January 2015

Web Based Cyber Forensics Training For Law Enforcement

Nicholas A. Sturgeon
Purdue University

Graduate School Form 30
Updated 1/15/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Nicholas A. Sturgeon

Entitled
WEB BASED CYBER FORENSICS TRAINING FOR LAW ENFORCEMENT

For the degree of Master of Science

Is approved by the final examining committee:

Dr. Marcus Rogers
Chair

Dr. John Springer

Dr. J. Eric Dietz

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Dr. Marcus Rogers

Approved by: Jeffrey Whitten 11/29/2015
Head of the Departmental Graduate Program Date

WEB BASED CYBER FORENSICS TRAINING FOR LAW ENFORCEMENT

A Thesis

Submitted to the Faculty

of

Purdue University

by

Nicholas A. Sturgeon

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

December 2015

Purdue University

West Lafayette, Indiana

This is dedicated to my wife Heather and our three beautiful daughters. Without your continued encouragement and support, I could not have come close to completing this degree. The commitment you made to put our lives on hold for these two years is greatly appreciated. Thank you for all your patients, love and support during this journey**.**

ACKNOWLEDGEMENTS

There are several acknowledgements that have to be made. First and foremost I want to take the time to acknowledge and thank the Indiana State Police Department (ISP) for being flexible and working with me while I was pursing this degree. The flexibility allowed me to adjust my work schedule around the crazy class schedule. Secondly, I specifically want to thank ISP Sgt. Brian Bunner and F/Sgt. Don McCay for the many conversations and lending their expertise, which has truly been beneficial to my research. Next, I want to thank Dr. Sam Liles for his mentorship, for his straight forward approach to teaching and for pushing me to think at a higher level. I truly appreciate your leadership and friendship. I want to thank the members of my committee, Dr. Eric Dietz, Dr. John Springer and Dr. Marcus Rogers. Thank you all for helping me grow as a researcher. Additional thanks to Dr. Marcus Rogers for his support and guidance over the course of this degree. It was his suggestion that lead me down the path to complete the work on this thesis. I also have to thank my programmer buddies John Burns, Jamison Hemmert and John Lambert for their assistance in the development of the web pages used for this research. As well I want to thank all the Eric Katz and the other Cyber Forensic and CERIAS students that I have meet and become friends with. The conversations and discussions have been truly enlightening.

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

Table Page

Appendix Table

Appendix Table Page

LIST OF FIGURES

Figure Page

Appendix Figure

Appendix Figure Page

LIST OF ABBREVIATIONS

CBK: Common Body of Knowledge

CF: Cyber Forensics

CSV: Comma Separated Value

CRIME: Computer-Related Investigations, Management and Education

DB: Database

DF: Degrees of Freedom

DEM: Denominator

DET: Digital Evidence Triage

GAO: Governmental Accounting Office

IPAC: Indiana Prosecuting Attorney Council

HTML: Hypertext Markup Language

ISP: Indiana State Police

IT: Information Technology

LEA: Law Enforcement Agency

LEO: Law Enforcement Officers

LMS: Learning Management System

KSA: Knowledge, Skills, Abilities

NBT: Narrative Based Learning

NIST: National Institute of Standards and Technology

NSTISSC: National Security Telecommunications and Information Systems Committee

OS: Operating System

NUM: Numerator

PBL: Problem Based Learning

PD: Police Department

PHP: Hypertext Preprocessor

RBL: Resource Based Learning

SD: Standard Deviation

SE: Standard Error

SEM: Standard Error Mean

SP: Special Publication

GLOSSARY

Andragogy: is a theory which is vastly in contrast to the traditional pedagogical model and it advocates both the self-directed learning concept and the teacher as the facilitator of learning (Knowles, 1990).

Aptitude: is defined as: “(1) The quality of being apt or appropriate; fitness; (2) natural tendency or inclination; (3) a natural ability or talent; (4) quickness to learn or understand.” (Webster, 1988, p. 68).

Digital Evidence Triage: The on-scene examination of potential digital evidence.

Ontology and ontology: Ontology is a systematic account of existence, and ontology describes a situations where classification schemes are being built (Brinson, Robinson & Rogers, 2006).

Problem Based Learning (PBL): An approach that requires learners to collect information in a self-directed manner in order to learn the necessary knowledge that will assist them to discover, analyze and solve realistic problems.

Tacit knowledge: As defined by Sternberg and Hedlund “is generally unspoken knowledge which distinguishes the more expert individual in a particular domain and that reflects the practical ability to learn from experience (as cited by Taylor et al., 2013)”

ABSTRACT

Sturgeon, Nicholas A. M.S., Purdue University, December 2015. Cyber forensics web based training for law enforcement. Major Professor: Rogers, Marcus.

Training and education are two of the most important aspects within cyber forensics. These topics have been of concern since the inception of the field. Training law enforcement is particularly important to ensure proper execution of the digital forensics process. It is also important because the proliferation of technology in to society continues to grow at an exponential rate. Just as technology is used for good there are those that will choose to use it for criminal gains. It is critical that Law Enforcement have the tools and training in cyber forensics. This research looked to determine if web based training was a feasible platform for cyber forensics training. A group of Indiana State Police Troopers were asked to participate in an online study where they were presented cyber forensics training material. That study showed that there was statistical significance between the treatment groups and the control group. The results from the study showed that web based training is an effective means to train a large group of law enforcement officers.

Keywords: Web Based, Cyber Forensics Training, and Law Enforcement.

CHAPTER 1. INTRODUCTION

What does the cyber investigator of the future look like? What training, skills, tools, and challenges will these cyber investigators have? With the capabilities of technology doubling approximately every 24 months (Moore, ND) what changes are current cyber investigators going to have to make, what type of training and education will they need to have to keep up with these changes? Digital forensics training and education is one issue that had been written on and discussed going back to the beginning of the field. With that being said it seems that there has been little progress in addressing those issues.

As pointed out by Brinson, Robinson and Rogers (2006), "The one area that seems to be lacking in this research is what exactly the people involved in cyber forensics are supposed to do to prepare them, not the discipline. How do they specialize or certify themselves? (p. 6)" Training and education was listed as one of the 10 critical priorities of law enforcement when dealing with electronic crime (Stambaugh et al., 2001). The article states that "law enforcement officers and forensic scientist need specific training and certification to correctly carry out their respective roles when investigating electronic crime (Stambaugh et al., 2001, p. 3)." What does this actual mean for Law Enforcement Agencies?

1.1 Statement of the problem

The beginning of Cyber Forensics in law enforcement started in the late 1990's and into the early 2000's. Cyber Forensics is the scientific methods or processes of collecting digital evidence (SWGDE, 2001). Specifically in this domain, one of the continual problems for Law Enforcement has been with training. In 2001, Cyber Forensics training was one of the top 10 problems facing law enforcement (Stambaugh et al., 2001). The issue with training has not gone away. As well the use of technology has exponentially increased since 2001. In 2014 a mobile technology fact sheet was published online. This fact sheet contained findings from the Pew Internet Project. This project conducted research on mobile technology. There were 2008 individuals who took the survey. Some of the key findings from the survey included (Pew, 2014):

- October 2014:
    - American adults who owned a smartphone was at 64%.
- January 2014:
    - American adults who owned a cell phone was at 90%.
    - American adults who owned an e-reader was at 32%.
    - American adults who owned a tablet computer was at 42%.

This fact sheet also included a table from a 2013 survey the Pew Research Center conducted. This specific survey had 2076 respondents. The survey was to check the some of the more popular activities of Americans when it came to the use of their cell phones (Duggan, 2013). Table 1.1 lists those eight (8) popular activities from that Pew Research Center survey.

Table 1.1: Popular Cell Phone Activities

Cell phone activities % of cell phone owners who use their cell phone to…	
81	Send or receive text messages
60	Access the internet
52	send or receive email
50	download apps
49	get directions, recommendations, or other location-based information
48	listen to music
21	participate in a video call or video chat
8	"check in" or share your location

First, there are a number of different cyber forensics software applications. Second, there is a wide variety of training programs offered. In many cases, companies that develop these applications will provide training courses on the use of the software or applications. Both the initial cost of these applications and the annual licenses are expensive. With some companies, the cost of the software includes the cost of their training courses. Law Enforcement Agencies (LEA) operate on fixed budgets. Funding for training, in general, is competing against cars, guns, bullets, and gas. When an agency does spend money on cyber forensics training, the number of officers they can send is limited. Finally, consideration must be taken with the methodologies by which these courses are taught. The approach these companies take can have a drastic impact to the practical use of their software, by those trained officers.

1.2 Scope

There are three topic areas on which this research was focused on. The primary area and the basis for this research was in cyber forensics training. Specifically, this was narrowly focused on United States law enforcement agencies: Federal, State, County, and City. This is due to the unique needs of U.S. law enforcement agencies. The second topic area that was encompassed, was in law enforcement training methodologies. This thesis looked at previous work to determine what training methodologies would be best suited for web based training specifically geared to Law Enforcement Agencies (LEA) and officers. The third and final topic area, was in the development of cyber forensic courses for academia. There were two reasons for this, there is a large body of work to draw from and the research is more current than that of the primary area.

1.3 Significance

Since the beginning of the digital forensics field, training and education have been among the top 10 issues. The reasons this has been a continual issue were summarized to not having a formal training model, not having realistic training data, and the high cost of the training programs (Garfinkel, 2010). Since then, there has been no significant progress to unify or standardize the field. In addition to the reasons stated above, the issues are compounded by the overwhelming number of different technologies officers and cyber forensic examiners can encounter. Going forward it is important for Law Enforcement Agencies to be able to send a greater number of their officers to digital forensic training. Being that most agencies are funded by tax dollars, this research could make it feasible to get digital forensics training to entire agencies. The goal of this research is to develop a web based training site that will enhance the basic officer’s knowledge of digital forensics.

There were several significant outcomes of this training to include cost savings for the agencies, consistent training material, cross domain information sharing, and provide the officers with another “tool” for their tool box.

1.4 Research Question

The main research question for this thesis was:

- Is web based cyber/digital forensics training an effective medium to train a large group law enforcement officers compared to a traditional class room?

1.5 Assumptions

There were several assumption made about this study.

- That all subjects would complete the training in time frame that they were given.
- It was assumed that all subjects would answer the entrance and exit survey honestly and to the best of their ability.
- That the subjects taking the training, had no previous cyber forensics training. Any previous training could potential skew the scores on the pre and posttest.
- That the subjects would not use outside resources to answer the questions when taking the pretest and posttest.
- Was concerning the statistical data cited from outside sources? There were two parts to this assumption, first was that the data used for that study was collected properly. Secondly, that the analysis of the data was accurate.

- That the technology and web site will perform the way that it was designed to perform.
- That the subjects were given the time to take the training by their agency. It was assumed that the subjects would have some basic understanding of how to navigate through a web site.
- That the subjects learned in a similar way. It was assumed that the subjects have access to the Internet either in their vehicles or at the stations.
- The final assumptions is that the officers will read the instructions, take the training seriously and perform to the best of their abilities.

A crucial piece of this study was getting the backing of the Indiana State Police (ISP) as well as organizations like the Indiana Prosecuting Attorneys Council (IPAC). Without their support the credibility of this study could be diminished. Their support was needed to get access to the road/beat officers.

1.6 Limitations

There were only a couple of limitations of this study.

1. The first limitation was on the subjects for the study. Only those with the rank of Trooper, S/Trooper, M/Trooper and Sergeant were selected
2. The second limitation was due to the time constraints the development of training material was limited to two to three treatment groups/delivery methods.
3. The third limitation of this study was the HTML programming ability of the author.

1.7 Delimitations

It was the intent of this study to determine if web based training would be an effective medium to train a large group of officers. Delimitations for this study include:

- The material presented was to increase the knowledge level of the basic beat/road officers.
- The intent of this study was not to make every officer a digital forensic examiner or expert.
- As well this study was not intended to replace traditional training and to be used to help supplement the traditional setting.
- This study was only interested in those officers that have no prior cyber/digital forensics training.
- It was possible that the results could be skewed if there were subjects in this study with prior training. This study did not account for every single learning style. The subjects were asked in the exit survey if they had any prior cyber forensics training.

1.8 Summary

This chapter has described the driving factors for this thesis. This chapter has listed the scope, significance, assumptions, limitations, delimitations, definitions and acronyms. The next chapter is a review of the literature relevant to this research. There are two broad categories the literature fall under cyber forensics training and law enforcement training methodologies.

CHAPTER 2. LITERATURE REVIEW

As the literature review for this research evolved, the question on how to organize those readings needed to be answered. There were a couple of different methods that quickly came to the forefront. The first method was to organize the readings in a straight chronological order. Because the topic crosses two main domains, that ordering did not make the most sense. The other method was to split the readings into two general or broad topic areas. The latter option was the method selected for this paper. Each topic area contains information that is relevant to the independent and dependent variables.

The first area will be comprised of those readings that have to do specifically with digital/cyber forensics. Some of the literature review placed in this category covers Information Security training. The fields of information security and digital forensics are closely related and in some cases overlap each other. It was for this reason that those papers/articles were put in this category. The second topic area will be those articles, journals, papers discussing training methods for law enforcement officers. The readings will be further organized chronologically. The review of the literature will cover how and why it is important for this thesis. The literature placed in the digital forensics category will be covered first and the literature in the law enforcement training category will be covered last. The literature reviewed came from online resources including Purdue’s online library, Elsevier and other online databases.

2.1 Cyber Forensics Training for Law Enforcement

As mentioned above, the topic of digital/cyber forensics training has always been a major issue within the field. Most of the literature reviewed, in some capacity, mentioned training. However, through the review on this subject, it was apparent that there had been little done to actually address or even solve this issue for law enforcement. Much of what has been reviewed, was from what academia has done to develop digital/cyber forensics curriculum at both the undergraduate and graduate levels. Though there are a couple of examples addressing law enforcements need and they have been covered in this literature review. There are three papers that are the foundation of this research. The first paper was written by Brinson, Robinson and Rogers titled, *A cyber forensics ontology: Creating a new approach to studying cyber forensics*. The second article was case study written by Kessler titled *Online Education in Computer and Digital Forensics: A Case Study*. The third is a special publication from the National Institute of Standards and Technology (NIST). The special publication gives the framework for how courses should be developed.

2.1.1 NIST SP 800-16

The NIST Special Publication (SP) 800-16 titled *Information Security Training Requirements: A Role and Performance based Model* was published in 1998. Currently, there is an update to this publication that is in draft form. The SP is a 188 page document that lays out a framework for information security training. Cited in the SP was a report from the Government Accounting Office (GAO), which addressed the need for training in information security. The GAO report stated that Information Technology (IT) security was “a new high-risk area that touches virtually every major aspect of government operations (report# GAO/HR-97-30)” (Wilson, M., deZafra, D., Pitcher, S., Tressler, J., & Ippolito, J., 1998, p.5). The GAO report listed several recommendations from a previous report as underlying non-technical factors to the information security risks in the government. Some of those factors included: “insufficient awareness and understanding of information security risks among senior agency officials,” “poorly designed and implemented security programs,” “a shortage of personnel with the technical expertise needed to manage controls,” and “limited oversight of agency practices” (Wilson et al., 1998 p.5).

800-16 replaced special publication 500-172 as the Information Security Training framework. In the old SP the training methodology or principle was based on the job tiles. The main training principle for SP 800-16 was based on results based learning. The principle is broken in two six categories (Wilson et al., 1998 p. 14 -16).

1. The first category was that training was “based on roles, responsibilities or job function.” In this category, the authors stated that “Everyone needs basic training in IT security concepts and principles” (p. 14).
2. The second category “delineates the differences among awareness, training, and education” (p. 14)”. Here the authors state there are difference between “awareness programs” and “training programs” as well as a difference between “training” and “education” (p. 15).
3. The third category is “Provides an integrated framework (planning tool) to identify training needs throughout the workforce and ensure that everyone

receives appropriate training" (p. 15). The third category is training "provides a course development tool" (p.15).

4. The fourth category "provides a structure for evaluating learning effectiveness (p.15)".
5. The fifth category "is extensible" meaning that the training is easily updated to keep up with the changing landscape (p.15 -16).

NIST introduced their training model called the "IT Security Learning Continuum" in this publication (Wilson et al, 1998). Figure 2 shows the model they developed.

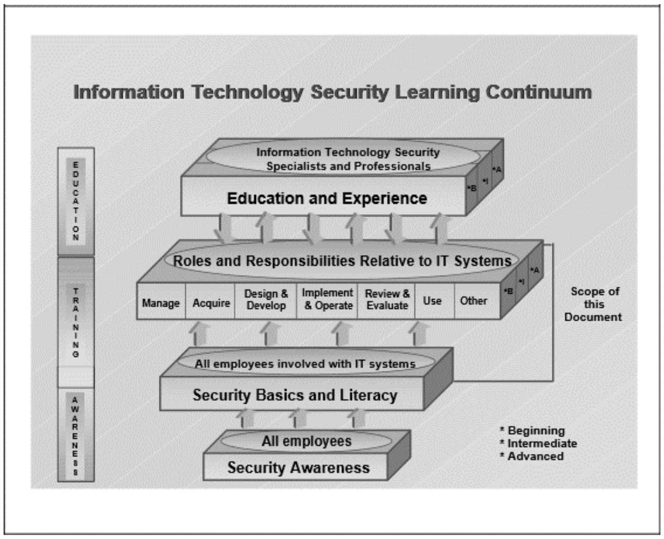

Information Technology Security Learning Continuum
EDUCATION
TRAINING
AWARENE88
Information Technology Security Specialists and Professionals
Education and Experience
*B
*I
*A
Roles and Responsibilities Relative to IT Systems
Manage
Acquire
Design & Develop
Implement & Operate
Review & Evaluate
Use
Other
*B
*I
*A
Scope of this Document
All employees involved with IT systems
Security Basics and Literacy
All employees
Security Awareness
* Beginning
* Intermediate
* Advanced

Figure 2.1: Information Technology Security Learning Continuum

The model starts with the basic security awareness programs that suggest all employees need to have. With the second layer of the model, all IT employees should receive basic training in security and have a basic literacy of IT security. The next level up is when the training focuses down and is based on the roles and responsibilities of the individual. The last level of the model is where the employees receive the highest levels of training. The goal at this level is to ensure that employees can keep their skills fresh and up to date. This is in order “to further the IT security profession and to keep pace with threat and technology changes” (Wilson et al., 1998, p. 23). To assist in differentiating the variances between the three levels, Awareness, Training and Education, NIST developed a cooperative framework. Within the cooperative frame work, NIST defined a basic testing measure for each of the levels. Table 2.1 which is labeled in the special publication as exhibit 2.2, defines those measures.

Table 2.1: Comparative Framework

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning Objectives	Recognition and Retention	Skill	Understanding
Example Teaching: Methods	Media -Videos -Newsletters -Posters	Practical Instructions -Lecture and/or demo -Case study -Hands-on practice	Theoretical Instruction -Seminar and discussion -Reading and Study -Research
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving, ie Recognition and Resolution (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-Term	Intermediate	Long-term

NIST recognized that individual’s do not all learn the same way. The ideal way for a person to learn is based on three things, their learning style, education, and prior experience. Everyone has a learning style and that style can either have a positive or negative effect based on the instruction they are receiving (Wilson et al., 1998). It is important to take this fact in to consideration when developing training. Training courses should have material presented in different ways to account for the different learning styles (Wilson et al., 1998). Education and experience of the audience is another factor that needs to be taken in to account when developing training courses. This is so that the proper level of training material is presented to that audience (Wilson et al., 1998). Students will learn differently based on their level of education and/or work experience. The example given in the SP is a person with an advanced degree might take a different approach to new learning material than someone who has extensive on the job training (Wilson et al., 1998). Additional consideration is needed to be made for adult learning. Adults will typically relate new information to past experiences whether it's from past education or past work experiences. This could cause the new information to be misinterpreted or miscommunicated (Wilson et al., 1998).

In Chapter four of NIST SP 800-16 there are six role categories that relate to the three fundamental training categories. The three fundamental training categories are Laws and Regulations Security Programs and System Life Cycle Security. Each of the categories list the type of Knowledge Skills and Abilities:

- Laws and Regulations
- Security Program
- System Life Cycle Security

The Information Technology Security Training Matrix was created from these six role categories, the three training areas and an additional “other” category (Wilson et al., 1998). Table 2.2 is the graphical representation of the IT Security Training Matrix.

Table 2.2: NIST IT Security Training Matrix

	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulation	1A	1B	1C	1D	1E	1F	
2. Security Program							
2.1 Planning	2.1A	2.1B	2.1C	2.1E	2.1E		
2.2 Management	2.2A	2.2B	2.2C	2.2E	2.2E		
3 Systems Life Cycle Security							
3.1 Initiation	3.1A	3.1B	3.1C		3.1E	3.1F	
3.2 Development	3.2A	3.2B	3.2C	3.2D	3.2E	3.2F	
3.3 Test and Evaluate			3.3C	3.3D	3.3E	3.3F	
3.4 Implementation	3.4A	3.4B	3.4C	3.4D	3.4E	3.4F	
3.5 Operations	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	
3.6 Termination	3.6A			3.6D	3.6E		
4 Other							

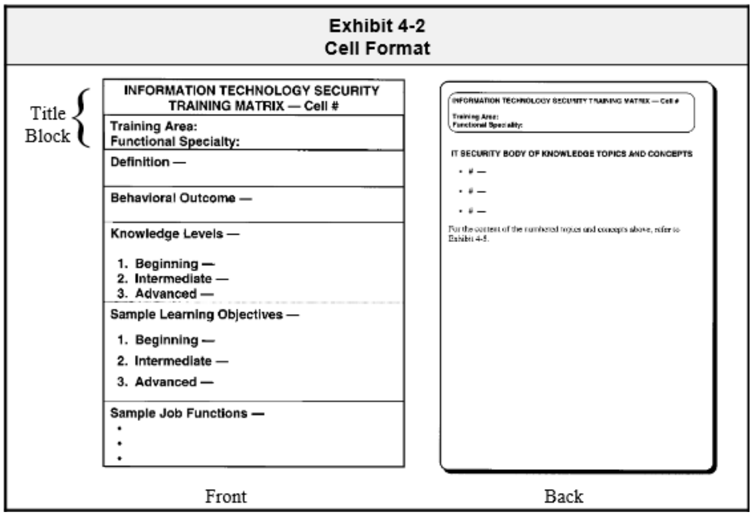


Exhibit 4-2
Cell Format

INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell #

Training Area:
Functional Specialty:

Definition —

Behavioral Outcome —

Knowledge Levels —

1. Beginning —
2. Intermediate —
3. Advanced —

Sample Learning Objectives —

1. Beginning —
2. Intermediate —
3. Advanced —

Sample Job Functions —

-
-
-

INFORMATION TECHNOLOGY SECURITY TRAINING MATRIX — Cell #

Training Area:
Functional Specialty:

IT SECURITY BODY OF KNOWLEDGE TOPICS AND CONCEPTS

- # —
- # —
- # —

For the content of the numbered topics and concepts above, refer to Exhibit 4-5.

Figure 2.2: NIST Cell Format

Chapter five is titled “Value of Evaluation in a training Program”. The first two paragraphs of the chapter make a particularry important statement. The first statement is “Evaluating training effectiveness is a vital step to ensure that the training delivered is meaningful. Training is “meaningful” only when it meets the needs of both the student (employee) and the organization” (Wilson et al., 1998, p. 157). This means that if the training is not pertinent to the role, outdated or unfitting it has no value to either the employee or the organization (Wilson et al., 1998). Not only does the information of the training have to be valuable but the manner in which it is delivered is important. The methods in which the material is presented to the audience can have a drastic impact on how the students perform (Wilson et al., 1998). The second statement made in the beginning of this chapter was that all meaningless training is expensive. Governmental agencies operate on limited budgets and “cannot afford to waste limited budges on ineffective training meaningless training” (Wilson, et al., p. 157). It is important to make sure that a training program met the needs of all of the stakeholders. NIST developed a means to make this determination. This consits of four levels of effectivness, which can be used to determine the over all effectiveness of all training courses. (Wilson et al., 1998 p. 160):

- Level 1: End of Course Evaluations (Student Satisfaction)
- Level 2: Behavioral Objective Training (Learning Effectiveness, also a measure of Teaching Effectiveness
- Level 3: Job Transfer Skills (Performance Effectiveness)
- Level 4: Organizations Benefit (Training Program Effectiveness)

Independently, the scores for each level may not show significance one way or the other. The scores should be used together to get a better understanding of how effective the training really is.

This special publication gives a very detailed framework to be able to create a training program whether it be in a traditional class room setting or using new platforms such as web based training. Since Information Security and cyber forensics are so closely related, the framework, principles and methods from this SP can be easily adopted to web based cyber forensic specific training.

2.1.2 National Institute of Justice

The National Institute of Justice (NIJ) published a research brief in 2000 titled *State and Local Law Enforcement Needs to Combat Electronic Crime*. The brief was written as a summary to a full report that they released later that same year. The key issue of that brief were "a compelling need exists to better address the requirements of State and local law enforcement agencies in detecting investigating, and prosecuting individuals who commit electronic crimes" (Stambaugh et al., 2001, p 1). There were three key findings from their research that were specific to those participants from State and local agencies:

- Law Enforcement has a short window in containing cyber-crimes.
- Law Enforcement does not have adequate training, equipment and staff to be able to fight the current levels of cyber-crime nor are they prepared for future needs.
- There is a need for "greater awareness of electronic crime" should be promoted across all those who have a stake in cyber-crime (Stambaugh et al., 2001, p 2).

The target audience for this brief was state and local policy makers, law enforcement officers, and administrators (prosecutors and judges), State and national training centers, academia, industry computer engineering and security development specialists (Stambaugh et al., 2001). It was in this article that a uniform training and certification course was listed as one of the top 10 priorities for law enforcement (Stambaugh et al., 2001). The reason this was called for was because of the specific training levels that law enforcement officers and forensic scientists need to competently investigate electronic crimes. The brief also states that there needs to be basic or entry level training in addition to advance training for law enforcement officers, prosecutors, judges, defense attorneys, probation and parole officers (Stambaugh et al., 2001). This brief recognized that there will be greater challenges that law enforcement would continue to face as the use of technology increased (Stambaugh et al., 2001).

2.1.3 Information Systems Security Curricula Development

The need and urgency for curriculum development for information security training courses was made a priority in 1998. This urgency came from the Presidential Decision Directive 63. The directive stated that it was essential to protect “cyber-based” systems that were central for the “minimum operations for the economy and government” (Crowley, 2003, p. 1). The paper by Crowley is one of several papers reviewed by this author, in which there was a survey on the topic of information security training and education (Crowley, 2003). One of the areas covered by Crowley was Information Assurance Education Attributes. Those attributes included: Context Sensitive, Dynamic, Multidisciplinary, and Active. Focusing on these attributes is important to prepare students in this area (Crowley, 2003). Crowley also focused on the fact that there was not a mature common body of knowledge (CBK) in this area. Having a CBK is required so that training is consistent and standardized. Crowley also cites NIST SP 800-16 and the National Security Telecommunications and Information Systems Security Committee's (NSTISSC) training standard 4011 as a basis for developing training standards and a CBK in this area.

2.1.4 High-Tech Forensics

Moving into the early 2000's police officers were still unprepared to deal with computer crime. At that point in time the "average" police officer received little to no cyber forensics training. The early cyber forensics labs and high tech units were staffed by officers or detectives who had "limited specialized preparation" (Harrison, Heuston, Mocas, Morrissey, & Richardson, 2004 p 1). In 2004, the Hillsboro (Oregon) Police Reserve Specialist (PRS) program was formed. The PRS program allowed qualified citizens from that community to assist the Police Department (PD) with criminal investigations. It is stated that because of the "dramatic proliferation in cases involving digital evidence requires prosecutors and law enforcement agents to deal with artifacts such as computer logs, email, word-processing documents, image files and so on" (Harrison et al., 2004 p. 1). Without the technical knowledge of how computers work, cases "may never reach trail and those that do may not lead to recover of assets or damages" (Harrison et al., 2004 p. 2). As cited Harrison et al., the losses due to cyber criminals could reach in to the $100 billions of dollars (2004). The history of the PRS program started as a result of a meeting between the Hillsboro police Chief and the

Computer-Related Investigations, Management and Education (CRIME and is made up of individuals from academia, industry, and law enforcement (Harrison et al., 2004). One of the goals of the PRS program was to close the gap between those law enforcement agencies who has expertise in investigations, not in technology and those in industry or academia who have the expertise in technology (Harrison et al., 2004). This article highlights the need for law enforcement agencies to have their personnel trained in digital forensics.

2.1.5 Computer Forensics – A critical need in Computer Science Programs

Another example from academia on the need for computer forensics/cyber-forensics curriculum comes from a paper written by John D. Fernandez (2005). The first section of the paper covered the beginnings of the cyber-forensics field. The second portion of the paper discussed a few of major computer crimes. Where this paper directly relates to this thesis is in third to last section. Fernandez addresses the challenge that law enforcement has when it comes to presenting electronic evidence to the courts (Fernandez, 2005). Fernandez specifically points out that digital forensics are different from the other forensic sciences. He says it requires “specialized knowledge of computer technology (both hardware and software), including various operating systems, file storage techniques and file recovery techniques” (p. 320). The challenge Fernandez states, is that it is locating people that have these skills and then to maintain those skills with current tools and training (Fernandez, 2005). This paper highlights the continuing fact that training and education are among the top issues within the cyber-forensics field. The paper also states that one of the main challenges the field faces was due to the lack of a national framework for curriculum development and no golden standard for professional certifications (Fernandez, 2005).

2.1.6 Computer Forensics Programs in Higher Education

Since the start of the cyber forensics field, colleges and university have been working on developing undergraduate and graduate programs. The paper from Metropolitan State University, written by Gottschalk, Liu, Dathan, Fitzgerald and Stein (2005), discusses the need for trained computer forensic experts. The authors examined what other colleges and universities were doing to provide computer forensics training to their students. Mentioned early in the paper is the fact that the need of computer forensic experts would continue to grow. The authors pointed to a Carnegie Melon University study that showed that business to business e-commerce was estimated to be $1.5 trillion dollars for that year. The authors also put emphasis on the fact that the computer forensics is multidisciplinary, made from the combination or criminology and information technology (Gottschalk, Liu, Dathan, Fitzgerald & Stein, 2005). When discussing the curriculum for any cyber forensics course work, it would need to include topics from those two fields. For the criminology discipline, topics to include would be: criminal justice, law procedures, court procedures, and criminal investigation ethics. For the Information Technology discipline course would need to include: computer hardware, computer software, computer programming, networking, computer security and computer forensics (Gottschalk et al., 2005). This paper references to Yasinsac et al. who has four distinct roles, identifies the proper level of education and training and the responsibilities for those roles (Gottschalk et al., 2005).

Table 2.3: Yasinsac's Roles, Education and Responsibilities

Roles	Education	Responsibilities
Technician	Associates or Bachelors	Retrieving digital/electronic evidence
Enterprise Policy Makers	Training Courses	Responsible for developing and making polices
Forensic Professionals	Associates or Bachelors	Convert the policies to procedures that in turn are carried out by the technicians.
Researchers	Masters or Doctoral	Conduct research in the field.

The analysis of this paper shows that course work should be made up of elements from the areas of criminal justice, law enforcement, ethics political sciences, computer sciences and information technology. The paper also identified four educational approaches to this field, associate degrees, baccalaureate degrees, graduate programs and certificate programs (Gottschalk et al., 2005).

2.1.7 Case Study: Information Security Curriculum Creation

As discussed in the first section of this literature review, information security directly relates to cyber forensics. The curriculum creation for this topic area has been discussed for nearly as long as cyber forensics. The technical expertise required for those in information security is almost identical to that needed in cyber forensics. In 2005, there was a case study conducted by Bogolea and Wijekumar from Pennsylvania State University. The purpose of the paper was to make their case for creating curriculum that would improve existing undergraduate programs in Information Technology and Computer Science (Bogolea & Wijekumar, 2005). It is important to point out that the authors acknowledged three things, the rapid increase of technology, the increased abuses of that technology and the need for more information security professionals (Bogolea & Wijekumar). For the case study, Bogolea and Wijekumar reviewed five graduate level programs: Carnegie Melon University, James Madison University, Purdue University, Johns Hopkins University, and George Mason.

2.1.8 A Cyber Forensics ontology

One of the foundations for this research is from the journal paper *A cyber forensics ontology: creating a new approach to studying cyber forensics*. This article was written in 2006 by Brinson, Robinson and Rogers, which addressed the need of creating a methodology for “defining the correct levels of education, certification and specialization” in the cyber forensics field (Brinson, Robinson, & Rogers, 2006, p.37). The base of the methodology used in this paper are from the two different ontologies, Ontology and ontology. The first one is a “situation where classification schemes are being built.” The last one is a “systematic account of existence” (Brinson, et al. 2006 p37). At this point in the cyber forensics field was still early on in its infancy. The specializations and certifications were still being developed. Brinson et al. developed and proposed a five layer hierarchal model.

At the top most layer is Cyber Forensics, under that layer are two categories: Technology and Profession. The five layers are: Technology hardware, Technology software, Profession law, Profession academia, and Profession Military. The model is then broken up into additional sub layers that cover specific topics or areas. For example, under Profession law there are two sub layers. Enforcement and Courts. Enforcement includes additional layers of “Collection and Analysis” and “Evidence” (Brinson et al., 2006, p. 38). The third section of the paper focused on certification areas. The authors recommend that certifications "could and should be obtained" in those areas relevant to the area they want to specialize in (Brinson et al., 2006, p. 42). One of the purposes of this ontological model was curriculum development. The curriculum would be developed from each of the sub layers and as other areas are discovered additional courses could be added. The Brinson, Robinson, Rogers Ontological model was also designed to be used for course curriculum development. The authors stated that the third layer would be the layer that would become potential courses (Brinson et al, 2006, p. 42).

2.1.9 Cyber Katrina

In 2006, a report written by Rahul Bhaskar was published in the Communications of the ACM journal. The title of the article was *State and Local Law Enforcement is not Ready for a Cyber Katrina*. Bhaskar opens the article with how poorly the response was to Hurricane Katrina and makes the comparison that State and Local law enforcement agencies are not ready to respond to a "Cyber Katrina" (Bhaskar, 2006). Bhaskar states the main reason for this is that "there is simply not enough law enforcement officers at the state level with appropriate computer forensics and computer crime investigative skills to protect their part of the infrastructure" (p. 81). The report referenced a survey of 530 law enforcement agencies from the United States Midwest region. From those surveyed, only a small portion of officers had a basic knowledge of computer forensics (Bhaskar, 2005). From the survey of local law enforcement officers, for the category of "Sworn Law Enforcement Officers assigned to investigate computer crimes"- 49.2%, for "Sworn Law Enforcement Officer trained in computer forensics" – 12.3%, and for

“Personnel with formal computer science training” – 6.8% (Bhaskar, 2006). Bhaskar said, “A serious shortage of law enforcement officers trained in computer forensics presents a significant challenge to any computer security response plan” (p. 83). There were two key points in this report. The first one was that the knowledge of computer forensics is extremely limited throughout the entire law enforcement community. The second point is that there is also a limited amount of trained legal support when it comes to computer forensics (Bhaskar, 2006). This article is important in showing the continual need for law enforcement to have a broader range of their officers training in cyber forensics.

2.1.10 Online Education in Computer and Digital Forensics: Case Study

One of the first documented instances that this author was able to discovery, of a law enforcement entity reaching out to an academic institution was in the early 2000’s. This was in response to a local Vermont Internet Crimes Against Children (ICAC) task force needing specific training and instruction in digital investigations and forensics (Kessler, 2007). This ICAC taskforce reached out to Champlain College. The end result from this collaboration was the development of the first digital forensics class in the fall of 2002 at Champlain College. With the success of those courses, it lead the instructor and coordinator to believe their digital forensics curriculum would fill a national need (Kessler, 2007). In 2003, their Computer and Digital Forensics undergraduate degree and academic certification was introduced. This would lead to 2004, where an online version of the Computer Forensics I course was developed.

This course was not only offered in the traditional class room setting, but also the online version was offered through the College's WebCT Learning management System (LMS). The online courses had an almost identical syllabus as the in-class course and it was taught in the same 15-week semester (Kessler, 2007). In review of the Champlain's WebCT LMS, Kessler points out a couple of advantages of the virtual class room over the traditional class room (Kessler, 2007).

1. Communication capabilities
2. Enhanced one-on-one sessions between the instructor and student
3. Flexibility of the schedule
4. The high availability of the training material.
5. The tools built in to the system for grading, feedback.
6. The ability for self-tests and quizzes.
7. Integration of the Internet into the course

Additionally, both the on-line and in-class courses had the same learning objectives. Kessler stated that the "quality of online courses come from content" (Kessler, 2007 p. 2). As stated in the introduction of the paper there was a focus on the hands-on portion of the online training courses. One of the most important aspects considered in the development of the online course, was that it had to have the correct mix of each pedagogic models (Kessler, 2007). In Kessler's research, he discovered a constant similarity between the different pedagogies. That similarity was active learning (2007). The five pedagogies used were: constructivism, resource based learning (RBL), collaborative learning, problem based learning (PBL), and narrative based teaching (NBT).

The online version of the Champlain digital forensics course was developed for adult learners According to Kessler, adult learners, “are more mature and self-directed than traditional-aged students” (Kessler, 2007 p. 4). Adult learners tend to perform better with active, PBL methods. There are several guidelines listed by Kessler that serve as basic concepts and guidelines for online course development (Kessler, 2007 p. 4):

- Clearly stated goals and objectives.
- Learning modules are as small as possible.
- Self-assessment tools and quizzes should be used as much as possible
- Be advised upfront of time requirements and expectations
- The technology be transparent.
- Support a wide variety of web browsers
- Balance the computer power and network bandwidth to suite the material being delivered
- Keep the technology sophistication as low as possible.
- Good technical support available to assist the students to reduce their frustrations.
- Focus on the content and not the technology.
- Have a well-designed web site (aesthetically pleasing)

In 2006, there was a study conducted by Champlain to compare the results from the online computer forensics courses to the results of the in-class courses. The study used the course results from the online and in-class courses from the 2005 calendar year (Kessler, 2007). The design of the study was set up to take the grades from each student, which included scores from the course homework, quizzes, projects and tests. They used those scores to measure the level of success of the students (Kessler, 2007). Neither pretesting nor posting were used in this study. The total sample size (n) was 176 students. The null hypothesis used was “there was no significant difference in learning outcomes between the online and on-campus delivery mode” (Kessler, 2007 p. 7).

Analysis of Variance (ANOVA) was used for the statistical analysis, specifically a two way table. The final grades, the dependent variable, were normalized to a 4.0 GPA scale. The independent variable was the delivery modes (Kessler, 2007). For this study α = .05, for course and mode the p-value = .062 and was statistically significant. The p-value for delivery mode only was .242 and was not statistically significant (Kessler, 2007). Based on these results from the study, they determined that the course alone affected the final grade (Kessler, 2007). Though there was no statistically significant deference between the two delivery modes, the online course had a slightly higher average than the in-class mode (Kessler, 2007). The statistical results of the study are shown in Table 2.4. Kessler stated, “The pedagogic background shows that online courses are not merely online correspondence courses, but designed based upon well-founded learning theories (Kessler, 2007 p. 4).”

Table 2.4**:** ANOVA Results from Kessler

Source	df	F	Sig.	Partial Eta Squared
Course	3	3.374*	0.02	0.057
Mode	1	1.379	0.242	0.008
Course*Mode	3	7.491	0.062	0.043
Error	168	-0.484		

2.1.11 Growing Challenge of Computer Forensics

In 2007, a partnership between Purdue University, the National White Collar Crime Center (NW3C) and the Indiana State Police was formed (Cohen, 2007). This partnership was developed to make a major shift within digital forensics. There were four issues that are shared among police detectives, prosecutors and digital forensics examiners:

- A back log of devices waiting for examinations.
- Because of the long waiting period, the leads produced from the examinations are generally old.
- Detectives don’t typically understand computer forensics and how it can be used in their investigations.
- In turn the digital investigators do not have an understanding of the investigations and could potentially miss valuable information (Cohen, 2007).

The goal of the partnership between the three organizations was to allow a flow of information and to build on the strengths of the each.

This article introduced a four "tiered approach to digital forensics" (Cohen, 2007, p. 2). Figure 2.3, used with permission of *The Police Chief IACP*, shows the Cohen's tiered approach. At the base of the approach are all of the officers in a department. At this level is from which a majority of investigations were generated. At this level the officers needed to be able to identify all the different types of evidence, prepare all the necessary documents, avoid destroying evidence, and know how to integrate electronic evidence into the investigation (Cohen, 2007). The next level was the Crime Scene Investigators (CSI): this level required a slightly higher level of training than the officers. At this level the CISs needed to locate, identify, and package evidence (Cohen, 2007). The third level in this approach was the cyber-crime first responders. At this level the level of knowledge was greater and there were more specialized training for those who hold those roles. This level required the officers to remove electronic evidence and preview the evidence in a forensically sound manner (Cohen, 2007). At the top layer was the cybercrimes units, these units are the most specialized and highest trained in an organization. At this level the officers' conducted full on examinations, were subject matter experts and conduct research in this field (Cohen, 2007).

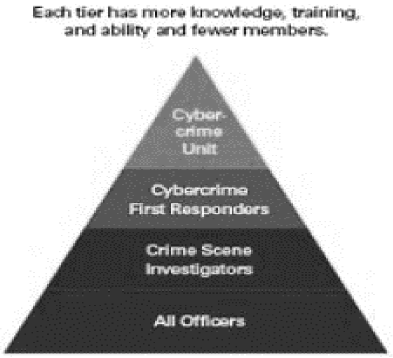

Each tier has more knowledge, training, and ability and fewer members.
Cyber-crime Unit
Cybercrime First Responders
Crime Scene Investigators
All Officers

Figure 2.3: Cohen's Tiered Approach to Digital Forensics

As stated by the author, training for these individuals can cost tens of thousands of dollars. This tiered approach is designed to efficiently use the limited resources. Cohen states "It is the role of police managers to ensure that each officer has the requisite knowledge, training, and ability" (p. 3).

2.2 Law Enforcement Training Methodologies

There are many training demands that are placed on law enforcement agencies and their officers. These demands come from a variety of different sources, legislative, judicial and internal. Due to the unique requirements placed on agencies and officers there has been extensive research into which methods are the best for training law enforcement officers. The invention of the computer has been an aid in training Law Enforcement officers but it has also added a layer of complexity. The following papers and articles cover those methodologies that are important to this thesis.

2.2.1 Teaching Style and the application of adult learning principles by police instructors

Andragogy as defined by Knowles (1990) and as cited by McCoy, is "a theory which is vastly contrast to the traditional pedagogical model and it advocates both the self-directed learning concept and the teacher as the facilitator of learning. (p. 2)" McCoy also listed Knowles's five "basic assumptions of adult learning" (McCoy, 2006, p. 57):

- Adult learners "are increasingly self-directed"
- Adult learners "have a broad range of experiences to learn from and to share with others."
- Adult learners "are stimulated to learn by immediate life situations."

- Adult learners “are motivated by internal incentives.”
- Adult learners “are problem centered.”

McCoy states to successfully and effectively implement Knowles’s five principles of andragogy, the student must be active in establishing the objectives of the learning activity (2006).

A major change to how training and education in law enforcement came with the Community Oriented Policing methodology (McCoy, 2006). This caused police officers to handle a wider range of issues as well it was expected that the officer would be more proactive in identifying issues in their communities (McCoy, 2006). McCoy stated that traditional training methods were not ineffective in teaching critical thinking skills, problem solving, leadership and judgment skills (2006). According to McCoy, “a shift in education philosophy” from teacher-centered to learner-centered was needed to make that transition” (McCoy, 2006, p. 79).

2.2.2 Cops, computers and the curriculum

The computer has become such a necessity for law enforcement agencies and their officers. They allow for a broader range of connective between the officers, dispatchers, and prosecutors (McCoy, 2006). They give officers access to a greater amount of investigative information. Computers in general have increased the efficiency and effectiveness of officers. According to McCoy (2006), most of all law enforcement agencies have some type of functionality that involves computers. Statistics listed by McCoy, showed that 90% of municipal departments have used computers for record keeping, 85% use computers for crime analysis and 82% for criminal investigation.

McCoy stated that the effect computers have had on agencies forced tough questions when it has come to “designing questions for designing curricula for law enforcement education and training” (McCoy, 2006 p. 154). There were seven principles listed in this journal article on how to introduce computers in to basic police training. These principles can be applied to web based training (McCoy, 2006 p. 154-155):

- There must be detailed planning before introducing computers
- The administration must support “buy in” to the training and they must participate in the training.
- Having officers be excited about the training will ensure their participation in that training.
- Officer should have their own computers. This leads to a since of ownership which leads to them using the computer more.
- The training /curriculum must be flexible, included peer support, resource personnel and class room instruction.
- The curriculum should allow for the officers to experiment with the software.
- Management support is necessary so that the training/curriculum is developed in a way that meets the needs of the department.

According to research done by McCoy (2006), adults learn the best when the lectures are kept small and there is more time for hands on with the computer. As cited by McCoy, “programs without hands-on experience are not as successful” (Amador, 1986, p. 82). These principles along with the suggestions for Amador, certainly still applicable to web based learning as they were when computers were first being introduced into police departments.

2.2.3 In-service training

In-service training is an important and necessary part of law enforcement. Nearly every state has a yearly requirement for officers to complete in-service training in order to maintain the police officer certification (Etter & Griffin, 2009). The study done by Etter and Griffin was mainly focused on officers between the age ranges of 40 – 60 years old. The primary contribution from this paper are the principles of adult learning/education or andragogy (Etter & Griffin, 2009). Etter and Griffin state that training instructors have to be cognitive of the different learning styles to ensure that they are providing the most effective training. Similar to what McCoy listed, Etter and Griffin, list six conditions “that must be met for officers to learn effectively” (p. 242). This six factors were (Etter & Griffin, 2009 p. 242):

- “Officers have to realize that the training is needed. If they don’t think so prior to the training, it is likely that performance requirements will change their minds.”
- “Officer must understand that they are expected to learn and/or perfect specific tasks and overall skills.”
- “Officers must have the opportunity to practice what they have learned and demonstrate their skills.”
- “Officers must get reinforcement that they are learning.”
- “Officers must progress through training presented in a logical sequence.”

- "Officers must be willing to learn and participate with the motivation to improve or fine-tune their skills."

Griffin and Etter list three types of in-service training: Mandatory training, Operational training, and Career oriented training. Cyber Forensics training could fall into either the Mandatory training category or Operational training category.

2.2.4 Problem Based Learning

Different models have been used to training police recruits. In the past, some of these models have received criticism for a couple of different reasons. One reason is that they are heavily teacher-centered. A second reason is that the training is too narrow in focus and does not allow for critical thinking and problem solving skills to develop (Shipton, 2009). The methodology that police training has been moving towards in Problem Based Learning (PBL). Problem Based Learning "requires learnings to collect information in a self-directed manner in order to learn the necessary knowledge that will assist them to discover, analyze and solve realistic problems" (Shipton, 2009 p. 59). This paper is directed to new police recruits and one of the potential issues with PBL is that it would over load the cognitive ability of new learners and thus reducing the effectiveness of the training (Shipton, 2009). However other studies cited by Shipton show that increasing the flexibility and properly designed framework reduce the overload (2009). The model proposed by Shipton titled "Police PBL" was a hybrid model combining elements of the Croal Model, web based resources, lectures and non-PBL tutorials (2009). Figure 2.4 is the design view of Shipton's hybrid Police PBL model.

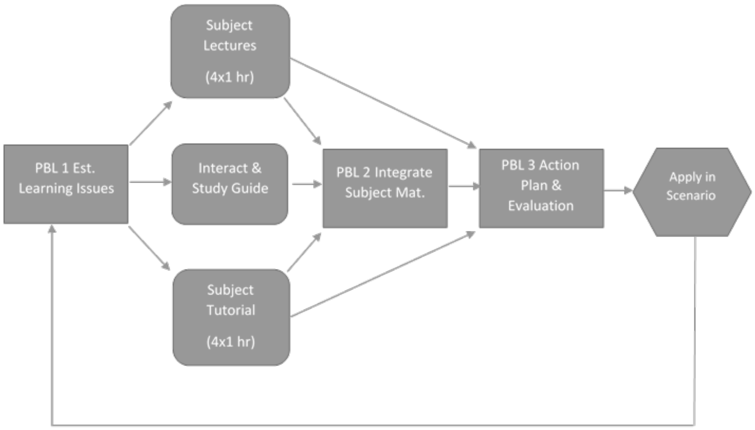

Subject Lectures (4x1 hr)
PBL 1 Est. Learning Issues
Interact & Study Guide
PBL 2 Integrate Subject Mat.
PBL 3 Action Plan & Evaluation
Apply in Scenario
Subject Tutorial (4x1 hr)

Figure 2.4**:** Shipton’s Hybrid Model

Shipton proposed this model to be the framework that could be applied to various topics taught to police recruits. Shipton concluded that this model would be used to “facilitate deeper learning and integrate subject matter in authentic policing problems similar to those confronted in police practice” (Shipton, 2009 p. 67).

2.3 They are old enough to carry guns, should we teach them like Children? The application of adult learning strategies in police training

This was from McCay’s (2011) dissertation on the application of adult learning techniques for police academy trainings (p. ix). The research conducted by McCay looked at several things:

1. The history and development of policing in the United States
2. The methodologies currently used by police academies to teach recruits
3. Police training in and around Indiana

The overall purpose of the study was to “examine what was most impactful about the police academy experience” and to and this information to the police training body of knowledge (McCay, 2010 p. 10). The study specifically evaluated the training model that was being used at a regional police academy in Indiana, to evaluate how the experience shaped those who lived it (McCay, 2011 p. 11). The research questions that were asked in this study were (McCay, 2011 p. 12):

- What professional characteristics does the current pedagogic/militaristic training model develop in its police recruit students?
- What police academy events or circumstances are most impactful to police recruits and why?
- What strengths and weaknesses are exhibited in police recruits trained under the current pedagogic/militaristic practices?
- How can any weaknesses be mitigated and strengths accentuated through the use of andragogic techniques?

The main take way from this study as it relates to this research is from the results section of the dissertation. From the full data set, the recruits showed that they wanted more hands on training and practical skill development. This fact was also recognized as important by the academy instructors. One of the co-researchers who stated that their own experience would have been improved if there would have been more “practice-based hands-on activities (McCay, 2011, p. 87).”

2.4 Chapter Summary

In almost all of the literature reviewed, the lack of digital forensics or information security training was one of the primary issues for law enforcement. The answer to how to address this issue can be drawn from a combination of all of the reviewed literature. The mechanism to deliver the training to a large group of officer is via on-line courses. In the paper written by Kessler, online courses offer a greater variety of tools to both the instructors and the students. Through the experiment conducted at Champlain, it would appear that the critical piece to the success of the students is in the design of the course and not necessarily the mean by which the material is delivered. To address that specific need using a framework similar to the one developed by NIST in conjunction with applying andragogy principles of adult and Problem Based Learning, would ensure that any online course developed for officers would be successful.

CHAPTER 3. METHODOLOGY

This chapter describes the methodologies, the convenient sample, study sample, data sources, data analysis, and threats to validity, that were used for this study. The following chapter also describes out how the results were recorded.

3.1 Background

This research was the result of project that was completed during the summer 2014. During that summer term, the Digital Evidence Triage (DET) training course offered by Purdue's Cyber Forensics Laboratory, was converted from a traditional class room format to a web based format. The DET training is a three day course that is offered to Law Enforcement Officers (LEOs). In the traditional setting, the DET course was comprised of classroom learning that includes lectures and practical exercises. The material consists of 15 power point presentations containing approximately 246 slides. Each day of the course is structured to fit in the three days. Table 1.1 outlines the objectives for the three days. There is a large portion of this training that is hands on. This gives the officers practical experience with the software and tools.

Table 3.1: DET Course outline

Day	Day 2	Day 3
Context	User Profiles I	Web Artifacts
Basic Computer Components	User Profiles II	Social Networks
Write Blockers	Searching for Graphics	Data Carving
Forensic Imaging	Chronologies & Timelines	Practical Exercise
Evidence Identification & Collection	Memory Analysis	
Digital Evidence Triage Model		

Table 1.2 shows the detailed tasks covered in the three day traditional course. There are a total of 20 different tasks which included the power point presentations and the hands on labs.

Table 3.2: DET Class room task list

Modules		
Welcome/Context	Lab 3 Memory	Lab 5 Timelines
Basic Computer Components	CF Triage Model	Data Carving
Lab 1 - Computer Components	User/Usage Profiles I	Web Artifacts
Write Blockers	User/Usage Profiles II	Lab 6 Web Artifacts
Forensics Imaging	Searching for Graphics	Social Networks.
Lab 2 - Imaging/HWB	Lab 4 Graphics	
Evidence Identification and Collection	Chronology Timelines	
Memory Analysis		

The web based training, modified the original structure to six different modules based on the six different labs. Each module was constructed to flow from one set of power point slides to the next and finishing up at a quiz. Once the fifth module was completed there was a short course review then a comprehensive final test. Table 1.3 shows the outline of the web based course.

Table 3.3: DET Web Based Training Outline

Module 1	Module 2	Module 3	Module 4	Module 5	Module 6
Intro/Welcome (8:30)	Lab 1 - Basic Computer Components	Evidence Identification & Collection	User/Usage Profiles I	Chronology & Timelines	Lab 6 – Email/IM/Chat/History
Course Context	Write Blockers	Memory Collection & Analysis	Use Usage Profiles II	Lab 5 – Timelines	
Basic Computer Components & Documentation	Forensic Imaging	Lab 3 Memory		Data Carving	Review of Course
	Lab 2 – Write Blockers/ Imaging with FTK	CF Triage Model	Lab 4 Graphics	Web Artifacts	Practical Test
Quiz 1	Quiz 2	Quiz 3	Quiz 4	Quiz 5	

Once the structure of the course was completed, the development of the web site was started. The development of the site was broken into several different tasks: determine the programing languages and format the slides, develop the structure for the site, develop questions and answers for the module quizzes and final test, begin development of the site, beta test and refine the site, and deliver the final product. There were three languages used for the development of this site: HTML, MySQL, and PHP. The slides were originally developed for a Macintosh Operating System (OS) and were converted to Microsoft Power Point. From there the Power Point slides were uploaded to Microsoft’s One Drive and code was generated so the slides could be embedded in to the DET website. The structure of the web site was based on the structure outlined above in Table 1.3. Figure 1.1 is shows the structure and flow of the web site.

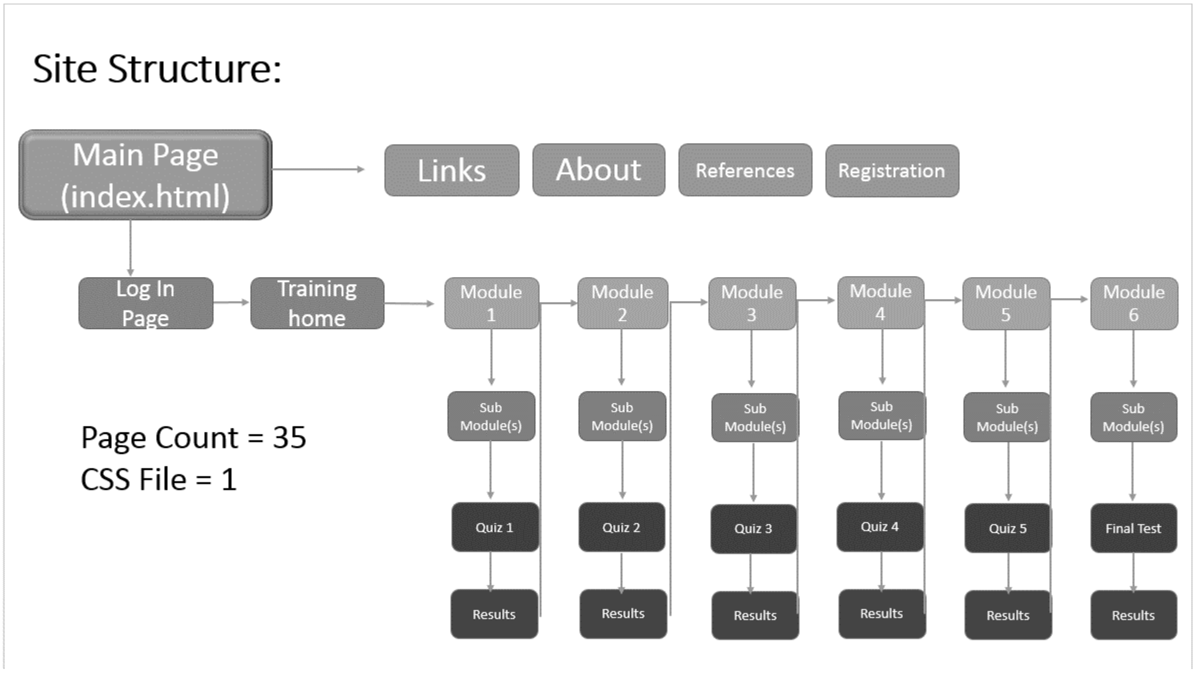


Figure 3.1: DET Web site structure and flow

Once the development of the site was completed beta testing the final product was devilvered to the Cyber Forensics Labartory.

3.2 Hypotheses

For this study there was only be one null hypothesis and one alternative hypothesis. The hypotheses for this thesis was:

H_0: Web based cyber forensics training is not an effective medium to train a large group of law enforcement officers.

H_A: Web based cyber forensics training is an effective medium to train a large group of law enforcement officers.

H_{A1}: Is there a significant difference between the control and treatment 1?

H_{A2}: Is there a significant difference between the control and treatment 2?

H_{A3}: Is there a significant difference between the treatment 2 and treatment 3?

The α for this study is .05, the Margin of Error will be 5%, and the response rate has been set to 50%.

3.3 Convenient Sample

The sample was from 616 field/road personnel from the Indiana State Police Department. The author has been given access to this group by the Superintendent of the Indiana State Police. The sample for this study as stated above came from the field/road officers from the Indiana State Police. Based on the numbers in Section 3.1 the sample size comes to n = 248. Since 248 does not evenly divided into three the sample size was increased to 252. The officers were broken up into three equal groups. Group 1 will be set as the control group. The study is set to last two weeks. At the beginning of the study, all of the officers were given the same pretest. The control group did not go through any of the training material. The other two groups of officers were presented with one of two different treatments. Each treatment covered the same material but were presented in a different manner. Once the officers completed the training material they were presented with the same posttest. At the end of study which lasted one week, the control group was presented with the posttest. Following the posttest, an analysis of the pretest and posttest results was conducted. Figure 3.1 shows the graphical representation of the experimental design.

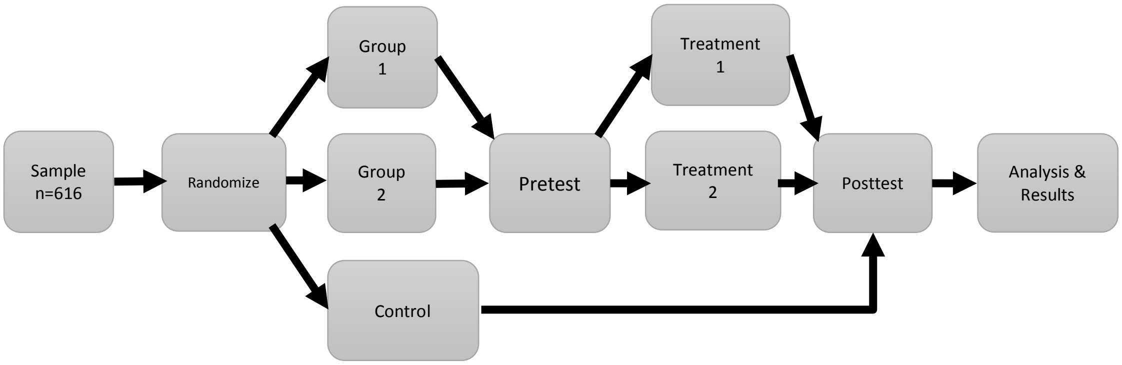


Figure 3.2: *Experiment Design*

3.4 Data Sources

At the end of the study, the subjects were given the option to take an exit survey The survey collected basic information about the subjects: years of service in law enforcement, prior cyber forensics or information security training, if they thought the training was beneficial to them, and if they thought cyber forensics training was needed as a basic part of their duties. The main data sources for this experiment came from the pretests and posttest scores of the three groups. The data will be captured in a MySQL database (DB). The data will be extracted from the DB to a comma separated value (CSV) format. This data will also be compared to data collected from the different journals and papers covered in the literature review.

3.5 Data Analysis

The analysis of the data was conducted of using SAS. The main test that was run was an Analysis of Variance (ANOVA) test. The pretest will be used to determine the base line for each individual. At the group level, the scores will be combined to get the average score and will be used as the baseline for the groups. The average scores as well as the percentage scores for each group were used to compare against the other groups. These scores were used to determine how well the training methods did in presenting the material. Finally, the overall scores were compared to one another to determine which method if any was the most effective at delivering the training material.

3.6 Threats to validity

There were a few different threats of validity of this experiment. One threat was if the subjects already have prior cyber forensics knowledge. A second threat was in the design of the pre and posttests. A third threat was in the design of the survey questions. A fourth threat was in the design of the two different treatments. A fifth threat was in the interpretation of the data from the literature review and the experiment. A six threat was the internal and external construct of the study.

3.7 Chapter Summary

This chapter covered the research question, null hypothesis, alternative hypothesis, population, sample, data sources, data analysis and threats to validity. The data and the analysis from this study will be covered in the next chapter.

CHAPTER 4. FINDINGS

This chapter will discuss the results and findings from the study that was conducted during September 6th, 2015 to September 12, 2015. The main focus of the study was to determine if web based training is an effective medium. For the purposes of this study only those subjects who completed both the pretest and posttest have been included in the analysis (*N*= 616). There were two main data sets used for this analysis, pretest and posttest. Each data set went through a data cleansing process that examined for duplicate entries and missing data points. In the pretest data set there were 19 duplicate entries. This included three users who had three or more entries. From the posttest data set there were only eight users that had duplicate entries. This came to two users with duplicates in Control, one user with a duplicate for Treatment 1 and five users with duplicates for Treatment 2. The first entry for each user in both the pretest and posttest data sets were kept, any additional entries for that subject were purged. In the posttest data set there were three rows that the usernames did not get recorded. In the event there were answers missing in a cell, an ‘X’ was placed in that cell so the data set could be run through SAS.

4.1 Descriptive Statistics

That criteria for selecting subjects was, any officer holding the rank of Trooper, Senior Trooper, Master Trooper, or Squad Sergeant, assigned to road patrol duties from one of the 14 Indiana State Police districts. The convenient sample size for this study came to *N* =616. From the 616 officers, 600 subjects were recruited. These subjects were broken up evenly in to three groups of 200. The groups were designated with the following label:

- Control = Group 1,
- Treatment 1 = Group 2
- Treatment 2 = Group 3

There were a total of 256 subjects that created a username for the study. From those 256 subjects, 215 subject subjects actually started the study by taking the pretest. Though there were 144 subjects that took the posttest, there were six subjects that a pretest score could not be located or did not have a user id associated with it. Those six records were not included in the final comparison analysis. That put the total number of subjects for this study N = 138. The response rate at the adjusted n = 138 was 64.19%

Table 4.1: Basic Study Statistics

Measure	Result
N	616
# Signed up	256
# Started	215
# Finished	144
Response Rate	42.66%
Completion Rate	66.97%

Note. Numbers before data validation

For each test group, the number of points possible and the number of points scored were totaled. The total points scored by each group was calculated. The pretest had 20 questions with each question worth one point. The posttest had 40 questions worth one point each. These totals were used to calculate the grade percentage for the groups. The basic break down of the groups for the pretest can be seen in Table 4.2. This table includes the total score possible and the total points scored for each group for both tests. The number of subjects for the control group (Group 1) and treatment 1 (Group 2) are exactly the same. There is a noticeable difference between the posttest scores for the treatment groups. This is most like attributed to there being an additional nine subjects in group three. For the most part the number of subjects in each group was distributed fairly even. The means for each of the groups for the pretest are fairly close to each other, which shows that the subjects had about the same level of knowledge of cyber forensics prior to the study.

4.2 Data Exploration

The hypothesis for this research stated that "Web based cyber forensics training was not an effect medium to train a large group of law enforcement officers. The main test that was used on this data set was the three way ANOVA test. This test was designed to reveal if there were any interaction effects between three independent variables "GroupID" on the dependent variable "percentchanged." The syntax used in SAS was:

```
ods graphics on; proc mixed data=prepost; class groupid; model percentchange =
groupid /residual; lsmeans groupid / alpha=.05; run;]
```

To determine if the data sets were normal, a QQplot was generated based on the residuals of the variable “Percentchanged” (residual = actual – predicted). The results showed that the data was normal.

4.3 Hypothesis Testing

The statistics for this study were *N* = 616, *n* = 138, *r = .012* and α = .05. The Type 3 Test of Fixed Effects was run to examine the significance of the independent variable “Group ID.” This test shows that there is statistical significance and that the null hypothesis can be rejected.

Table 4.2: Type 3 Test of Fixed Effects

Type 3 Tests of Fixed Effects				
Effect	Num DF	Den DF	F Value	Pr > F
GroupID	2	135	14.83	<.0001

To further test the three questions in table 4.2, an ANOVA test was used to test the depended variable “Percentchanged” to the independent variable “GroupID”. This method used the combination of the observed values to test the relationship between the independent value and the depended value. This test was specifically used because the study was looking at the change in the scores from the pretest to the posttest. The mixed ANOVA showed an effect of percent changed on Group ID. The control group *Standard Error Mean* (*SEM)* = .02, *Standard Error SE* = 0.17, *t*(135) = 1.36 and *p* = .1768. For treatment group 1 *SEM* = .139, *SE*= 0.17, *t*(135) = 8.11 and *p* = <.0001. For treatment group 2 *SEM* = .132, *SE* = .015, *t*(135)= 8.52 and *p* = <.001. The results show that the subjects in the treatment group 1 and treatment group 2 had statistical significantly higher scores at the end of the study than the control group with the treatment groups.

4.3.1 Hypothesis Treatment 1

Question one asked "Is there statistical significance between treatment one and the control group. The results from the ANOVA test show that there is a statistical significance. The p-value for treatment 1 *p* = <.0001, which is below α = .05 and the estimate (.139) falls within the *CI* (.1051, .1728). The decision based on this result is to reject the null hypothesis.

Table 4.3: ANOVA Results Control vs. Treatment 1

Effect	Group ID	Estimate	Std Err	DF	t Value	Pr > |t|	Alpha	95% Confidence Interval	
								Lower	Upper
Group ID	**1**	0.02326	0.01713	135	1.36	0.1768	0.05	-0.01062	0.05713
Group ID	**2**	0.1390	0.01713	135	8.11	<.0001	0.05	0.1051	0.1728

4.3.2 Hypothesis Treatment 2

Question two asked “Is there statistical significance between treatment one and the control group. The results from the ANOVA test show that there is a statistical significance. The p-value for treatment 2 *p* = <.0001, which is below α = .05 and the estimate (.02) falls within the *CI* (.1019, .1635). The decision based on this result is to reject the null hypothesis.

Table 4.4: ANOVA Control vs. Treatment 1

Effect	Group ID	Estimate	Std Err	DF	t Value	Pr > |t|	Alpha	95% Confidence Interval	
								Lower	Upper
Group ID	**1**	0.02326	0.01713	135	1.36	0.1768	0.05	-0.01062	0.05713
Group ID	**3**	0.1327	0.01557	135	8.52	<.0001	0.05	0.1019	0.1635

4.3.3 Hypothesis Treatment 1 and Treatment 2

To determine if there was a statistical significance between the two treatments there were a couple of points in the ANOVA test that can be used. First, looking at the estimates for each group. The two estimates are extremely close. Second, the standard errors are extremely close as well. The last set of numbers to be used were the lower/upper limits or the confidence intervals for each group. There is considerable overlap between the two confidence intervals.

Table 4.5: ANOVA Treatment 1 vs. Treatment 2

Effect	Group ID	Estimate	Std Err	DF	t Value	Pr > |t|	Alpha	95% Confidence Interval	
								Lower	Upper
Group ID	2	0.1390	0.01713	135	8.11	<.0001	0.05	0.1051	0.1728
Group ID	3	0.1327	0.01557	135	8.52	<.0001	0.05	0.1019	0.1635

4.4 Chapter Summary

The response rate to the study was 41.55%. The completion rate was 66.97%. As documented in the exit survey there were some technical issues with the website. The ANOVA test run on the data set of the 138 subjects who completed the study, showed that there was statistical significance between the control and treatment 1. There was also statistical significance between the control and treatment 2.The p-value for both treatment 1 and treatment 2 was *p* = <.0001. With these results, there is enough evidence to reject the null hypothesis. The exit survey was completed by 106 of the 138 subjects who completed the study. The response rate for the exit survey was 76.81%. The full results of the exit survey can be found in Appendix C.

CHAPTER 5. DISCUSSION AND CONCLUSION

The hypothesis of this study was that web based cyber forensics training was not an effective medium to train a large group of law enforcement officers. The data provided enough evidence that the percentage change in the posttest scores from the pretest scores are significantly different and that H_0, can be rejected. The results from this study are similar to the study performed at Champlain University in 2007. In that study there was significance between the control and the two delivery modes (Kessler, 2007). The results of this study would go to validate the results from the Champlain study. There was one major difference between their study and this one: this study focused solely on Law Enforcement Officers.

The training material that was presented to the officers was not originally designed to be presented in a web based learning environment and it was designed for an audience with technical experience. Additionally, the web site was designed to only facilitate the basic functions of the study. The biggest reason for that was to make it as simple as possible to navigate and to minimize the potential technical problems that could possibly occur. Even with that, there were still technical issues, some of which, were documented in the exit survey. It would appear that the biggest issue was with the slides not playing. More than likely with the demand the 138 subjects accessing the slides at the same time, was causing delays and the slides to be non-responsive. Given those circumstances, the web based training was able to effectively deliver the cyber forensics training material to those subjects in both treatment groups.

There were some comments that the training was too technical and that it was too in-depth. It is this author's opinion that these statements go to strengthen the need for the tiered approach that Cohen introduced in the March 2007 article in Police Chief Magazine. This need for tiered training is also echoed in NIST SP 800-16 in the Information Technology Security Learning Continuum. More so the learning continuum needs to be incorporated with the "Cyber Forensics Ontology" proposed by Brinson et al.

5.1 Implications of the Study

This author was only able to locate a small amount of research that specifically addressed how to solve the training needs, issues and problems of the cyber forensics field. One of the goals of this research was to add to that body of knowledge. With the results of this study there are several important implications from showing that web based training is an effective means to teach and train a large group of law enforcement officers in cyber forensic,

First, this gives agencies the opportunity to present this material to their officers without having to cause major interruptions to their operations. Second, the agencies would not have the additional cost of housing, fuel and per diem. A third implication of this study was that there is a clear picture on how to create a training gold standard in cyber forensics. This type of standard is needed in the domain. Even anecdotally observed in the exit survey, that some sort of cyber forensics training is needed as part of the basic performance for officers. The vast majority of the respondents to the exit survey, 84%, responded positively to this statement.

Fourth, quality training is critical for any law enforcement agency. When an officer is testifying in a court hearing, their training can be called into question and be heavily scrutinized. As well, an agency can be held liable under 42 U.S.C, 1983 for not properly training its employees (Walker and Hemmens, 2008). Thus any training they receive must be able to stand up to those legal challenges. The quality of the training is not only important for the purposes of court but it will also aid in the buy-in within the law enforcement community. Lastly, the successfulness web based training it is extremely important that at every stage of the development it should be documented, reviewed, and assessed by the administration, to ensure it stands up to the most challenging tests.

Last, the financial restraints of the traditional classroom courses, operational needs of an agency, travel costs, per diem costs, classroom sizes and troopers away from their districts are all major issues that have to be considered. There are also issues with presenting these courses in academies due to the considerable demand on the agencies to cover all of the material required by state law.

5.2 Lessons learned

The main purpose of the exit survey was to get a subjective view of the training from the Troopers who went through the entire study. The results of the exit study were used to get an idea of the areas where the training was weak, the areas that were strong, to determine what works for this level of officer and to observe those things that did not work. There were some very brutally honest remarks and criticisms about this study. However, on the other side of the spectrum, there were comments and suggestions that will prove extremely valuable in any future development of web based cyber forensics training. There were few key take a ways from the exit survey:

- Future training needs to be further refined for the basic road officer tier.
- The technology that runs the training slides needs to be robust to handle a high level of demand.
- At the end of each training module, quizzes or other methods need to be used to reinforce the material that was covered.

The lessons that are discussed by McCay (2011), Shipton (2009), McCoy (2006), and Etter and Griffin (2009), in some aspect, have been observed in this study. McCoy discusses the amount of investigative information that officers can have access to through computers. This amount is exponentially multiplied when cyber forensics is involved. There have been several advancements in technology since 2006, when McCoy published his article. With the technology available today, a person’s smart phone collects information about every aspect of their day. When an officer or detective is investigating a crime, this information could quickly exclude a person from their investigation or it could speed the investigation to include an individual. Speaking directly about this type of training, McCoy continued that the training/curriculum must be flexible, include peer support, and class room instruction. These also should be paired with components of the training being hands on and including practical exercises (McCay, 2011). As well, management and administration support is key in the development of the training to insure that the training meets the needs of that department (McCoy, 2006). These officers do see the value in which cyber forensics can add to their basic duties. The same percentage of respondents also said they would attend other web based training if it was provided to them for free.

5.3 Future Research

One thing is evident from this study, more research is needed. There are a several areas that need further study. All of these areas have one thing in common, how to increase the effectiveness of web based cyber forensics training. First, the research should be conducted on the different web based training approaches. These results could also be used against current data points of traditional classroom approaches. Additional research could be conducted with the Indiana State Police to see if there was an increase in the number of cyber forensics cases generated by the district troopers. With the given nature of the profession, officers are often interrupted during their shift. Additional research could should be conducted to understand how much of the information is retained if they were to get interrupted while going through a module. Supplementary research is needed to understand how the addition of quizzes, interactive features and other retention methods can be used to increase the effectiveness of web based cyber forensics training.

Additional research is needed to determine the proper blend of the different leaning methods to maximize the effectiveness. This includes the need for this training to be hands on. McCay's 2011 study has shown that officers have a strong preference for hands on scenario based training (p. 87). More research is needed to determine how to replicate or virtualize the hands on experience that is typically found in traditional classrooms. As well further research should be conducted to discover effective alternativeness to replicate the overall class experience. This experience of being able to interact with other students and the instructor(s) is a variable that could affect the overall effectiveness of a training course. Finally, another important area to continue to research surrounds the development of the two treatments from this study. The specific slides from this study should be thoroughly analyzed to determine the areas that were the most effective. From that analysis a new set of training modules should be developed.

5.4 Conclusion

The use of technology is continually growing at an exceedingly rapid pace. The continued integration of devices to the Internet is showing no sign of slowing down. The data that is contained on these devices can turn into information that is extremely valuable to law enforcement officers. Acquiring this data and understanding what it means is going to require a new type of officer. For this to happen, it would require a major paradigm shift with the level of technical abilities needed by these future law enforcement officers. There are currently skills that LEO’s have that are technical in nature. The reason they learn those skills is to increase their self-sufficiency in the performance of their daily responsibilities. This is also true for the basic technical skills needed for cyber forensics. With all the reasons previously described, the need for LEOs to have these Knowledge Skills, Abilities (KSAs) and have the means to learn this them, is long past due. Web based training is a very realistic and viable medium to give all law enforcement officers the necessary KSAs in cyber forensics to meet those growing demands.

LIST OF REFERENCES

LIST OF REFERENCES

Amador, S. L. (1986). Adult computer literacy: A marketing opportunity with financial rewards. New Directions for Adult and Continuing Education, 1986(29), 79-87.

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. *Communications of the ACM*, 49(2), 3.

Bogolea, B. & Wijekumar, K. (2004). Information security curriculum creation: A case study, *InfoSecCD Conference 2004.*

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Elsevier, 7*.

Cohen, C. (2007). Growing challenge of computer forensics. *Police Chief Magazine 3*(74).

Crowley, E. (2003). Information systems security curricula development, *CITC4*, *11*, 16-18.

Duggan, M (2013). Cell phone activities 2013. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.

Etter, G., Griffin, R. (2009) In-service training of older law enforcement officers: an andragogical argument. *Policing: An International Journal of Police Strategies & Management*, *34*(2), 233-245 DOI 10.1108/13639511111148861.

Fernandez, J. (2005). Computer forensics: A critical need in computer science programs. *Consortium for Computing Sciences in Colleges*, *4*, (315-322).

Garfinkel, S. (2010). *Digital forensics research: The next 10 years*. Elsevier, Digital Investigation *7*(S64 eS73).

Gottschalk, L., Liu, J., Dalhan, B., Fitzgerald, S., Stien, M. (2005). Computer forensics programs in higher education: A preliminary study, *SIGCSE 2005*, (147-151).

Knowles, M.S. (1990). *The Adult Learner: A Neglected Species*, 4th ed., Gulf Publishing Company, Houston, TX.

Harrison, W., Hueston, G., Mocas, S., Morrissey, M, & Richardson, J. (2004). High tech forensics. Communications of the ACM, 47(7), 5.

Kessler, G. (2007). Online education in computer and digital forensics: A Case Study. *Hawaii International Conference on System Sciences*, (1-10).

McCoy, M. (2006). Cops, computers and the curriculum. *International Journal of Police Science & Management*, *8*(2), (153-158).

McCoy, M. (2006). Teaching style and the application of adult learning principles by police instructors. *Policing, an International Journal of Police*, 29(1), (77-91).

Pew Research Center. (2014). Mobile technology fact sheet. *Pew Research Center*. Retrieved from http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

Scientific Working Group Digital Evidence, 2001, (SWGDE). Digital evidence: standards and principles. Forensic Science Communications, Volume 2 (Issue 2).

Shipton, B. (2009). *Problem based learning:* Does it provide appropriate levels of guidance and flexibility for use in police recruit education? Journal of Learning Design, *3*(1), 11.

Stambaugh, H., Beaupre, D., Icove, D., Cassaday, W., & Williams, W. (2001). State and local law enforcement needs to combat electronic crime. National Institute of Justice Research in Brief.

Taylor, T.Z., Elison - Bowers, P., Werth, E., Bell, E., Carbajal, J., Lamm, K, & Velazquez E. *A police officer's tacit knowledge inventory (POTKI): establishing construct validity and exploring applications* Police Practice and Research: An International Journal, *14*(6) 478-490, DOI: 10.1080/15614263.2013.802847

Webster. (1988). *Webster's new world dictionary of American English* (3rd College Ed.). New York, NY: Webster's New World.

Wilson, M., deZafra, D., Pitcher, S., Tressler, J., Ippolito, J. (1998). Information technology security training requirements: A Role- and Performance-Based Model. *NIST* 800-16.

APPENDICES

Appendix A Consent Form

Purpose of Research: The purpose of this research is to determine if web based cyber forensics training is an effective medium to train a large group of Law Enforcement Officers

What will I do if I choose to be in this study? The anonymous, online training will be administered using a secure website. Once you have read this consent form, and agree to voluntarily participate, you will be taken to a secure website to complete the online training. You may withdraw from the survey at any time or any reason

How long with the study be? You should expect to spend a minimum of 2 hours but it may take as much as 8 hours to complete this training. We understand that this is a lengthy time commitment. This training does not have to be completed in a single session. It is self-paced and you can return to the place where you left off.

What are the possible risks? The risks to you are minimal. They are not greater than those ordinarily encountered in daily life. Please know that this is an anonymous survey that uses a secure link. The survey is anonymous because we will not be able to link your responses back to you – we do not ask for any identifiable information (Ex. name). While completing the training the only risk to you might be if someone were to see your pretest and post test scores. In addition, some of the questions may contain law enforcement sensitive material. We recommend you take this training in an area way from public view Even then, your responses to the survey could never be linked back to you. We appreciate your participation in this scientific research.

Are there any potential benefits? This training is designed to improve your knowledge, skills, and abilities in cyber forensics. There are no direct benefits to you. The information you learn from this training can be used in your day to day assigned duties. However, this training will not make you a certified cyber forensics examiner or expert. This is to give you another tool for your tool box.

Will information about me and my participation be kept confidential? We do not ask for your name or any other information that could be used to identify you at any time before, during, or after the survey. No IP addresses will be recorded. There will be no way to determine where the training was taken or by whom. Instead, the training software will assign an ID number to you upon clicking the submit button. This means that the responses to the pre and posttest cannot be linked or matched to you, which means your responses will remain completely anonymous. Only researchers associated with this study will have access to the data. In addition to the data being anonymous, it will be stored electronically in an encrypted format. The encrypted data will be kept indefinitely and will be used only for research purposes. The project's research records may be reviewed by departments at Purdue University responsible for regulatory and research oversight.

What are my rights if I take part in this study? Your participation in this study is completely voluntary and you may withdraw from the study at any time or skip any questions that you feel uncomfortable answering.

Who can I contact if I have questions about the study? If you have any questions about this survey either before or after completion, you may contact Dr. Marcus Rogers, rogersmk@purdue.edu. If you have questions about your rights as a person taking part in a research study, or if you would like to make suggestions or file complaints and concerns, you may call 765-494-5942. For technical assistance please contact your training section, give them your assigned user ID and they will make contact with technical support.

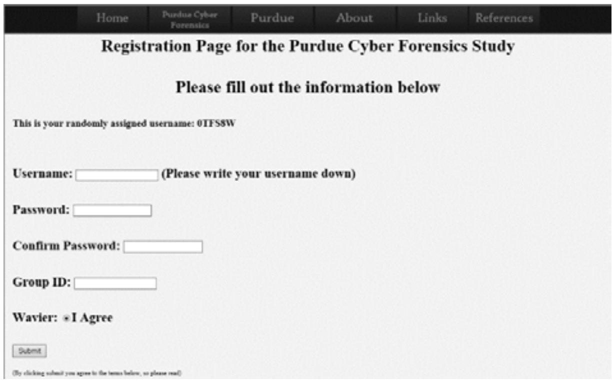
If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email)irb@purdue.edu) or write to

Human Research Protection Program - Purdue University
Ernest C. Young Hall, Room 1032
155 S. Grant St.
West Lafayette, IN 47907-2114

You’re Consent to Continue. If you are 18 years of age or older, you freely agree to participate in this study, have had the opportunity to read this consent form, had the research study explained, had the opportunity to ask questions about the project and have them answered, then please click on the “I Agree” button above. Otherwise, do not proceed any further.

Appendix B Study Directions

1. The subjects were directed to enter the randomly generated user name into the user name field, enter in a password, confirm the password, and enter in the group id they were emailed. By them clicking on the submit button they agreed to the consent form and agreed to waive their signature.



Registration Page for the Purdue Cyber Forensics Study

Please fill out the information below

This is your randomly assigned username: 0TFS8W

Username: (Please write your username down)

Password:

Confirm Password:

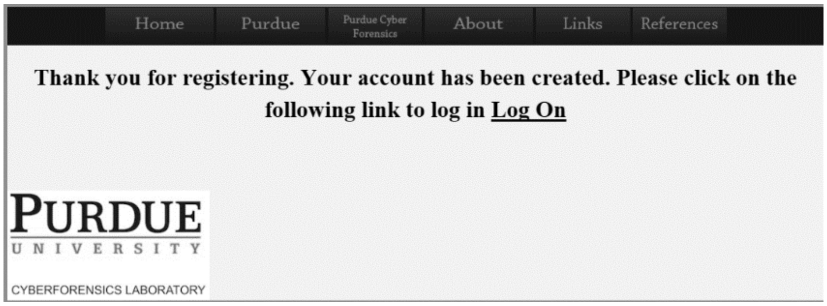
Group ID:

Wavier: ● I Agree

(By clicking submit you agree to the terms below, so please read)

Figure B.1: Study Registration Page

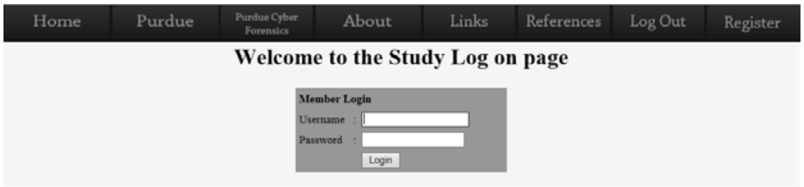
2. After clicking on the submit button the subjects were redirected to a new page. They subjects were given the option to log.



Thank you for registering. Your account has been created. Please click on the following link to log in Log On

Figure B. 2: Registration Confirmation Page

3. Either after clicking on the link from the confirmation page or entering in the URL in to their browser, they were directed to the log in page for the study.



Welcome to the Study Log on page

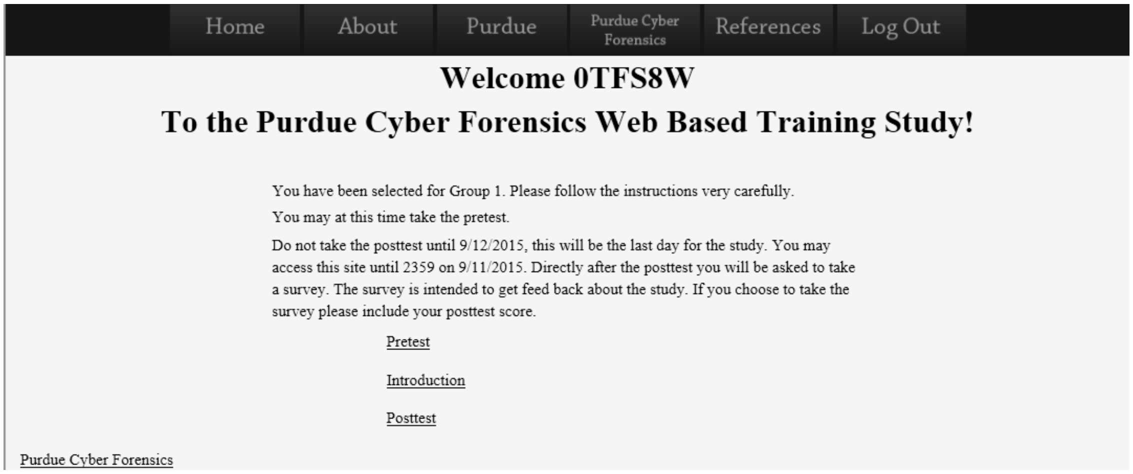
Member Login

Username :

Password :

Figure B.3: Log on page

4. Depending on what group the subject entered when they registered determined what content they were shown.



Welcome 0TFS8W

To the Purdue Cyber Forensics Web Based Training Study!

You have been selected for Group 1. Please follow the instructions very carefully.

You may at this time take the pretest.

Do not take the posttest until 9/12/2015, this will be the last day for the study. You may access this site until 2359 on 9/11/2015. Directly after the posttest you will be asked to take a survey. The survey is intended to get feed back about the study. If you choose to take the survey please include your posttest score.

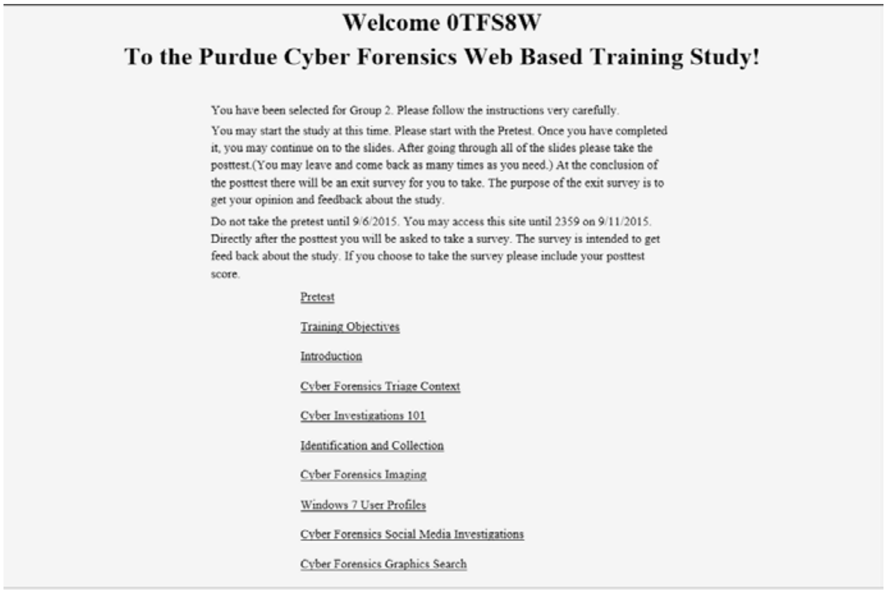
Pretest

Introduction

Posttest

Purdue Cyber Forensics

Figure B.4: Group 1 Study Home Page



Welcome 0TFS8W

To the Purdue Cyber Forensics Web Based Training Study!

You have been selected for Group 2. Please follow the instructions very carefully.

You may start the study at this time. Please start with the Pretest. Once you have completed it, you may continue on to the slides. After going through all of the slides please take the posttest.(You may leave and come back as many times as you need.) At the conclusion of the posttest there will be an exit survey for you to take. The purpose of the exit survey is to get your opinion and feedback about the study.

Do not take the pretest until 9/6/2015. You may access this site until 2359 on 9/11/2015. Directly after the posttest you will be asked to take a survey. The survey is intended to get feed back about the study. If you choose to take the survey please include your posttest score.

Pretest

Training Objectives

Introduction

Cyber Forensics Triage Context

Cyber Investigations 101

Identification and Collection

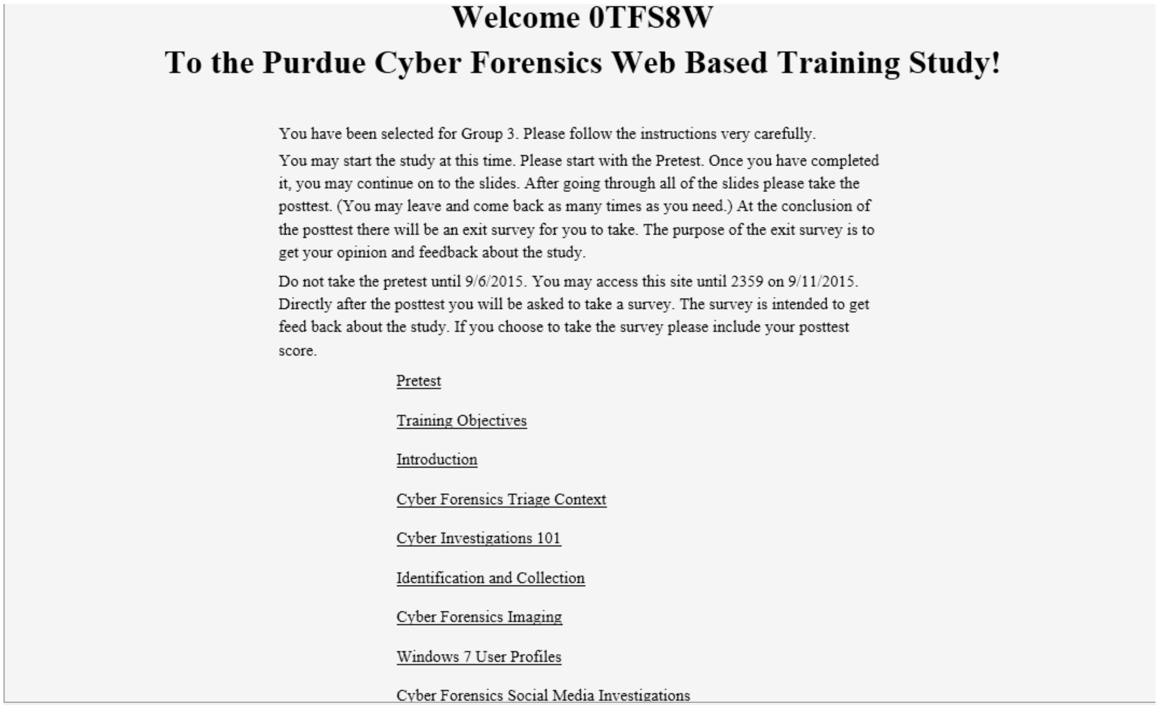
Cyber Forensics Imaging

Windows 7 User Profiles

Cyber Forensics Social Media Investigations

Cyber Forensics Graphics Search

Figure B.5: Group 2 Study Home Page



Welcome 0TFS8W

To the Purdue Cyber Forensics Web Based Training Study!

You have been selected for Group 3. Please follow the instructions very carefully.

You may start the study at this time. Please start with the Pretest. Once you have completed it, you may continue on to the slides. After going through all of the slides please take the posttest. (You may leave and come back as many times as you need.) At the conclusion of the posttest there will be an exit survey for you to take. The purpose of the exit survey is to get your opinion and feedback about the study.

Do not take the pretest until 9/6/2015. You may access this site until 2359 on 9/11/2015. Directly after the posttest you will be asked to take a survey. The survey is intended to get feed back about the study. If you choose to take the survey please include your posttest score.

Pretest

Training Objectives

Introduction

Cyber Forensics Triage Context

Cyber Investigations 101

Identification and Collection

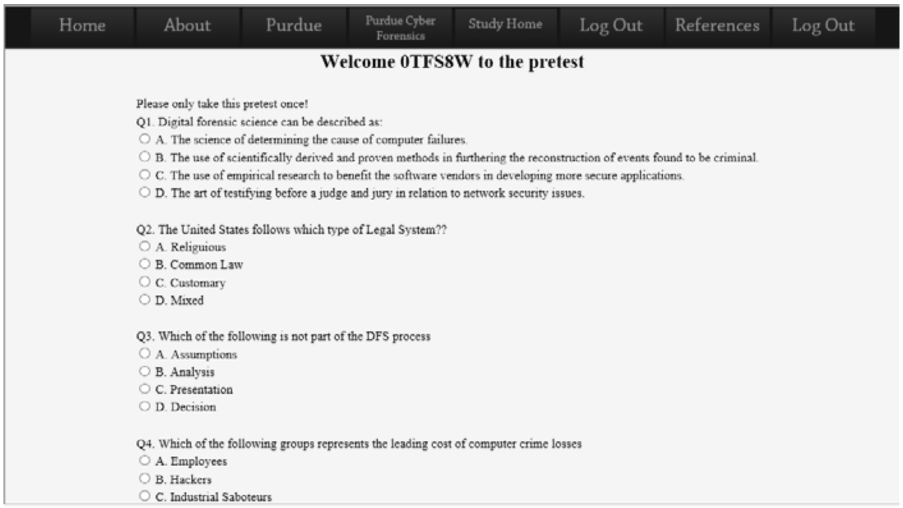
Cyber Forensics Imaging

Windows 7 User Profiles

Cyber Forensics Social Media Investigations

Figure B.6: Group 3 Study Home Page

5. Each group was then asked to take the pretest. The pretest questions can be found in Appendex D. Figure B6 shows how the page looked to the study subjects.



Welcome 0TFS8W to the pretest

Please only take this pretest once!

Q1. Digital forensic science can be described as:

○ A. The science of determining the cause of computer failures.
○ B. The use of scientifically derived and proven methods in furthering the reconstruction of events found to be criminal.
○ C. The use of empirical research to benefit the software vendors in developing more secure applications.
○ D. The art of testifying before a judge and jury in relation to network security issues.

Q2. The United States follows which type of Legal System??

○ A. Religuious
○ B. Common Law
○ C. Customary
○ D. Mixed

Q3. Which of the following is not part of the DFS process

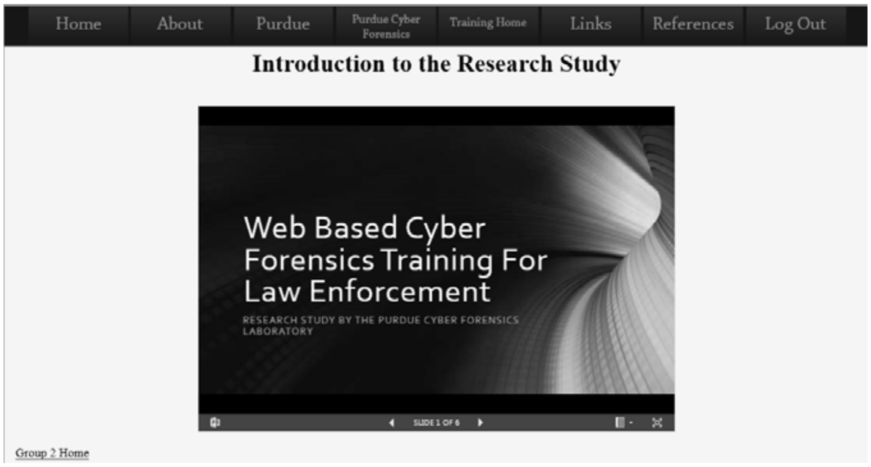
○ A. Assumptions
○ B. Analysis
○ C. Presentation
○ D. Decision

Q4. Which of the following groups represents the leading cost of computer crime losses

○ A. Employees
○ B. Hackers
○ C. Industrial Saboteurs

Figure B.7: Pretest Page

6. After completing the pretest, the subjects were directed to an introductory set of slides. These slides covered the purpose of the study and reiterated the major points from the waiver (i.e. that their participation was completely voluntary.



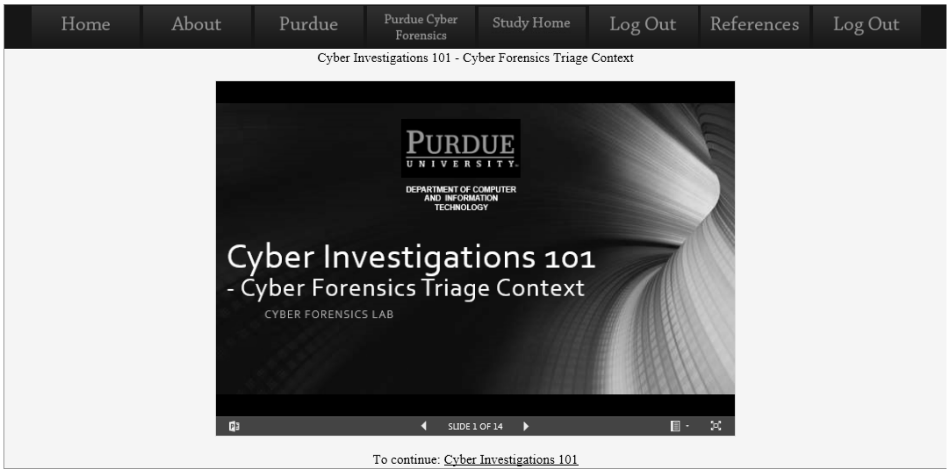
Introduction to the Research Study

Web Based Cyber Forensics Training For Law Enforcement

RESEARCH STUDY BY THE PURDUE CYBER FORENSICS LABORATORY

Figure B.8: Introduction Slides

7. The first set of training slides the subjects were presented was titled “Cyber Investigations 101 – Cyber Forensic Triage Context.” There were 14 slides that made up this module.



Cyber Investigations 101 - Cyber Forensics Triage Context

DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGY

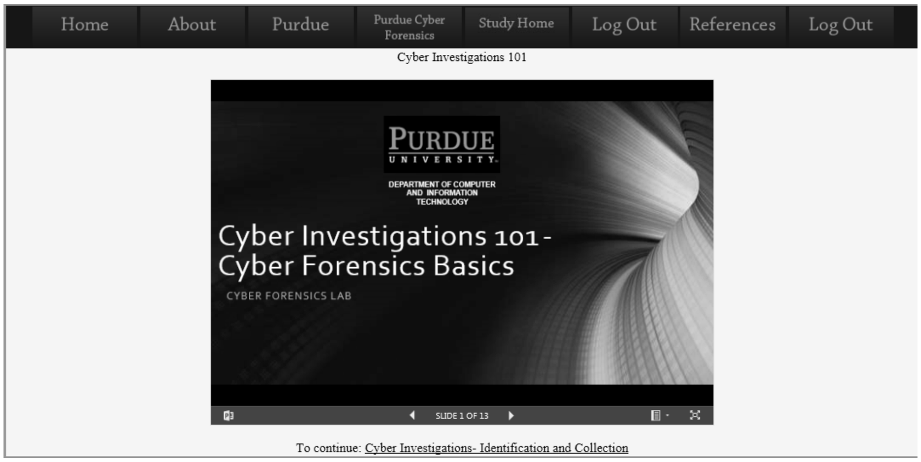
Cyber Investigations 101 - Cyber Forensics Triage Context

CYBER FORENSICS LAB

To continue: Cyber Investigations 101

Figure B.9: Cyber Investigations 101 – Cyber Forensic Triage Context

8. The second set of training slides for the study was titled “Cyber Investigations 101 – Cyber Forensics Basics.” There were



Cyber Investigations 101

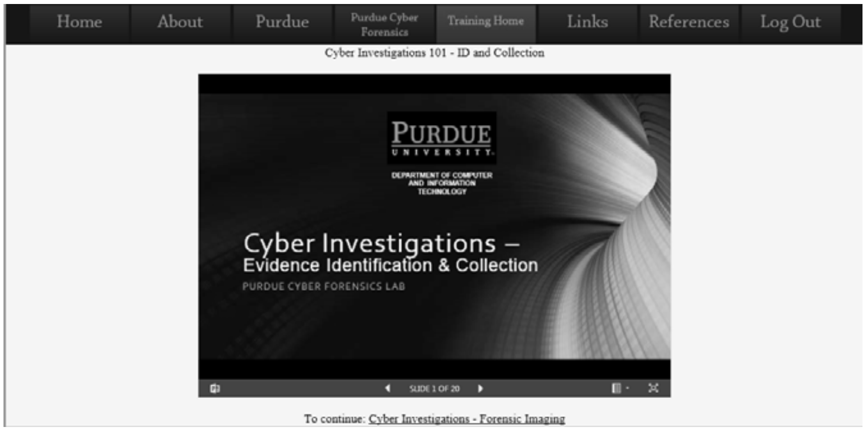
Cyber Investigations 101 - Cyber Forensics Basics

CYBER FORENSICS LAB

To continue: Cyber Investigations- Identification and Collection

Figure B. 10: Cyber Investigations 101 – Cyber Forensics Basics

9. The third set of traing slide for the study was titled “Cyber Investigations – Evidence Indentification & Collection.”



Cyber Investigations 101 - ID and Collection

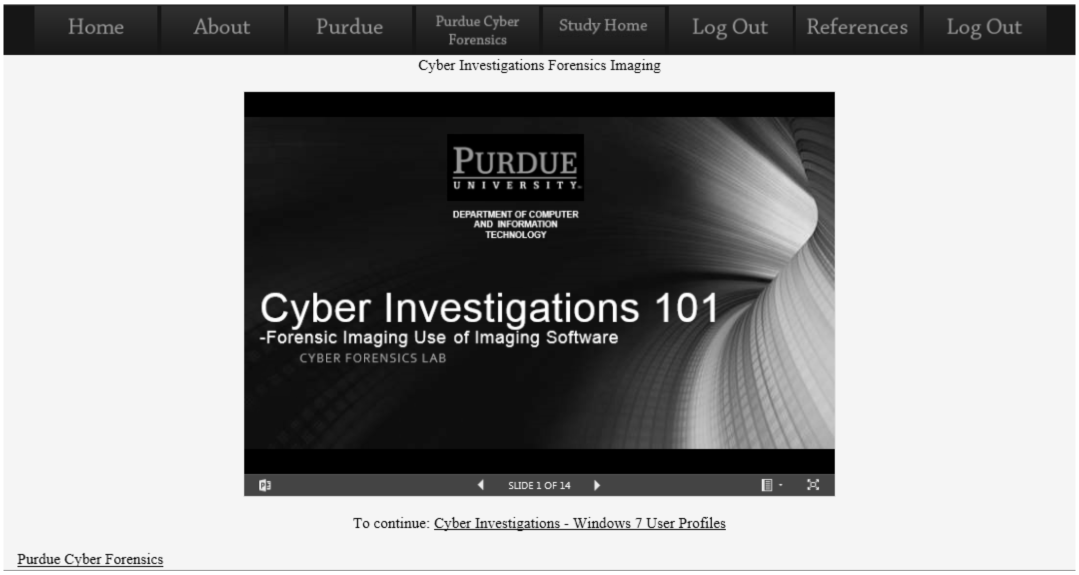
Cyber Investigations – Evidence Identification & Collection

PURDUE CYBER FORENSICS LAB

To continue: Cyber Investigations - Forensic Imaging

Figure B.11: Cyber Investigations – Evidence Identification & Collection

10. The fourth set of traing slide for the study was titled “Cyber Investigations 101 – Forensics Imaging Use of Imaging Software.”



Cyber Investigations Forensics Imaging

PURDUE UNIVERSITY

DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGY

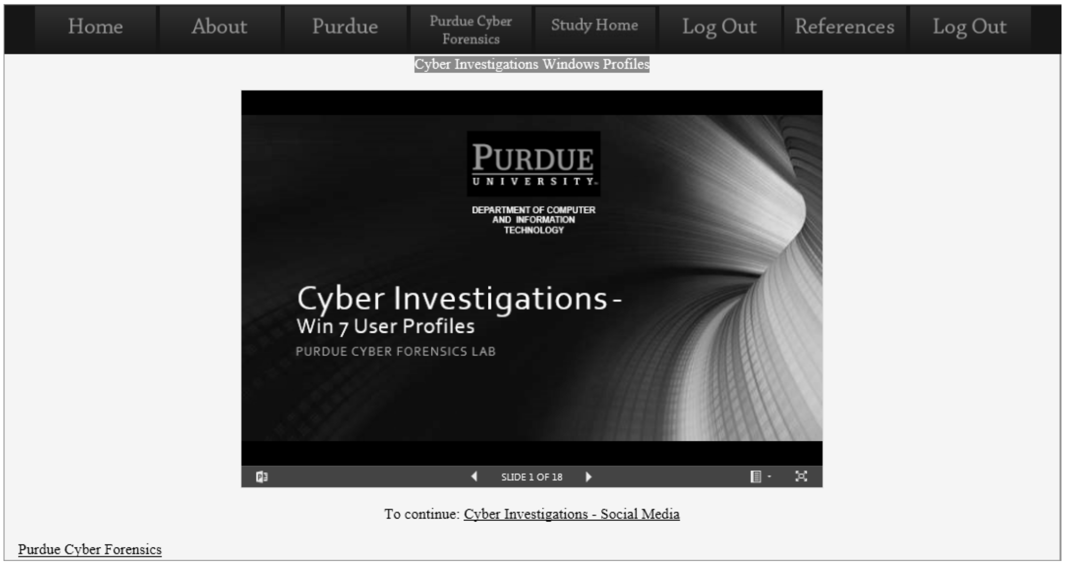
Cyber Investigations 101
-Forensic Imaging Use of Imaging Software
CYBER FORENSICS LAB

To continue: Cyber Investigations - Windows 7 User Profiles

Purdue Cyber Forensics

Figure B.12: Cyber Investigations 101 – Forensics Imaging Use of Imaging Software

11. The fifth set of traing slide for the study was titled “Cyber Investigations Windows 7 User Profiles.”



Cyber Investigations Windows Profiles

PURDUE UNIVERSITY

DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGY

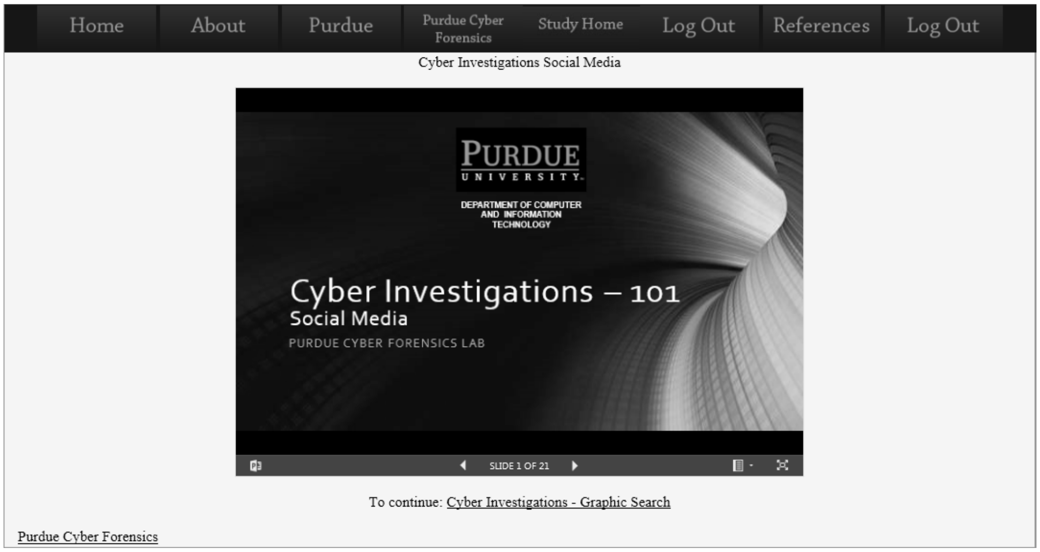
Cyber Investigations -
Win 7 User Profiles
PURDUE CYBER FORENSICS LAB

To continue: Cyber Investigations - Social Media

Purdue Cyber Forensics

Figure B.13: Cyber Investigations Windows 7 User Profiles

12. The sixth set of traing slide for the study was titled “Cyber Investigations - 101 Social Media.”



Cyber Investigations Social Media

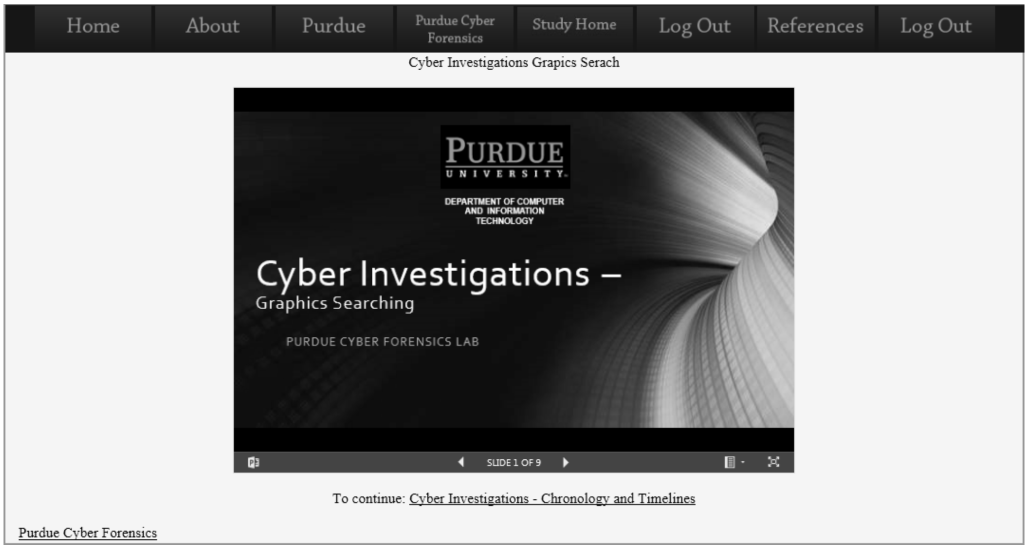
Cyber Investigations – 101
Social Media
PURDUE CYBER FORENSICS LAB

To continue: Cyber Investigations - Graphic Search

Purdue Cyber Forensics

Figure B.14: Cyber Investigations Windows 7 Social Media

13. The seventh set of traing slide for the study was titled “Cyber Investigations Graphics Searching.”



Cyber Investigations Grapics Serach

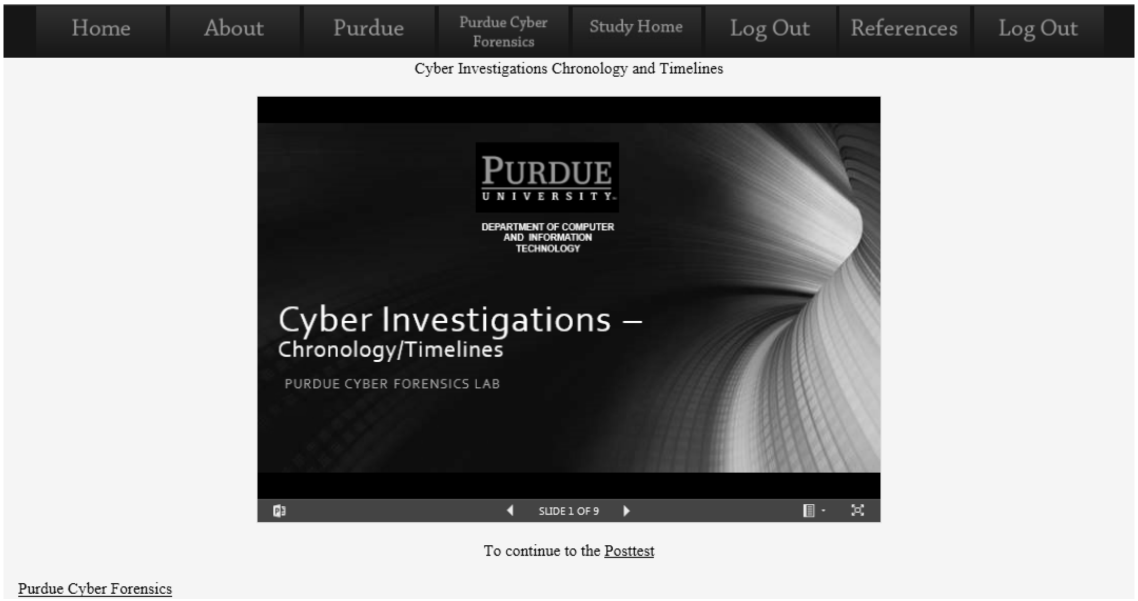
Cyber Investigations –
Graphics Searching
PURDUE CYBER FORENSICS LAB

To continue: Cyber Investigations - Chronology and Timelines

Purdue Cyber Forensics

Figure B.15: Cyber Investigations Graphics Searching

14. The seventh set of traing slide for the study was titled “Cyber Investigations Graphics Searching.”



Cyber Investigations Chronology and Timelines

PURDUE UNIVERSITY
DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGY

Cyber Investigations – Chronology/Timelines

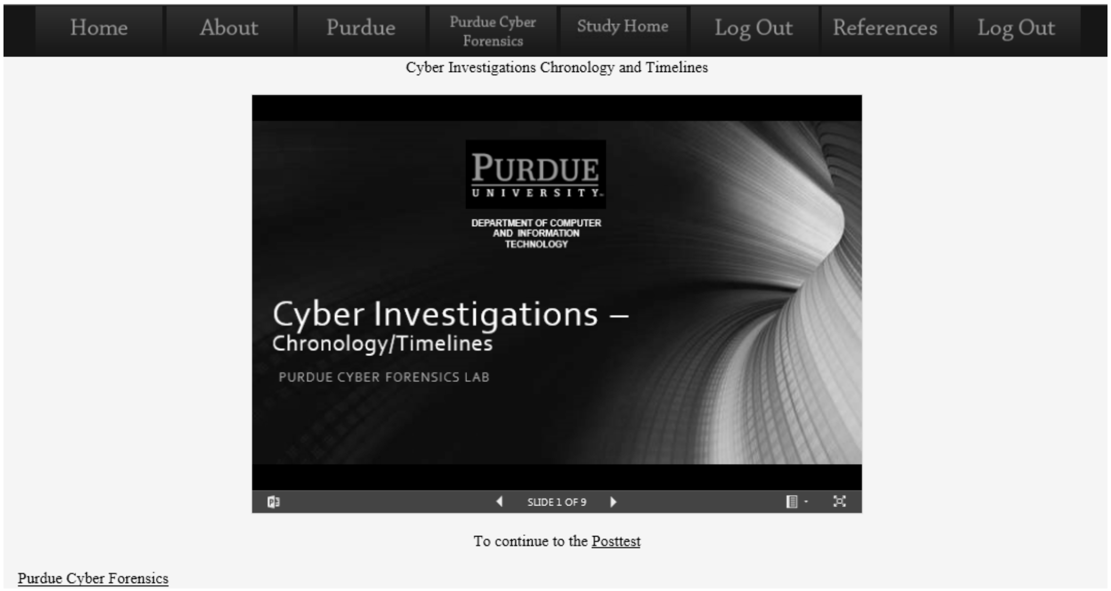
PURDUE CYBER FORENSICS LAB

To continue to the Posttest

Purdue Cyber Forensics

Figure B.16: Cyber Investigations Graphics Searching

15. The last set of slides the subjects were presented was "Cyber Investigations – Chronlogy/Timelines."



Cyber Investigations Chronology and Timelines

PURDUE UNIVERSITY
DEPARTMENT OF COMPUTER AND INFORMATION TECHNOLOGY

Cyber Investigations – Chronology/Timelines

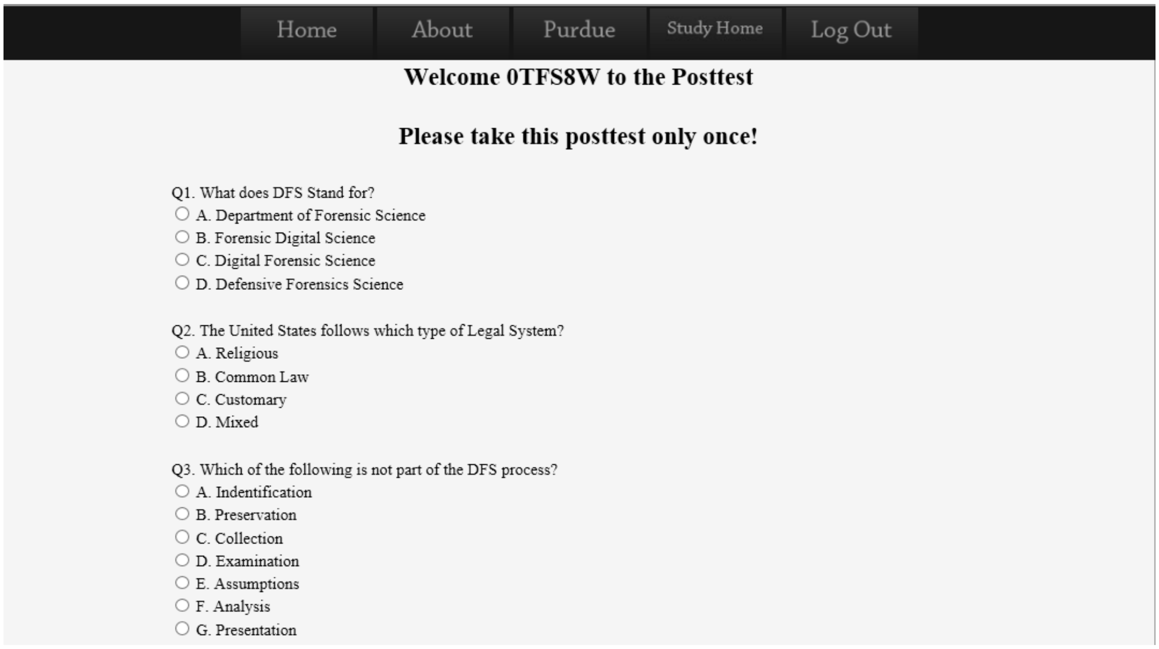
PURDUE CYBER FORENSICS LAB

To continue to the Posttest

Purdue Cyber Forensics

Figure B.17: Cyber Investigations – Chronology/Timelines

16. The second to last step in this study was for the subjects to take the posttest. The posttest questions can be seen in Appendix E.



Welcome 0TFS8W to the Posttest

Please take this posttest only once!

Q1. What does DFS Stand for?
○ A. Department of Forensic Science
○ B. Forensic Digital Science
○ C. Digital Forensic Science
○ D. Defensive Forensics Science

Q2. The United States follows which type of Legal System?
○ A. Religious
○ B. Common Law
○ C. Customary
○ D. Mixed

Q3. Which of the following is not part of the DFS process?
○ A. Indentification
○ B. Preservation
○ C. Collection
○ D. Examination
○ E. Assumptions
○ F. Analysis
○ G. Presentation

Figure B.18: Posttest page

Appendix C Exit Survey Results

At the conclusion of the posttest, each subject was given an opportunity to take the exit survey. The survey was designed to add context to the results of the study. Additionally, the intent of the exit survey was to pull from the subjects their opinions about the study and opinions about ways to improve the training. As mentioned above the exit survey consisted of 12 questions. The questions consisted of yes/no, ratings, multiple choice, and free form text. As with the main study, the exit survey was anonymous. There were 106 subjects that responded to the exit survey this was a 73.61% response rate (106/144). In this section the questions and results will be broken down.

Question 1 ask "Have you ever had any Cyber/Digital Forensics Training?" Of the 106 responses five (5) stated "Yes" and 101 stated "No."

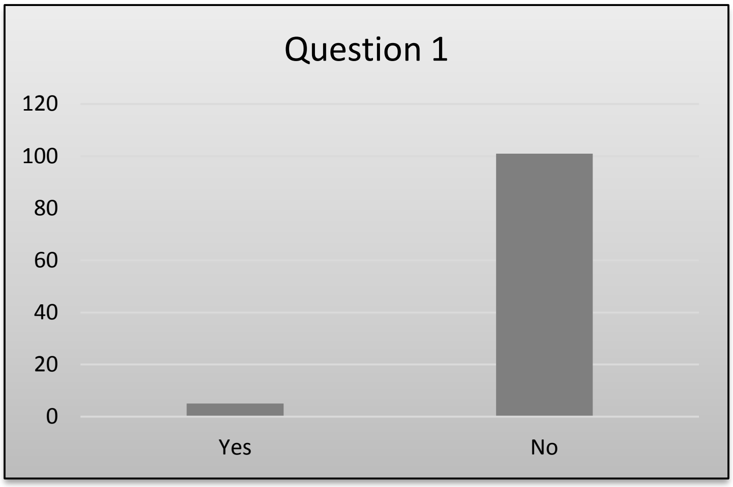


Figure C.1: Question 1 Bar Graph

Table C.1: Exit Survey Question 1 Results

#	Answer	Response	%
``	Yes	5	5%
2	No	101	95%
	Total	**106**	**100%**

Question 2 asked "Please rate the quality of the training material. 1 Poor - 10 High." There were 104 responses to this questions. The mean score was 4.82. This question was designed to rate training satisfaction.

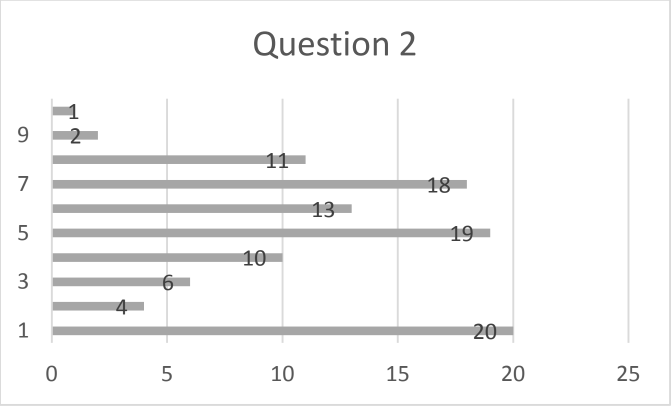


Figure C.2: Question 2 Bar Graph

Table C.2: Exit Survey Question 2 Results

#	Question	1	2	3	4	5	6	7	8	9	10	Total Responses	Mean
1	Rating	20	4	6	10	19	13	18	11	2	1	104	4.82

Statistic	Rating
Min Value	1
Max Value	10
Mean	4.82
Variance	6.09
Standard Deviation	2.47

Question 3 asked “Do you think this training will be beneficial for all officers in your agency?” There were 106 responses to this question. 58 responded “No” and 48 responded “Yes.”

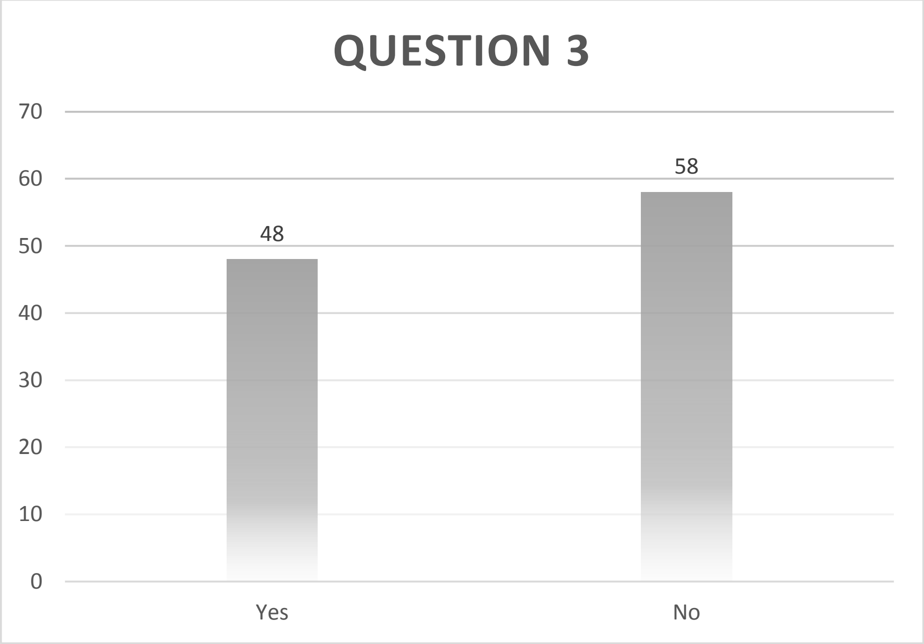


Figure C.3: Question 3 Bar Graph

Table C.3: Exit Survey Question 3 Results

#	Answer	Response	%
1	Yes	48	45%
2	No	58	55%
	Total	106	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.55
Variance	0.25
Standard Deviation	0.50
Total Responses	106

Question 4 asked “What would you change about this training?” There were 104 responses to this question. They subjects were giving six options to choose from. Choice

3, “How it was presented” had the highest response with 39. The least chosen was Choice 2, “Quality” with 4. Only 13% of the respondents choose content as something they would change. There were 20 respondents that selected the other.

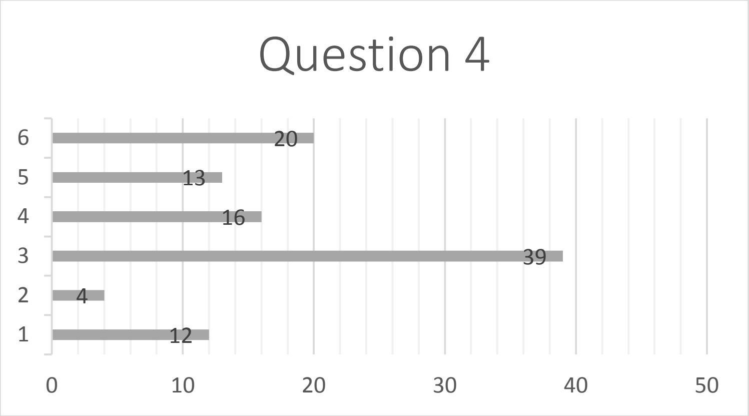


Figure C.4: Question 4 Bar Graph (Legend: 1 Length, 2 Quality, 3 How it was presented, 4 Content, 5 Nothing & 6 Other)

Table C.4: Question 3 Results

#	Answer	Response	%
1	Length	12	12%
2	Quality	4	4%
3	How it was presented	39	38%
4	Content	16	15%
5	Nothing	13	13%
6	Other	20	19%
	Total	104	100%

Statistic	Value
Min Value	1
Max Value	6
Mean	3.71
Variance	2.40
Standard Deviation	1.55

Table C.5 has the free text entries from the 20 respondents that selected “Other” in question 2.

Table C.5: Question 3 “Other” Free text entries

Test froze up on first attempt, retried several hours later
spelling issues and the way it was presented was hard to follow
Not trained
All the above with the exception of nothing
hands on
All of it
A little too technical for novices such as myself
testing after each segment to ensure understanding
All Of The Above
ALL
layman terms
I was group 1 there was no training
More detail
It assumes technical computer terms as common knowledge
Narrow the scope/too broad
Font size
I have no knowledge of this subject. Simply taking the tests have not provided any knowledge of the subject
powerpoint didn't work
N/A, Group 1
give the training to all groups, group 1 got none

Question 5 asked the subjects “Was this training beneficial for you?” This question was also designed for determining training satisfaction. There were 106 responses. There were 53 responses for “Yes (1)” and 53 responses for “No (2)”.

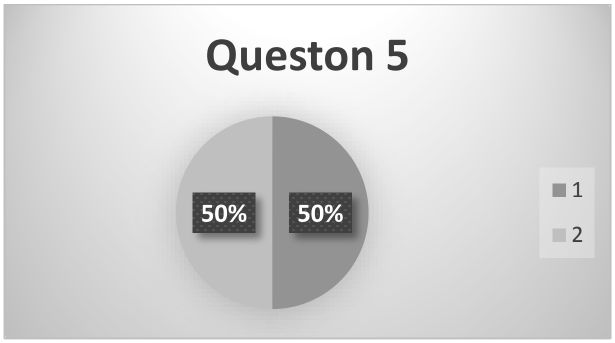


Figure C.5: Question 5 Pie Chart

Table C.6: Question 5 Exit Survey Results

#	Answer	Response	%
1	Yes	53	50%
2	No	53	50%
	Total	106	100%

Min Value	1
Max Value	2
Mean	1.50
Variance	0.25
Standard Deviation	0.50
Total Responses	106

Question 6 asked "How many years have you been in Law Enforcement?" There were 106 responses to this question. The top three selections were, 30 of the respondents that had 6-10 years of service, there were 20 respondents that had 1-5 years of service and 21 respondents had 16-20 years of service. The time of service least represented was group 7, 30+ years of service.

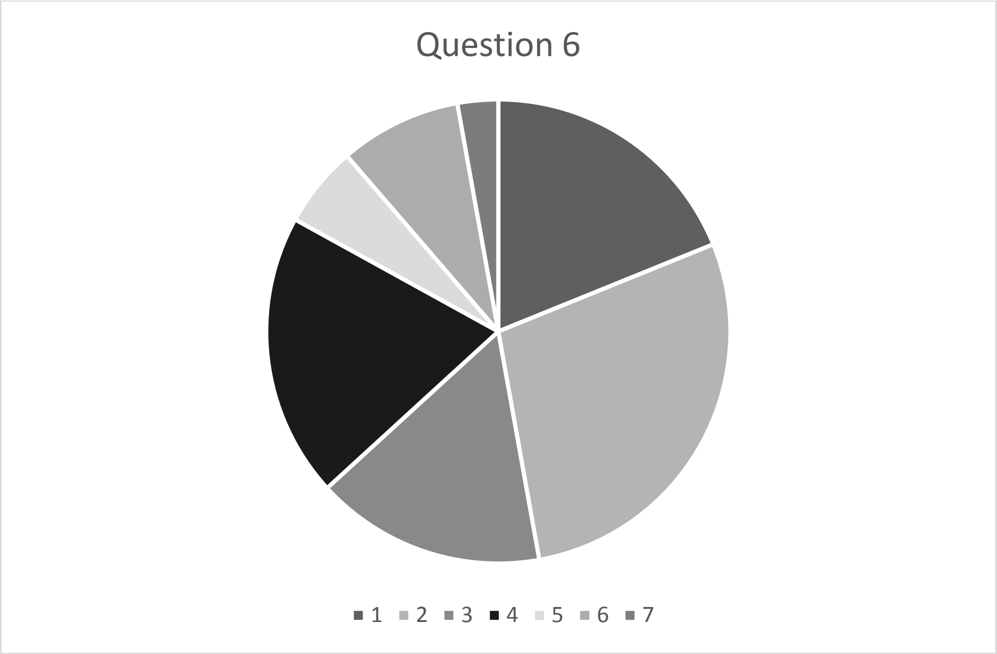


Figure C. 6: Question 6 Pie chart

Table C.7: Question 6 Exit Survey Results

#	Answer	Response	%
1	1-5	20	19%
2	6-10	30	28%
3	11-15	17	16%
4	16-20	21	20%
5	21-25	6	6%
6	26-30	9	8%
7	30+	3	3%
	Total	106	100%

Statistic	Value
Min Value	1
Max Value	7
Mean	3.02
Variance	2.70
Standard Deviation	1.64

Question 7 asked "Do you think that some level of cyber forensics knowledge is needed, as part of the basic performance for officers?" There were 105 responses to this question. 84 subjects answered "Yes" to this questions and 21 subjects answered "No."

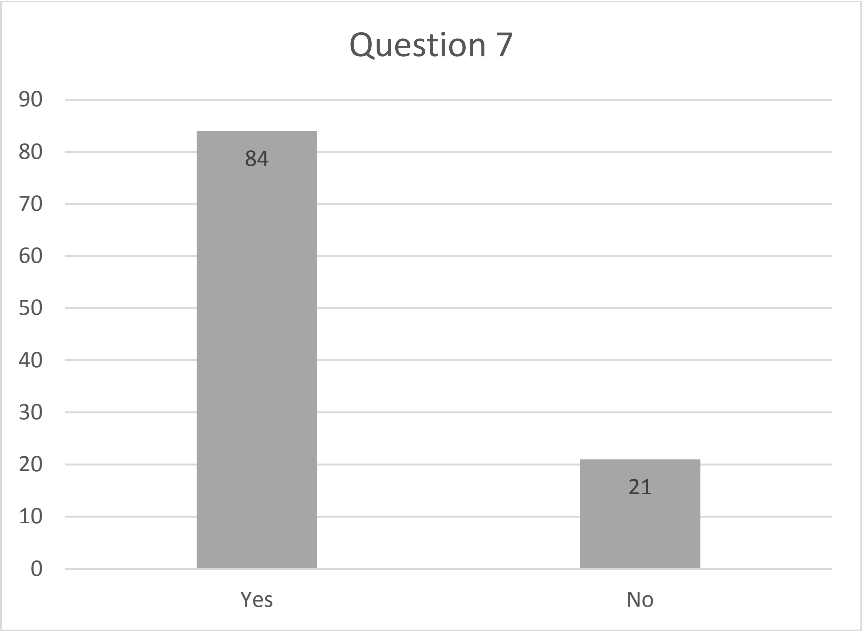


Figure C.7: Bar Graph for Question 5

Table C.8: Question 7 Exit Survey Results

#	Answer	Response	%
1	Yes	84	80%
2	No	21	20%
	Total	105	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.20
Variance	0.16
Standard Deviation	0.40

Question 8 asked the subjects “Would you attend other web based training if it was provided for free?” There were 106 respondents to this question, 77 subjects responded “Yes” and 29 responded “No”.

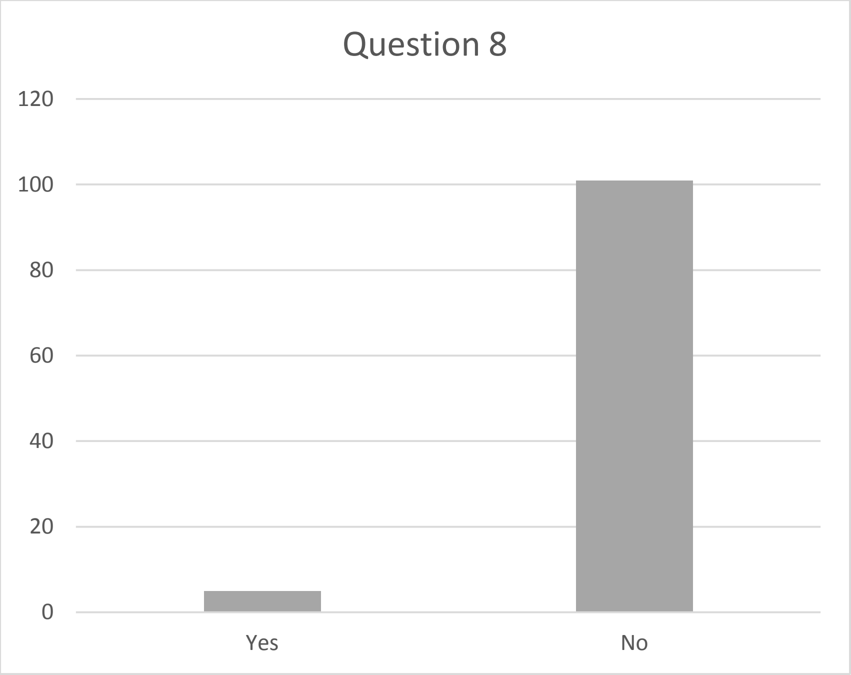


Figure C.8: Question 9 Bar Graph

Table C.9: Question 8 Exit Survey Results

#	Answer	Response	%
1	Yes	77	73%
2	No	29	27%
	Total	106	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.27
Variance	0.20
Standard Deviation	0.45
Total Responses	106

Question 9 asked “Have you attended any other web based training in the past?” There were 105 responses to this question, 71 subjects answered “Yes” and 34 subjects answered “No”.

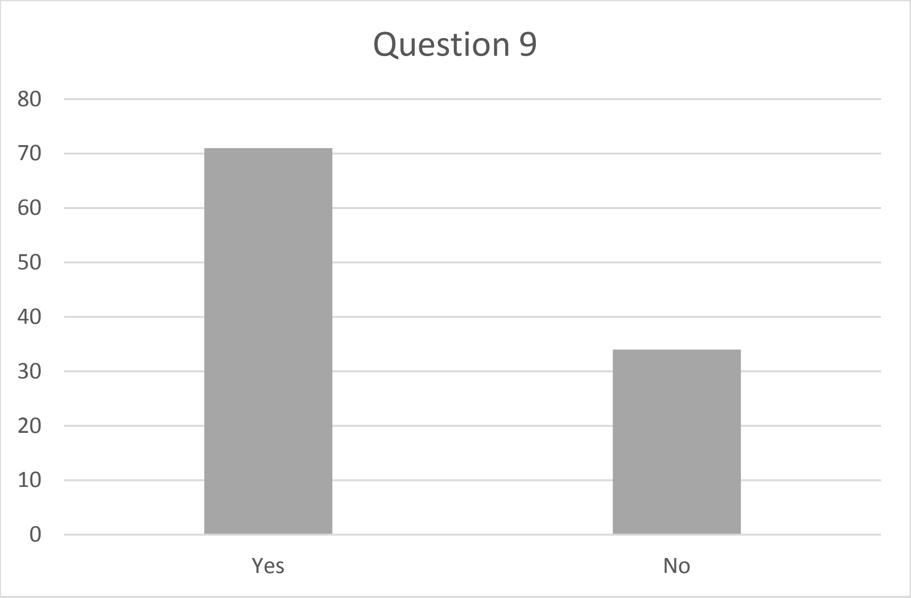


Figure C.9: Bar Graph for Question 9

Table C.10: Question 9 Exit Survey Results

#	Answer	Response	%
1	Yes	71	68%
2	No	34	32%
	Total	105	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.32
Variance	0.22
Standard Deviation	0.47
Total Responses	105

Question 10 asked “Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you during a criminal investigation?” This question was designed to determine training effectiveness. There were 105 responses to this question, 68 subjects responded “Yes” and 37 subjects responded “No.”

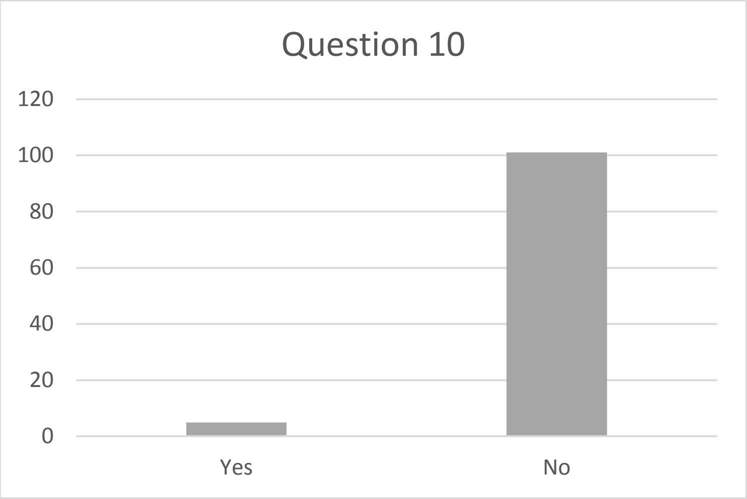


Figure C.10: Question 10 Bar Graph

Table C.11: Question 10 Exit Survey Results

#	Answer	Response	%
1	Yes	68	65%
2	No	37	35%
	Total	105	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.35
Variance	0.23
Standard Deviation	0.48
Total Responses	105

Question 11 asked “What specific knowledge, skills, abilities (KSAs) or techniques did you learn from this training?” This question was a free form text entry. There were 67 responses to this question. The question was designed to allow the subjects to reiterate specific things they learned from the training.

Table C.12: Question 11 Exit Survey Results

Question 11 Text Entries
digital forensics components
That there is a very particular process to handle evidence involved with technology crimes
The software available for investigations
A better general understanding of the process
how to package electronic devices and what to look for at a crime scene
Specific definitions as well as evidence processing involved with cyber forensics.
I was in group 1...no training
`None
Take photographs of the screen, store evidence in static proof bags.
None. There was nothing taught, only tests.
nothing

Table C.12 Continued

I learned a little more about the insides of a computer, what MAC was and the Dauber standard.
Documenting, storing, transporting
None. The training format was very poor.
Nothing
Gained some insight on what to do initially and what to look for
whoami command line prompt, Differences in Backup and Imaging of a device
USE SOCIAL MEDIA TO FIGHT CRIME.
How to secure and document the scene to gather digital evidence
that there are many types of computer crimes and ways to gain information from persons habits
Terminlolgy pertaining to this topic
None
N/A
Photograph computer screens when arriving on scene
What to look for in a cyber crime scene, where to look and how sensitive this all is.
No new knowledge was gained from this training
I learned not to just pull the plug without taking picture of the screen first
I was group 1. I only took the pretest, posttest, and exit survey.
good basics, but too technical for non-specialist
To not turn off systems, but can unplug exterior units from the computer
HOW MUCH EVIDENCE CAN BE RETRIEVED ON ALL DEVICES AND HOW MUCH CAN BE RETRIEVED ON HIDDEN FILES
None. As a Police Officer of 30 years, I lack computer technology skills.
What to initially do when confronted with a Forensic Case
That I woukd need help to properly secure digital equipment.
I took only the pre-test and the post-test.
New ways in which to track people.
how to secure a computer
To store evidence in a static free environment.
To take a pictue of the screen if the comuter is on.
Collection of evidence, differences in Windows,

Question 12 asked the subjects “Please add any additional comments or feedback about this study.” There were 51 responses to this question. The full list of responses can be found in the appendix. Table 4.20 list several of the responses given by the subjects. This question was designed to give the subjects an opportunity to give a subjective view of the study.

Table C.13: Question 12 Exit Survey Results

Question 12 Results
Good survey, I had to attempt to take the test two different times as it locked up.
Most patrol officers don't have the time to deal with these investigations. Most are forwarded to other investigators on the Department.
The slides seemed that they were designed to be presented with audio of some sort, I did not have any audio along with my slides.
I am a hands on learner. For me to fully understand Cyber Forensics I would need to be able to see and do. I do not believe having knowledge of Cyber Forensics will change day to day investigations for most Officers.
the test questions had spelling errors and were worded wrong.
None
I have no idea what half the stuff in the training is or means and 99% if not more of the material from this course will be forgotten by this afternoon.
For officers that have been in law enforcement longer, there needs to be a means available to ask questions more.
Would enjoy hands on acutal experience when looking for files and what exactly to use for search warrant docs
A physical instructor is necessary for teaching such foreign material.
I don't know any LEO that has 2-8 hours to complete a web based training. Worthless
Though the program was long, it was very detailed. However, I believe that a lot of Officers will not read through/listen to all of the presentation material due to the length. I feel that they will begin to just skip through the slides in order to get to the end. I have a very good understanding of computers prior to this training and found it to be a useful refresher. I feel, however, that most officers are not technologically inclined and will get bored quickly with the training and dismiss it as "yet another training that we are forced to do." I think it is good training for all Officer's due to the increase in computer related crimes, however, I feel that only a small percentage of Officer's will actually use any of the material or skills learned.

Table C.13 Continued

This training was too in depth for the average patrol officer. The average patrol officer only would benefit on how to document a scene and remove the evidence for further examination. Also on what evidence might be available on social media sites.
Even with thorough notes I found it hard to identify answers to some of the questions
I was in group 1, I was asked to take a pretest and a posttest. The only information I was supplied was the 6 slides that were in the instructions. Maybe I was just doing it wrong but I doesn’t see the point of taking a test without being supplied proper training/guidance.
NONE
This was very deep training for my level or ability
NA
Think this is way too much "tech" knowledge for the road officer. As far as road officer should only be trained on how to protect, preserve and document the evidence secured. Would be good course for our "IT" people.
This information if provided should be in a classroom setting with instructors available to explain and answer questions.
I was unfamiliar with alot of the terminology used in with computer parts and programs
I cannot give a fair exit survey because I did not take part in the actual training (group 1).
I was in group one so I didnt get to study anything. I was just asked to take the pretest and post test. My answers were based on my existing knowledge of cyber crimes.
Too technical of a process...should be limited to specialist to prevent destruction of evidence and court process
I feel that as no more knowledge that I have dealing with computers that a web based training faile to meet any positive training. I need to be able to ask questions and talk to someone. This may work for someone younger who has a least a working knowledge of computers to be helpful
Web based training for non computer interested or knowledged people is going to leave people completely lost
None.
N/A
Either more detail on securing physical evidence of electronics, or explanations of computer files.
N/A

Table C.13: Continued

This training did not make me any more comfortable to handle an investigation involving cyber materials.
most of it was over my head, mainly due to no interest.
I am not sure what the study really ment to accomplish. It only convienced or reinforced my belief that I could not and/or would not, attempt to secure any information from an electronic device. Too much information and too detailed in some instances. I will not remember much of what I read. I had to read some of the material several times and still did not understand some of what I read. I just know I will take pictures and request assistance.
This contained a lot of broad information that could be broken down into individual, more specific training that would still be useful for all law enforcement. Would not only apply to cyber crimes officers.
I would have liked more details and better explained definitions
I have been a "road troop" or a "street level cop" for almost 16yrs. I have never needed this information during my duties. I could see this class being beneficial for our investigations division but not for the average road troop. I scored 31/40 on the posttest.
I felt that much of the information provided was directed toward someone who would be analyzing the digital media rather than a "road officer".
Nothing more at this time.
This training is helpful for a trooper my age (53) who grew up in the late 70's and has little knowledge of computers, cell phones, tablets, etc.
maybe more practical exercises and examples
I would have a audio component to the powerpoint slides that reads the text on each slide that the individual can control for speed in order to both read and hear the content of the slide
I found the study very informative but it did not give me the training, knowledge, or confidence to feel that I would be able to look for the evidence without bringing in the Indiana State Police Cyber Crimes troopers who look at computers everyday. It did allow me to be more comfortable with what to look for at a scene and what articles should be secured for our specialized units to examine. The other problem I had was with the web based training. I was logged off multiple times and when I completed my post test 32/40 right it logged me off and then when i logged back on to get to this survey through the post test none of my answers were on it. I am not sure if they already submitted.
great training, i enjoy learning more in classroom environment
SOME ASPECTS WERE TOO TECHNICAL FOR WEB BASED TRAINING.

Table C.13: Continued

HAVING LIMITED COMPUTER KNOWLEDGE I FOUND THE CONTENT TO BE CONFUSING
some modules of the power point were constructed in a way that were easier to read and understand.
powerpoint didn't work
need audio and video for the presentation
For an average patrol officer the training should focus on recognition of crime scene. Future training should focus on how to identify digital crime scene and secure the scene. Most road officers will not be conducting the digital forensic evaluations, as this is a specialized job/position. The information contained in this training was great, but unfortunately not particularly useful for a road officer. The best sections were those on social media as crime scenes.
Some questions didn't apply as i was in group 1, didn't see the actual training
Group 1 took pretest and post-test with no education between. I saw absolutely no reason or purpose for this. I would have liked to have received some training in between.

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
Have you ever had any Cyber/Digital Forensics Training?	*Chi Square*	*106.00**	*4.36**	*2.55**	*1.13**	*1.89**	*10.12**	*0.00**	*1.98**	*2.51**	*0.53**
	Degrees of Freedom	*1*	*9*	*1*	*5*	*1*	*6*	*1*	*1*	*1*	*1*
	p-value	*0.00*	*0.89*	*0.11*	*0.95*	*0.17*	*0.12*	*1.00*	*0.16*	*0.11*	*0.46*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.1: Chi Square 1

		Have you ever had any Cyber/Digital Forensics Training?	Please rate the quality of the training material. 1 Poor - 10 High - Rating	Do you think this training will be beneficial for all officers in your agency?	What would you change about this training?	Was this training beneficial for you?	How many years have you been in Law Enforcement?	Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...	Would you attend other web based training if it was provided for free?	Have you attended any other web based training in the past?	Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...
Please rate the quality of the training material. 1 Poor - 10 High - Rating	Chi Square	4.36*	936.00*	30.38*	71.62*	49.74*	90.56*	8.43*	22.48*	5.91*	32.35*
	Degrees of Freedom	9	81	9	45	9	54	9	9	9	9
	p-value	0.89	0.00	0.00	0.01	0.00	0.00	0.49	0.01	0.75	0.00

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.2: Chi Square 2

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
Do you think this training will be beneficial for all officers in your agency?	*Chi Square*	*2.55**	*30.38**	*106.00*	*4.88**	*34.27*	*10.68**	*13.85*	*23.74*	*2.20*	*15.43*
	Degrees of Freedom	*1*	*9*	*1*	*5*	*1*	*6*	*1*	*1*	*1*	*1*
	p-value	*0.11*	*0.00*	*0.00*	*0.43*	*0.00*	*0.10*	*0.00*	*0.00*	*0.14*	*0.00*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.3: Chi Square 3

		Have you ever had any *Cyber/Digital Forensics Training?*	*Please rate the quality of the training material. 1* *Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics* *knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or* *techniques to aid you d...*
What would you change about this training?	*Chi Square*	*1.13**	*71.62**	*4.88**	*520.00**	*1.34**	*21.50**	*5.53**	*0.94**	*7.18**	*4.56**
	Degrees of Freedom	*5*	*45*	*5*	*25*	*5*	*30*	*5*	*5*	*5*	*5*
	p-value	*0.95*	*0.01*	*0.43*	*0.00*	*0.93*	*0.87*	*0.36*	*0.97*	*0.21*	*0.47*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.4: Chi Square 4

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
Was this training beneficial for you?	*Chi Square*	*1.89**	*49.74**	*34.27*	*1.34**	*106.00*	*13.95**	*4.61*	*17.14*	*6.61*	*44.49*
	Degrees of Freedom	*1*	*9*	*1*	*5*	*1*	*6*	*1*	*1*	*1*	*1*
	p-value	*0.17*	*0.00*	*0.00*	*0.93*	*0.00*	*0.03*	*0.03*	*0.00*	*0.01*	*0.00*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.5: Chi Square 5

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
How many years have you been in Law Enforcement?	*Chi Square*	*10.12**	*90.56**	*10.68**	*21.50**	*13.95**	*636.00**	*8.68**	*1.22**	*9.30**	*6.96**
	Degrees of Freedom	*6*	*54*	*6*	*30*	*6*	*36*	*6*	*6*	*6*	*6*
	p-value	*0.12*	*0.00*	*0.10*	*0.87*	*0.03*	*0.00*	*0.19*	*0.98*	*0.16*	*0.32*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.6: Chi Square 6

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...	*Chi Square*	*0.00**	*8.43**	*13.85*	*5.53**	*4.61*	*8.68**	*105.00**	*20.02*	*5.60*	*5.34*
	Degrees of Freedom	*1*	*9*	*1*	*5*	*1*	*6*	*1*	*1*	*1*	*1*
	p-value	*1.00*	*0.49*	*0.00*	*0.36*	*0.03*	*0.19*	*0.00*	*0.00*	*0.02*	*0.02*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.7: Chi Square 7

		Have you ever had any Cyber/Digital Forensics Training?	Please rate the quality of the training material. 1 Poor - 10 High - Rating	Do you think this training will be beneficial for all officers in your agency?	What would you change about this training?	Was this training beneficial for you?	How many years have you been in Law Enforcement?	Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...	Would you attend other web based training if it was provided for free?	Have you attended any other web based training in the past?	Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...
Would you attend other web based training if it was provided for free?	Chi Square	1.98*	22.48*	23.74	0.94*	17.14	1.22*	20.02	106.00	3.44	16.10
	Degrees of Freedom	1	9	1	5	1	6	1	1	1	1
	p-value	0.16	0.01	0.00	0.97	0.00	0.98	0.00	0.00	0.06	0.00

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.8: Chi Square 8

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
Have you attended any other web based training in the past?	*Chi Square*	*2.51**	*5.91**	*2.20*	*7.18**	*6.61*	*9.30**	*5.60*	*3.44*	*105.00*	*10.09*
	Degrees of Freedom	*1*	*9*	*1*	*5*	*1*	*6*	*1*	*1*	*1*	*1*
	p-value	*0.11*	*0.75*	*0.14*	*0.21*	*0.01*	*0.16*	*0.02*	*0.06*	*0.00*	*0.00*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.9: Chi Square 9

		Have you ever had any Cyber/Digital Forensics Training?	*Please rate the quality of the training material. 1 Poor - 10 High - Rating*	*Do you think this training will be beneficial for all officers in your agency?*	*What would you change about this training?*	*Was this training beneficial for you?*	*How many years have you been in Law Enforcement?*	*Do you think that some level of cyber forensics knowledge is needed, as part of the basic perform...*	*Would you attend other web based training if it was provided for free?*	*Have you attended any other web based training in the past?*	*Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...*
Did this training identify any new knowledge, skills, abilities (KSAs) or techniques to aid you d...	*Chi Square*	*0.53**	*32.35**	*15.43*	*4.56**	*44.49*	*6.96**	*5.34*	*16.10*	*10.09*	*105.00*
	Degrees of Freedom	*1*	*9*	*1*	*5*	*1*	*6*	*1*	*1*	*1*	*1*
	p-value	*0.46*	*0.00*	*0.00*	*0.47*	*0.00*	*0.32*	*0.02*	*0.00*	*0.00*	*0.00*

*Note: The Chi-Square approximation may be inaccurate - expected frequency less than 5.

Table C.1: Chi Square 10

Appendix D Pretest questions

Q1. 1. Digital forensic science can be described as:
A. The science of determining the cause of computer failures.
B. The use of scientifically derived and proven methods in furthering the reconstruction of events found to be criminal.
C. The use of empirical research to benefit the software vendors in developing more secure applications.
D. The art of testifying before a judge and jury in relation to network security issues.

Q2. The United States follows which type of Legal System?
A. Religious
B. Common Law
C. Customary
D. Mixed

Q3. Which of the following is not part of the DFS process?
A. Identification
B. Preservation
C. Collection
D. Examination
E. Assumptions
F. Analysis
G. Presentation
H. Decision

Q4. Which of the following groups represent the leading cost of computer crime losses
A. Employees
B. Hackers
C. Industrial Saboteurs
D. Foreign Agents

Q5. True or False: You should ask the suspect for all of usernames, passwords, and pin codes they use to access their accounts?
True
False

Q6. If a computer is powered what is the first thing you are to do?
A. Pull the plug from the wall
B. Turn it off
C. Take pictures of the screen
D. None of the Above

Q7. What does MAC sand for?
A. Macintosh
B. Minutes Acceleration
C. Modified, Accessed, Created
D. Multiple, Attribute, Configuration

Q8. Challenges in Digital Forensics?
A. Multitude of OS platforms and file systems
B. Incredibly large storage capacity
C. No International agreements on extraditions
D. Networked environments
E. All of the Above

Q9. Which part is an essential part of a computer?
A. Hard disk
B. Motherboard
C. Central Processing Unit (CPU)
D. Random Access Memory (RAM)
E. All of the Above

Q10. . What type of Bag is used for transporting Computer Storage Mediums?
A. Waterproof bags
B. Anti-Static bags
C. Conductive bags
D. Secure labeled bags

Q11. Why is it so important to document pin settings and the order in which the cables are connected to the hard drives?
A. A job well done.
B. The only way to put it back
C. It shows what goes where
D. It helps identifying the boot sequence

Q12. The chain of custody of evidence describes who obtained the evidence and _______________:
A. Who secured it and controlled it
B. Who controlled it and transcribed it
C. Who secured it and validated it
D. Who controlled it and duplicated it

Q13. Why is it challenging to collect and identify digital evidence to be used in a court of law?
A. The evidence is mostly intangible
B. The evidence is mostly corrupted
C. The evidence is encrypted
D. The evidence is mostly tangible

Q14. "False Positive" is a
A. A trace in a log file that is misinterpreted as a normal system event.
B. A trace in a log file that lists its destination port as above 1024
C. A trace in a log file that lists its destination port as below 1024
D. A trace in a log file that is misinterpreted as an abnormal system event.

Q15. In order to verify the integrity of the images created the following process should be used:
A. Run MD5SUM on both the source media and the copies and compare the hash totals
B. Encrypt both the source and the copies to prevent tampering
C. Store the copies on write once media.
D. Initial and date the source and all copies.

Q16. What are the 3 A's in digital forensics? -
A. Authentication, Authorization, Accounting
B. Acquire, Authenticate, Analyze
C. Attitude, Awareness, Authenticity
D. American Automobile Association

Q17. According to Palmer (2002) evidence and methodologies/techniques used to uncover it needs to be:
A. Accepted in industry and in law enforcement
B. Accurate and Repeatable
Appendix A Accurate, Reliable, Accepted in the field as a standard
D. None of the Above

Q18. There are no US Federal laws dealing with computer specific criminal offences.
True
False

Q19. There is not a "gold standard" professional designation for computer forensics professionals?
True
False

Q20. When you delete a file, the file is automatically removed from your system and the data area is immediately overwritten
True
False

Appendix E Posttest Questions

Q1. What does DFS Stand for?
A. Department of Forensic Science
B. Forensic Digital Science
C. Digital Forensic Science
D. Defensive Forensics Science

Q2. The United States follows which type of Legal System??
A. Religious
B. Common Law
C. Customary
D. Mixed

Q3. Which of the following is not part of the DFS process?
A. Identification
B. Preservation
C. Collection
D. Examination
E. Assumptions
F. Analysis
G. Presentation
H. Decision

Q4. What are the 3 A's in digital forensics?
A. authentication, authorization, accounting
B. Attitude, Awareness, Authenticity
C. Acquire, Authenticate, Analyze
D. American Automobile Association

Q5. What is Cyber or Digital Forensics?
A. Analyzing digital evidence and presenting it in a court of Law.
B. The scientific examination and analysis of digital evidence in such a way that the information can be used as evidence in a court of law
C. Scientific Examination of the Hard drive and mobile phones and presenting it in a court of Law
D. All of the Above

Q6. Challenges in Digital Forensics?
A. Multitude of OS platforms and file systems
B. Incredibly large storage capacity
C. No International agreements on extraditions
D. Networked environments
E. All of the Above
Q7. Which part is an essential part of a computer?
A. Hard disk

B. Motherboard
C. Central Processing Unit (CPU)
D. Random Access Memory (RAM)
E. All of the Above

Q8. What type of Bag is used for transporting Computer Storage Mediums?
A. Waterproof bags
B. Anti-Static bags
C. Conductive bags
D. Secure labeled bags

Q9. Why is it so important to document pin settings and the order in which the cables are connected to the hard drives?
A. A job well done.
B. The only way to put it back
C. It shows what goes where
D. It helps identifying the boot sequence

Q10. “False Positive" is a
A. A trace in a log file that is misinterpreted as a normal system event.
B. A trace in a log file that lists its destination port as above 1024
C. A trace in a log file that lists its destination port as below 1024
D. A trace in a log file that is misinterpreted as an abnormal system event.

Q11. What is the difference between a backup or a copy & forensic Imaging?
A. Forensic imaging is a bit by bit copy of the original device.
B. Backup and simple copying only copies information and files identified by the system as available.
C. Forensic copy includes slack space data and deleted files
D. All the Above is correct
E. There is no difference

Q11. How many copies of our digital forensic image should we have?
A. One working copy
B. Two, working copy and one in the evidence room
C. Three, a working copy, backup, and in the evidence
D. Four, Working copy, Backup, Evidence room, External USB storage

Q12. The chain of custody of evidence describes who obtained the evidence and _______________:
A. Who secured it and controlled it
B. Who controlled it and transcribed it
C. Who secured it and validated it
D. Who controlled it and duplicated it

Q13. Why is it challenging to collect and identify digital evidence to be used in a court of law?
A. The evidence is mostly intangible
B. The evidence is mostly corrupted
C. The evidence is encrypted
D. The evidence is mostly tangible

Q14. In order to verify the integrity of the images created the following process should be used:
A. Run MD5SUM on both the source media and the copies and compare the hash totals
B. Encrypt both the source and the copies to prevent tampering
C. Store the copies on write once media.
D. Initial and date the source and all copies.

Q15. What does FTK stands for?
A. Forensic Triage kit
B. Forensic ToolKit
C. Flotek Industries, Inc.
D. Forensic Technology Kit)

Q16. What files can be found in both a logical and a physical copy?
A. Deleted files
B. Slack space
C. Hidden files
D. Fragmented files

Q17. Which of the following groups represent the leading cost of computer crime losses
A. Employees
B. Hackers
C. Industrial Saboteurs
D. Foreign Agents

Q18. What are the boundaries to look for on a computer?
A. How many people use the computer?
B. How often is the computer used?
C. How Many user accounts are there?
D. Which account is connected to the evidence?
E. Answers A, C, & D
F. Who registered the computer?

Q19. Which applies to a user’s profile?
A. Desktop
B. My Documents
C. Temporary Internet Files
D. All of the above

Q20. Evidence found in a user’s home directory is a strong indicator of what?
A. Framed
B. Culpability
C. Malware
D. Fraud

Q21. What caveats should you check upon finding evidence?
A. Check permissions
B. Who else has the account password?
C. Who created the file?
D. B and C
E. A and B
F. None of the above

Q22. Where are Windows 7 user profiles located by default?
A. C:\Documents and Settings\
B. C:\Profiles\
C. C:\Users\
D. None of the above

Q23. When you delete a file, the file is automatically removed from your system and the data area is immediately overwritten
True
False

Q24. What is the major difference in the MyDocuments folder from XP to Win7?
A. There is no difference, it stays the same.
B. The MyDocuments folder is no longer the default container for all files and media and now has separate folders for Documents, Downloads, Music, and Videos.
C. The MyDocuments folder is no longer in the user’s home directory and is located on root specific to the user’s SID.
D. The MyDocuments folder is no longer the default container for all files and media which now default to the desktop.

Q25. According to Palmer (2002) evidence and methodologies/techniques used to uncover it needs to be:
A. Accepted in industry and in law enforcement
B. Accurate and Repeatable
C. Accurate, Reliable, Accepted in the field as a standard
D. None of the Above

Q26. What does MAC sand for?
A. Macintosh
B. Minutes Acceleration
C. Modified, Accessed, Created
D. Multiple, Attribute, Configuration

Q27. When constructing a timeline of events which should you NOT do?
A. Work backwards
B. Adjust time and date to examiners time zone
C. Identify most current users and actions
D. Confirm the date
E. Look for sequences and patterns with files MAC

Q28. Which type of email is stored locally?
A. Cloud-based
B. Web-based
C. Action-based
D. Client-based

Q29. There are no US Federal laws dealing with computer specific criminal offences.
True
False

Q30. What is NOT a helpful web artifact found on a computer?
A. .pst files
B. Index.dat
C. .xlsx
D. .ini files
E. History.dat

Q31. Digital artifacts associate with which three of the following: a) email, b) IM, c) browses, d) MFT, e) recycler, f) most recently opened
A. C, D, F
B. A, B, C
C. B, A, E
D. F, B, C
E. C, A, F

Q32. Which devices can store digital evidence?
A. Desktop Computers
B. Smart Phones
C. Hard Drives
D. Wireless Routers
E. All of the above

Q33. If a computer is powered what is the first thing you are to do?
A. Pull the plug from the wall
B. Turn it Off
C. Take pictures of the screen
D. None of the Above

Q34. True or False: The Principle of Exchange states, when a person commits a crime something is always at the scene that was not present when the person arrived!
True
False

Q35. There is not a "gold standard" professional designation for computer forensics professionals?
True
False

Q36. What are the steps in the scene evidence collection process?
A. Plan the seizure, secure the scene, and document the scene.
B. Plan the seizure, document the scene, and secure the scene, interviewing, and transportation
C. Interview the witness and transportation of the evidence.
D. None of the above)

Q37. True or False: In Computer Forensics there is only physical evidence.
True
False

Q38. Which of the following statements is true about digital evidence?
A. Is never electronic
B. Can always be de-contaminated
C. It is extremely volatile
D. Never follows chain of custody rules

Q39. True or False: Social networks such as Facebook and Twitter can contain evidence to a crime?
True
False

Q40. True or False: You should ask the suspect for all of usernames, passwords, and pin codes they use to access their accounts?
True
False

Appendix F Recruitment Letter

All,

You have been randomly selected to participate in a study being conducted by Purdue's Cyber Forensics Laboratory. This study is seeking to determine if web based cyber forensics training is an effective medium to train a large group of law enforcement officers. The training is designed for officers who are assigned to road duties. With technology becoming more and more important in today's society and with the misuse of that technology it is crucial for law enforcement to keep up. The long term goal of this study is to increase the overall knowledge, skills and abilities of every law enforcement officer. You have been assigned to group (#).

Instructions:

1. Go to http://web.ics.purdue.edu/~nsturgeo/study_reg.php
2. A random log in id will be generated. Copy and paste the ID in to the username field, type in a password, confirm the password and type in the group number you were assigned to.
3. Please read the Informed Consent and Waiver at the bottom of the page. This training is completely voluntary and anonymous, no personal information will be kept.
4. If you agree to the Informed Consent and Waiver click the submit button.
5. To log in you will need to go to http://web.ics.purdue.edu/~nsturgeo/studylogon.php
6. If you are in Group 1 you will only be asked to take the pretest, posttest and exit survey. If you are in Groups 2 and 3 will be asked to go through a series of power point training slides. It should take a minimum of 2 hours but may take up to 8 hours to complete the training.
7. After the posttest please take the exit survey. This is for you to rate the training and give feedback about the overall course.

If you have any questions or technical issues please send an email and include your randomly generated username.

Respectfully,

ISP Training Section

Appendix G Cyber Forensics Training Matrix

Training Area: Application, Laws and Regulation Functional Specialty: Road/Beat Officer

Definition: This training has been designed specifically for the road/beat officer.

Behavioral outcome: At the conclusion of this training officer will be able to understand the types of potential evidence that can be ascertained from various electronic devices. Will be able to describe proper procedures, documentation, and collection of digital evidence.

Knowledge Levels: 1. Beginner 2. Intermediate

Learning Objectives:

- Explain the context of computer forensics
- Describe some of the specific and general challenges faced by digital forensics
- Define the term computer forensics
- Discuss the 3 A's of computer forensics
- Identify and explain how to disassemble the components of a basic computer system
- Discuss how to properly document the computer hardware setup and hard drive(s) of a computer system
- Discuss what information can be obtained from the computer BIOS
- Discuss similarities between physical and digital crime scenes
- Explain the importance of proper evidence seizure
- Recognize and Identify possible digital evidence items
- Describe proper procedures, documentation, and collection of digital evidence at the scene
- Explain what other information can be possibly be obtained at the scene
- Define Cyber Forensics Triage
- Discuss the objectives of the CFT process
- Explain the various factors that must be considered before using CFT
- Compare and contrast live vs. static analysis at a high level
- Identify possible types of evidence on MySpace, Facebook, Twitter, Google+ accounts
- Describe the LE process for contacting MySpace, Facebook, Twitter, and Google
- Describe how to use a website ripper

Job Functions:

- Road/Beat Officer

Appendix H: IRB Approval

To:	MARCUS ROGERS KNOY225
From:	JEANNIE DICLEMENTI, Chair Social Science IRB
Date:	08/25/2015
Committee Action:	Approval
IRB Action Date	08/25/2015
IRB Protocol#	1506016173
Study Title	Web Based Cyber Forensics Training for Law Enforcement
Expiration Date	08/24/2016

Following review by the Institutional Review Board (IRB), the above-referenced protocol has been approved. This approval permits you to recruit subjects up to the number indicated on the application form and to conduct the research as it is approved. The IRB-stamped and dated consent, assent, and/or information form(s) approved for this protocol are enclosed. Please make copies from these document(s) both for subjects to sign should they choose to enroll in your study and for subjects to keep for their records. Information forms should not be signed. Researchers should keep all consent/assent forms for a period no less than three (3) years following closure of the protocol.

Revisions/Amendments: If you wish to change any aspect of this study, please submit the requested changes to the IRB using the appropriate form. IRB approval must be obtained before implementing any changes unless the change is to remove an immediate hazard to subjects in which case the IRB should be immediately informed following the change.

Continuing Review: It is the Principal Investigator's responsibility to obtain continuing review and approval for this protocol prior to the expiration date noted above. Please allow sufficient lime for continued review and approval. No research activity of any sort may continue beyond the expiration date. Failure to receive approval for continuation before the expiration date will result in the approval's expiration on the expiration date. Data collected following the expiration date is unapproved research and cannot be used for research purposes including reporting or publishing as research data.

Unanticipated Problems/Adverse Events: Researchers must report unanticipated problems and/or adverse events to the IRB. If the problem/adverse event is serious, or is expected but occurs with unexpected severity or frequency, or the problem/even is unanticipated, it must be reported to the IRB within 48 hours of learning of the event and a written report submitted within five (5) business days. All other problems/events should be reported at the lime of Continuing Review.

We wish you good luck with your work. Please retain copy of this letter for your records.

Ernest C. Young Hall, 10th Floor · 155 S. Grant St. · West Lafayette, IN 47907-2114 · (765) 494-5942 · Fax. (765) 494-9911

For IRB Use Only

APPROVED

AUG 25 2015

EXPIRES 8.24.2016

PURDUE UNIVERSITY
INSTITUTIONAL REVIEW BOARD

RESEARCH PARTICIPANT CONSENT FORM

Web Based Cyber Forensics Training for Law Enforcement Dr. Marcus K. Rogers
Computer and Information Technology
Purdue University

What is the purpose of this study?

The purpose of this research is to determine if web based cyber forensics training is an effective medium to train a large group of Law Enforcement Officers compared to a traditional class room

What will I do if I choose to be in this study?

The anonymous, online training will be administered using a secure website. Once you have read this consent form, and agree to voluntarily participate, you will be taken to the secure website to complete the online training. You may withdraw from the study at any time or any reason.

How long will I be in the study?

You should expect to spend a minimum of 2 hours but it may take as much as 8 hours to complete the training. We understand that this is a lengthy time commitment. This training does not have to be completed in a single session. It is self-paced and you can return to the place where you left off.

What are the possible risks or discomforts?

The risks to you are minimal. They are not greater than those ordinarily encountered in daily life. Please know that this is an anonymous study that uses a secure link. The study is anonymous because we will not be able to link your responses back to youwe do not ask for any identifiable information (Ex. name). While completing the training the only risk to you might be if someone were to see your pretest and post test scores. In addition, some of the questions may contain law enforcement sensitive material. We recommend you take this training in an area way from public view Even then, your responses to the study could never be linked back to you. We appreciate your participation in this scientific research.

Are there any potential benefits?

This training is designed to improve your knowledge, skills, and abilities in cyber forensics. There are direct benefits to you. The information you learn from this training can be used in your day to day assigned duties. However, this training will not make you a certified cyber forensics examiner or expert. This is to give you another tool for your tool box.

Will information about me and my participation be kept confidential?

We do not ask or any other information that could be used to identify you at any time, before, during, or after tq'¢"survey. No IP addresses will be recorded. There will be no way to determine where the training was t ken or by whom. Instead, the training software will assign a random alphanumeric ID to youupon clicking the submit button. This means that the responses to the pre and posttest cannot be linked or matched to you, which means your responses will remain completely anonymous.' Only researchers associated with this study will have access to the data. In addition to the data being anonymous, will be stored electronically in an encrypted format. The encrypted data will be kept indefinitely and will be used only for research purposes. The project's research records may be reviewed by departments at Purdue University responsible for regulatory and research oversight.

What are my rights if I take part in this study?

Your participation in this survey is completely voluntary and you may withdraw from the survey at any time or skip any questions that you feel uncomfortable answering.

Who can I contact if l have questions about the study?

If you have any questions about this survey either before or after completion, you may contact Dr. Marcus Rogers, rogersrnk@purdue.edu. If you have questions about your rights as a person taking part in a research study, or if you would like to make suggestions or file complaints and concerns, you may call 765-494-5942. For technical assistance please contact your training section, give them your assigned user ID and they will make contact with technical support.

If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write *to:*
Human Research Protection Program - Purdue University
Ernest C. Young Hall, Room 1032
155 S. Grant St.
West Lafayette, IN 47907-2114

If you are 18 years of age or older, you freely agree to participate in this study, have had the opportunity to read this consent form, had the research study explained, had the opportunity to ask questions about the project and have them answered, then please click on the "I Agree" button below. Otherwise, do not proceed any further.

Appendix I Statistical Graphs

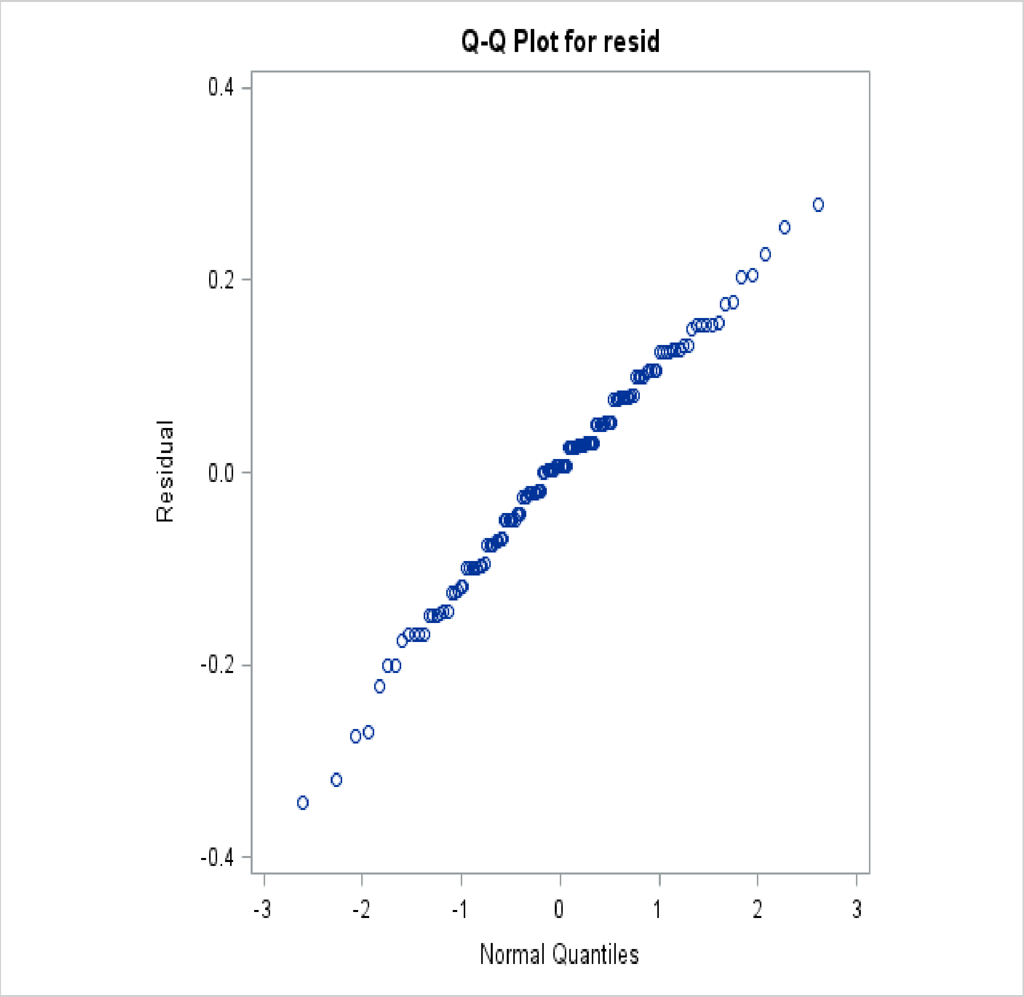
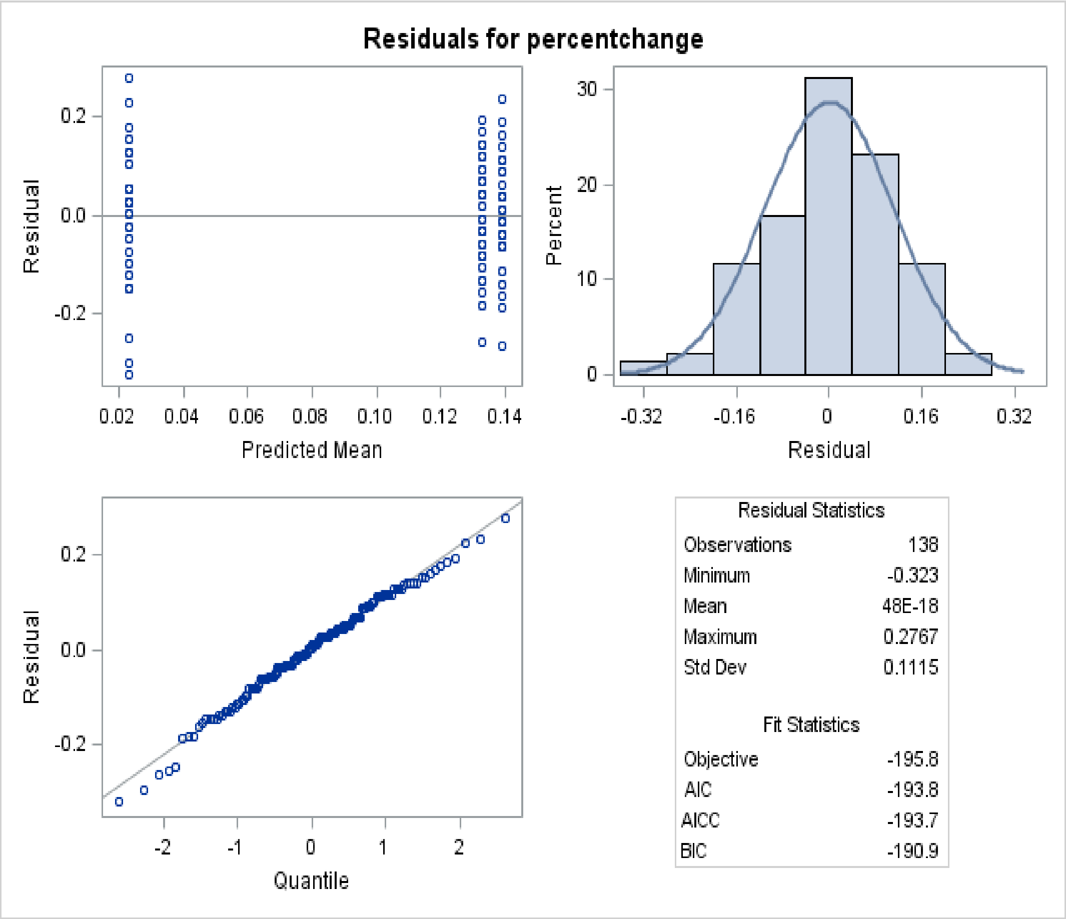


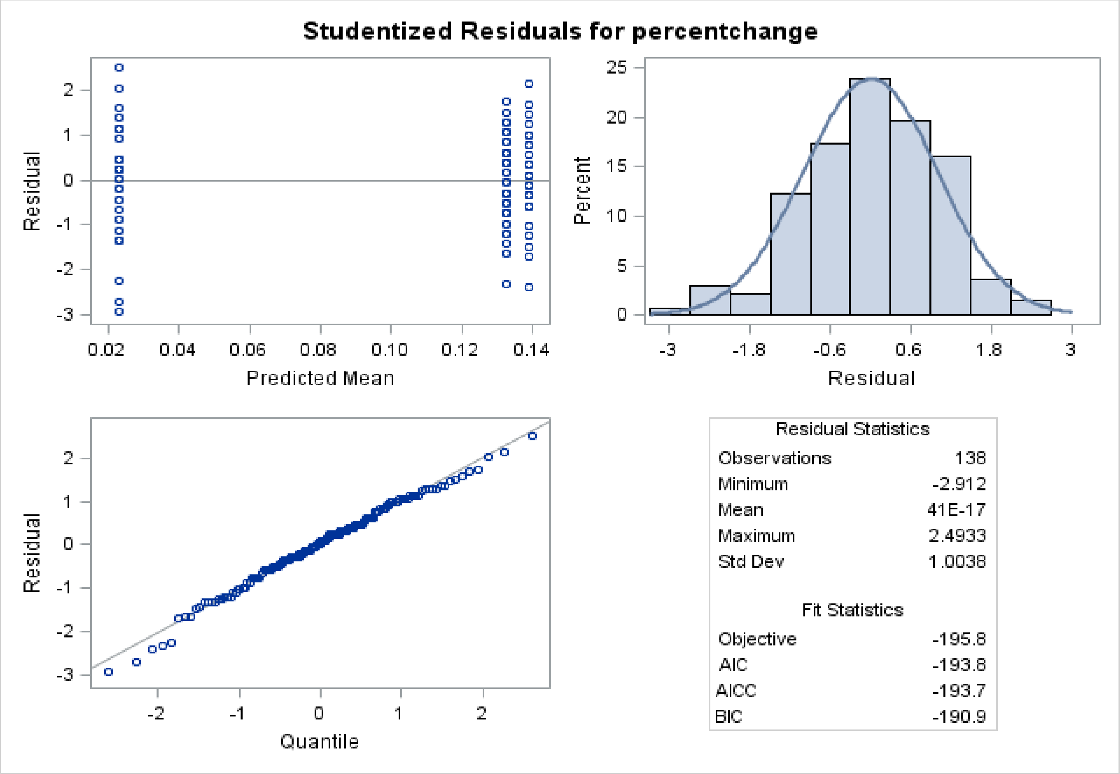
Figure J.1: QQPlot Percentchanged Residual



Residual Statistics	
Observations	138
Minimum	-0.323
Mean	48E-18
Maximum	0.2767
Std Dev	0.1115

Fit Statistics	
Objective	-195.8
AIC	-193.8
AICC	-193.7
BIC	-190.9

Figure J.2: Residual Graphic

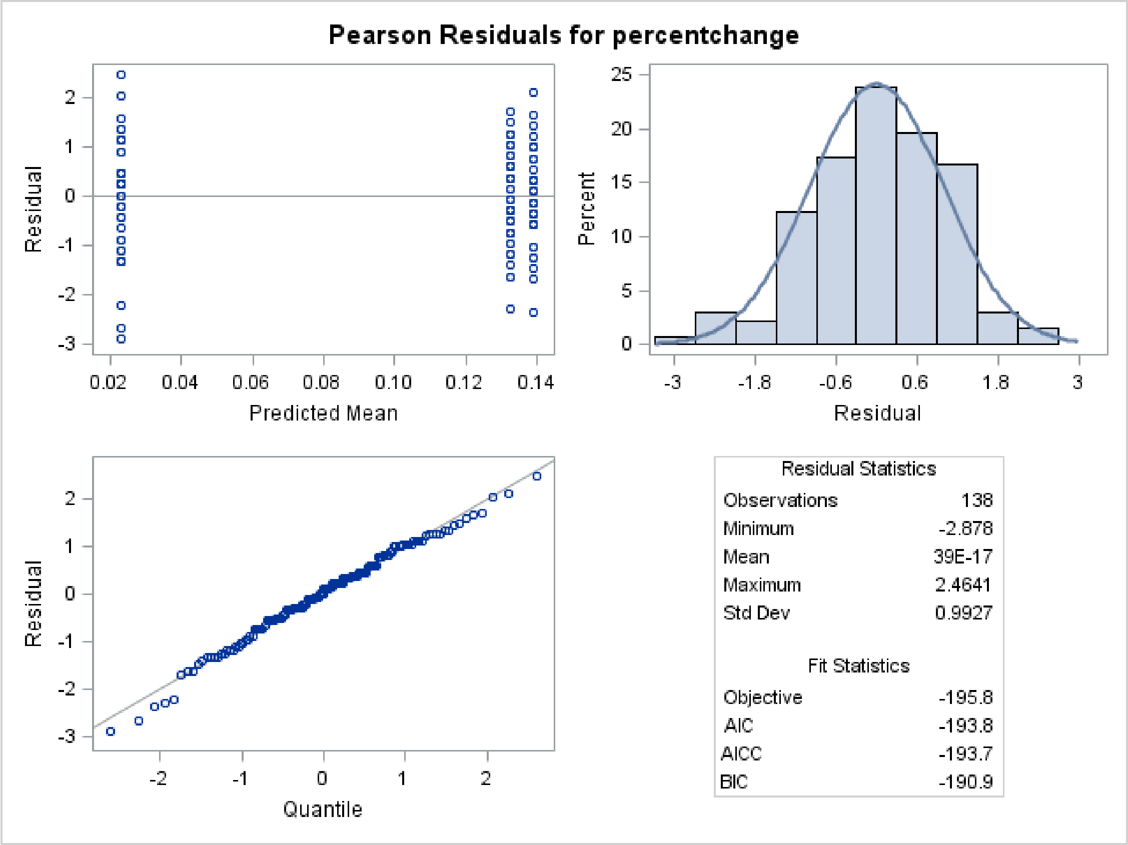


Studentized Residuals for percentchange

Residual Statistics	
Observations	138
Minimum	-2.912
Mean	41E-17
Maximum	2.4933
Std Dev	1.0038

Fit Statistics	
Objective	-195.8
AIC	-193.8
AICC	-193.7
BIC	-190.9

Figure J.3: Studentized Residuals for Percent Change



Pearson Residuals for percentchange

Residual Statistics	
Observations	138
Minimum	-2.878
Mean	39E-17
Maximum	2.4641
Std Dev	0.9927

Fit Statistics	
Objective	-195.8
AIC	-193.8
AICC	-193.7
BIC	-190.9

Figure J.4: Pearson Residuals for precentage