. For instance, when a user denies the creation of a specific file, this analysis is employed to identify who created that file and the last time it was accessed. This analysis is usually used in conjunction with timeframe analysis to observe when a particular person used the computer and had access to a particular file.

2.5.4 Types of computer investigation model

Ciardhuain [17] believes that the available models are general models of cybercrime investigation that concentrate only on part of the investigative process (dealing with gathering, analysing and presenting the evidence). These models are usually designed to assist public and corporate forensic investigations. Therefore, it appears that there are two types of computer forensic model: specific and general.

2.5.4.1 Specific models

These focus on improving just one computer forensic process by producing appropriate procedures or techniques in order to assist the investigation in its handling of e-evidence.

- The Good Practice Guide for Computer-based Electronic Evidence [2] provides guidance for public and corporate investigators with regard to criminal investigations involving computers and electronic devices. It is designed only to collect physical and electronic evidence at the crime scene, and to illustrate how to deal

with the computer(s) at the crime scene when they are switched off or on. It is useful for collecting volatile evidence at a crime scene.

However, the Practice Guide does not focus on the analysis process, and does not provide the investigation with suitable tools for data collection, for example, the tools that can be used to image a suspect's hard drive.

- The Technical Working Group for Electronic Crime Scene Investigation [6] is also wholly designed as a procedure for improving the collection process. This procedure deals with the recognition, collection, preservation, transportation and storage of e-evidence. It provides the investigation with the location of evidence for specific crimes.

However, it has the same shortcomings as the Good Practice Guide for Computer-based Electronic Evidence. Furthermore, there are no instructions on how to collect volatile data.

- The Digital Forensic Research Workshop (DFRWS) [63] has proposed a model for computer forensic analysis, but it has not yet been completed. The main advantage of DFRW is that it is one of the first large associations for this purpose that is led by academia rather than law enforcement [63]. It focuses the direction of the scientific community towards the challenges of digital forensics [63]. However, the DFRW model is just a basis for future work [70].
- The International Association of Computer Investigative Specialists (IACIS) [92] has focused on the process of computer forensic examination by developing a guide for forensic examinations. This guide provides useful information about the examination of the OS and file systems, such as FAT and the location of the most important evidence. However, proper examination tools are not provided. IACIS's guide focuses on passive examination of the target or suspect computers only.

2.5.4.2 *Generic models*

These are concerned with appropriate procedures including guidance on how to conduct all the processes of computer forensic investigation (reporting a crime and collecting, examining, analysing, reporting on and presenting the evidence).

- Casey [12] has proposed a very general framework for dealing with computer crime on network layers and standalone systems. It describes how to collect, examine and analyse data. This model is designed to ensure appropriate evidence handling and reduce the chance of mistakes being created by other potential pitfalls;
- Ciardhuain [17] has proposed an extended model for cybercrime investigation by addressing certain activities such as presenting the information flow in an investigation and capturing its full scope, rather than merely processing the evidence. This model assists the development of modern investigative tools. Although this model is generic, it concentrates on the management perspective. Investigative tools for conducting investigations are not provided.
- Haggerty and Taylor [37] have provided a framework for the management of computer forensic facilities and activities within a corporate setting. This framework demonstrates how to conduct computer forensic investigations within an organisation by means of procedures including coverage of how to secure evidence, how to preserve the integrity of the evidence and how to produce an audit trail for all the forensic steps that have been taken in order to reach the final conclusion. However, the framework provides guidance on managing forensic investigation tasks rather than being a comprehensive guideline for forensic computer examination.
- Mitropoulos *et al.* [58] have also proposed a management framework with a structured methodology that includes practices for handling security incidents. Their management framework discusses how to identify the source of an attack by using both passive incident response procedures (such as examining the sys-

tem log) and active incident response procedures (such as examining the computer domain and the network).

- Windows [52] provides useful guidance for conducting computer investigations for Windows platforms. This guideline identifies the location of evidence and suitable tools for recovering data. However, it is not suitable for distinguishing between insider and outsider attacks.

Table 9 explains the process of computer forensics for both general and specific models

Table 9: Process of computer investigation for general and specific models

		Process of Computer Forensics				
Models of Computer Investigations		Collection	Examination	Analysis	Report	
General Models	Casey [12]	X	X	X	X	
	Ciardhuain [17]	X	X	X	X	
	Haggerty and Taylor's framework [37]	X	X	X	X	
	Windows [52]	X	X	X	X	
	Model proposed by Nelson <i>et al.</i> [60]	X	X	X	X	
Specific Models	DFRWS [63]			X		General framework for analysis
	Technical Working Group for Electronic Crime Scene Investigation [6]	X				
	ACPO[2]	X				
	IACIS [92]		X			

2.5.5 Corporate security investigations

A corporate computer investigation is defined by Wang *et al.* [102] as an investigation that can be conducted by an organisation, without the involvement of law enforcement agencies, in order to deal with violations of the organisation's policies or for purposes of civil litigation. The investigation should be able to deal with insiders so as to prove that a crime has been committed and, if so, to identify the insider. It is often the case that an electronic crime has been committed and the guilty party (the insider) needs to be identified.

A corporate computer investigation is usually required to reveal e-evidence, from networks or computers, that may be destined for use in court. Nowadays, organisations are increasingly making use of computer forensics and investigation in areas such as fraud, accessing and distribution of pornography, and harassment cases [37]. An organisation's computers, servers and laptops are increasingly becoming targets of crime, as well as being potential tools for committing crimes, or a repository of information used or generated in the commission of a crime [37].

However, the lack of forensic readiness is a serious challenge that faces corporate computer investigators when dealing with e-crime [42; 37; 81]. For instance, research into computer security in the private sector in Saudi Arabia has demonstrated that the detection and identification of the source of attacks is limited. However, the proportion of crime detection without identifying the source of an attack is high [3]. Kent and Ghalvalas [42] believe that organisations are usually slow in recognising the importance and implications of computer-based evidence.

Based on the above discussion, it appears that organisations still find difficulty in dealing with traditional crimes, such as breaking into the system. Therefore, they have yet to consider advanced methods of attack by outsiders. There is still no investigation model in existence that can distinguish between insider and outsider attacks in an organisation. Thus, when addressing the lack of forensic readiness within organisations, it becomes clear that little effort has been made to improve forensic capability within organisations.

2.5.5.1 The issue for corporate security investigation of distinguishing between insider and outsider attacks

Based on the above discussion, it can be said that outsiders exploit the weakest link in an organisation's computer security chain, namely that of authorised users/insiders, to gain unauthorised access to an organisation's system. It appears that the methods of attack have become extremely sophisticated in recent years, since outsiders are able to take their insiders (victims) outside the organisation's network security (beyond the organisation's control). Such an attack assists the outsider in gaining insider access while hiding their abnormal behaviour and their identity. Figure 4 illustrates the problem of insider and outsider attacks. An outsider used insider access to access an organisation's computer. Then an abusive email has been sent to a worker. The co-worker reported this incident to an IT security department. After that, an insider's computer was collected and analysed. The evidence supported that the email had been sent by an insider, whereas the insider refuted this allegation. Finally, the wrong decision was made based on the incorrect evidence.

1. On the other hand, it appears that the above model of computer investigation is usually designed to deal with traditional old-fashioned computer attacks, such as breaking into networks or computer systems. The single largest gap in the current models is that they do not focus on the distinction between insider and outsider attacks. These models focus on incorporating the requirements of legal systems into IT systems in order to conduct proper computer forensic investigations. Casey [12] has stated that every investigation is unique and can bring about unforeseeable challenges. Therefore, because these models do not focus on the distinction between insider and outsider attacks, they do not provide investigators with the proper requirements for distinguishing between those types of attack, as follows:
 - what type of data is to be collected?
 - which tools should be used to collect the data:
 - which procedures should be followed to analyse the data?

Furthermore, another critical gap in the current models is that little effort has been put into the process of computer analysis [103]. From examining cases of outsider and insider attack, it is clear that there is no computer forensic analysis tool for dealing with the distinction between insider and outsider attacks. This is because, as in the case of the university professor mentioned above, two totally opposing conclusions can be reached. Unfortunately, these issues mislead investigators who are performing *ad hoc* investigations with the aim of distinguishing between insider and outsider attacks, because no specific analysis model for that distinction exists to guide the investigation towards collecting proper evidence. The consequence of this is an increased chance of mistakes being made in identifying the right suspects, which could lead to the mishandling of evidence and putting the organisation into a financially disadvantageous situation and negative publicity.

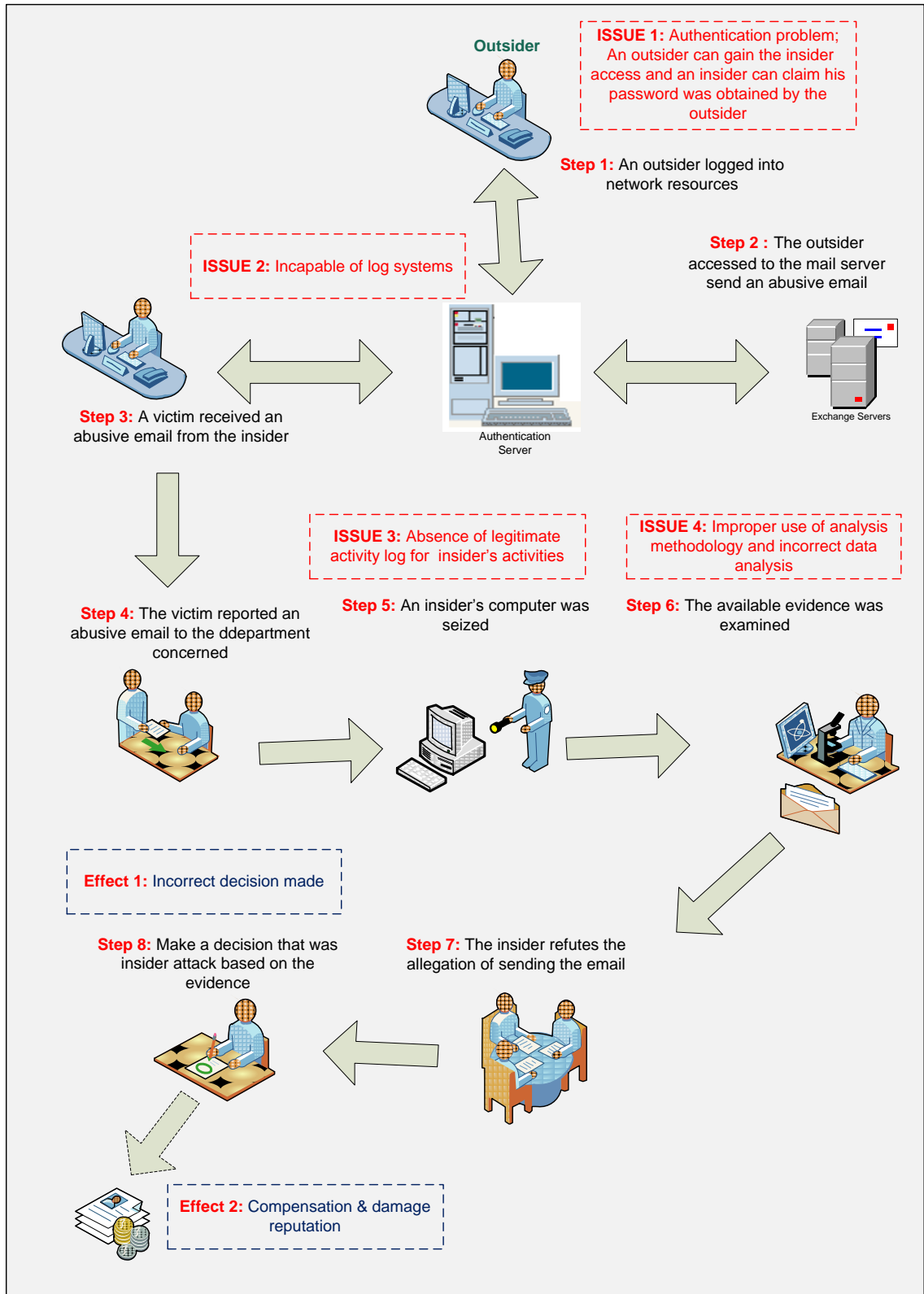


Figure 4: Issue of Insider and Outsider Attacks

2.6 Summary

Based on the literature review, it can be concluded that the difficulties in distinguishing between insider and outsider attacks, when an insider denies carrying out an attack, fall into five main categories as follows:

- 1- Intensive research on a distinction between insider and outsider attacks has not yet been conducted.
- 2- Advanced technology, if possessed by a skilled attacker, significantly influences the methods used for gaining insider access without detection. As a result of insider access being gained by someone with the ability to bypass the security mechanisms of an organisation, by exploiting the weaknesses of various components of the Internet, the crime scene can extend beyond the control of the organisation. Furthermore, outsiders can exploit weaknesses in the organisation's network to gain insider access without detection. Therefore, the task of distinguishing between insider and outsider attacks becomes extremely difficult when an insider denies carrying out an attack.
- 3- Incorrect types (or aspects) of evidence can be used to identify the differences between insider and outsider attacks. This is because these aspects are suitable for dealing with traditional attacks such as when outsiders penetrate an organisation's network by overriding firewalls. As previously discussed, these aspects include the location of attack initiation, attacks within an organisation's control, and authorised access. Therefore, these aspects are not suitable for distinguishing between types of attack.
- 4- Lack of physical evidence collection because suspect computers are not under an organisation's control, such as when the computer belongs to an outsider or an insider's personal computer is being used at home. Therefore, a limited amount of logical data is available for forensic collection.
- 5- No conclusive model of computer forensic analysis exists that includes the distinction between insider and outsider attacks. In general, there is

limited research on computer forensic analysis models, such as the first model of computer forensic analysis which was designed by Palmer [63]. However, models for distinguishing between insider and outsider attacks are non-existent. This issue prevents a corporate computer investigator from conducting an investigation with the aim of distinguishing between insider and outsider attacks. There has been a lack of effort in identifying the types of data to be collected and the location of the data, determining the tools to be used to collect and analyse it, and also in determining the methodology that should be employed to conduct an investigation.

Furthermore, this chapter has also defined insiders as trusted individuals who have been hired by an organisation and gained authorised access to their organisation's IT resources (facilities) in order to perform their particular job responsibilities/role. On the other hand, outsiders are defined as users who gain insider access (unauthorised) to an organisation's IT facilities through their ability to bypass security mechanisms and with no prior knowledge of the insider's job responsibilities.

Following the literature review, which illustrated the difficulties in distinguishing between insider and outsider attacks, the next chapter will discuss classifications of computer and network attacks in detail. Then, it will present the assumptions of the thesis about the environment in which a computer investigation can be conducted.

3 User Activities and Assumptions

Objectives:

-
- to discuss suspicious activities (computer incidents/attacks)
 - to discuss user job activities and legitimate activities
 - to develop the thesis's assumptions
-

After understanding the issues of involved in distinguishing between insider and outsider attacks, this chapter discusses the categorisation of attacks. It extends the classification of computer and network attacks devised by Hansman and Hunt to include a number of other types of attack [38]. It also develops the assumptions made by the thesis, which enhance the collection and analysis process of computer investigations, in order to improve the process of distinguishing between insider and outsider attacks.

3.1 Job responsibilities/roles

This section aims to identify the job responsibilities/role of an employee and determine what constitutes legitimate activity. Comprehension of the insider's job responsibilities is essential in order to distinguish between insider and outsider attacks. Job responsibilities comprise a list of the tasks and roles of each position [51]. They define an employee's job title because they detail the tasks that an employee is expected to undertake in return for his/her salary. They also include information about the applications and equipment used by an employee and their relationships with other positions within the organisation [51]. Therefore, job responsibilities are important when making a distinction between insider and outsider attacks, for a number of reasons:

- **Identification of insider's job responsibilities/tasks:** corporate security investigators should identify and collect insider's job responsibilities from an organi-

sation's human resource management. This is because the analysis process of distinction between insider and outsider attacks requires this information

- **No prior knowledge of the insider's job responsibility:** most outsiders who gain insider access have no prior knowledge of the insider's job responsibility. They usually focus on hiding their identity when computer attacks are carried out;
- **Identification of legitimate activities:** job responsibilities help to identify whether the activities performed at the time of the incident are related to the insider's job responsibilities or not;
- **Identification of relationships:** job responsibilities help to identify the relationships between the activities that were performed at the time of attack and an attacker. If these activities match with a job responsibility, the attack is classified as an insider attack

3.2 Legitimate user activities

After identifying an employee's job responsibilities, it is necessary to understand what constitutes a legitimate employee/user activity. Every organisation allows its employees to utilise its IT resources (facilities), such as remote login, file transfer, email or Internet access, in order that they can perform their job responsibilities/roles. These activities are deemed to be legitimate because an organisation specifies which employees are granted access to IT facilities and which operations, such as create, read and modify, can be performed on the software and hardware to which such access is granted [27]. These activities include the following:

- **Install and upgrade:** employees who have administrator privilege can install software such as Operating Systems (OS) or applications. They can also update software or applications;
- **Access to specific application servers:** permission has been granted for specific employees to access the following application servers in order to create and modify data, download or upload files:
 - Database Application Server
 - File Application Server

- FTP Server
 - **Browse the Internet:** many employees require access to the Internet to perform their jobs; for example, researchers need the Internet when finding conference and journal papers;
 - **Files and folders:** employees usually create, modify and store files and folders on their desktops. These files or folders are related to their job responsibilities.
 - **Access to network servers:** employees can use their organisation's network server, such as its email service for sending and receiving emails. These emails are usually business emails. Employees can also use their organisation's printer to print files and folders.

These legitimate activities are a main source of distinction between insider and outsider attacks, because these activities would be uniquely undertaken by employees. The collection and examination of details of these activities would help to reveal the insider's job responsibilities.

Figure 5 shows an example of an organisation's structure, the job responsibilities/roles of sample employees, and their legitimate activities. This Figure divides the organisation's resources between subjects and objects. A subject would be an employee who has been assigned by the organisation to perform a list of specific tasks that include accessing passive objects via specific operations. The objects comprise IT resources and facilities, such as application servers, email servers and file servers.

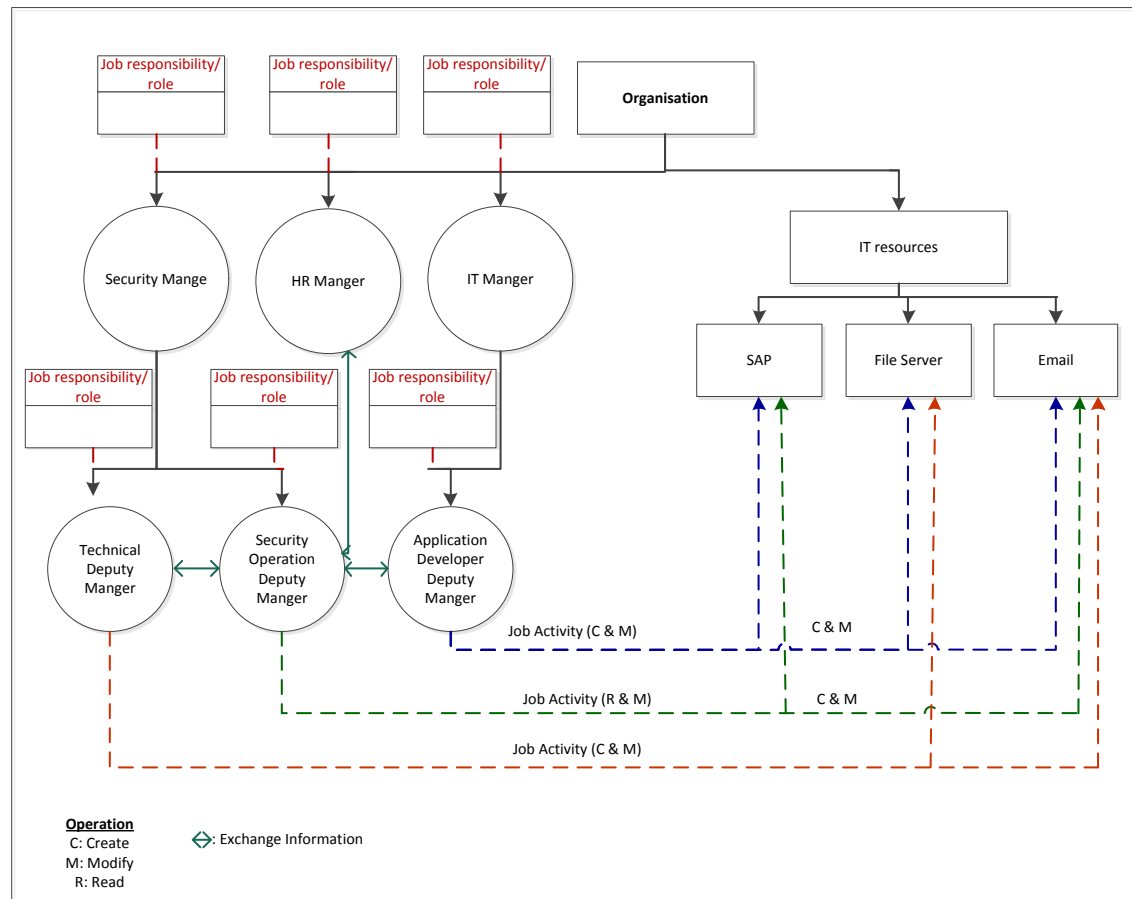


Figure 5: An organisation's structure

It appears that there is a difference between a user's job responsibilities/activities and legitimate activities. A user's job responsibilities include a set of tasks and activities that are needed to produce certain results, such as writing a memo, writing spreadsheets, updating a database, or sending and receiving business emails. However, a legitimate activity allows an employee to access an organisation's resources, such as a database server, in order to perform their job activities. For example, once insider access to an organisation's email system has been gained by an outsider, a security mechanism would classify this activity as being legitimate but without verifying whether this activity is included among the user's job responsibilities or not. Therefore, the content of the email should be analysed.

The researcher believes that if the activity includes organisational user's job responsibility it is called "legitimate activity" otherwise; it is called "suspicious activity".

3.3 Suspicious activity/taxonomy of attacks

This section aims to identify suspicious activities that have been performed by insiders to annoy co-employees or harm their organisation's systems. These activities can also be performed by outsiders using insider access to hide their identity. Any organisation's computer connected to the public network is under threat from malicious attacks, such as viruses and attacks from crackers. Therefore, a corporate security investigator needs to understand the nature of these attacks in order to be able to determine which types of suspicious activity can be expected to occur.

The aim of a classification is to provide a useful means of describing attacks because, at present, attacks are often described differently by different organisations. Hansman and Hunt [38] have proposed a common classification that can be shared between organisations. The classification comprises viruses, worms, Trojans, buffer overflows, denial of service (DoS), network attacks, physical attacks, password attacks and information-gathering attacks.

It appears that this classification of attacks does not include some important types of attack such as client-side attacks, impersonation, spoofing and email attacks. Graves [34] states that outsiders can use one of these methods to gain insider access and attack an organisation's IT resources. Therefore, this chapter extends the classification to cover these attacks.

3.3.1 Client-side attacks

The only way to attack an organisation's IT facilities is through gaining insider access [34]. However, outsiders currently use advanced techniques for committing a crime that allow them to gain insider access without detection and then carry out an attack.

One of these techniques is client-side attacking that is designed to exploit a vulnerability remotely, via client applications such as an Internet browser. One encouragement for this type of attack is the fact that 35 per cent of organisations have no control over employees' use of instant messaging [7]. Further encouragement for the attacker comes from about 70 per cent of organisations having no control over Internet access by their

employees, whereas the remaining 30 per cent restrict Internet access to only some of their staff [7]. Therefore, it is quite possible that client-side attacking is one of the main threats facing an organisation's computer clients, because the majority of organisations implement client/server networks. The attack can occur via any client/server pair, for example email, FTP and instant messaging [75].

In 2007, the SANS Institute reported that client-side vulnerabilities are among the biggest threats facing computer users [35]. For example, an outsider can use websites that include codes that are designed to obtain information, such as passwords, from an insider's computer [1]. It is remarkable that many codes are often designed to download themselves automatically as soon as an insider accesses a web page. Furthermore, other sites prompt the insider to accept what appears to be legal software but is in fact a malicious program [1]. One example of this type of attack was in 2005 when insiders, who had not patched their computers, browsed the MySpace and YouTube websites. Their PCs were infected if they clicked on an advertisement or banner, which secretly installed Spyware on their computers to log keystrokes and capture user names and passwords [1; 104].

It is evident that outsiders employ websites to carry malicious software which aims to obtain usernames and passwords. As mentioned in the previous chapter, analysts at Google discovered that 4.5 million web pages that were suspicious in nature [104].

Beer reported that more than a million were found to have launched downloads of malicious software, collected sensitive data, and then emailed that data to a temporary email account [7]. This is because organisations tend not to scan outgoing emails for confidential data. This is true, for example, of 84 per cent of organisations in the UK [6].

3.3.2 Malicious software

Malicious software or malware is a piece of software that is implemented for fraudulent reasons with the intention of causing damage on personal or corporate computers. It includes computer viruses, worms and Trojan horses [39].

3.3.2.1 Viruses

These are computer programs that are usually capable of causing harm to a file system or another program [11]. Insiders and outsiders use emails to distribute harmful content to the organisation's network. They can bypass firewalls by tunnelling through the email, if the email content has not been analysed. Viruses often deliver destructive payloads that can devastate data and bring down entire mail systems. Email is also employed to install Trojans (see below) in order to obtain an organisation's confidential information or gain control of their computers [11].

Viruses have become widespread in the past few years and are becoming more complex. Various types of virus are developed daily and involve different methods of information gathering.

3.3.2.2 Trojan Horses

These comprise hidden instructions which, when executed, allow an outsider to control an insider's system by opening a communication channel between them. The insider's system can then be used as a tool to commit another crime in order to hide the identification of the outsider. A Trojan horse can even send passwords and personal details to the outsider, and it is also one of the main ways of installing a malicious program, such as a virus or a worm.

3.3.2.3 Logic bombs

These are aimed at planting damaging programs in a computer system that execute when some specific condition is met. Magklaras and Furnell [48] reported that an employee of Lance Incorporated resigned from the company. Two months after his resignation, a file server suddenly lost valuable data and became inoperable. After a computer forensic investigation was conducted, it was found that the server was the subject of a logic bomb that the ex-employee had implanted on the server. This incident cost the company about \$1 million [48].

3.3.2.4 Time bombs

These bombs are also programs implanted in a computer system, with the intention of being executed when a specific date or time is met, in order to damage a target.

3.3.2.5 Unauthorised user access

After an outsider gains unauthorised access, they can obtain administrator rights by using software such as GetAdmin for Windows OS. This software is a powerful utility which can give a user administrator-level rights. It is often able to penetrate a computer server, and it then assigns administrative rights to an outsider.

3.3.2.6 Key loggers

Key loggers are used for recording data that an insider may enter. They can be in the form of hardware or software. The hardware is invisible to the user and is usually installed as an extension between the keyboard and the port. Only an executable file needs to be installed on the system for software key loggers to be kept completely hidden from the user.

3.3.3 Spoofing

This attack occurs when an outsider uses the identity of an organisation's resources, e.g. a network computer, in order to gain unauthorised access. There are several common types of spoofing, such as IP and machine [11].

3.3.3.1 Web-spoofing

This is a way by which an organisation's users are led to believe that they are looking at an original website which, of course, they are not. This requires the outsider to be highly skilled in order to redirect the insiders to the outsider's website. When any identifying or sensitive information is entered by an insider, it will be stored and used for malicious purposes.

Web pages can be precise copies of the original with all the content correctly linked to the original web page. The main difference is that there are minor changes which allow for insider information to be stored on the outsider's servers.

3.3.3.2 DNS spoofing

Spoofing is a form of impersonation of resources. A DNS can be redirected to point to a false resource [11]. For instance, an outsider creates a fake website for an insider's organisation (an impersonation of an organisation's website), and then redirects legitimate

(insider) requests for this website to the false site which the attacker has created. This type of attack can be carried out through one of the following methods [45; 76]:

- **spoofing DNS response:** a man-in-the middle attack occurs when an outsider places himself between the DNS client and the legitimate DNS server. When a DNS request is initiated, the outsider immediately sends a false response (redirects the insider to an incorrect machine) before the legitimate DNS server can reply.
- **DNS server compromise:** an outsider gains full control of the legitimate DNS and then directly inputs incorrect data.
- **DNS cache poisoning:** this occurs when an outsider sends incorrect information (false name information) to the DNS server and the server enters the incorrect information as legitimate data. Therefore, when an insider asks the DNS server to resolve a name that has been incorrectly entered in the DNS server, it directs the insider to the false destination.

3.3.4 Impersonation

This attack is designed to steal the identity of a legitimate user. This is designed to steal the identity of a legitimate user. An outsider can use the identity of an insider to gain unauthorised access to a system without detection. For example, an insider's email password can be obtained by an outsider who then uses the insider's email account to send an abusive email to someone else in order to hide the identity of the outsider. Outsiders can get the information they need to assume an insider's identity from a variety of sources, such as a stolen wallet, items thrown away, or from a credit card or bank statement [25].

3.3.5 Denial of Service (DoS) attack

A Denial of Service attack prevents a legitimate user from accessing organisational network resources such as a mail server. This attack is characterised as an attempt to flood a network, to disrupt connections between two computers and thus prevent an

individual from accessing a service, or to disrupt service to a specific system or person. There are many types of DoS attack, as described next [45; 53; 54].

3.3.5.1 Buffer overflow

The program writes more information into the buffer than can be contained in the space that has been allocated in the memory. An attacker can overwrite the data which controls the program execution path and hijack control of the program in order to execute the malicious code (the attacker's code) instead of the process code.

3.3.5.2 Ping of death

This is aimed at sending IP packets of a size greater than 55,535 bytes to the target computer [45]. This size is illegal, but applications that are capable of sending such packets can be built. Some programmed OSs could detect illegal IP packets, but fail to handle them.

3.3.5.3 Smurf attacks

These are aimed at exploiting IP broadcast addresses in order to create DoS. ICMP echo request packets are directed to IP broadcast addresses from remote locations so as to generate DoS attacks [16]. Three parties are involved in this attack: the attacker, the intermediary and the victim. The intermediary receives an ICMP echo request packet directed to the IP broadcast address of their network. When all machines on a network respond to this ICMP echo request, the result can be severe network congestion or outages.

The attacker does not use the IP address of his own machine as the source address; instead, he creates forged packets that contain the spoofed source address of the attacker's intended victim [16].

3.3.5.4 TCP SYN attacks

An attacker can send a number of connection requests very rapidly and then fail to respond to the replies. This leaves the first packet in the buffer so that other, legitimate, connection requests cannot be accommodated. The packet in the buffer is dropped after

a short period of time without a reply. The effect of many such bogus connection requests is to make it difficult for legitimate requests for a session to be established.

3.3.5.5 Teardrop

This attack is aimed at exploiting the way by which the IP requires a packet that is too large for the next router to handle to be divided into fragments. The attacker's IP puts a confusing offset value in the second or a later fragment. Sometimes the system can crash if the receiving OS does not have a plan to handle this situation.

3.3.6 Physical attacks

These are designed to damage the physical components of an organisation's network or computer. It is well known that, given physical access to a computer, an attacker can compromise it by rebooting from a CD or swapping the hard drives.

3.3.7 Password attacks

Passwords are what users know and use to enable access to files, computers or programs. They are the main method used to authenticate users. However, they present a well-known problem in computer security, because the users' chosen passwords are naturally insecure. Password attacks are designed to obtain a password by cracking encrypted passwords, using dictionary and brute force attacks, and by decoding and scrambling passwords.

3.3.8 Social engineering

This is a method of manipulating individual insiders when the outsider has a certain target in mind that is usually fraudulent [32]. Computers are not necessary for a social engineer, as communications skills appear to be more useful than having a technical background. Outsiders might try to harm a business or gain access to a company's private information by using social engineering techniques in order to achieve their purpose. The aim is to persuade an insider to disclose willingly any information the outsider needs to know. Attacks can be conducted in the following ways, either by influencing the insider psychologically or by gaining physical access [32]:

3.3.8.1 Impersonation

The outsider pretends, either in person or over the phone, to be a trustworthy person, such as an IT helpdesk operator or an insider, and then tricks a person, usually a member of the personnel department, to reveal the information they require. This might be a username or password, or other sensitive information that is of value to the outsider.

3.3.8.2 Reverse social engineering

Here, the attacker presents himself as an authorised person who can help an insider to address a problem. The problem will have been caused by the outsider, usually by disrupting the network's traffic. Therefore, the insider will contact the outsider, thinking that he can sort out the problem [28]. The outsider then either creates a relationship of trust with the insider or carries out a direct attack [33].

3.3.9 Information-gathering attacks

These are designed to monitor data travelling over a network. They are aimed at stealing personal credentials and critical information for use in a further attack. An attacker with physical access to network devices such as a hub or a router is able to sniff the traffic.

3.3.10 Theft of an organisation's devices and information

The next technique used by outsiders to gain insider access is local information theft. This is a form of confidentiality attack; however, it is hard to detect. Physical access to an organisation and use of suitable software or hardware are required to obtain sensitive data that travels in clear text across trusted networks. Outsiders therefore seek to gain insider access by exploiting the weakness of password encryption mechanisms [88]. An organisation's password policy is sometimes inadequate, such that an organisation can select a vulnerable password encryption protocol or allow an insider to create a weak password, such as their spouse's name [88].

3.3.10.1 Theft of information for financial gain

An insider or an outsider steals confidential or proprietary information such as customer information, source code or other sensitive data from the organisation for financial gain [57].

3.3.10.2 Theft of information for business gain

Insider theft of intellectual property (IP) for business advantage is a crime whereby insiders intentionally misuse an authorised level of access to networks or data in order to steal confidential information from the organisation [84]. They then use it to get another job, help a new employer or promote their own private business [56].

3.3.10.3 Theft of an organisation's device

Another technique of outsider attack is the theft of laptops or disks. In 2008, 78 per cent of organisations in the UK that had computers stolen had not encrypted their hard disks [7]. In 2006, 7 per cent of organisations in the UK had computers stolen. The theft of organisations' devices has increased sharply, reaching its highest level in 2008 [7]. A further encouragement for carrying out attacks is that 54 per cent of organisations in the UK allow their employees to access their systems remotely [7]. Because an organisation's devices are loaded with confidential information, this presents a good opportunity for outsiders to gain remote access to an insider's computer. An example of gaining insider access by an outsider is cited by the BBC [10]; a memory stick with user names and passwords for a key government computer system was lost and later found in a public car park.

Storage devices belonging to an organization, such as hard disks and USB keys, can pose a problem because they hold sensitive insider information. This information can be extracted from either stolen or sold storage devices on which sensitive information, such as personal information and e-mail messages, is held. A study conducted by the University of Glamorgan [9] showed that out of 105 hard drives, 57 per cent contained sensitive personal information.

3.3.11 Computer and Internet abuse

This is aimed at wasting time with email messages and websites that have nothing to do with employees' jobs [8]. This type of attack not only wastes employees' time but potentially creates legal liabilities for the organisation.

The BBC [8] reported that a company which makes about £700,000 profit on turnover of £10-12m could be losing 15 per cent of its profit because of net and email abuse.

Computer Economics state that online shopping, stock trading, car buying, looking for a new house and visiting pornographic sites have become daily practices for about 25 per cent of the workers in the United States companies that have access to the Internet in their offices. A survey conducted by Young and Case [107] found that 83 per cent of companies were concerned with inappropriate employee usage of the Internet and the resulting legal liabilities and negative publicity. It also found that 70 per cent of employee Internet abuse resulted in lost productivity and slow network response [107].

3.3.12 Email attacks

Employees can use emails to send racist, sexist or other offensive material that can make an organisation vulnerable from a legal point of view [29]. UK firm Holden Meehan Independent Financial Advisors had to pay a former employee £10,000 for failing to protect her from email harassment in 2003 [29]. Chevron had to pay \$2.2 million to four employees after they had allegedly received sexually harassing emails. Under UK law, employers are responsible for emails written by employees in the course of their employment. Norwich Union Insurance was asked to pay £450,000 in an out-of-court settlement as a result of emailed comments relating to their competition [29].

3.3.12.1 Spam

Zhuang [108] has defined spam liberally to include traditional advertising email messages as well as phishing email messages, email messages containing viruses, and other unwanted email messages. Unwanted or harmful messages have become a particular problem for electronic mail, because it has recently been estimated that 80 per cent of all email traffic is spam [80]. Furthermore, this form of attack is aimed at sending emails to a large number of users. It can be made worse if a large number of recipients reply to those emails.

Xie [106] believes that laundering email spam through open proxies or compromised PCs is a commonly used trick to hide real spam sources and reduce the cost of spamming in the underground email spam industry. He also states that spammers have been plaguing the Internet by exploiting a large number of spam proxies.

3.3.12.2 Email bombing

This form of attack sends email messages repeatedly to a particular address at a victim's site. Usually, these messages will be large and constructed from meaningless data in order to consume network resources [15]. Most email bombs have the primary objective of flooding the email server so that it becomes unavailable. These email attacks may also be used to forge the identity of the attacker, degrade the availability of communication systems, or undermine the integrity of organisations.

3.3.12.3 Phishing

This form of attack is an attempt to ask for personal information from unsuspecting users by using social engineering techniques [98]. These emails aim to entice users to click on a link that will take the user to a fraudulent web site that appears to be legitimate. Furthermore, these web sites may contain malicious code. Phishing is the use of email messages that look as though they are from a trusted destination such as a bank [57]. For example, an attacker may send an email, seemingly from a reputable credit card company that requests account information. When the victim responds with the requested information, the attacker can use it to gain access to the victim's account.

Fildes [26] has reported that a large number of accounts on the web-based email system Hotmail have been compromised in a phishing attack. Greenwood [36] reports that in 2004, phishing has cost British banks more than a million pounds, and the bill could rise as the attacks become more sophisticated.

3.3.12.4 Harassment

Harassment can be construed as messages that threaten or intimidate the recipient [65]. Forgery and harassment by email usually go hand-in-hand [65]. Senders of harassing emails usually aim to hide their identity. The harassment often stems from some breakdown in a personal relationship between the parties, such as a romantic relationship having recently ended, a debt owed, etc., and there is no basis for legal action in what amounts to a personal dispute [65].

3.3.12.5 Email spoofing

This aims to trick the user into making a damaging statement or releasing sensitive information [14].

A recipient receives an email that appears to have come from a particular source whereas it was actually sent from another source. It is easy to spoof email because SMTP lacks authentication. If a mail server is configured to allow connections to the SMTP port (25), an attacker can connect to the SMTP port of a site and issue commands that will send emails that appear to have come from the address of the individual's choice.

Emails have two addresses. The first address is the envelope address that is applied to deliver email to the correct destination (receiver), but email users do not see this address detail when the email is received. Email servers use this address to deliver email to the destination's email account. The second address is the header of the email message. This address, which includes To: and From:, is seen by email users. The critical point here is that the second address is not required to be correct for the message to be delivered to the recipient. As a result, this address can be forged.

Therefore, any user can implement their MUA software to send emails bearing any name, email address and reply-to address. The thesis experiment will use this type of attack to send an abusive email to a victim.

Table 10 illustrates various types of insider and outsider attack, the aim of these attacks and their consequences. Currently, impersonation and harassment by email usually go hand-in-hand. An outsider steals and uses the identity of an insider to send harassing emails to another party. The advantage of stealing the identity of the insider is to hide the outsider's identity. On the other hand, an insider who carries out an attack can exploit this weakness by claiming that someone else stole his password and sent the harassing email.

Table 10: Illustration of insider and outsider attacks

	Types of attack	Aim	Consequences
1	Malicious software	Gain insider's credential	Steal information or destroy resources
2	Client side		Gain access to an organisation's system
3	Spoofing		Use identity of an organisation's resources
4	Password attack		Unauthorised access to an organisation's system
5	Information gathering		Use in a further attack
6	Theft of devices and information		Gain access to an organisation's system
7	Impersonation	Hide an identity of outsiders	Use identity of insiders to gain access to the system
8	DoS	Prevent a legitimate user from accessing an organisation's network	Disrupt connection between computers
9	Physical attack	Damage Physical components of organisation's network	Unavailability of an organisation's network devices
10	Internet abuse	Revenge	Potentially creating legal liability for an organization
11	Email attack	Bother and annoy a victim	

We have proved that incidents/crimes can be committed by insiders or outsiders. Insiders can commit crimes/attacks by abusing their legitimate access for reasons of financial or political revenge. They can then deny any allegation of committing an attack. On the other hand, insider access can be obtained by outsiders who seek to commit a crime and hide their identity. Outsiders can use one of the attack methods described above to obtain insider access and then attack the system. As a result, insiders can be guilty or innocent. An organisation's computers and networks are able to record these suspicious activities, because both insiders or outsiders use methods such installing malicious software or browsing illegal websites. Therefore, this research has designed a model to prove or disprove allegations of committing incidents/crimes by insiders.

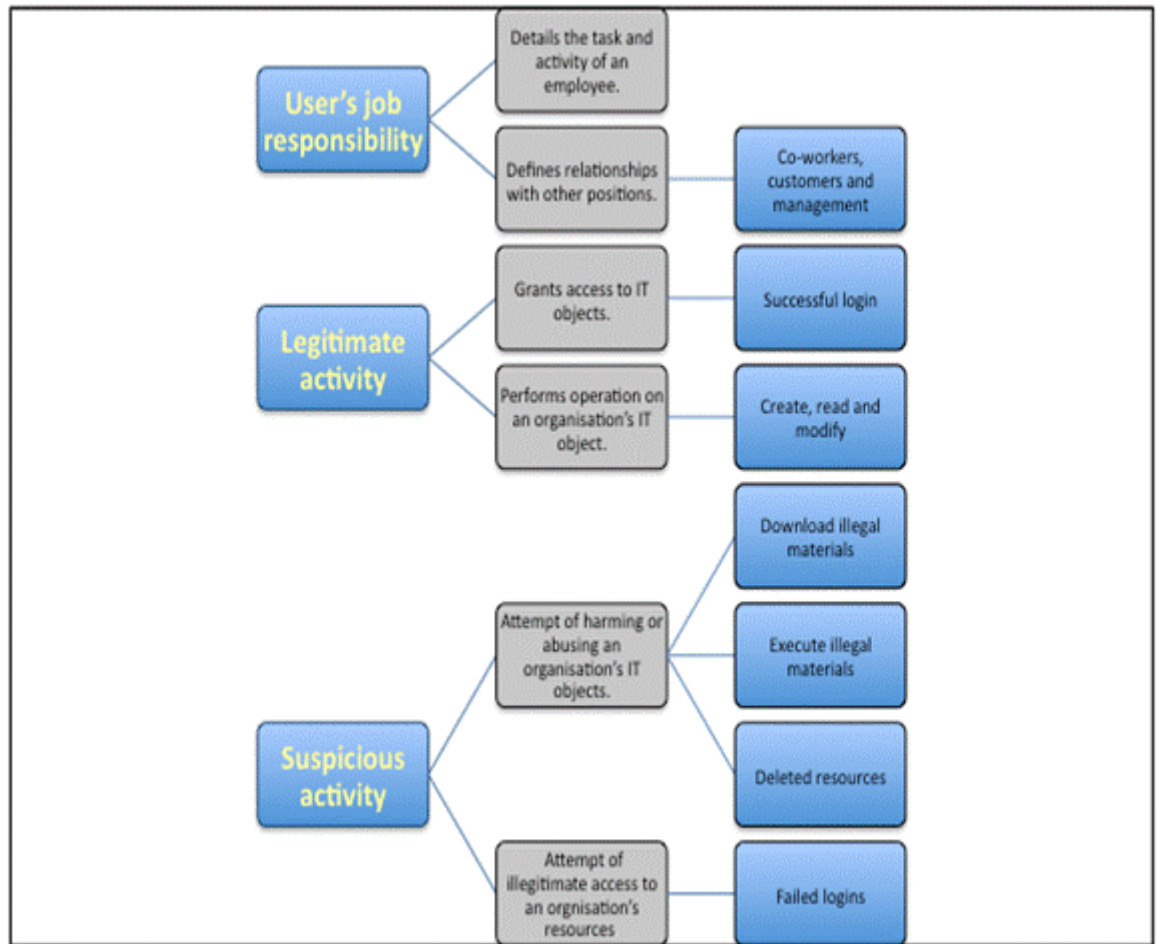


Figure 6: Type of information

Figure 6 shows this type of information. Firstly, it is necessary to understand how a user's job tasks relate to their responsibilities. Secondly, we need to identify the legitimate activities that allow a user to access an organisation's IT facilities and the limits of what they are permitted to do in order to discover which legitimate activities conform to their responsibilities. Thirdly, in terms of suspicious activity, we should understand if a computer's security could easily have been compromised.

3.4 Location of user activities

This researcher believes that any corporate security investigator should know the location of the above activities in order to collect and analyse information about them. This analysis leads to ascertaining whether the attack was committed by an insider or an outsider. There are many potential sources of evidence available within an organisation's networks. Many of these are existing records and logs. The research also requires an understanding of precisely how to turn this information about activities into evidence. These sources of evidence can be divided, based on activity functions, into three groups: legitimate activity logs, security logs and personal (insider's) storage. These groups are illustrated below:

3.4.1 Legitimate activity logs

These logs record an insider's legitimate computer activity. The corporate security investigator can find recent and past activity including recently accessed files and passwords. These logs can also assist the investigator in identifying emails that have been received and sent, websites that have been browsed and files that have been created and modified. They will assist in the reconstruction of the insider's job activities (responsibilities) so as to identify any abnormalities in behaviour. These activities are usually located in the following logs:

- email activity
- web activity
- file access/ database activity
- application activity
- remote access activity

3.4.2 Security logs

These logs are usually configured to maintain records of suspicious computer events [82]. These suspicious events include logs of failed accesses, and the detection and destruction of viruses and Trojans, as well as detection of forms of hacking. Security logs can identify an insider's abnormal activity, and they are strong evidence when

tracking activity on a computer system [82]. These suspicious activities can be found in the following logs:

- access control
- anti-virus and spy
- intrusion detection
- firewall

3.4.3 Personal devices

These devices are another source of distinction between insider and outsider attacks, because they contain an insider's activities. These personal devices, such as an insider's computer, laptops or USB flash memory, should be collected in order to reveal an insider's legitimate and suspicious activities. For instance, an insider can save an organisation's secret files to his USB flash memory.

3.5 Assumptions

There is no conclusive model of computer analysis investigation that covers the distinction between insider and outsider attacks, which leaves scope for a variety of opinions on the matter. The present work has made a number of assumptions in this regard, in conformity with its key goal of improving the analysis and collection processes of computer investigation. To address this issue, it is necessary to log information or data that has some investigative value before any incident can take place.

One of the assumptions just mentioned is that all legitimate and suspicious user activities have been recorded by the organisation's IT system, before the incident took place. Another is that none of the organisation's operating systems have been altered for any reason, while a third is that an organisation's users would have to be agreeable to the security policy, which would include constant monitoring of their activities.

3.5.1 Conditions attached to assumptions

In order for the assumptions underlying this thesis to be borne out in practice, the following conditions should be present:

3.5.1.1 The organisation's business processes are based totally on its IT system

Organisations should rely on computer systems to perform tasks and improve their businesses because of the ability of those systems to process, transmit, store and retrieve data. Daily jobs should be performed electronically, which will generate a history of all users' activities.

3.5.1.2 Client/server environment

As mentioned in Chapter 2, most organisations implement client/server environments, and control their network resources through security policies based on such environments. These environments enable the maintenance of log files for each of the organisation's resources, so that all user activities on every network can be monitored and recorded.

3.5.1.3 No prior knowledge of employees' job responsibilities

Outsiders do not usually understand these responsibilities, because their aim in obtaining insider access is to bypass the security mechanisms implemented by the organisation. Moreover, outsiders do not perform employees' tasks, which are only performed by the organisation's own users (i.e. its employees).

3.5.1.4 Log system capability

Log files are created by networked computers or information systems that contain information on transactions, connections and other activities. Timestamping plays a significant role in identifying the times at which user activities, such as gaining access to a system and creating files, were conducted [43]. These timestamps need to be accurate.

An organisation's IT Security Department or system administrators should protect log files from misuse or alteration. These files should be kept locally on a server or remotely by using a centralised log server. A centralised log server prevents an attacker

from altering the logs. Organisations should identify what is logged. This research suggests that logs should not only be set to record suspicious activities but they should also record legitimate activities, because they should be able to prove whether an attack has been committed by an insider or an outsider. The basic requirements of what such logs should cover are as follows:

- timestamp of an activity (see the analysis process)
- IP address of the source and destination
- MAC address of the source and destination
- port number of the source and destination
- data (content of a message)
- successful and failed logins
- changes of computer settings, and policies
- installation or execution of software

3.5.2 Information and technology requirements

In order to apply the thesis's hypothesis and assumptions, the following minimum information and technology requirements should be implemented, but not be limited to them:

3.5.2.1 Recording of activities

Legitimate user activity is an essential aspect for distinguishing between insider and outsider attacks. An organisation's IT system should not only record suspicious security events but should also be extended to include a record of legitimate user activities. The job-related activities of users should also be identified.

3.5.2.2 Retention policy

This policy relates to retention periods for records that are created and maintained by an organisation's IT department. Retention periods vary between organisations, but they are usually between six months and one year. This policy is useful when gathering evidence; for example, when an insider removes an email from a list of deleted items or when an insider deletes an entire mailbox.

3.5.2.3 Firewall

Most firewall policies are configured to drop an unauthorised connection without recording it [34]. They should not only drop such a connection but should also record it, because this would help to identify if an outsider has tried to gain access to an organisation's system or not. The firewall policy should also be configured to record an authorised connection in order to examine legitimate activities by an organisation's users. Therefore, this research proposes that the firewall log should include the following information:

- date and time of packets
- TCP information including source and destination port numbers
- IP information including source and destination IP
- MAC information includes source and destination addresses
- packet state such as drop or accept

3.5.2.4 Virtual Private Network (VPN) server

The research proposes that this policy should be configured to record information in local logging files for remote access VPN connections. This log would assist in tracking remote access usage and authentication attempts. This remote access policy should be to record both accepted and rejected connections.

3.5.2.5 Intrusion Detection System (IDS)

An IDS policy should be configured to achieve the following goals:

- verifying threats, whether from inside or outside the organisation
- recording all statistic of employees' day-to-day work activities, such as accessing various services and servers
- identifying any malicious network behaviour or anything done that is contrary to the organisation's policies
- detecting any successful intrusions
- identifying attack patterns and trends in order to allow a corporate security investigation to observe the most frequent points of attack

- detecting any modification of files or suspicious activity (on critical workstations and servers)

3.5.2.6 Network traffic monitoring

Network traffic should be monitored to achieve the following goals:

- detecting a connection between an inside computer and an outside computer
- detecting the content of conversation between these two machines
- detecting sensitive information, such as username, passwords and any other information passing between these machines

3.5.2.7 Workstations

The security event policy should be configured to achieve the following aims:

- recording successful logins to identify which are legitimate
- recording failed logins to identify access attempts
- recording events that relate to the use of resources, such as creating, opening or deleting files

Having access to a workstation is useful for collecting details, such as file attributes, of a user's job activities; for example, accessing timestamps and finding out what operations have been performed.

3.5.2.8 Network servers

Each network server, such as the web server and exchange server, should be configured to record the following information:

- client IP addresses
- name of the user
- date and time of access
- operations performed on the resources
- any attempted and successful attacks

3.5.2.9 Imaging tools

As this thesis focuses on the distinction between insiders and outsiders, a static image is employed. This image is made in respect of a detained computer. There are many types of static image, as follows [60]:

- a disk-to-image file makes a bit-by-bit copy of the insider's disk drive. This method allows more than one copy of the insider's computer to be made and allows most computer forensic tools to read this file. However, this method is not suitable for a large disk drive because collecting evidence from a large computer can take many hours or several days.
- a logical image records only specific files that are of interest to an incident. This method is useful for collecting only specific records from a large server. It is also useful for email investigations that only need to collect .pst files.
- a sparse image is similar to a logical image but it collects deleted data. This method is useful for examining specific data.

The purpose of this process is to protect the integrity of the insider's computer. Therefore, a corporate security investigator should understand that using imaging tools that run in Windows alters the evidence on a disk drive. To address this issue, a write-blocker is required to ensure that any writing to the hard disk being imaged is blocked.

3.5.2.10 Analysis tools

These are used for analysing data, retrieving deleted and partially overwritten files from the insider's computer, retrieving hidden files and performing email analysis tasks such as:

- FTK Tools:

FTK can analyse data from different sources such as image files from different vendors [60]. It has password cracking tools as follows:

- Password Recovery Toolkit is able to recover passwords from many applications such as Microsoft Word.

- Distributed Network Attack (DNA) is able to recover password-protected files by using the power of machines across the network or across the world to decrypt passwords.
- Email Examiner: an email examination tool. This is used for recovering active and deleted mail messages from deleted items. An example of this type of tool is Paraben's e-mail examiner.

3.6 Summary

The aim of this chapter has been to identify the data that should be collected and analysed in order to distinguish between insider and outsider attacks. It has found the main aspects of distinction between insider and outsider attacks to be the user's (insider's) job responsibilities, and the user's legitimate and suspicious activities. It also found that there is a difference between a user's job responsibilities/activities and legitimate activities. A user's job responsibilities comprise a set of tasks and activities that are needed to produce certain desired results. An outsider has no prior knowledge of the insider's job responsibilities. However, through their legitimate activities, an employee (insider) is allowed to access an organisation's resources, such as a database server, in order to perform their job functions. The researcher found that if the activity includes user's job activity is called "legitimate activity". This is because an organization's resources are used for business purposes.

Furthermore, several suspicious activities have been discussed, using Hansman and Hunt's classification. However, this classification has been extended to include other important activities or attacks such as client-side attacks, impersonation, spoofing and email attacks. Many attacks, such as client-side attacks, malicious software, physical key loggers and social engineering, allow outsiders to gain an insider's credential details. These methods assist outsiders in accessing an organisation's resources without detection, enabling them to hide their identity and then commit a crime. This suspicious activity should be understood by corporate security investigators when looking into the malicious tools that are used to gain insider access. Impersonation and harassment attacks via email are selected in the thesis experiments as methods of computer attack (see chapter 5). This chapter has discussed the location of legitimate and suspicious activities within the client/server environment.

Also, the assumption has been made that all user activities before the attack incident took place will have been recorded by an organisation's IT system. This assumption is formulated according to four main conditions. The first condition is that an organisation's business processes are based totally on an IT system. The second condition is that a client/server environment has been implemented. The third condition

is that outsiders have no prior knowledge of an insider's job responsibilities. The final condition is the presence of adequate log file systems. In addition, this chapter recommends that certain policies are implemented and appropriate technology should be used to collect and examine evidence of user activity.

The next chapter will create a Digital Analysis Model for Distinguishing between Insider and Outsider Attacks (DAMDIOA) in order to improve the process of distinguishing between these attacks. It will also discuss the drawbacks of DAMDIOA.

DRAFT

4 Digital Analysis Model for distinguishing between Insider and Outsider Attacks (DAMDIOA)

Objectives:

-
- to discuss the shortcomings of the Digital Forensic Research Workshop (DFRWS) Method
 - to provide a digital model for distinguishing between insider and outsider attacks
-

As discussed in Chapter 2, the principle of computer forensics and investigation is to discover, obtain, identify, analyse and preserve e-evidence. It was also mentioned in that chapter that there is no model or framework by which to distinguish between insider and outsider attacks. Chapter 3 discussed the basic requirements for such a distinction, the main one being identification of the type of information to be recorded. Others are the use of a client/server environment and the capability to maintain log files and to employ technology.

In this chapter the design of a process for obtaining, examining and analysing activities to distinguish between insider and outsider attacks will be described, and a Digital Analysis Model for Distinction between Insider and Outsider Attacks (DAMDIOA) model that improves on the Digital Forensic Research Workshop (DFRWS) methods created.

4.1 Limitations of DFRWS

As mentioned, DFRWS methods are general ones used to conduct computer forensic investigations [63]. They contain the following processes [63]:

- identification
- preservation
- collection

- examination
- analysis
- decision

In addition, DFRWS methods provide a good foundation for computer forensic analysis, because it was the first approach to be led by academia rather than law enforcement [64; 70]. It provides researchers with many methods of computer forensic analysis. However, its methods are unable to distinguish between insider and outsider attacks. They do not include a method of relational analysis. Furthermore, the DFRWS approach is usually a general model that does not consider how to conduct an investigation into insider and outsider attacks. It does not develop a data collection process, for example, that determines what data should be collected and why, how it should be analysed and what tools should be used to perform these processes., These shortcomings do not therefore provide sufficient information on the suspect, and ultimately impact upon the decision process.

4.2 DAMDIOA

This section addresses this issue of the distinction between insider and outsider attacks by improving DFRWS's methods. It proposes DAMDIOA, which has been created to help corporate security investigators carry out investigations into digital crime by distinguishing between these two types of attack by focusing on improving the process of data collection and analysis. It uses a combination of two types of analysis: "timeline activity" analysis and "relational" analysis. These methods reconstruct an insider's activity from the various outputs of an organisation's security and personal devices in order to identify normal and abnormal activities, such as activities before and after a particular incident. The analysis subsequently identifies a relationship between these activities and the insider's job responsibilities. This model brings about a decision on whether the attack has been committed by an insider or an outsider. It therefore achieves the following aims:

- it reduces the risk of wrongly identifying suspects
- it avoids financial loss for the organisation

- it protects an organisation's reputation
- it provides corporate security investigations with a structured investigation process for distinguishing between insider and outsider attacks

Because any investigation that seeks to distinguish between the two types of attack starts with a large amount of data (job responsibilities, legitimate and suspicious activities), using deduction to extract the relevant evidence, DAMDIOA is represented by an inverted triangle. The evidence revealed usually exposes the differences between insider and outsider activities. This model is therefore used to distinguish between insider and outsider attacks after an insider denies allegation of breaching security. Figure 7 demonstrates the main processes of DAMDIOA.

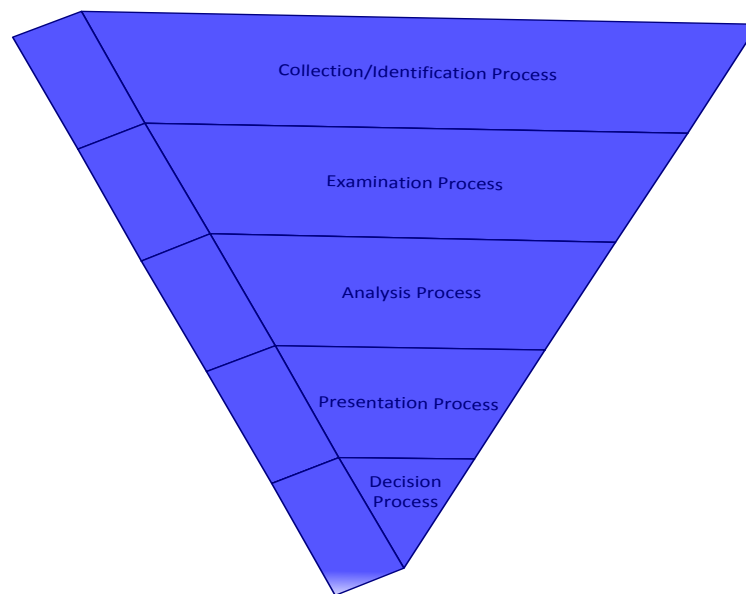


Figure 7: DAMDIOA Model

DAMDIOA consists of many main processes.

4.2.1 Collection/identification process

This process is concerned with searching and collecting all user (i.e. insider) activities in order to provide an analysis process with sufficient information to make a distinction. It is intended to maximise the retrieval of all user actions and to provide data that is

useful for investigating malicious insider activities that occur during an attack. It uses stored information located in many sources. Certain information such as the time and type of incident would be useful before the investigation proper begins, in order to save the investigators time and effort.

4.2.1.1 Review of Network Diagram

It is essential for corporate security investigators to review the diagram of an organisation's IT infrastructure before conducting a digital investigation to distinguish between insider and outsider attacks. This diagram of an IT infrastructure leads to an understanding of the structure of an organisational network, as well as identifying the locations of both legitimate and suspicious activities. It facilitates the identification and collection of general and technical details such as:

- determining which security devices are being used
- which computers were involved in the incident
- which computers contain investigative information

For example, Figure 8 illustrates general and technical information for organisational IT networks, which consist of three parts: external, DMZ and internal networks. In this example two firewalls are set up, both of which have two interfaces. The interfaces of the first firewall connect the external and the demilitarized zone (DMZ) networks respectively, while those of the second connect the DMZ network and an internal network respectively. The diagram also implies that there is a chance of retrieving valuable information from the internal firewall log, as well as showing that there are not many application servers; for example, this company has no file server and no web server. Therefore, these activities have been retrieved from:

- the mail server (emails)
- the insider's computer (files/folders)

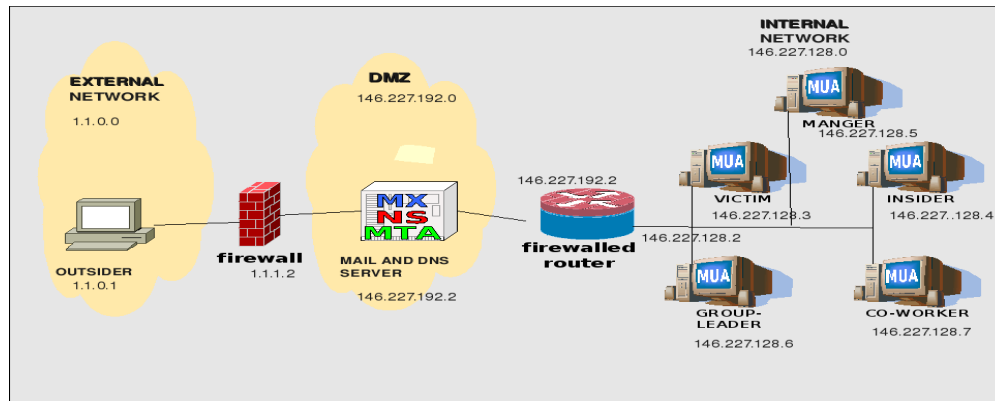


Figure 8: Diagram of IT infrastructure

4.2.1.2 Collection of job role/responsibilities for an insider

Following the review of the diagram of an organisation's IT infrastructure, the insider's job responsibilities should be reviewed. The main purpose of this is to understand the insider's job activity. This review assists in mapping the relationship between any computer activities such as emails and the insider's job activity. For example, reviewing the insider's responsibilities will help identify their business emails, and any files and folders that have been created and modified for them. This job responsibility information should be collected from the Human Resources Department or from an insider's supervisor.

4.2.1.3 Collection of legitimate and suspicious activities

Collection of devices, such as an insider's computer that may have been involved in a security incident or that may contain legitimate activities, is a critical step because it may involve the collection of real-time information that might otherwise be lost, as well as stored information. Because the investigation is designed to distinguish between insider and outsider attacks, it is necessary to identify precisely which computers have been involved in a crime, and which computers' networks or systems contain legitimate data and which contain suspicious data that would be subject to investigation for the purpose of identifying a suspect.

Collection also creates an opportunity for a corporate security investigation to collect large amounts of volatile data from an insider's computer. Volatile data is valuable investigative data that is available for only a certain period of time; it includes network

connections, running processes and memory dumps, and can help identify any connection between an insider's and an outsider's computers, as well as identifying any business activities performed by an insider.

This step is also responsible for identifying which organisational resources an insider is allowed to access, so that the logs specific to them can be obtained, as well as being responsible for protecting the integrity of the original data by securing and forensically imaging, fully or partially, the organisation's or insider's devices such as hard disks, laptops and USB memory sticks, which are usually involved in a crime and contain data of use to an investigation.

4.2.1.4 Collection of information regarding previous security incidents

The purpose of collecting information about technical history, such as a previous security incident, is to establish whether the insider's computer was subject to penetration by an outsider. It should consider how a network administrator or a help desk dealt with the security incident. For example, it should collect the following information:

- whether any incident report has been received from the insider or security logs (an IDS)
- if it has, whether the security log for the insider's computer has been checked and any failed logins noticed.
- whether the anti-virus has been run to check the computer's applications, or whether the password has been changed?.

This information can be collected from a network administrator or a help desk. Figure 3 shows the information sources from which data may be collected that may help distinguish between insider and outsider attacks.

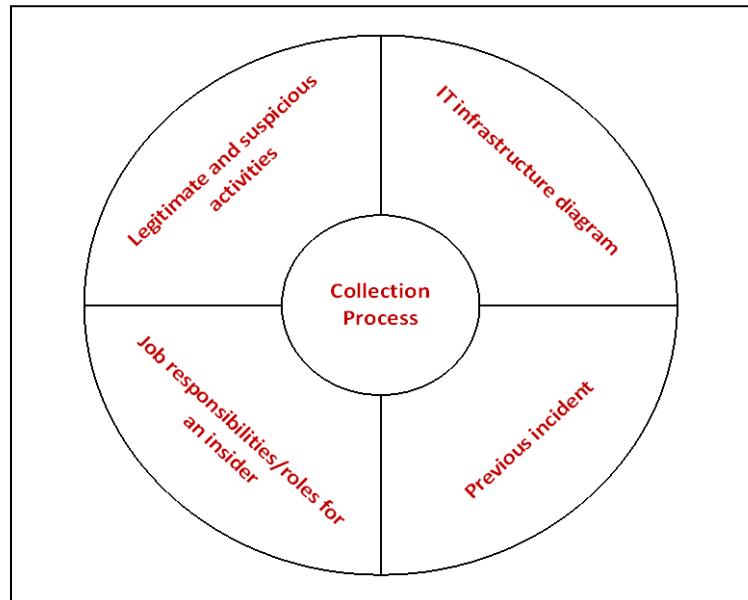


Figure 9: Information sources of data collection

Data collection is therefore responsible for retrieving the following information:

- the date and time of an incident
- the type of incident
- the source of legitimate and suspicious activities as follows:
 - i. devices that contain information of potential use to an investigation. These are:
 - programs that have been used as tools to commit digital crime by allowing outsiders to gain insider access to the latter's computers, which have specific vulnerabilities
 - information stored on the hard disk that may contain users' job responsibilities
 - ii. information as evidence on the log file that allows the revealing of the time of activities as follows:
 - when the insider accessed the Internet or Intranet
 - when they accessed their online banking and shopping accounts
 - when they created and modified a file
 - when they sent, forwarded and received an email

- when they accessed an application server or a database server
 - when they downloaded or uploaded data
 - when they made a call from their business landline or business mobile
- iii. identification of the insider's job responsibility

Figure 10 shows the process of data collection in order to distinguish between insider and outsider attacks.

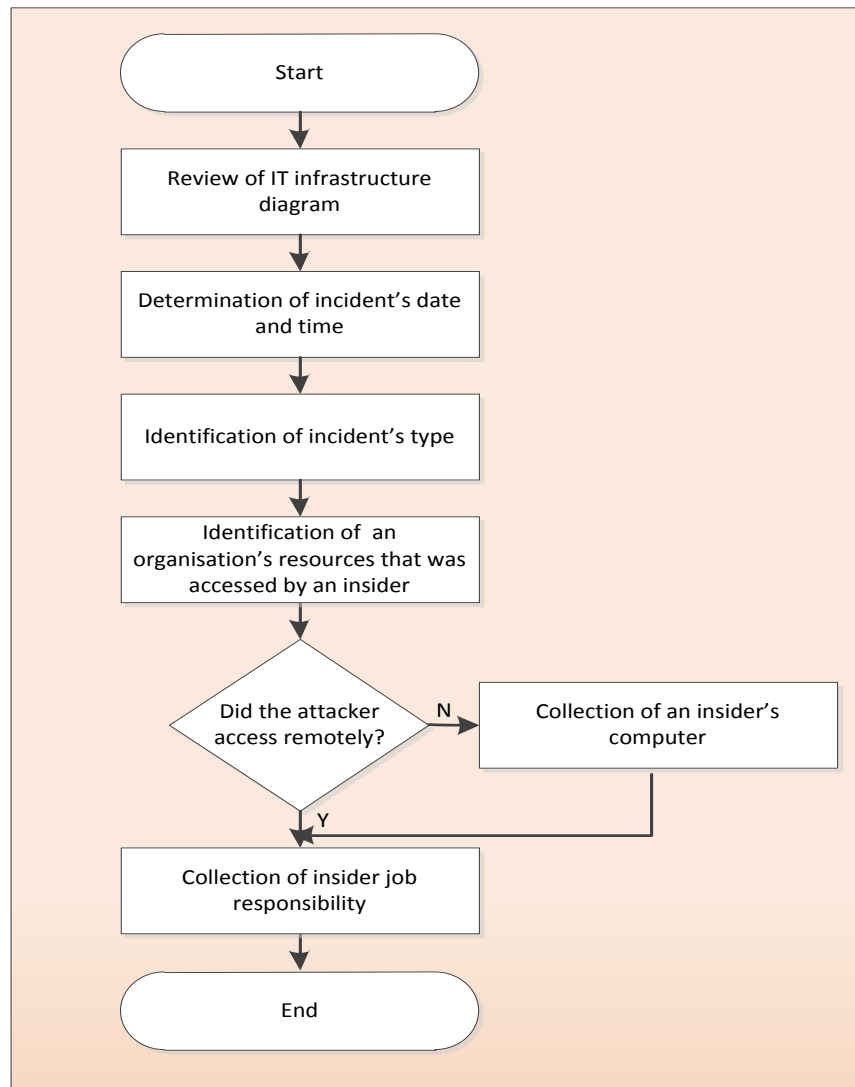


Figure 10: Data collection process

4.2.2 Examination process

This aims to examine all the user activities collected in order to retrieve all insider activities from log files and from the insider's computer during the period of an attack. The process begins by checking the logs of interest – those that log the insider's activities.

The process is also intended to search for and recover the insider's protected data and deleted files. Insiders may use passwords to protect their files and folders on their local hard disks. These files and folders should be examined to establish whether or not these files and folders are part of their job responsibilities. The passwords are stored on the Security Account Manager (in Windows) or password or shadow file (in Linux). They can be recovered by using any available password cracking software such as AccessData or John Ripper. Figure 11 shows the examination process used to distinguish between insider and outsider attacks.

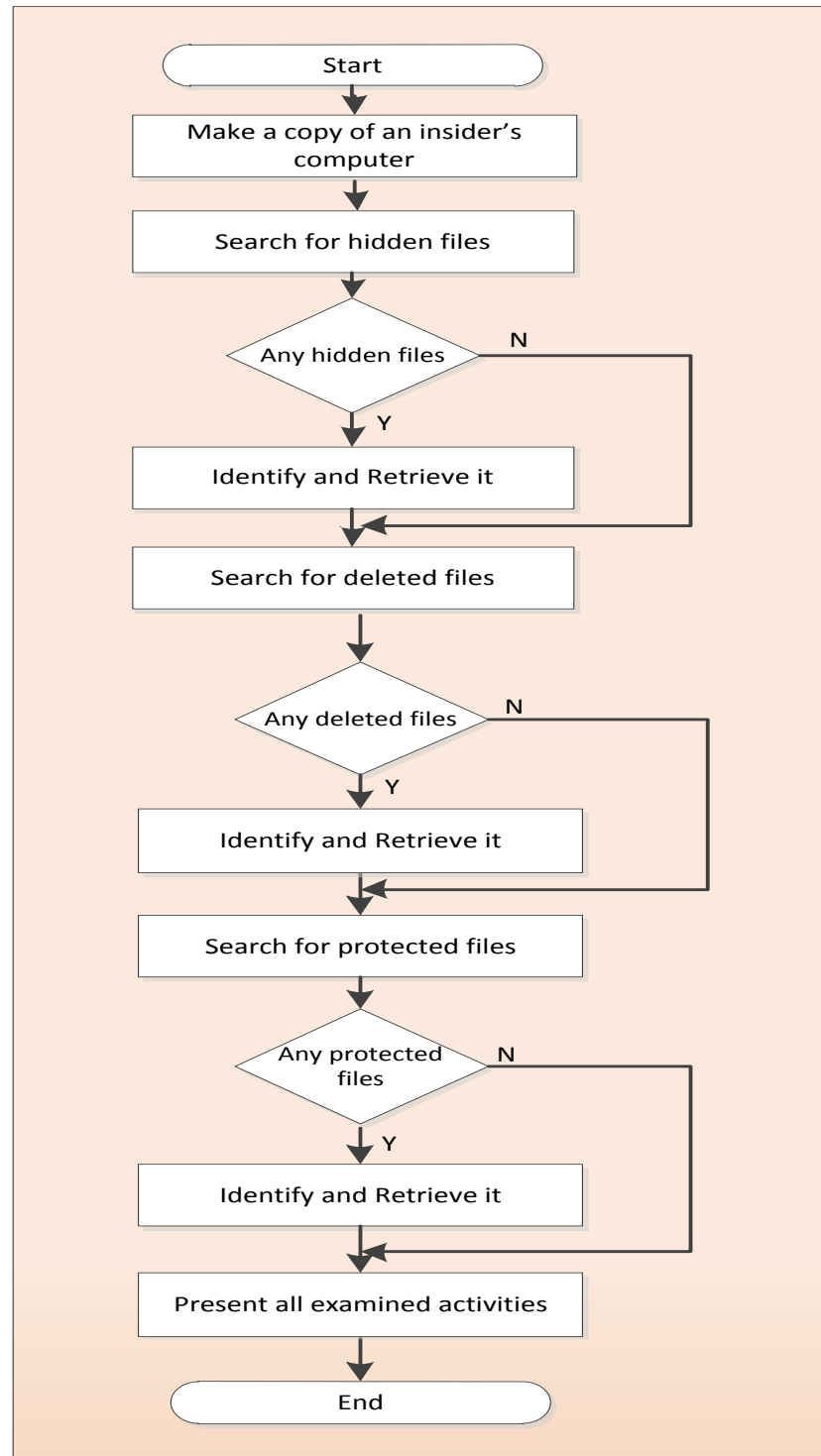


Figure 11: Examination process

4.2.3 Analysis process

This step is extremely important, because it is where evidence may be discovered that assists in distinguishing between insider and outsider attacks. It is responsible for reconstructing employee activities by reviewing and analysing information such as email activities, file activities and system logs. It also links insider or outsider attacks with particular malicious events such as downloading and executing a Trojan horse or sending an abusive email, these being distinct from normal activities such as creating reports. Analysis could also be used to determine whether an insider's computer that was involved in a crime was vulnerable to penetration. It may even be able to discover new evidence, which requires identifying and capturing more data from different devices such as firewall logs or IDS logs. "Timeline" and "relational" analysis" are used to distinguish between insider and outsider attacks.

4.2.3.1 Timeline analysis

"Timeline" or "timestamp" is a date or time stored or communicated by an electronic medium. Computer systems store timestamps in many ways as determined by various rules [103]. Timestamps are usually stored whenever a file is created, modified or accessed. Furthermore, the majority of computer systems have logging functions that use timestamps to log activities. Timelines are important in digital forensics in establishing the correct sequence of events and associating a particular user with a particular time [43; 44]. It is also a fundamental method of activity reconstruction during case investigations [103]. Timeline analysis may therefore help identify patterns and anomalies, and may lead to other sources of evidence [12]. It shows what activities had been performed before and after the occurrence of an incident. The researcher employs timeline analysis to identify this time period.

- ***Identification of attack period/session***

Identification of the attack period is significant if a distinction between insider and outsider attacks is to be made so that relevant user activities can be discovered and time spent collecting data can be reduced. The attack period is the time interval from the time

of login before the attack to the time logout after it. To identify this period, the following information should be determined:

- date and time of the attack
- login and logout activities for the attack period

The following hypothetical example demonstrates the use of timeline analysis. At 0910 a background file on a file server was accessed and then modified. At 1046 an email was sent to a Background Investigation Agent. At 1050 an abusive email was sent, and an email was subsequently received from the Background Investigation Agent. In addition, a Weekly Security Incident Report was created on an insider computer at 1158.

The report should identify the date and time of the incident. The incident took place on the 3rd of March 2010 at 1050; the report should collect user activity for that date, and should then classify these activities as a series of sessions based on the time of login and logout. After that, it should identify the session in which the attack took place in order to analyse these user activities. Figure 11 shows that there are 3 sessions of user activities, each of which starts with the user's computer (i.e. client) login and ends with its logout. This figure shows that the attack, called the "attack session", took place in Session 1. Figure 12 presents these activities by using timeline analysis to identify and obtain relevant user activities during the attack period.

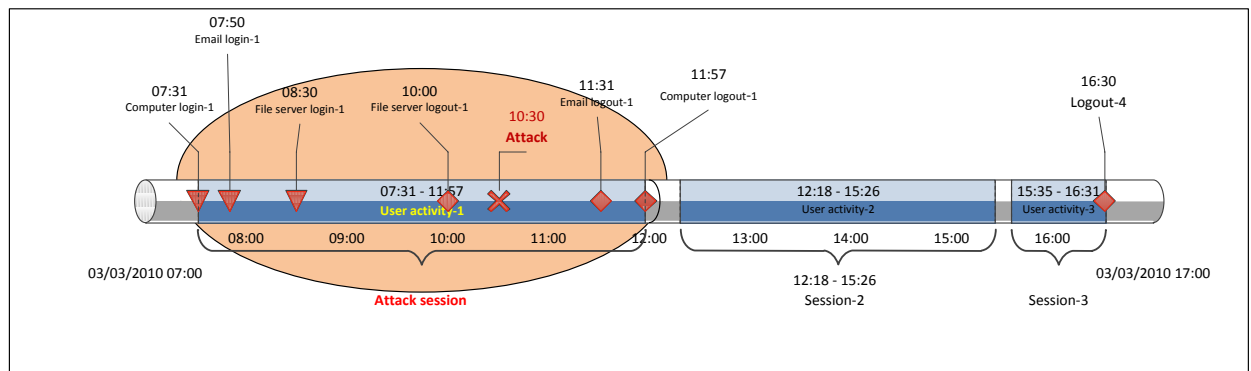


Figure 12: Timeline analysis revealing attack session

Identification of the attack session helps the collection and analysis of particular user activities, resulting in reduced effort and time spent on such analysis.

- **Attack session analysis**

After the attack session has been identified, the user activities carried out during it are analysed in order to provide relational analysis with data regarding particular user activities. Figure 13 shows that many activities were performed during the time of the incident, including the sending of two emails and the accessing of two files. These activities must be analysed in order to identify whether or not they were carried out by the insider.

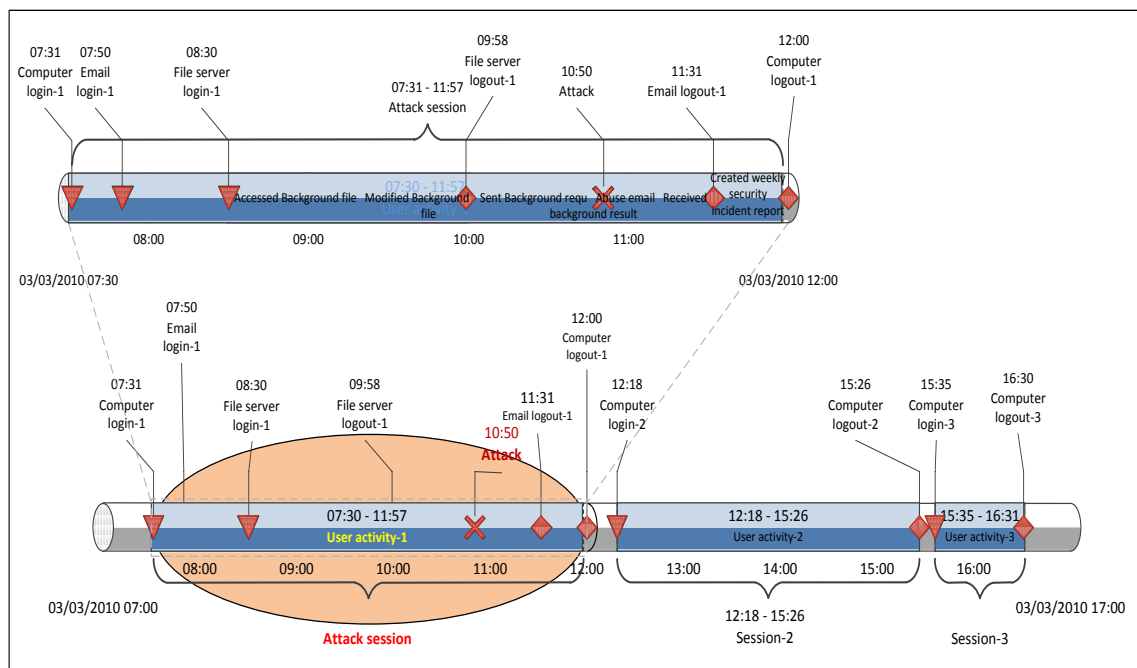


Figure 13: Review attack period activity

It is important that the analysis of a given network's log should consider the gap between sessions, because the attacker may carry out a legitimate activity on another server during this period. The insider's own computer should also be examined for the same period in order to collect this data concerning this activity, which could help

distinguish between insider and outsider attacks. Figure 14 shows these gaps between sessions.

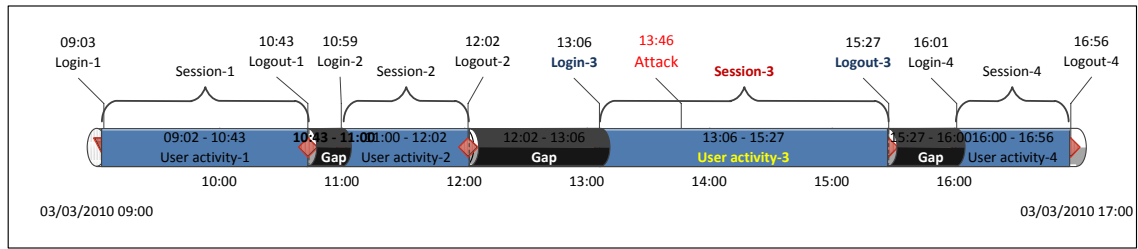


Figure 14: Examine gap between sessions

For example, at 1205 the insider logged onto a file server, created a monthly statistical security incident report and modified a statistical background report, logging out at 1305. Figure 15 shows that analysis of the gap before the incident took place (i.e. Session 3, between 1210 and 1310) reveals some user activities to have been performed on a file server.

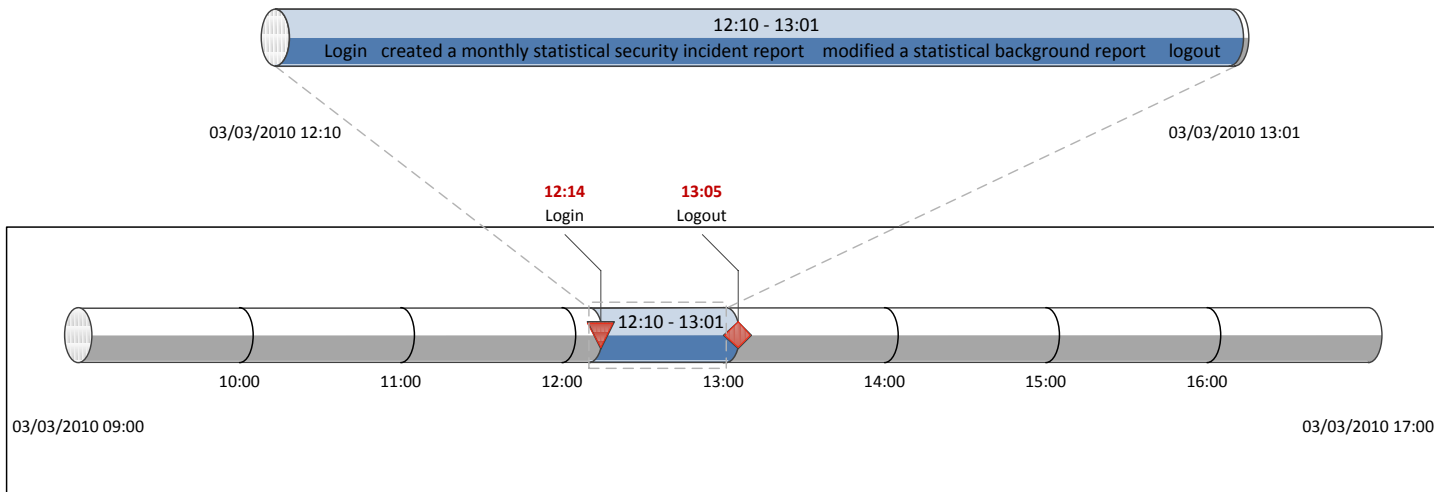


Figure 15: Analysis of the gap between login activities

However, timeline analysis alone is insufficient to distinguish between insider and outsider attacks, because it usually identifies patterns and anomalies only. Because it highlights activities before and after the time of an incident, it can point the way to other sources of evidence. It does not, however, analyse the relationship between these

anomalies and the insider's ordinary activities. Relational analysis, whereby relationships between a suspect's activities and an insider's job responsibilities are identified, is also required in order to address this issue. Timeline analysis is useful to identify the following:

- attack period
- activities during the attack period
- the time that these activities took place

4.2.3.2 Relational analysis

This creates nodes representing insiders' day-to-day activities as well as their alleged malicious ones in order to determine if there are connections between them [12].

Relational analysis is used to identify the following:

- Activities carried out before and after the time of an incident, in order to identify possible matches between them and the insider's job responsibilities. As mentioned previously, insiders are classed as such largely by virtue of the authorised access that allows them to perform their legitimate tasks. Relational analysis should identify whether these activities are indeed legitimate. The occurrence of an insider attack may be indicated by an instance of malicious activity in a series of legitimate ones, because an outsider often has no prior knowledge of an insider's job responsibilities. The aforementioned timeline analysis shows an anomaly – a malicious event occurring as part of a series of legitimate ones carried out by the insider. Figure 16 shows that there were user activities and that their content was examined, after which they were compared with insider job responsibilities. If there is a link between these activities and the job responsibilities, it is a sign of an insider attack.

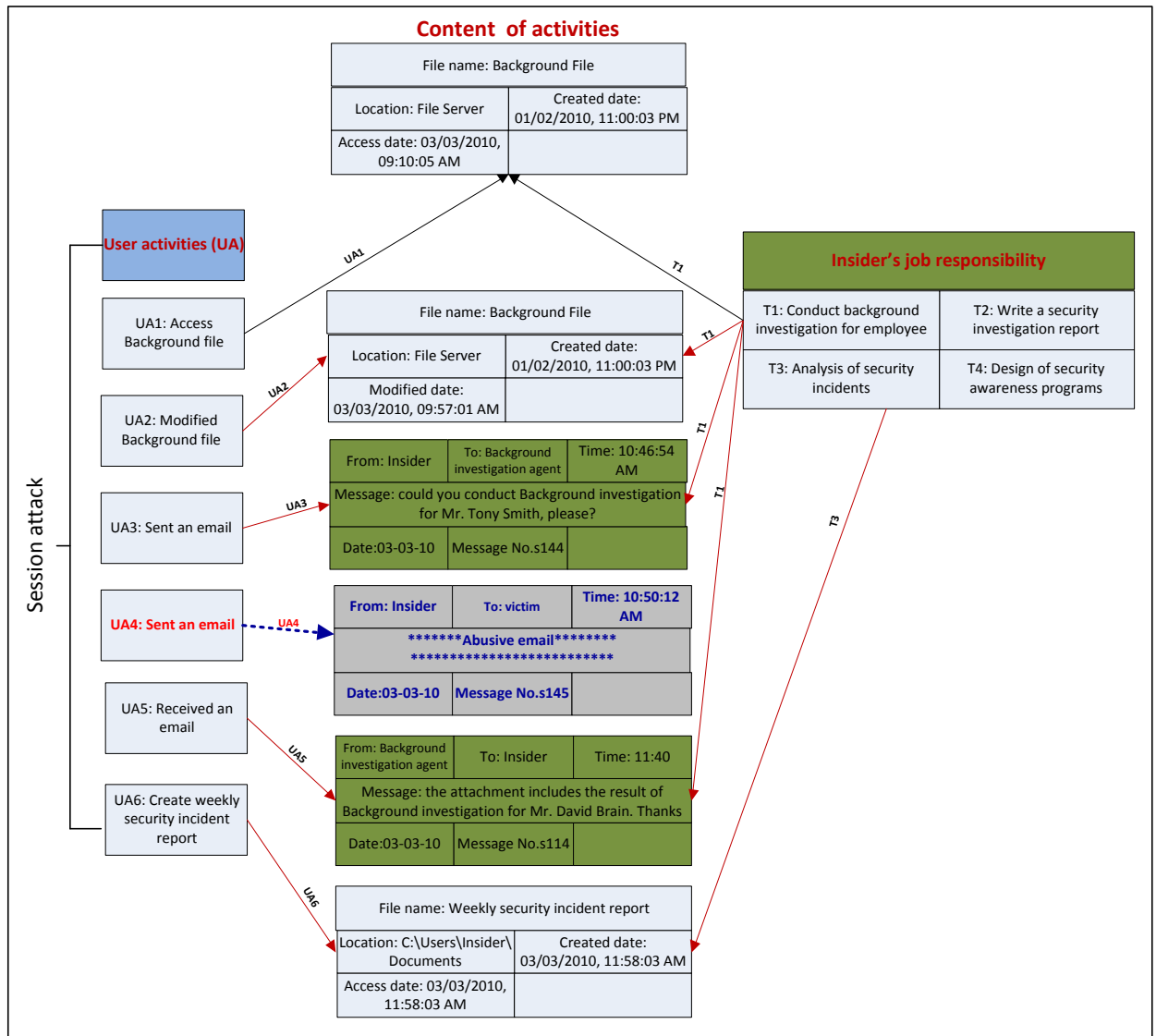


Figure 16: Relational analysis examination of the activities relation

- A relationship between an insider and a victim, an example being an abusive e-mail. The relational analysis will review previous emails for a certain period in order to establish a pattern of behaviour in determining if the malicious occurrence is an obvious anomaly. This examination is beyond the scope of this research, however.
- A relationship between suspicious events and an exploitation of a system's vulnerability. As already mentioned, one method of outsider attack involves the exploitation of a client-side application. An example of what this could lead to if

a system is not properly maintained it codes automatically downloading themselves as soon as an insider accesses a Web page.

Relational analysis is useful means of establishing a link between malicious events and an outsider's activities. For instance, when an outsider installs a Data-Sending Trojan on an insider's computer, this Trojan provides an outsider with passwords and other confidential data. Insiders' keystrokes can also be sent to the outsider, via email or by connecting to the outsider's website, by means of key-loggers installed by Data-Sending Trojans. Relational analysis will therefore be used to analyse the relationship between these activities and an outsider. It will also analyse how an outsider gained insider access by determining whether the insider's computer was vulnerable. Figure 17 shows the analysis process.

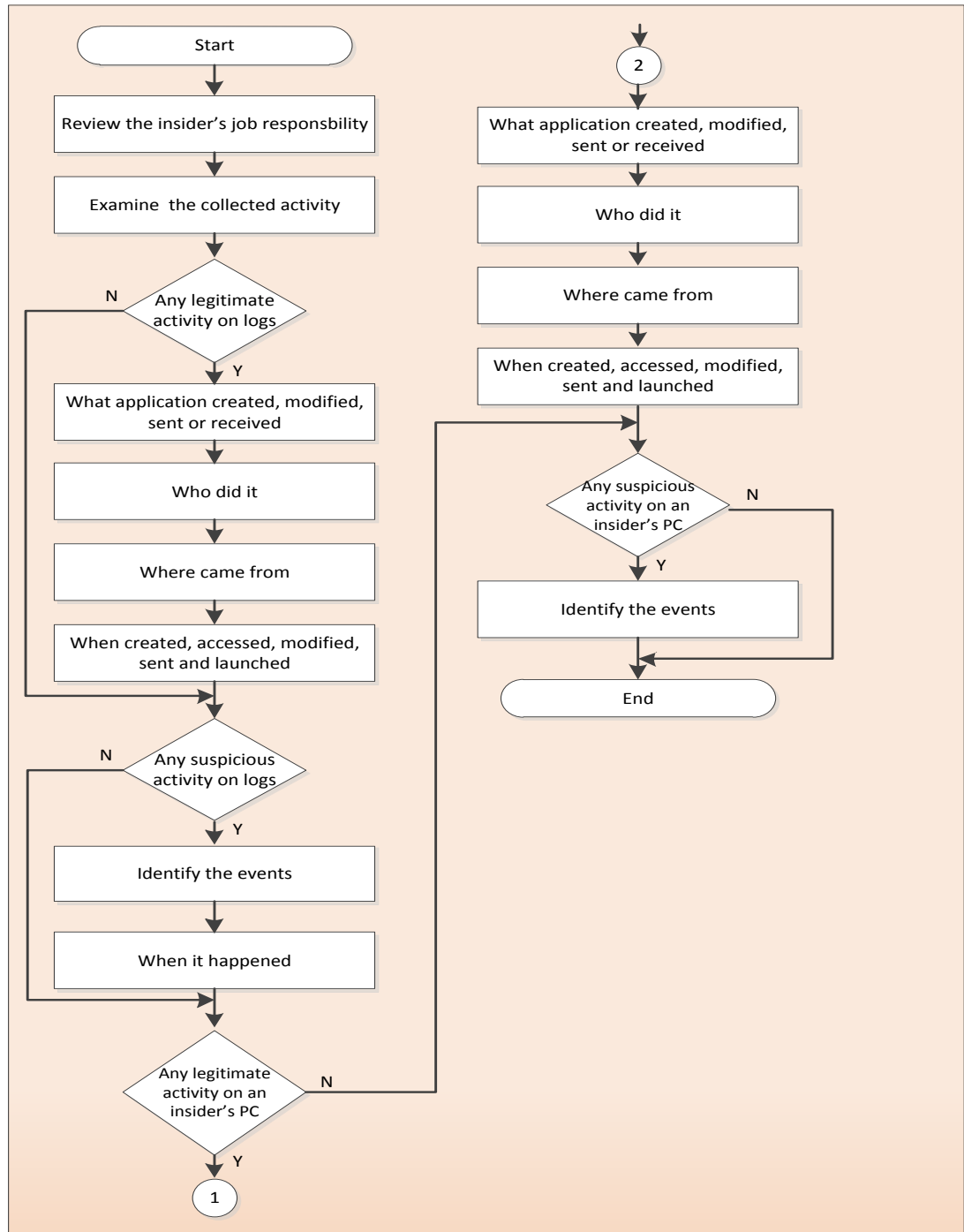


Figure 17: Analysis process

4.2.4 Presentation process

This is concerned with assigning the analysed activities a numerical value in order to

facilitate the distinction between insider and outsider attacks. Insider job activities are represented by “-1”, whereas suspicious activities (i.e. those not part of an insider's job responsibilities) are represented by “1”. An attack is represented by “0”.

4.2.5 Decision

After representing each activity i with a numerical value a_i , the decision process is the final step to distinguish between insider and outsider attacks. This thesis proposes two types of decision process as follows:

4.2.5.1 Fixed decision

This type of decision is based on a predetermined logical condition, which is why it is simple to implement. The average of the activity types is calculated by using this equation: average of activities $A = \sum a_i$ (total of activities that were being performed) / N (total number of activities). If $A < 0$, the attack is likely to be insider, while if $A > 0$, it is likely to be outsider. If $A=0$, it is likely unknown attack.

According to the aforementioned example of relational analysis, a type of user activity presented in table 11.

Table 11: Type of user activity

Timeline activity	Type of activity
9:10:05	-1
9:57:01	-1
10:46:54	-1
10:50:12	0
11:40:54	-1
11:58:03	-1

$$A = -5/6 = -0.83$$

$A < 0$; it is likely an insider attack.

4.2.5.2 Customisable/tailored decisions

In this section, a new approach is proposed which uses a threshold of suspicious activities to distinguish between insider and outsider attacks. The flexible equation is as follows:

N_l : number of legitimate activity

N_s : number of suspicious activity

N_a : number of attack

R : proportion of suspicious activity

$$R = \frac{N_s}{N_l + N_s + N_a}$$

Th: Threshold

Decision:

If $R > Th$ is outsider

If $R < Th$ is insider

If $R = Th$ is unknown attack

This decision is based on the proportion of suspicious activities. An organisation can customise its threshold of tolerance for such activities based on its level of concern for the type of attack involved. Each organisation develops its security policies on the basis of risk analysis. It collects data on the threats that its type of business may face and attempts to rate each hazard in terms of the cost to it of each incident [82]. This type of decision will help the organization focus on the incident because the threshold it has already determined allows it to adjust its response to the level of suspicious activity involved.

According to the aforementioned example of relational analysis, it was found that the number of legitimate activities $N_l = 5$, the number of suspicious activities $N_s = 0$ and the number of attack $N_a = 1$.

$N_l : 5$

$$N_s : 0$$

$$N_a : 1$$

$$R = \frac{0}{5+0+1} = 0 \text{ the proportion of suspicious activities} = 0$$

For example, if the insider work for a bank which is vulnerable to fraud, both from insiders and outsiders. A bank can customise $th = 0.2$. Therefore, if $r > th$, it is most likely to be an outsider attack. Otherwise it is more likely an insider attack. The attack in this example is therefore most likely to be an insider one. Chapter 6 will discuss the differences between the levels of threshold and the differences between fixed and customisable decision.

4.3 Summary

The main aim of this chapter was to discuss the advantages and disadvantages of DFRWS methods and to present DAMDIOA. Chapter 4 discussed the former's advantages and disadvantages. Advantages include the fact that it is the first approach to have been led by academia, and that DFRWS methods provide researchers with many means of computer forensic analysis. On the other hand, relational analysis is not considered, and the model, being a general one, does not take into account how to conduct an investigation into insider and outsider attacks, nor does it identify which data should be collected.

The process by which DAMDIOA distinguishes between insider and outsider attacks was discussed. These processes are:

- **Collection**, in which the interest logs and computers involved in the crime or which hold investigative information are gathered
- **Examination**, in which these activities are reviewed and deleted, hidden and protected data are retrieved
- **Analysis**, in which the relationship between these activities and the insider's job responsibilities is ascertained
- **Presentation**, in which the analysed data is presented
- **Decision**, in which the culprit is identified

The following chapter will test and evaluate this framework. A virtual network and computers will be implemented, and email attacks will be carried out on them. The model will be used to collect, examine, analyse and present these activities, after which a decision will be made regarding whether these attacks were carried out by insiders or outsiders.

5 Experiments

Objectives:

-
- to test the hypothesis
 - to conduct experiments discuss the results
 - to evaluate the results of experiments by using fixed and customisable decision
-

This chapter aims at testing the hypothesis, by conducting a number of email attack experiments which will either support or refute the hypothesis. It also evaluates the results of this model.

5.1 Hypothesis

This research proposes that, under certain circumstances, it is possible to distinguish between insider and outsider attacks when conducting computer incident investigations.

5.2 Experiment components

This section discusses the network infrastructure, software and tools used in the experiment. This experiment is designed to build a virtual network in order to carry out an email attack; the thesis hypothesis will then be tested. Table 12 summarizes the components of the experiment's infrastructure.

Table 12: Components of the Experiment's infrastructure

	Infrastructure	Description
1	Linux-Ubuntu	Operating system
2	Netkit	Free software to create virtual network for Test company that contains 8 machines
3	EXIM4-mail	MTA program to send emails between MUA
4	PINE-mail	MUA program to read and write emails
5	BIND	DNS to translate IP address to names
6	MX	collect incoming mails for a domain (test.com)
7	Tcpdump	Collect and log all TCP/IP packets
8	Wireshark	Analyse all collected TCP/IP packets
9	Iptables-firewall	Implement security policy

5.2.1 Experiment design

This chapter designs eight experiments, which cover all the possibilities of computer attack investigations. These possibilities include authorised access, stolen insider password, password guessing, blank password, exploiting the weakness of SMTP authentication, initiation attacks from inside and outside an organisation and attacks within an organisation's control. An experiment was designed to conduct a digital investigation into distinguishing between insider and outsider attacks.

The scenario is that a victim has received an abusive email apparently from an insider. The insider refutes the allegation of sending the email, and claims that his credentials (user name and password) were illegally obtained by an outsider.

5.2.1.1 Type of attack

This experiment involves an abusive email attack, which is common attacks because an employee can send an abusive email or send an organisation's file out an organisation. This attack does not always need skill to be carried out. Forgery and harassment by email usually go hand-in-hand [66].

5.2.1.2 Reason for the investigation

The reason for carrying out this investigation is to establish whether this attack has been committed by an insider or an outsider.

- Insider: incidents or attacks committed by authorised users. An insider is assigned many job responsibilities to perform.
- Outsider: incidents or attacks committed by unauthorised users who gain insider's passwords.

5.2.1.3 Investigation methods

- Timeline analysis of legitimate activities
- Relation analysis

5.2.1.4 Collecting data

- Full-content monitoring is used to collect TCP/IP headers and a datagram by using tcpdump to sniff all legitimate and suspicious activities over the network.

The purpose of conducting full-content monitoring is to analyse the TCP/IP headers (ICMP and SMTP) and datagram. A TCP/IP header will identify a source and the destination IP addresses, plus the destination port numbers and time and date of the packet. The analysing datagram will retrieve and identify insider job activities.

5.2.1.5 Analysing data

- Wireshark is used to analyse the legitimate and suspicious activities identified by tcpdump;
- “Ls”: this command is used to review the insider's files and folders;
- “Ls -l”: this command is used to review the creation of the insider's files and folders and review the time of their creation or modification;
- “Ls-a”: this command is used to list hidden files;

5.2.2 Established parameters of the experiment

Many parameters were used, as follows:

- Methods of Access (MA);
- Insider activities (IA);
- Time (T);
- Security Policy (SP).

These parameters are important, because both a timeline of activities and relational analysis (see Literature Review) were employed to distinguish between insider and outsider attacks.

5.2.2.1 Methods of access (MA)

There are many types of access to a network's resources (such as mail servers), including as follows:

- Password Guessing (PG): an outsider tries to find words used as insider passwords by guessing. Failed logins will be found in the security event log;
- Social Engineering (SE): an outsider tries to find the insider's password without guessing; for example, by finding a password written on a small slip of paper

placed close to an insider's computer. No failed login can be found;

- Authorised access (AC): access to an insider's account.

5.2.2.2 Insider Activities

An insider can be responsible for many activities, for example:

- gathering car accident reports;
- gathering injured employee reports;
- reducing the number of car accidents;
- producing a morning report that includes the number of car accidents and injured employees.

- **Emails**

Emails are one of the main ways by which an insider conducts an organisation's job activities. They are the main source for collecting information about an insider's activities and can help to distinguish between insider and outsider activities. This experiment divides emails as follows:

- **Business Email (BE):** the insider uses an organisation's email system to send and receive emails as one of his job activities. Therefore, if emails relate to one of the insider's job activities, they are called Business Emails (BE);
- **Non Business Email (NBE):** an organisation's email system is used to send and receive personal emails. If emails do not contain material relevant to the insider's job activities, they are called Non-Business Emails (NBE).

- **Insider Data Stored**

The insider uses an organisation's computer to create, modify, read and store files/folders. The insider's computer is another source from which information about their activities can be collected; it can also be used to help to distinguish between insider and outsider activities. If these files/folders are relevant to job activities, they are called Business Files/Folders (BF).

If these files/folders are not relevant to job activities, they are called Non-Business Files/Folders (NBF).

5.2.2.3 *Timestamp (T)*

The time parameter is used to establish the correct sequence of events before and after an incident. It comprises the time of access and an activity timeline.

- All activities (methods of insider access, email activities and PC activities) during attack sessions

5.2.2.4 *Security Policy*

The security policy is designed and implemented to log both the legitimate activities and suspicious activities of an insider in order to analyse these activities and then create a match between these activities and the insider's job responsibilities.

- Legitimate activities: legitimate user activities are logged in order to determine all the activities undertaken before and after the incident;
- Failed logins: all failed logins aimed at accessing the insider's email inbox are logged in order to discover any intruder activities.

5.2.3 *Network Infrastructure*

The experiment comprises setting up a virtual network. A virtual network comprises three elements of an organisation's network, as follows:

- an external network
- a Demilitarised Zone (DMZ)
- an internal network.

Figure 18 illustrates the network structure for the experiments. Further information about the technical infrastructure is presented in Appendix A4.

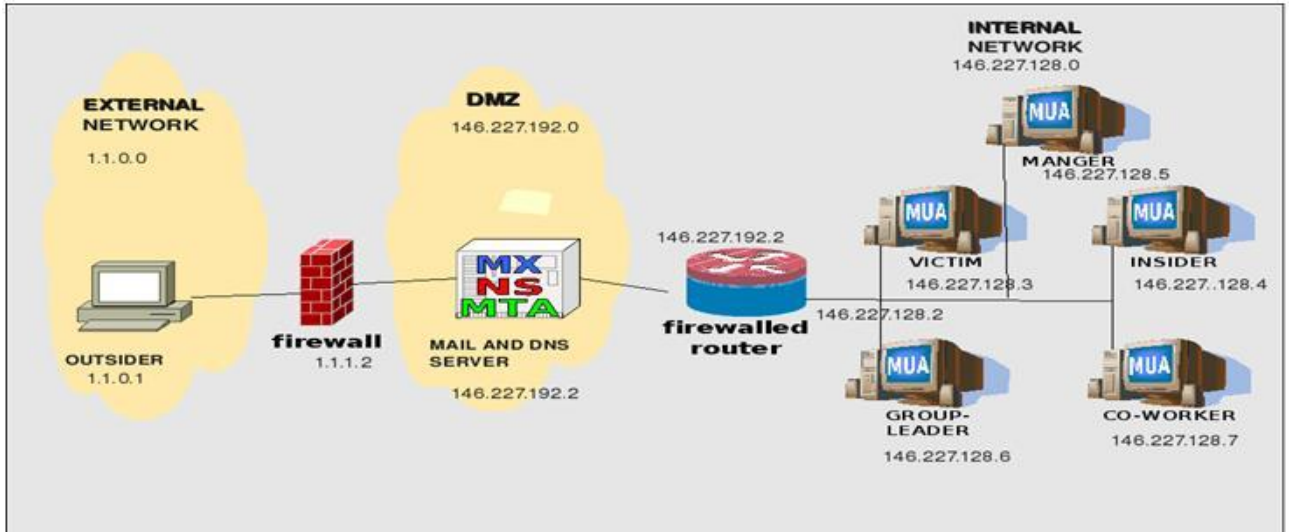


Figure 18: Network infrastructure for Experiments

5.2.3.1 Virtual Network Components

- Five clients are set up in the internal network at the same domain, as follows:
 - 1- victim (Alice) is configured with IP 146.227.128.3;
 - 2- insider (Bob) is configured with IP 146.227.128.4;
 - 3- manager (Tim) is configured with IP 146.227.128.5;
 - 4- group-leader is configured with IP 146.227.128.6;
 - 5- co-worker (Sarah) is configured with IP 146.227.128.7.

- One server is set up in the DMZ to provide different services, as follows:
 - 1- Mail Exchange (MX) (see the next section)
 - 2- Name Services (NS)
 - 3-Mail Transfer Agent (MTA)

Figure 19 shows the components of the mail server: MX, NS and MTA.

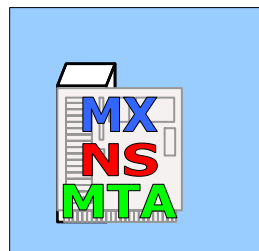


Figure 19: Components of the experiment's mail server

- Two routers are set up between the external and internal networks as follows:
 - 1- Firewall (fw-1)
 - 2- Firewall (fw-2)

Fw-1 has two interfaces: the first interface connects to an external network and the second interface connects to a DMZ network. Fw-2 also has two interfaces: the first interface connects to the DMZ network and the second interface connects to an internal network.

Further information about setting up the network and how it works is presented in Appendix A5.

5.2.3.2 Iptables Policy

Iptables is a command line program that is used to configure the Linux Ipv4 packet filtering rule set. It is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Further information about iptables is presented in Appendix A1.

The firewall policy is configured as follows:

- This policy records any traffic that comes to port 25 that is also from the source IP address 146.227.128.4 to the destination IP address 146.227.192.2.

```
iptables -A FORWARD -p tcp --dport 25 -s 146.227.128.4
-d 146.227.192.2 -j LOG --log-prefix ***mailattack***-
-log
```

- This policy records any traffic that comes to port 110 that is also from the source IP address 146.227.128.4 to the destination IP address 146.227.192.2.

```
iptables -A FORWARD -p tcp --dport 110 -s
146.227.128.4 -d 146.227.192.2 -j LOG --log-prefix
***mailattack***--log
```

- This policy records any traffic that comes to port 143 that is also from the source IP address 146.227.128.4 to the destination IP address 146.227.192.2.

```
iptables -A FORWARD -p tcp --dport 143 -s
146.227.128.4 -d 146.227.192.2 -j LOG --log-prefix
***mailattack***--log
```

- This policy allows the specific subnet to connect to the mail server, port number 25 (IP address 146.227.192.2).

```
iptables -A FORWARD -p tcp --dport 25 --source  
146.227.128.0/26 --destination 146.227.192.2 -j ACCEPT
```

- This policy allows the specific subnet to connect to the mail server, IP address 146.227.192.2 and port number 110.

```
iptables -A FORWARD -p tcp --dport 110 --source  
146.227.128.0/26 --destination 146.227.192.2 -j ACCEPT
```

- This policy allows the specific subnet to connect to the mail server, port number 143 (IP address 146.227.192.2).

```
iptables -A FORWARD -p tcp --dport 143 --source  
146.227.128.0/26 --destination 146.227.192.2 -j ACCEPT
```

5.2.4 Software

5.2.4.1 Operating System (OS)

Linux-Ubuntu 9.04 Desktop is distributed as free and open source software [93]. It comprises multiple software packages typically distributed as free software or under an open source licence. Further information about Ubuntu's requirements is presented in Appendix A2.

5.2.4.2 Netkit

This software was conceived as an environment for setting up and performing networking experiments at low cost [61]. Netkit allows the creation of many virtual network components that can be interconnected in order to develop a network on a single personal computer or a laptop. Further information about Netkit's requirements is presented in Appendix A3.

5.2.4.3 Pine

Program for Internet News & Email (Pine) is a common mail user agent [96]. It allows a user to read, send and manage emails. It also allows connections to mail servers and manages incoming/outgoing email [96]. Users must be authenticated on the incoming mail server to get their incoming emails. Post Office Protocol (POP3) port 110 is used

to read emails from a local client and Interactive Mail Access Protocol (IMAP) port 143 is used to view emails from the email server.

5.2.4.4 Exim4

A Mail Transfer Agent (MTA) is a server acting as an outgoing mail dispatcher [94]. It does the job of transferring messages from one host to another. After the mail reaches its destination hosts, the agent delivers it into user mailboxes or to the processes that manage user mailboxes. Simple Mail Transfer Protocol (SMTP) port 25 is used to transfer outgoing mail. It was originally designed for passing messages between MTAs, but that was later subverted for the purpose of submitting new messages to an MTA, which is quite a different kind of operation [94].

5.2.4.5 BIND

Berkeley Internet Name Domain is a hierarchical naming system for computers and services connected to a LAN or Internet. It is responsible for translating hostnames into IP addresses [95].

5.2.4.6 Message Exchange (MX)

This is a server that collects incoming emails for a specific domain (test.com). Each domain which allows users must have at least one mail exchanger [95]. MX records are part of the DNS information for a domain [95].

When a foreign mail server wants to send a message to an address at test.com, the foreign server will first attempt to deliver the message to mail.test.com.

5.2.4.7 Investigation Tools

- **Tcpdump**

This is a network packet analyser tool that allows an investigator to intercept and display TCP/IP being transmitted or received over a LAN [92]. It allows the logging of the content of email packets. Tcpdump runs under the command-line. It prints out the headers of packets on a network interface. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis [92].

- **Wireshark**

This software is one of the best network protocol analysers [105]. The current experiment uses Wireshark to conduct analysis of insider network activities (sending and receiving of emails). Wireshark also has display filters and is able to read and capture file formats for tcpdump.

5.3 Conduct of Experiments

The experiment in fact comprises a series of experiments, conducted in order to test the hypothesis by looking for evidence which shows that it is possible to distinguish between insider and outsider attacks. This section presents only the analysis and decision processes of each experiment (see Appendix B for further information about the experiment as a whole).

5.3.1 Experiment (Ex) 1

A victim reported that she received an abusive email from her co-worker, which is his email address insider@test.com. The IT security interviewed an “alleged” suspect and he denies this allegation.

5.3.1.1 Timeline analysis

The OS usually records the time of the very last action that was performed in terms of user activities, such as file and folder activity. This information is a valuable source of evidence which can assist in distinguishing between insider and outsider attacks. Moreover, the system stores file timestamps to keep a record of the file creation time, the last time the file was accessed and the last time the file was modified. Therefore, user activity timeline analysis helps in identifying the file creation time, as well as the last time the file was modified on the insider’s computer and the emails that were sent and received. In the experiment, when the timeline analysis had identified all the insider's activities (email activity and file activity), it helped to identify the sequence of all the activities. It found that the abusive email had been sent when the insider was carrying out activities consistent with his job responsibilities. After the insider had logged out from the mail server, he created several files and stored them on his computer.

Figure 20 shows that the period during which the attack took place was from 10:30 p.m. to 12:03 p.m. It also shows that some activities were performed before and during the period of the attack, including emails being received and sent.

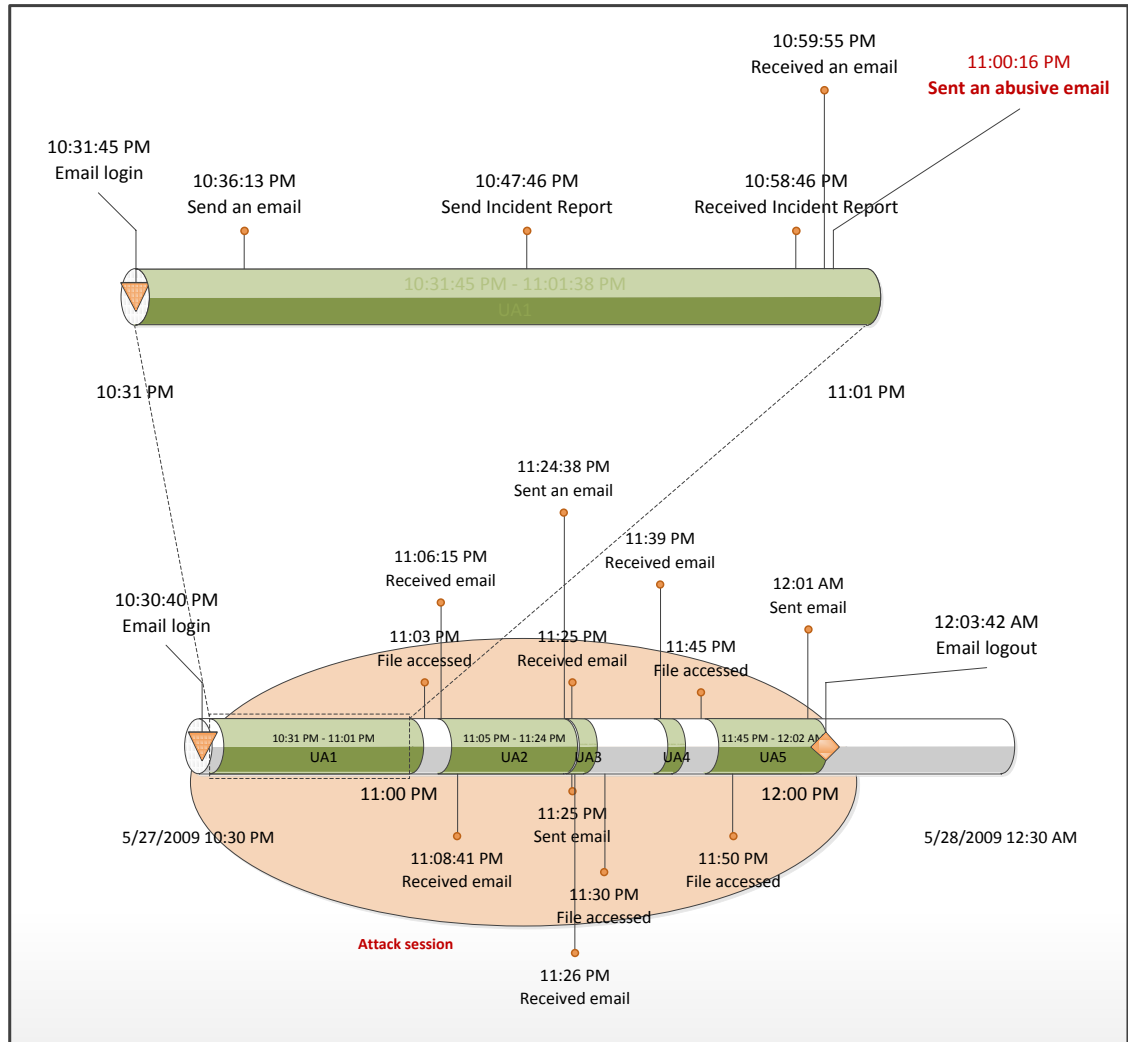


Figure 20: Timeline analysis for Experiment 1

The timeline analysis of logs and an insider’s computer showed that several activities were performed by the insider, as presented in the table 13 below:

Table 13: User activity for Experiment 1

Session Attack Activity	
User activity	Number of activity
Logins	1
Emails	13
Files/folders	4

The timeline analysis revealed the following facts:

- one login
- 12 emails had been sent and received
- one abusive email
- four files were being accessed

5.3.1.2 Relational analysis

Relational analysis is used to analyse an insider's activities to identify matches between these activities and the insider's job responsibilities. When relational analysis was used to analyse the above activities, it revealed the following facts:

- 10 emails were BE
- two emails were NBE
- an abusive email was sent among the business activities
- four BF were being accessed and updated

Figure 21 shows that most of the email activities matched the insider's job responsibilities. It also shows that the file activities matched the insider's job responsibilities.

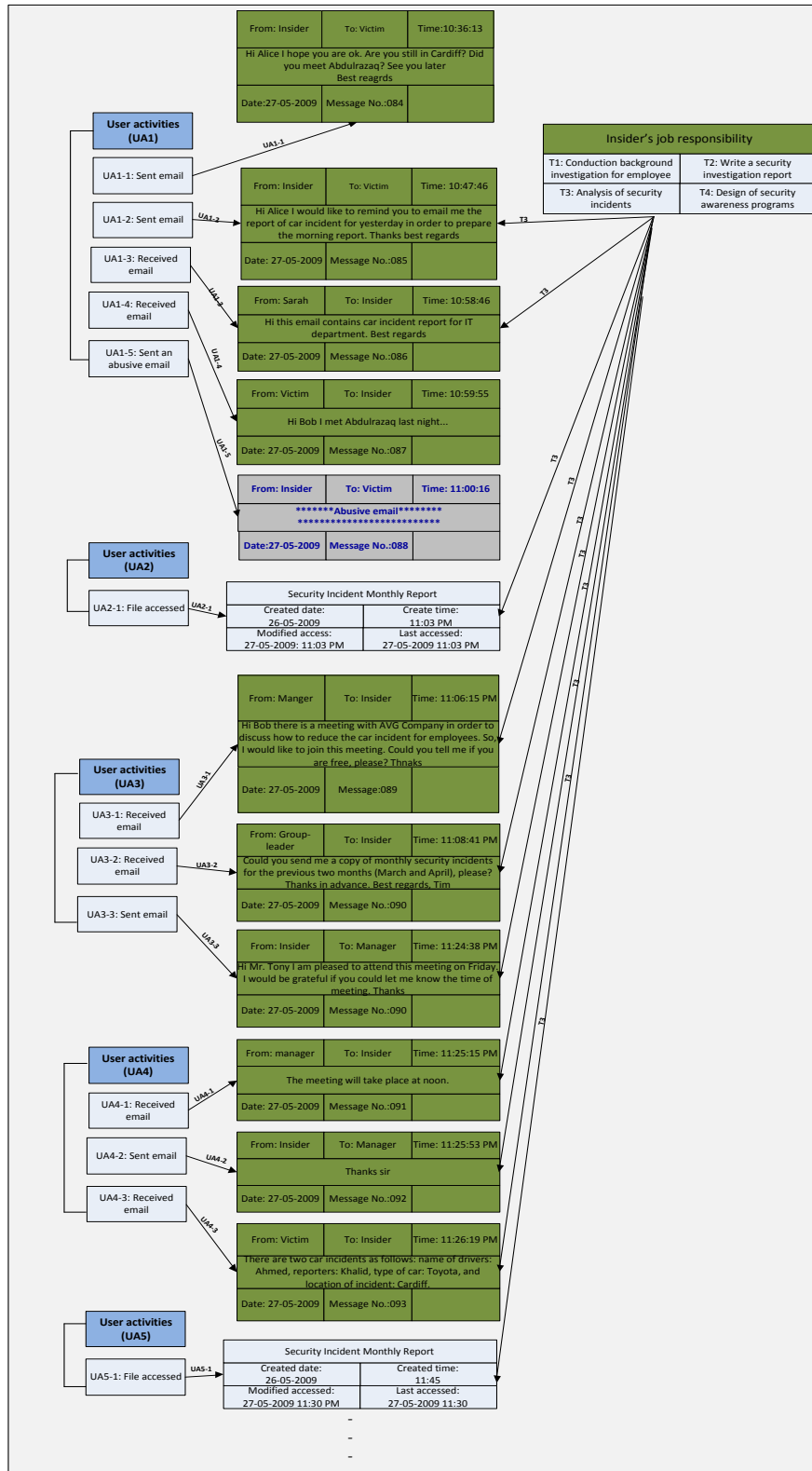


Figure 21: Relational analysis for Experiment 1

Figure 22 shows the communications that took place between the insider and other computer users in the organisation. It shows that these emails were business emails.

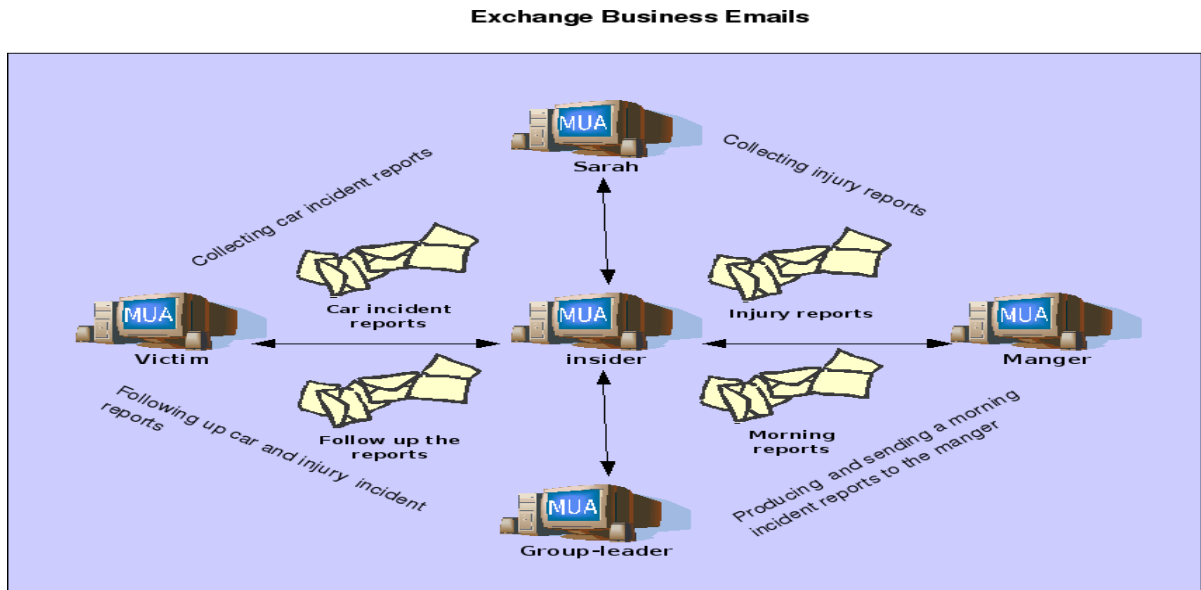


Figure 22: Insider's business emails

5.3.1.3 Decision

An activity is expressed as a number in order to distinguish between insider and outsider attacks.

Legitimate activities = -1

Abusive email = 0

Suspicious activities = 1

- An average of activities is used to identify the type of attack as follows:
- $A = \sum a_i / N$

Where n is the number of activities.

- If total $A < 0$, it is likely an insider attack
- If total $A > 0$, it is likely an outsider attack
- If $A=0$, it is likely unknown attack

$A = -13/18 = -0.72$

Table 14 shows the activities timeline and type of activities performed by the insider. These activities are expressed as a number in order to help identify any attack by type, and whether the attack was carried out by an insider or an outsider.

Table 14: Experiment 1 result

Timeline of activity	Type of activity
10:31:45	-1
10:36:13	1
10:47:46	-1
10:58:46	-1
10:59:07	1
11:00:55	0
11:03:00	-1
11:06:15	-1
11:08:41	-1
11:24:38	-1
11:25:15	-1
11:25:53	-1
11:26:19	-1
11:30:00	-1
11:39:03	-1
11:45:50	-1
11:50:45	-1
12:01:43	-1
Average	-0.72

Table 14 shows that the result is less than zero. Therefore, the attack was more likely an insider attack because $a < 0$.

Further details about this experiment are presented in Appendix B1. Ex1.

5.3.2 Experiment (Ex) 2

A victim reported that an abusive email was received from insider@test.com. The email was received on September 8, 2009 at 22:29:24. 136008000.

The preliminary investigation showed that this email was sent by the insider but the insider denied the allegation of sending an abusive email. Therefore, the first step was to collect evidence of legitimate and suspicious activity by the insider from the logs and from the insider's computer. These activities were then examined in order to provide the analysis process with information about the insider's activities.

5.3.2.1 Timeline Analysis

The timeline analysis presents all user activities before and during the period of the attack. Figure 23 shows that the period of the attack was from 09:57 p.m. to 11:05 p.m. It also shows that some activities, including the sending and receiving of emails, were performed before and during the period of the attack. Email login was then granted very shortly afterwards and the abusive email was sent.

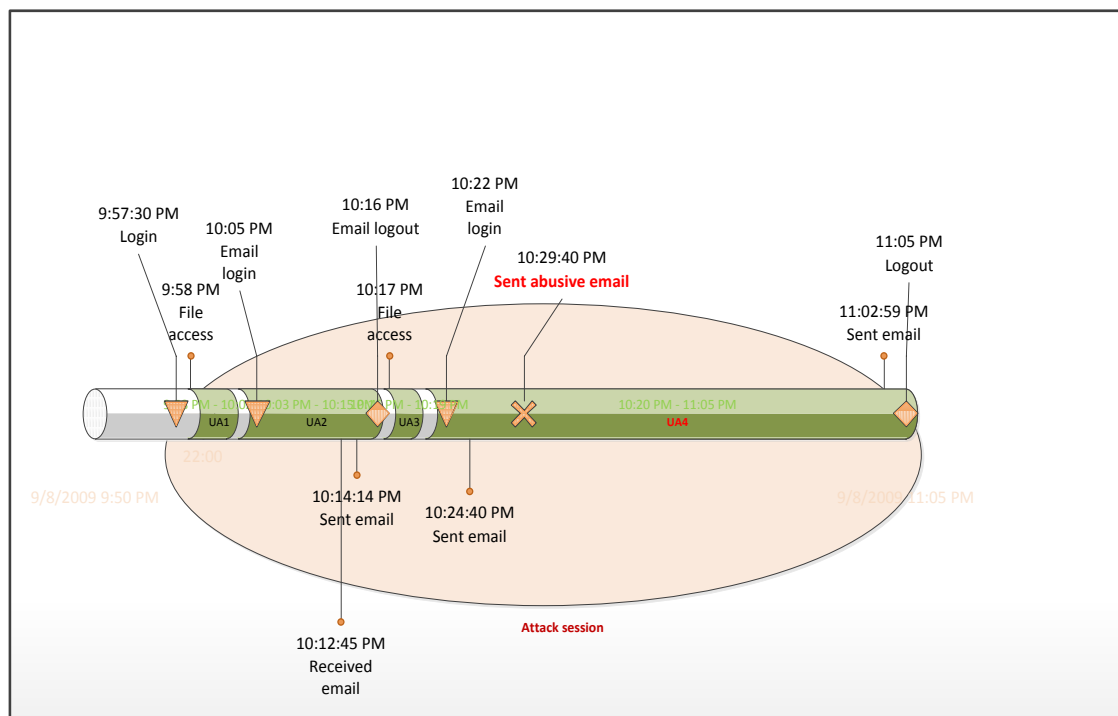


Figure 23: Timeline analysis for Experiment 2

The timeline analysis of the logs and the insider's computer showed that several activities were performed by the insider, as presented in Table 15 below:

Table 15: User activity for Experiment 2

User Activity	
User activity	Number of times activity was performed
Login	3
Email	5
File/Folder	2

The timeline analysis revealed the following facts:

- three logins
- five emails were sent and received
- two files were being accessed

5.3.2.2 Relational Analysis

The relational analysis presents the relationships between user activities and insider's job responsibilities. Figure 24 shows that the email activities matched the insider's job responsibilities. It also shows that the file activities matched the insider's job responsibilities.

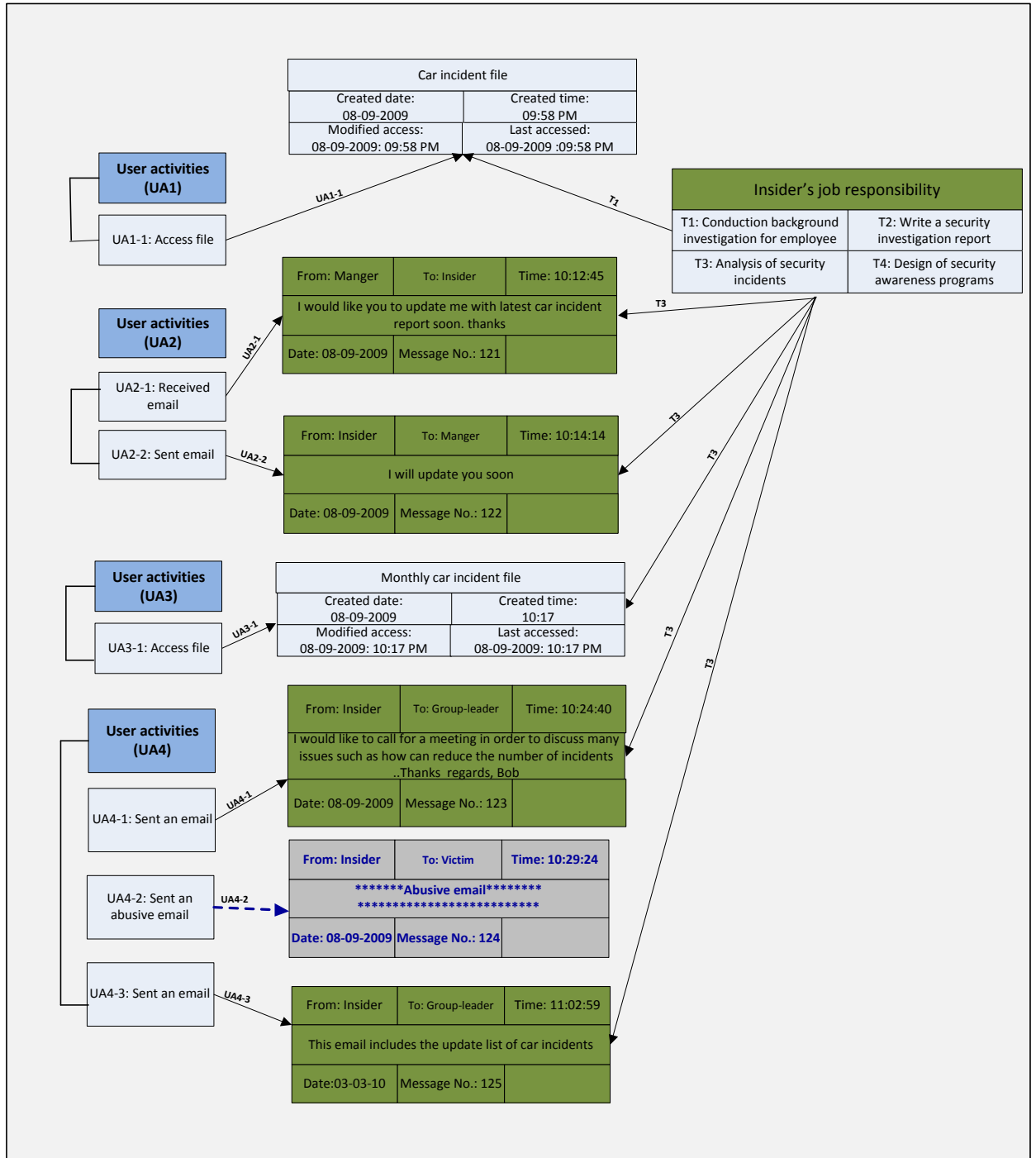


Figure 24: Relational analysis for Experiment 2

The analysis process found the following facts:

- These activities were legitimate:
 - there is a match between the email activities and the insider's job

responsibilities;

- there is a match between the file activities and the insider's job activities;
- the insider was successful in accessing the mail server. Therefore, the method of access was authorised accessed;
- An abusive email was sent to the victim, alongside the insider's legitimate job activities.

5.3.2.3 Decision

Table 16 shows the activities timeline and type of activities performed by the insider. These activities are expressed as a number in order to help identify the type of any attack, and whether the attack was carried out by an insider or an outsider.

$A = -9/10 = -0.9$ (it is more likely to be an insider attack).

Table 16: Experiment 2 results

Timeline activity	Type of activity
09:57:30	-1
09:58:00	-1
10:05:02	-1
10:12:45	-1
10:14:14	-1
10:17:00	-1
10:22:00	-1
10:24:40	-1
10:29:40	0
11:02:59	-1
Average	-0.9

For further details about the conduct of Experiment 2, see Appendix B1, Ex2.

5.3.3 Experiment (Ex) 3

The victim reported that an abusive email was received from insider@test.com. The email was received on December 3, 2009 at 20:42:43.527593000.

The preliminary investigation showed that this email was sent from the insider's computer but the insider denied the allegation of sending an abusive email because he was out of his office at the time. Therefore, the first step was to collect information about both legitimate and suspicious activity by the insider from the logs and the insider's computer. These activities were then examined in order to provide the analysis process with details of the insider's activities.

5.3.3.1 Timeline Analysis

The timeline analysis shows all user activities during the period of the attack. Figure 25 shows that the period of the attack was from 8:35 p.m. to 8:48 p.m. This analysis reveals that some suspicious activities, including one failed login, were performed during the period of the attack. There were several suspicious activities, including attempting of sending emails logins and an abusive email.

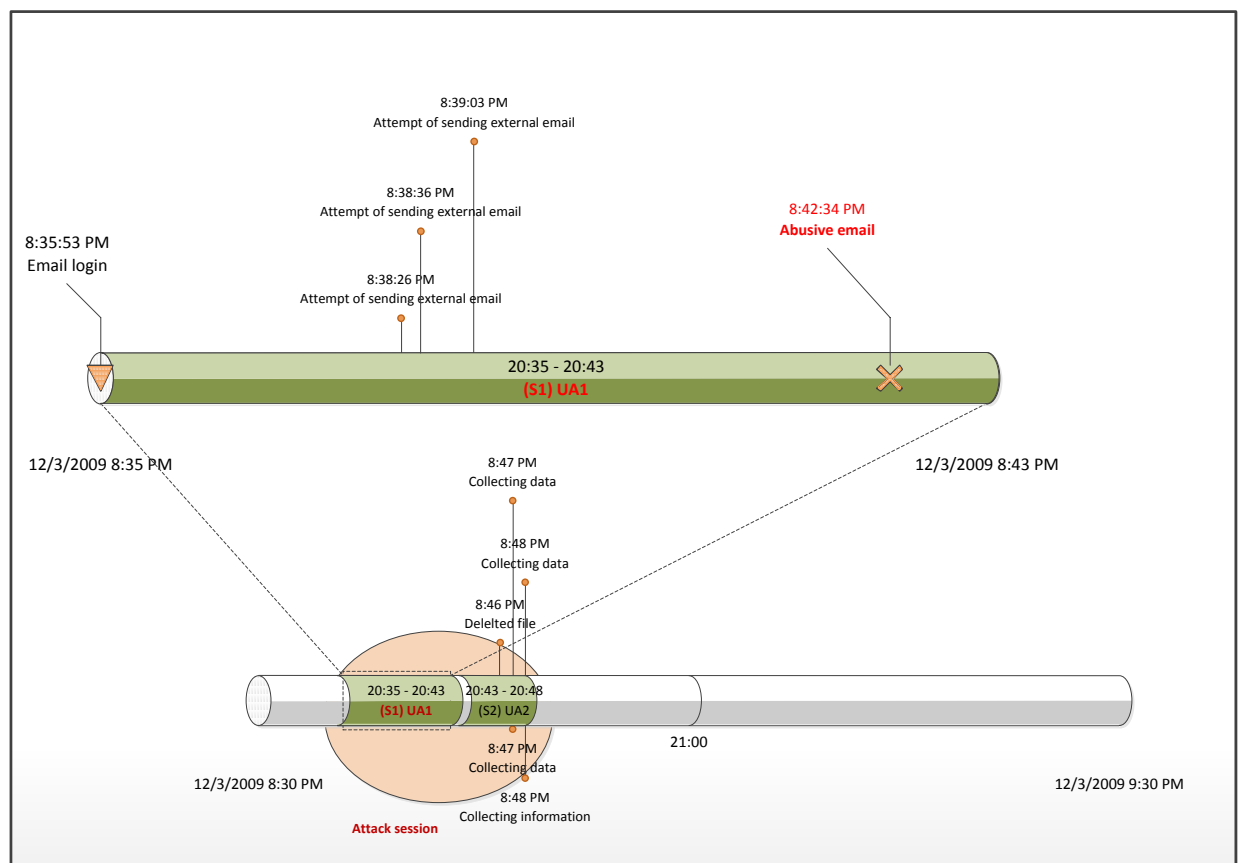


Figure 25: Timeline analysis for Experiment 3

The timeline analysis of logs and an insider's computer shows that several activities were performed by the insider, as presented in the table 17 below:

Table 17: User activity for Experiment 3

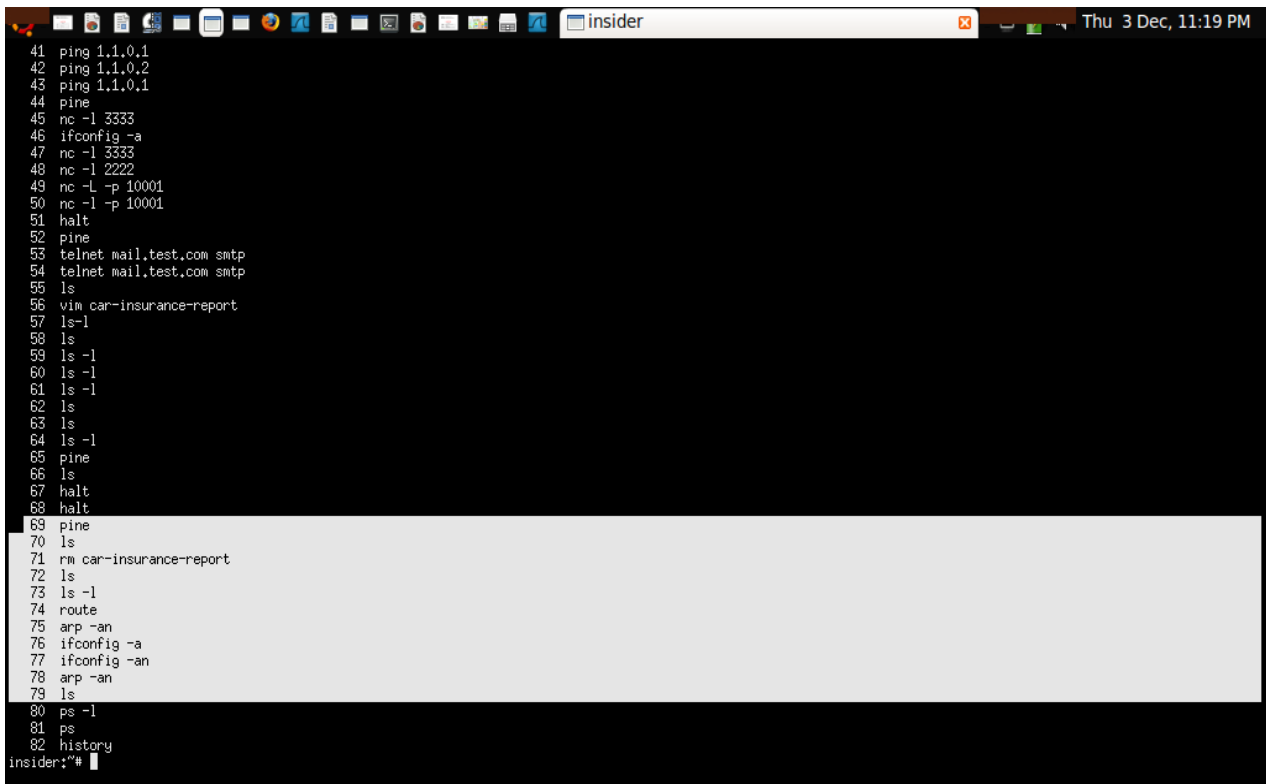
Attack Session Activity	
User activity	Number of activity
Logins	1
Emails	4
Files/folders	1
Others	4

This analysis revealed the following results:

- there were four times of failed attempts to send emails to external parties
- several command-lines were used to collect technical information about the organisation's network in order to:
 - identify the default gateway for the insider's computer and interface to the network
 - collect information about IP and MAC addresses for the gateway computer and any computer communicating with the insider's computer (route, ifconfig-a and ifconfig-an)
 - identify the IP and MAC addresses for the insider's computer (arp-an).

Figure shows these commands

- the abusive email occurred
- one file had been deleted

A screenshot of a terminal window titled 'insider' with a timestamp of 'Thu 3 Dec, 11:19 PM'. The terminal displays a series of commands and their outputs, numbered 41 through 82. The activities include ping tests, network configuration (ifconfig), netcat (nc) listener and client operations, telnet connections, file operations (ls, vim, rm), and system status checks (ps, history).

```
41 ping 1.1.0.1
42 ping 1.1.0.2
43 ping 1.1.0.1
44 pine
45 nc -l 3333
46 ifconfig -a
47 nc -l 3333
48 nc -l 2222
49 nc -L -p 10001
50 nc -l -p 10001
51 halt
52 pine
53 telnet mail.test.com smtp
54 telnet mail.test.com smtp
55 ls
56 vim car-insurance-report
57 ls-l
58 ls
59 ls -l
60 ls -l
61 ls -l
62 ls
63 ls
64 ls -l
65 pine
66 ls
67 halt
68 halt
69 pine
70 ls
71 rm car-insurance-report
72 ls
73 ls -l
74 route
75 arp -an
76 ifconfig -a
77 ifconfig -an
78 arp -an
79 ls
80 ps -l
81 ps
82 history
insider:~#
```

Figure 26: User activities for collecting information

5.3.3.2 Relational Analysis

The relational analysis shows that there was no relationship between user activity and the insider's job responsibilities during the period of the attack and before and after the attack, but one business file had been deleted after the attack. Figure 27 shows the relational analysis for these activities.

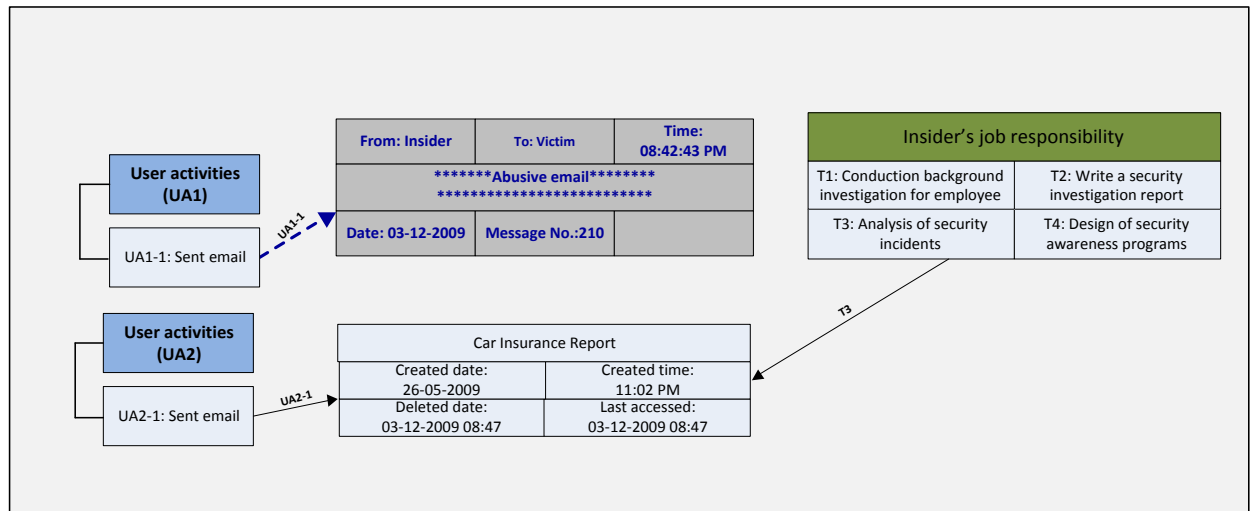


Figure 27: Relational analysis for Experiment 3

The relational analysis process found the following facts:

- the only email activity was the abusive email
- the deleted file was a business file
- no insider job responsibilities were carried out during the attack session:
 - Non business emails were sent or received
 - None Business files were created or modified

5.3.3.3 Decision

Table 18 shows the activities timeline and type of activities performed by the outsider. These activities are expressed as a number in order to help identify the type of attack, and whether the attack was carried out by insider or an outsider. It appears that:

- the attacker had no prior knowledge of the company's IT infrastructure and no prior knowledge of any insider's job responsibilities
- these activities were illegitimate:
 - suspicious activities were found relating to the collection of technical information about the network
 - these activities were performed out of working hours;
- an abusive email was sent to the victim when the outsider tried to email the recipients who were not known to the mail server

$A = 5/10 = 0.5$ (it is more likely to be an outsider attack)

Table 18: Experiment 3 results

Timeline of activity	Type of activity
08:35:53	-1
08:38:27	1
08:38:37	1
08:39:04	1
08:42:43	0
08:46:00	-1
08:47:00	1
08:47:30	1
08:48:00	1
08:48:30	1
Average	0.5

Further details about this experiment are presented in Appendix B1, Ex3.

5.3.4 Experiment (Ex) 4

The victim reported that an abusive email was received from Tim@hotmail.com. The email was received on Monday, 30 November 2009 at 03:22:2. Figure 28 shows that the content of the abusive email header included the date of the email, its source address, recipient address, subject of the email and the body of the message.


```
PINE 4.64  MESSAGE TEXT
Date: Mon, 28 Nov 2009 01:00:01 +0410 (CEST)
From: Tim <tim@hotmail.com>
To: victim@test.com
Subject: abuse email

*****abuse email*****
*****_abuse email*****
*****
*****
tim
```

Figure 28: Content of the abusive message

Preliminary investigation shows that Tim's account is a personal account and Tim is not working for Test Company. Therefore, the first step was to review fw-1 (firewall) log. When reviewing the log, it appeared that there was no connection between the mail server and another computer. This led us to examine the mail envelope header of the abusive message in order to identify the source IP address of the email envelope. The envelope header is usually hidden when an email is viewed, and the message header is usually visible. It contains information that is essential to email delivery. The envelope header of the abusive message showed that the source IP address was 146.227.128.4.

When reviewing the header, it revealed two suspicious issues as follows:

- 1- Date and time of email was unreliable because the envelope header showed that delivery date and time of email was Mon, 30 Nov 2009 03:22:27 whereas, the email header shows that the date and time of email was Mon, 28 Nov 2009 01:00:01.

2- The envelope header showed that source IP address was 146.227.128.4. This IP address belongs to the insider's computer. Therefore, this IP source belongs to Test Company.

Figure 29 shows that the content of the full header of the abusive email includes envelope header and message header. This information contains return-path, envelope-to, delivery-date, received from, date of email, the source address and the recipient address, subject of email and the body of this message.

```
Return-path: <tim@hotmail.com>
Envelope-to: victim@test.com
Delivery-date: Mon, 30 Nov 2009 03:22:27 +0000
Received: from [146.227.128.4] (port=44201 helo=Tim.test.com)
    by mail-server with esmtp (Exim 4.69)
    (envelope-from <tim@hotmail.com>)
    id 1NEwkM-000097-Gx
    for victim@test.com; Mon, 30 Nov 2009 03:22:27 +0000
Date: Mon, 28 Nov 2009 01:00:01 +0410 (CEST)
From: Tim <tim@hotmail.com>
X-X-Sender: root@insider
Reply-To: tim@hotmail.com
To: victim@test.com
Subject: abuse email
Message-ID: <Pine.LNX.4.64.0604032208335.264@insider>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed

*****abuse email*****
*****abuse email*****
*****
*****
tim
```

Figure 29: Full header of an abusive email

5.3.4.1 Timeline Activities

The timeline analysis shows all user activities before and during the period of attack. Figure 30 shows that the period of attack was from 01:52 a.m. to 03:20 a.m. It also shows because there are no emails received, and only one other sent, as it stands.

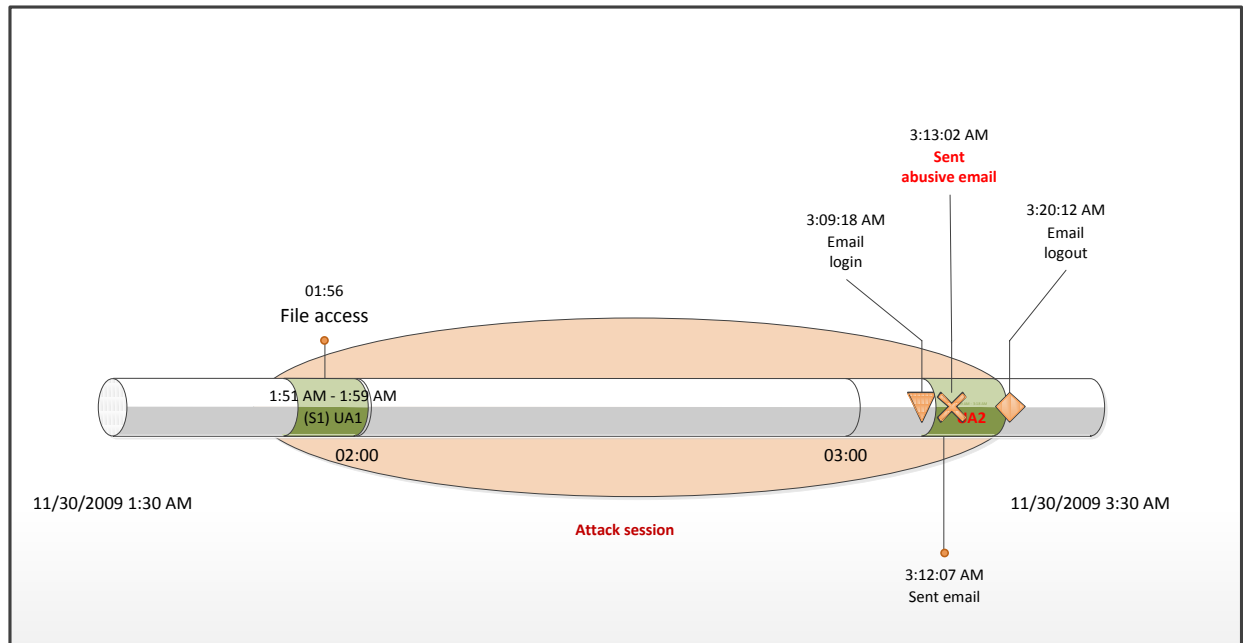


Figure 30: Timeline analysis for Experiment 4

The timeline analysis of logs and an insider's computer showed that several activities were performed by the insider, as presented in the Table 19 below:

Table 19: User activity for Experiment 4

Attack Session Activity	
User activity	Number of activity
Login	1
Email	2
Files/folders	1

This analysis revealed the following results:

- one login
- one email had been sent
- an abusive email was sent
- one file accessed

5.3.4.2 Relational Analysis

The relational analysis shows the relationships between the user activities that were

performed before and during the period of the attack and the insider's job responsibilities. Figure 31 shows that the email activities matched the insider's job responsibilities. It also shows that the file activities matched the insider's job responsibilities.

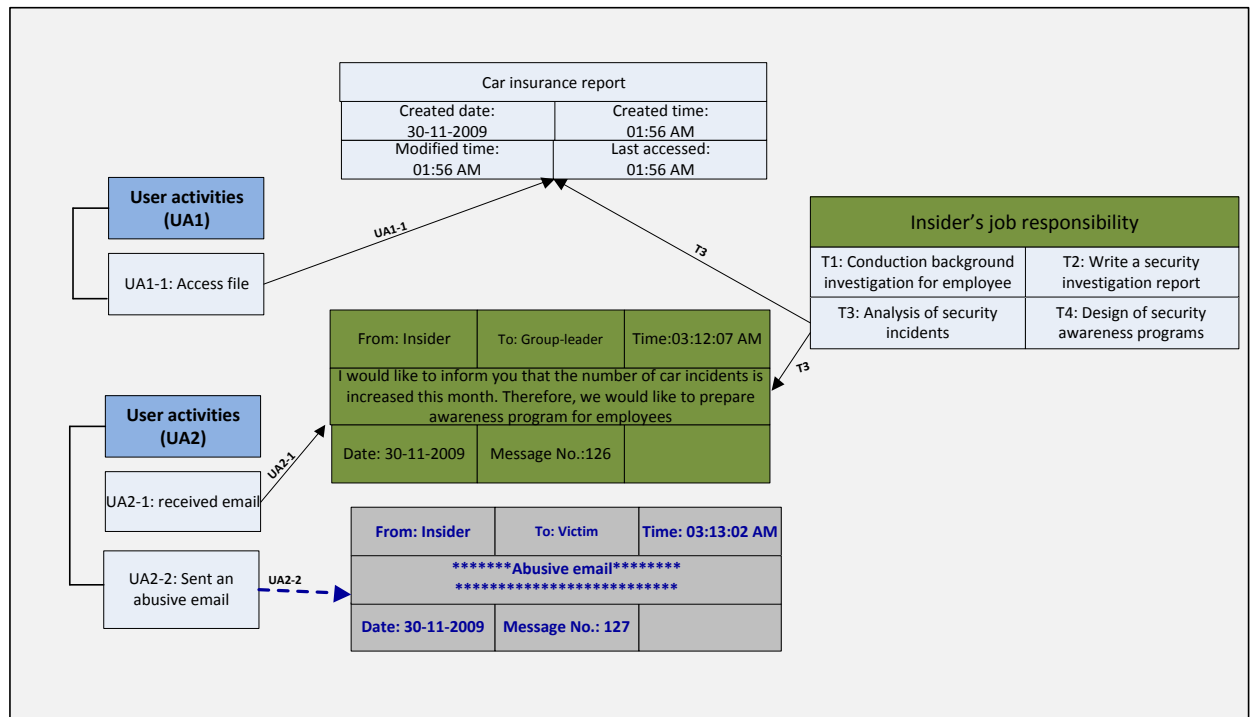


Figure 31: Relational analysis for Experiment 4

The analysis process found the following facts:

- these activities were legitimate:
 - there is a match between email activities and the insider's job responsibilities
 - there is a match between file activities and the insider's job activities;
 - the insider accessed the email server by using the SMTP protocol
- an abusive email was sent to the victim while the insider was performing his legitimate job activities;

5.3.4.3 Decision

Table 20 shows the activities timeline and type of activities performed by the insider. $A = -3/4 = -0.75$ (it is more likely to be an insider attack).

Table 20: Experiment 4 results

Timeline of activity	Type of activity
01:56:00	-1
03:09:18	-1
03:12:07	-1
03:13:02	0
Average	-0.75

Further details about this experiment are presented in Appendix B1, Ex4.

5.3.5 Experiment (Ex) 5

The victim reported that an abusive email was received from insider@test.com. The email was received on Monday, 30 November 2009 at 02:53:20. However, the insider denied the allegation of sending an abusive email, because he was out of his office when the email was sent. The insider claimed that his password had been stolen.

The preliminary investigation showed that the insider's account belonged to Test Company and, because the insider worked for Test Company, the first step was to review the fw-2 (internal firewall) log. When reviewing the log, it appeared that there was no connection between the mail server and the insider. This led us to examine the mail envelope header of the abusive message in order to identify the source IP address of the email envelope.

5.3.5.1 Timeline Analysis

The timeline analysis shows all user activities before and during the period of the attack. Figure 32 shows that the period of the attack was from 02:24 a.m. to 02:43 a.m. It also shows that two emails were sent.

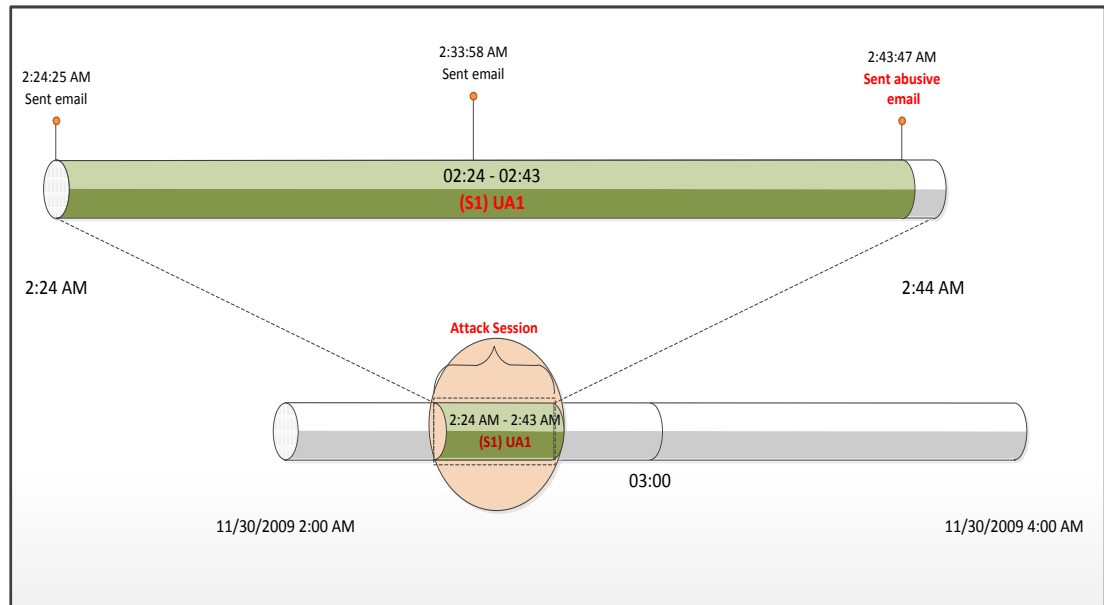


Figure 32: Timeline analysis for Experiment 5

The timeline analysis of logs and an insider's computer showed that several email activities were performed by the insider, as presented in the table 21 below:

Table 21: User Activity for Experiment 5

Attack Session Activity	
User activity	Number of times activity was performed
Login	0
Email	3
File/Folder	0

The timeline analysis revealed the following facts:

- no login
- two emails had been sent and received
- one abusive email

5.3.5.2 Relational Analysis

The relational analysis shows the relationships between the user activities that were performed during the period of the attack and the insider's job responsibilities. Figure 33 shows that the activities mentioned in the emails matched the insider's job

responsibilities.

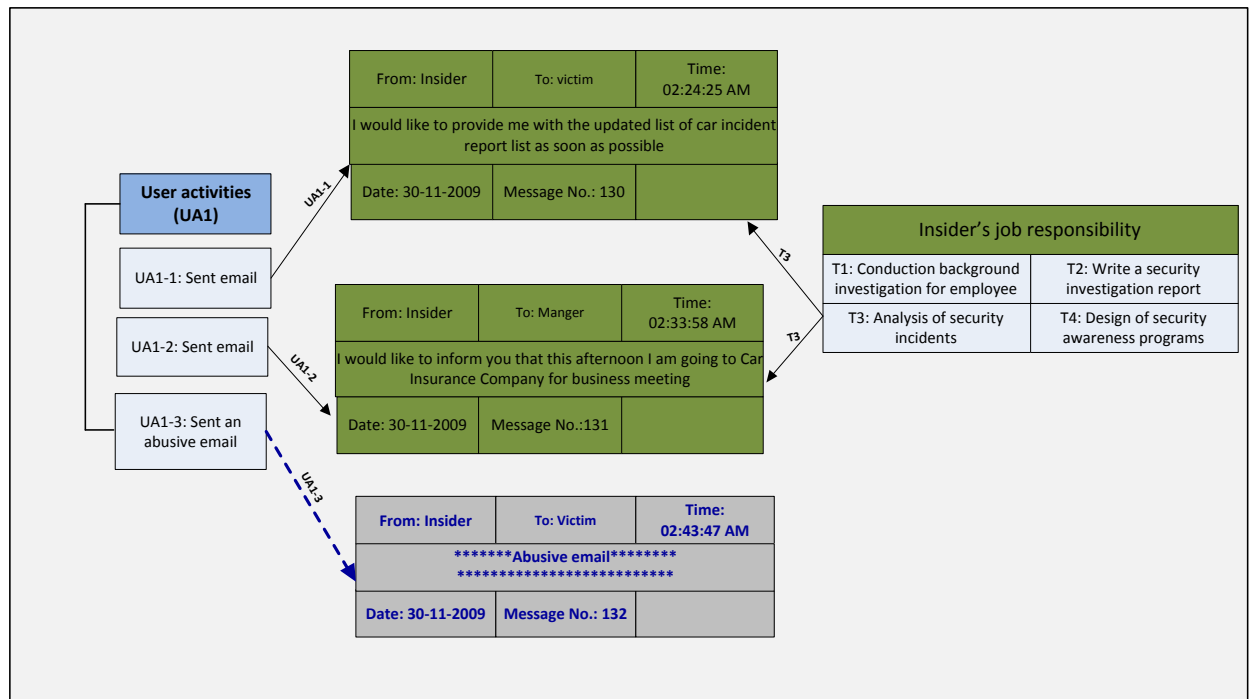


Figure 33: Relational analysis for Experiment 5

TCPdump logs revealed that the insider did not use his password to access to the organisation's network but he used SMTP commands to send emails, which were two business emails and an abusive email. Analysis of abusive header email revealed that this message came from insder@test.com but from an external machine, the source IP address was an external 1.1.0.1. Then the external firewall (fw-1) logs were being examined and showed that there were SMTP connections between the external machine and the email server.

The analysis process found the following facts:

- the insider used SMTP commands to send emails and the abusive email
- these email activities were legitimate:
 - there is a match between the email activities and the insider's job responsibilities

- an abusive email was sent to the victim when the insider was performing his job activities

5.3.5.3 Decision

Table 22 shows the activities timeline and type of activities undertaken by the insider.

$A = -2/3 = -0.66$, therefore, it is more likely to be an insider attack.

Table 22: Experiment 5 results

Timeline of activity	Type of activity
02:24:25	-1
02:33:58	-1
02:43:47	0
Average	-0.66

Further details about this experiment are presented in Appendix B1, Ex5.

5.3.6 Experiment (Ex) 6

A victim reported that an abusive email was received from this source: insider@test.com. The email was received on September 6, 2009 at 20:33:14.634794000.

A preliminary investigation showed that this email had been sent from the insider's account but the insider denied the allegation of sending an abusive email. Therefore, the first step was to collect information about legitimate and suspicious activity on the part of the insider from the logs and from the insider's computer. These activities were then examined in order to provide the analysis process with information about the insider's activities. The examination process provided the following information.

5.3.6.1 Timeline Analysis

The timeline analysis shows all user activities during the period of the attack.

Figure 34 revealed that the period of the attack was from 8:30 p.m. to 8:37 p.m. There were several suspicious activities, including two failed logins and an abusive email.

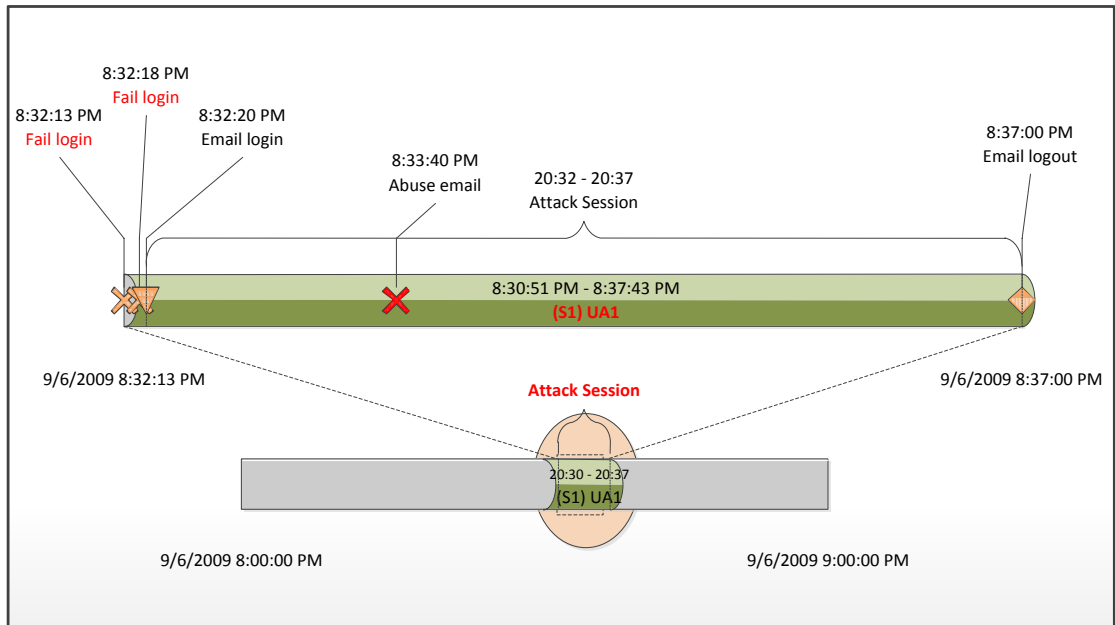


Figure 34: Timeline analysis for Experiment 6

The timeline analysis of the logs and the insider's computer showed that several activities were performed by the user, as presented in the table 23 below:

Table 23: User activity for Experiment6

Attack Session Activity	
User activity	Number of times activity was performed
Login	3
Email	1
File/Folder	0

This analysis provided the following information:

- the activities included two failures to gain authenticated access to the mail server
- the method of access was password guessing to gain insider's access
- the attacker used the insider's email account to send an abusive email to the victim

5.3.6.2 Relational Analysis

The relational analysis shows that there is no relationship between user activity and insider's job responsibilities during the period of the attack and before and after the attack. Figure 35 shows the relational analysis for these activities

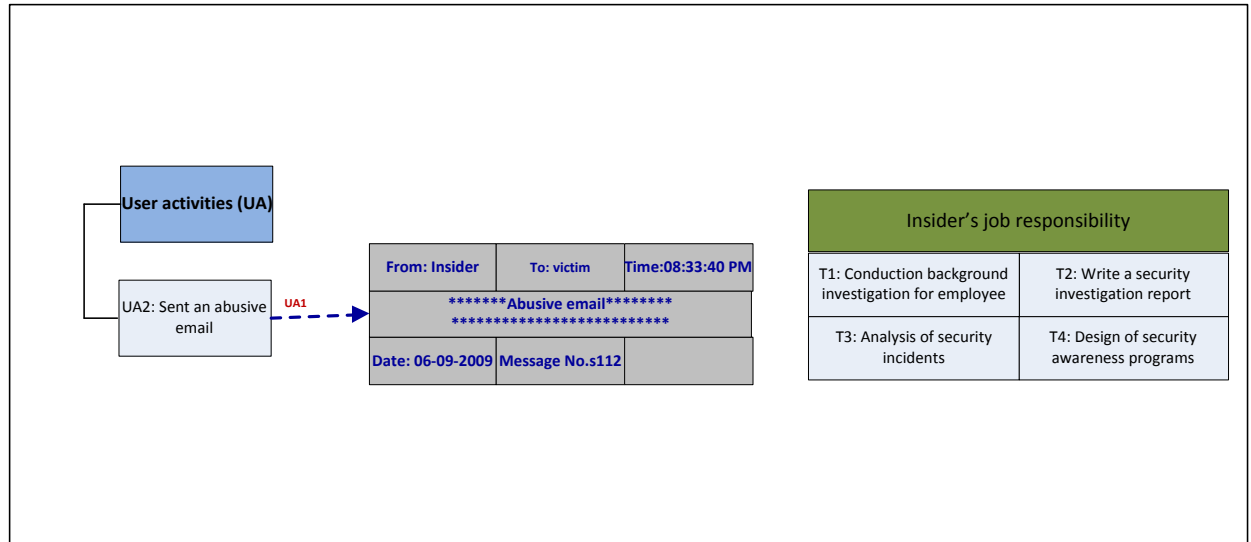


Figure 35: Relational analysis for Experiment 6

The relational analysis process found the following facts:

- the only email activity was the abusive email;
- no insider job responsibilities were carried out:
 - No business email was sent or received;
 - No business file was created or modified.

The relational analysis shows that there is no relationship between user activity and insider's job responsibilities during the period of the attack, and neither before nor after the attack.

5.3.6.3 Decision

Table 24 shows the timeline activities and type of these activities, which were performed by an outsider because the suspect had no prior knowledge of the insider's job responsibilities. These activities are represented by numbers in order to help identify

the type of attacks, as to whether the attack was carried out by an insider or an outsider.

$A = 1/4 = 0.25$ (it is more likely to be an outsider attack)

Table 24: Experiment 6 Result

Timeline of activity	Type of activity
08:32:13	1
08:32:18	1
08:32:20	-1
08:33:40	0
Average	0.25

Further details of this experiment are presented in Appendix B1, Ex6.

5.3.7 Experiment (Ex) 7

The victim reported that an abusive email was received from insider@test.com. The email was received on December 3, 2009 at 09:49:01.273294000.

The preliminary investigation showed that this email had been sent from the insider's account but the insider denied the allegation of sending the abusive email. Therefore, the first step was to collect information about legitimate and suspicious activities relating to the insider from the logs, and then to examine these activities in order to provide the analysis process with information about the insider's activities.

5.3.7.1 Timeline Analysis

The timeline analysis shows all user activities during the period of the attack. Figure 36 shows that the period of attack was from 09:47 p.m. to 09:51 p.m. This analysis reveals that some suspicious activities, including one failed login, were performed during the period of the attack. Email login was then granted very shortly afterwards and the abusive email was sent.

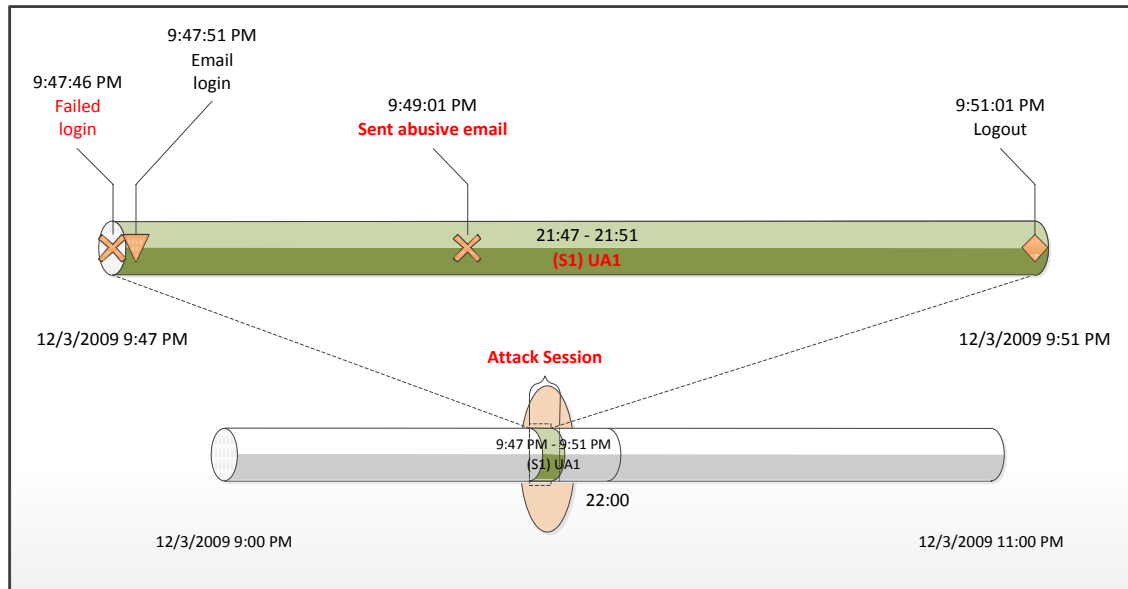


Figure 36: Timeline Analysis for Experiment 7

The timeline analysis of logs and an insider's computer showed that several email activities were performed by the insider, as presented in the table 25 below:

Table 25: User activity for Experiment 7

Attack Session Activity	
User of activity	Number of activity
Logins	2
Emails	1
Files/folders	0

This analysis provided the following information:

- one failed login
- one authorised login
- an abusive email was being sent

5.3.7.2 Relational Analysis

The relational analysis shows that no user activities were performed during the period of the attack, apart from the sending of the abusive email. Therefore, this attack should most probably be an outsider attack; however, this methodology finds it difficult to

identify for certain whether this attack has been committed by an insider or an outsider, because there is a lack of activities to examine. Figure 37 shows no matching between user activity and the insider's job responsibilities.

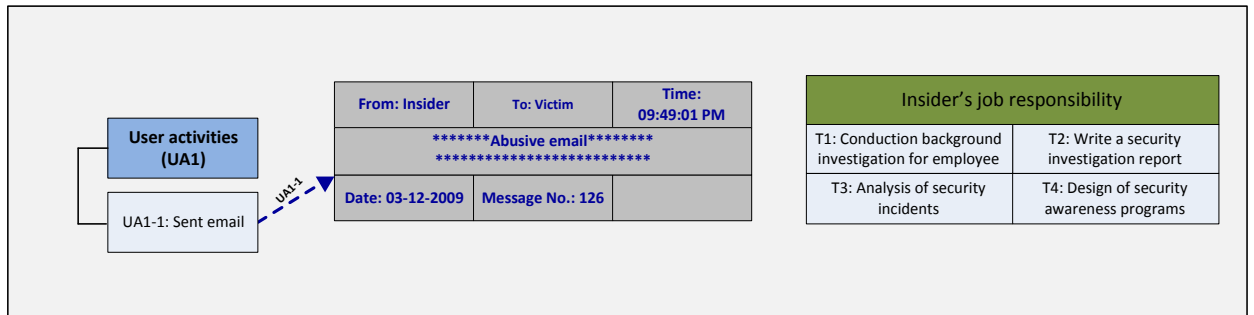


Figure 37: Relational analysis for Experiment 7

The analysis process found the following facts:

- one failed login
- the only email activity was the abusive email
- No business email was sent or received
- No business file was created or modified

5.3.7.3 Decision

Table 26 shows the activities timeline and the type of activities that were being performed. These activities are expressed as a number in order to help identify the type of attack, and whether the attack had been carried out by an insider or an outsider.

$A = 0/3 = 0$ (it is more likely to be an unknown attack)

Table 26: Experiment 7 results

Timeline activity	Type of activity
09:47:46	1
09:47:51	-1
02:43:47	0
Average	0

Further details about this experiment are presented in Appendix B1, Ex7.

5.3.8 Experiment (Ex) 8

The victim reported that an abusive email was received from this source: insider@test.com. The email was received on January 10, 2010 at 21:55:26.

The preliminary investigation showed that this email had been sent from the insider's account but the insider denied the allegation of sending an abusive email. Therefore, the first step was to collect information about both the legitimate and suspicious activities of the insider from the logs and the insider's computer. These activities were then examined in order to provide the analysis process with information about the insider's activities.

5.3.8.1 Timeline Analysis

The timeline analysis shows all user activities during the period of the attack. Figure 38 shows that the period of the attack was from 09:38 p.m. to 09:55 p.m. This analysis revealed that some suspicious activities, including three failed computer login attempts, were performed during the period of the attack. Email login was then granted and the abusive email was sent. Also, the computer password had been changed before the attack took place.

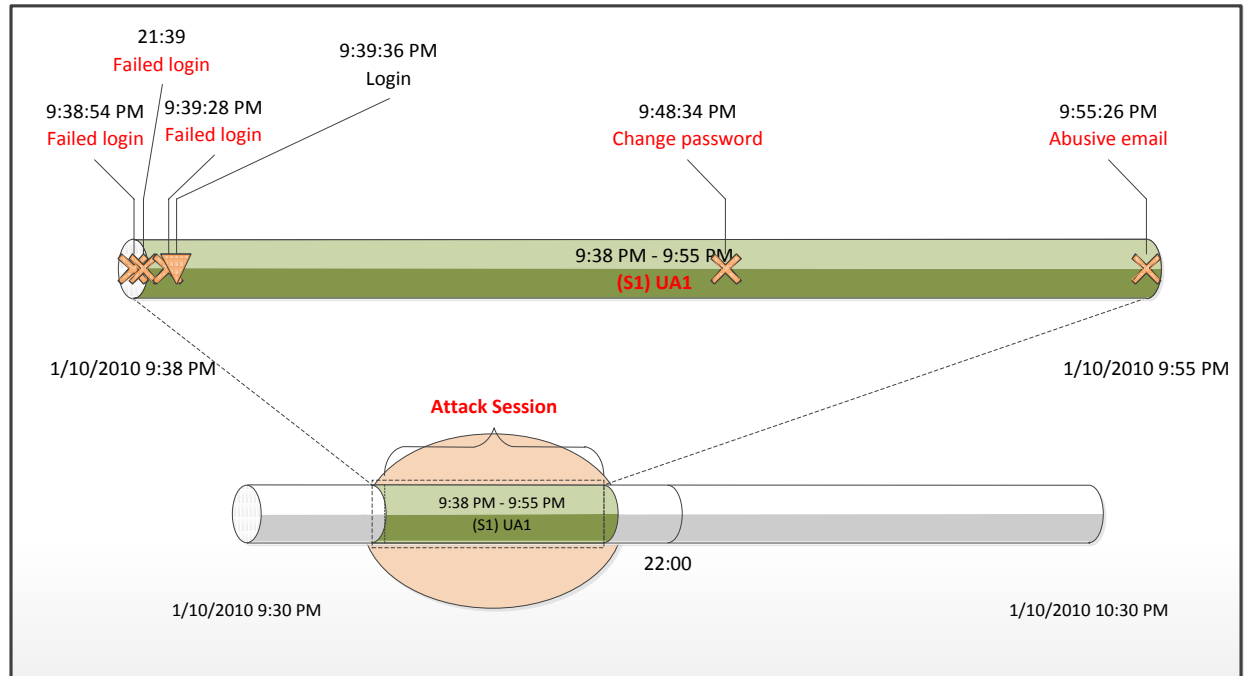


Figure 38: Timeline analysis for Experiment 8

The timeline analysis of logs and an insider's computer showed that several email activities were performed by the insider, as presented in the table 27 below:

Table 27: User activity for Experiment 8

Attack Session Activity	
User of activity	Number of activity
Logins	4
Emails	1
Files/folders	0
Others	1

This analysis provided the following information:

- the authenticated activities failed three times in accessing the insider's computer
- the method of access was by using password guessing to gain access
- the insider's access had been changed before the abusive email was sent
- the attacker used the insider's email account to send an abusive email to the

victim

5.3.8.2 Relational Analysis

The relational analysis shows that no user activities were performed during the attack session, apart from the sending of an abusive email. Figure 39 shows that there was no match between user activity and insider's job responsibilities.

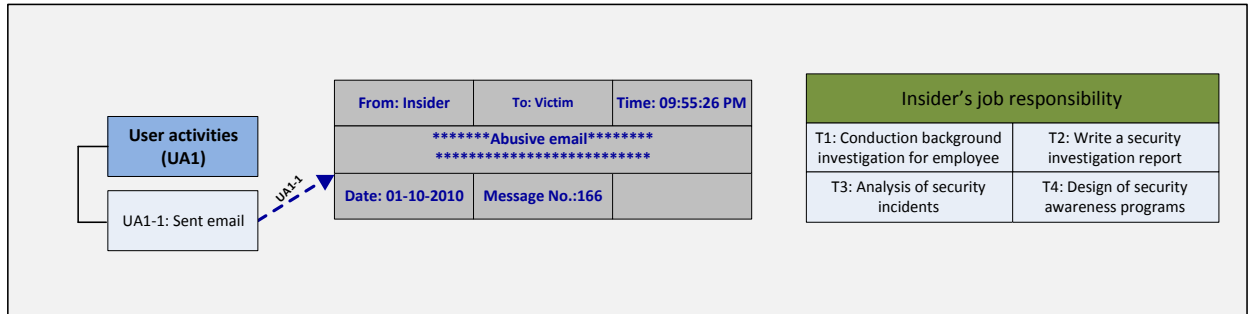


Figure 39: Relational analysis for Experiment8

The relational analysis process found the following facts:

- the abusive email was the only email activity performed during the attack session
- no insider job responsibilities were carried out before or during the attack session:
 - No business email was sent or received
 - No business file was created or modified

5.3.8.3 Decision

Table 28 shows the activities timeline and type of activities performed by the insider. These activities are expressed as a number in order to help identify the type of attack and whether the attack had been carried out by an insider or an outsider.

$A=3/6= 0.5$ (it is more likely to be an outsider attack)

Table 28: Experiment 8 results

Timeline activity	Type of activity
09:38:54	1
09:39:04	1
09:39:28	1
09:39:36	-1
09:48:34	1
9:55:26	0
Average	0.5

Further details about this experiment are presented in Appendix B1, Ex8.

5.4 Discussion

This section discusses the results of these experiments. DAMDIOA revealed that Exs.1, 2, 4 and 5 had been committed by the insider. It uses legitimate activities as a method of distinguishing between insider and outsider attacks. The researcher believes that legitimate activities should not only depend on access but also on execution of the user's job responsibilities. This proposed method allows corporate security investigators to compare activities carried out during the attack session with these responsibilities. In the present case, relational analysis was used to identify these relationships. DAMDIOA found that Exs.3, 6 and 8 were committed by the outsider because no job responsibilities had been carried out.

In Experiment 7, DAMDIOA failed to differentiate between an insider and an outsider attack; the attack was therefore classed as unknown. The reason for this is that the number of suspicious activities equalled the number of legitimate ones. It also found that there was not enough information to analyse. The conclusion is that this is apparently one of the main problems with this model. The researcher believes, however, that the problem is not with the model itself but with IT security policies. Chapter 7 will propose a corporate security model with recommendations in order to address this issue

Table 29: Results of Experiments

Experiments	Type of attack	DAMDIOA
Ex1	Insider	Insider
Ex2	Insider	Insider
Ex3	Outsider	Outsider
Ex4	Insider	Insider
Ex5	Insider	Insider
Ex6	Outsider	Outsider
Ex7	Outsider	Unknown
Ex8	Outsider	Outsider

5.5 Tailored decisions

This section discusses how the threshold can differentiate between insider and outsider attacks and what similarities and differences there are between tailored and predetermined decision. It reports the results of these attack experiments based on the proportion of suspicious activities (r). The threshold of suspicious activities has been adjusted to meet the requirement of different levels (from 0.1 to 1).

Tailored decisions are able to distinguish between insider and outsider attacks with different false positive rates because those decisions are based on an adjustable threshold. The researcher tested all level of thresholds from 0.1 to 1, and found that:

- Th = 0.7, 0.8, 0.9 and 1 failed four times to make such distinctions
- Th = 0.2 and 0.3 made correct distinctions

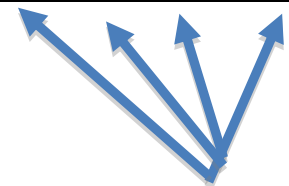
The table 30 shows the proportion of suspicious activity for each experiment, together with the different levels of threshold, illustrating how the types of incident depend on this level of threshold.

Table 30: Results of experiments based on portion of suspicious activities

		Likely types of incidents	Customisable decision									
			Threshold=Th									
			Th=0.1	Th=0.2	Th=0.3	Th=0.4	Th=0.5	Th=0.6	Th=0.7	Th=0.8	Th=0.9	Th=1
Exp no.	Likely types	R	If $R < Th$ it is more likely Insider ; if $R > Th$, it is more likely Outsider; if $R = Th$, it is more likely unknown attack									
Ex1	Insider	0.11	Outsider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider
Ex2	Insider	0	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider
Ex3	Outsider	0.7	Outsider	Outsider	Outsider	Outsider	Outsider	Outsider	Unknown	Insider	Insider	Insider
Ex4	Insider	0	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider
Ex5	Insider	0	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider	Insider
Ex6	Outsider	0.50	Outsider	Outsider	Outsider	Outsider	Unknown	Insider	Insider	Insider	Insider	Insider
Ex7	Outsider	0.33	Outsider	Outsider	Outsider	Insider	Insider	Insider	Insider	Insider	Insider	Insider
Ex8	Outsider	0.66	Outsider	Outsider	Outsider	Outsider	Outsider	Outsider	Insider	Insider	Insider	Insider



Correct decision



The highest level of wrong decision

5.5.1 Similarities and comparisons between fixed and the tailored decisions

This section discusses the similarities and differences between the identification of the type of attack based on fixed and tailored decisions. The researcher selected the adjustable threshold $Th=0.2$ and 0.3 because their results were similar to fixed decision ones.

The outcomes were:

- Both fixed and tailored decisions ($Th = 0.2$ and 0.3) returned the same results
- Tailored decisions are able to differentiate between these attacks, whereas fixed ones failed to identify the type of attack in Ex.7
- Fixed decisions were unable to identify the type of attack in Ex.7 because the number of user suspicious activities is equal to the number of legitimate ones (0)
- Tailored decisions ($Th=0.2$ and 0.3) are able to address the fixed decision issue by identifying the types of unclassified attack

Table 31 illustrates these decisions and their distinction between these attacks.

Table 31: Comparison between fixed and tailored decision

		Fixed	Tailored	
			Th=0.2	Th=0.3
Ex1	Insider	Insider	Insider	Insider
Ex2	Insider	Insider	Insider	Insider
Ex3	Outsider	Outsider	Outsider	Outsider
Ex4	Insider	Insider	Insider	Insider
Ex5	Insider	Insider	Insider	Insider
Ex6	Outsider	Outsider	Outsider	Outsider
Ex7	Outsider	Unknown	Outsider	Outsider
Ex8	Outsider	Outsider	Outsider	Outsider

5.6 Summary

This chapter aimed to test the hypothesis by running a number of insider and outsider attacks using DAMDIOA to distinguish between them. The experiments consisted of the following components:

- Netkit to build a virtual client/server network
- TCPdump to intercept TCP packets and record activities
- Wireshark to analyse activities

Password attacks and forged emails using SMTP were used as methods of attack. Both legitimate and suspicious activities were collected using TCPdump and command lines such as ls-l and ls-a. The resulting data were analysed and examined using timeline analysis to identify the attack session and relational analysis to identify the relationship between the activities performed in the attack session and the user's job responsibilities.

The researcher found that, when DAMDIOA used predetermined decisions based on legitimate activities, it was able to differentiate the type of attack in seven of the eight experiments conducted. It was the tailored decisions with threshold levels $Th=0.2$ and 0.3 that conferred the ability to make such distinctions.

6 Test and Evaluation

Objectives:

-
- to discuss the results of the experiments
 - to evaluate DAMDIOA
 - to present case studies that have used DAMDIOA in real computer incidents
 - to discuss limitations of DAMDIOA
-

This chapter analyses the experimental results and discusses similarities and contrasts between the current methods of distinguishing between insider and outsider attacks (methods based on the three elements of authorised access, locations of attack initiation and attack within an organisation's control) and the proposed method of making such distinctions, based on the conduct of legitimate activities. It discusses similarities and contrasts between DAMDIOA and other models. DAMDIOA was used once each by two companies and proved able to distinguish between the two types of attack. The limitations of DAMDIOA will also be discussed.

6.1 Discussion

This section discusses the similarities and differences between methods by which insider and outsider attacks are distinguished. It also compares DAMDIOA with the other models.

6.1.1 Comparisons between current methods of distinguishing insider from outsider attacks

The current methods of differentiation as outlined above will be compared with the proposed one with regard to their respective efficiency. Table 32 illustrated these methods and their distinction between these attacks.

Table 32: Results of experiments to determine the best factor for distinguishing the type of attack

Experiment	Type of attack	Methods of distinction between insider and outsider attacks				
		Proposed method		Current methods		
		Legitimate activities with tailored decision (Th=0.2 and 0.3)	Legitimate activities with fixed decision	Authorised access	Location of initiation of attacks	Attacks from within an organisation's control
Ex.1	Insider	Insider	Insider	Insider	Insider	Insider
Ex.2	Insider	Insider	Insider	Insider	Insider	Insider
Ex.3	Outsider	Outsider	Outsider	Insider	Insider	Insider
Ex.4	Insider	Insider	Insider	Insider	Insider	Insider
Ex.5	Insider	Insider	Insider	Unknown	Outsider	Outsider
Ex.6	Outsider	Outsider	Outsider	Outsider	Insider	Insider
Ex.7	Outsider	Outsider	Unknown	Insider	Insider	Insider
Ex.8	Outsider	Outsider	Outsider	Outsider	Insider	Insider
Number of attacks correctly identified		8	7	5	3	3

6.1.1.1 Legitimate activities and location from which attacks are initiated

The method of distinguishing between insider and outsider attacks is based on the locations from which these attacks are initiated. If they are carried out from inside an organisation they are called “insiders”; otherwise they are known as “outsiders”. These experiments reveal that the locations from which attacks are launched (discussed in Chapter 2) can be misleading when attempting to make such a distinction. Experiments 3, 6, 7 and 8 illustrate how an outsider can carry out an attack from inside an organisation using an insider's access and computer. Experiment 5 also demonstrates how an insider can carry out an attack from outside an organisation. The vulnerability of SMTP, namely its lack of authentication, was exploited to carry out this attack and

send an abusive email. However, in Experiments 1, 2 and 4 this method proved able to differentiate between these attacks.

Of eight experiments attempting to determine the type of attack by ascertaining the location from which it was launched, only three successfully did so. The results of experiments 1, 2 and 4 show that both legitimate activities and locations of initiation were able to identify the types of attack.

The researcher therefore disagrees with the position of Melara and Sarriegui [50] and Graves [34], who believe that the differences between insider and outsider attacks are based on whether they are initiated from inside or outside the organisation.

6.1.1.2 Legitimate activities and authorised access

The main difference between insiders and outsiders is that the former have authorised access. The experiments conducted for this research have found that authorised access is not always a trustworthy aspect by which such distinctions can be made. Experiments 3 and 7 demonstrate that outsiders were successfully authenticated on the system using the insider's password, which classifies them as insiders. Experiment 5 shows that authorised access cannot identify the type of attacks because no password was used to login into the system, that field not being a required one, or the password was so easily guessed as to be a mere formality. Vulnerability due to the lack of SMTP authentication was exploited to carry out this attack and send business emails. However, analysis based on legitimate activities was able to distinguish between these attacks.

Experiments 1, 2, 4, 6 and 8 found that both legitimate activities and authorised access were able to make such distinctions. Of the eight experiments using authorised access, three failed to discover whether the attack was launched by an insider or an outsider. The researcher's position is opposed to that of Rowlingson [74], Schultz [78] and Randazzo *et al.* [68], who hold authorised access to be one of the main aspects involved in such a distinction. The inadequacy of this approach is demonstrated by its classification of outsiders as insiders when they gain authorised access. Such access alone, while being useful, is not enough to distinguish between insider and outsider attacks. The crucial factor in this regard is establishing the relationship between

authorised access and the legitimate activity involved in the discharge of an organisational user's job responsibilities. Consideration of access is particularly useful in cases where different passwords are allocated for different functions, as when a user has one password for accessing a database server and a different one for accessing their computer.

6.1.1.3 Legitimate activities and attacks within an organisation's control

These experiments prove that attacks from areas within an organisation's control (discussed in Chapter 2) do not always discriminate correctly between insider and outsider attacks. Outsider attack Experiments 3, 6, 7 and 8 illustrate how an outsider can carry out an attack from such areas, while Experiment 5 demonstrates the contrary: insiders can also carry out attacks from areas outside an organisation's control. Legitimate activities, however, are able correctly to make such distinctions, as Experiments 3, 5, 6 and 8 demonstrate.

Of the eight experiments based on attack from within an organisation's control, five incorrectly identified the types of attack. For this reason the present researcher disagrees with Walton's [101] belief that the differences between insider and outsider attacks are based on attacks from within the organisation's control.

The three aspects used by current methods prove unable to distinguish between insider and outsider attacks, resulting in an increased risk that corporate security investigators will misidentify suspects and that organisations will consequently be financially penalised.

The present research did find, however, that legitimate activity in the form of insider job responsibilities can provide the basis for correctly distinguishing between such attacks. Of eight experiments using legitimate activities, seven correctly identified the source of the attack. The single failure was due to the dearth of activities to analyse, and the fact that the number of legitimate activities equalled the number of suspicious ones. DAMDIOA's ability to distinguish between these attacks could diminish the risk of misidentification of suspects. Figure 40 shows correct and false decisions for each method.

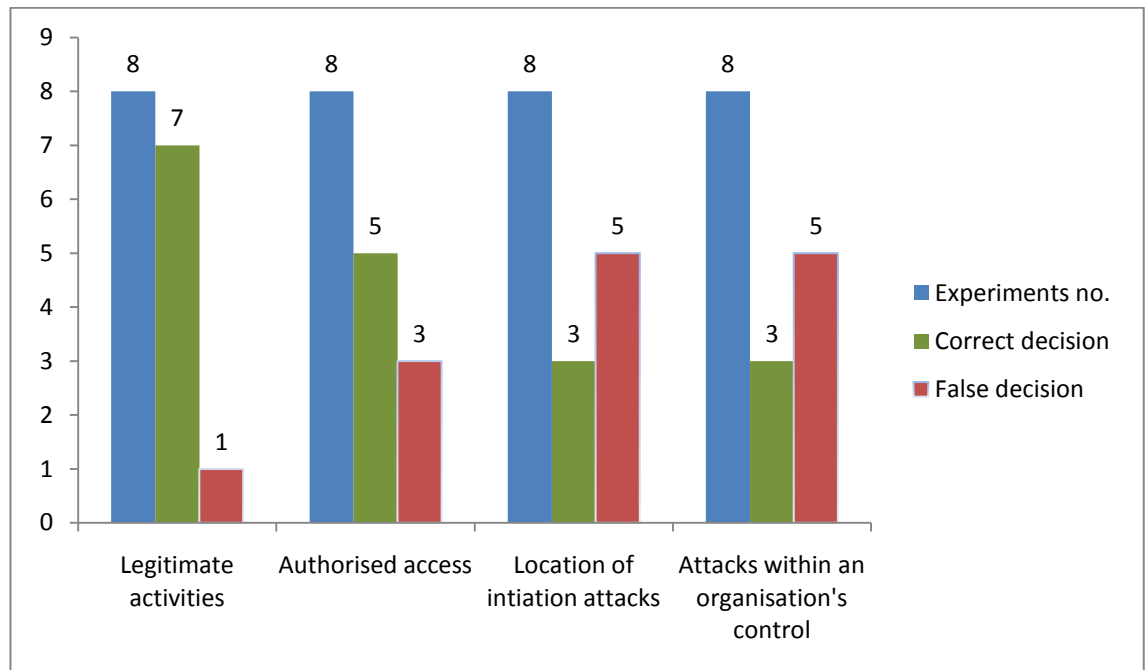


Figure 40: Number of false and correct decision

6.1.2 Comparison between the proposed model and existing models

6.1.2.1 Collection data

Most of the existing computer forensic models such as Haggerty and Taylor's framework [37], DFRWS methods [63] and the model developed by Nelson *et al.* [60], do not determine what user activities are logged, and thereby fail to collect enough information with which to analyse the insider's activities. They focus only on recording suspicious user activities, which by itself is not enough to improve the process of distinguishing between insider and outsider attacks. This leads to an increased chance of mistakes being made in identifying suspects correctly, which could in turn result in mishandled evidence and organisations being put at financial risk. Some network forensic research, such as that of Rowlingson [73], indeed focuses on forensic readiness that maximises an organisation's ability to collect digital evidence, but this ability is not directed towards the necessary distinction revealed by the present research.

DAMDIOA, on the other hand, identifies which user activities are logged, as well as determining which activities are necessary to carry out an investigation. DAMDIOA provides the corporate investigator with a procedure by which to collect enough information to proceed with the inquiry.

6.1.2.2 Analysis data

Most existing computer forensic models such as Haggerty and Taylor's framework [37], DFRWS methods [63] and the model developed by Nelson *et al.* [60] do not offer a methodology or techniques for analysing collection data, nor do they usually focus on analysing suspicious rather than legitimate user activities, although some research into computer security does study the detection and analysis of both, analyses that cover insider PC and network logs.

On the other hand, DAMDIOA offers a means of focusing on analysing both legitimate and suspicious user activities by using a combination of two analysis methods, timeline and relational analysis. Timeline analysis enables the investigation to narrow its focus to a specific day, while relation analysis facilitates the discovery of any link between these activities and an insider's job responsibilities. This model also provides corporate

security investigations with an analysis procedure, as well as using the Wireshark tool as a network traffic analysis [105]. This research has found Wireshark to be a useful analysis tool that can help corporate computer investigators find specific pieces of information in the mass of evidence that has been collected, and then to use this as evidence to distinguish between insider and outsider attacks.

6.1.2.3 Decision

Most existing computer forensic models, such as Haggerty and Taylor's framework [37], IACIS [92], DFRWS methods [63] and the model developed by Nelson et al. [60] are not able to distinguish between insider and outsider attacks. They conduct digital investigations based on *ad hoc* rather than structured methods.

DAMDIOA, however, is designed as a structured model that is able to make such a distinction, which it does by the two proposed methods of fixed and customisable decisions. The former is based on a predetermined logical condition, whereas the other derives from thresholds of suspicious activities. This is useful, for example, when an organisation has employees perform specialised job responsibilities such as medication, mathematics and engineering. In such cases, if the proportion of suspicious activity is more than 80 per cent, the perpetrator is more likely to be an insider, because an outsider could not perform the insider's job responsibilities.

6.2 Case studies

This section discusses that DAMDIOA was used in two different cases and it made differentiate between insider and outsider attacks.

6.2.1 Case study 1

6.2.1.1 Background

This educational organisation located in Saudi Arabia has 1,000 employees and uses a client/server network environment. The two types of operating system for clients are MAC and Windows XP, while the server operating systems are Windows Exchange and Linux. This organisation relies on computer systems to perform, process, transmit, store and retrieve data.

IT security is responsible for securing the organisation's network and seizing organisational devices that are being misused. The organisation's Corporate Security Service is responsible for conducting computer forensic investigations.

6.2.1.2 Misuse of an organisation's computer

A report reached the Corporate Security Service that an organisation's PC on the second floor, Security Reception Desk at Building 1, was being misused. It was found that this PC, on at least one occasion, was consuming about 17 per cent of the organisational network's bandwidth. This PC was among the top ten system abusers in the whole organisation. This type of bandwidth use usually indicates the downloading of movies or software from the Internet.

As a result of their investigation, this PC was seized by IT Security which, together with the Corporate Security Service, conducted a technical analysis of the system and found that this PC was in fact used to download movies and games from the Internet as well as accessing inappropriate websites. According to IT Security, the consequences of consuming that much bandwidth impacts on overall network performance. Accessing inappropriate web sites is (depending on the site) also against Saudi law. Another potential problem is that the PC could be infected with viruses as a result of visiting

these inappropriate sites, and therefore the organisation's network could be impacted as well.

6.2.1.3 Initial findings

As part of the investigation, IT security sent the suspect PC to Corporate Security Service for further analysis. That analysis included reviews of system applications and activities such as files, folders and web histories. It found that a number of movies and games were downloaded and pornography was accessed by using a piece of proxy software called Hotspot Shield. This software allows a user to bypass King Abdulaziz City Web filtering, which is controlled by the Saudi Government's Internet Services Unit. This analysis also determined that the majority of this activity took place between 2300 and 0600.

After analysing the PC system, the Corporate Security Service identified an insider, a security officer, who appeared to be assigned to the evening security shift on the second floor security desk in Building 1. The Corporate Security Service interviewed him and he denied the allegation, stating that he did not download any inappropriate software. It was also determined that the password for this system was commonly known: it was a default password, the easily guessed "123456", and the computer was located in an open area. The officer stated that, during the course of any given shift, he might leave the security desk post to patrol or to cover for someone else's break, thereby leaving the system unprotected. It was hard for Corporate Security Service to find evidence linking the insider with these illicit activities.

6.2.1.4 DAMDIOA findings

DAMDIOA was used to investigate this allegation. Analysis of the insider activities showed the Corporate Security Service that four business emails were sent from the insider's email account and two were received by it. One of the most important emails was one he received from the Human Resource Department containing his performance appraisal and asking him to read and sign it. The signed appraisal was saved on the document folder on the hard disk. The insider attached this appraisal and sent it to the Human Resource Department at 0150. At 0157, another important email was a security

status report he sent to his supervisor. Hotspot Shield was received by email and downloaded at 0200. The pornographic movie was accessed at 0230, and at 0300 he emailed a security incident report to the security control center. At 0330 he received a message from a security officer located in Building 15 asking him to cover a post in that building because he needed to take a break. At 0335 the insider emailed his supervisor informing him of this.

The Corporate Security Service interviewed the insider again and presented him with these facts, whereupon he admitted in writing that he had indeed downloaded movies and on one occasion had accessed a pornographic website, because he had received an email including that website's link. He further stated that he had downloaded the inappropriate software "Hotspot Shield".

6.2.2 Case study 2

6.2.2.1 Background

One of the biggest private companies in Saudi Arabia has about 20,000 employees [4]. This organisation relies on computer systems to perform, process, transmit, store and retrieve data. The organisation uses a client/server operating system. Clients are organisational users' computers that request data or services such as email and directory services from organisational servers.

Active Directory (AD) is a critical database of users, computers and network resources; it makes the latter accessible to users and applications [4]. The groups are stored in the AD and are monitored by Microsoft Operations Manager (MOM). MOM can monitor, manage and secure a wide range of resources including computers, applications, Web server farms and corporate servers [4].

Two types of policy are implemented for Internet access in this organisation. The first is restricted access for one hour only for employees, while the second is unlimited access to the Internet for managers and above.

The company's IT security is responsible for securing IT resources and conducting computer forensic investigations.

6.2.2.2 A case of violation of the organisation's IT policies

An AD administrator reported to IT security that an employee – i.e. an insider – violated the organisation's IT policy by logging into its domain controller (DC) using a domain administrator account and illegally added his account and that of his co-worker to the manager's group, granting him unlimited Internet access.

Figure 41 demonstrates the electronic evidence that the insider's account was moved to open the Internet policy.

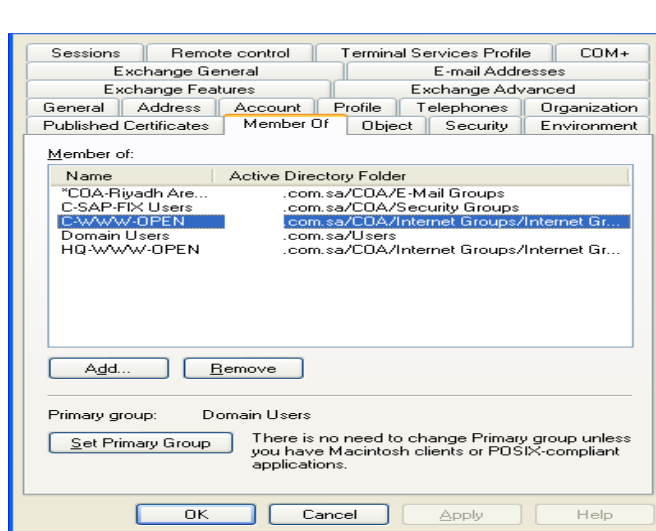


Figure 41 Evidence of modification Internet Policy

6.2.2.3 Initial findings

As a part of their investigation, the insider's PC was seized by IT Security, which conducted a technical analysis of its system and found that it was in fact used to access the DC. The insider gained administrator access in order to modify the policy by moving his account and another one from restricted to unlimited access. MOM detected the insider's breach of the organisation's Internet policy and sent an email to the AD administrator.

- **The server:**
 - Audit logs: the investigators found that the insider was successfully logged on to the administrator domain account in the AD at 1052;

- A message from MOM to confirm that the Internet policy had been changed by the insider at 1110
- **The insider's computer:**
 - Audit log: the investigator found that the insider had successfully accessed his computer at 0900.

The investigator interviewed the insider, who denied the allegation by claiming that he was out of his cubicle for more than two hours. He also stated that he always logged in to his computer and left it without logging out

6.2.2.4 DAMDIOA findings

The following information was collected:

- the insider's emails from the email servers
- those resources' log files that had been accessed by the insider
- the insider's job responsibilities

The insider's job was a company IT trainer responsible for teaching the company's employees how to use Microsoft software packages such as Word, Excel, Access and PowerPoint. He was also authorised to access SAP, which allowed him to input trainee's names into a company database.

This investigation revealed the following:

- **one business email has been sent to co-workers**

Analysis of the insider's email showed that one email sent to a co-worker included a list of trainees nominated to attend a Microsoft PowerPoint course. The content of this email matched one of the insider's job responsibilities.

- **two personal emails have been sent to his friends**

Analysis of the insider's email also revealed that he sent a message to his brother who worked for the same company but at a different branch. Another personal email had been forward to his co-worker (might be suspicious if not allowed).

- **the SAP application had been accessed and a file modified**

Analysis of SAP's file log found that 0925 the insider successfully accessed a training database, and that at 1021 he had added the names of those trainees that had

passed the Microsoft Excel course and submitted the list to the company's Training Manger Department for approval.

- **AD had been accessed**

After the data, including emails, access to SAP and modified files, were collected, the insider was questioned. Upon being presented with these facts, he admitted that he changed the policy because he wanted to access the Saudi Stock Market. Table 33 presents the time line of the insider's activities

Table 33: Timeline of the insider's activities

Timeline	Activities	Type of activities
9:12:28	Computer login	-1
9:25:00	Login SAP	-1
9:33:12	Forward personal email	1
10:21:00	Modified a file	-1
10:52:03	Access to AD	1
11:01:53	Send email to co-worker	-1
11:15:13	Change policy	0
11:47:42	Modified a file	-1
12:03:14	Send personal email	1

6.3 Challenging the distinction between insider and outsider attacks

It is not always possible to distinguish between insider and outsider attacks, because digital analysis usually depends upon output from protective security components [63]. The basic issues confronting corporate security in distinguishing between these attacks is therefore as follows:

6.3.1 The model's incapability of model to distinguish between co-workers

DAMDIOA is an unsuitable model by which to distinguish between attacks by co-workers. As previously mentioned, an outsider has no prior knowledge of an insider's job responsibilities. However, co-workers do have such information, because some jobs require more than one employee to perform. It is therefore very difficult for this model to determine which co-worker has carried out an attack.

6.3.2 The model's inability to model to distinguish between insider and outsider attacks

In some cases, DAMDIOA cannot distinguish between these attacks. As previously mentioned, an outsider has no prior knowledge of an insider's job responsibilities. However, if outsiders do manage to become familiar with these, (for example by using a physical key-logging), it is very difficult for corporate security investigators to ascertain who has carried out an attack. Also, if the number of legitimate activities is equal to the number of suspicious ones, a predetermined decision cannot differentiate between them.

6.3.3 Classification of activities

The problem this model has is that legitimate and suspicious activities must be classified. For example, it classes personal activities as suspicious because legitimate ones only include employees' job responsibilities. These activities must therefore be properly classified.

6.3.4 Relative weighing of activities

Legitimate activities are given the same significance. For example, both email login and read email are assigned values of -1. These values must be reconsidered in order to improve this mode.

6.3.5 Mis-configured security components

Security components such as firewalls or Intrusion Detection Systems (IDS) are hardware or software used to protect an organisation's system by filtering out unwanted network traffic and recording suspicious computer events. This record is essential if one is to comprehend the computer incident and the behaviour of the attacker. For example, if an IDS cannot correctly detect Trojans or any tools of hacking a loss of evidence of an attempt to steal an insider's access will result.

6.3.6 Lack of implementation of full-content network monitoring

The employment of trap and trace monitoring is one of the main problems in distinguishing between insider and outsider attacks, because it does not record a conversation's content, or payload. Trap and Trace monitoring only logs the transaction data summarising this network activity, consisting of IP address, port and username. This does not allow corporate security investigators to analyse the payload containing the substantive content of the packet.

6.3.7 Lack of preservation of the log files

Corporate security investigators sometimes face a problem if log files are not preserved correctly, because the integrity of log files is affected. Outsiders alter these logs upon gaining unauthorised access, thereby hiding the evidence of their crimes. In this case, it is very difficult to distinguish between insider and outsider attacks. These log files should preserve in a separate server to protect the integrity of these files.

6.3.8 Lack of recording of legitimate activities

Many security professionals focus on recording suspicious security events, but this alone is not enough to distinguish between insider and outsider attacks because it does

not indicate if the insiders are performing their jobs when the incidents in which they are involved occur. Furthermore, this lack of recording affects the identification of the relationship between insider job responsibilities and the activities carried out before and after the incidents in question.

6.3.9 Lack of retention policy

Another issue facing corporate security investigators is the fact that many organisations do not have retention policies. Only 50 per cent of U.S. organisations, for example, have formally embedded such policies [19] which are responsible for keeping security computer event and legitimate activity logs for certain periods of time. The lack of such a policy leads to the loss of evidence that can help distinguish between insider and outsider attacks.

6.4 Summary

This chapter aimed to evaluate the results of the eight experiments by comparing current methods of distinction between insider and outsider attacks (authorised access, location of initiation attack and attack within an organisation's control) and the proposed one of legitimate activity. The researcher found that the criterion of authorised access failed three times to make these distinctions. This method of distinction is useless when there is a blank or shared password. He also discovered that both the location from which an attack was launched and attack within an organisation's control failed five times to differentiate between such attacks. There are no substantive differences between these methods. The single instance in which the proposed method failed to make these distinctions was because the number of legitimate activities equalled the number of suspicious ones.

This chapter also discussed this model's use in the real world, in which it succeeded both times in making this distinction. The first case was when an insider in the form of an IT trainer violated the policy of his organisation by moving his account and that of a co-worker from restricted to unlimited Internet use. This model was able to name the insider who had committed this violation. In the second case another insider, a security officer, violated the organisation's policy by downloading a video pornographic. He denied this allegation until DAMDIOA was used to identify that particular violation with that employee.

The researcher also discussed the disadvantages of this model, one of these being that when outsiders have prior knowledge of insiders' job responsibilities, this model cannot distinguish between them. Another is that it misclassifies some activities such as the sending and receipt of personal emails, classifying them as suspicious because legitimate activities include employees' job responsibilities. The final disadvantage is that this model puts equal weight on all activities.

7 Recommendations

Objectives:

-
- to enhance security mechanism for the organisation's users
 - to improve the collection process of digital investigations
-

This chapter provides a number of recommendations in terms of ways to enhance the process by which an organisation can authenticate its users and maintain audit logs of security events. This chapter also facilitates the process of distinguishing between insider and outsider attacks by proposing a physical and logical log management system. This log management system comprises a centralised database for all employee activities. These recommendations will lead to improvements in the process of distinguishing between insider and outsider attacks.

7.1 Recommendations for enhancing an organisation's resource authentication

The researcher found that an organisation's user authentication is one of the main problems face a corporate security investigators when they dealing with distinction between insider and outsider attacks. This is because the insider access can be gained easily. Therefore, this section provides some recommendation to address this issue.

7.1.1 User authentication

Passwords are a universal form of authentication. However, password authentication is open to attack, as follows:

- it is subject to guessing; organisation
- the password may be written down and placed in a visible area
- it is subject to eavesdropping
- it is subject to social engineering

Based on the thesis experiments, , an outsider can exploit these vulnerabilities in order to obtain an insider's credentials. An organisation should enhance its IT security policy in order to prevent outsiders from obtaining insiders' credentials (passwords). In order to enhance the password policy, it should maintain and include the following:

7.1.1.1 Implementation of two factor authentication

Simple authentication schemes use a user-name and password to authenticate an organisation's user. This satisfies only a minimal security requirement because these passwords are often not difficult to guess. In two factor authentication, passwords still depend in part on something known by the user. However, in the most common implementation of two factor authentication, an organisation's users also use something they have, such as smart cards or something they are, such as biometrics, in order to enhance employee authentication. The researcher believes that the use of two factor authentication can prevent outsiders from gaining insiders' credentials.

7.1.1.2 Enable password complexity

This policy involves the checking of passwords to ensure that they meet strong password requirements, such as:

- not containing users' names or genuine names
- containing characters, digits and non-alphabetic characters
- not containing a dictionary word

7.1.1.3 Define the minimum password length:

Passwords should consist of at least a specific number of characters, usually more than fourteen characters. The main advantage of enforcing this policy is that it prevents an organisation's users from using blank passwords. It also forces users to create passwords that contain a certain number of characters.

7.1.1.4 Login security

This policy delays logins after incorrect attempts. Successful and failed logins are recorded.

The researcher suggests that employees should also protect their passwords from being obtained by outsiders. Employees should consider the following advice:

- do not reveal a password in an email message
- do not mention a password in front of others
- do not hint at the format of a password
- do not reveal a password to co-workers or to managers
- do not create easily guessed passwords, such as one's wife's name or "2010"
- do not choose a single password (Single Sign-On or SSO) for all applications, but choose a different password for each application (see the next section)

7.1.2 Enabling of different passwords for different applications

SSO allows an organisation's user to log in just once and navigate across many applications without the need to enter their credentials for each application. This makes it easy for the employee to login once and be able to access all the applications they want. SSO reduces the need for users to remember many logins and passwords. On the other hand, if outsiders obtain an insider's login then SSO makes it easy for access all the applications they want. Moreover, the key point here is that a single logon for the whole system will fail to capture individual activities; only separate logons for different applications will record activities in the detail necessary for forensic investigators.

To address this issue, a different password policy should be implemented. This policy would require different passwords for different services. The reason for this is that doing so would minimise the risk of an outsider obtaining an insider's passwords. If an outsider obtains a password or cracks an insider's computer, the organisation will want to limit him/her from getting access to more applications. For example, an employee should have two different access passwords: one for accessing their computer and the other for accessing their email account. Should an outsider obtain the password for an insider's computer, he is not then able to access the insider's email account and misuse the email service, due to different passwords being required.

7.2 Recommendations for enhancing an organisation's log files

To distinguish between insider and outsider attacks, it should enhance an organisation's log files. The researcher makes many recommendations to enhance these files.

7.2.1 Creating multiple event records

A main advantage of enabling different passwords for different applications is that there will be multiple security event records. The audit record can be implemented for each application's login to record security event information such as:

- successful and failed authentication attempts
- file access

The most important advantage of implementing monitoring/auditing for each login activity is that it generates security events for the activities of each login application. As a result of this action, the information collection process for distinguishing between insider and outsider attacks could be improved. It could also provide the analysis process with sufficient information. Therefore, employees should use different passwords for their various access needs.

7.2.2 Enabling of communication records

Communication records can provide corporate security with a list of dialled and received calls. This call list is another source of evidence that can help to support or refute any suggestion that the attack was committed either by an insider or an outsider. This log will help to identify whether the insider was in his office or not during the time of the initiation of an attack. It will also help to determine whether these calls were business-related or not.

7.3 Implementation of physical access controls

Organisations should enhance their security mechanisms by implementing physical access controls with two factor authentication, such as a smart card with that also requires a PIN. If the attack was initiated from inside the organisation, the physical access will be another source of evidence to support or deny a claim that the insider was

in his office during the time of the incident. The main advantage of physical access control is that it prevents an outsider from accessing an insider's office in person and implementing a physical keystroke logger on the insider's computer in order to obtain the insider's passwords. The physical access logs will provide a corporate security investigation with useful information, such as the last time the insider accessed his office and when he left his office, such as the last time the insider was using his office and when he left it.

7.4 Physical access control logs

A physical access log file, such as a card reader or CCTV tape, determines when the insider accessed the specific location, such as an organisation's building, floor or department. This source of evidence can be essential to show whether the attack was initiated from inside the organisation or not. This evidence will help to confirm whether the insider entered the premises or not.

Figure 42 shows the advantages of implementing recommendations that enhance the process of information collection and analysis for the purpose of distinguishing between insider and outsider attacks.

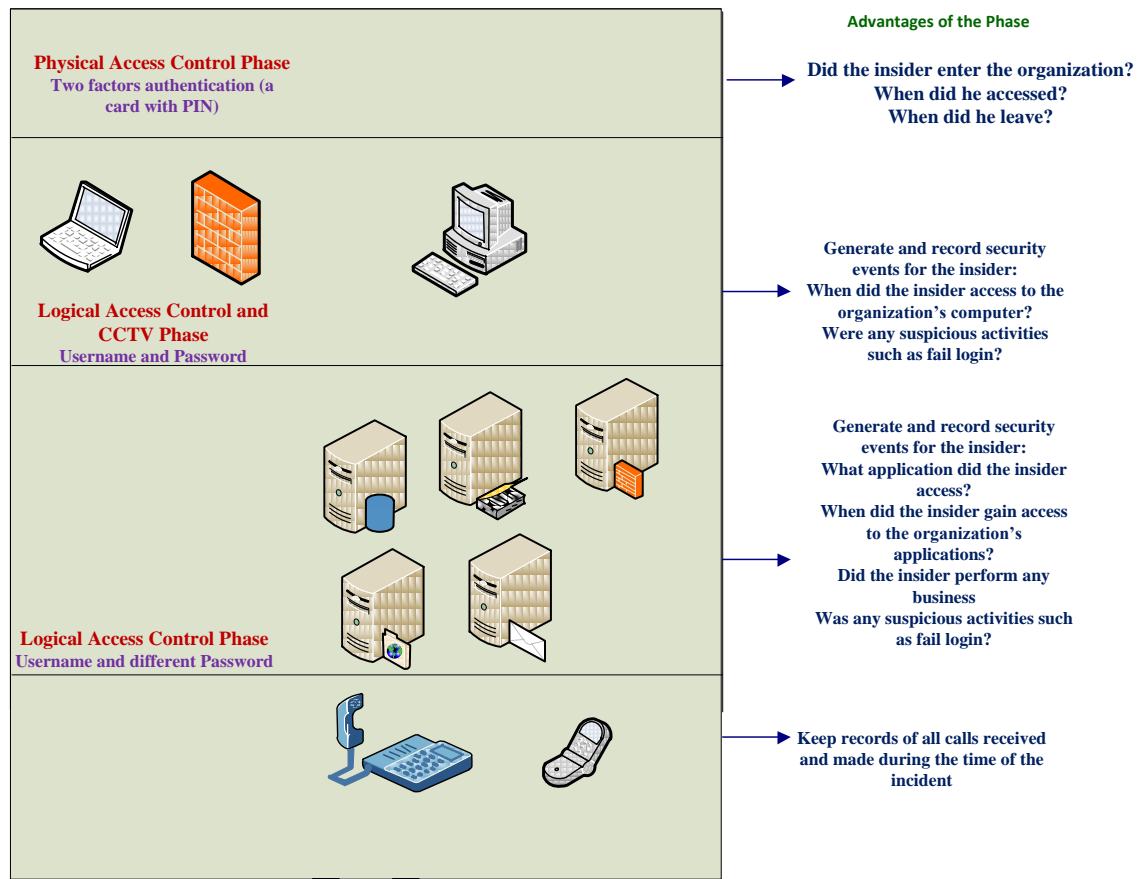


Figure 42: Advantages of enhancing the collection process

7.5 Insider and outsider activities log management

Following the success of manual investigation methods for distinguishing between insider and outsider attacks, the researcher suggests that automated methods could be implemented to facilitate these processes. As we saw in the research, log files are important to the success of such an investigation. An organisation should maximise its ability to collect physical and digital evidence in order to log all employee events in a centralised server. Therefore, the researcher suggests the creation and management of logs that can collect both digital and physical evidence.

7.5.1 Log management

The organisation should develop procedures for performing log management. Log management is aimed at creating and maintaining centralised physical and logical log files that record and store employees' activities, such as when an insider had access to a specific building, the last time he accessed his email account and when he left his office. Logs containing information relevant to security management are generated by many sources including:

- firewalls
- intrusion detection systems
- operating systems
- switches
- workstations
- applications
- physical card readers
- others

Moreover, this procedure should define minimal physical logging requirements in order to record and store sufficient detail for distinguishing between insider and outsider attacks, as follows:

- first and last name
- an organisation's employee ID
- date and time in
- destination
- date and time out
- description of activity

7.5.2 Components of logs management

These logs are designed to collect information for distinguishing between insider and outsider attacks. They consist of a number of components, as follows:

- log generation: as previously described, these logs are generated from many of the organisations' devices, such as servers, applications and firewalls. Each device generates its own log files
- log transmission and storage: these logs should be transferred from the original servers or computers to a designated log server (a collector). They should be protected from breaches of their confidentiality and integrity. These logs are transferred to the server either in a real-time or near-real-time manner, or in infrequent batches based on a schedule or the amount of log data waiting to be transferred;
- log analysis: in order to distinguish between insider and outsider attacks, two types of analysis will be employed: "timeline" and "relational" analysis. This analysis will provide the following advantages:
 - the log analysis is responsible for reconstructing activities, by reviewing and analysing the evidence, such as email activities, file activities and system logs
 - the log analysis provides a link between insider or outsider attacks and particular malicious events;
 - the log analysis could also be used to determine whether an insider's computer which has been involved in a crime was vulnerable to penetration
 - the log analysis shows what activities had been undertaken before and after the time of an incident;
 - the log analysis usually identifies patterns and anomalies
 - the log analysis identifies activities that were performed before and after the time of an incident in order to spot a possible relationship between these activities and the insider's job responsibilities (day-to-day organisational activities). As mentioned previously, one of the main characteristics of an insider is that they have authorised access to enable them to perform legitimate tasks; this analysis should identify whether these activities are indeed legitimate. If a malicious activity is found

among the legitimate activities, this may be an indication of an insider attack, because an outsider often has no prior knowledge of an insider's job responsibilities;

- a relationship between an insider and a victim, e.g. in the case of abusive e-mails, can be identified;
- a relationship between suspicious events and the exploitation of a system's vulnerability can be spotted;

This physical and logical log management will lead to improvements in the analysis process for distinguishing between insider and outsider attacks, because it will analyse not only an insider's computer activities, but extend to physical activities.

7.6 Interview insiders

The researcher believes that the aim of interview employees/insiders is to obtain some relevant facts about their job responsibilities and other information as follows:

- identify their secondary tasks
- identify their interest websites
- identify their coworkers and customers
- identify the requirement to perform their tasks

Another aim of this interview is to check the investigation findings with the information had been collected from the insider.

7.7 Security incident report policy

An organisation should create a security incident policy in order to report, as quickly as possible, all security incidents and events that may constitute a breach of security. The reporter (victim or IT security) should, as quickly as possible, write an email that presents the details. These incidents should be logged.

The purpose of gathering information about a previous security incident is to understand whether the insider's computer was the subject of penetration. It should consider how a

network administrator or a helpdesk operator dealt with the security incident. For example, it should collect the following information:

- has any an incident report been received from the insider or an IDS? If yes,
- has a security log for the insider's computer been checked, and any failed logins noticed?
- has an anti-virus program been run to check the applications on his computer?
Or was his password changed?

This information can be collected from a network administrator or a help desk. The researcher has created a basic sample of a Computer Incident Report (see the appendix).

7.8 Defining of user's job responsibilities

Human resource management (HRM) is another critical source of collecting employee information, which includes user's job responsibilities. This information helps to improve the process of distinction between insider and outsider attacks. However, the researcher believes that corporate security investigators may face an issue of defining a user's job responsibilities. To tackle this issue, the investigators should set up a regular meeting with HRM. An organisation's HRM should identify the following:

- lists the main activities an employee has to carry out
- role set which identify relation to other employees
- to whom is the employee responsible
- personal information from employee's file such as his/her personal email, his/her bank details and other information
- equipment and tools that are required to perform their tasks

7.9 Summary

This chapter has suggested a number of recommendations. These recommendations would improve the organisation's resources authentication such as enhancing password policy and enabling different passwords for different applications. They would also improve the audit log files for recording employee activities. Furthermore, the researcher suggests the creation and management of physical and logical logs in order to facilitate the process of distinguishing between insider and outsider attacks.

The researcher also suggests creating a security incident policy in order to report all security incidents and events that may constitute a security incident. Another suggestion is that user's job responsibilities should be identified by human resource management. These recommendations will improve the process of distinction between insider and outsider attacks.

8 Conclusion

This research has established both the importance and the possibility of distinguishing between insider and outsider attacks when conducting investigations into computer crime, in order to correctly identify suspects, to save organisations time and money, to avoid negative publicity for both the organisation and for the wrongly accused employee, and to forestall legal action. Recognising the impossibility of making this distinction purely on the basis of legitimate access (which outsiders may gain in an unauthorised fashion in order to launch criminal attacks on the organisation or its employees, or use to attack a third party), the researcher has clarified the current definitions of insiders and outsiders to reflect the importance of job responsibilities. He has then constructed a model, DAMDIOA, that builds on current ones in order to fulfil this function.

The researcher identified the main issues facing corporate security investigators involved in distinguishing between insider and outsider attacks as follows:

- None of the current methods of making such distinctions (methods involving the location from which the attack was initiated, attacks within an organisation's control and authorised access) address the problem.
- The lack of an organisation's resources authentication (for example, a single sign on or a weak password policy) allows outsiders easily to gain insider access.
- There is no conclusive model of computer forensic analysis of the distinction between insider and outsider attacks.

The researcher then identified the types of information required to collect and analyse in order to distinguish between these attacks, namely insider job responsibilities, legitimate and suspicious activities. The researcher also believed that legitimate activity should depend not only on access but also on execution of the user's job responsibilities. For example, if an organisational user's activity includes their job responsibilities, it is more likely to be legitimate activity; otherwise that activity is more liable to be sus-

picious. The researcher decided on legitimate activity incorporating job responsibilities as a basis for distinguishing between the types of attack because authorised access can easily be obtained by outsiders.

A Digital Analysis Model for Distinction between Insider and Outsider Attacks (DAM-DIOA) was therefore created by developing the DFRWS method to make it possible to make this distinction. DAMDIOA includes collection, examination, analysis, presentation and decision processes. Two analysis methods, timeline and relational analysis, were used to enable analysis of legitimate and suspicious activity.

Timeline analysis was used to establish the correct sequence of events, associating particular users with specific time periods, and to show what activities had been carried out before and after the occurrence of incidents. It also helped to identify an attack session. Relational analysis was used to analyse activities performed before and after an incident, if it proved necessary to do so, as well as during an attack session in order to identify a possible relationship between these activities and the insider's job responsibilities.

DAMDIOA also proposed two types of decision process: fixed decisionmaking, based on a predetermined logical condition, and decisions that can be tailored to the proportion of suspicious activity. The main difference between these decisions is that an organisation can customise the threshold of tolerance for such activity based on its level of concern for the type of attack involved. Sometimes, tailored decisions based on these threshold levels can address the problem of an attack whose type is unknown.

The success of this thesis has been measured according to the following criteria:

1. **Evaluation.** This research conducted a network simulation in which a network experimental test involving eight experiments based on both fixed and tailored decisions was set up to carry out computer incidents. One of the eight experiments, based on fixed decisions, failed to make that distinction because the number of suspicious activities equalled that of legitimate ones. Current methods of distinction between these attacks (authorised access, attacks within an organisation's control and locations of initiation attack) and the proposed method (legitimate activities) were compared.

Authorised access failed three times to distinguish between these attacks, in part because it was found not to be a suitable method of distinction between such attacks if blank or weak passwords are used. Attacks within an organisation's control as well as locations from which attacks were initiated failed five times to make this distinction. The researcher's findings therefore differ from those of Melara and Sarriegui [50] and Graves [34], who believe that the differences between insider and outsider attacks are based on whether they are initiated from inside or outside the organisation. The present findings also differ from those of Rowlingson[74], Schultz [78] and Randazzo *et al.* [68] because of their position that one of the main aspects of the distinction is authorised access.

2. **Comparative analysis**, which compares the proposed model with other computer forensic models. The researcher finds that the main differences between DAMDIOA and others are as follows:
 - Purpose: DAMDIOA has been designed to deal with the distinction between insider and outsider attacks, whereas other models such as DFRWS are general model that do not take the conduct of investigations into insider and outsider attacks into account.
 - Collection: DAMDIOA has identified types of data to be collected, whereas other models do not, instead usually focusing on collecting evidence of suspicious rather than legitimate user activities.
 - Analysis: DAMDIOA has employed both timeline and relational analysis to examine the user activities collected in the previous stage in order to identify the relationship between these activities and a user's job responsibilities. However, other models do not prescribe how to analyse collection data and what analysis methodology was used to analyse that data. For example, DFRWS was unable to distinguish between these attacks because of its omission of a method of relational analysis.
 - Decision: DAMDIOA's flexible decision process proposes two types of decision that allow an organisation to customise the level of threshold. No other models have this level of flexibility, relying instead on *ad hoc* methods.
3. Case study:

Two companies used this model to identify whether incidents were carried out by their employees or by another party. The first case concerned an IT trainer who violated the organisation's IT policy by logging into the Domain Controller using a domain administrator account and illegally added his account and that of his co-worker to the manager's group, granting him unlimited Internet access. DAMDIOA was used to determine whether or not this incident was in fact committed by the IT trainer. It did indeed find a link between the activities carried out during the incident and the trainer's job responsibilities.

In the second, a number of movies and games were downloaded and pornography was accessed by using a piece of proxy software. It was alleged that the organisation's employee, who worked as a security officer, downloaded inappropriate software. It was determined that the password for this system was commonly known: it was a default password, easily guessed, and the computer was located in an open area. However, DAMDIOA revealed that there were links between the activities carried out and the security officer's job responsibilities. The officer admitted in writing that he had indeed downloaded movies and on one occasion had accessed a pornographic website.

The researcher also discussed the limitations of DAMDIOA. One of these is that this model misclassifies employees' personal activities such as personal emails as suspicious activities, because legitimate activities only include employees' job responsibilities. It also allocates the same weighting of -1 to activities such as read emails and database logins. Neither can DAMDIOA's fixed decisions be able to distinguish between insider and outsider attacks when the number of legitimate activities equals the number of suspicious ones. Another limitation is DAMDIOA's inability to distinguish between such attacks when outsiders or co-workers have prior knowledge of insiders' job responsibilities.

Difficulties facing DAMDIOA include misconfigured security components, lack of implementation of network monitoring, overwriting or deletion of log files, failure to record legitimate activities and lack of a retention policy.

The researcher made many recommendations to enhance both the authentication process of an organisation's users and the audit logs of security events. These recommendations would lead to improvements in the process by which insider and outsider attacks are distinguished. The researcher also suggests creating a physical and logical log management system in order to facilitate the process by which this distinction is made

8.1 Future Work

8.1.1 Clustering of activities

To improve the process of distinguishing between insider and outsider attacks, user activities should be clustered into legitimate and suspicious activities. Two main issues must be tackled:

- I. What constitutes an "activity"?
- II. How activities be compared (for example, by similarity measures)?

8.1.2 Identification of the most important information

Based on the experimental results, it is not important to collect some legitimate activities such as reading emails or visiting public websites such as the BBC. However, some personal insider information such as access to personal email or bank accounts, is important in making this distinction. The researcher believes that studies should be conducted to identify the most important information that should be collected in order to improve the quality of the process of distinguishing between the two types of attack. This research may help address the issue of unclassified attacks.

8.1.3 Assigning relative weightings to legitimate and suspicious activities

A significant task for future research is to establish the values of legitimate and suspicious activities in order to evaluate their relative importance. The researcher found that some legitimate user activities are of no great importance for distinguishing between the two types of attack. For example, insider access, including computer logins, can be obtained without detection, so such activities do not help to establish which types of attack have been carried out.

However, some legitimate user activities such as logins to specific application services (e.g. email, database, SSH and personal email logins) are significant indicators of the type of attack, because they usually require different passwords. For this reason, assigning a relative weight to suspicious and legitimate activities may also improve the quality of this model, which does not prescribe this function. Table 36 shows the current weightings for legitimate activities..

Table 34: Relative weightings assigned to legitimate activities

Timestamp	Activities	Type of activities	Weight	
9:10:00	Computer login	-1	-1	low weight
9:12:00	Database login	-1	-3	high weight
11:18:00	Email login	-1	-3	high weight
11:23:00	Database login	-1	-3	high weight
12:00:00	Install specific software	-1	-2	
12:00:15	Computer login	1	1	
12:10:00	Modify file	0	0	
4:10:00	Forward email	-1	-1	low weight
5:10:00	Access bank account	-1	-5	high weight

8.1.4 Develop DAMDIOA:

Another task for future research is the development of DAMDIOA to work automatically as an investigation analysis tool that will lead to the collection of legitimate and suspicious employee activity in order to facilitate the distinction between insider and outsider attacks.

8.1.5 Applicability to various types of incident

The researcher believes that DAMDIOA can be applied to investigations into various types of offence, such as intellectual property (IP), information theft and the downloading of pornographic material. He suggests improving this model by using it to carry out real attacks in order to distinguish between insider and outsider attacks and evaluating the results.

8.1.6 Users' job responsibilities/roles

Another area in which improvement is required concerns that of users' job responsibilities. These should be better defined, and their collection should be improved through the use of a standard method. In this regard it is necessary to establish precisely what information, such as personal email accounts and previous employers, is relevant, and should therefore be collected from employees' files

9 References

- [1] Ackerman, E. (2007). Hackers' infections slither onto Web sites. The Seattle Times: http://seattletimes.nwsourc.com/html/business/technology/2003556913_hackers05.html, [Last Accessed: 12/11/2008]
- [2] ACPO (2005). Good Practice Guide for Computer based Electronic Evidence. UK.
- [3] Al-Anazi, S. (2003). The means of the investigation in the information systems crimes. police Science Department, Naif Arab University for Security Sciences: 428.
- [4] Al-Murjan A. and K.Xynos, 2008, "Network Forensic Investigation of Internal Mis-use/Crime in Saudi Arabia: a Hacking Case", 2008 ADFSL: Association of Digital Forensics, Security and Law, University of Oklahoma, USA
- [5] Anderson, P. (1980). Computer Security Threat Monitoring and Surveillance, James P. Anderson Co.
- [6] Ashcroft, J. (2001). A Guide for First Responders.: http://209.85.229.132/search?q=cache:2SKC2uT62vcJ:www.crimesceneforum.com/document%2520files/cyber_crime_investigation.pdf+Technical+Working+Group+for+Electronic+Crime+Scene+Investigation+2001&cd=5&hl=en&ct=clnk&gl=uk [Last Accessed: 02/11/2008]
- [7] BERR (2008). 2008 Information Security Breaches Survey. UK.
- [8] BBC (2002). Internet abuse costs big money. Available from: <http://news.bbc.co.uk/1/hi/technology/2381123.stm> [Last Accessed: 08/01/2010]
- [9] BBC (2005). Warning on hard drives' security. 2006: http://news.bbc.co.uk/2/hi/uk_news/wales/4272395.stm [Last Accessed: 27/11/2008]
- [10] BBC (2008). Probe into data left in car park. 2009: http://news.bbc.co.uk/2/hi/uk_news/wales/4272395.stm [Last Accessed: 10/12/2009]
- [11] Blyth, A. and G. L. Kovacich (2006). Information Assurance. USA, Springer.
- [12] Casey, E. (2004). Digital Evidence and Computer Crime. California, Academic Press.
- [13] Casey, E. (2004). "Network traffic as a source of evidence: tool strengths, weaknesses, and future needs." Digital Investigation 1(1): 28-43.
- [14] CERT. (2002). Spoofed/Forged Email. **2009**: http://www.cert.org/tech_tips/email_spoofing.html [Last Accessed: 10/12/2009]
- [15] CERT. (2002). Email Bombing and Spamming. **2009**: http://www.cert.org/tech_tips/email_spoofing.html [Last Accessed: 10/12/2009]

- [16] CERT. (2009). Smurf Attacks. 2009: <http://www.cert.org/advisories/ca-1998-01.html> [Last Accessed: 12/12/2009]
- [17] Ciardhuain, S. (2004). "An extended Model of Cybercrime Investigations." *International Journal of Digital Evidence* 3(1).
- [18] CSI/FBI: CSI/FBI. (2006). "Computer crime and security survey, " Computer Security Institute, USA
- [19] CSI/FBI: CSI/FBI. (2008). "Computer crime and security survey, " Computer Security Institute, USA
- [20] Dark Reading. 2006, Social Engineering the USB Way, <http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634> [Last Accessed: 14/09/2008]
- [21] Dataclinic (2008). Forensic Computer Crime Invesatigations-Case Studies & Testimonials. 2008: <http://www.dataclinic.co.uk/computer-case-studies.htm> [Last Accessed: 08/08/2009]
- [22] Dhillon, G. (1999). "Managing and controlling computer misuse." *Information Management & Computer Security* 7(4).
- [23] Dhillon, G. Moore, S. (2001). "Computer crimes: theorizing about the enemy within." *Computers & Security* 20(8): 715-723
- [24] Endicott-Popovsky, B., D. Frincke, et al. (2007). "A Theoretical Framework for Organisational Network Forensic Readiness." *Journal of Computers* 2(3): 1-11.
- [25] FBI (2009). Common Fraud Schemes. 2009: <http://www.fbi.gov/majcases/fraud/fraudschemes.htm> [Last Accessed:12/11/2009]
- [26] Fildes, J. (2009). Phishing attack targets Hotmail. 2009: <http://news.bbc.co.uk/2/hi/8291268.stm> [Last Accessed: 20/10/2009].
- [27] Furnell, S. (2004). "Enemies within: the problem of insider attacks." *Computer Fraud & Security* 2004(7): 6-11.
- [28] Gartner, 2002, There Are No Secrets: Social Engineering and Privacy 1 (1): <http://www.gartner.com/gc/webletter/security/issue1/> [Last Accessed: 06/12/2007]
- [29] GFI (2009). Protecting your network against email threats. 2009: <http://www.gfi.com/whitepapers/network-protection-against-email-threats.pdf> [Last Accessed:12/12/2009]
- [30] Gojzman, J. and P. Rawles (2000). *Local Area Networks A Business-Oriented Approach*, John Wiley & Sons.

- [31] Gollmann, D. (2006). Computer Security. UK, Wiley.
- [32] Granger S. (2001). Social Engineering Fundamentals, Part I: Hacker Tactics, Internet: <http://www.securityfocus.com/infocus/1527> [Last Accessed: 15/1/2008]
- [33] Gragg D., 2002, A multi-level defence against Social Engineering: <http://www.sans.org/rr/papers/51/920.pdf> [Last Accessed: 06/12/2007]
- [34] Graves, K. (2007). CEH Official Certified Ethical Hacker, Wiley.
- [35] Greene, T. (2007). Client Side attacks on the rise. **2008:** <http://www.networkworld.com/news/2007/112807-client-side-attacks-rise.html> [Last Accessed: 10/12/2009]
- [36] Greenwood, L. (2004). E-mail scams cost banks £1m: <http://news.bbc.co.uk/2/hi/programmes/moneybox/3654311.stm> [Last Accessed: 08/07/2009]
- [37] Haggerty, J. and Taylor, M. (2006). "Managing corporate computer forensics." Computer Fraud & Security 2006(6): 14-16.
- [38] Hansman, S. and R. Hunt (2005). "A Taxonomy of Network and Computer Attacks." Computers and Security 24(1): 31-43.
- [39] IANA, 2005, Port Numbers, 2007: <http://www.iana.org/assignments/port-numbers> [Last Accessed: 1/11/2007]
- [40] Keeney, M., E. Kowalski, et al. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, CarnegieMellon Software Engineering Institute.
- [41] Kemp, M. (2005). "Barbarians Inside the Gates: Addressing Internal Security Threats." Network Security 2005(6): 11-13.
- [42] Kent, J. and B. Ghavalas (2005). "The Unique of Collecting Corporate Evidence." Digital Investigation 2(4): 239-243.
- [43] Kleiman, D., K. Cardwell, et al. (2007). The Official CHFI Exam 312-49. USA, Syngress.
- [44] Koen, R. and S. Olivier (2008). The Use of File Time stamps in Digital Forensics. Information Security for South Africa 2008 Innovative Minds Conference, University of Johannesburg, ISSA.
- [45] Komar, B. S. a. B. (2003). Microsoft Windows Security Resource Kit, Microsoft Press.
- [46] Levin, K. and C. Simon (2005). Recent developments concerning electronic discovery. **2009:** <http://www.sifma.org/services/hrdiversity/pdf/KramerLevinPresentation.pdf> [Last Accessed: 25/05/2009]

- [62] Nykodym, N., R. Taylor, et al. (2005). "Criminal profiling and insider cyber crime." *Digital Investigation* 2(4): 261-267.
- [63] Palmer, G. (2001). *A Road Map for Digital Forensic Research*. New York.
- [64] Park, J. S. and J. Giordano (2006). The Access Control Requirements for Countering Insider Threats. IEEE Symposium on Intelligence and Security Informatics (ISI) Conference, San Diego, California.
- [65] Pennsylvania University. (2008). E-mail Forgery and Harassment. **2009**: <http://www.upenn.edu/computing/security/advisorries/forgery.php> [Last Accessed: 12/11/2009]
- [66] PriceWaterHouseCoopers (2006). Information Security Breaches Survey 2006- Technical Report.
- [67] Pouwelse, J. Garbaki, P., et al. (2005). *The Bittorrent P2P File-Sharing System: Measurements and Analysis*, Springer Berlin 3640 (2005).
- [68] Randazzo, M. Keeney, M. et al. (2005). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, Carnegie Mellon Software Engineering Institute: 1-21.
- [69] Rasmussen, J. (2006). Password Authentication. *HandBook of Information Security*. H. Bidgoli. U.S.A, John Wiley & Sons, Inc. 3: 1124.
- [70] Reith, M., C. Clint, et al. (2002). "An Examination of Digital Forensic Models." *International Journal of Digital Evidence* 1(3).
- [71] Roberts, C. (2005). *Voice over IP*, Centre for Critical Infrastructure Protection., New Zealand.
- [72] Rogers, K. (2006). Internal Security Threats. *HandBook of Information Security*. B. H. U.S.A, John Wiley & Sons, Inc. 3: 1124.
- [73] Rowlingson, R. (2004). "A Ten Step Process for Forensic Readiness." *International Journal of Digital Evidence* 2(3).
- [74] Rowlingson, R. (2005). Inside and out? The Information Security Threat From Insiders. 4th European Conference on Information Warfare and Security, University of Glamorgan, UK, Academic Conferences Limited.
- [75] Riden, J. (2008). Client-Side Attacks. 2008: <http://www.honeynet.org/node/157> [Last Accessed: 13/06/09]
- [76] Schiffman, M. D., A. J. O'Donnell, et al. (2003). *Hacker's Challenge2: Test Your Network Security and Forensic Skills*, Corel Ventura.
- [77] Schneier, B. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.

- [78] Schultz, E. E. (2002). "A Framework for Understanding and Predicting Insider Attacks." *Computer & Security* 21(6): 526-531.
- [79] Schweitzer D. (2002). *Internet Security Made Easy, A Plain-English guide to protecting yourself and your company online*, Amacom, U.S.A.
- [80] Sculley, D. and G. Cormack (2008). "Filtering Email Spam in the Presence of Noisy User Feedback", CEAS 2008- the Fifth Conference on Email and Anti-Spam, Mountain View, USA.
- [81] Selamat, S., R. Yusof, et al. (2008). "Mapping Process of Digital Forensic Investigation Framework." *International Journal of Computer Science and Network Security* 8(10): 163-169.
- [82] Sommer, P. (2005). *Directors and Corporate Advisors Guide to Digital Investigations and Evidence*. London, Information Assurance Advisory Council.
- [83] Sommer, P. (2006). "Criminalising Hacking Tools." *Digital Investigation*: 68-72.
- [84] Spooner, D., D. Cappelli, et al. (2009). *Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations*, Carnegie Mellon University.
- [85] Stallings, W. (2002). *Network Security Essentials: Applications and Standards*. New Jersey, Prentice Hall.
- [86] Stanton, J. M. and K. R. Stam (2006). *The Visible Employee*. New Jersey.
- [87] Stanton, J. M., K. R. Stam, et al. (2004). "Analysis of end user security behaviors." *Computers and Security* 24(2): 124-133.
- [88] Sullivan, B. and Howard, M. (2005). *The Microsoft SDL and the CWE/SANS Top 25*. 2009: <http://209.85.229.132/search?q=cache:h3s9T0A9qXoJ:download.microsoft.com/download/C/A/9/CA988ED6-C490-44E9-A8C2-DE098A22080F/Microsoft%2520SDL%2520and%2520the%2520CWE-SANS%2520Top%252025.doc+Weak+access+control+to+secret+data+Howard+2005&cd=1&hl=en&ct=clnk> [Last Accessed:10/11/2009]
- [89] Tanenbaum, A. (2002). *Computer Networks*, Pearson Education.
- [90] Taylor, J. and D. Haggerty. (2007). *Criminal Offences and Corporate Computer Forensics*. ACSF 2007 Proceedings of the 2nd Conference on Advances in Computer Security and Forensics, Liverpool, UK, Liverpool JMU.
- [91] Tcpcap (2009). *Tcpcap/Libpcap*. 2009: <http://www.tcpcap.org/> [Last Accessed: 15/07/2009]
- [92] The International Association of Computer Investigative Specialists, (2007). "Forensic Procedure". 2007:<http://www.iaicis.net/forensicprocedures> [Last Accessed: 15/07/2008]

- [93] Ubuntu (2008). What is Ubuntu? **2009:** <http://www.ubuntu.com/products/whatisubuntu> [Last Accessed: 10/06/2009]
- [94] Ubuntu (2008). Exim4. **2009:** <https://help.ubuntu.com/community/Exim4> [Last Accessed: 14/06/2009]
- [95] Ubuntu Geek (2008). DNS server setup using bind in Ubuntu. **2009:** <http://www.ubuntugeek.com/dns-server-setup-using-bind-in-ubuntu.html> [Last Accessed: 14/06/2009]
- [96] UK Statistics Authority. (2008): <http://www.statistics.gov.uk> [Last Accessed: 25/03/2008]
- [97] University of Washington. (2008). Pine Information Center. **2009:** <http://www.washington.edu/pine/> [Last Accessed: 05/06/2009]
- [98] US-CERT. (2009). Report Phishing. **2009:** http://www.us-cert.gov/nav/report_phishing.html [Last Accessed:15/12/2009]
- [99] Vidalis, S. and Jones, A. (2005). Analyzing Threat Agents& Their Attributes, Glamorgan University: 369-390.
- [100] Walker, P. (2008). American expats caught up in Indian bomb blast inquiry. 2008: <http://www.guardian.co.uk/world/2008/jul/29/india.terrorism> [Last Accessed: 27/12/2008]
- [101] Walton, R. (2006). "Balancing the insider and outsider threat." Computer Fraud & Security 2006(11): 8-11.
- [102] Wang, Y., J. Cannady, et al. (2005). "Foundation of computer forensics: A technology for the fight against computer crime." Computer Law & Security Report 21(2): 119-127.
- [103] Willassen, S. and S. Mjolsnes (2005). "Digital forensics research." Telektronikk (Information Society and Security) 1.2005: 92-97.
- [104] Wilson, C. (2008). CRS Report for Congress: Botnets, Cybercrime, and Cyberterrorism: Vulnerability and Policy Issues for Congress: <http://www.fas.org/sgp/crs/terror/RL32114.pdf> [11-05-2009]
- [105] Wireshark (2009). Wireshark. **2009:** <http://www.wireshark.org/> [Last Accessed: 17/06/2009]
- [106] Xie, M., H. Yin, et al. (2006). An "An Effective Defense Against Email Spam Laundering", the 13th ACM Conference on Computer and Communications Security, Alexandria, USA.
- [107] Young, K., Case, Y. (2004). Internet Abuse in the Workplace: New Trends in Risk Management. CyberPsychology and Behavior.

-
- [108] Zhuang, L., Dunagan, J., et al. (2008). characterizing botnets from email spam records. Usenix Workshop on Large-Scale Exploits and Emergent Threats, USA, USE-NIX Association.

Appendixes

Appendix A: Build configuration of experiment

A1. Iptables

Each table comprises several built-in chains and may also contain user-defined chains. Furthermore, each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. Table 35 illustrates filter packet chain types.

Table 35: Filter Packet Chain Types

Queue Type	Queue Function	Packet Chain	Function
Filter	Packet filtering	Forward	Filters packets to servers accessible by another NIC on the firewall
		Input	Filters packets destined to the firewall
		Output	Filters packets originating from the firewall

Table 36 illustrates the policy of the Iptables chains [47].

Table 36: Policy of Iptables Chains

Target	Description
Accept	<ul style="list-style-type: none"> ▪ Iptables stops further processing ▪ The packet is handed over to the end application or the OS for processing
Drop	<ul style="list-style-type: none"> ▪ Iptables stops further processing ▪ The packet is blocked
Log	<ul style="list-style-type: none"> ▪ The packet information is sent to the syslog daemon for logging ▪ Iptables continues processing with the next rule in the table ▪ It is common to have two similar rules in sequence. The first rule will log the packet, the second rule will drop it
Reject	<ul style="list-style-type: none"> ▪ Works like Drop target

A2. Ubuntu Requirement:

The minimum system requirements of Ubuntu Desktop are as illustrated in the below Table 37 [93]:

Table 37: Minimum System Requirements of Ubuntu

	Minimum System Requirements	Recommended minimum Requirements
Processor	300 MHz	700 MHz
Memory	256 MB	384 MB
Hard drive (Capacity)	4 GB	8 GB
Graphic Card	640x480	1024x768

A3. Netkit Requirements:

It requires the following parts to work properly [61]:

- Core;
- Kernel of virtual machines;
- File systems.

The minimum system requirements of Netkit are illustrated in the below Table 38:

Table 38: Minimum System Requirements of Netkit

	Minimum System Requirements
Processor	600 MHz
Memory	256 MB
Hard drive (Capacity)	800 MB

A4. Technical Configuration Description

Technical configuration for the experiment is described as follows:

- LAB_DESCRIPTION=" set-up and conduct experimental test (small network)"
- LAB_VERSION=1
- Outsider-pc[0]="a"
- Outsider-pc[mem]=24

External firewall Machines hosting the Firewall and log files need more memory

- Fw-1[0]="a"
- Fw-1[1]="b"
- Fw-1[mem]=64

DMZ Machines hosting the exim4 MTA need more memory

- Mail-server[0]="b"
- Mail-server[mem]=32

Internal firewall Machines hosting the Firewall and log files need more

- Fw-2[1]="b"
- Fw-2[0]="c"
- Dnsorg[mem]=64
- Victim1[0]="c"
- Victim1[mem]=24
- Insider[0]="c"
- Insider[mem]=24
- Co-worker[0]="c"
- Co-worker[mem]=24
- Group-leader[0]="c"
- Groupleader[mem]=24
- Manager[0]="c"
- Manager[mem]=24

A5. Setting the Network

It sets up a network between 5 virtual machines. A network with 5 hosts connected to the same collision domain:

1- Creating the 5 Vms as follows:

- Create insider and a console window for insider
 - vstart insider –eth0=a
- Configure network interface
 - ifconfig eth0 146.227.128.4 netmask 255.255.255.0
- Test the network connection between machines to make sure machines can reach each other.
 - Ping 146.227.128.3. Figure 43 shows the experiment's network connection reach each other.

```

— Starting Netkit phase 1 init script —
Mounting /home/tiger on /hosthome...
Mounting /home/tiger/test-1 on /hostlab ...
— Netkit phase 1 initialization terminated —

Starting system log daemon...
Starting kernel log daemon...

— Starting Netkit phase 2 init script —

>>> Running insider specific startup script...
>>> End of insider specific startup script.

*****

Lab directory (host): /home/tiger/test-1
Version: 1
Author: A. Al-Morjan
Email: almorjan@dmu.co.uk
Web: <none>
Description:
Configuration and operation of the First Experimental small network
*****

— Netkit phase 2 initialization terminated —

insider login: root (automatic login)
Last login: Tue Oct 6 21:58:14 UTC 2009 on tty0
insider:~# ping 146.227.128.3
PING 146.227.128.3 (146.227.128.3) 56(84) bytes of data:
64 bytes from 146.227.128.3: icmp_seq=1 ttl=64 time=7.39 ms
64 bytes from 146.227.128.3: icmp_seq=2 ttl=64 time=1.03 ms
64 bytes from 146.227.128.3: icmp_seq=3 ttl=64 time=0.371 ms
64 bytes from 146.227.128.3: icmp_seq=4 ttl=64 time=0.316 ms
64 bytes from 146.227.128.3: icmp_seq=5 ttl=64 time=0.890 ms
^C
--- 146.227.128.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4050ms
rtt min/avg/max/mdev = 0.890/2.361/7.999/2.819 ms
insider:~#

```

Figure 43: Using Ping for testing Experiment network connection

The rest of VMs are configured the same way but the IP addresses for the following machines are different. Table 39 shows the IP addresses for the rest machines.

Table 39: IP Address for Experiment's Client Machines

Machine Names	IP Addresses
Victim	146.227.128.3
Manager	146.227.128.5
Group-leader	146.227.128.6
Co-worker	146.227.128.7

2- Creating fw-2 and configuring network interface as follows:

- Ifconfig eth0 146.227.128.2 netmask 255.255.255.0 up
- Ifconfig eth1 146.227.192.3 netmask 255.255.255.240 up
- Route add -net 1.1.1.0 netmask 255.0.0.0 gw 146.227.192.1 dev eth1
- Route add -net 146.227.128.0 netmask 255.255.255.0 gw 146.227.128.2

dev eth0

- `Route add -net 146.227.192.0 netmask 255.255.255.240 gw 146.227.192.3 dev eth1`

Iptables Policy is configured 'forward chain' as follows:

- `Iptables -A FORWARD -p tcp --dport 25 -s 146.227.128.4 -d 146.227.192.2 -j LOG --log-prefix ***mailattack***--log`
- `Iptables -A FORWARD -p tcp --dport 110 -s 146.227.128.4 -d 146.227.192.2 -j LOG --log-prefix ***mailattack***--log`
- `Iptables -A FORWARD -p tcp --dport 143 -s 146.227.128.4 -d 146.227.192.2 -j LOG --log-prefix ***mailattack***--log`

3- Creating fw-1 and configuring network interface as follows:

- `Ifconfig eth0 1.1.0.2 netmask 255.0.0.0 up`
- `Ifconfig eth1 146.227.192.1 netmask 255.255.0.0 up`
- `Route add -net 146.227.128.0 netmask 255.255.0.0 gw 146.227.192.3 dev eth1`

Iptables Policy is configured forward chain as follows:

- `Iptables -A INPUT -p tcp --destination 146.227.192.2 -i eth0 --dport 25 -j ACCEPT`
- `Iptables -P INPUT DROP`

4- Creating Mail-server and configuring network interface as follows:

- `Ifconfig eth0 146.227.192.2 netmask 255.255.255.240 up`
- `Route add default gw 146.227.192.3`
- `Route add default gw 146.227.192.1`

Also

- `/etc/init.d/bind start`

- /etc/init.d/exim4 start
- /etc/init.d/inetd start

5- Configure MUA (pine) on PCs:

- Start Pine on insider
- Type password (insider) to login into incoming mail server
- Select set-up (configure pine option)
- Press C to move to a main menu
 - 1-Identifying the sender:
 - Personal-name =Bob
 - 2- Identify the name of the local domain:
 - User-domain =Test.com
 - 3- Identify outgoing (SMTP) mail server:
 - Smtplib-server =Mail.test.com
 - 4- Identify the location of the incoming mailbox (server name; protocol; user=username folder name)
 - Inbox-path =imap.test.com/user=insider}inbox
 - 5- Tick (x) reply-always-users-reply-to
 - 6- Customized -header = Reply-To: insider@test.com
 - 7- Exit set-up

Figure 44 shows a configuration of MUA for the insider's machine.

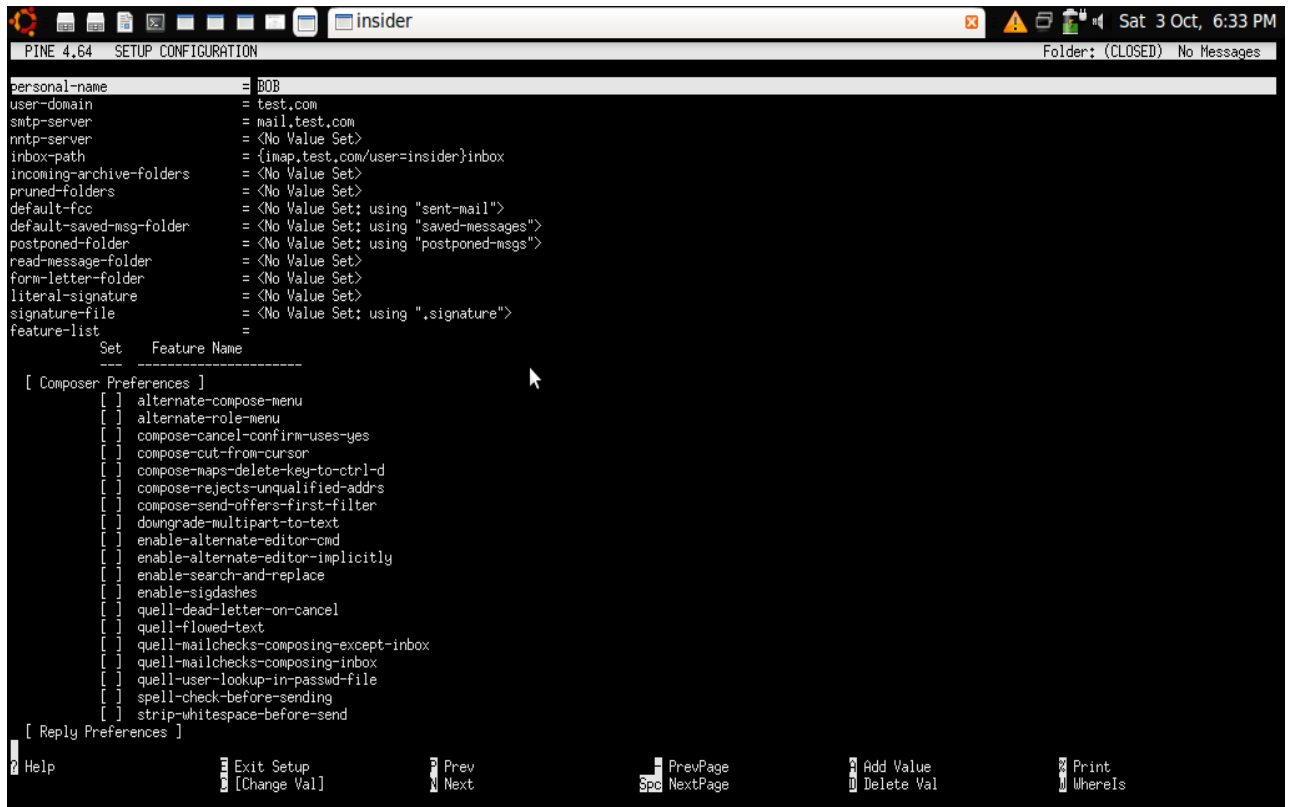


Figure 44: Configuration of MUA for insider's client

The rest of PCs are configured pine in the same way but instead of insider typing victim, manager, group-leader and co-worker.

□ 6- Configuring email servers, sending and receiving emails:

1-Configure MTA (exim4):

- Create exim4.conf file:
 - Gedit /etc/exim4/exim4.conf
 - Identify domains for which mail is accepted as a final destination. type domain name: Main-Local-Domains = @:localhost:test.com
 - Identify subnet:Main_Relay_Nets = 164.227.0.0/24
- Create inetd.conf
- Determine email protocols 110 for pop3 or 143 for imap
 - Pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/ipop3d
 - Imap stream tcp nowait root /usr/sbin/tcpd /usr/sbin/imapd

where stream is socket type; nowait is only applicable to datagram sockets; root is name of the user who starts daemon; /usr/sbin/tcpd is daemon name and tcpd is providing logging and access control capabilities.

Pop and imap server running on the mxs provide access to the mailboxes of the users.

2- Create new five user accounts on the MX

- An “insider” user account is defined on the mx password:insider
- An “outsider” user account is defined on the mx password:outsider
- A “manager” user account is defined on the mx password:manager
- A “group-leader” user account is defined on the mx password:group-leader
- A “co-worker” user account is defined on the mx password:co-worker

Figure 45 shows that new five accounts were created in MX.

```
mail-server:~# cat /etc/shadow
root:~:14219:0:99999:7:::
daemon:*:14219:0:99999:7:::
bin:*:14219:0:99999:7:::
sys:*:14219:0:99999:7:::
sync:*:14219:0:99999:7:::
games:*:14219:0:99999:7:::
man:*:14219:0:99999:7:::
lp:*:14219:0:99999:7:::
mail:*:14219:0:99999:7:::
news:*:14219:0:99999:7:::
uucp:*:14219:0:99999:7:::
proxy:*:14219:0:99999:7:::
www-data:*:14219:0:99999:7:::
backup:*:14219:0:99999:7:::
list:*:14219:0:99999:7:::
irc:*:14219:0:99999:7:::
gnats:*:14219:0:99999:7:::
nobody:*:14219:0:99999:7:::
libuuid:!:14219:0:99999:7:::
bind:*:14219:0:99999:7:::
messagebus:*:14219:0:99999:7:::
dnsmasq:*:14219:0:99999:7:::
Debian-exim:!:14219:0:99999:7:::
freerad:*:14219:0:99999:7:::
statd:*:14219:0:99999:7:::
sshd:*:14219:0:99999:7:::
pdns:!:14219:0:99999:7:::
proftpd:!:14219:0:99999:7:::
ftp:*:14219:0:99999:7:::
quagga:*:14219:0:99999:7:::
snmp:*:14219:0:99999:7:::
snort:*:14219:0:99999:7:::
telnetd:*:14219:0:99999:7:::
uwl-net:*:14219:0:99999:7:::
xorp:*:14219:0:99999:7:::
quest:~:14219:0:99999:7:::
insider:$1$PMLUXZHM$9adToXUjFTzrLxIWTvSDt.:14520:0:99999:7:::
victim:$1$ZUST,ABW$9C8IYd,G1EEYM4yocxzcP0:14520:0:99999:7:::
manager:$1$SVUAPkbn$ADl/.,jexFtA3Sy/sF9ur8.:14520:0:99999:7:::
group-leader:$1$YnCTrac1$TpT67UpQR09HEbtct7Tj2x0:14520:0:99999:7:::
co-worker:$1$7_bvqNXY9NSxmZo5/BGn./ut56ocJl:14520:0:99999:7:::
mail-server:~#
```

Figure 45: Creation of new five accounts in MX

3- Configure DNS:

- Geidt /etc/bind/db.com.test

- Identify the following services in the same host:
- Name service: @ dns.test.com
- The mail exchanger for domain: @ MX 5mail.test.com
- Imap.test.com
- Pop.test.com
- Mail.test.com

1-Configure NS:

- Gedit (/etc/bind/) named.confin order to associate between zone and name server
- Identify where to find information about the root name server: type hint; file “/etc/bind/db.root”
- Identify the primary master for zone: type zone “test.com”
- Identify the location where to find data about names in the zone: type file “/etc/bind/db.com.test”

2- Authoritative information:

- Gedit db.com.test
- Determine time to live in seconds (long a resource record should be cached)
TTL 60000
- Type @ in SOA mail.test.com (2009031801; serial
28; refresh
14; retry
3600000 ; expire
negative cache ttl)
 - Where IN: record class (Internet)
 - SOA: record type (Start of Authority)
 - Mail.test.com: primary master server for the zone mail.test.com

3- Configure slave/master server:

- 2009031801: serial number that includes year(yyyy), month(mm), day (dd) and number of change within that day (nn).

- 28; refresh: (refresh interval) informs a slave how to check that data for zone is up to date.
- 14; retry: interval between subsequent attempts to contact the master.
- 3600000 ; expire: slave expire time: when the slave fails to contact the master for this amount of time, it considers the zone data old and stops giving replies about it.
- Negative cachettl: ttl for negative responses from authoritative name servers

4- Association between name and IP addresses:

- Identify the authoritative name server for the zone (test.com) is dns.test.com:
@ IN NS dns.test.org
- Identify the mail exchanger for domain test.com
@ IN MX 5 mail.test.com.

Where 5 is a preference value and mail.test.com is the mail exchanger for domain test.com.

- Determine the number of pcs (6) in this zone:
 - Victim IN A 146.227.128.3
 - Insider IN A 146.227.128.4
 - Manager IN A 146.227.128.5
 - Group-leader IN A 146.227.128.6
 - Co-worker IN A 146.227.128.7
 - IMAP IN A 146.227.192.2
 - POP IN A 146.227.192.2
 - Mail IN A 146.227.192.2

Note: imap.test.com, pop.test.com and mail.test.com are the same host.

Figure 46 shows the configuration of experiment's server (NS).

```

$TTL 60000
@      IN      SOA     mail.test.com      root.dns.test.com. (
                2009031801 ; serial
                28 ; refresh
                14 ; retry
                3600000 ; expire
                60000 ; negative cache ttl
                )
@      IN      MX     5      mail.test.com.
@      IN      NS     dns.test.com.
insider-pc IN A      146.227.128.4
victim-pc IN A      146.227.128.3
co-worker IN A      146.227.128.7
group-leader IN A    146.227.128.6
manger  IN A      146.227.128.5

imap    IN A      146.227.192.2
pop     IN A      146.227.192.2
mail    IN A      146.227.192.2
telnet  IN A      146.227.192.2

```

Figure 46: Configuration of Experiment's server (NS)

▪ User Activities:

1- Insider Activities: Many activities are conducted as follows:

- Business emails are sent;
- No business email is sent;
- No business email is received;
- Business emails are received;
- Business files are stored in his pc;
- An abusive email is sent.

2- Victim Activities: Many activities are conducted as follows:

- Business emails are sent;
- Business emails are received;
- An abusive email is received from the insider.

3- Manager, co-worker and group-leader Activities: Many activities are conducted as follows:

- Business emails are sent;

- Business emails are received.

7- TCPdump:

TCPdump is downloaded on the PC by using this command-line `apt-get install tcpdump`. Then TCPdump is used on fw-2 to sniff all packets that travels over the network. The command line to perform a full packet monitoring and log it is as follows [92]:

- `Tcpdump -n -i eth1 -s 1518 -w /hosthome/tiger/log27-05-09.pacp &`
 - -n: Do not convert addresses (such as host addresses, port numbers, etc) to names. Display the numerical address;
 - -i: Listen on the specific interface and capture the traffic of a particular interface eth1;
 - -s: Number of bytes captured per packet (default is 68)
 - -w: Write the raw packet to a file log27-05-09.pacp

8- Launching the experiment: After configuring the components of this experiment, the next step is to run this experiment. The components of this experiment are automatically launching and comprises of the follows:

- 7 virtual machines are started;
- All interfaces are configured;
- Name server automatically configured and started;
- MTA is automatically configured and started;
- MUAs are automatically configured.

9- Sending an emails: To send an email and record the activities of the insider, it should follow these steps:

- Place on fw-2;
- Start tcpdump;
 - `Tcpdump -n -i eth1 -s 1518 -w /hosthome/tiger/log27-05-09.pacp &`
- Place on insider;

- Start pine (password: insider) and compose an email to one of the following addresses:
 - Victim@test.com;
 - Manager@test.com;
 - Group-leader@test.com;
 - Co-worker@test.com;
- Press Ctrl-X to send the message.

10- Receiving an email: To receive an email, it should follow these steps:

- Place on insider;
- Start pine and check for incoming messages;
- On the main menu select folder list;
- Select inbox to check the incoming messages;
- Select the message.

11- Investigation of an abusive email

When a victim received an abusive email and the insider is refuting the allegation of sending the abusive email, the investigation is conducted to find out evidence that supports whether it was sent by the insider or the outsider.

12- Abusive email

On the 27th of May 2009 at 11:49:24 pm, Alice (a victim user) received an abusive email and reported it to the computer forensic team. The header of the email indicated that the email was sent by Bob (an insider). When an investigation was conducted, the insider refuted the allegation of sending the abusive email. The insider claims that the password was gained by a hacker (an outsider) and he was not on his computer during the time of the incident. Therefore, computer forensic investigation should be carried out to prove/disapprove whether the insider sent the email or not.

13- The abusive email: the following details are the information of the abusive email:

Date: 27 May 2009 23:00:55.338698000 (UTC)

From:insider user <root@test.com>

Reply-To: insider@test.com

To: victim@test.com

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

xxxabuse emailXXXXXXXXXX

xxxabuse emailXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Appendix B: The Process of Analysis the Attack Experiments

B1.Ex1:

▪ 1.Collection process:

Because of analysing the legitimate activity of the insider, it needs to review job description/ responsibility for the insider and the location of the legitimate activities. The main purpose of gathering information from various sources is to gain an understanding of the insider's responsibilities and the case. This experiment employs two types of information gathering: network diagram and job description/ responsibility for an insider.

2.Review of Network Diagram:

Before conducting a digital investigation for distinction between insider and outsider attacks, network diagram should be reviewed in order to understand the structure of an organisational network and identify the location of the activity (evidence). This diagram gives further technical details about security devices such as number of firewalls and identifies computers that were involved in this issue.

Figure 47 shows that there are three parts of an organisational network: external, DMZ and internal networks. Two firewalls are set up. The first firewall has two interfaces. The first interface connects the external network and the second interface connects a DMZ network. The second firewall also has two interfaces. The first interface connects the DMZ network and the second interface connects an internal network. The diagram also showed that there is a chance to retrieve valuable information from the internal firewalls log.

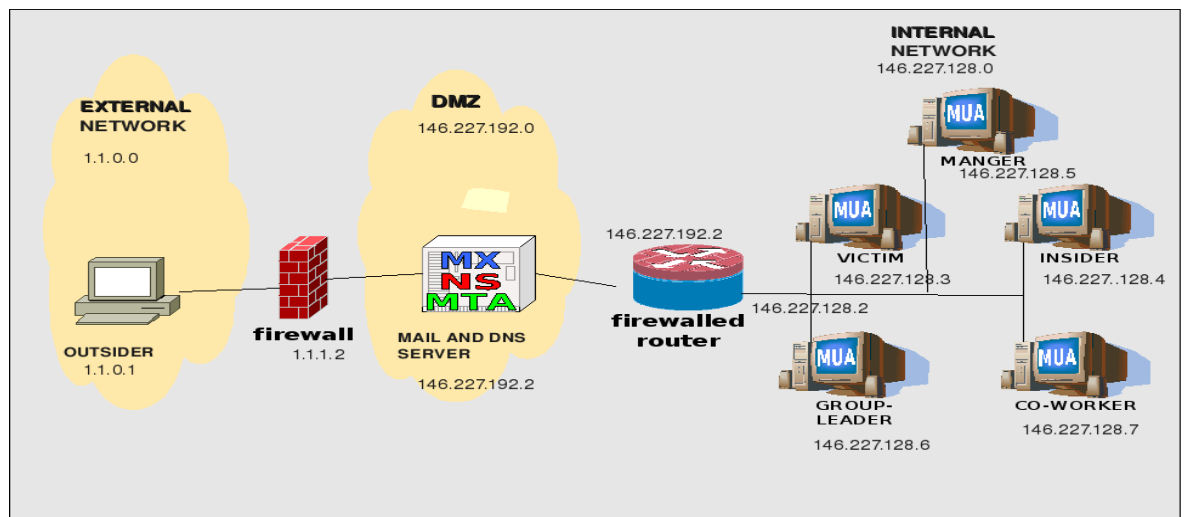


Figure 47: Review Experiment's network

This diagram shows that there is no file server and no web server for this company. Therefore, these activities retrieve from:

- Mail server (emails);
- The insider's computer (files/folders).

Analysis email activities assist to identify the relationship between the emails and the insider's job (business) activities. Analysis files and folders help to identify the relationship between the insider's files/folders and the insider's job activities. Importantly, a review of job description and responsibility for the insider is needed to make a match of relationships between the insider and these activities to distinguish between insider and outsider attacks.

Collecting packets:

After conducting a full-packet monitoring, it logged 4340 packets. The next step is to extract these activities for the insider from these packets. Wireshark is used to retrieve and analyse these packets. Figure 48 showed that there are 4340 packets and different IP addresses and different protocols.

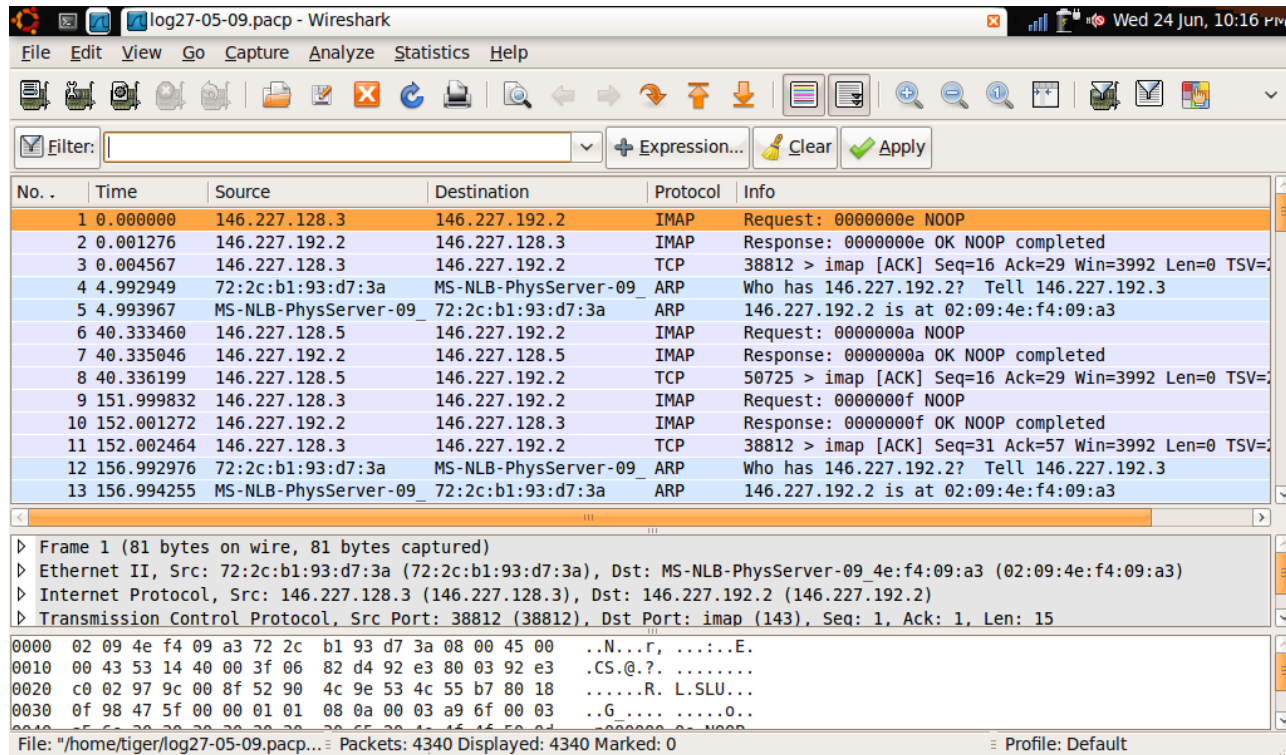


Figure 48: Examine the insider's activity

However, it is not easy to analyse 4340 packets. An employment of Wireshark can reduce the number of the packets by customising filter. To reduce the number of packets, it should identify the insider's IP address and protocol. The experiment is interested in an insider's IP address 146.227.128.4 and email protocols, two protocols IMAP (port no. 143) and SMTP (port no. 25). A following command is used:

- `imap and ip.addr == 146.227.128.4`

The purpose of using this command is as follows:

- Reducing the number of analysing packets from 4340 to 183;
- Displaying only the insider email activities;
- Displaying login and logout for the inbox email.

Another command was used as follows:

- `smtp and ip.addr == 146.227.128.4` command

The aim of this command is as follows:

- Reducing a number of analysing packets from 4340 to 194;
- Displaying only the insider's sending emails.

Figure 49 shows that imap activity for the insider reduces the number of packets that

subject to examine.

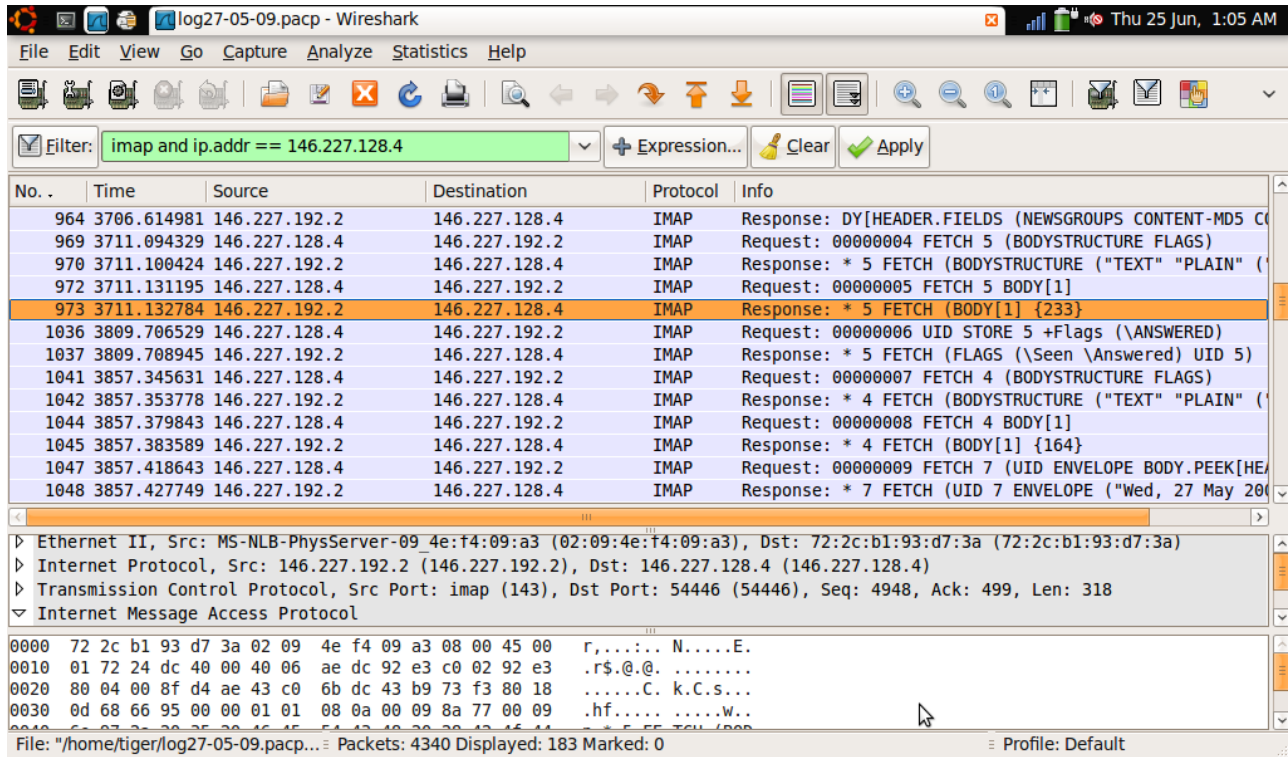


Figure 49: IMAP insider's activity

Figure 50 shows that SMTP activity for the insider reduces the number of packets that subject to examine.

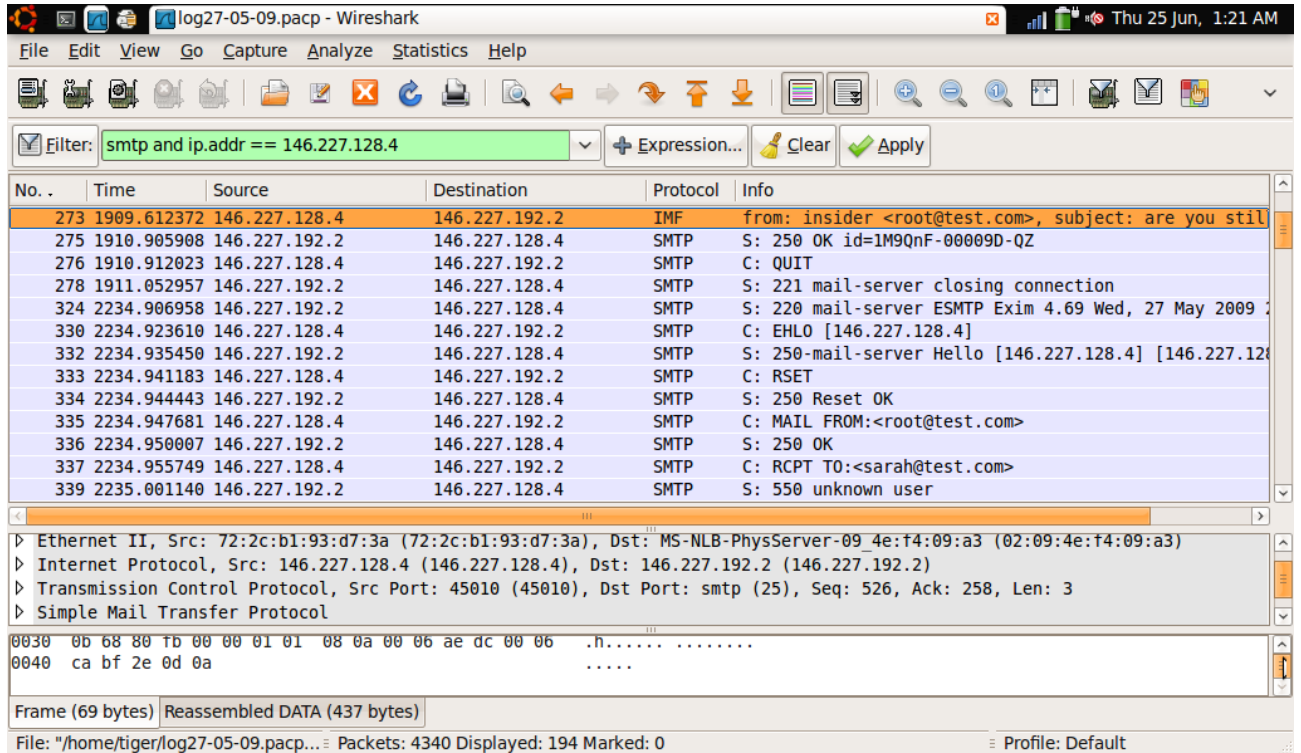


Figure 50: SMTP insider’s activity

3.Examination Data:

The goal of this analysis is to examine exchange mail messages that had been sent and received by the insider. After reducing the packets, the next step is to extract/examine the mail messages for the insider in order to analyse these emails. There is a list of legitimate activities generated by the insider as follows:

Login no.1: This login was the first login activity of the insider for this night on the 27th of May 2009. The insider's computer (146.227.128.4) logged into a mail server (146.227.192.2) at 22:31:56. This login activity indicated that this is a legitimate access because there was no failed login. Therefore, the access method is classified as an AC.

Figure 51 shows that when using Wireshark tool, the technical information connection between the insider computer and a mail server occurred. This information showed that a packet's header includes source and destination IP, source port number 53319 and destination port no 143 (IMAP). It also showed that body packet includes authentication login.

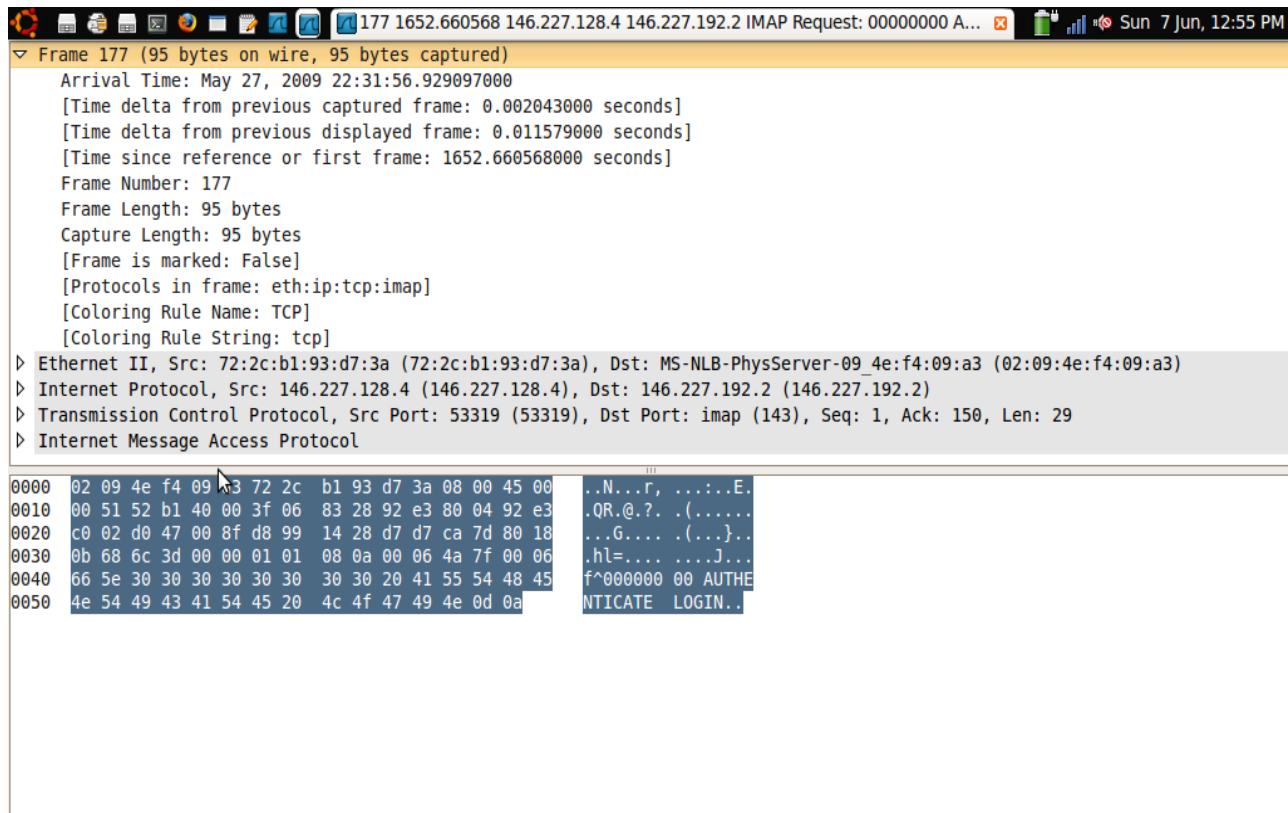


Figure 51: Examine insider's authentication login

Email no.1: The message had been sent from an insider (Bob) to a victim (Alice). It showed that the insider asked whether Alice was still in Cardiff or not and whether she met Abdulrazaq or not. The source IP address of the message was 146.227.128.4, the destination IP address was 146.227.192.2 and the destination port no. was 25 at 22:36:13. The content type of the message was text/plain.

At this stage is not easy to identify the type of a message whether it was a business email or a personal email because there is no relationship between Abdulrazaq and their organisation. Moreover, there is no match between insider's job responsibilities and the content of this message. Therefore, this email is classified as NBE.

Figure 52 showed that the header of a packet contained source and destination IP addresses and source port no 45010 and destination port no 25 (SMTP). It is also showed that the body of a packet included the content of the message.

```

Frame 271 (182 bytes on wire, 182 bytes captured)
  Arrival Time: May 27, 2009 22:36:13.871122000
  [Time delta from previous captured frame: 0.001744000 seconds]
  [Time delta from previous displayed frame: 0.001744000 seconds]
  [Time since reference or first frame: 1909.602593000 seconds]
  Frame Number: 271
  Frame Length: 182 bytes
  Capture Length: 182 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:smtp]
  [Coloring Rule Name: tmp_color_filter_01]
  [Coloring Rule String: (ip.addr eq 146.227.128.4 and ip.addr eq 146.227.192.2) and (tcp.port eq 45010 and tcp.port eq 25)]
  Ethernet II, Src: 72:2c:b1:93:d7:3a (72:2c:b1:93:d7:3a), Dst: MS-NLB-PhysServer-09_4e:f4:09:a3 (02:09:4e:f4:09:a3)
  Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
  Transmission Control Protocol, Src Port: 45010 (45010), Dst Port: smtp (25), Seq: 410, Ack: 258, Len: 116
  Simple Mail Transfer Protocol

0000  02 09 4e f4 09 a3 72 2c b1 93 d7 3a 08 00 45 00  ..N...r, ...:..E.
0010  00 a8 68 09 40 00 3f 06 0d 79 92 e3 80 04 92 e3  ..h.@.7. my.....
0020  c0 02 af d2 00 19 d2 0d ca cb d2 00 b3 91 80 18  ..h.....
0030  0b 68 28 81 00 00 01 01 08 0a 00 06 ae dc 00 00  ..hi Ali ce..i ho
0040  ca bf 68 09 20 41 6c 69 63 65 0d 0a 69 20 68 6f  ..pe you a re ok. a
0050  70 65 20 79 6f 75 20 61 72 65 20 6f 6b 2e 20 61  ..re you s till in
0060  72 65 20 79 6f 75 20 73 74 69 6c 6c 20 69 6e 20  ..Cadiff? did you
0070  43 61 64 69 66 66 3f 20 64 69 64 20 79 6f 75 20  ..meet Abd ulrazaq?
0080  6d 65 65 74 20 41 62 64 75 6c 72 61 7a 61 71 3f  ..see yo u later.
0090  0d 0a 73 65 65 20 79 6f 75 20 6c 61 74 65 72 0d  ..best regards.
00a0  0a 0d 0a 62 65 73 74 20 72 65 67 61 72 64 73 0d  ..Bob..
00b0  0a 42 6f 62 0d 0a
  
```

Figure 52: Examine insider's email activity

Email no.2: The message had been sent from the insider to Alice showed that Bob sent a reminder email to Alice in order to ask her to email him a car incident report as soon as possible. The email was sent at 22:47:46 and the content type of the message was text/plain. The analysis of email content identified that one of the insider job activity is to follow up car incident reports for Test Company. It is also to prepare a security morning report. There are matches between the insider's job responsibilities and the content of this message. Therefore, this email is classified as a BE.

Figure 53 shows that the content of this message included a business email because it contains one of the insider's job responsibilities.

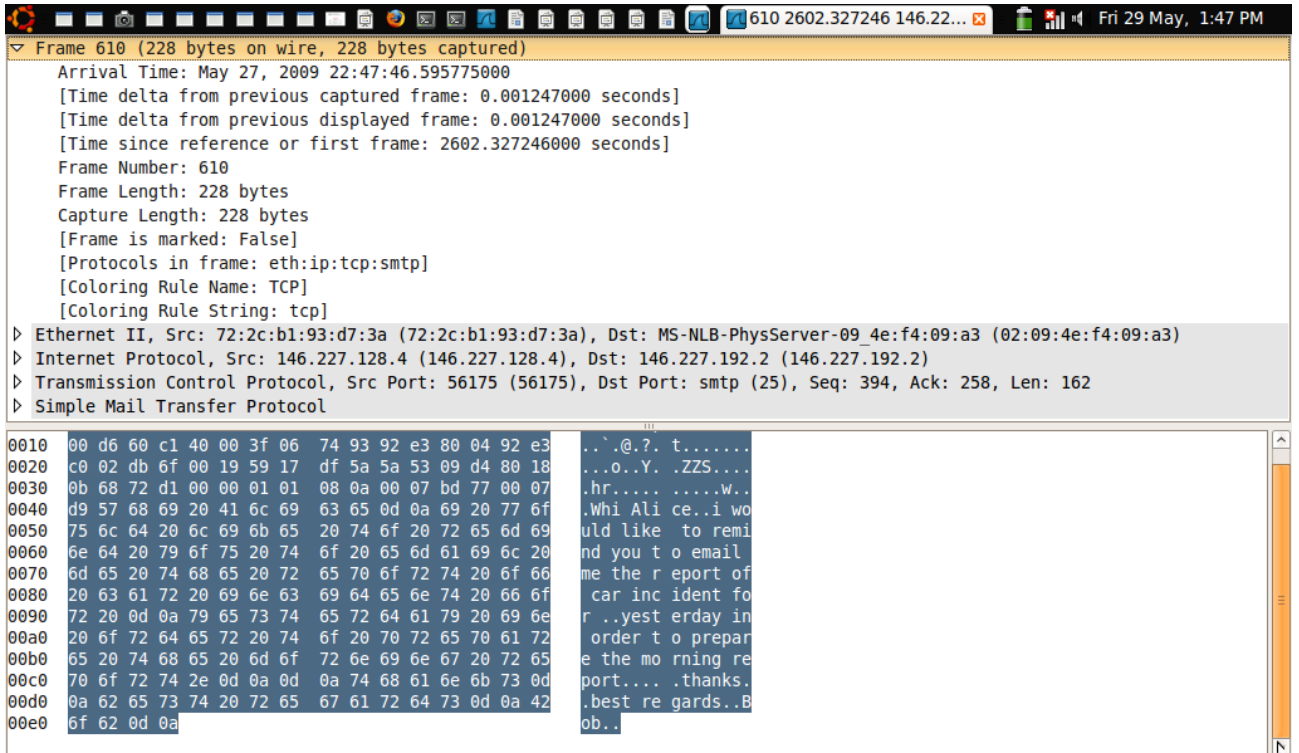


Figure 53: Examine insider’s email activity

Email no.3: The message had been sent from Sarah to the insider. It contained a car incident report. There is an exchange of business data between the insider and Sarah. This message indicated that another insider job activity is to collect car incident reports. There is a match between the insider's job responsibility and this email. Therefore, this email is classified as a BE. The email was received at 22:58:46 and the content type of the message was text/plain.

Email no.4: This message is a reply email from the victim to the insider. This exchange message showed that there is no business data between the insider and the victim because it a contained personal message (informal relationship). However, this investigation is not going to analyse this relationship. There is no matching between the insider's job responsibilities and this email. Therefore, this email is classified as NBE. The email was received at 22:59:07 and the content type of the message was text/plain.

Email no.5: The message had been sent from the insider to the victim. It contained an abusive email. This message was sent at 23:00:55 and the content type of the message was text/plain. Importantly, the message was sent among the insider's business activity.

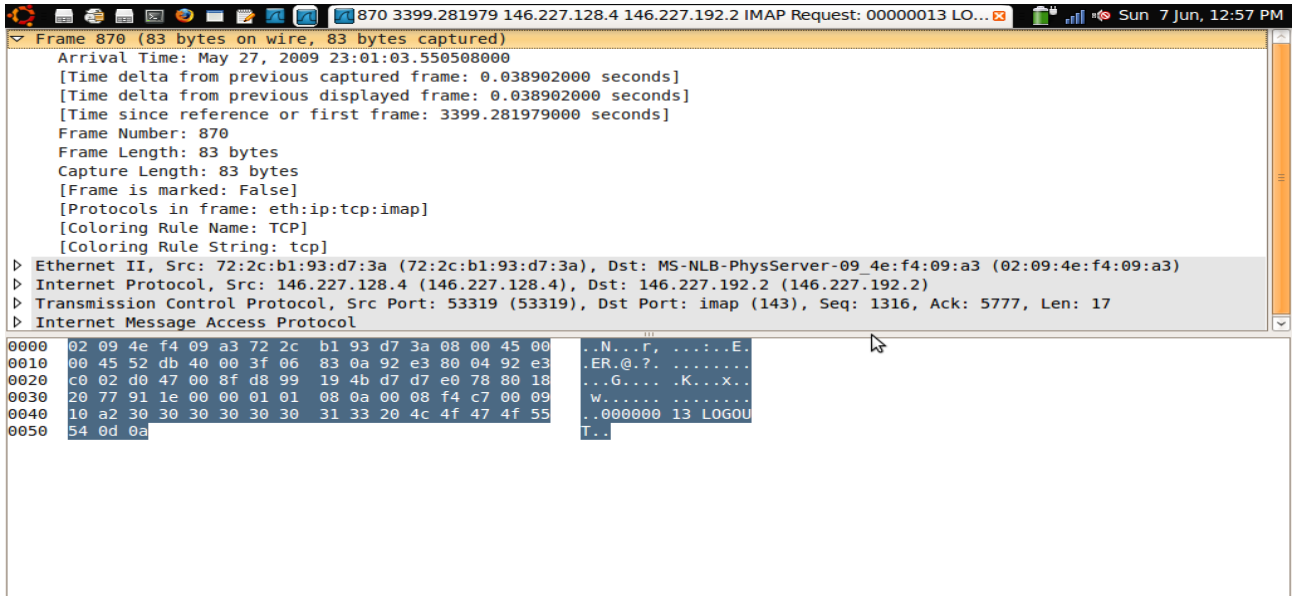


Figure 55: Examine insider’s logout activity

Login no.2: After 4 minutes from the insider’s logged out from the mail server, the insider logged into the server again at 23:05:49. The method of access is classified as an AC. Figure 56 shows that insider’s authentication was successful.

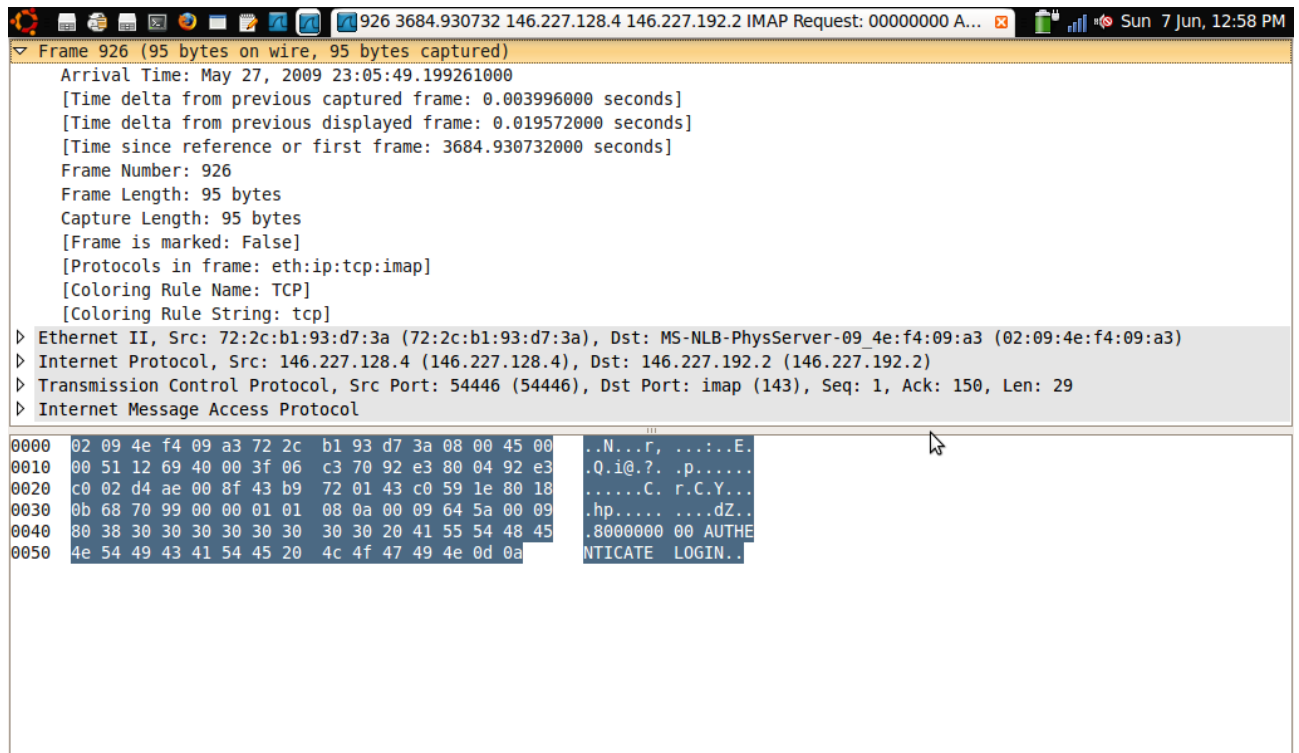


Figure 56: Examine insider’s authentication login

Email no.6: The message had been sent from the manager to the insider. This email indicated that the insider is not only responsible for collecting car accident reports but is also responsible for reducing the number of car incidents which leads to directly reducing the cost for the company. In addition, the analysis of this email showed that the manager asked the insider to attend a formal meeting with AVG Company. This meeting is aimed at discussing how to reduce car accidents for Test Company employees. The manager will expect a reply message from the insider. Therefore, series of messages will be exchanged between them. There is match between the insider's job responsibilities and this email's content. Therefore, this email is classified as a BE. The email was received at 23:06:15 and the content type of the message was text/plain.

Figure 57 shows that the insider received a message from his manager. This message indicated there was a meeting with AVG Company.

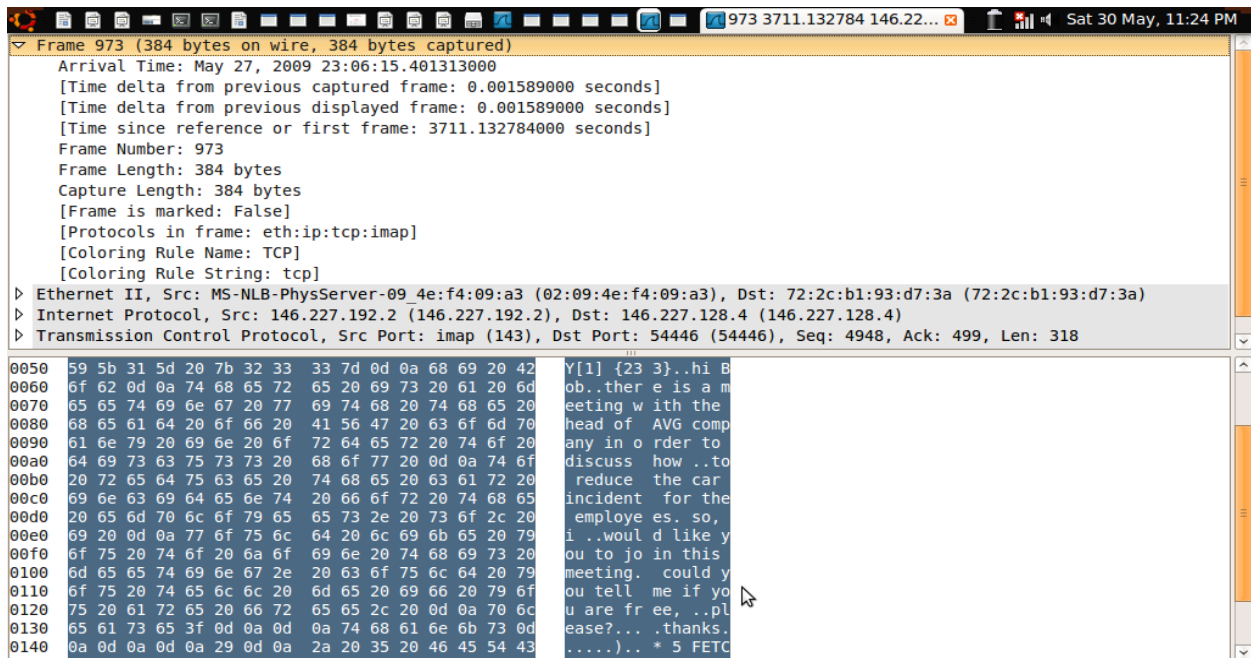


Figure 57: Examine insider’s email activity

Email no.7: The message had been sent from the group-leader to the insider. This email showed that the insider is responsible for creating a monthly report for car accidents and storing them. In addition, the analysis of this email showed that there is a business relation between the group-leader and the insider. There is a match between the insider's

job responsibilities and this email content. Therefore, this email is also classified as a BE. The requested email was received at 23:08:41 and the content type of the message was text/plain.

Figure 58 shows that the message's content included a monthly security incident request from the group leader.



Figure 58: Examine insider's email activity

Email no.8: The message had been sent from the insider to the manager. It contained the insider's reply to his manager's Email no.6. The insider informed his manager that he is going to attend the meeting. He also asked his manager when the meeting will take place. The insider will expect a reply message from the manager. A series of messages will be exchanged between them. Moreover, there is matching between the insider's job responsibilities and the email content. Therefore, this email is classified as a BE. The BE was sent at 23:24:27 and the content type of the message was text/plain. Figure 59 showed that the message content contained the insider replied to his manager's email.

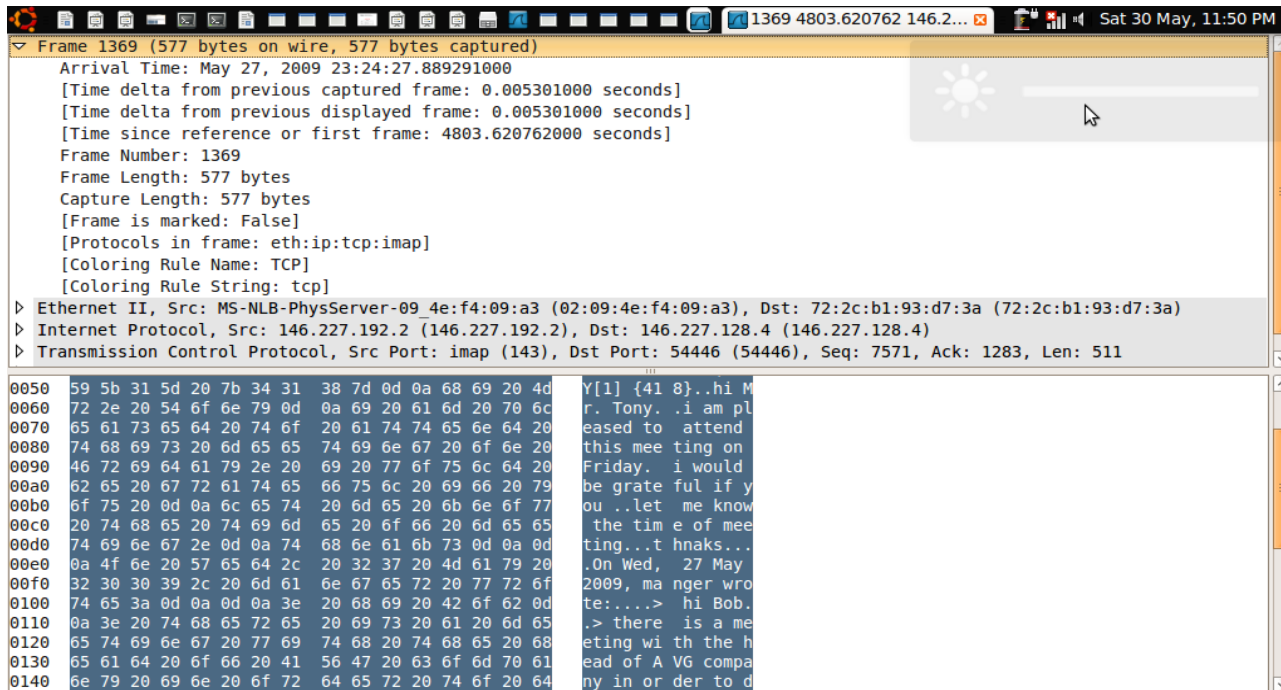


Figure 59: Examine insider’s email activity

Logout: When the insider replied to his manager's email, he logged out at 23:24:38.

Figure 60 shows that the insider was logged out from the mail server.

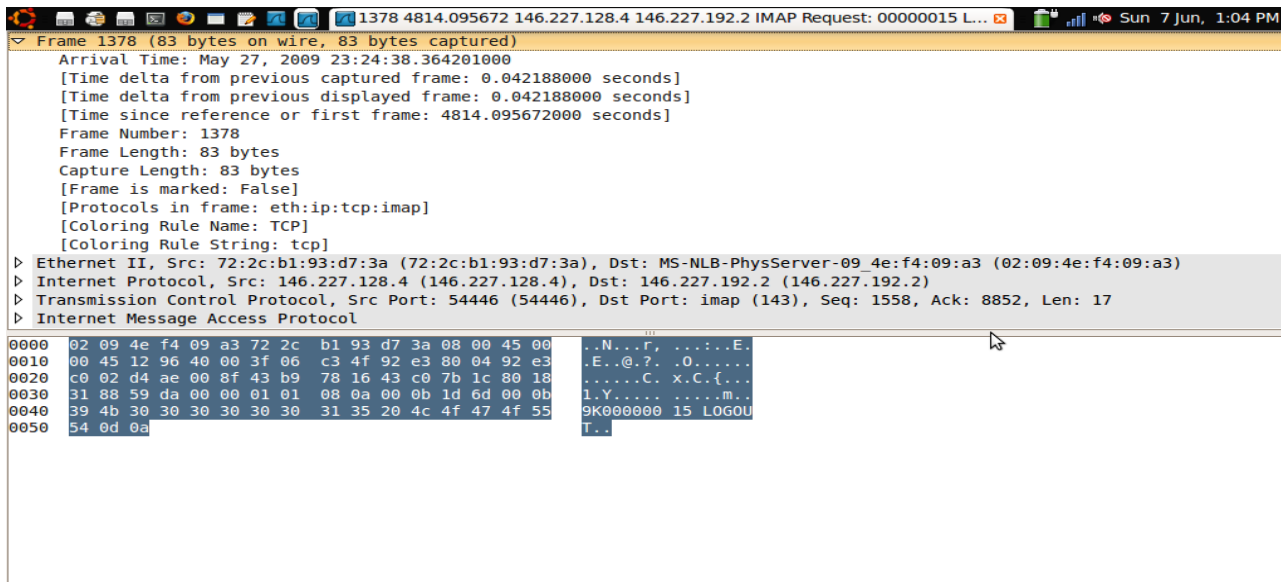


Figure 60: Examine insider’s logout activity

Login no3: After a few seconds, the insider logged into the mail server at 23:24:54

PM. The method of access is recognised as an AC because the login was successful.

Figure 61 shows that the insider was authenticated logging.

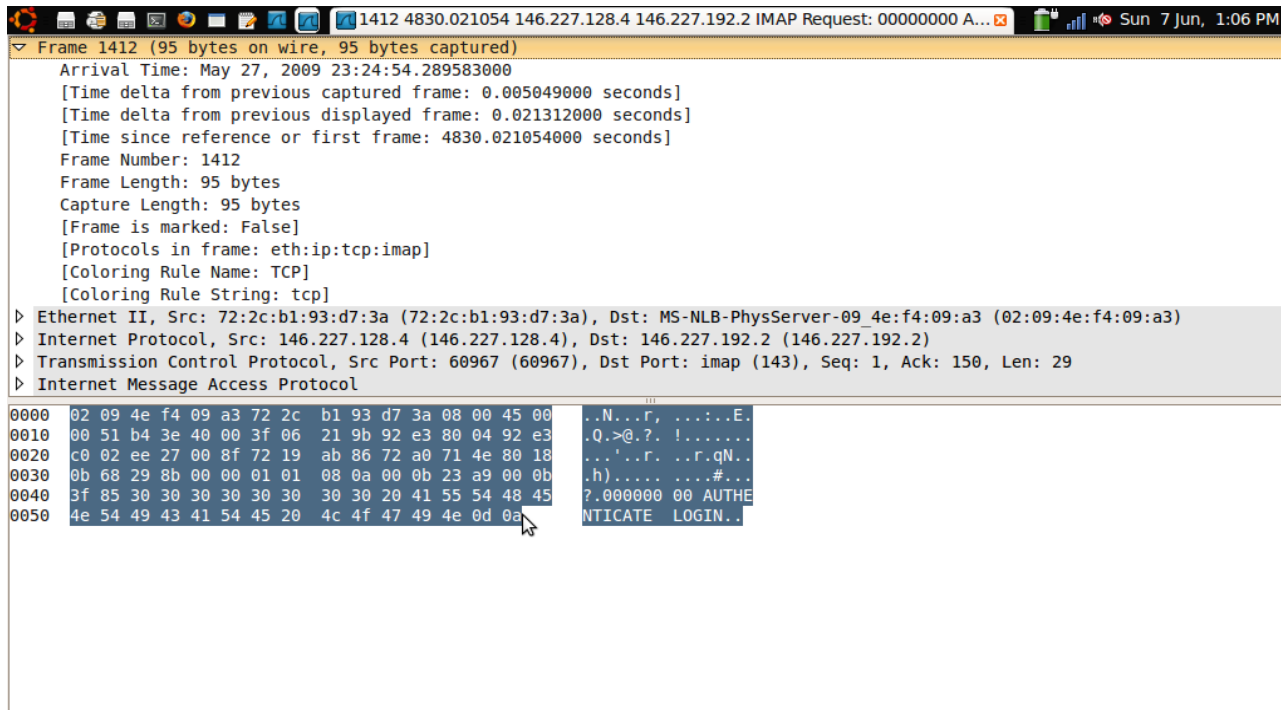


Figure 61: Examine insider’s login activity

Email no.9: The message had been sent from the manager to the insider. This is one of the series of exchange email between them. The manager replied to the insider by determining the time of meeting. There is a matching between the insider's job responsibilities and this email content. Therefore, the insider received the message and this message is recognised as a BE. The message was received at 23:25:15 and the content type of the message was text/plain.

Figure 62 shows that the message was received by the insider. The message content confirmed the meeting time.

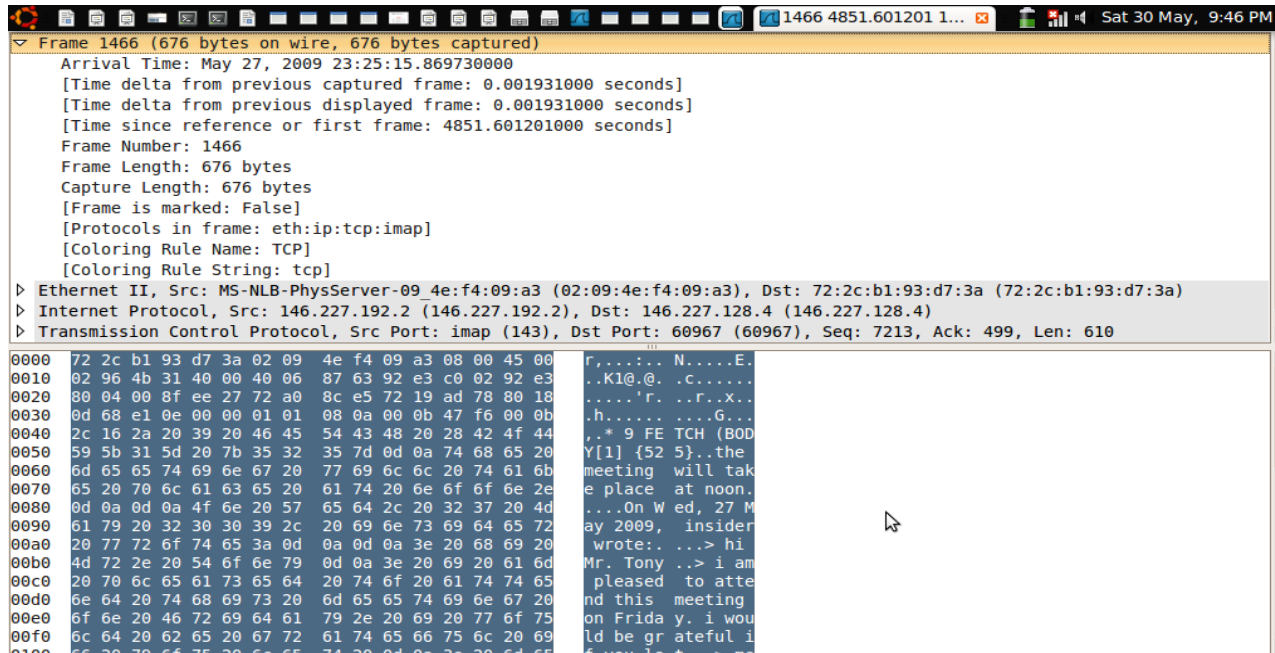


Figure 62: Examine insider's email activity

Email no.10: The message had been sent from the insider to the manager. The insider replied to his manager's Email no.9 and he thanked his manager for his reply. This is the last part of the exchanged messages between parties regarding the meeting. There is match between the insider's job responsibilities and the content of this message. Therefore, this email is classified as a BE. The email was sent at 23:25:53 and the content type of the message was text/plain.

Figure 63 shows that message contained the insider's reply to his manager's email.

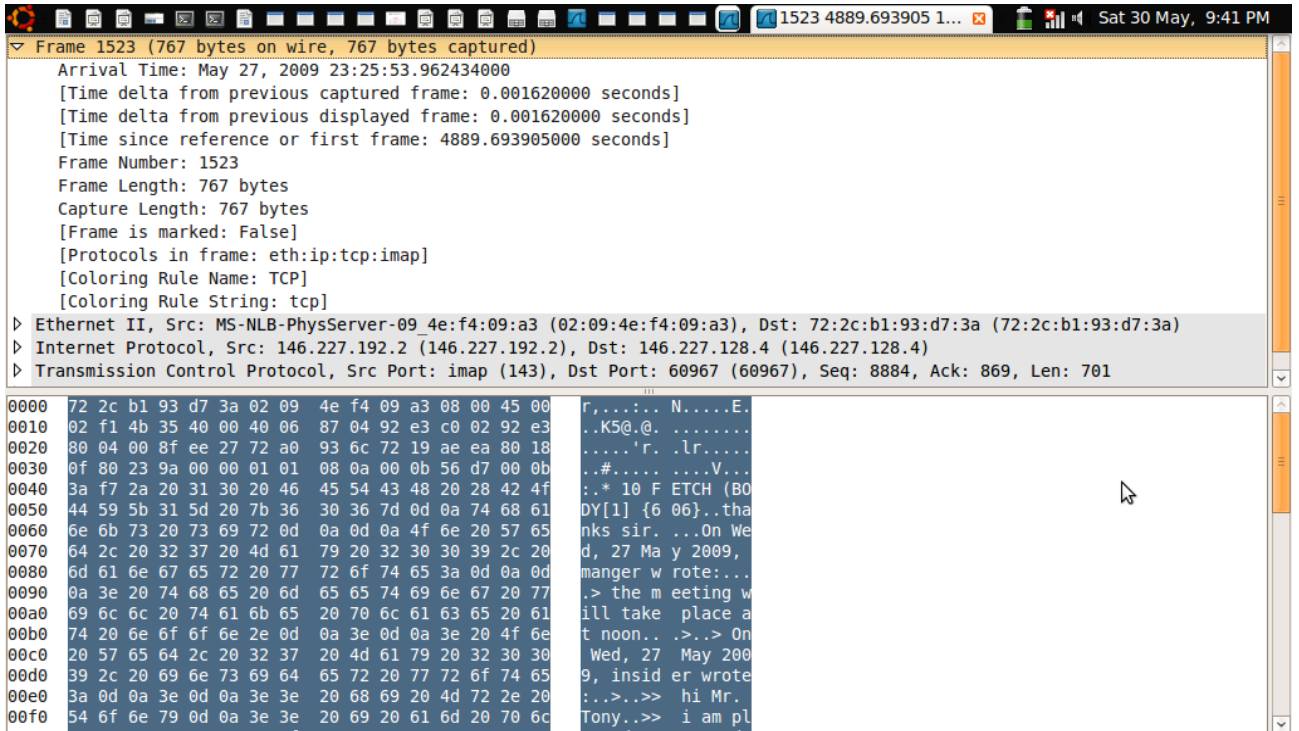


Figure 63: Examine insider’s email activity

Email no.11: The message was a replied email from the victim to the insider. This exchange message showed that the victim replied to the insider's reminder message by informing him that two car incidents had been reported. There is match between the insider's job responsibilities and the message content. Therefore, this email is classified as a BE. The email was received at 23:26:19 and the content type of the message was text/plain.

Figure 64 shows that the insider received a car incident report from the victim.

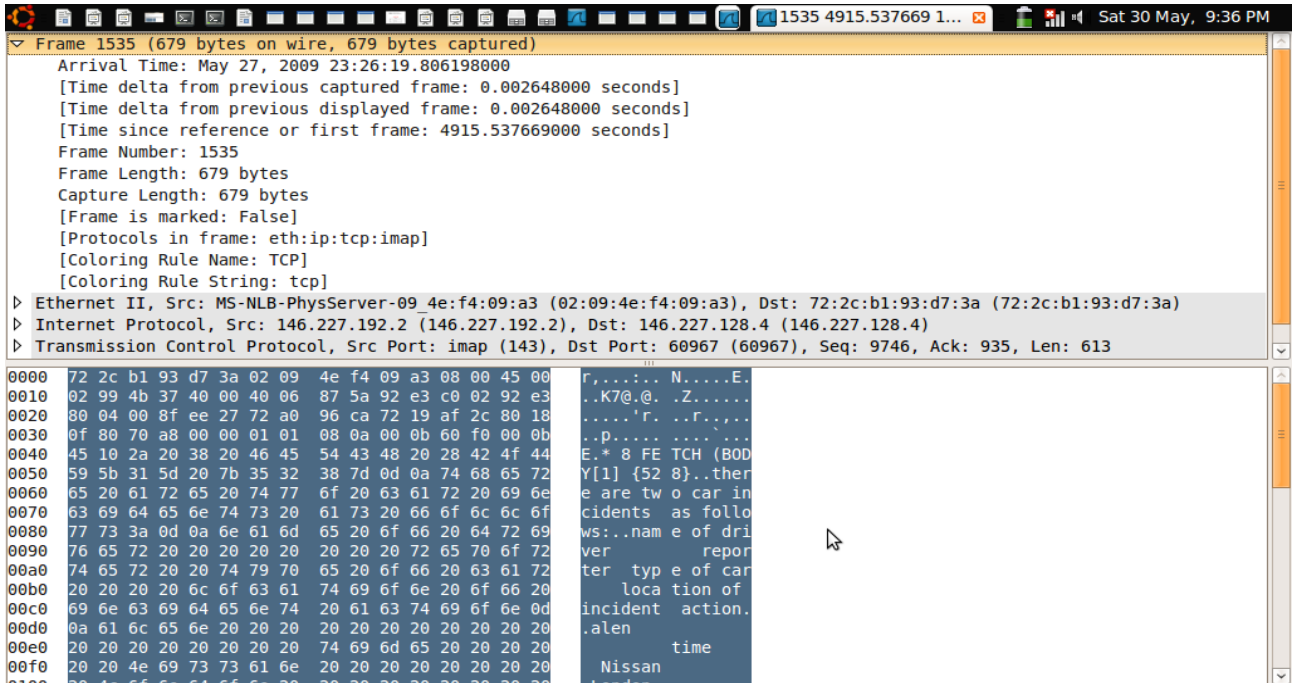


Figure 64: Examine insider’s email activity

Logout: after the insider received the car incident report from the victim, he logged out from the mail server at 23:27:36.

Login no.4: Eleven minutes after logging out, the insider logged into the mail server at 23:38:08. Therefore, the method of access is classified as an AC because the login was successful. Figure 65 shows that the insider was logging successfully.

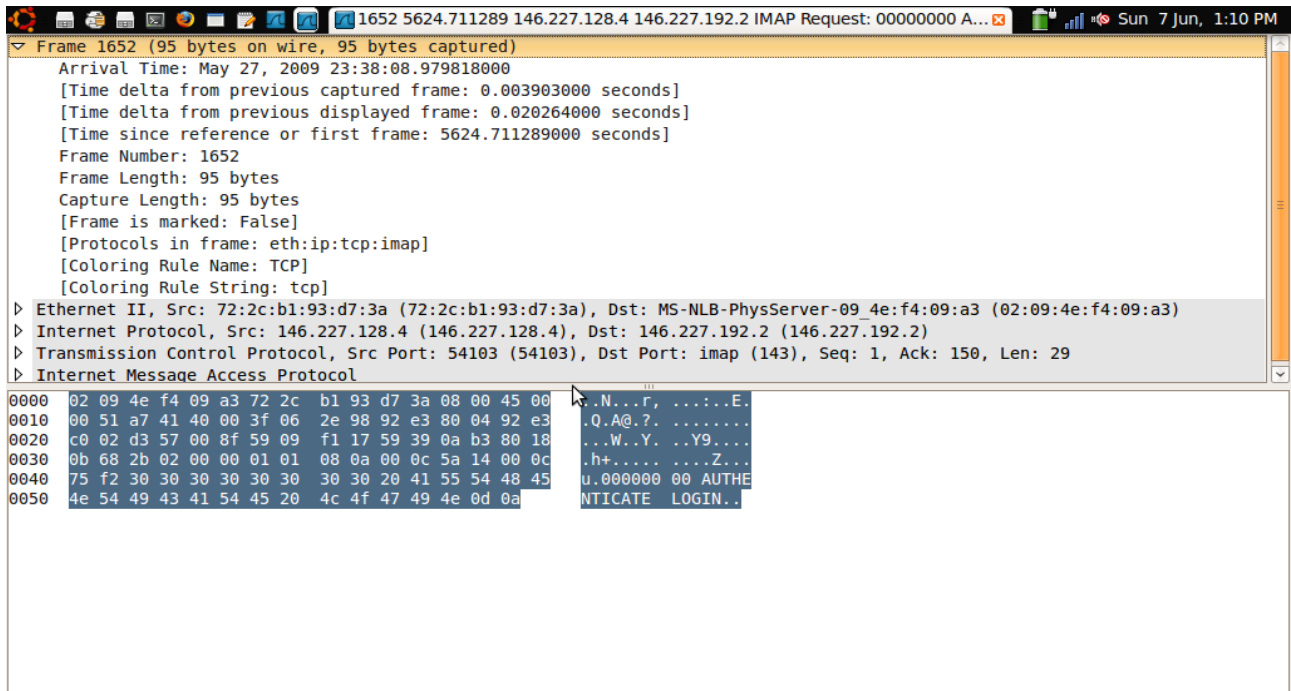


Figure 65: Examine insider's authentication login activity

Email no.12: The message had been sent from the group-leader to the insider. The group-leader informed the insider that two employees were injured. This email identified that the insider is also responsible for collecting injured employee reports. There is a match between the insider's job responsibilities and this message content. Therefore, this email is classified as a BE. This email was received at 23:39:03 and the content type of the message was text/plain. Figure 66 shows that the message was received by the insider contained an injury report.


```

1719 5715.345819 146.227.128.4 146.227.192.2 IMAP Request: 00000007 L...
Frame 1719 (83 bytes on wire, 83 bytes captured)
  Arrival Time: May 27, 2009 23:39:39.614348000
  [Time delta from previous captured frame: 0.038356000 seconds]
  [Time delta from previous displayed frame: 0.038356000 seconds]
  [Time since reference or first frame: 5715.345819000 seconds]
  Frame Number: 1719
  Frame Length: 83 bytes
  Capture Length: 83 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:imap]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  > Ethernet II, Src: 72:2c:b1:93:d7:3a (72:2c:b1:93:d7:3a), Dst: MS-NLB-PhysServer-09_4e:f4:09:a3 (02:09:4e:f4:09:a3)
  > Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
  > Transmission Control Protocol, Src Port: 54103 (54103), Dst Port: imap (143), Seq: 518, Ack: 9024, Len: 17
  > Internet Message Access Protocol
0000  02 09 4e f4 09 a3 72 2c b1 93 d7 3a 08 00 45 00  ..N...r, .....
0010  00 45 a7 53 40 00 3f 06 2e 92 92 e3 80 04 92 e3  .E.S@.?.....
0020  c0 02 d3 57 00 8f 59 09 f3 1c 59 39 2d 5d 80 18  ...W..Y. ..Y9-]..
0030  31 88 44 03 00 00 01 01 08 0a 00 0c 7d 79 00 0c  I.D.... ..y..
0040  99 58 30 30 30 30 30 30 30 37 20 4c 4f 47 4f 55  .X000000 07 LOGOU
0050  54 0d 0a  T..

```

Figure 67: Examine insider's logout activity

Login no.5: Sixteen minutes after logging out, the insider logged into the mail server at 23:55:45 PM. The access method is classified as an AC because the login was successful. Figure 68 shows that the insider was logging successfully.

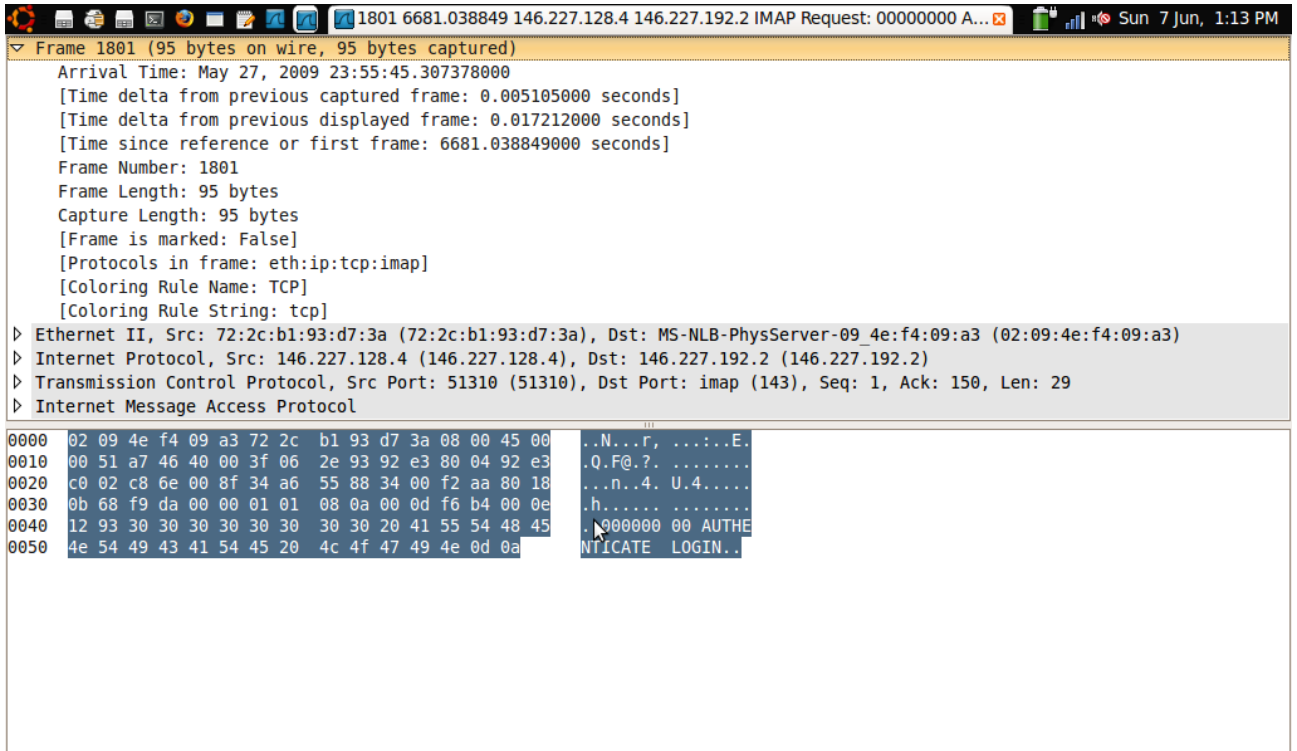


Figure 68: Examine insider's authentication activity

Email no.13: The message had been sent from the insider to the manager. The insider sent a morning report for car accidents to his manager. The analysis of this message showed that the insider is also responsible for sending a morning report to the manager. It also showed that after the insider collects the car accident report and injured report, he makes a report. Then the insider sent this report to his manager. This message also contains a morning report attachment. There is a match between the insider's job responsibilities and the content of the message. Therefore, this email is recognised as a BE.

Furthermore, the email was sent at 00:01:43 and the content type of the message was text/plain. Figure 69 shows that the insider sent a morning report to his manager and the message contained an attachment.

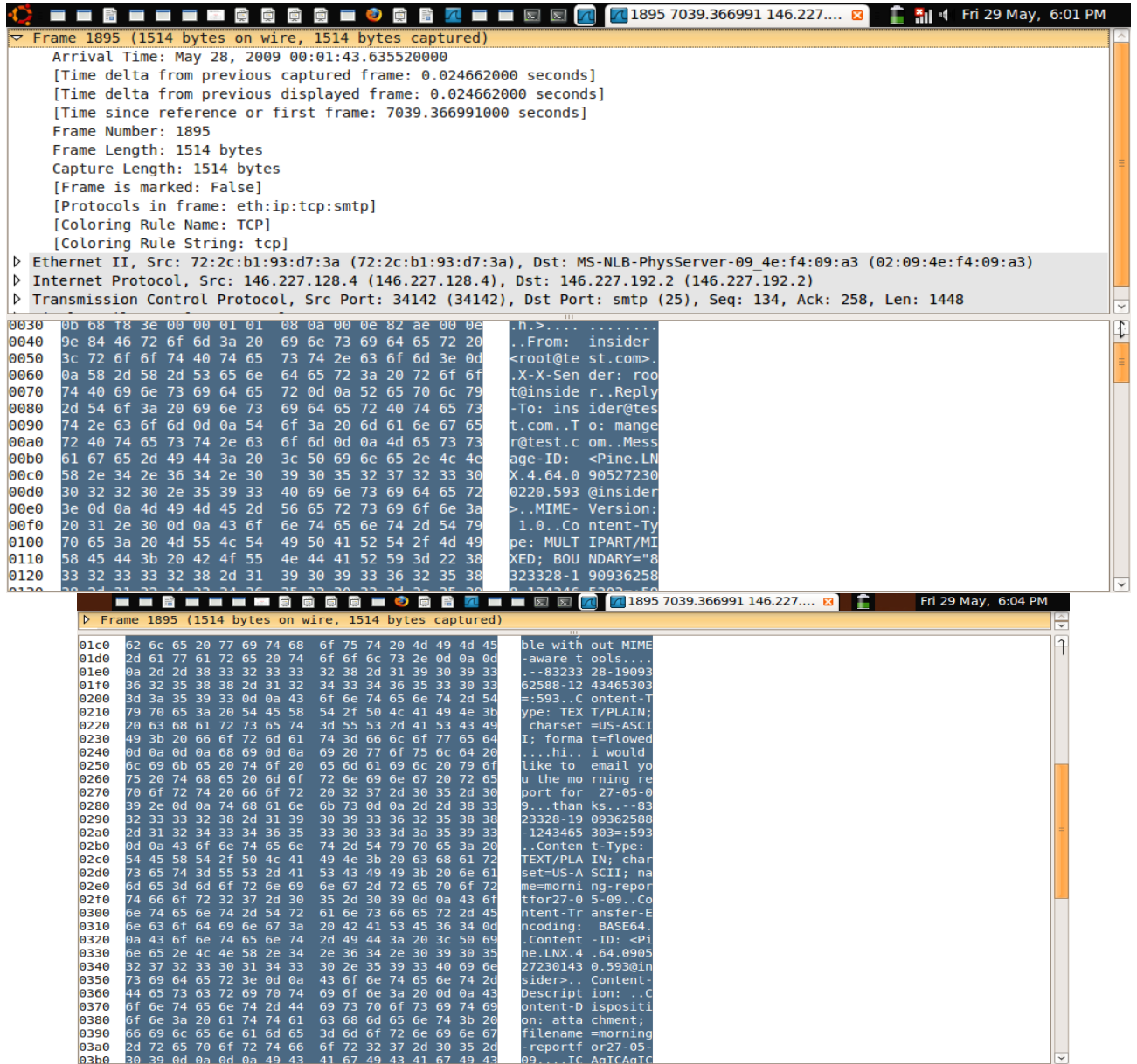


Figure 69: Examine insider's email activity

Logout: After the insider sent a morning report to his manager, he logged out from the mail server at 00:02:03. This activity was the last logout activity from the mail server for the insider. Figure 70 shows that the insider logged out from the server.

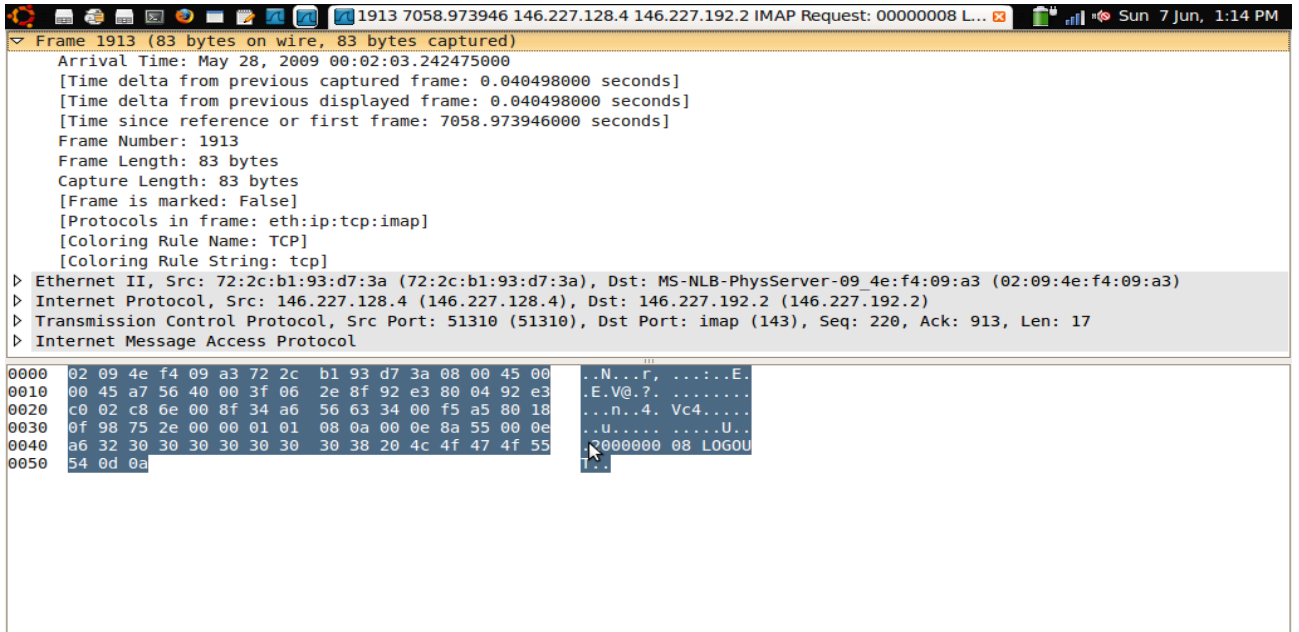


Figure 70: Examine insider’s logout activity

As a result of the email activity analysis, it was that the insider sent and received a number of business emails. These business emails contained the insider's job activities.

```

tiger@tiger-desktop: ~/Desktop
File Edit View Terminal Tabs Help
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$
tiger@tiger-desktop:~/Desktop$ cat insider

total 96
10753 drwxr-xr-x  3 guest guest 1024 2009-05-21 22:51 .
10858 drwxr-xr-x  2 root  root  1024 2009-05-21 22:50 mail
10856 -rw-----  1 root  root  1775 2009-05-21 10:58 .bash_history
10755 -r--r--r--  1 guest guest  698 2009-05-21 10:58 .bashrc
10754 -r--r--r--  1 root  root   140 2009-05-21 10:58 .profile
10857 -r-----  1 root  root 13667 2009-05-21 10:46 .pine-debug1
10860 -r--r--r--  1 root  root 17237 2009-05-21 10:46 .pinerc
10874 -r-----  1 root  root   877 2009-05-27 23:50 morning-report
10869 -r-----  1 root  root  2285 2009-05-21 03:39 .addressbook.lu
10861 -r-----  1 root  root 14011 2009-05-21 03:35 .pine-debug2
10863 -r-----  1 root  root  3642 2009-05-21 03:35 .viminfo
10865 -r-----  1 root  root 13908 2009-05-21 03:21 .pine-debug3
10872 -r-----  1 root  root   477 2009-05-27 23:45 injury-report
10862 -r-----  1 root  root 13264 2009-05-21 03:15 .pine-debug4
10873 -r-----  1 root  root   390 2009-05-27 23:30 car-incident-report
10871 -r-----  1 root  root  1038 2009-05-21 03:01 dead.letter
10868 -r--r--r--  1 root  root    0 2009-05-21 02:18 .addressbook
10864 -r-----  1 root  root    0 2009-05-27 23:03 security-incident-monthly-report
  2 drwxr-xr-x 26 guest guest 1024 2008-12-06 16:53 ..

./mail:
total 9
10858 drwxr-xr-x  2 root  root  1024 2009-05-27 22:51 .
10753 drwxr-xr-x  3 guest guest 1024 2009-05-27 22:51 ..
10859 -rw-r--r--  1 root  root  5037 2009-05-27 10:49 sent-mail
10867 -rw-----  1 root  root  1196 2009-05-27 03:42 postponed-msgs
tiger@tiger-desktop:~/Desktop$

```

Figure 71: Examine insider's computer analysis

▪ 4.File/Folder Timeline Activity Analysis:

OS system usually records the time of the very last action that was performed on a file/folder. This information is a valuable source of evidence which can assist to distinguish between insider and outsider attacks. Moreover, the system stores file timestamps to keep record of the file creation time, the last time the file was accessed and the last time the file was modified. Therefore, file/folder timeline analysis identifies the file creation time and the last time the file was modified on the insider computer. When timeline analysis identifies all insider's activity (email activity and file activity), it helps to identify the sequences of all activities. It found that the abusive email was sent among the insider's job responsibilities. After the insider's logged out from the mail server, he created some files and stored them in his computer. Figure 71 shows the sequences of all activities email, file, login and logout activities that were generated by the insider.

B1. Ex2:

The victim reported that an abusive email was received from insider@test.com. The email was received on September 8, 2009 at 22:29:24 . 136008000.

Preliminary investigation showed that this email was sent from the insider but the insider denied the allegation of sending an abusive email. Therefore, the first step was to collect legitimate and suspicious activity of the insider from the logs and from the insider's computer. Then these activities were examined in order to provide analysis process with insider's activities. The examination process provided the following information:

1. MA:

- **Email login:**

The login from the insider's computer was successfully authenticated on September 8, 2009 at 21:59:55. 854317000. It indicated that the attacker was successful in accessing the mail server. The following information is revealed from TCPDump:

Frame No. 355 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: IMAP Deception: User INSIDER AUTHENTICATED.

Figure 72 shows that the authenticated login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

```

355 3002.058453 146.227.128.4 146....x3 Sun 29 Nov, 5:08 AM
> Frame 355 (95 bytes on wire, 95 bytes captured)
> Ethernet II, Src: 72:2c:b1:93:d7:3a (72:2c:b1:93:d7:3a), Dst: MS-NLB-PhysServer-09_4e:f4:09:a3 (02:09:4e:f4:09:a3)
> Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
< Transmission Control Protocol, Src Port: 54973 (54973), Dst Port: imap (143), Seq: 1, Ack: 149, Len: 29
  Source port: 54973 (54973)
  Destination port: imap (143)
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 30 (relative sequence number)]
  Acknowledgement number: 149 (relative ack number)
  Header length: 32 bytes
  Flags: 0x18 (PSH, ACK)
  Window size: 5840 (scaled)
  Checksum: 0xd39c [correct]
  Options: (12 bytes)
  Internet Message Access Protocol

0000 02 09 4e f4 09 a3 72 2c b1 93 d7 3a 08 00 45 00  .N...r, .....E.
0010 00 51 a9 89 40 00 3f 06 2c 50 92 e3 80 04 92 e3  .Q..@.? ,P.....
0020 c0 02 d6 bd 00 8f 71 71 4d 61 71 51 bb 01 80 18  ....qq MaqQ...
0030 0b 68 d3 9c 00 00 01 01 08 0a 00 0d e8 d9 00 0d  .h.....
0040 fe 11 30 30 30 30 30 30 30 30 20 41 55 54 48 45  ..000000 00 AUTHE
0050 4e 54 49 43 41 54 45 20 4c 4f 47 49 4e 0d 0a  NTICATE LOGIN..

```

Figure 72: Authentication login activity

2.Email Activities:

The logs showed that there were a number of emails that were sent and received by the insider as described below:

Email No.1:

TCPDump revealed that the first email asked for the updated car incident report and received it from Bob. In this experiment, one of the main job responsibilities for the insider is collecting car incident reports. Therefore, these activities are indeed legitimate because there is a relationship between this email and the insider's job responsibilities (day-to-day organisational activities). This email was received by the insider on September 8, 2009 at 22:12:45. 717668000. The following summary information is revealed from TCPDump log:

Frame No. 60 Destination IP address: 146.227.128.4 Source IP address: 146.227.192.2 Protocol Type: IMAP Deception: BODY.

Figure 73 shows that the TCPDump information login is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

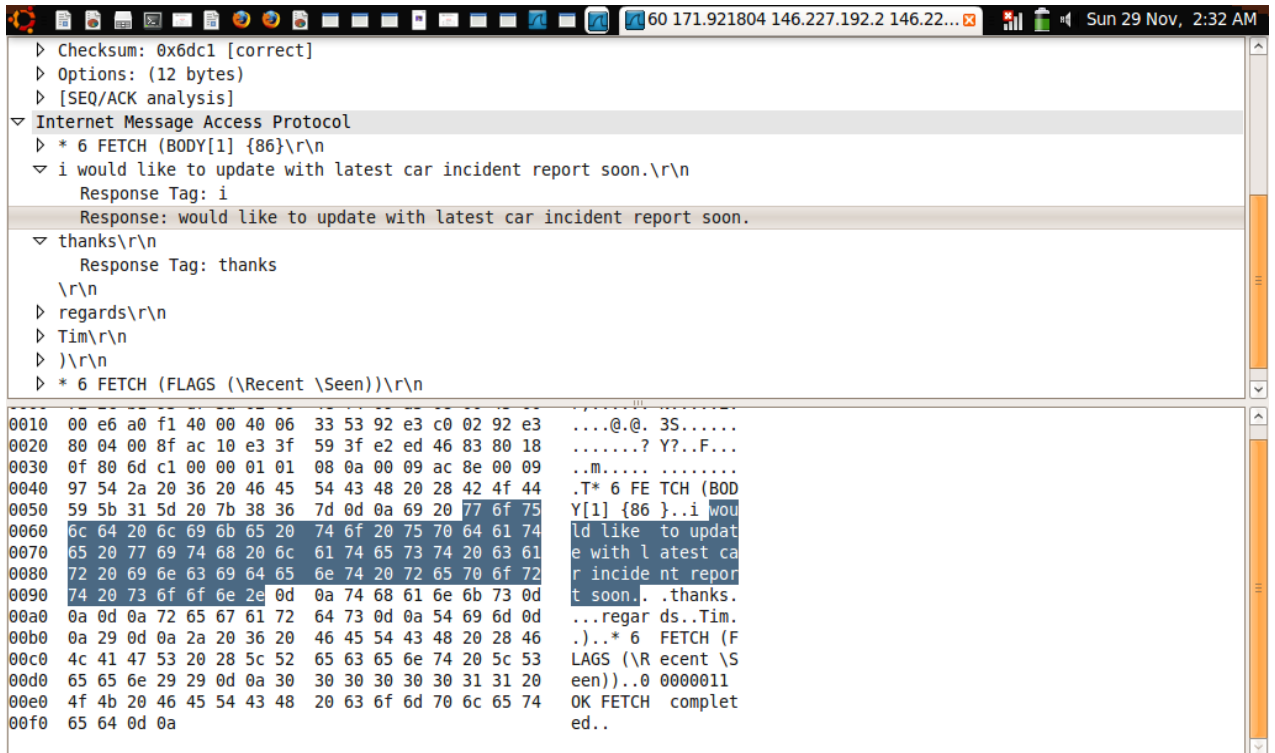


Figure 73: Examine insider’s email activity

Email No.2:

TCPDump revealed that the insider replied to the manager's email. This email was sent to the manager on September 8, 2009 at 22:14:14 . 064381000. The following summary information is revealed from TCPDump log:

Frame No. 99 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: SMTP Deception: DATA.

Figure 74 shows that the TCPDump information login is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

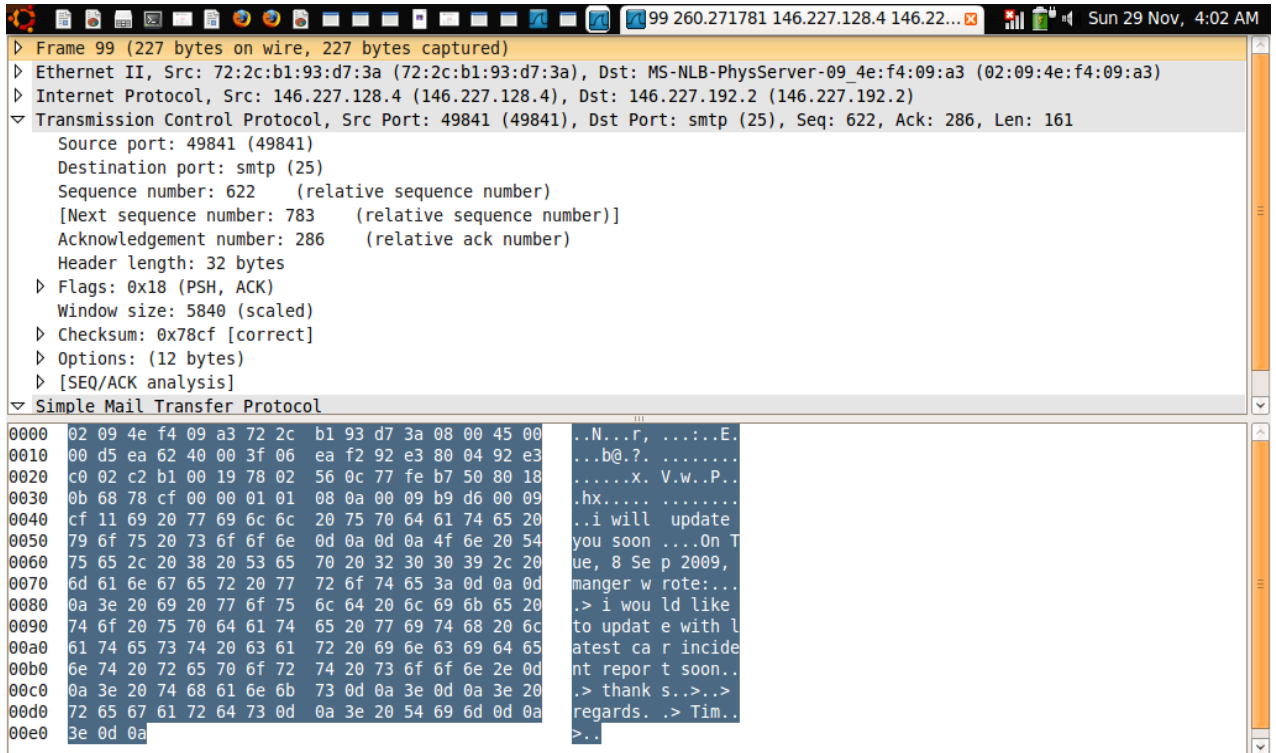


Figure 74: Examine insider’s email activity

Email No.3:

TCPDump revealed that the insider sent an email to the group-leader. The email's content was calling for a business meeting and it was sent on September 8, 2009 at 22:24:40. 136008000. As previously mentioned, one of the main job responsibilities for the insider is collecting and analysing car incident reports. Therefore, these activities are indeed legitimate because there is a relationship between this email and the insider's job responsibilities (day-to-day organisational activities). The following summary information is revealed from TCPDump log:

Frame No. 187 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: SMTP Deception: DATA.

Figure 75 shows that the TCPDump information email is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

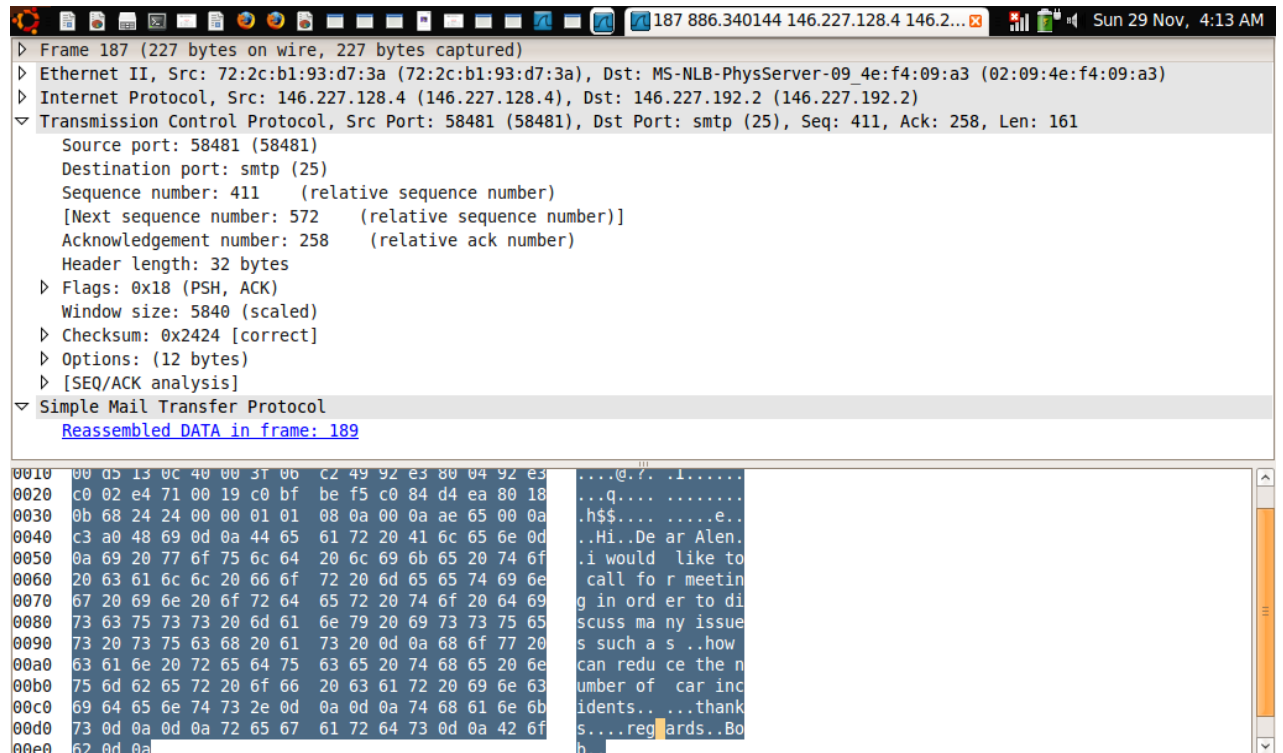


Figure 75: Examine insider's email activity

Email No.4:

TCPDump revealed that the insider sent an abusive email to the victim. This email was sent among insider job activities and it was sent on September 8, 2009 at 22:29:24 . 136008000. The following summary information is revealed from TCPDump log:

Frame No. 247 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: SMTP Deception: DATA.

Figure 76 shows that the TCPDump information email is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

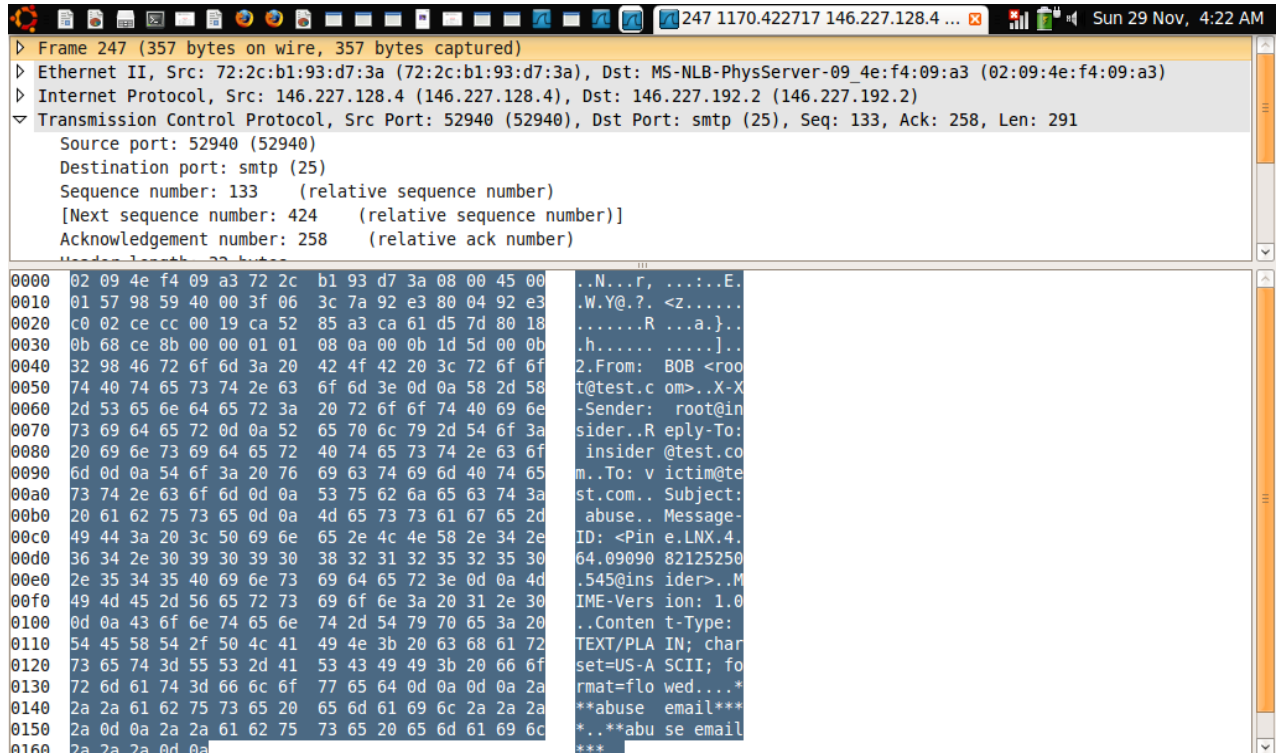


Figure 76: Examine abuse email

Email No. 5:

TCPDump revealed that the insider replied to the group-leader. This email contained an updated list of car incidents and it was sent on September 8, 2009 at 23:02:59 . 758933000. This activity is also indeed legitimate because there is a relationship between the content of the email and the insider's job responsibilities (day-to-day organisational activities). The following summary information is revealed from TCPDump log:

Frame No. 447 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: SMTP Deception: DATA.

Figure 77 shows that the TCPDump information email is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

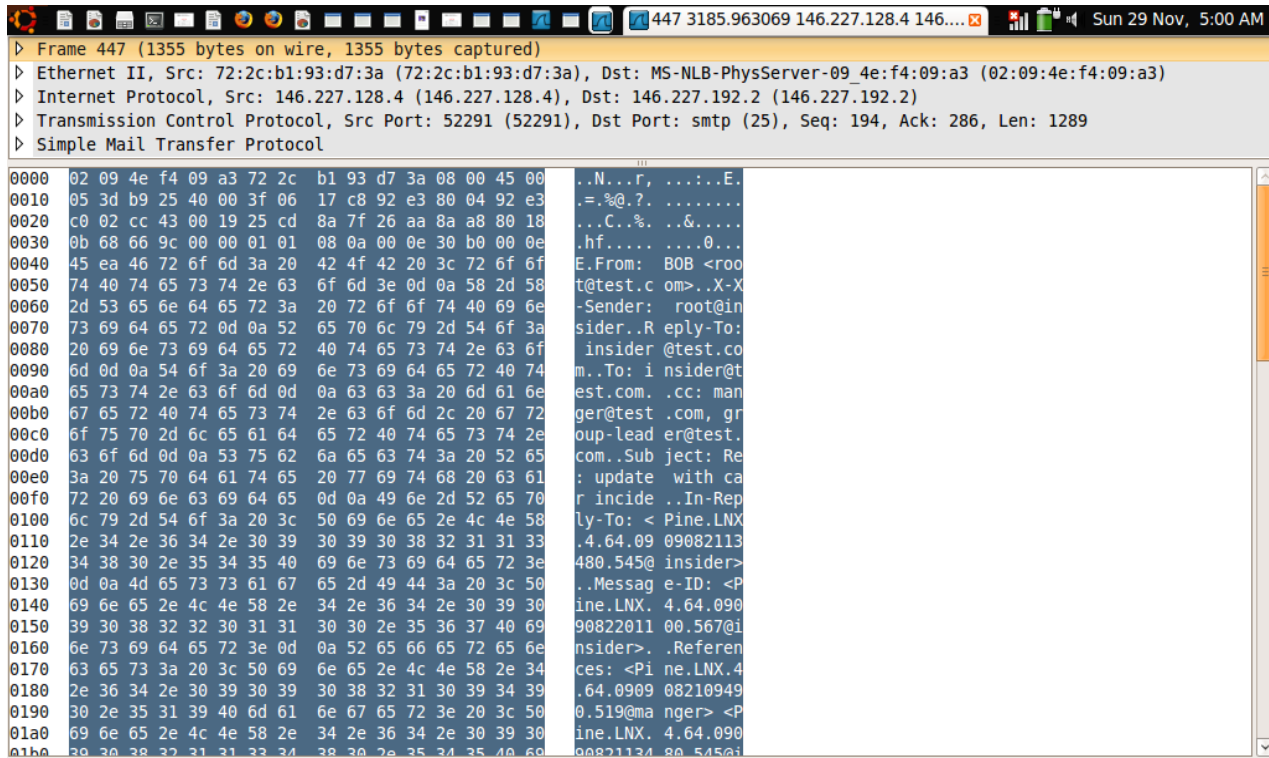


Figure 77: Examine insider's email activity

3.Examination of an insider's computer

By using ls -l command, it shows that there were two files. These files are car-incident and monthly-car incident. Car-incident file was last accessed on September 08, 2009 at 21:58. Monthly-car file was last accessed on September 08, 2009 at 22:17. These file activities are indeed legitimate because there is a relationship between these files and the insider's job responsibilities. Figure 78 shows the insider's computer activity.

```

insider
Configuring network interfaces...done.
Starting portmap daemon....
INIT: Entering runlevel: 2

--- Starting Netkit phase 1 init script ---
Mounting /home/tiger on /hosthome...
Mounting /home/tiger/test-1 on /hostlab ...
--- Netkit phase 1 initialization terminated ---

Starting system log daemon....
Starting kernel log daemon....

--- Starting Netkit phase 2 init script ---

>>> Running insider specific startup script...
>>> End of insider specific startup script.

#####

Lab directory (host): /home/tiger/test-1
Version: 1
Author: A. Al-Morjan
Email: almorjan@dmu.co.uk
Web: <none>
Description:
Configuration and operation of the First Experimental small network.

#####

--- Netkit phase 2 initialization terminated ---

insider login: root (automatic login)
Last login: Sat Nov 28 18:44:13 UTC 2009 on tty1
insider:~# ls -l
total 4
-rw-r--r-- 1 root root 0 2009-09-06 21:04 146,227,132.2
-----r-- 1 root root 621 2009-09-08 21:58 car-incident
-rw----- 1 root root 353 2009-10-03 17:31 dead.letter
dirmx-xr-x 2 root root 1024 2009-10-03 05:12 mail
-----r-- 1 root root 931 2009-09-08 22:17 monthly-car
insider:~#

```

Figure 78: Examine insider's computer activity

B1.Ex3:

The victim reported that an abusive email was received from insider@test.com. The email was received on December 3, 2009 at 20:42:43.527593000.

Preliminary investigation shows that this email was sent from the insider but the insider denied the allegation of sending an abusive email because he was out of his office. Therefore, the first step was to collect legitimate and suspicious activity for the insider from the logs and the insider's computer. Then these activities were examined in order to provide analysis process with insider's activities. The examination process provides the following information:

1.MA:

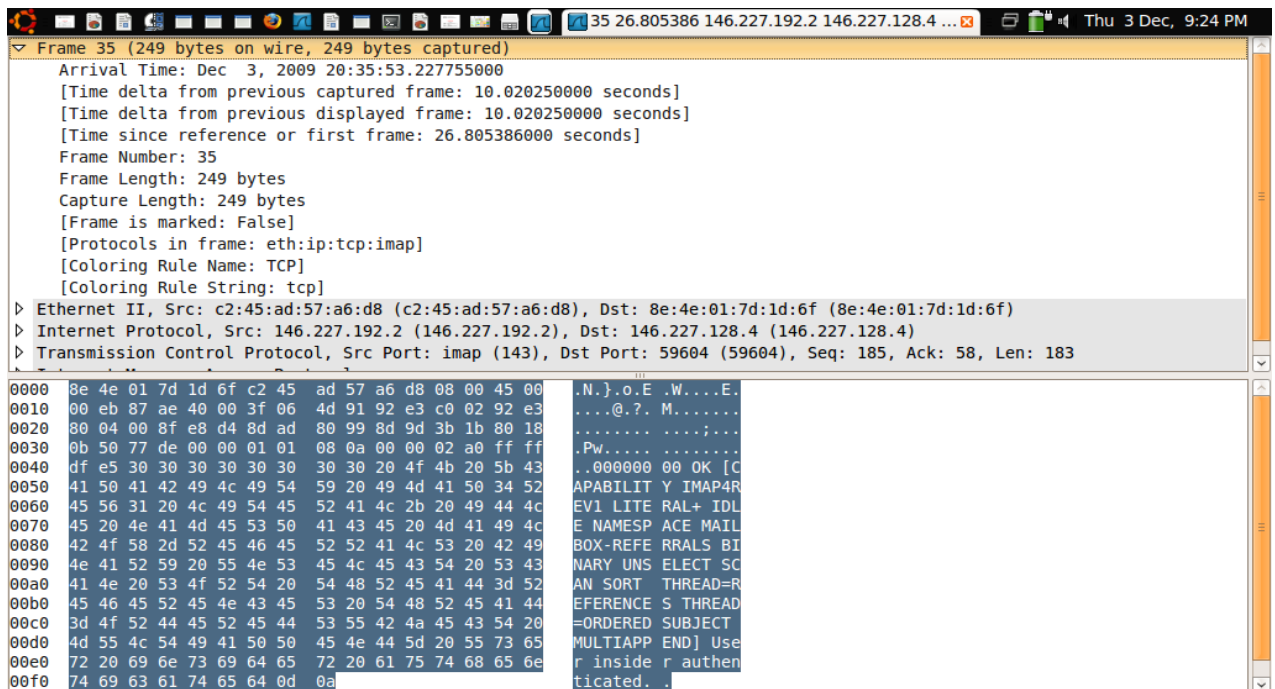
- **Login activities:**

The login from the insider's computer was successfully authenticated on the 3rd of December 2009 at 20:35:53.227755000. This login displays when an organisation's user

attempts to access the organisation's Mail server and the Mail server authentication system is able to recognize the user. It indicated that the attacker was success in accessing the mail server. The following information is revealed from TCPDump:

Frame No. 35 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** Response: 0000000 OK [CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY UNSELECT SCAN SORT THREAD=REFERENCES THREAD=ORDEREDSUBJECT MULTIAPPEND] **User** **INSIDER AUTHENTICATED.**

Figure 79 shows that the authenticated login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.



```

Frame 35 (249 bytes on wire, 249 bytes captured)
  Arrival Time: Dec  3, 2009 20:35:53.227755000
  [Time delta from previous captured frame: 10.020250000 seconds]
  [Time delta from previous displayed frame: 10.020250000 seconds]
  [Time since reference or first frame: 26.805386000 seconds]
  Frame Number: 35
  Frame Length: 249 bytes
  Capture Length: 249 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:imap]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  ▸ Ethernet II, Src: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8), Dst: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f)
  ▸ Internet Protocol, Src: 146.227.192.2 (146.227.192.2), Dst: 146.227.128.4 (146.227.128.4)
  ▸ Transmission Control Protocol, Src Port: imap (143), Dst Port: 59604 (59604), Seq: 185, Ack: 58, Len: 183

0000  8e 4e 01 7d 1d 6f c2 45  ad 57 a6 d8 08 00 45 00  .N.)o.E .W...E.
0010  00 eb 87 ae 40 00 3f 06  4d 91 92 e3 c0 02 92 e3  ....@.?. M.....
0020  80 04 00 8f e8 d4 8d ad  80 99 8d 9d 3b 1b 80 18  .....;...
0030  0b 50 77 de 00 00 01 01  08 0a 00 00 02 a0 ff ff  .Pw.....
0040  df e5 30 30 30 30 30 30  30 30 20 4f 4b 20 5b 43  ..000000 00 OK [C
0050  41 50 41 42 49 4c 49 54  59 20 49 4d 41 50 34 52  APABILIT Y IMAP4R
0060  45 56 31 20 4c 49 54 45  52 41 4c 2b 20 49 44 4c  EV1 LITE RAL+ IDL
0070  45 20 4e 41 4d 45 53 50  41 43 45 20 4d 41 49 4c  E NAMESPACE MAIL
0080  42 4f 58 2d 52 45 46 45  52 52 41 4c 53 20 42 49  BOX-REFE RRALS BI
0090  4e 41 52 59 20 55 4e 53  45 4c 45 43 54 20 53 43  NARY UNS ELECT SC
00a0  41 4e 20 53 4f 52 54 20  54 48 52 45 41 44 3d 52  AN SORT  THREAD=R
00b0  45 46 45 52 45 4e 43 45  53 20 54 48 52 45 41 44  EFERERE S THREAD
00c0  3d 4f 52 44 45 52 45 44  53 55 42 4a 45 43 54 20  =ORDERED SUBJECT
00d0  4d 55 4c 54 49 41 50 50  45 4e 44 5d 20 55 73 65  MULTIAPP END] Use
00e0  72 20 69 6e 73 69 64 65  72 20 61 75 74 68 65 6e  r inside r authen
00f0  74 69 63 61 74 65 64 0d  0a  ticated.

```

Figure 79: Examine authentication login

2.Email Activity:

Email.1:

1- TCPDump revealed that the first email was sent to abdulrazaq@kaust.com and contained safety awareness program for employees in order to reduce the number of car incidents. This email was sent by the insider on December 3, 2009 at 20:38:27.840514000. The following summary information is revealed from TCPDump log:

Frame No. 62 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4
Protocol Type: SMTP **Deception:** **RCPT**
TO: <abdulrazaq@kaust.com>.

Figure 80 shows the activity of attempting send an email outside the organisation.

```

Frame 62 (98 bytes on wire, 98 bytes captured)
  Arrival Time: Dec 3, 2009 20:38:27.840514000
    [Time delta from previous captured frame: 0.001863000 seconds]
    [Time delta from previous displayed frame: 0.001863000 seconds]
    [Time since reference or first frame: 181.418145000 seconds]
  Frame Number: 62
  Frame Length: 98 bytes
  Capture Length: 98 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:smtp]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  > Ethernet II, Src: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f), Dst: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8)
  > Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.128.2 (146.227.128.2)
  > Transmission Control Protocol, Src Port: 58802 (58802), Dst Port: smtp (25), Seq: 56, Ack: 188, Len: 32
  > Simple Mail Transfer Protocol
    0000  c2 45 ad 57 a6 d8 8e 4e 01 7d 1d 6f 08 00 45 00  .E.W...N...}.o..E...
    0010  00 54 ff 87 40 00 40 06 d5 4e 92 e3 80 04 92 e3  .T.@.@. .N.....
    0020  c0 02 e5 b2 00 19 36 ec df e6 37 fa e5 07 80 18  ....6. .7.....
    0030  0b 68 d5 68 00 00 01 01 08 0a 00 00 20 3a 00 00  .h.h.....:..
    0040  3f 05 52 43 50 54 20 54 4f 3a 3c 61 62 64 75 6c  ?.RCPT T O:<abdul
    0050  72 61 7a 61 71 40 6b 61 75 73 74 2e 63 6f 6d 3e  razaq@ka ust.com>
    0060  0d 0a  ..
  
```

Figure 80: Examine email activity

The mail server did not know how to reach kaust.com domain. The following summary information is revealed from TCPDump log:

Frame No. 63 Destination IP address: 146.227.128.4 **Source IP address:** 146.227.192.2
Protocol Type: SMTP **Deception:** **550 relay not permitted.**

Figure 81 shows that the authenticated login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

```

63 181.443999 146.227.192.2 146.227.128.... Thu 3 Dec, 9:54 PM
Frame 63 (91 bytes on wire, 91 bytes captured)
  Arrival Time: Dec 3, 2009 20:38:27.866368000
  [Time delta from previous captured frame: 0.025854000 seconds]
  [Time delta from previous displayed frame: 0.025854000 seconds]
  [Time since reference or first frame: 181.443999000 seconds]
  Frame Number: 63
  Frame Length: 91 bytes
  Capture Length: 91 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:smtp]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  > Ethernet II, Src: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8), Dst: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f)
  > Internet Protocol, Src: 146.227.192.2 (146.227.192.2), Dst: 146.227.128.4 (146.227.128.4)
  > Transmission Control Protocol, Src Port: smtp (25), Dst Port: 58802 (58802), Seq: 188, Ack: 88, Len: 25
  > Simple Mail Transfer Protocol

0000  8e 4e 01 7d 1d 6f c2 45 ad 57 a6 d8 08 00 45 00  .N}.o.E .W...E.
0010  00 4d da b5 40 00 3f 06 fb 27 92 e3 c0 02 92 e3  .M.@.?.'.....
0020  80 04 00 19 e5 b2 37 fa e5 07 36 ec e0 06 80 18  .....7. .6....
0030  0b 50 bd f4 00 00 01 01 08 0a 00 00 3f 08 00 00  .P.....?...
0040  20 3a 35 35 30 20 72 65 6c 61 79 20 6e 6f 74 20  :550 re lay not
0050  70 65 72 6d 69 74 74 65 64 0d 0a                permitte d..

```

Figure 81 : Examine email activity

2- TCPDump revealed that there was another attempt to send email to abdulrazaq@kaust.com. The insider attempted to send this email on December 3, 2009 at 20:38:37.952632000. The following summary information is revealed from TCPDump log:

Frame No. 96 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4
Protocol Type: SMTP **Deception:** **RCPT**
TO: <abdulrazaq@kaust.com>.

Figure 82 shows the email header address.


```

Thu 3 Dec, 10:14 PM
▼ Frame 96 (98 bytes on wire, 98 bytes captured)
  Arrival Time: Dec 3, 2009 20:38:37.952632000
  [Time delta from previous captured frame: 0.004602000 seconds]
  [Time delta from previous displayed frame: 0.004602000 seconds]
  [Time since reference or first frame: 191.530263000 seconds]
  Frame Number: 96
  Frame Length: 98 bytes
  Capture Length: 98 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:smtp]
  ▶ Ethernet II, Src: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f), Dst: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8)
  ▶ Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
  ▶ Transmission Control Protocol, Src Port: 58803 (58803), Dst Port: smtp (25), Seq: 56, Ack: 188, Len: 32
  ▶ Simple Mail Transfer Protocol

0000  c2 45 ad 57 a6 d8 8e 4e 01 7d 1d 6f 08 00 45 00  .E.W...N }.o..E.
0010  00 54 f9 dc 40 00 40 06 da f9 92 e3 80 04 92 e3  .T..@.@. ....
0020  c0 02 e5 b3 00 19 40 ed de 01 40 e2 1c 01 80 18  .....@. ..@....
0030  0b 68 85 89 00 00 01 01 08 0a 00 00 24 2b 00 00  .h.....$+..
0040  42 f5 52 43 50 54 20 54 4f 3a 3c 61 62 64 75 6c  B.RCPT T 0:<abdu
0050  72 61 7a 61 71 40 6b 61 75 73 74 2e 63 6f 6d 3e  razaq@ka ust.com>
0060  0d 0a  ..

```

Figure 82: Examine email activity

The mail server did not know how to reach kaust.com domain. The following summary information is revealed from TCPDump log:

Frame No. 97 Destination IP address: 146.227.128.4 **Source IP address:** 146.227.192.2 **Protocol Type:** SMTP **Deception:** **550 relay not permitted.**

Email.2:

TCPDump revealed that there was another attempt to send email to Ali@kaust.com. The insider attempted to send this email on December 3, 2009 at 20:39:04.543178000.

The following summary information is revealed from TCPDump log:

Frame No. 125 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4 **Protocol Type:** SMTP **Deception:** **RCPT TO:<Ali@kaust.com>.**

Figure 83 shows that the authenticated login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events. It shows the attempt of sending a second email outside the organisation.

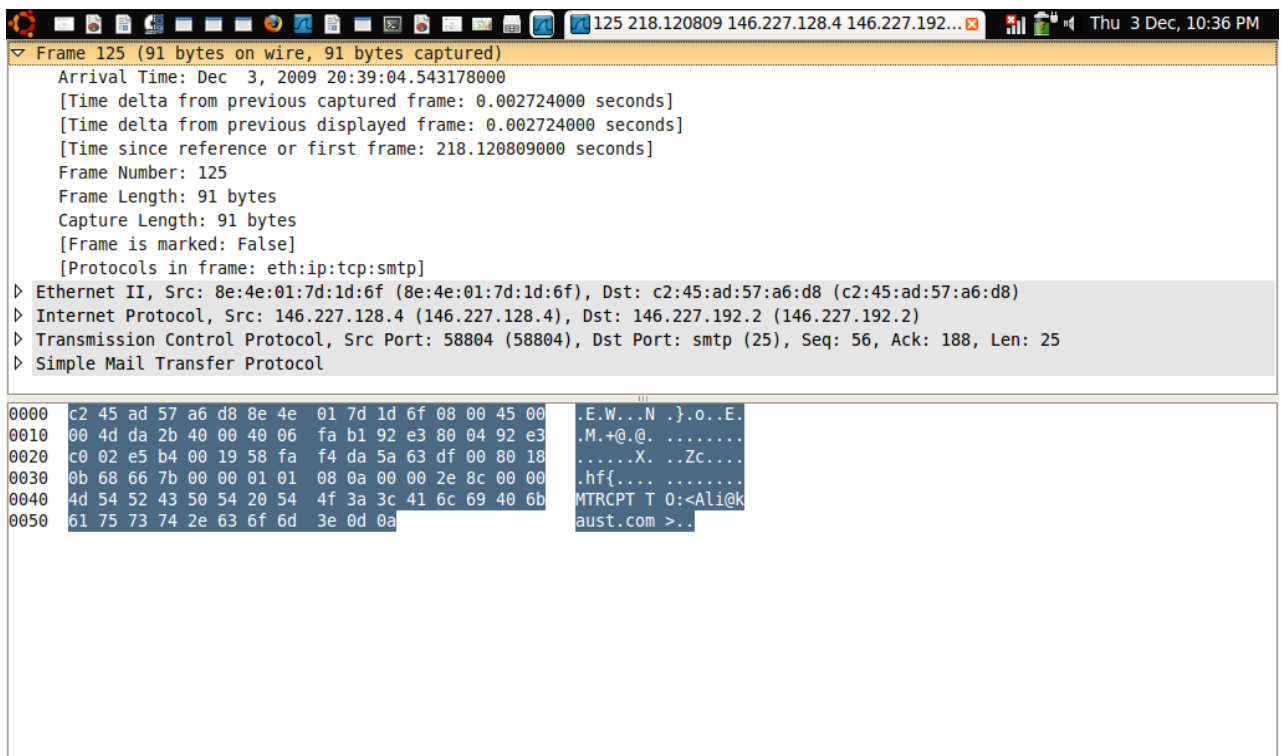


Figure 83: Examine email activity

The mail server did not know how to reach kaust.com domain. The following summary information is revealed from TCPDump log:

Frame No. 126 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** SMTP **Deception:** **550 relay not permitted.**

Email.3:

TCPDump revealed that there was one abusive email that was forwarded to the victim on the 3rd of December 2009 at 20:42:43.527593000. The following summary information is revealed from TCPDump log:

Frame No. 201 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMF **Deception:** **Malformed Packet.**

Figure 84 shows that the TCPDump information login is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

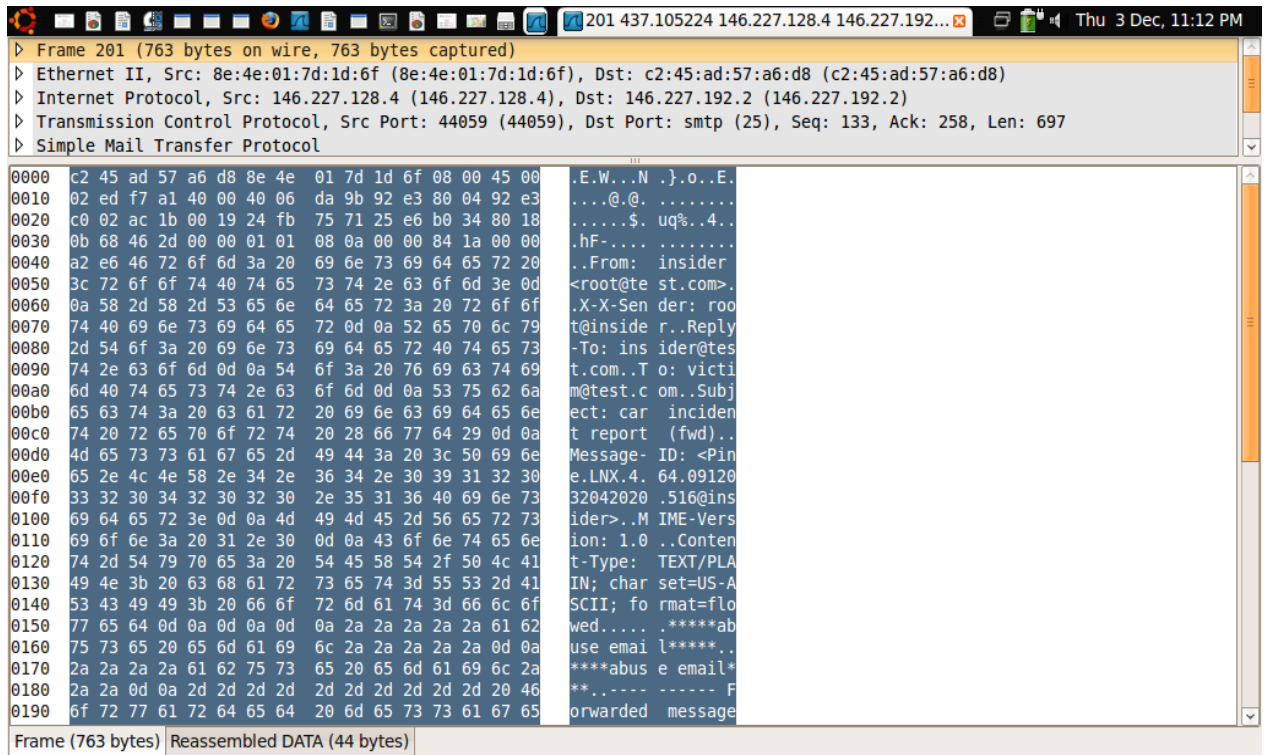


Figure 84: Examine abusive email

3.Examination and analysis of the insider's PC

After completing the examination of email activities, the next step is to examine the insider's computer. Firstly, the security corporate searched for any BF had been created or modified. This was done by using “ls -l” command; this command showed that there was NBF. Figure 85 shows that there was NBF in the insider's computer.

```

Loading kernel modules...done.
Setting kernel variables (/etc/sysctl.conf)...done.
Setting up networking...
Configuring network interfaces...done.
Starting portap daemon...
INIT: Entering runlevel: 2

--- Starting Netkit phase 1 init script ---
Mounting /home/tiger on /home...
Mounting /home/tiger/test-7 on /hostlab ...
--- Netkit phase 1 initialization terminated ---

Starting system log daemon...
Starting kernel log daemon...

--- Starting Netkit phase 2 init script ---

>>> Running insider specific startup script...
>>> End of insider specific startup script.

*****

Lab directory (host): /home/tiger/test-7
Version: 1
Author: A. Al-Morjan
Email: almorjan@dmu.co.uk
Web: <none>
Description:
Configuration and operation of sending an abusive email by using insider computer the sixth Experiment

*****

--- Netkit phase 2 initialization terminated ---

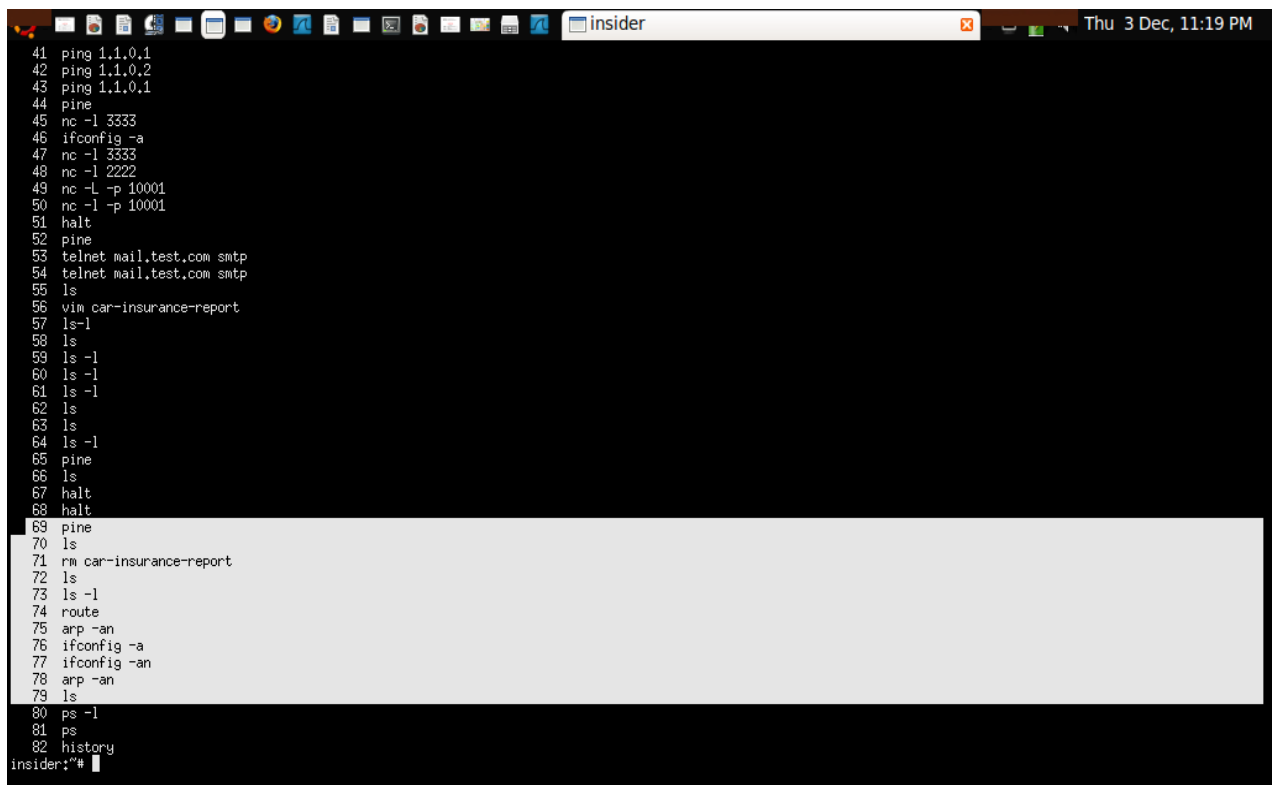
insider login: root (automatic login)
Last login: Thu Dec 3 20:32:27 UTC 2009 on tty1
insider:~# ls -l
total 2
-rw-r----- 1 root root 841 2009-12-03 20:41 dead.letter
drwxr-xr-x 2 root root 1024 2009-12-03 20:42 mail
insider:~#

```

Figure 85: Examine insider's computer activity

Then the corporate security examined if there was any suspicious activities on this computer. This was done by using “history” command. This command revealed a number of suspicious commands as follows: ls, rm, route, arp-an and ifconfig.

The last three commands (route, arp -an and ifconfig -a) are usually used to collect technical information about network infrastructure. Figure 86 shows that history list of commands that are used by the attacker to collect valuable information about the network.



```
41 ping 1.1.0.1
42 ping 1.1.0.2
43 ping 1.1.0.1
44 pine
45 nc -l 3333
46 ifconfig -a
47 nc -l 3333
48 nc -l 2222
49 nc -L -p 10001
50 nc -l -p 10001
51 halt
52 pine
53 telnet mail.test.com smtp
54 telnet mail.test.com smtp
55 ls
56 vim car-insurance-report
57 ls-l
58 ls
59 ls -l
60 ls -l
61 ls -l
62 ls
63 ls
64 ls -l
65 pine
66 ls
67 halt
68 halt
69 pine
70 ls
71 rm car-insurance-report
72 ls
73 ls -l
74 route
75 arp -an
76 ifconfig -a
77 ifconfig -an
78 arp -an
79 ls
80 ps -l
81 ps
82 history
insider: #
```

Figure 86: Examine insider's computer activity

B1. Ex4:

Preliminary investigation shows that Tim's account is a personal account and Tim is not working for Test Company. Therefore, the first step was to review fw-1 (firewall) log. When reviewing the log, it appeared that there was no connection between the mail server and another computer. This led us to examine the mail envelope header of the abusive message in order to identify the source IP address of the email envelope. The envelope header is usually hidden when an email is viewed, and the message header is usually visible. It contains information that is essential to email delivery. The envelope header of the abusive message showed that the source IP address was 146.227.128.4. When reviewing the header, it revealed two suspicious issues as follows:

mail server (IP address 146.227.192.2 and port # 25). This information indicated that this attack initiated from inside the company. Figure 88 shows the firewall activity logs.

```

Nov 30 03:16:18 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=56409 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 03:17:59 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=98 TOS=0x10 PREC=0x00 TTL=63 ID=56410 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:18:29 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=81 TOS=0x10 PREC=0x00 TTL=63 ID=56411 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:18:48 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=78 TOS=0x10 PREC=0x00 TTL=63 ID=56412 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:19:29 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=79 TOS=0x10 PREC=0x00 TTL=63 ID=56413 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:19:45 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=73 TOS=0x10 PREC=0x00 TTL=63 ID=56414 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:20:04 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=74 TOS=0x10 PREC=0x00 TTL=63 ID=56415 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:20:55 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=107 TOS=0x10 PREC=0x00 TTL=63 ID=56416 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:21:06 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=71 TOS=0x10 PREC=0x00 TTL=63 ID=56417 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:21:53 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=111 TOS=0x10 PREC=0x00 TTL=63 ID=56418 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:21:54 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=54 TOS=0x10 PREC=0x00 TTL=63 ID=56419 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:06 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=99 TOS=0x10 PREC=0x00 TTL=63 ID=56420 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:14 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=87 TOS=0x10 PREC=0x00 TTL=63 ID=56421 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:18 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=98 TOS=0x10 PREC=0x00 TTL=63 ID=56422 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:22 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=83 TOS=0x10 PREC=0x00 TTL=63 ID=56423 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:25 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=57 TOS=0x10 PREC=0x00 TTL=63 ID=56424 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:27 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=55 TOS=0x10 PREC=0x00 TTL=63 ID=56425 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 03:22:27 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=56426 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 03:22:32 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=58 TOS=0x10 PREC=0x00 TTL=63 ID=56427 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 03:22:32 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=56428 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 03:22:32 fw-2 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=146,227,128,4 DST=146,227,192,2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=56429 DF PROTO=TCP SPT=44201 DPT=25 WINDOW=2920 RES=0x00 ACK FIN URG=0
fw-2:~#

```

Figure 88: Firewall activity log

The next step was to examine the insider's activities from the TCPdump log and it revealed the following activities:

1. MA:

- **Login activities**

There was one login activity to the Mail server from the insider's computer. The login from the insider's computer was authenticated on November 30, 2009 at 03:09:18.338867000. The Mail server authentication system is able to recognize the insider. The following information is revealed from TCPDump:

Frame No. 35 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: IMAP Deception: USER INSIDER THENTICATED.

Figure 89 shows that the login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

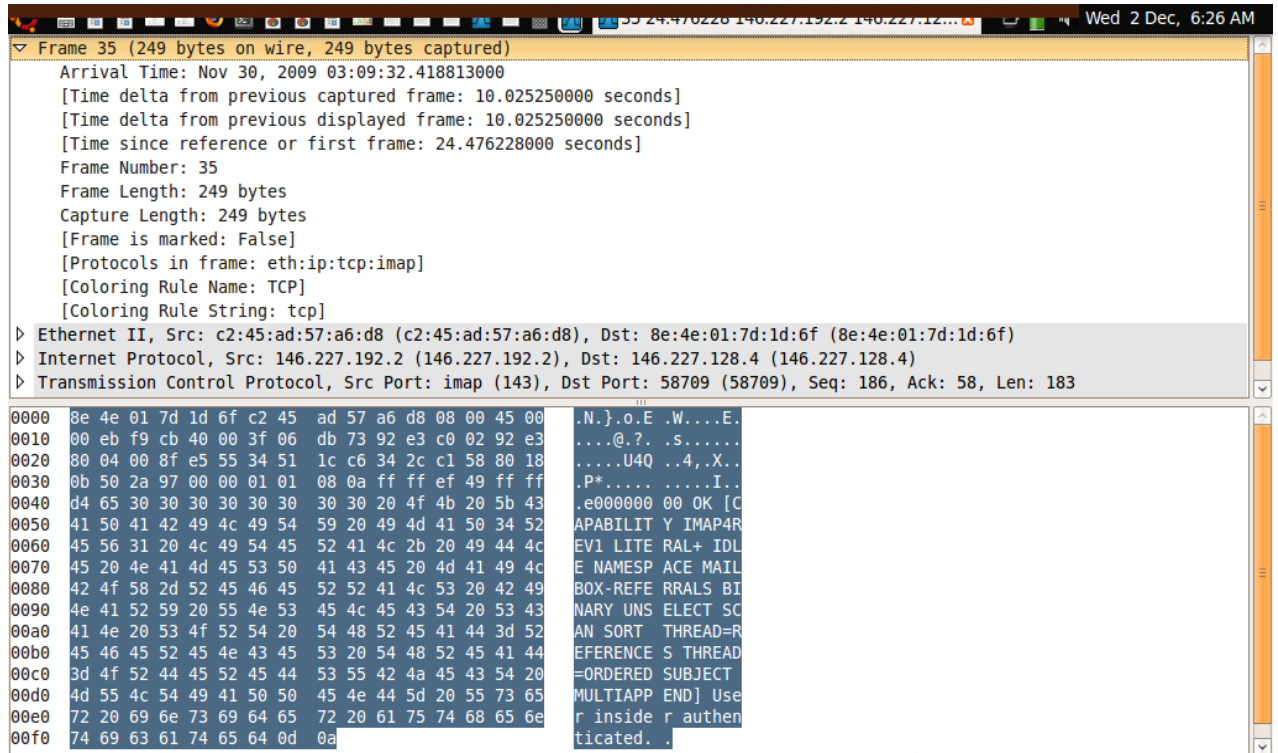


Figure 89: Insider’s authentication login activity

2.Email Activities:

The logs showed that there were a number of emails that were sent and received by the insider as described below:

Email No.1:

TCPDump revealed that the first email was sent to the group-leader and contained safety awareness program for employees in order to reduce the number of car incidents. Another primary job responsibility for the insider is managing safety awareness. Therefore, this email is indeed legitimate because there is a relationship between this email and the insider's job responsibilities. This email was sent by the insider on November 30, 2009 at 03:12:15. 198370000. The following summary information is revealed from TCPDump log:

- 1- **Frame No. 73 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA Fragmented.**
- 2- **Frame No. 75 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: IMF Deception: Malformed Packet.**

Figure 90 shows this email,

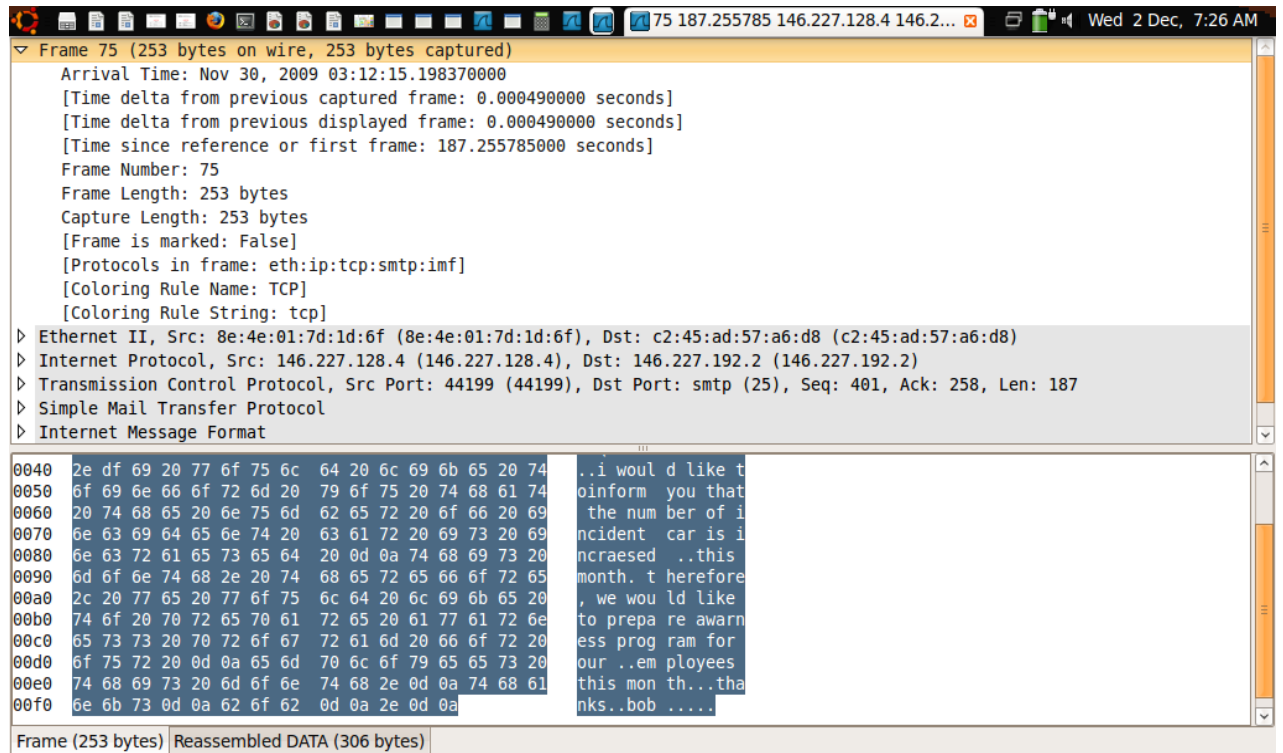


Figure 90: Examine email activity

On November 30, 2009, the insider logged out from the mail server at 03:12:19.354163000. The following information is revealed from TCPDump:

Frame No. 89 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: IMAP Deception: **BYE mail-server IMAP4rev1 server terminating connection.**

3- SMTP Connection between the Insider and the Mail Server:

On Nov 30, 2009 03:13:02, TCPDump revealed some suspicious activities after the insider logged out from the mail-server. The insider attempted to set up a SMTP session with the mail server as described below:

1- The insider used EHLO command to greet a target remotely. The following information is revealed from TCPDump:

Frame No. 109 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: **EHLO**

2- EHLO command was invalid because the insider did not identify the source. The following information is revealed from TCPDump:

Frame No. 111 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4 **Protocol Type:** SMTP **Deception:** **501 Syntactically invalid EHLO argument(s)**

3- The insider again used EHLO command to greet a target remotely. The following information is revealed from TCPDump:

Frame No. 138 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4 **Protocol Type:** SMTP **Deception:** **EHLO Tim.hotmail.com**

4- The greet was accepted by the mail and was ready to establish SMTP connection with Tim. The following information is revealed from TCPDump:

Frame No. 140 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4 **Protocol Type:** SMTP **Deception:** **250-mail-server Hello Tim.test.com [146.227.128.4] | 250-SIZE 52428800 | 250-PIPELINING | 250 HELP**

5- The insider sent an email by using Mail From command and the insider typed the source of email: Tim@hotmail.com. The following information is revealed from TCPDump:

Frame No. 147 Destination IP address: 146.227.128.2 **Source IP address:** 146.227.192.4 **Protocol Type:** SMTP **Deception:** MAIL FROM:<tim@hotmail.com>.

Figure 91 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the packet.

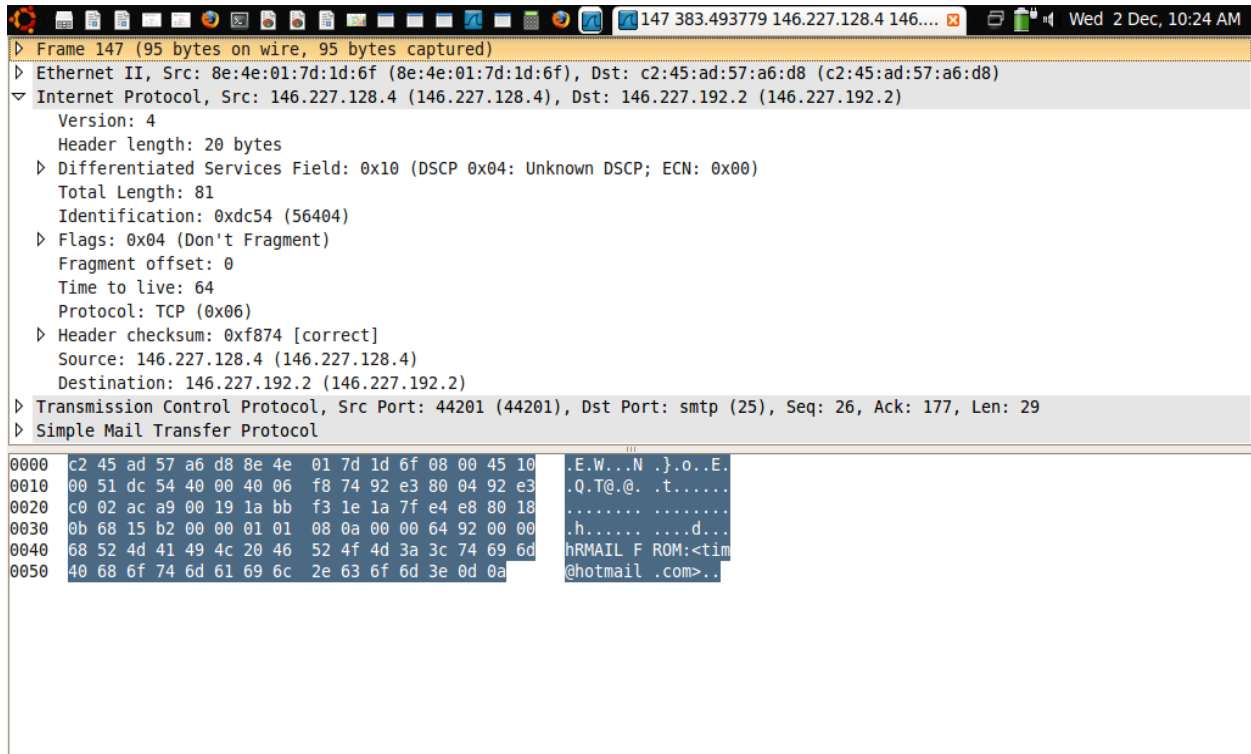


Figure 91: Examine SMTP email activity

6- After the Mail server accepted the sender address as the following detail:

Frame No. 148 Destination IP address: 146.227.192.4 Source IP address: 146.227.128.2 Protocol Type: SMTP Deception: 250 OK.

The insider sent an email to victim by using RCPT TO command. The following information is revealed from TCPDump:

Frame No. 152 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: RCPT TO:<victim@test.com>

Figure 92 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the packet.

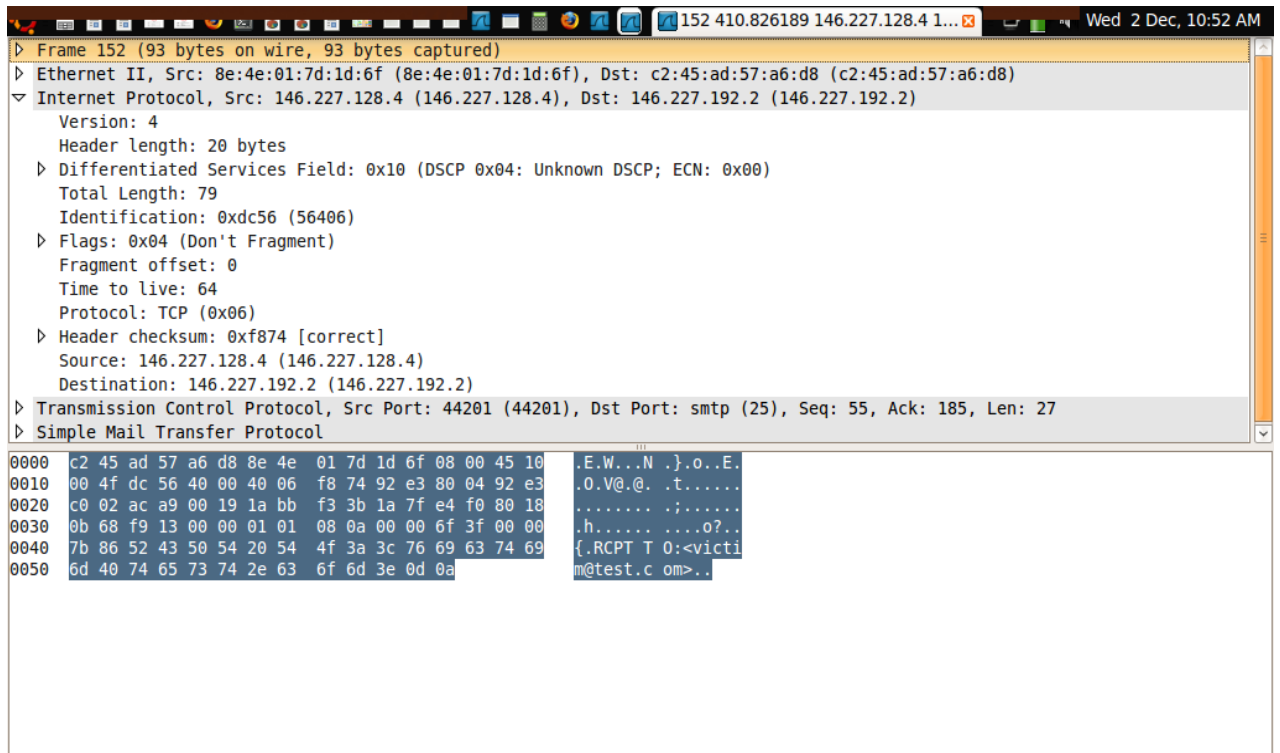


Figure 92: Examine SMTP email activity

7- After the envelope was finished, the data of the email message just as it is followed. The data consists of the email's body as well as the header fields. The command to initiate the state that makes the mail server accept the message is DATA. The following information is revealed from TCPDump:

Frame No. 155 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA

8- The insider started with the header of the message by entering day, date and time of the email. The following information is revealed from TCPDump:

Frame No. 160 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA fragment

Figure 93 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the packet. It shows that the time and date of the email was modified. It also shows the first step of creating a fake email.

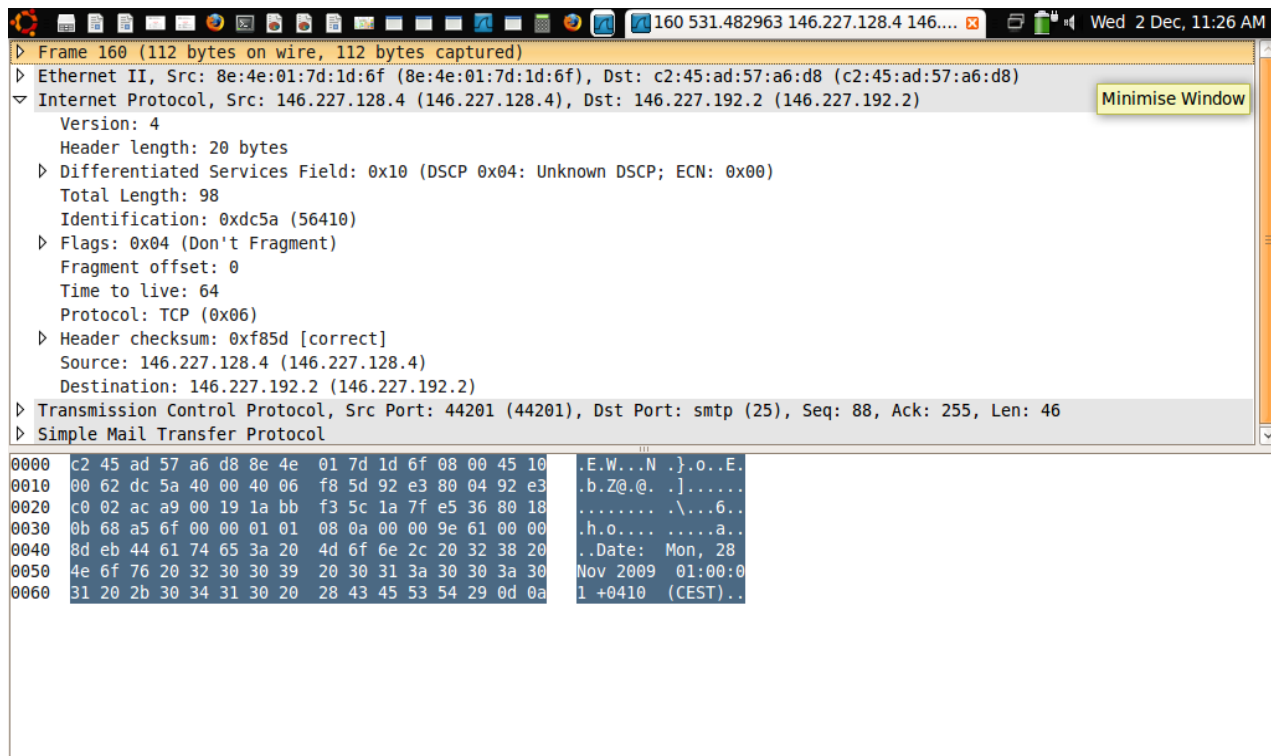


Figure 93: Examine SMTP activity for the first step of creating a fake email

The insider sent From: Tim@hotmail.com. The following information is revealed from TCPDump:

Frame No. 164 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA fragment.

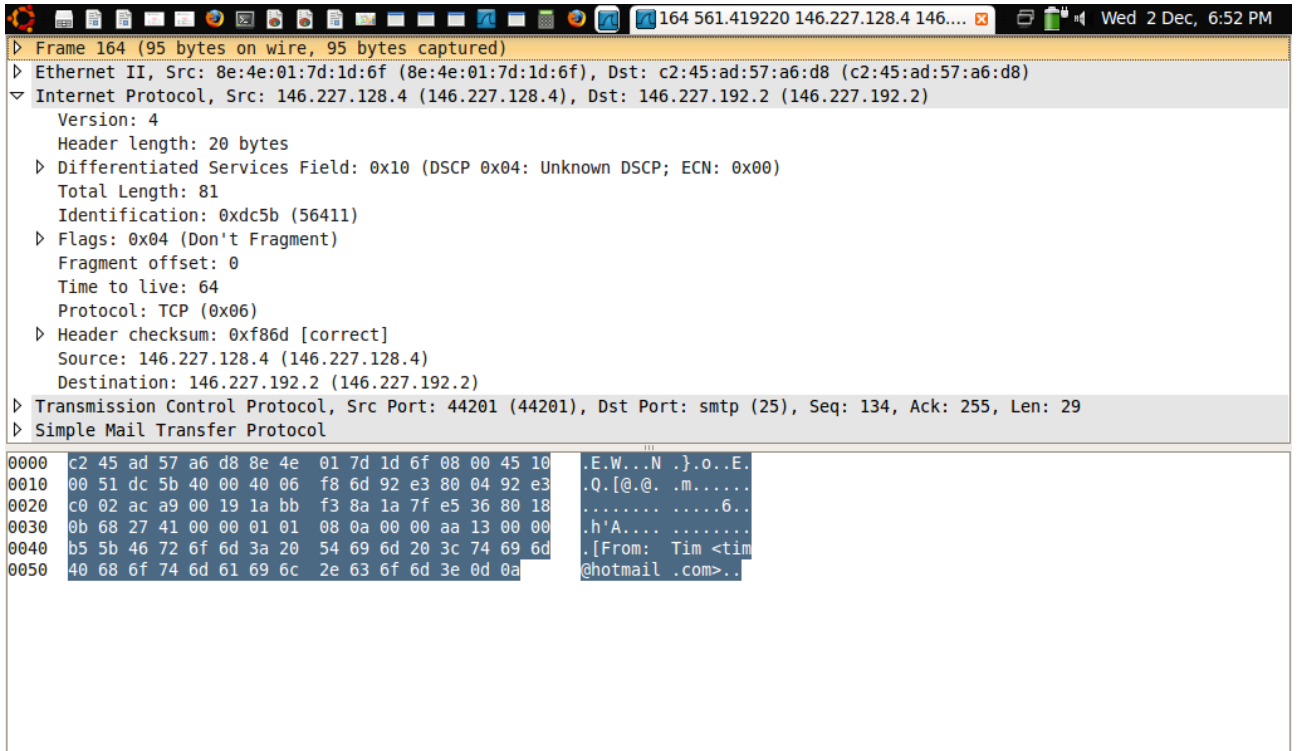


Figure 94: Examine SMTP activity for the second step of creating a fake email

Figure 94 shows the email was sent from tim@hotmail.com. It shows the second step of creating a fake email.

The insider typed Reply-To: tim@hotmail.com. The following information is revealed from TCPDump:

Frame No. 170 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA fragment.

Figure 95 shows that the third step of creating a fake email.

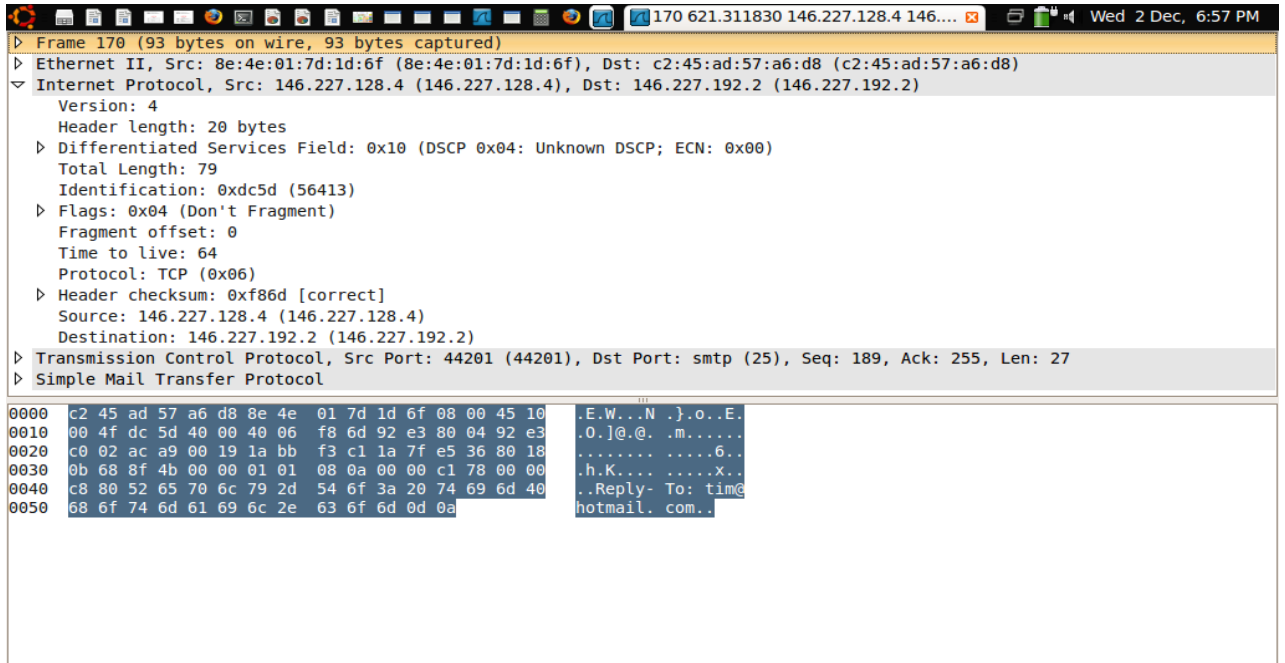


Figure 95: Examine SMTP activity for the third step of creating a fake email

The insider sent To: victim@test.com. The following information is revealed from TCPDump:

Frame No. 164 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA fragment

Figure 96 shows the fourth step of creating a fake email.

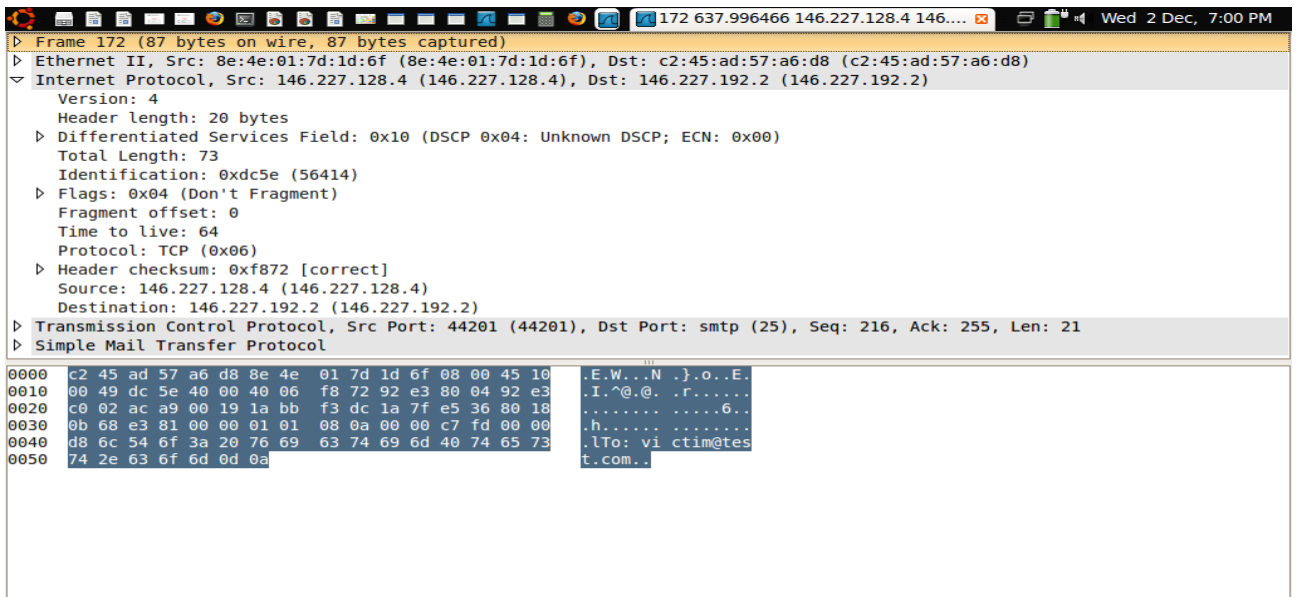


Figure 96: Examine SMTP activity for the fourth step of creating a fake email

The insider typed Subject: abuse email. The following information is revealed from TCPDump:

Frame No. 176 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA fragment

Figure 97 shows the fifth step of crating a fake email.

```

176 656.121350 146.227.128.4 146...
  Frame 176 (88 bytes on wire, 88 bytes captured)
  Ethernet II, Src: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f), Dst: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8)
  Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
    Total Length: 74
    Identification: 0xdc5f (56415)
    Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0xf870 [correct]
    Source: 146.227.128.4 (146.227.128.4)
    Destination: 146.227.192.2 (146.227.192.2)
  Transmission Control Protocol, Src Port: 44201 (44201), Dst Port: smtp (25), Seq: 237, Ack: 255, Len: 22
  Simple Mail Transfer Protocol
    0000 c2 45 ad 57 a6 d8 8e 4e 01 7d 1d 6f 08 00 45 10 .E.W..N.}.o..E.
    0010 00 4a dc 5f 40 00 40 06 f8 70 92 e3 80 04 92 e3 .J.@.@.p.....
    0020 c0 02 ac a9 00 19 1a bb f3 f1 1a 7f e5 36 80 18 .....6...
    0030 0b 68 12 4a 00 00 01 01 08 0a 00 00 cf 11 00 00 .h.J.....
    0040 de f1 53 75 62 6a 65 63 74 3a 20 61 62 75 73 65 ..Subject: abuse
    0050 20 65 6d 61 69 6c 0d 0a email..
  
```

Figure 97: Examine SMTP activity for the fifth step of creating a fake email

The insider typed Message-ID Pine. LNX. 4.64.0604032208335.264@insider. The following information is revealed from TCPDump:

Frame No. 178 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA fragment.

Figure 98 shows the sixth step of creating of a fake email.

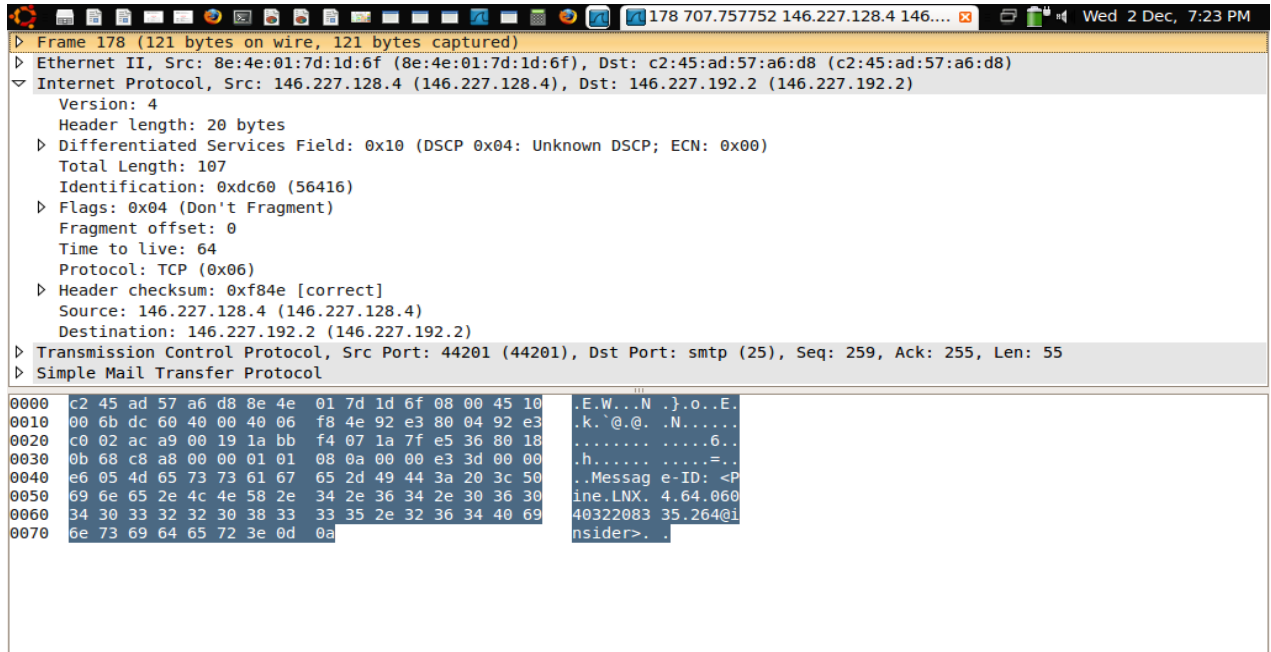


Figure 98: Examine SMTP activity for sixth step of creating a fake email

The insider identified the content type of email. Figure 99 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content type of email entered by the insider. It shows the seventh of creating a fake email.

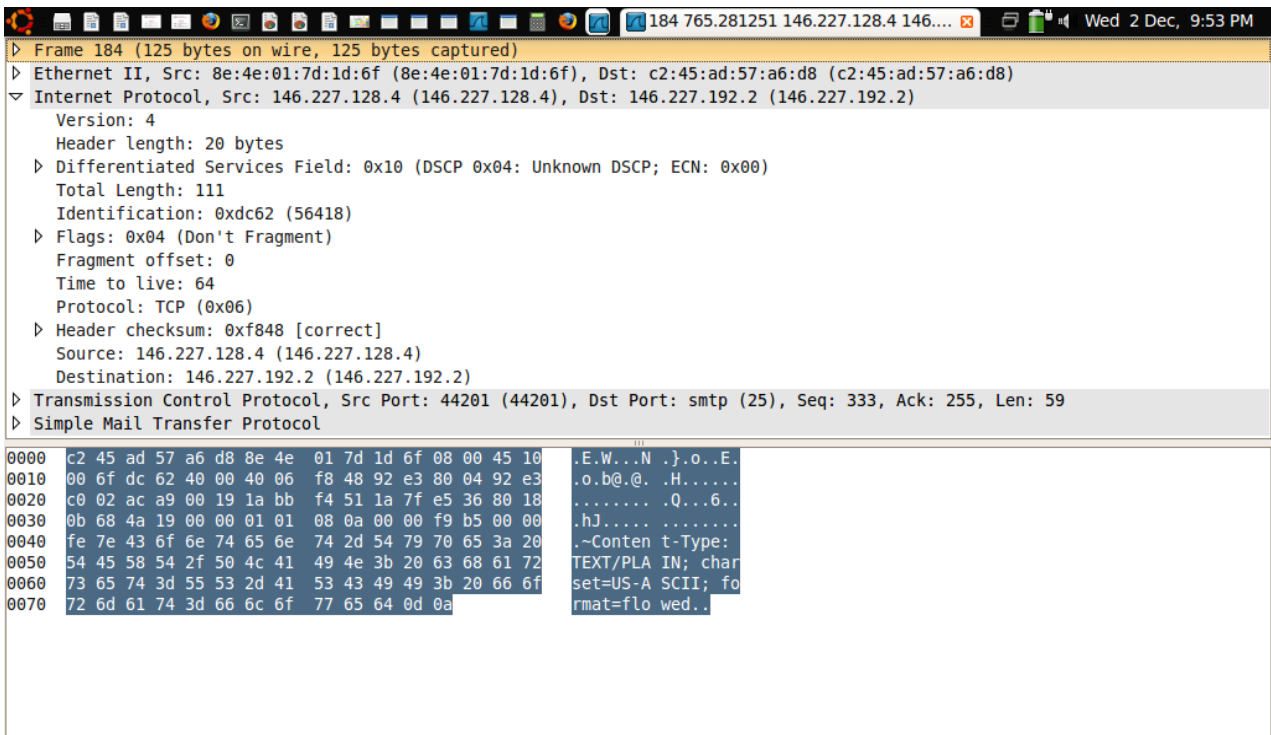


Figure 99: Examine SMTP activity for the seventh step of creating a fake email

The insider wrote the body of the message (an abusive message). The following information is revealed from TCPDump:

Frame No. 147 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: DATA.

Figure 100 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the body of the message which contained the email abuse. It also shows the eighth step of creating a fake email.

```

190 778.587083 146.227.128.4 146...
  ▸ Frame 190 (113 bytes on wire, 113 bytes captured)
  ▸ Ethernet II, Src: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f), Dst: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8)
  ▾ Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
    Version: 4
    Header length: 20 bytes
    ▸ Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
    Total Length: 99
    Identification: 0xdc64 (56420)
    ▸ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    ▸ Header checksum: 0xf852 [correct]
      Source: 146.227.128.4 (146.227.128.4)
      Destination: 146.227.192.2 (146.227.192.2)
    ▸ Transmission Control Protocol, Src Port: 44201 (44201), Dst Port: smtp (25), Seq: 394, Ack: 255, Len: 87
    ▸ Simple Mail Transfer Protocol
      .E.W...N .}.o..E.
      .c.d@. .R.....
      .....6.
      .h.....
      .*****
      **abuse email**
      *****
      .
  0000 c2 45 ad 57 a6 d8 8e 4e 01 7d 1d 6f 08 00 45 10 .E.W...N .}.o..E.
  0010 00 63 dc 64 40 00 40 06 f8 52 92 e3 80 04 92 e3 .c.d@. .R.....
  0020 c0 02 ac a9 00 19 1a bb f4 8e 1a 7f e5 36 80 18 .....6.
  0030 0b 68 f4 01 00 00 01 01 08 0a 00 00 fe e8 00 01 .h.....
  0040 10 fb 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a .*****
  0050 2a 2a 61 62 75 73 65 20 65 6d 61 69 6c 2a 2a 2a **abuse email**
  0060 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d *****
  0070 0a .
  
```

Figure 100: Examine SMTP activity for the eighth step of creating a fake email

The insider terminated the SMTP connection with the mail server by using QUIT command. The following information is revealed from TCPDump:

Frame No. 204 Destination IP address: 146.227.128.2 Source IP address: 146.227.192.4 Protocol Type: SMTP Deception: QUIT.

Figure 101 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the QUIT command. It shows the ninth step of creating a fake email.

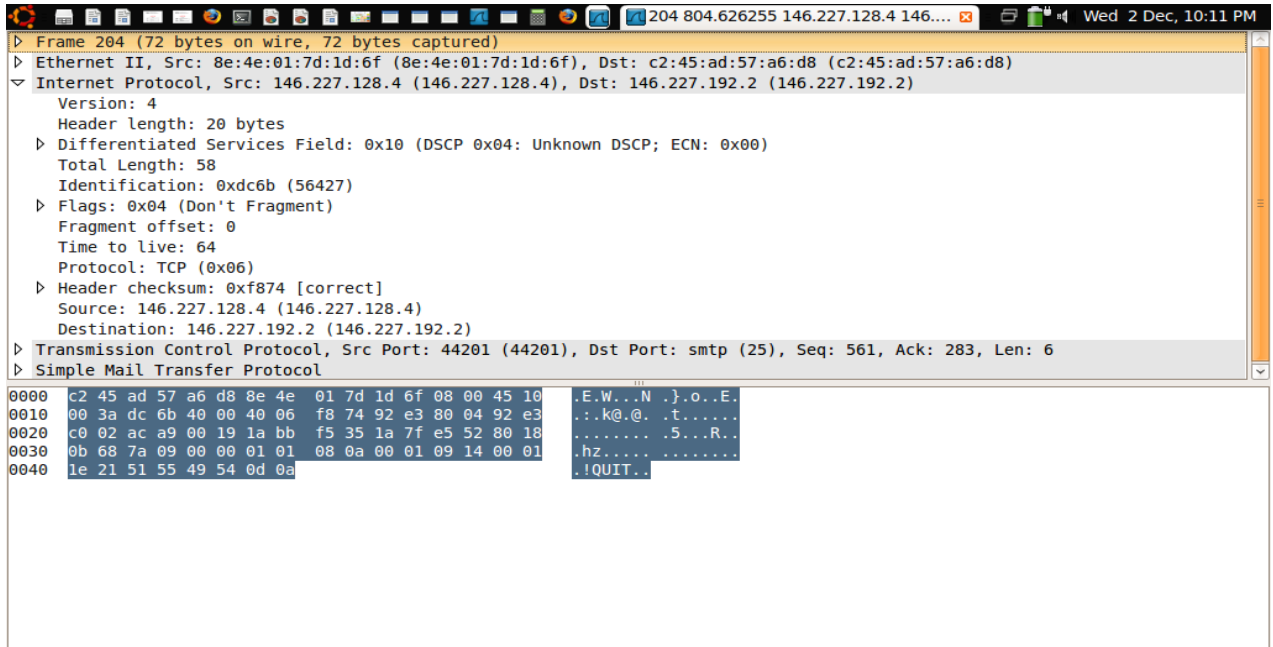


Figure 101: Examine SMTP activity for the ninth step of creating a fake email

The mail server terminated the SMTP connection with the insider. The following information is revealed from TCPDump:

Frame No. 206 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: SMTP Deception: 44201 [FIN, ACK] Seq=319 Ack=567 Win=5792 Len=0 TSV=73736 TSER=67860

3. Examination and Analysis Insider's PC

By using `ls -l` command, it showed that there was one file. This file was car-insurance-report and was last accessed on the 30th of November 2009, at 1:56. Another job responsibility for the insider is collecting car insurance reports. Therefore, this file is indeed legitimate because there is a relationship between this file and the insider's job responsibilities. This file was classified as a BF. Figure 102 shows the name of the file and the last date of access.

```

Thu 3 Dec, 1:30 AM
Mounting /home/tiger on /hosthome...
Mounting /home/tiger/test-5 on /hostlab ...
--- Netkit phase 1 initialization terminated ---
Starting system log daemon...
Starting kernel log daemon...

--- Starting Netkit phase 2 init script ---

>>> Running insider specific startup script...
>>> End of insider specific startup script.

=====

Lab directory (host): /home/tiger/test-5
Version: 1
Author: A. Al-Morjan
Email: almorjan@dmu.co.uk
Web: <none>
Description:
Configuration and operation of the SMTP third Expermint
=====

--- Netkit phase 2 initialization terminated ---

insider login: root (automatic login)
Last login: Wed Dec 2 22:40:12 UTC 2009 on tty1
insider:~# ls -l
total 1
-rw-r--r-- 1 root root 0 2009-11-30 01:56 car-insurance-report
drwxr-xr-x 2 root root 1024 2009-11-30 03:12 mail
insider:~# ls
car-insurance-report mail
insider:~# ls
car-insurance-report mail
insider:~# ls -l
total 1
-rw-r--r-- 1 root root 0 2009-11-30 01:56 car-insurance-report
drwxr-xr-x 2 root root 1024 2009-11-30 03:12 mail
insider:~#

```

Figure 102: Examine insider's computer activity

B1. Ex5:

The victim reported that an abusive email was received from insider@test.com. The email was received on Monday, 30 November 2009 at 02:53:20. Figure 103 shows that the content of an abusive email header includes date of email, the source address and the recipient address, subject of email and the body of this message. However, the insider denied the allegation of sending an abusive email because he was out of his office, when the email was sent. The insider claimed that his password was stolen.

Preliminary investigation showed that the insider account belonged to Test Company and because the insider worked for Test Company, the first step was to review fw-2 (internal firewall) log. When reviewing the log, it appeared that there was no connection between the mail server and the insider. This lead us to examine the mail envelope header of the abusive message in order to identify the source IP address of the email envelope.

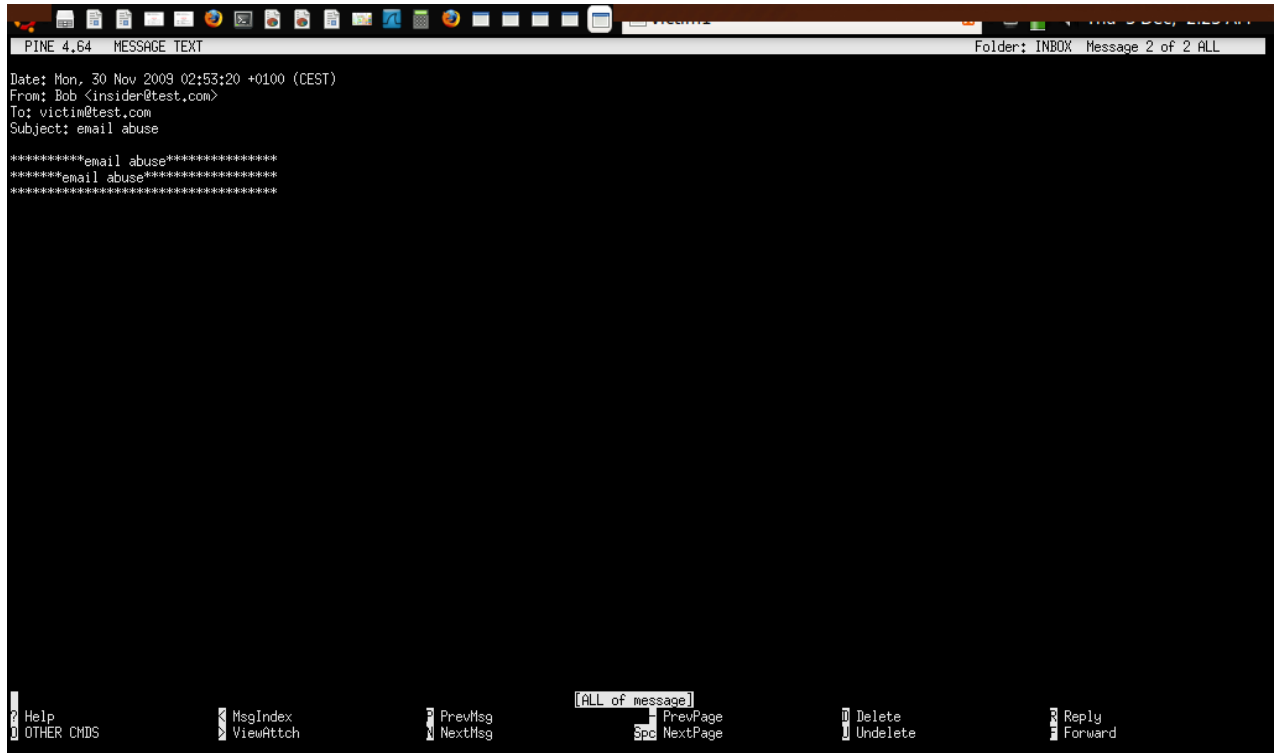


Figure 103: Examine email abusive

Interestingly, the envelope header of the abusive message showed that the source IP address was an external IP address 1.1.0.1. The preliminary result of the investigation showed that the abusive email was coming from the outside and using the insider account. The next investigation step was to examine fw-1 (external firewall) log in order to identify the connection.

Figure 104 shows firewall's activity log.

```

WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:45:19 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=12287 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 02:45:55 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=98 TOS=0x10 PREC=0x00 TTL=63 ID=12288 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:47:05 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=82 TOS=0x10 PREC=0x00 TTL=63 ID=12289 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:47:25 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=78 TOS=0x10 PREC=0x00 TTL=63 ID=12290 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:48:26 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=80 TOS=0x10 PREC=0x00 TTL=63 ID=12291 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:48:43 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=73 TOS=0x10 PREC=0x00 TTL=63 ID=12292 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:48:58 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=73 TOS=0x10 PREC=0x00 TTL=63 ID=12293 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:49:59 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=107 TOS=0x10 PREC=0x00 TTL=63 ID=12294 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:50:11 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=71 TOS=0x10 PREC=0x00 TTL=63 ID=12295 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:00 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=111 TOS=0x10 PREC=0x00 TTL=63 ID=12296 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:01 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=54 TOS=0x10 PREC=0x00 TTL=63 ID=12297 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:10 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=90 TOS=0x10 PREC=0x00 TTL=63 ID=12298 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:20 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=90 TOS=0x10 PREC=0x00 TTL=63 ID=12299 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:24 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=90 TOS=0x10 PREC=0x00 TTL=63 ID=12300 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:25 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=54 TOS=0x10 PREC=0x00 TTL=63 ID=12301 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:31 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=55 TOS=0x10 PREC=0x00 TTL=63 ID=12302 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:31 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=12303 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 02:51:38 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=58 TOS=0x10 PREC=0x00 TTL=63 ID=12304 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK PSH URG=0
Nov 30 02:51:38 fw-1 kernel: ***mailattack***--logIN=eth0 OUT=eth1 SRC=1.1.0.1 DST=146.227.192.2 LEN=52 TOS=0x10 PREC=0x00 TTL=63 ID=12305 DF PROTO=TCP SPT=45994 DPT=25
WINDOW=2920 RES=0x00 ACK URG=0
Nov 30 02:51:47 fw-1 kernel: device eth0 left promiscuous mode
fw-1: #

```

Figure 104: Examine firewall activity log

- **SMTP Connection between the insider and the Mail server**

The log shows that there was an SMTP connection between the mail server 146.227.192.2 and an outsider computer 1.1.0.1. This information lead to examining the email activities between these computers. Therefore, the TCPDump log was useful to examine theses activities.

- **Email No.1**

1- An attacker tried to connect to mail (mail.test.com) remotely at 02:24:25. The following information is revealed from TCPDump:

Frame No. 58 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1

Protocol Type: DNS Deception: Standard query AAAA mail.test.com

2- EHLO command was used to establish a connection between the outsider 1.1.0.1 and the Mail server. The following information is revealed from TCPDump:

Frame No. 71 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1

Protocol Type: SMTP Deception: EHLO insider.test.com

3- The greet was accepted by the Mail and ready to establish SMTP connection with the insider. The following information is revealed from TCPDump:

Frame No. 73 Destination IP address: 1.1.0.1 **Source IP address:** 146.227.128.2
Protocol Type: SMTP **Deception:** 250-mail-server Hello insider.test.com [1.1.0.1] |
250-SIZE 52428800 | 250-PIPELINING | 250 HELP

4- The insider sent an email by using Mail From command and the insider typed the source of email: insider@test.com. The following information is revealed from TCPDump:

Frame No. 80 Destination IP address: 146.227.128.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** MAIL FROM:<insider@test.com>.

5- After the mail server accepted the sender address as the following detail:

Frame No. 81 Destination IP address: 1.1.0.1 **Source IP address:** 146.227.192.2
Protocol Type: SMTP **Deception:** 250 OK

the insider sent an email to the victim by using RCPT TO command. The following information is revealed from TCPDump:

Frame No. 83 Destination IP address: 146.227.192.2 **Source IP address:** 1.10.1
Protocol Type: SMTP **Deception:** RCPT TO:<victim@test.com>

6- After the envelope was finished, the data of the email message just as it is followed. The data consists of the email's body as well as the header fields. The command to initiate the state that makes the mail server accept the message is DATA. The following information is revealed from TCPDump:

Frame No. 88 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** DATA

7- The insider started with header of the message by entering day, date and time of the email. The following information is revealed from TCPDump:

Frame No. 91 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** DATA fragment

The insider sent From: Bob insider@test.com. The following information is revealed from TCPDump:

Frame No. 95 Destination IP address: 146.227.192.2 Source IP address: 1.1.10.1 Protocol Type: SMTP Deception: DATA fragment

The insider typed Reply-To: insider@hotmail.com. The following information is revealed from TCPDump:

Frame No. 101 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1 Protocol Type: SMTP Deception: DATA fragment

The insider sent To: victim@test.com . The following information is revealed from TCPDump:

Frame No. 103 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1 Protocol Type: SMTP Deception: DATA fragment

The insider typed Subject: asking for updated car incident report. The following information is revealed from TCPDump:

Frame No. 107 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1 Protocol Type: SMTP Deception: DATA fragment

The insider typed Message-ID Pine. LNX. 4.64.0604032208331.264@insider. The following information is revealed from TCPDump:

Frame No. 111 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1 Protocol Type: SMTP Deception: DATA fragment

The insider identified the content type of email by typing Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed.

The insider wrote the body of the message. The following information is revealed from TCPDump:

**Frame No. 125 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA.**

Figure 105 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the body of the message.

```

Frame 125 (162 bytes on wire, 162 bytes captured)
  Arrival Time: Nov 30, 2009 02:33:04.372490000
  [Time delta from previous captured frame: 57.520835000 seconds]
  [Time delta from previous displayed frame: 57.520835000 seconds]
  [Time since reference or first frame: 851.820766000 seconds]
  Frame Number: 125
  Frame Length: 162 bytes
  Capture Length: 162 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:smtp]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  ▸ Ethernet II, Src: 42:54:a1:43:7f:f3 (42:54:a1:43:7f:f3), Dst: f2:b8:1e:21:0a:29 (f2:b8:1e:21:0a:29)
  ▸ Internet Protocol, Src: 1.1.0.1 (1.1.0.1), Dst: 146.227.192.2 (146.227.192.2)
  ▸ Transmission Control Protocol, Src Port: 59418 (59418), Dst Port: smtp (25), Seq: 429, Ack: 253, Len: 96
  ▸ Simple Mail Transfer Protocol

0000  f2 b8 1e 21 0a 29 42 54 a1 43 7f f3 08 00 45 10  ...!)BT .C....E.
0010  00 94 47 8d 40 00 40 06 9e df 01 01 00 01 92 e3  ..G.@. ....
0020  c0 02 e8 1a 00 19 71 fc 54 07 73 b2 ba e4 80 18  ....q. T.s....
0030  0b 68 70 f8 00 00 01 01 08 0a 00 00 df e7 00 01  .hp....
0040  34 56 69 20 77 6f 75 6c 64 20 6c 69 6b 65 20 79  4vi woul d like y
0050  6f 75 20 74 6f 20 70 72 6f 76 69 64 65 20 6d 65  ou to pr ovide me
0060  20 77 69 74 68 20 74 68 65 20 75 70 64 61 74 65  with th e update
0070  64 20 6c 69 73 74 20 6f 66 20 63 61 72 20 69 6e  d list o f car in
0080  63 69 64 65 6e 74 20 72 65 70 6f 72 61 73 20 73  cident r eporas s
0090  6f 6f 6e 20 61 73 20 70 6f 73 73 69 62 6c 65 2e  oon as p ossible.
00a0  0d 0a
  
```

Figure 105: Examine email activity

The insider terminated the SMTP connection with the mail server by using QUIT command. The following information is revealed from TCPDump:

**Frame No. 139 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: QUIT.**

It appeared that it is a business email because there is matching between the insider's job activities and this email.

- **Email No.2:**

1- An attacker tried to connect the mail (mail.test.com) remotely at 02:33:58. The following information is revealed from TCPDump:

Frame No. 149 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: DNS **Deception:** **Standard query AAAA mail.test.com**

2- EHLO command was used to establish a connection between the outsider 1.1.0.1 and the mail server. The following information is revealed from TCPDump:

Frame No. 160 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **EHLO insider.test.com**

3- The greet was accepted by the mail and ready to establish SMTP connection with the insider. The following information is revealed from TCPDump:

Frame No. 162 Destination IP address: 1.1.0.1 **Source IP address:** 146.227.192.2
Protocol Type: SMTP **Deception:** **250-mail-server Hello insider.test.com [1.1.0.1] | 250-SIZE 52428800 | 250-PIPELINING | 250 HELP**

4- The insider sent an email by using Mail From command to type the source of the email: insider@test.com. The following information is revealed from TCPDump:

Frame No. 167 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** MAIL FROM:<insider@test.com>.

5- After the mail server accepted the sender address as the following detail:

Frame No. 168 Destination IP address: 1.1.0.1 **Source IP address:** 146.227.192.2
Protocol Type: SMTP **Deception:** **250 OK**

the insider sent an email to victim by using RCPT TO command. The following information is revealed from TCPDump:

Frame No. 172 Destination IP address: 146.227.192.2 **Source IP address:** 1.10.1
Protocol Type: SMTP **Deception:** **RCPT TO:<manager@test.com>**

6- After the envelope was finished, the data of the email message just as it is followed. The data consists of the email's body as well as the header fields. The command to initiate the state that makes the mail server accept the message is DATA. The following information is revealed from TCPDump:

Frame No. 177 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **DATA**

7- The insider started with header of the message by entering day, date and time of the email. The following information is revealed from TCPDump:

Frame No. 180 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **DATA fragment**

The insider sent From: Tim@hotmail.com. The following information is revealed from TCPDump:

Frame No. 184 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **DATA fragment**

The insider typed Reply-To: insider@hotmail.com. The following information is revealed from TCPDump:

Frame No. 190 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **DATA fragment**

The insider sent To: manager@test.com. The following information is revealed from TCPDump:

Frame No. 164 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **DATA fragment**

The insider typed Subject: going to car insurance company. The following information is revealed from TCPDump:

Frame No. 196 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** **DATA fragment**

The insider typed Message-ID Pine. LNX. 4.64.0604032208332.264@insider. The following information is revealed from TCPDump:

Frame No. 200 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment

The insider identified the content type of email by typing Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed.

The insider wrote the body of the message (abuse message). The following information is revealed from TCPDump:

Frame No. 212 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA.

Figure 106 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the body of the message.

The screenshot shows a network traffic analysis window for Frame 212 (178 bytes on wire, 178 bytes captured). The frame details include:

- Arrival Time: Nov 30, 2009 02:42:46.378910000
- [Time delta from previous captured frame: 68.207429000 seconds]
- [Time delta from previous displayed frame: 68.207429000 seconds]
- [Time since reference or first frame: 1433.827186000 seconds]
- Frame Number: 212
- Frame Length: 178 bytes
- Capture Length: 178 bytes
- [Frame is marked: False]
- [Protocols in frame: eth:ip:tcp:smtp]
- [Coloring Rule Name: TCP]
- [Coloring Rule String: tcp]

The protocol stack is shown as:

- ▶ Ethernet II, Src: 42:54:a1:43:7f:f3 (42:54:a1:43:7f:f3), Dst: f2:b8:1e:21:0a:29 (f2:b8:1e:21:0a:29)
- ▶ Internet Protocol, Src: 1.1.0.1 (1.1.0.1), Dst: 146.227.192.2 (146.227.192.2)
- ▶ Transmission Control Protocol, Src Port: 35642 (35642), Dst Port: smtp (25), Seq: 419, Ack: 253, Len: 112
- ▶ Simple Mail Transfer Protocol

The hex dump shows the message body content:

```

0000 f2 b8 1e 21 0a 29 42 54 a1 43 7f f3 08 00 45 10  ...!)BT .C...E.
0010 00 a4 78 26 40 00 40 06 6e 36 01 01 00 01 92 e3  ..x&@.@. n6.....
0020 c0 02 8b 3a 00 19 8a 4a 8e db 8b ce d1 a0 80 18  ..:..J .....
0030 0b 68 ce de 00 00 01 01 08 0a 00 01 c3 40 00 02  .h..... @...
0040 14 e3 69 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74  .i woul d like t
0050 6f 20 69 6e 66 6f 72 6d 20 79 6f 75 20 74 68 61  o inform you tha
0060 74 20 74 68 69 73 20 61 66 74 65 72 6e 6f 6f 6e  t this a fternoon
0070 20 69 20 61 6d 20 67 6f 69 6e 67 20 74 6f 20 74  i am go ing to t
0080 68 65 20 63 61 72 20 69 6e 73 75 72 61 6e 63 65  he car i nsurance
0090 20 63 6f 6d 70 61 6e 67 20 66 6f 72 20 61 20 62  compang for a b
00a0 75 73 69 6e 65 73 73 20 6d 65 65 74 69 6e 67 2e  usiness meeting.
00b0 0d 0a

```

Figure 106: Examine email activity

The insider terminated the SMTP connection with the mail server by using QUIT command. The following information is revealed from TCPDump:

**Frame No. 234 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: QUIT.**

Figure 107 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the packet.

It appeared that this email was a business email because there is a match between the insider's job activities and this email.

```

Frame 204 (72 bytes on wire, 72 bytes captured)
  Ethernet II, Src: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f), Dst: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8)
  Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
  Total Length: 58
  Identification: 0xdc6b (56427)
  Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0xf874 [correct]
  Source: 146.227.128.4 (146.227.128.4)
  Destination: 146.227.192.2 (146.227.192.2)
  Transmission Control Protocol, Src Port: 44201 (44201), Dst Port: smtp (25), Seq: 561, Ack: 283, Len: 6
  Simple Mail Transfer Protocol
  0000 c2 45 ad 57 a6 d8 8e 4e 01 7d 1d 6f 08 00 45 10 .E.W.N}.o.E.
  0010 00 3a dc 6b 40 00 40 06 f8 74 92 e3 80 04 92 e3 ..k@.t.....
  0020 c0 02 ac a9 00 19 1a bb f5 35 1a 7f e5 52 80 18 .....5..R..
  0030 0b 68 7a 09 00 00 01 01 08 0a 00 01 09 14 00 01 .hz.....
  0040 1e 21 51 55 49 54 0d 0a !QUIT.
  
```

Figure 107: Examine email activity

- **Email No.3:**

1- An attacker tried to connect the mail (mail.test.com) remotely at 02:43:47. The following information is revealed from TCPDump:

**Frame No. 240 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: DNS Deception: Standard query AAAA mail.test.com**

2- EHLO command was used to establish a connection between the outsider 1.1.0.1 and the mail server. The following information is revealed from TCPDump:

**Frame No. 255 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: EHLO insider.test.com**

3- The greet was accepted by the mail and ready to establish SMTP connection with the insider. The following information is revealed from TCPDump:

Frame No. 257 Destination IP address: 1.1.0.1 **Source IP address:** 146.227.192.2
Protocol Type: SMTP **Deception:** 250-mail-server Hello insider.test.com [1.1.0.1] | 250-SIZE 52428800 | 250-PIPELINING | 250 HELP

4- The insider sent an email using Mail From command and the insider typed the source of email: insider@test.com. The following information is revealed from TCPDump:

Frame No. 264 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** MAIL FROM:<insider@test.com>.

5- After the Mail server accepted the sender address as the following detail:

Frame No. 265 Destination IP address: 1.1.0.1 **Source IP address:** 146.227.192.2
Protocol Type: SMTP **Deception:** 250 OK

the insider sent an email to victim by using RCPT TO command. The following information is revealed from TCPDump:

Frame No. 269 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** RCPT TO:<victim@test.com>

6- After the envelope was finished, the data of the email message just as it is followed. The data consists of the email's body as well as the header fields. The command to initiate the state that makes the mail server accept the message is DATA. The following information is revealed from TCPDump:

Frame No. 272 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** DATA

7- The insider started with header of the message by entering day, date and time of the email. The following information is revealed from TCPDump:

Frame No. 277 Destination IP address: 146.227.192.2 **Source IP address:** 1.1.0.1
Protocol Type: SMTP **Deception:** DATA fragment

The insider sent From: insider@hotmail.com. The following information is revealed from TCPDump:

**Frame No. 281 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment**

The insider typed Reply-To: insider@hotmail.com. The following information is revealed from TCPDump:

**Frame No. 287 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment**

The insider sent To: victim@test.com. The following information is revealed from TCPDump:

**Frame No. 291 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment**

The insider typed Subject: email abuse. The following information is revealed from TCPDump:

**Frame No. 293 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment**

The insider typed Message-ID Pine. LNX. 4.64.0604032208333.264@insider. The following information is revealed from TCPDump:

**Frame No. 297 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment**

The insider identified the content type of email by typing Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed.

**Frame No. 303 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA fragment**

The insider wrote the body of the message (abuse message). The following information is revealed from TCPDump:

**Frame No. 309 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: DATA.**

Figure 108 shows that the TCPDump information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the body of the message.

```

309 1938.155139 1.1.0.1 146.22...
Frame 309 (104 bytes on wire, 104 bytes captured)
  Arrival Time: Nov 30, 2009 02:51:10.706863000
  [Time delta from previous captured frame: 4.975186000 seconds]
  [Time delta from previous displayed frame: 4.975186000 seconds]
  [Time since reference or first frame: 1938.155139000 seconds]
  Frame Number: 309
  Frame Length: 104 bytes
  Capture Length: 104 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:smtp]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  ▸ Ethernet II, Src: 42:54:a1:43:7f:f3 (42:54:a1:43:7f:f3), Dst: f2:b8:1e:21:0a:29 (f2:b8:1e:21:0a:29)
  ▸ Internet Protocol, Src: 1.1.0.1 (1.1.0.1), Dst: 146.227.192.2 (146.227.192.2)
  ▸ Transmission Control Protocol, Src Port: 45994 (45994), Dst Port: smtp (25), Seq: 400, Ack: 253, Len: 38
  ▸ Simple Mail Transfer Protocol

0000  f2 b8 1e 21 0a 29 42 54 a1 43 7f f3 08 00 45 10  ...!.)BT .C...E.
0010  00 5a 30 0a 40 00 40 06 b6 9c 01 01 00 01 92 e3  .Z0.@.@. ....
0020  c0 02 b3 aa 00 19 b0 01 f6 ac af bc 8c 50 80 18  .....P..
0030  0b 68 91 9b 00 00 01 01 08 0a 00 02 88 41 00 02  .h.....A..
0040  f0 e3 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 65 6d 61 69  .***** **email
0050  6c 20 61 62 75 73 65 2a 2a 2a 2a 2a 2a 2a 2a 2a  l abuse* *****
0060  2a 2a 2a 2a 2a 2a 0d 0a  *****..

```

Figure 108: Examine email activity

The insider terminated the SMTP connection with the mail server by using QUIT command. The following information is revealed from TCPDump:

**Frame No. 321 Destination IP address: 146.227.192.2 Source IP address: 1.1.0.1
Protocol Type: SMTP Deception: QUIT.**

B1. Ex6:

A victim reported that an abusive email was received from this source: insider@test.com. The email was received on September 6, 2009 at 20:33:14.634794000.

Preliminary investigation showed that this email was sent from the insider but the insider denied the allegation of sending an abusive email. Therefore, the first step was to collect legitimate and suspicious activity for the insider from the logs and the insider's computer. Then these activities were examined in order to provide analysis process with insider's activities. The examination process provided the following information:

1. MA:

- **Email login:**

There were three login activities to the mail server from the insider's computer. The first login from the insider's computer was a failed login on September 6, 2009 at 20:32:13.408412000. This failed login displays when an organisation's user attempts to access the organisation's Mail server and the Mail server authentication system is unable to recognize the user. The following information was revealed from TCPDump:

Frame No. 61 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** NO AUTHENTICATE LOGIN failed.

Figure 109 shows that the fail login information was presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

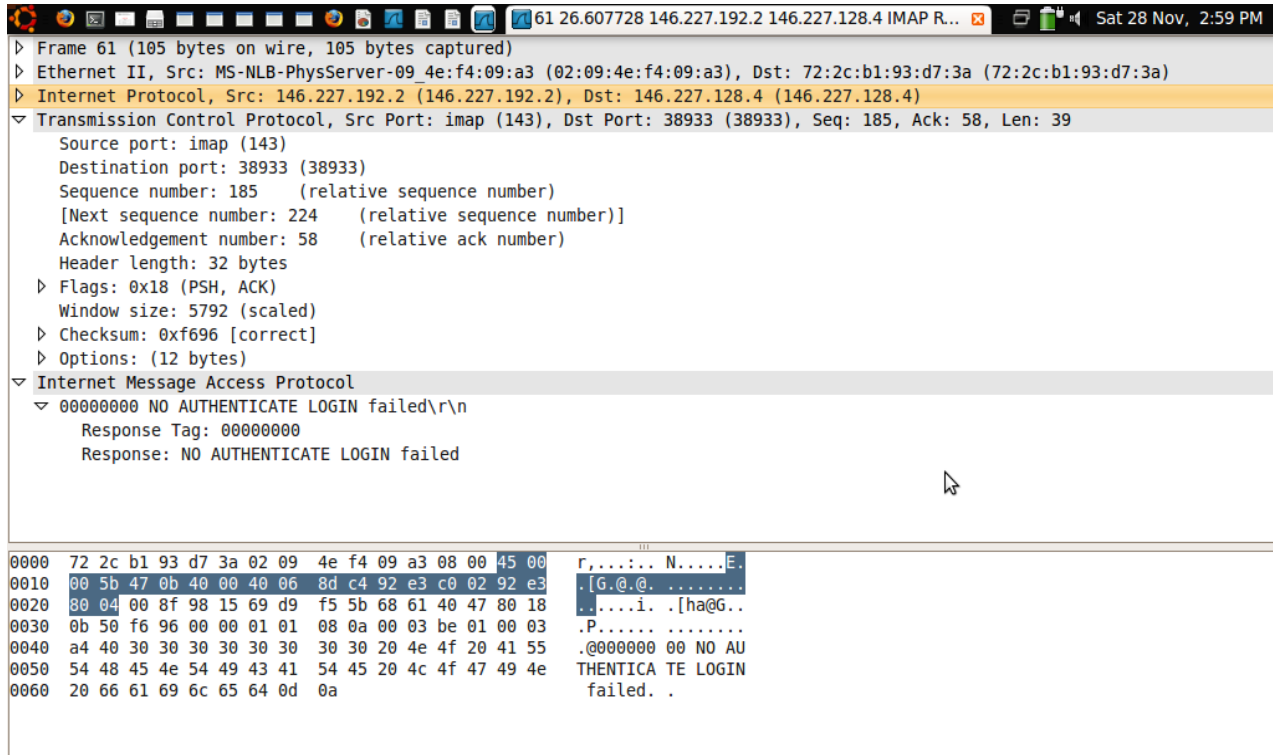


Figure 109: Authentication login activity

The second login from the insider's computer was also a failed login on September 6, 2009 at 20:32:18. 618219000. The following summary information is revealed from TCPDump log:

Frame No. 77 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** NO AUTHENTICATE LOGIN failed.

Figure 110 shows that the fail login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

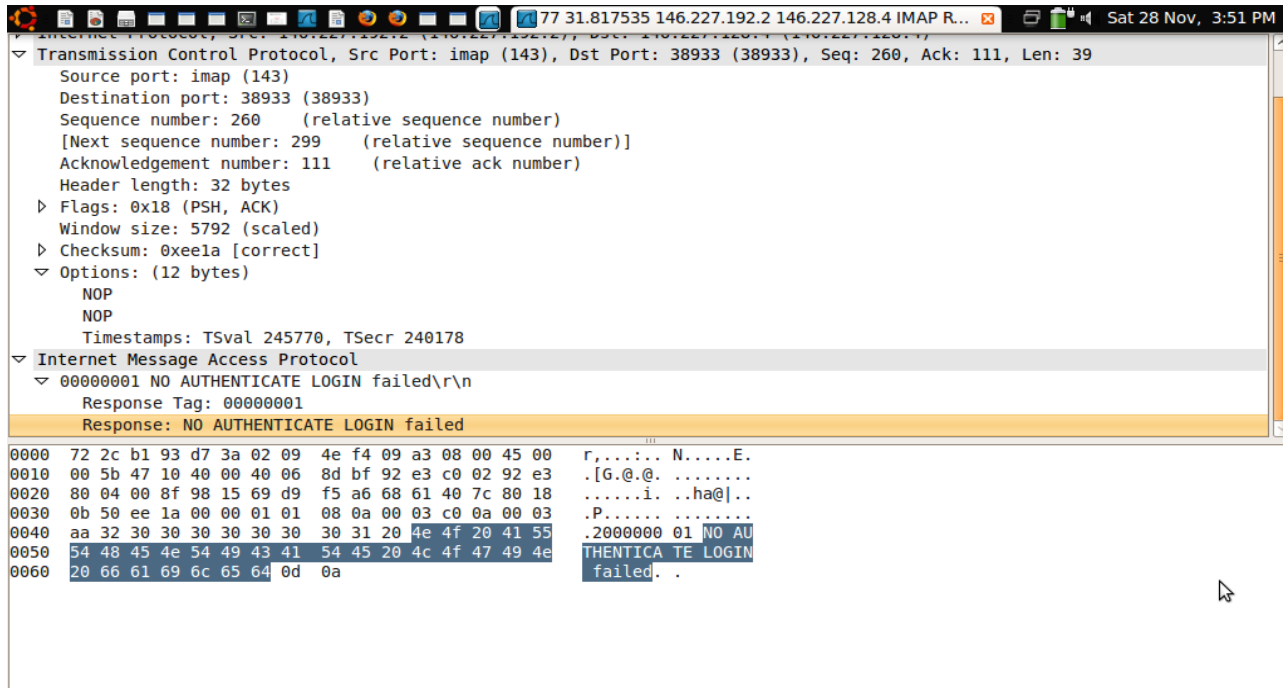


Figure 110: Authentication login activity

The third login from the insider's computer was successfully authenticated on September 6, 2009 at 20:32:23.710038000. This login displays when an organisation's user attempts to access the organisation's Mail server and the Mail server authentication system is able to recognize the user. It indicated that the attacker was successful in accessing the mail server. The following information is revealed from TCPDump:

Frame No. 88 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** Response: 00000002 OK [CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY UNSELECT SCAN SORT THREAD=REFERENCES THREAD=ORDEREDSUBJECT MULTIAPPEND] **User** **INSIDER AUTHENTICATED.**

Figure 111 shows that the authenticated login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

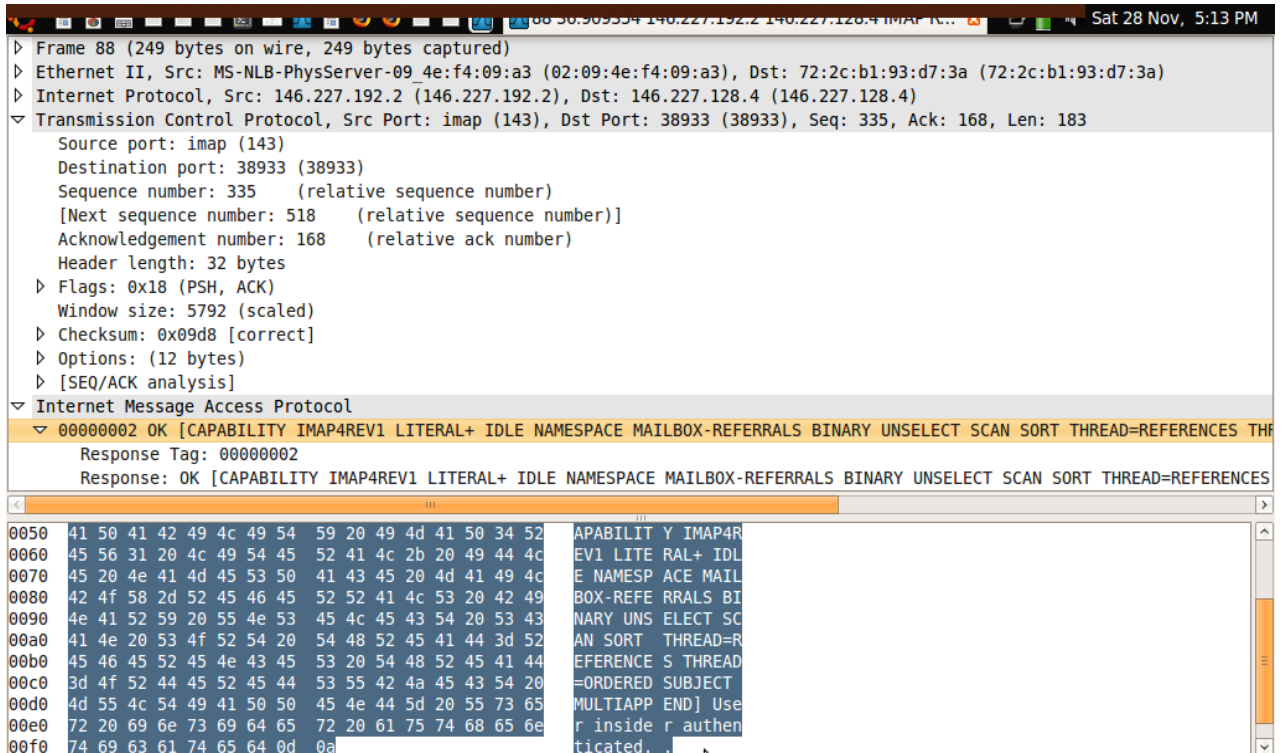


Figure 111: Authentication login activity

2. Email Activities:

An abusive email was sent.

B1.Ex7:

The victim reported that an abusive email was received from insider@test.com. The email was received on December 3, 2009 at 09:49:01.273294000.

Preliminary investigation showed that this email was sent from the insider but the insider denied the allegation of sending the abusive email. Therefore, the first step was to collect legitimate and suspicious activity for the insider from the logs and examined these activities in order to provide analysis process with insider's activities. The examination process provided the following information:

1. MA:

- **Email login:**

There were two login activities to the mail server from the insider's computer. The first login from the insider's computer failed on the 3rd of December 2009 at 09:47:46.693596000. This failed login displays when an organisation's user attempts to

access the organisation's Mail server and the Mail server authentication system is unable to recognize the user. The following information is revealed from TCPDump:

Frame No. 35 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** NO AUTHENTICATE LOGIN failed. Figure 112 shows the failed login.

```

Frame 35 (105 bytes on wire, 105 bytes captured)
  Arrival Time: Dec  3, 2009 09:47:46.693596000
  [Time delta from previous captured frame: 12.974375000 seconds]
  [Time delta from previous displayed frame: 12.974375000 seconds]
  [Time since reference or first frame: 27.598368000 seconds]
  Frame Number: 35
  Frame Length: 105 bytes
  Capture Length: 105 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:imap]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  > Ethernet II, Src: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8), Dst: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f)
  > Internet Protocol, Src: 146.227.192.2 (146.227.192.2), Dst: 146.227.128.4 (146.227.128.4)
  > Transmission Control Protocol, Src Port: imap (143), Dst Port: 46009 (46009), Seq: 185, Ack: 50, Len: 39
  > Internet Message Access Protocol

0000  8e 4e 01 7d 1d 6f c2 45  ad 57 a6 d8 08 00 45 00  .N.)o.E .W...E.
0010  00 5b 07 bb 40 00 3f 06  ce 14 92 e3 c0 02 92 e3  .[...@.? .....
0020  80 04 00 8f b3 b9 17 8f  ce 0d 16 ef e9 c7 80 18  .....
0030  0b 50 cf 42 00 00 01 01  08 0a 00 00 d5 93 00 00  .P.B.....
0040  b9 ee 30 30 30 30 30 30  30 30 20 4e 4f 20 41 55  ..000000 00 NO AU
0050  54 48 45 4e 54 49 43 41  54 45 20 4c 4f 47 49 4e  THENTICA TE LOGIN
0060  20 66 61 69 6c 65 64 0d  0a                                failed..
  
```

Figure 112: Examine login activity

The second login from the insider's computer was successfully authenticated on the 3rd of December 2009 at 09:47:51.550259000. This login displays when an organisation's user attempts to access the organisation's Mail server and the Mail server authentication system is able to recognize the user. It indicates that the attacker was success in accessing the mail server. The following information is revealed from TCPDump:

Frame No. 45 Destination IP address: 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** Response: 00000002 OK [CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY UNSELECT SCAN SORT THREAD=REFERENCES THREAD=ORDEREDSUBJECT MULTIAPPEND] **User** **INSIDER AUTHENTICATED.**

Figure 113 shows that the authenticated login information is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

The screenshot displays a network traffic analysis tool interface. The top bar shows the current frame: Frame 45 (249 bytes on wire, 249 bytes captured). Below this, the arrival time is Dec 3, 2009 09:47:51.550259000. The tool provides time deltas from previous frames and the time since the first frame. The frame number is 45, and the length is 249 bytes. The capture length is also 249 bytes. The frame is not marked. The protocols in the frame are eth:ip:tcp:imap. The coloring rule is TCP, with the string 'tcp'. The frame details are as follows:

- Ethernet II, Src: c2:45:ad:57:a6:d8 (c2:45:ad:57:a6:d8), Dst: 8e:4e:01:7d:1d:6f (8e:4e:01:7d:1d:6f)
- Internet Protocol, Src: 146.227.192.2 (146.227.192.2), Dst: 146.227.128.4 (146.227.128.4)
- Transmission Control Protocol, Src Port: imap (143), Dst Port: 46009 (46009), Seq: 260, Ack: 107, Len: 183
- Internet Message Access Protocol

The packet bytes are displayed in hexadecimal and ASCII. The ASCII portion shows the start of an email header:

```

0000 8e 4e 01 7d 1d 6f c2 45 ad 57 a6 d8 08 00 45 00 .N}.o.E .W...E.
0010 00 eb 07 c0 40 00 3f 06 cd 7f 92 e3 c0 02 92 e3 ...@.?. .....
0020 80 04 00 8f b3 b9 17 8f ce 58 16 ef ea 00 80 18 .....X.....
0030 0b 50 e7 48 00 00 01 01 08 0a 00 00 d7 78 00 00 .P.H.... .x...
0040 c0 e4 30 30 30 30 30 30 30 31 20 4f 4b 20 5b 43 ..000000 01 0K [C
0050 41 50 41 42 49 4c 49 54 59 20 49 4d 41 50 34 52 APABILIT Y IMAP4R
0060 45 56 31 20 4c 49 54 45 52 41 4c 2b 20 49 44 4c EV1 LITE RAL+ IDL
0070 45 20 4e 41 4d 45 53 50 41 43 45 20 4d 41 49 4c E NAMESP ACE MAIL
0080 42 4f 58 2d 52 45 46 45 52 52 41 4c 53 20 42 49 BOX-REFE RRALS BI
0090 4e 41 52 59 20 55 4e 53 45 4c 45 43 54 20 53 43 NARY UNS ELECT SC
00a0 41 4e 20 53 4f 52 54 20 54 48 52 45 41 44 3d 52 AN SORT THREAD=R
00b0 45 46 45 52 45 4e 43 45 53 20 54 48 52 45 41 44 EREFERENCE S THREAD
00c0 3d 4f 52 44 45 52 45 44 53 55 42 4a 45 43 54 20 =ORDERED SUBJECT
00d0 4d 55 4c 54 49 41 50 50 45 4e 44 5d 20 55 73 65 MULTIAPP END] Use
00e0 72 20 69 6e 73 69 64 65 72 20 61 75 74 68 65 6e r inside r authen
00f0 74 69 63 61 74 65 64 0d 0a ..ticated.

```

Figure 113: Examine login activity

2.Email Activities:

The logs showed that there was only activity as described below:

TCPDump revealed that there was one email activity from the insider. This activity was an abusive email that sent to the victim on the 3rd of December 2009 at 09:49:01.273294000. The following summary information is revealed from TCPDump log:

Frame No. 76 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: IMF Deception: Malformed Packet.

Figure 114 shows that the TCPDump information login is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

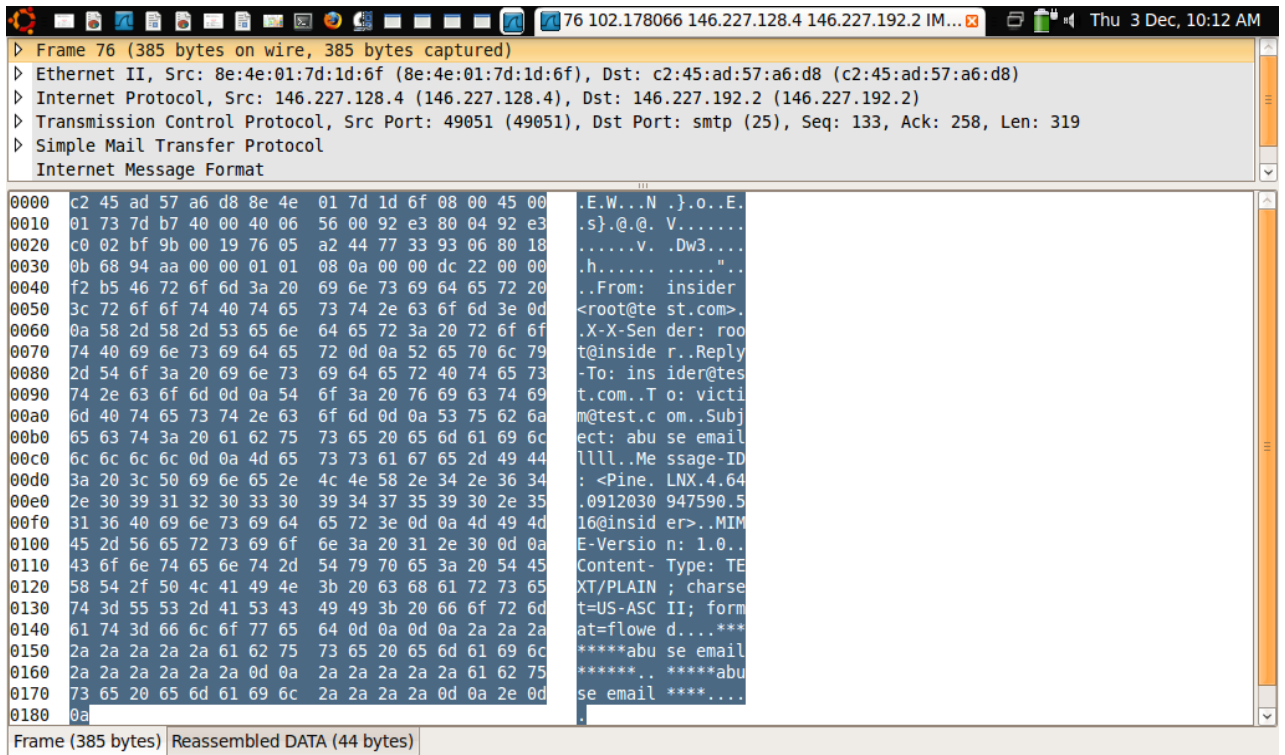


Figure 114: Examine abusive email

B1: Ex8.

The victim reported that an abusive email was received from this source: insider@test.com. The email was received on January 10, 2010 at 21:55:26.

Preliminary investigation showed that this email was sent from the insider but the insider denied the allegation of sending an abusive email. Therefore, the first step was to collect legitimate and suspicious activity of the insider from the logs and the insider's computer. Then these activities were examined in order to provide analysis process with insider's activities. The examination process provided the following information:

1.MA:

- **Insider's computer login:**

It was previously mentioned that the main advantage of enhancing the insider's password for the virtual machine (the insider's computer) is to enhance auditing/log. The “/var/log/auth.log” command is used to reveal the legitimate and suspicious login activities for the insider machine. The first suspicious activities were that there were

four failed login activities into the insider's computer. These failed logins indicated that there were illegitimate access activities. Then the attacker accessed the virtual machine. The second suspicious activities were that after the successful access to the insider computer, the insider's password was successfully changed. Figure showed that there were many failed activities. Figure 115 shows that the suspicious activities for the insider's login into the virtual machine.

```

Jan 10 18:05:00 insider login[489]: ROOT LOGIN on 'tty1'
Jan 10 18:10:24 insider login[486]: pam_unix(login;auth): check pass; user unknown
Jan 10 18:10:24 insider login[486]: pam_unix(login;auth): authentication failure
; logname=LOGIN uid=0 euid=0 tty=tty0 ruser=rhost=
Jan 10 18:10:28 insider login[486]: FAILED LOGIN (1) on 'tty0' FOR 'UNKNOWN', User
not known to the underlying authentication module
Jan 10 18:10:49 insider login[486]: pam_unix(login;auth): check pass; user unknown
Jan 10 18:10:52 insider login[486]: FAILED LOGIN (2) on 'tty0' FOR 'UNKNOWN', User
not known to the underlying authentication module
Jan 10 18:10:58 insider login[486]: pam_unix(login;session): session opened for
user guest by LOGIN(uid=0)
Jan 10 18:18:56 insider passwd[501]: pam_unix(passwd;chauthtok): new password not
acceptable
Jan 10 21:38:51 insider login[501]: pam_unix(login;auth): authentication failure
; logname=LOGIN uid=0 euid=0 tty=tty0 ruser=rhost= user=root
Jan 10 21:38:54 insider login[501]: FAILED LOGIN (1) on 'tty0' FOR 'root', Authentication
failure
Jan 10 21:39:04 insider login[501]: FAILED LOGIN (2) on 'tty0' FOR 'root', Authentication
failure
Jan 10 21:39:14 insider login[501]: TOO MANY LOGIN TRIES (3) on 'tty0' FOR 'root'
Jan 10 21:39:14 insider login[501]: pam_mail(login;session): pam_putenv: delete
non-existent entry; MAIL
Jan 10 21:39:14 insider login[501]: pam_unix(login;session): session closed for
user root
Jan 10 21:39:14 insider login[501]: PAM 2 more authentication failures; logname=
LOGIN uid=0 euid=0 tty=tty0 ruser=rhost= user=root
Jan 10 21:39:25 insider login[503]: pam_unix(login;auth): authentication failure
; logname=LOGIN uid=0 euid=0 tty=tty0 ruser=rhost= user=root
Jan 10 21:39:28 insider login[503]: FAILED LOGIN (1) on 'tty0' FOR 'root', Authentication
failure
Jan 10 21:39:36 insider login[503]: pam_unix(login;session): session opened for
user root by LOGIN(uid=0)
Jan 10 21:39:36 insider login[504]: ROOT LOGIN on 'tty0'
Jan 10 21:48:23 insider groupadd[527]: new group: name=insider, GID=1001
Jan 10 21:48:24 insider useradd[531]: new user: name=insider, UID=1001, GID=1001
, home=/home/insider, shell=/bin/bash
Jan 10 21:48:31 insider passwd[538]: pam_unix(passwd;chauthtok): password change
d for insider
Jan 10 21:48:34 insider chfn[539]: changed user `insider' information
insider:~#

```

Figure 115: Examine insider's login activity

- **Email login:**

As we have seen in the unknown attack experiment 1, the outsider had already known the insider's email password. Therefore, there was one login activity from the insider's

computer to the mail server. The login from the insider's computer was successfully authenticated on January 10, 2010 at 21:53:25.758059000. It indicated that the attacker was successful in accessing the mail server. The following information is revealed from TCPdump:

Frame No. 982 **Destination IP address:** 146.227.192.2 **Source IP address:** 146.227.128.4 **Protocol Type:** IMAP **Deception:** **USER INSIDER AUTHENTICATED.**

Figure 116 shows that the successful login information was presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and description of events.

```

Frame 982 (249 bytes on wire, 249 bytes captured)
  Arrival Time: Jan 10, 2010 21:53:25.758059000
  [Time delta from previous captured frame: 1.530018000 seconds]
  [Time delta from previous displayed frame: 9.976098000 seconds]
  [Time since reference or first frame: 1284.415303000 seconds]
  Frame Number: 982
  Frame Length: 249 bytes
  Capture Length: 249 bytes
  [Frame is marked: False]
  [Protocols in frame: eth:ip:tcp:imap]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  ▸ Ethernet II, Src: MS-NLB-PhysServer-09_4e:f4:09:a3 (02:09:4e:f4:09:a3), Dst: 72:2c:b1:93:d7:3a (72:2c:b1:93:d7:3a)
  ▸ Internet Protocol, Src: 146.227.192.2 (146.227.192.2), Dst: 146.227.128.4 (146.227.128.4)
  ▸ Transmission Control Protocol, Src Port: imap (143), Dst Port: 46062 (46062), Seq: 186, Ack: 58, Len: 183
  ▸ Internet Message Access Protocol
    0010 00 e0 0e c0 40 00 00 45 72 92 e3 c0 02 92 e3  . . . @ . . . . .
    0020 80 04 00 8f b3 ee b7 9a 8b 8d b7 9a a2 16 80 18  . . . . .
    0030 0b 50 c5 2f 00 00 01 01 08 0a 00 02 0d ff 00 01  .P./...
    0040 f6 3e 30 30 30 30 30 30 30 30 20 4f 4b 20 5b 43  .>000000 00 OK [C
    0050 41 50 41 42 49 4c 49 54 59 20 49 4d 41 50 34 52  APABILIT Y IMAP4R
    0060 45 56 31 20 4c 49 54 45 52 41 4c 2b 20 49 44 4c  EV1 LITE RAL+ IDL
    0070 45 20 4e 41 4d 45 53 50 41 43 45 20 4d 41 49 4c  E NAMESP ACE MAIL
    0080 42 4f 58 2d 52 45 46 45 52 52 41 4c 53 20 42 49  BOX-REFE RRALS BI
    0090 4e 41 52 59 20 55 4e 53 45 4c 45 43 54 20 53 43  NARY UNS ELECT SC
    00a0 41 4e 20 53 4f 52 54 20 54 48 52 45 41 44 3d 52  AN SORT  THREAD=R
    00b0 45 46 45 52 45 4e 43 45 53 20 54 48 52 45 41 44  EFERENCE S THREAD
    00c0 3d 4f 52 44 45 52 45 44 53 55 42 4a 45 43 54 20  =ORDERED SUBJECT
    00d0 4d 55 4c 54 49 41 50 50 45 4e 44 5d 20 55 73 65  MULTIAPP END] Use
    00e0 72 20 69 6e 73 69 64 65 72 20 61 75 74 68 65 6e  r inside r authen
    00f0 74 69 63 61 74 65 64 0d 0a  . . . . .
  
```

Figure 116: Examine email activity

2. Email activities:

After the examination of logins is completed, the next step is to examine email activities. The TCPdump log showed that there was only one email activity that was performed by the attacker as described below:

Email No.1:

TCPdump revealed there was one email activity from the insider. This activity was an abusive email sent to the victim on January 10, 2010 at 21:55:26. 772200000. The following summary information is revealed from TCPdump log:

Frame No. 1061 Destination IP address: 146.227.192.2 Source IP address: 146.227.128.4 Protocol Type: IMF Deception: BODY.

Figure 117 shows that the TCPdump information login is presented destination and source IP addresses; destination and source MAC addresses; destination and source port numbers; and the content of the email.

Therefore, TCPdump log showed that NBE was identified before and after the incident. Now, the corporate security should also examine the insider's computer in order to look for more evidence to support whether this attack was committed by the insider or the outsider.

```

1061 1405.429444 146.227.128.4 146.227.192.2 IMF [M... Mon 11 Jan, 11:08 PM
  > Frame 1061 (395 bytes on wire, 395 bytes captured)
  > Ethernet II, Src: 72:2c:b1:93:d7:3a (72:2c:b1:93:d7:3a), Dst: MS-NLB-PhysServer-09_4e:f4:09:a3 (02:09:4e:f4:09:a3)
  > Internet Protocol, Src: 146.227.128.4 (146.227.128.4), Dst: 146.227.192.2 (146.227.192.2)
  > Transmission Control Protocol, Src Port: 42963 (42963), Dst Port: smtp (25), Seq: 134, Ack: 258, Len: 329
  > Simple Mail Transfer Protocol
  Internet Message Format
0000 02 09 4e f4 09 a3 72 2c b1 93 d7 3a 08 00 45 00 ..N...r, ...:..E.
0010 01 7d dc e1 40 00 3f 06 f7 cb 92 e3 80 04 92 e3 .).@.?. .....
0020 c0 02 a7 d3 00 19 3f 3d f6 0d 3f 80 c5 e4 80 18 .....?= ..?.....
0030 0b 68 b3 a5 00 00 01 01 08 0a 00 02 29 6e 00 02 .h.....)n..
0040 3d 45 46 72 6f 6d 3a 20 69 6e 73 69 64 65 72 20 =EFrom: insider
0050 3c 72 6f 6f 74 40 74 65 73 74 2e 63 6f 6d 3e 0d <root@te st.com>.
0060 0a 58 2d 58 2d 53 65 6e 64 65 72 3a 20 72 6f 6f .X-X-Sen der: roo
0070 74 40 69 6e 73 69 64 65 72 0d 0a 52 65 70 6c 79 t@inside r.Reply
0080 2d 54 6f 3a 20 69 6e 73 69 64 65 72 40 74 65 73 -To: ins ider@tes
0090 74 2e 63 6f 6d 0d 0a 54 6f 3a 20 76 69 63 74 69 t.com..T o: victi
00a0 6d 40 74 65 73 74 2e 63 6f 6d 0d 0a 53 75 62 6a m@test.c om.Subj
00b0 65 63 74 3a 20 61 62 75 73 65 20 65 6d 61 69 6c ect: abu se email
00c0 0d 0a 4d 65 73 73 61 67 65 2d 49 44 3a 20 3c 50 ..Messag e-ID: <P
00d0 69 6e 65 2e 4c 4e 58 2e 34 2e 36 34 2e 31 30 30 ine.LNX. 4.64.100
00e0 31 31 30 32 31 35 34 33 32 30 2e 35 35 33 40 69 11021543 20.553@i
00f0 6e 73 69 64 65 72 3e 0d 0a 4d 49 4d 45 2d 56 65 insider>..MIME-Ver
0100 72 73 69 6f 6e 3a 20 31 2e 30 0d 0a 43 6f 6e 74 rsion: 1 .0..Cont
0110 65 6e 74 2d 54 79 70 65 3a 20 54 45 58 54 2f 50 ent-Type : TEXT/P
0120 4c 41 49 4e 3b 20 63 68 61 72 73 65 74 3d 55 53 LAIN; ch arset=US
0130 2d 41 53 43 49 49 3b 20 66 6f 72 6d 61 74 3d 66 -ASCII; format=f
0140 6c 6f 77 65 64 0d 0a 0d 0a 2a 2a 2a 2a 2a 2a 2a lowed... *****
0150 61 62 75 73 65 20 65 6d 61 69 2a 2a 2a 2a 2a 2a abuse em ai*****
0160 0d 0a 2a 2a 2a 61 62 75 73 65 20 65 6d 61 69 6c ..***abu se email
0170 2a 2a 2a 0d 0a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a ***.*** *****
0180 2a 2a 2a 2a 2a 2a 0d 0a 2e 0d 0a ***** ..
Frame (395 bytes) Reassembled DATA (45 bytes)

```

Figure 117: Examine abuse email

3.Examining and analysing insider's computer

After examining the email activities, the next step is to examine the insider's computer to identify the insider's activities. The corporate security revealed the insider's files by

using “ls” command. This command showed that NBF was created or modified before and/or after the incident. Figure 118 shows the insider’s computer activity.

```

— Starting Netkit phase 1 init script —
Mounting /home/tiger on /hosthome...
Mounting /home/tiger/test-5 on /hostlab ...
— Netkit phase 1 initialization terminated —

Starting system log daemon...
Starting kernel log daemon...

— Starting Netkit phase 2 init script —

>>> Running insider specific startup script...
>>> End of insider specific startup script.

#####

Lab directory (host): /home/tiger/test-5
Version: 1
Author: A. Al-Morjan
Email: almorjan@dmu.co.uk
Web: <none>
Description:
Re-do the Expermint 5

#####

— Netkit phase 2 initialization terminated —

Welcome to Netkit

insider login: root
Password:

Login incorrect
insider login: root
Password:
Last login: Mon Jan 11 23:20:12 UTC 2010 on tty0
insider:~# ls
.mail
insider:~# ls -a
. .*.addressbook .addressbook.lu .bash_history .bashrc .mail .pine-debug1 .pine-debug2 .pine-debug3 .pine-debug4 .pinerc .profile .viminfo
insider:~#

```

Figure 118: Examine the insider’s computer activity

Moreover, the corporate security used “ls -a” command to reveal hidden files. These hidden files will not be listed in the output of “ls” without specifying “-a” flag. This helps to find files that have been moved from their original location, or modified recently, which should support ferret out the hiding place in use by a particular attacker in a particular incident. Ls -a command showed that there was NBF was created or modified before and/or after the incident.