12-4-2013

Including Network Routers In Forensic Investigation

Brian Cusack
Edith Cowan University, brian.cusack@aut.ac.nz

Raymond Lutui
Auckland University of Technology, raymond.lutui@aut.ac.nz

DOI: 10.4225/75/57b3c682fb86d
11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

INCLUDING NETWORK ROUTERS IN FORENSIC INVESTIGATION

Brian Cusack[1,2], Raymond Lutui[1]
[1]Auckland University of Technology, Auckland, New Zealand
[2]Security Research Institute, Edith Cowan University, Perth, Australia
brian.cusack@aut.ac.nz, raymond.lutui@aut.ac.nz

Abstract
Network forensics concerns the identification and preservation of evidence from an event that has occurred or is likely to occur. The scope of network forensics encompasses the networks, systems and devices associated with the physical and human networks. In this paper we are assessing the forensic potential of a router in investigations. A single router is taken as a case study and analysed to determine its forensic value from both static and live investigation perspectives. In the live investigation, tests using steps from two to seven routers were used to establish benchmark expectations for network variations. We find that the router has many attributes that make it a repository and a site for evidence collection. The implications of this research are for investigators and the inclusion of routers in network forensic investigations.

Keywords
Router, Networks, Forensics, Evidence, Investigation

INTRODUCTION

Digital forensics concerns the investigation of any matter of information or data, stored or transmitted in a binary form that may be relied upon as evidence. As a consequence many specialist sub fields are encapsulated by digital forensics including network forensics, computer forensics, satellite forensics, browser forensics and so on (Balen, Martinovic & Hocenski, 2012). This paper concerns Network forensics and the one instance that of the router (Battisha, 2008). A network forensic investigation requires the capturing, recording and analysing of network evidence and the audit trails (Choi & Dai, 2004). The outcome of such investigations may deliver security audit, security knowledge to harden a system or evidence for legal purposes. The scope of this paper is to focus solely on the legal evidential value of the router (Cisco, 2008; Cisco, 2009). As a consequence both the static and the dynamic potential for evidence disclosure are evaluated and the systematic approach for investigation documented. Consideration is also made for including the router in the scope of investigations and as a critical component in a forensically ready computer network.

THE SCOPE OF NETWORK INVESTIGATION

Digital investigation concerns scientific tasks, techniques and practices used in the investigation of stored or transmitted binary information or data. The scope of investigation is bounded by devices and systems in which binary data is transmitted, processed and stored. The people associated with the networks and computing systems are also in scope and may provide valuable evidence and access to evidence. In these senses the deliverable from an investigation is evidence for the requirements of an IT audit, a post event system hardening, or legal action. In each instance the theoretical framework for collection and the methods for processing the evidence are different (see Figure 1). An IT audit (internal or external) is conducted to assess the performance of the security controls against benchmarks and risk criteria (Figure 1: A). These audits include forensic audit of breaches and security audits of vulnerabilities. The scope is based on the determined audit objectives; for example of security (confidentiality, integrity and availability), quality (effectiveness and efficiency), fiduciary (compliance and reliability), service and capacity (Cui, Xu, Xu, & Wu, 2002). The outcome of an IT Audit is a report that addresses the audit objective. Security audit and Digital forensic investigation overlap in the area of post-event evaluation (see Figure 1: B). Security audit provides an explanation of an event in terms of the variation around controls and can show system strengths, the untreated residual risks, and the vulnerabilities. The security audit report provides guidance for the IT developers on how they should harden the system against future attack and to

implement system improvement in IT terms. In the same space Digital forensic investigation may also occur to explain the same event in terms of the legal consequences. The consequences may be to prosecute an attacker, defend against prosecution or any other related legal action. The output of such investigation is a technical report that is prepared in accordance with the rules for an expert witness and using professional processes that are compliant with the admissibility of evidence to courts. This report has different criteria and evidence collection methods than a report for system improvement and may be equally applied to areas B and C (see Figure 1: C). The legal report from area C may be used for civil or criminal matters or for prosecution or defence of matters. In this paper we are principally concerned with investigation that is compliant with area C of Figure 1 and the inclusion of router evidence in the scope the investigation.

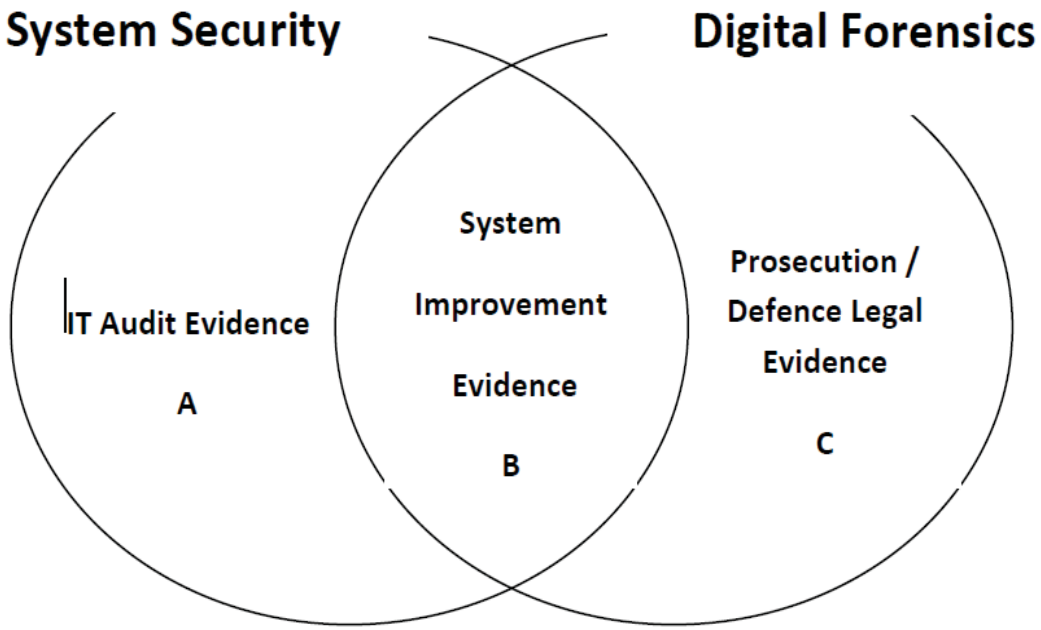


Figure 1. Classification by Use of System Investigation Evidence

Network forensics has traditionally focused on the capture, recording and analysis of network events in order to discover evidential information about the source of security attack (Feng & Hamdi, 2009; Fernandez, Pelaez & Larronodo-Petrie, 2007). This view of network forensics fits area B of Figure 1 and reflects the function of digital forensics to provide evidence for the improvement (hardening) of the security system. Unlike computer forensics that mainly deals with imaging static evidence in physical devices such as hard drives, memory sticks and other digital repositories; traditional network forensics is live and largely deals with network packet filters, firewalls and wireless frames (Gottlieb, Greenberg, Rexford & Wang, 2003). However, such a scope better fits area B of Figure 1. In area C of Figure 1 the scope of network forensics requires the investigator to have the ability to determine the full extent of network related evidence that is inclusive of the network, the devices and systems associated and the people involved. Such a scope is wider than the traditional view of network forensics and involves theoretical frameworks that are IT related, legally related and mediating mechanisms to facilitate differences. The focus of such investigation requirements extends the scope of network forensic investigation into multi-disciplinary domains and towards multi-tasking outcomes based on the classification by use of system investigation evidence (Hiromori, Yamaguchi, Yasumoto, Higashinoz & Taniguchi, 2003).

> *"This is the time to change our focus from the negative (hacker) to the positive (Internet Forensics specialist) dimension of this exciting new discipline"* (Hyung & Kang, 2011).

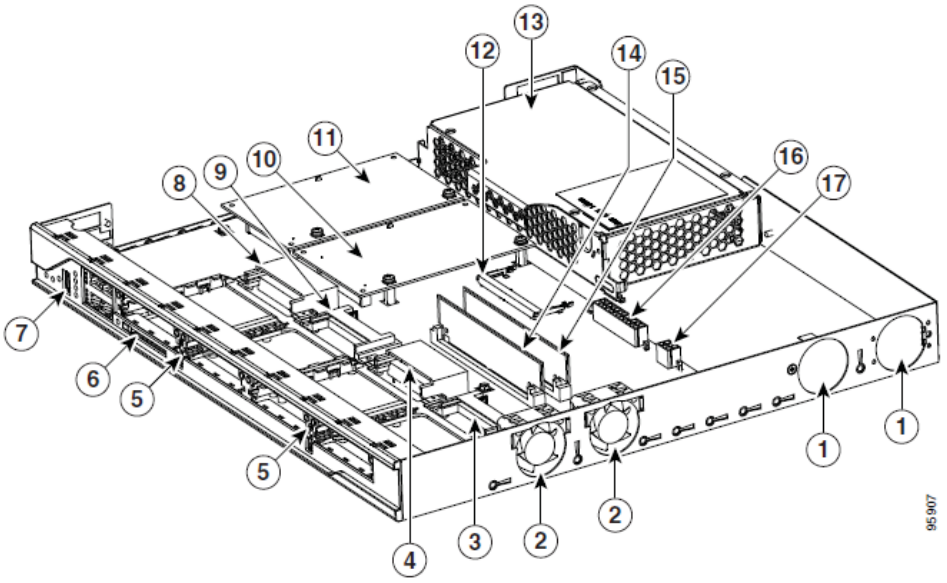
The current scope of network forensics is to be inclusive of social networks and to consider the preparation of a network for investigation (Kadloor, Gong, Kiyavash, & Venkitasubramaniam, 2010). The scope includes both static and live evidence and consequently techniques for the forensic processes of collection, examination, analysis and reporting of digital evidence must be appropriate respectively for both (Lammle, 2011a & b). The gathering of digital evidence in area C requires preparation for presented in a court of law. The implication is for integrity and cost efficiency. The volume of evidence available in a computer network is often far greater than the resources available to collect and preserve everything and the nature of many network components (such as memory repositories routers or intrusion detection systems) is such that much evidence is volatile and only momentarily available. Investigation procedures must comply with the standards of evidence for the identification and acquisition of digital evidence, preserving the integrity of the acquired evidence, forensic analysis or examination of acquired evidence, and the presentation and reporting of the obtained digital evidence in an appropriate manner (Lijun, Dan, Zhang & Rayehauduri, 2011). Forensically ready systems have designed sub-systems to collect acceptable evidence and to minimise the cost of such activity (McHugh, McLeod & Nagaonkar, 2008). An organisation may also have a strategic goal to prosecute attackers or to have sufficient evidence available of prioritised organisational activities so that effective and cost effective defences may be made. In such situations preparing a computer network for evidential purposes is within the scope of network forensics and prudent in the expectation of digital investigations.

ROUTER ARCHITECTURE

In our study we focused on one router from the Cisco 2800 series as a case study for static and live analysis. These routers were readily available in the laboratory and were used as a proxy to establish a general method for router investigations and to evaluate the evidential worth.

Static Analysis

A router is a network device that forwards data packets to other components of a computer network. Fundamentally the router receives incoming data packets, reads the header information, determines a destination and then forwards packet appropriately (McMillan, 2011). The determination of destination is made by the embedded routing table for the particular router (Misra & Kharoliwalla, 2001). The function of the router is operational in two planes; the control plane that uses a stored routing table and the physical interface connections or static routes, and the forwarding plane that manages the reading of incoming packets and the correct forwarding actions. The subject of static analysis is hence the physical router and its architecture (Murakami, Kai, Irie, & Sasaki, 2009).



1	ILP fan vents/vent blocking plate	10	AIM 0
2	System fans	11	AIM 1
3	VIC or VWIC connector	12	DIMM socket
4	VIC, VWIC, WIC, or HWIC connector	13	Mainline power supply
5	Card guide center rail	14	PVDM 1
6	External CompactFlash memory card slot	15	PVDM 0
7	Universal serial bus (USB) port	16	Main power supply connector
8	VIC, VWIC, WIC, or HWIC connector	17	ILP supply connector
9	VIC, VWIC, or WIC connector		

Figure 2. Cisco 2800 series Case Router Architecture [4]

The static analysis of the case router shows (Figure 2) many components that have fault value in areas A and B of Figure 1 and four that can act as repositories of stored information for an area C investigation. Components 6, 12, 14 and 15 (Figure 2) are memory chips of different types and of different worth to the functionality of a router. A series 2800 Cisco router has 64MB or 128MB of flash memory and 256MB of DRAM memory. In addition any of these slots may be customised with alternative capacities for memory. Modern routers have increased static and dynamic RAM buffers to enhance the performance of router path calculations and improve the general through put of packets (Narayan, Lutui, Vijayakumar & Sodhi, 2010). Although these enhancements have been made for performance reasons the benefit is also for static retention of evidence buffer load by buffer load. Simple RAM dump evidence collected using a number of different software and the potential for further research into sequences of buffer dumps in live acquisition is apparent.

Live Analysis

The functional value of a router is to principally receive, read headers, calculate the optimal address for forwarding, and to forward the data packets. Traditionally the role of network forensics has been in the monitoring and live acquisition of data packets. The objective is not only to detect exceptions but to attempt to trace back to the source of the event. Most exceptions are complex events where attempts have been made to hide the evidence required to prosecute an attacker. At best defensive actions may be taken to block traffic by profile identification, load balancing or header sniffing. Where the origin of a packet is hidden by spoofing the source IP addresses different IP traceback mechanisms were developed and most of them fall into the four main categories of; link-testing-hop-by-hop tracing, messaging, logging and packet marking'[22, 23]. These traceback mechanisms

were developed according to various situations and most of them depend on collecting a huge amount of packets from the routers along the attacking path. Without collecting sufficient packets, tracing back the hackers is extremely hard and sometimes impossible. Although trace back mechanisms can be very effective and precise in tracing back the hackers, it may be too costly and complicated to implement. Instead of collecting the stream of packets from the routers to reconstruct the attacking path, the Time-To-Live (TTL) field within theIP packet provides another source of valuable information for the investigators and is often called the hop count distance method. The method only requires one packet and identification of the originating Operating System (OS) in order to trace back to the nearest originating router (Cisco, 2008).

METHOD

In order to test the value of a router in static analysis only one router is required (Sabir, Fahiem & Mian, 2009). Principally the identification of storage repositories, the relative capacities, refresh rates and allocation algorithms are sufficient to fit an investigation scope. However, live forensic acquisition is more complex and requires many networked routers. In this research we selected Cisco 2800 series routers because they were available in the laboratory and they supported dynamic routing in IPv6 (Sarikhani, Mahranian & Hoseini, 2010). The network architecture was kept simple and started with two routers (see Figure 4) and was then scaled up to four and seven routers. Of the many factors influencing live analysis we selected measures of throughput in relation packet size, routing protocol and the number of routers as being helpful in establishing normal network behavioural patterns. Further testing measured delays (Jitter) in the processing of packages. Such a metric has value in locating exceptions from the benchmark baseline.

In the test bed the sender, receiver and two Cisco routers were connected in series using crossover cable. A megabit switch was squeezed in between sender and receiver to keep the data transmission to a maximum of 100 Mbps, as the crossover cables and network cards on sender, receiver and on routers is Gigabit capable.

The Hardware specification of both sender and receiver was:

Processors:	Intel Core 2 Duo, CPU 6300 @ 1.86GHz
RAM:	Module 1 - DDR2, 1024 Mbytes Module 2 - DDR2, 1024 MBytes
Network Card:	Broadcom 1 G/bit adapter. Intel Pro S/1000 (1 G/bit) adapter

Since Cisco Routers support multiple protocols (IPv4 & IPv6) on same interface we have configured IPv4 and IPv6 addresses on each interface of both Cisco Routers. Similarly both Routers are running RIP and RIPng simultaneously for IPv4 and IPv6 routing. In this test we have installed Server 2008 on both sender and receiver (Seong & Reddy, 2008). There is no particular reason for choosing Server 2008 as we can use any Operating System for testing. The log server was removed as both sender and receiver can act as the log servers. There were no other settings changed to enhance the Operating System's performance (Telidevara, Chandrasekaran, Srinivasan, Mukkamala & Gampa, 2010).

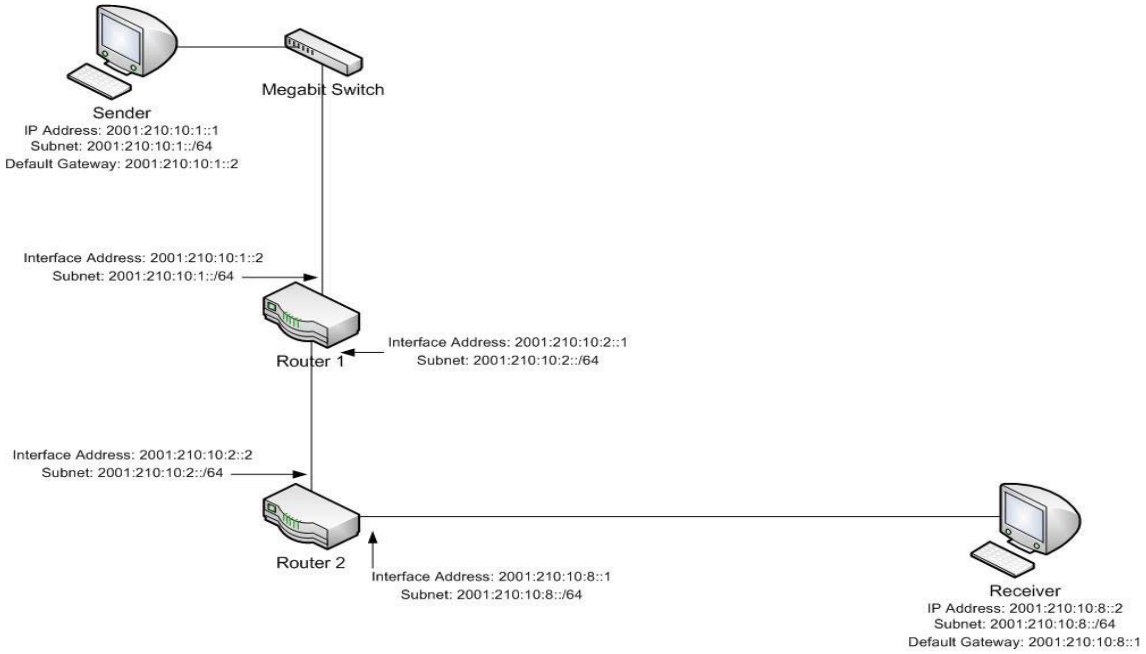


Figure 3. Live acquisition test bed

FINDINGS

The evaluation of the case proxy router for its evidential value showed both static and live potential for evidence collection. The ways a router has been customised in terms of the physical hardware, the logicware and the options that are being used (such as security and intrusion detection settings) adds variation to the amount and extent of evidence that may be available. The two problems arising in the research that have implications for investigators are the volatility of data in the static analysis and the immense volume of data in the live analysis. Evidence from investigation is hence a sub set of all possible evidence and consequently the methods and limitation of the evidence collection methods require declaration in the area C report.

Static Analysis

The principal challenge for an investigator in a static system analysis is the volatility of the data to be collected. Memory dumps may be obtained (using software such as HelixPro and others) but not all the evidence on a system is going to last very long. What is stored and how it is stored can be determined from the software configurations but the actual content value will only be a snapshot of the most recent events. Some evidence resides in storage that requires a consistent power supply; other evidence may be stored in memory that is continuously changing or being overwritten. When collecting the evidence in the experiment, we prioritised by volatility from the highest to the lowest and resolved Table 1 for a best practice guide.

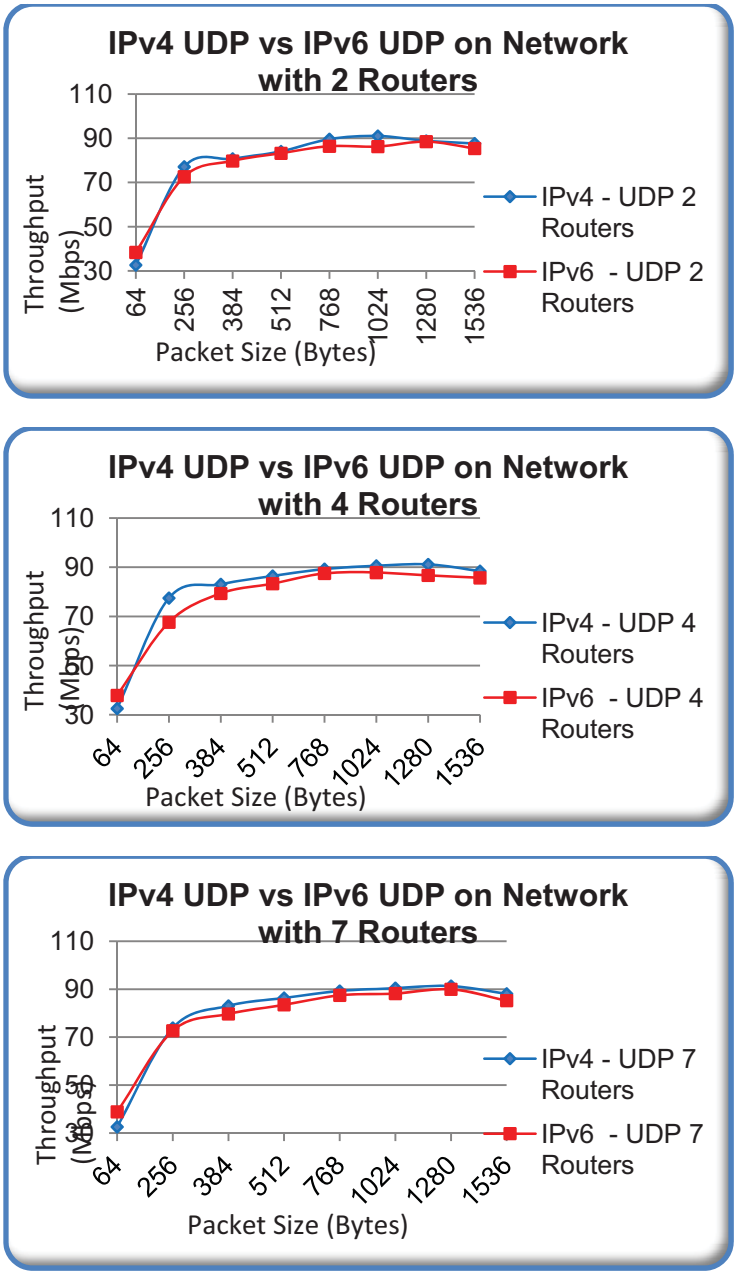
Table 1. Router evidence collection priorities by volatility

Order	Element
1	Registers and cache
2	Routing tables
3	Arp cache
4	Process table
5	Kernel statistics and modules
6	Main memory
7	Temporary file systems
8	Secondary memory
9	Router configuration
10	Network topology

Live Analysis

In the experiment matters that have been tested by other researchers were accepted as complete (for example TTL field metrics, traceback and so on) (Paruchuri, Durresi & Chellappan (2008); Pilli, Joshi & Niyogi, 2011a & b); and valuable to our research. Our focus was to test for other variations that have an influence on the identification of network evidence and to report measures that show the expected variations as benchmark measures (Vacca, 2005; Wei, 2005). The approach was designed to add knowledge that an investigator should consider within the scope of a router investigation. It is to minimise the inclusion of false leads (positive and negative) in an investigation. Consequently the results for UDP and TCP benchmarking are reported here, and the Jitter values of expect delays for a router noted (Yan & Sik, 2010; Zhou, Fei, Narayan, Haeberlen, Loo & Sherr, 2011).

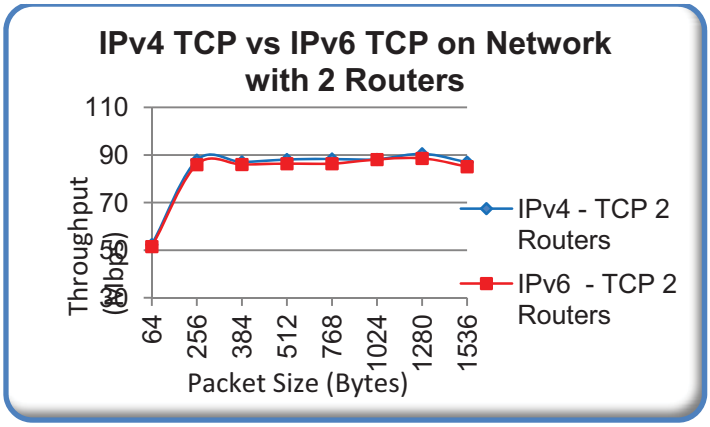
UDP Benchmarking

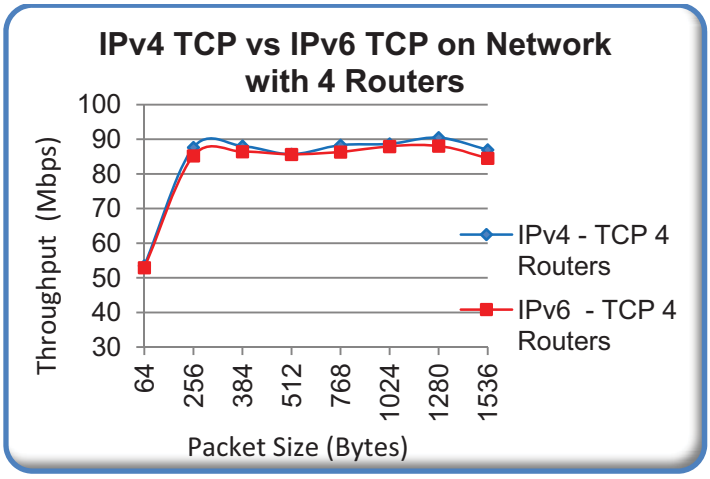


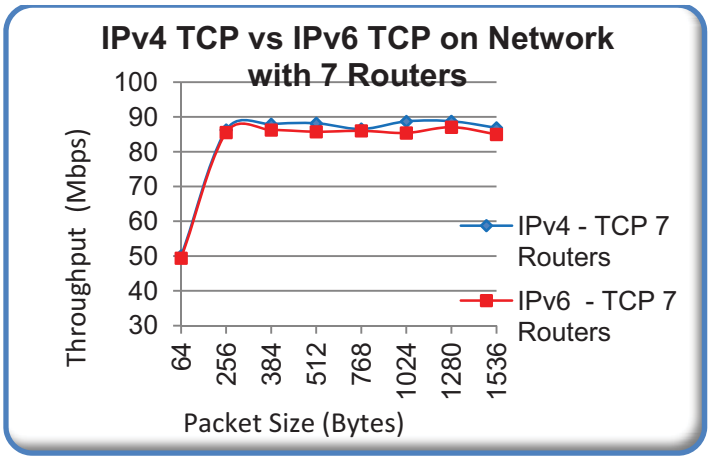
Charts 1-3. UDP Router performance

For the smallest packet size, UDP 64 Bytes, UDP IPv6 always gives 15% more throughput than IPv4 on all network setups. With the 2 router network, packet sizes 256, 768 and 1024 Bytes, IPv6 performance dropped by 5%. The rest of the packet sizes are very similar in regards to throughput values. On the network with 4 routers, packet sizes ranging from 256 to 1536 Bytes, IPv6 performance dropped by 10%. On the network with 7 routers, for all packet sizes ranging from 256 to 1536 Bytes, IPv6 performance dropped by 3%. From these results, it can be concluded that as the packet size increases, IPv6 performance degrades as compared to IPv4. These variations require consideration in live forensic evidence collection as a standard router performance will necessarily vary within the overall network performance and also in relation to other factors identified in the experiment. Tuning of detection systems and mining algorithms can minimize false positives and negatives in live analysis.

TCP Benchmarking







Charts 4-6. TCP Router performance

In a network with 2 Routers and a smaller packet size ranging from 64 to 384 Bytes IPv4 shows 1% higher throughput than IPv6. For rest of the packet sizes ranging from 512 to 1536 Bytes IPv4 shows 2% higher throughput than IPv6, except for the packet size of 1024 Bytes, where both IPv4 & IPv6 has similar throughput. In a network with 4 Routers IPv4 shows 2% higher throughput than IPv6 for packet size ranging from 64 to 384 Bytes. For the packet size of 512 Bytes both IPv4 and IPv6 has similar throughput. Similarly, for the packet size ranging from 768 to 1536 Bytes IPv4 throughput is 2% higher than IPv6 except for the packet size of 1024 Bytes, where the difference is 1%. In a network with 7 Routers IPv4 shows 1% higher throughput than IPv6 for the packet sizes ranging from 64 to 1536 Bytes, except packet size of 768 Bytes where both shows similar throughput. Therefore it can be concluded that IPv4 outperforms IPv6 by 2 percent.

These variations for protocol, packet size and network complexity require consideration in live forensic evidence collection as a standard router performance will necessarily vary within the overall network performance and these factors identified in the experiment. Tuning of detection systems and mining algorithms can minimize false positives and negatives in live analysis.

Packet Delay Benchmarking

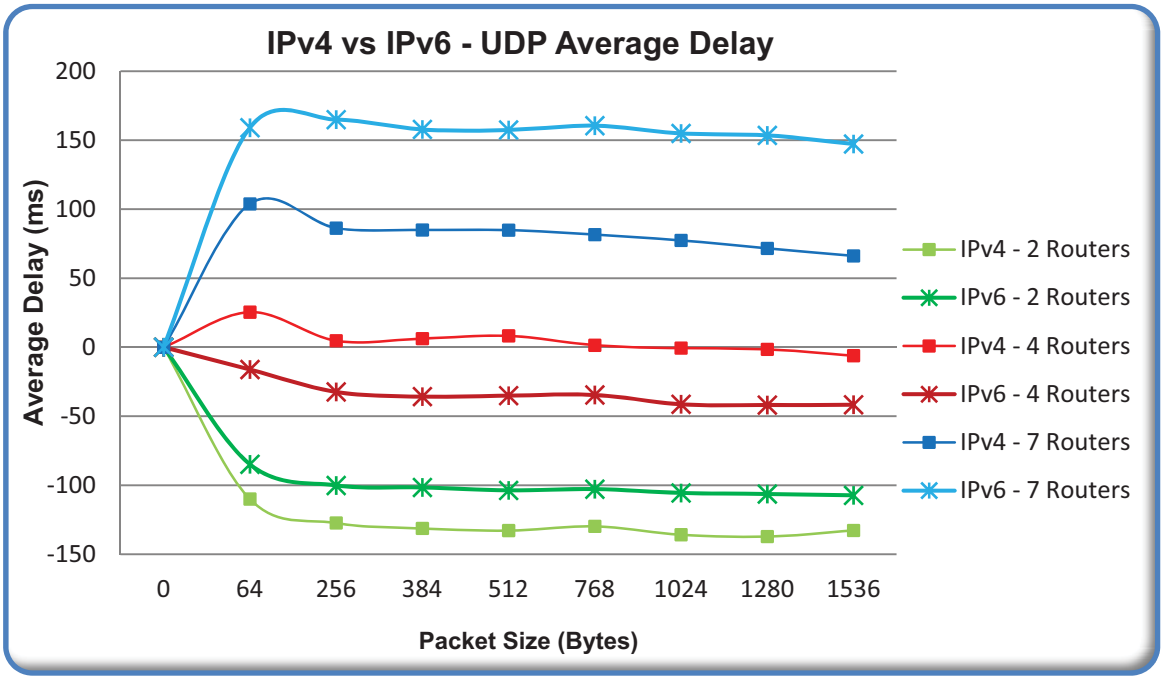


Chart 7. UDP Packet Delay

A network of 2 routers using UDP as the transport protocol, IPv6 has an average of 30 milliseconds more delay irrespective of packet size than network of 2 routers running on IPv4. In a network of 4 routers, also using UDP as transport protocol, IPv4 has an average of 50 milliseconds less delay irrespective of packet size than network of 4 routers running on IPv6. When increasing the number of network nodes to 7 routers, the network running on IPv6, using UDP as transmission protocol, it has a similar performance to a network running on IPv4 with the same number of nodes (Routers). IPv6 has an average of 75 milliseconds more delay. Based on all of the above statements, it can be concluded that, as the number of network nodes increases, IPv6 protocol generates more delays than IPv4 protocol. These delays for an expected distribution and events falling outside of these benchmarks may be interpreted as exceptions. Such exceptions require investigation whereas the values within the expected distribution may only require content analysis.

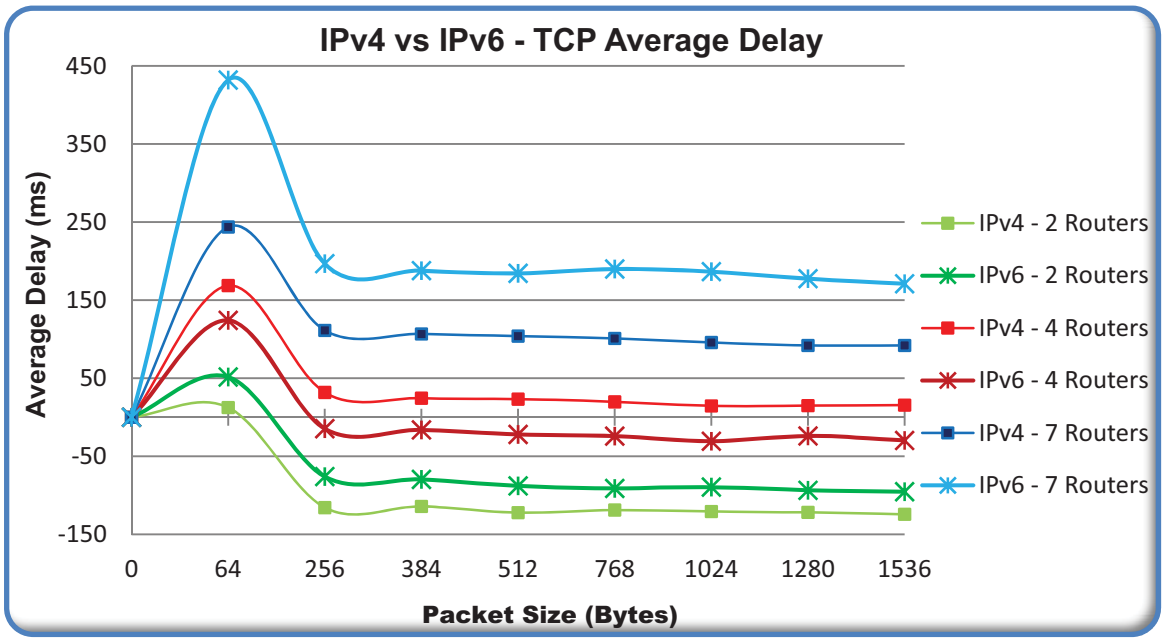


Chart 8. TCP Packet Delay

A network of 2 routers using TCP as transport protocol, IPv6 has an average of 34 milliseconds more delay irrespective of packet size than a network of 2 routers running on IPv4. In network of 4 routers, also using TCP as the transport protocol, IPv4 has an average of 42 milliseconds less delay irrespective of packet size, than network of 4 routers running on IPv6. When increasing the number of network nodes to 7 routers, the network running on IPv6, using TCP as transmission protocol again has more average delay than the IPv4. For a packet size of 64 Bytes in particular, IPv6 generated an average of 228 milliseconds more than IPv4. For larger packet sizes (256 to 1536 Bytes), a network running on IPv6 generated an average of 105 milliseconds more than a network of 7 Routers running using IPv4 protocol as transport protocol.

Based on all of the above statements and the relevant charts,it can be concluded that, as the number of network nodes increases, irrespective of packet size, IPv6 protocol generates more delays than IPv4 protocol. These are delays for an expected distribution and events falling outside of these benchmarks may be interpreted as exceptions. Such exceptions require investigation whereas the values within the expected distribution may only require content analysis. Our research helps an investigator to focus where to look for evidence, to filter out controlled system variations and to prioritise the use of resources.

CONCLUSION

The scope of digital investigation and network forensics ought to include routers. We have shown that from both a static and a live perspective valuable evidence may be found in routers. Our tests have shown that various factors contribute to network performance and these variations can be expected in the normal function of a computer network. Hence normal variations that are in control can be filtered out of focus for investigation and the technical resources applied for analysis of critical system attributes. Exceptions to the benchmarks (that must be established for each network) and content analysis require inclusion in investigations. We find that the router has many features that may assist the retention and identification of evidence when the all the features are switched on or programmed. The implications of this research extend beyond enhancing the scope for network investigations and into advice for preparing a forensically ready network. Further research is to be done to sequentially examine memory dumps in scenario testing and to write a best practice forensic readiness assurance guideline for network managers.

REFERENCES

Balen, G. Martinovic, M. and Hocenski, Z. (2012)."Network performance evaluation of latest windows operating systems," in Software, Telecommunications and Computer Networks (SoftCOM), 20th International Conference, pp. 1-6.

Battisha, M. (2008)."A framework for collection and correlation of network forensic evidence for quality of service degradation," 3352056 Ph.D., University of Louisville, Kentucky, USA.

Choi, H. and Dai, H. (2004). "A marking scheme using Huffman codes for IP traceback," Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks, pp. 421-428.

Cisco.Systems (2008), "Route Selection in Cisco Routers," in IP Routing, ed: Cisco.Systems.Inc, pp. 1-6.

Cisco.Systems.Inc, (2009). "Performance Routing (PfR) Integration," in IP Video Surveillance Whitepapers, ed. CA 95134-1706, USA: Cisco Systems.Inc, pp. 1-14.

Cui, Y..Xu, K. Xu, M. and Wu, J. (2002)."Stress testing of OSPF protocol implementation based on large-scale routing simulation," 10th IEEE International Conference on Networks, pp. 63-68.

Feng, J. and Hamdi, M. (2009). "Memory Subsystems in High-End Routers," Micro, IEEE, vol. 29, pp. 52-63.

Fernandez, E. Pelaez, J. and Larrondo-Petrie, M. (2007) "Attack Patterns: A New Forensic and Design Tool," in Advances in Digital Forensics III. vol. 242, P. Craiger and S. Shenoi, Eds., ed: Springer New York, pp. 345-357.

Gottlieb, J. Greenberg, A. Rexford, J. and Wang, J. (2003). "Automated provisioning of BGP customers," Network, IEEE, vol. 17, pp. 44-55.

Hiromori, A. Yamaguchi, H. Yasumoto, K. Higashinoz,T. and Taniguchi, K. (2003). "Reducing the size of routing tables for large-scale network simulation," Proceedings. Seventeenth Workshop on Parallel and Distributed Simulation, , 2003, pp. 115-122.

Hyung K. and Kang, K. (2011). "Network Forensic Evidence Acquisition (NFEA) with Packet Marking," Proceedings of the Parallel and Distributed Processing with Applications Workshops (ISPAW), pp. 388-393.

Kadloor, S. Gong, X. Kiyavash, N. and Venkitasubramaniam, P. (2010)."Designing router scheduling policies: a privacy perspective," Proceedings of the 17th ACM conference on Computer and communications security, Chicago, Illinois, USA.

Lammle, T. (2011a). CCNA Cisco Certified Network Associate Study Guide, 7th Edition : Cisco Certified Network Associate Study Guide (640-802) (7 ed.). Available: http://AUT.eblib.com.au/patron/FullRecord.aspx?p=675116

Lammle, T. (2011b). CCNA Cisco Certified Network Associate Study Guide, 7th Edition : Cisco Certified Network Associate Study Guide (640-802) (7 ed.). Available: http://AUT.eblib.com.au/patron/FullRecord.aspx?p=675116

Lijun, D. Dan, Z. Zhang, Y. and Raychaudhuri, D. (2011). "Performance evaluation of content based routing with in-network caching," Proceedings of the Wireless and Optical Communications Conference (WOCC), pp. 1-6.

McHugh, J. McLeod, R. and Nagaonkar, V. (2008). "Passive network forensics: behavioural classification of network hosts based on connection patterns," SIGOPS, vol. 42, pp. 99-111.

McMillan, T. (2011). Cisco Networking Essentials (1 ed.). Available: http://AUT.eblib.com.au/patron/FullRecord.aspx?p=817836

Misra, K. and Kharoliwalla, F. (2001)."Study of Internet Router Architectures," Technical report, Michigan State University.

Murakami, M. Kai, T. Irie, H. and Sasaki, R. (2009). "Extension and Evaluation of IP Traceback Method Using Departure Stamp in Edge Router," Computer Science and its Applications, pp. 1-8.

Narayan, S. Lutui, P. Vijayakumar, K. and Sodhi, S. (2010). "Performance analysis of networks with IPv4 and IPv6," in Computational Intelligence and Computing Research (ICCIC), pp. 1-4.

Paruchuri, V. Durresi, A. and Chellappan, S. (2008). "TTL Based Packet Marking for IP Traceback," in Global Telecommunications Conference, IEEE, pp. 1-5.

Pilli, E. Joshi, R. and R. Niyogi, (2011a)."Router and Interface Marking for Network Forensics," in Advances in Digital Forensics VII. vol. 361, G. Peterson and S. Shenoi, Eds., ed: Springer Berlin Heidelberg, pp. 209-220.

Pilli, E. Joshi, R. and Niyogi, R. (2011b) "Data reduction by identification and correlation of TCP/IP attack attributes for network forensics," presented at the Proceedings of the International Conference & Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India, 2011.

Sabir, M. Fahiem, M. and Mian, M. (2009). "An Overview of IPv4 to IPv6 Transition and Security Issues," Communications and Mobile Computing, pp. 636-639.

Sarikhani, A. Mahramian, M. and Hoseini, H. (2010). "Calculation of Cisco router processing power for a large network with thousands of nodes," Signal Processing Systems (ICSPS), pp. V3-757-V3-762.

Soo, K. and Reddy, A. (2008)."Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data," Networking, IEEE/ACM Transactions, vol. 16, pp. 562-575.

Telidevara, T. Chandrasekaran, V. Srinivasan, A. Mukkamala, R. and Gampa, S. (2010). "Similarity coefficient generators for network forensics," Information Forensics and Security (WIFS), IEEE International Workshop, pp. 1-6.

Vacca, J. (2005). Computer forensics: computer crime scene investigation vol. 1: Delmar Thomson Learning.

Wei, R. (2005). "Toward global Internet services to defend against DDoS by dynamic possibility-based packets marking trace back," Services Systems and Services Management, Vol. 1, pp. 589-592.

Yan S. and Sik, K. (2010)."A Hybrid Approach to CAM-Based Longest Prefix Matching for IP Route Lookup," Proceedings of the Global Telecommunications Conference, pp. 1-5.

Zhou, W. Fei, Q..Narayan, A. Haeberlen, B. Loo, T. and Sherr, M. (2011). "Secure network provenance," Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, Cascais, Portugal.