2021-06-14

Certifying Computer Forensics Skills

Michael Charles Watson
Brigham Young University

Certifying Computer Forensics Skills

Michael Charles Watson

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Justin S. Giboney, Chair
Amanda L. Hughes
Derek L. Hansen

School of Technology

Brigham Young University

ABSTRACT

Certifying Computer Forensics Skills

Michael Charles Watson
School of Technology, BYU
Master of Science

Computer forensics is an ever-growing technological field of complexity and depth. Individuals must strive to keep learning and growing their skills as they help combat cybercrime throughout the world. This study attempts to establish a method of evaluating conceptual expertise in computer forensics to help indicate whether or not an individual understands the five basic phases of computer forensics: preparation, seizure of evidence, acquisition of data, analysis of data, and reporting the findings of the analysis.

A survey was presented to a university class of 30 students taking a computer forensics course and as well as posted online asking computer forensics professionals to participate in the survey. Results show that novices that were enrolled in a computer forensics course were able to identify the phases of computer forensics more readily than professionals.

Keywords: digital forensics, computer forensics, conceptual expertise

ACKNOWLEDGEMENTS

I want to thank my wife, Janesa, for pushing me to be my best and encouraging me through the ups and downs; you have been a light in the darkness. Thank you to Dave, my twin, for the time you took from your busy schedule of classes and new family to look over my paper and give me some ideas. To my mom, thank you for helping me help iron out many grammatical and other writing mishaps that occurred along the way.

Also, a huge thank you to Justin Giboney for your tireless efforts to help and guide me in this effort. I've learned so much from this study and have been able to add many more tools to my cybersecurity toolbelt.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Who Are Computer Forensics Analysts?

Computer forensics analysts combine their technical skills with their forensic aptitude to recover information from computers and storage devices. They often assist law enforcement officers with cybercrimes in the retrieval process of digital evidence and to present findings in court. Computer forensics analysts also work with organizations when dealing with corporate espionage, misuse of corporate information, potential loss of data, and other potential hacking incidents (Marcella, J. & Greenfield, 2002).

Computer forensics analysts require developed problem-solving skills, knowledge of operating systems, data storage, network communications, and knowledge of cybersecurity principles. They often possess the aptitude and awareness of how hackers operate in order to assist them in finding hacking activity, entry and exit points on the network, and other methods and tools hackers may use in stealing data or denying service. In addition, they need to know how to legally seize computers and storage devices in order to acquire data from these devices that may be helpful in a case. Analysts then search for digital evidence on these devices while utilizing different pieces of software to create a story. During this process, they have to demonstrate that they were able to acquire the data in a repeatable fashion that would hold up in a legal court. (Marcella, J. & Greenfield, 2002).

1.2 The Phases of Computer Forensics

The stages or phases of computer forensics is vital for a professional to know and understand. If a professional does not follow a strict methodology, they can invalidate all the work they have completed. The computer forensics stages in this thesis are grouped into five separate phases: preparation, seizure of evidence, acquisition of data, analysis of data and reporting the findings of analysis.

The preparation stage features all the tasks and activities that are performed before an investigation or case is accepted by a Computer forensics professional. This is to ensure that the professional has the equipment, skills, environment and whatever else they may need in the course of their work. Examples of this would be preparing a laboratory for an upcoming client or to learn different skills that would be useful while performing any process a computer forensics professional would find themselves required to do.

The seizure stage is obtaining the physical or digital evidence. Computer forensics professionals are often required to obtain evidence in such a way that would be admissible in court to show that it had not been tampered with. The main objective here is to show that the evidence of each case has not been altered or damaged in any way throughout the process and to prepare it for the data acquisition stage. Examples of this would be physically taking evidence into their possession or filling out a chain of custody form.

The acquisition stage is collecting evidence off the devices that were collected. When acquiring the data, a computer forensics professional is now getting the data they obtained and getting it ready to be analyzed. This could be jailbreaking a device or using a script to image (or duplicate) a web server. Often the acquisition stage is getting data off the original devices onto devices that the data can be analyzed on. One step in this stage is to run the original data through

an encryption algorithm to produce a unique hash, or a value that is produced using a one-way mathematical function. Then, when the data is collected onto a different drive, the professional will run that device through the same algorithm to produce the same hash to show that the new device they are using for their analysis is identical.

The analysis stage is where most of a professional's technical skills, knowledge and abilities will be used. As can be inferred from the title of the stage, a professional will now analyze the data that has been seized and acquired. They will look for evidence of the crime that a criminal is being charged with. One thing a professional will perform in this stage is file carving, which is searching through a file system for a specific type of file or search term. They will look for evidence of obfuscation such steganography or for discrepancies throughout the whole file system..

The reporting stage is putting together all the steps the professional has performed up to this point, provide professional opinion on what the evidence may or may not suggest and prepare a digital and physical copy for the Court (or organization) to use in determining guilt. Professionals often give testimony in a court case and explain their findings so that a judge or jury may understand the technical nuances and meanings of what is being presented.

1.3 The Study

Assessing an individual's computer forensics skills and understanding of the field is vital to organizations. Recent advancements in measurements of conceptual expertise utilized in computer security (Giboney et al. 2016) will be used to measure computer forensics skills. They showed that professionals can recognize fundamental principles more easily than novices and utilized a technique to quickly measure the difference between novices and experts. Following

their guidelines, we propose to do the same for computer forensics expertise with the following research question: Can it be determined if a professional has more conceptual expertise than students by grouping like scenarios into the phase of computer forensics the scenario is performed in?

To answer this question, we will use different tasks cited from the National Institute of Standards and Technology (NIST) publication 800-181, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* (Newhouse et al., 2016). This framework provides an interdisciplinary reference structure for different tasks, aspects of cybersecurity knowledge, skills, and abilities (TKSAs) that can be applied to computer forensics. Using the TKSAs we will follow scale established development procedures to develop a survey to assess conceptual expertise. The steps are as follows: 1) conceptualization, 2) development of measures, 3) model specification, 4) scale evaluation and refinement, 5) validation, and 6) norm development (MacKenzie et al., 2011).

The results of this survey assess the depth and breadth of their understanding of the different computer forensics phases. This survey was given to IT students who had just taken and professionals I hypothesize that students and professionals will show differing competencies and understanding of the NIST knowledge points. I expect that professionals are able to easily identify the processes and steps of the computer forensics cycle and that students will only have a theoretical understanding of computer forensics and will score lower.

2 LITERATURE REVIEW

2.1 What is Conceptual Expertise?

This study is based off of a previous experiment performed to measure conceptual expertise in hackers. The project used the Security Expertise Assessment Measure (SEAM) which is a process that aims to, in part, gauge the practical application of situations to the goal wherein experts can show those skills they acquired and became proficient at (Giboney et al., 2016). This is measured in conceptual expertise and is meant to differ novices from experts in cybersecurity. Those who show proficiency with the different skills, knowledge and abilities will group different scenarios together in conceptual tasks to demonstrate thorough understanding of the fundamental processes of cybersecurity. Those who have not practiced nor "cognitively processed" not demonstrate that in the expertise in the SEAM process by pairings scenarios that have similar features but are not based on fundamental principles of cyber security.

This survey successfully proved that professionals had a thorough understanding of cyber security principles while students and self-proclaimed hackers had a superficial understanding (Giboney et al., 2016). In a similar way, the study aimed to construct a survey that would be able to assess the varying skills of computer forensics professionals and students to show the differences in understanding of computer forensics skills and principals.

The measures used to score the proficiency of survey takers was constructed in a manner following the methodology as outlined by MacKenzie, Podsakoff and Podsakoff (2011). This

process goes through five major steps: conceptualization, development of measures, model specification, scale evaluation and refinement, and validation.

As this process is adopted into this study, computer forensics conceptual expertise will demonstrate that an individual can understand the fundamentals of the computer forensics process. This conceptual expertise is demonstrated through pairing scenarios through surface features, deep features, or unexpected features.

A surface feature would be an object or context represented in a problem. These features are more "surface level" understanding of computer forensics. In the case of this study, surface features will be represented as a type of crime featured in a scenario. The types of crimes that can be paired in scenarios are fraud, murder, drug related, vandalism, and theft. If an individual pairs two scenarios based on surface features, then that demonstrates surface level knowledge.

Deep features are the underlying principles that demonstrate understanding in a certain area. They answer the "Why?" behind an action and focus on the big picture and the fundamental principles of computer forensics. In this experiment, we will use the five phases of computer forensics mentioned previously. Computer forensics is a profession that has to follow a strict methodology, or they can invalidate their results and work. With that in mind, the scenarios used are based on tasks listed in the NIST 800-181 publication. These generated scenarios contain a situation that involves only one phase of computer forensics, which if identified will demonstrate an individual's conceptual expertise.

Unexpected features are pairings of scenarios that do not belong to a surface feature or a deep feature. These pairings would feature scenario pairings that contain different types of crimes and/or different phases of computer forensics. For example, a pairing could have a drug related scenario with a vandalism scenario or a preparation scenario with a reporting scenario.

2.2 Skills Required of a Computer Forensics Professional

Computer forensics relies on expertise, computer self-efficacy and a structured and repeatable process to bring about the same results. Bandura (1986) defines self-efficacy as "People's judgements of their capabilities to organize and execute courses of action required to attain designated types of performances. It is concerned not with the skills one has but with judgments of what once (sic) can do with whatever skills one possesses (p. 391)."

As a computer forensics analyst, one must judge how to approach many different situations. Being able to have confidence to accurately judge a situation is a necessary quality to be an expert. Self-efficacy has three dimensions: magnitude, strength, generalizability. The magnitude of self-efficacy is the measure of being able to accomplish more difficult tasks. (Compeau & Higgins, 1995). Strength refers to the confidence in being able to complete designated tasks. Generalizability is the extent to which a person believes they can accomplish a task but only under certain circumstances. A computer forensics analyst will find themselves in many kinds of situations without being able to control what tasks must be performed.

Not only does a computer forensics analyst need to know how to judge a situation, they need to demonstrate proficient computer ability. There are many types of devices a computer forensics analyst will come into contact with: cell phones, laptops, security cameras, smart devices, etc. Being able to know how to use each one (and their variance) is vital in acquiring the proper information for an investigation (Cheney & Nelson, 1997). As technology develops and progresses, so does a computer forensics analyst's skills and knowledge must adapt and improve as well.

The ability to assess a computer forensics professional's skill has become increasingly difficult as the digital crimes committed have become more complex, varied, and frequent. The

professional has to keep up with the ever-evolving methodology, technology, tactics, and procedures of malicious actors to try to stay one step ahead of them (Horsman, 2017).

Some have even argued that digital crimes have become impossible to police due to the legal system not being able to stay abreast with digital crime (Brown, 2015). If digital crimes are impossible to enforce the law on, it would be less of a necessity to have computer forensics analysts on staff or at the ready. Brown sought to raise awareness about cybercrime and many of the loopholes they find to escape prosecution. Digital criminals can violate several countries' laws at a time while living in a place that does not police digital crime. For example, a Russian native can hack into a United States bank and most likely not receive any consequences. Russian law concerning cybercrime is lax and it would be impossible to extradite a citizen for any crimes committed in the United States (*IntSights Exposes Dark Side of Russia at Black Hat U.S.A*, 2021). If there are no legal ramifications for a digital crime, then how would a computer forensics professional thrive? Fortunately computer forensics will still be expanded and continued while the legal system slowly catches it policies, practices and procedures up-to-date with current cybercrimes (Horsman, 2017).

Computer forensics professionals need to acquire skills to recognize, combat, and counter cyber criminals (Barske et al., 2010). They need to know how to identify vulnerabilities, exploits, obfuscation techniques, and other signs of illicit activity. They also must perform all of the following functions:

- Ensure that there is proper legal authority to conduct the search and examination
- Ensure that the correct chain of custody is kept for the evidence
- Only use forensic tools that have been validated
- The use of imaging and hashing functions to acquire evidence

- The examination and analysis of the evidence
- Quality assurance to ensure that the examination and analysis, and the results thereof, are repeatable by another examiner
- Reporting of the findings
- Possible testifying as an expert witness in legal proceedings (Barske et al., 2010).

This requires legal knowledge of digital evidence requirements, how to preserve evidence, know how to use a variety of different digital tools, analyze and report their findings. Professionals must follow a cycle of maintaining up-to-date knowledge of strategies, policies and procedures, technology, computer forensics (referenced here as digital forensics) response methods, and compliance and monitoring to stay relevant. Technology and the skills required to perform computer forensics are increasing at a rapid rate and professionals have to do everything they can to not be left behind (Horsman, 2017).

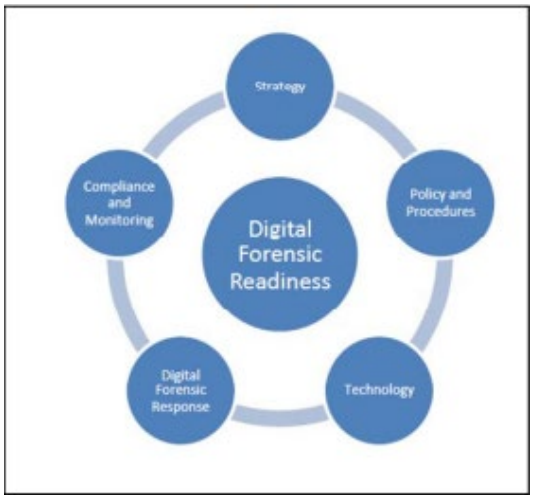


Figure 2.2: Maintaining Computer Forensics Readiness (Barske et al., 2010)

Compare the kind of cell phones that were available ten years ago. Smart phones were just introduced by Apple through the production of the iPhone and only a few individuals

possessed them. Today, ninety-seven percent of Adults in the United States of America own a cell phone and eighty-five percent own at least one smartphone devices (Center, 2021). Computer forensics policies have had to adapt to not only focus on modern computers and servers but extend to mobile devices as well. Mobile devices now carry as much information (or even more than) as personal computers such as GPS, email, texting, work communications and much more. Computer forensics professionals must know how each of these relatively new types of data on cell phone function. Wireless technologies have allowed individuals to have access to the internet in most places. Professionals must consider different standards of wireless communication and weaknesses associated with them.

To keep up with these ever evolving and changing cyber criminals, computer forensics professionals must keep learning and evolving their skills.

2.3 Learning Computer Forensics

There have been attempts to establish an education agenda to create a standard to evaluate computer forensics examiners. One attempt has been to create different education models to satisfy different needs such as legal examiners, military, law enforcement and corporations (Nance et al., 2010). They identified seven different communities that have unique computer forensics needs: law enforcement, expert witnesses, legal profession, policymakers and legislators, corporations, community, and higher education.

Law enforcement officers require knowledge about different computer forensic skills, the strict regulations revolving around digital evidence, and proven, repeatable procedural methods. The main stage of computer forensics that they need to be proficient in, is the seizure of evidence so that they do not accidentally tamper with the evidence. First responders need to not only recognize potential digital evidence, but also do not harm the evidence while

investigating it. Computer forensics analysts often have immense workloads and may not keep up with current technology so they need a set of standard procedures that will be valid for a wide variety of situations (Horsman, 2017). Law enforcement has to follow strict regulations as to help keep the legal system fair and equal. To do this, they must use repeatable, procedural methods to show that evidence has not been tampered with and that their findings are not skewed to defame or misrepresent a potential criminal.

Expert witnesses need to take digital evidence, evaluate the process the evidence went through and testify in court about it. Expert witnesses are individuals that the court uses to testify about technical details of a case to help those in the case to understand what the evidence means. They need to use specialized software and have enough experience and understanding of the computer forensics process to make sure that they are an impartial opinion and to not harm the evidence. They must ensure that the original data matches with what prosecutors or defense attorneys may show in court. These experts have to help non-technical individuals to understand what the cyber evidence shows and what it does not. Many individuals do not have a thorough understanding of how technology functions and these experts must be versed well enough to elaborate, translate and simplify digital findings to help those in a court to understand and determine if the evidence is viable.

The legal profession is an interesting community when it comes to computer forensics. Members in this community do not necessarily need to have the technical skills to process the evidence and find the evidence, but they do need to know what the process should be so that they can to understand if the evidence is viable in court.

Another group of individuals that need understanding of computer forensics are policymakers and legislators. Many of the individuals that are responsible for making laws and

policies relating to computer forensics come from a political or business background and may not understand the processes or even the technology relating to computer forensics. These individuals do not need to know the technical details and procedures, but they do need to know the limitations of what can be done and what evidence can be shown. Being able to create laws and policies that coincide with understanding of computer forensics technology will enable and protect the public, law enforcers and everyone who interacts with a digital device.

Businesses often require the aid of computer forensics analysts. They are subject to compliance laws and other regulations. These individuals need to identify and respond to cyber security incidents quickly and efficiently. Many incidents are time sensitive and early on need to be determined if law enforcement involvement is necessary. Regulations often have time requirements on reporting security breaches and a competent computer forensics analyst will discern what information has been possibly divulged and the possible need for reporting to regulation offices. Business cyber security professionals need to be proactive and seek out possible breaches within their corporation. These individuals often focus on the remediation side of computer forensics so that the problem can be remedied in a timely manner. This requires hands-on knowledge, experience, and deep understanding of technical processes.

The sixth identified group in this research (Nance et al., 2010) is the community which includes children and adults alike. Community members that have a basic understanding of how to keep themselves safe from a cyber security incident can act on minimizing the threat of digital crime. A population that is resistant to digital crime would provide a safer digital environment and a deeper understanding of how their information is used and how they can protect it.

The last identified group is Higher Education which consists of community colleges, undergraduate programs, graduate programs, technical programs, and educators. These

environments are an essential role in computer forensics for members of this community. Educators in this sector are the ones that prepare and train budding cyber security professionals. Educators need to be aware of the six different communities and to which community needs they are trying to prepare their students for. Educators may differ from professionals as they often focus on research, but as they teach to each student's needs, they can prepare them for the hands-on and experiential learning while the students are in a classroom.

Due to the vast differences between each community, an education agenda would help prepare students and individuals to enter and excel into the computer forensics field. Nance, Armstrong, & Armstrong (2010) found that by sorting students out into different categories according to their communities, they could more accurately teach to each group's varying computer forensics requirements for their profession. They also found that mixing two communities together often resulted in an experience where each community can teach each other some of the specialties that their community focuses on.

Various higher education institutions have established their own focuses. At Cypress College, they focus on practical skills while Florida A&M University tries to do a cross-disciplinary concentration with Sociology and Criminal Justice (Chi et al., 2010; Wassenaar et al., 2009). This study created an undergraduate certificate program that tried to balance theoretical and practical with a set of 2 types of classes, basic and advanced. Each had a practical lab associated with it (Lang et al., 2014). These courses and labs were designed to give students the hands-on experience with computer forensics mixed with the cyber forensics process to prepare them for computer forensics careers right out of university. They ran two pilot courses with computer science students and law students. Each group had varying degrees of success. The first class they found to be too technically heavy for the law students. They adjusted the

second class and focused on the investigation process. They found that the second class was able to reach their intended goal of teaching the cyber forensics process and giving students technical training. The computer science students were teamed up with the law students on mock investigations as a project. Together they were able to provide specialization and simulate the entire computer forensics process. Both studies were able to learn from each other and reported that their learning was enriched by interacting with other majors.

2.4 Professional Certifications

Most professionals demonstrate expertise through the acquisition of different professional certifications. Certifications, however, cannot always be a valid judge of skills. Because certifications are mostly focused on taking written and applicable tests, some people will commit the facts or principles necessary for the test to short-term memory and will forget them shortly thereafter (Rawson et al., 2013). Once someone takes a certification, they can renew it through Continuing Professional Education (CPE) credits. The CPE program was designed to meet the learning needs of professionals in many different fields (Cervero, 2001). As early as 1980 academics have been talking about the need for continuing professional education. In that decade, many such articles, proposals and books were written to convince corporations that the workforce needed to keep up to date with current knowledge, skills, and abilities to stay abreast in their fields (Houle, 1980).

Technology certifications go through a rigorous process to attempt to meet the highest standards set by overarching organizations such as the International Standards Organization (ISO) and International Electrotechnical Commission (IEC). Individuals have to study, learn, and know many different things.

Depending on the certification, CPE credits can be earned in various ways like taking classes and attending conferences ((ISC)2, 2020). While some CPE credits can enhance the skill and learning of a certification, the credits earned do not necessarily have to be related to the certificate an individual is renewing. For example, an option to maintain the Certified Information Systems Security Professional (CISSP) certificate requires forty hours a year of domain-related activities, which "relate directly to activities in the areas covered by the specific domains of the respective credential." Ten of those credits each year can be related to non-domain related professional development. However, the CISSP covers eight different domains: Risk Assurance, Asset Security, Security Architecture and Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

While these all relate to cyber security field, each domain by itself is a profession that one could spend a lifetime learning and perfecting. To be compliant with the requirements of maintaining the CISSP, an individual could spend years acquiring their CPE credits by choosing to focus on just one of these domains. Also, the CISSP was introduced in 1994, when technology was vastly different. Hard drives were around 400 MB while today's digital storage is usually measured in hundreds of terabytes. This means that a professional who did not keep up to date on all the various principles found in the CISSP exam, they would not know how to practice those principles ten or even fifteen years later in their career.

Therefore, merely by acquiring CPE credits can lead to gaps in a cyber security professional's understanding. It may be difficult to determine if that individual still has those acquired knowledge, skills, and principles from a specific certification from the time when they passed the test for the certification.

Unfortunately, individuals do not always keep up the skills they learned and certifications they hold cannot always be a proof that the holder can pass the certification again if they must. Thus, the renewal of a computer forensics certificate through CPE credits could possibly not be an accurate representation of the actual skill that the certificate holder has in the Computer Forensics field and can create difficulties for hiring managers and others wishing to assess computer forensic skill and understanding.

Due to the current inability to accurately measure an individual's skills and understanding of computer forensics principles quickly, this thesis and study investigates how to measure those principles in professionals and novices to add some value into the process of evaluating a professional's understanding of computer forensics principles.

There are quite a few variations of computer forensics certifications (Imam, 2019). These are some examples in Table 2.4:

Table 2.4 Example Certifications and Their Publisher

Acronym	Name of Certificate	Publishing Organization
ACE	AccessData Certified Examiner	AccessData
CFCE	Certified Forensic Computer Examiner	IACIS
CHFI	Computer Hacking Forensic Investigator	EC_Council
EnCe	EnCase Certified Examiner	EnCase
GCFA	GIAC Certified Forensic Analyst	GIAC
GCFE	GIAC Certified Forensic Examiner	GIAC

Most of these certifications are tied to a specific vendor, application, or operating system. Researchers Rogers and Seigfried said back in 2004,

> "To date, computer forensics has been primarily driven by vendors and applied technologies with very little consideration being given to establishing sound theoretical foundation" (Rogers & Seigfried, 2004).

These researchers also talk about how the judicial system had started to question the validity of many computer forensics procedures. The Supreme Court in *Daubert* vs *Merrell* provided specific criteria to rule on the admissibility of scientific evidence:

- whether the theory or technique has been reliably tested;
- whether the theory or technique has been subject to peer review and publication;
- what is known or potential rate of error of the method used; and
- whether the theory or method has been generally accepted by the scientific community.

Computer forensics certifications attempt to live up to a standard set by the international groups, the International Standards Organization (ISO) and International Electrotechnical Commission (IEC). They have established a technical committee that have demonstrated mastery, competence, and years of experience to help establish guidelines, policies, and bars of expectations that certifications must meet.

Many of the certifications requested in current computer forensics job postings stem from these companies, GIAC, (ISC)^2, IACIS, and the EC-Council. These groups have a wide variety of certifications ranging from entry level computer forensics to elite level programs where less than 300 individuals worldwide have demonstrated abilities to pass their certification tests.

2.5 Retaining Skills

It is common for people to forget knowledge and skills without incorporating them into daily life. Such as cramming for exams the night before, people often forget the information they

rushed to learn and remember (Rawson et al., 2013). The same applies with technology certifications. One must practice the same skills they learned for the certification test continuously to convert them to long-term memory. “Cognitive processes play a prominent role in the acquisition and retention of new behavior patterns” (Bandura, 1977). These behavior patterns reflect how the mind stores long-term memories. When individuals practice their skills they are better retained.

If the individuals who obtained these exams earned their Continuing Professional Education credits relating to computer forensics and continue to gain expertise in the field, then they should to retain their skills, abilities, and areas of knowledge that they gained and proved in the certifications. However, as discussed in the introduction, Continuing Professional Education credits do not always have to be related directly to their area of expertise. These are what Continuing Professional Education credits are supposed to emulate and encourage professionals to keep developing their skills, knowledge, and ability. While NIST 800-181 (Newhouse et al., 2016) does not advance as quickly as technology does, it does lay out the foundational and basic skills required for IT professionals. Basing the hypothesis of this thesis on these foundational principles will help keep the survey scenarios developed to be technology agnostic and apply to all situations a computer forensics professional may encounter. The conceptual expertise will gauge the fundamentals these professionals understand. Experts will perform and understand computer forensics tasks superior to novices as they have practical experience and time to solidify their knowledge in their field.

3 METHODOLOGY AND COLLECTION OF DATA

3.1 Development of Measures and Testing

As computer forensics is on the defensive side of cyber security, the SEAM process could be useful as it is a similar application, just directed at a different audience. A computer forensics analyst needs to know hacking methods and motivations. If they are familiar with a hacker's tactics, techniques, and procedures, then they can perform their job more effectively (Voiskounsky & Smyslova, 2003). Giboney (2016) discusses the benefits of a study with a survey over a qualitative experiment. As this study can assign a quantitative value to a qualitative result, one can start to measure expertise on a numerical scale.

Computer forensics expertise is similar to hacking. Knowing how to circumvent security controls and vulnerabilities will help them track down attack vectors and methods hackers commonly use to infiltrate systems. They can also demonstrate proficiency by their knowledge of file systems, how file permissions and read/write procedures of different operating systems, knowledge of finding hidden or obfuscated files and how to prepare evidence to stand in a legal court. Survey takers will be measured against their knowledge of these kinds of principles. Since NIST standards are accepted by the government and are often applied to data policies and government work, it seems that this would be a good document on which to base the assessment.

The measures in this survey will be based on principles from a publication of standards by the National Institute of Standards and Technology, NIST 800-181 (Newhouse et al., 2016).

While the ISO and the IEC have international standards, they can be a bit general. These standards by NIST are specific technological skills and knowledge points that have been laid out. Relevant tasks from this guide will be grouped according to their relations to computer forensics phases and stages. As participants correctly classify different tasks, then the depth of their knowledge and ability can be assessed according to the skills required to perform each task that the survey taker has learned about or used previously.

The surface feature categories have five different crimes involved in their situations: murder, drug-related crimes, fraud, theft, and vandalism. The deep feature categories consist of the five stages of computer forensics: preparation, seizure of evidence, acquisition of data, analysis of data and reporting the findings of analysis. Twenty-five scenarios, using an alphabetical list, will be created featuring one surface feature and one deep feature each.

This process is visually depicted in table 3.1. Situations in vertical columns are related deep features in each process stage of computer forensics. Situations in horizontal rows are related surface features which are grouped by crime. Each letter is a corresponds to a scenario given on the survey.

Table 3.1: Correlation of Surface and Deep Features

		Hypothesized Deep Features				
		Preparation	Seizure	Acquisition	Analysis	Reporting
Hypothesized Surface Features	Theft	X	L	E	S	O
	Vandalism	J	G	Q	V	B
	Murder	M	C	U	I	Y
	Drug Related	D	T	W	A	R
	Fraud	P	H	K	N	F

3.2 Mapping Scenarios to TKSA Points From NIST

In order to build the scenarios off technical standards, five principles from each stage of computer forensics were selected. Each principle is directly correlated to a Task, Knowledge Point, Skill or Ability (TKSA) outlined in the National Institute of Standards and Technology 800-181 (Newhouse et al., 2016). This allows for these situations to be based on a nationally accepted list of standards. Due to the situations being task oriented, most of the principles are based on expected tasks of a computer forensics professional over the skills, knowledge and abilities listed in the document.

The twenty-five scenarios are split into five groups where five scenarios are correlated with each computer forensics stage of the process. Most of the situations are directly related to a principle while others are based on the fundamental point of the principle.

Table 3.2-1: TKSA Principles Outlined by Computer Forensics Process

Preparation	**Principle**
Principle A	Examine Network Topologies to understand data flows through the network (pg. 11)
Principle B	Write Standard Operating Procedures (T0247)
Principle C	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures or other issuances (T0419)
Principle D	Employ IT systems and digital storage media to solve investigate and/or prosecute cybercrimes and fraud (T0479)
Principle E	Determine tactics techniques and procedures (TTPs) for intrusion sets (T290)
Seizure	**Principle**
Principle A	Ensure that chain of custody is followed for all digital media acquired in accordance with the federal rules of evidence (T0087)
Principle B	Capture and analyze network traffic associated with malicious activities using network monitoring tools. (T0240)
Principle C	Document original condition of digital and/or associated evidence (via digital photos, written reports, hash function checking (T0471)
Principle D	Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements (T0562)
Principle E	Apply and obey applicable statutes, laws, regulations and policies (T0574)

Table 3.2-1: Continued

Acquisition	**Principle**
Principle A	Extract data using data carving techniques (T0238)
Principle B	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence (T0241)
Principle C	Utilize different programing languages to write code, open files, read files and write output to different files (T0404)
Principle D	Decrypt seized data using technical means (T0049)
Principle E	Create a forensically sound duplicate of evidence (T0048)
Analysis	**Principle**
Principle A	Characterize and analyze network traffic to identify anomalous activity and potential threats (T0023)
Principle B	Conduct analysis of log files, evidence, and other info to determine best methods of identifying perp(s) of a network intrusion (T0027)
Principle C	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile (T0019)
Principle D	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information (T0260)
Principle E	Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data (T0439)
Reporting	**Principle**
Principle A	Present technical information to technical and nontechnical audiences (T0381)
Principle B	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation (T0047)
Principle C	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal actions (T0110)
Principle D	Prepare legal and other relevant documents (T0522)
Principle E	Assess the validity of source data and subsequent findings. (T0347)

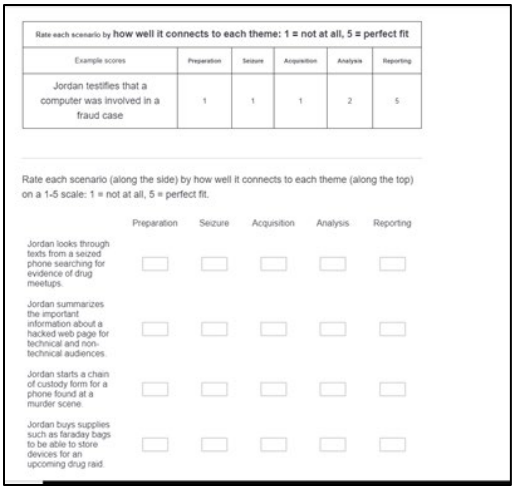
These situations focus on a gender-neutral individual named Jordan. In the survey it describes the actions they perform when completing common computer forensics duties. The situations are singular sentences stating what Jordan does in a single task. The sentence structure has been varied as to prevent any type of pattern that survey takers could use to fill out the assessment without understanding either the surface or deep features. The sentence either positions the type of crime first in the sentence or the forensic task first. An example of these differences would be “Jordan recovers a laptop discovered at the scene of a drug bust and Jordan goes to the scene of a drug bust to recover a laptop.”

This variation is to help differentiate which is featured first, the surface and deep features of a situation. The surface feature in this case would be that this crime involves drugs while the deep feature is recovering the laptop. Recovering the laptop would fit into the *Acquisition* phase of the computer forensics process. The goal is to have survey takers understand which phase of the computer forensics cycle the situation would fit into and not to use patterns or other methods to discern how the groupings should be made.

All situations were randomly assigned a position in the survey by using a random number generator. Twelve of the situations are phrased with the crime category first with the other thirteen starting with the forensics category first. Survey takers will be asked to group the situations by stage of forensics or by what crime the task is involved with. At the end of the survey, participants will also enter in how many years of experience and their current job role so that their results can be compared with their peers.

Apart from the surface features and deep features, there are many other ways to group each situation that could not be predetermined. If a situation is not within a deep or surface feature, it will be labeled as an unexpected feature and be scored differently to provide context for answers that don't fall into any of the expected categories.

To ensure that the scenarios were correctly attributed to the computer forensics stage they belonged to, a group of 15 IT students that had taken a computer forensics course were asked to rate each situation. They were asked to rate the situation on a scale of 1 – 5 of how well the situation fit inside the preparation, seizure, acquisition, analyzing and reporting stages, with 5 being a perfect fit. An example of this survey is represented by Figure 3.2-1 and the situations that were initially evaluated can be found in Table 3.2-2.



Rate each scenario by **how well it connects to each theme: 1 = not at all, 5 = perfect fit**

Example scores	Preparation	Seizure	Acquisition	Analysis	Reporting
Jordan testifies that a computer was involved in a fraud case	1	1	1	2	5

Rate each scenario (along the side) by how well it connects to each theme (along the top) on a 1-5 scale: 1 = not at all, 5 = perfect fit.

	Preparation	Seizure	Acquisition	Analysis	Reporting
Jordan looks through texts from a seized phone searching for evidence of drug meetups.					
Jordan summarizes the important information about a hacked web page for technical and non-technical audiences.					
Jordan starts a chain of custody form for a phone found at a murder scene.					
Jordan buys supplies such as faraday bags to be able to store devices for an upcoming drug raid.					

Figure 3.2-1: Assessment Rated by Students

The survey also provided a space for the responders to leave comments about the situations and if any steps were unclear to them. Responders were able to leave specific comments that were able to help improve the situations for future use. The comments, combined with the numerical results, were used to acknowledge where some situations may have been ambiguous to what phase they may have belonged to and refine the situations to be plain and straightforward about which computer forensics phase they belonged to.

If a given situation had a majority of responses correct, then the situation was then deemed that it would work for the survey and was kept as it was written. If a given situation's responses seemed to be confusing for the survey takers, the scenarios were reviewed to see why the proper category wasn't apparent in the situation. Six of the twenty-five situations were required to be tuned as the majority of response rates had put them into an incorrect category. These situations were then clarified so that the phase it belonged to would be apparent. Doing so would help the survey be more concise and make sure that the options presented would be fully focused on the correct surface and deep features.

Table 3.2-2: Initial Situations

Hypothesized Surface Feature	Hypothesized Deep Feature	Situation
Drug Related	Analysis	Jordan looks through texts from a seized phone searching for evidence of drug meetups.
Vandalism	Reporting	Jordan summarizes the important information about a hacked web page for technical and non-technical audiences.
Murder	Seizure	Jordan starts a chain of custody form for a phone found at a murder scene.
Drug Related	Preparation	Jordan buys supplies such as faraday bags to be able to store devices for an upcoming drug raid.
Theft	Acquisition	Jordan uses a write blocker to copy a hard drive brought to the forensics lab from a robbery case.
Fraud	Reporting	Jordan writes an assessment about data related to a bank fraud.
Vandalism	Seizure	Jordan captures the router connected to a hacker's computer that vandalized a website.
Fraud	Seizure	Jordan records network traffic of a hacker's computer that vandalized a website.
Murder	Analysis	Jordan uses file carving to investigate a murder suspect's computer.
Vandalism	Preparation	Jordan learns hacking methods in preparation to access data on a graffiti artist's device.
Fraud	Acquisition	Jordan obtains warrants for devices that may have been used by money launderers.
Theft	Seizure	Jordan takes a photo at a crime scene of a hard drive that contains stolen company secrets
Murder	Preparation	Jordan reads newly released legal proceedings from a murder case that used digital forensics.
Fraud	Analysis	Jordan identifies discrepancies in the financial books and data from a bank's server logs.
Theft	Reporting	Jordan shows the judge that the hashes of analyzed files are the same as the original hashes from an art heist case.
Fraud	Preparation	Jordan wins a contract to investigate fraud and decides to certify their forensics lab.
Vandalism	Acquisition	Jordan uses a script to automate the imaging of a hacked server.
Drug Related	Reporting	Jordan writes down in his report that a smart home device was used to coordinate the sale of drugs.
Theft	Analysis	Jordan determines that images on a device use steganography to convey stolen trade secrets.
Drug Related	Seizure	Jordan finds a phone at a drug bust and places it into a faraday bag.
Murder	Acquisition	Jordan decrypts the stored data on the desktop of a murdered billionaire.
Vandalism	Analysis	Jordan locates the wifi connections from a phone collected near recent graffiti activity.
Drug Related	Acquisition	Jordan collects a drug lord's phone and hashes its data.
Theft	Preparation	For a theft case, Jordan writes a set of standard procedures for processing and copying hard drives.
Murder	Reporting	Jordan testifies that the geolocation data of a smart watch matches the estimated time of death of a murder victim.

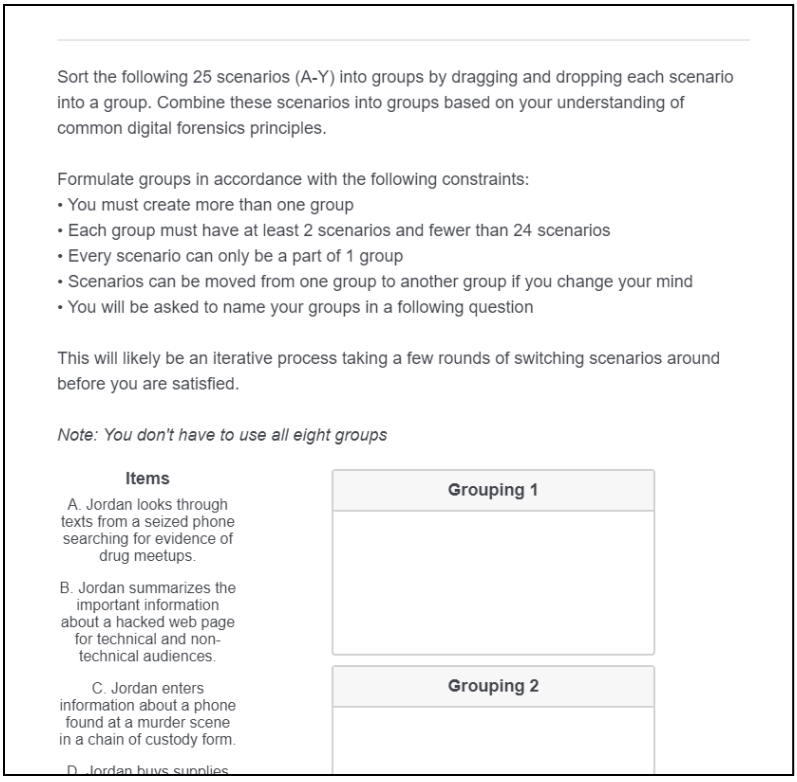


Figure 3.2.2-2: Final Survey Used in the Collection of Data

Survey takers could name any of the groupings how they saw fit. The order or the name of the groups did not factor into the calculation of surface, deep, or unexpected features. Allowing the freedom to let survey takers to think creatively as they evaluated the scenarios based on the instructions:

> Combine these scenarios into groups based on your understanding of common digital forensics principles.

All situations and their corresponding categories are listed below in Table 3.2.2-3: Final Edit of Proposed Situations. Each situation in the table is listed in order presented on the survey. The listed surface features and deep features are included for this report but were not present on the survey itself.

Table 3.2.2-3: Final Edit of Proposed Situations

Surface Feature	*Deep Feature*	*Situation*
Drug Related	Analysis	Jordan looks through texts from a seized phone searching for evidence of drug meetups.
Vandalism	Reporting	Jordan summarizes the important information about a hacked web page for technical and non-technical audiences.
Murder	Seizure	Jordan enters information about a phone found at a murder scene in a chain of custody form.
Drug Related	Preparation	Jordan buys supplies such as faraday bags to be able to store devices for an upcoming drug raid.
Theft	Acquisition	Jordan uses a write blocker to copy a hard drive brought to the forensics lab from a robbery case.
Fraud	Reporting	Jordan writes an assessment about data related to a bank fraud.
Vandalism	Seizure	Jordan captures the router connected to a hacker's computer that vandalized a website.
Fraud	Seizure	Jordan searches for all digital devices that employees used to scam bank customers.
Murder	Analysis	Jordan uses file carving to investigate a murder suspect's computer.
Vandalism	Preparation	Jordan learns hacking methods in preparation to access data on a graffiti artist's device.
Fraud	Acquisition	Jordan jail breaks devices to obtain data that may have been used by money launderers.
Theft	Seizure	Jordan takes a photo at a crime scene of a hard drive that contains stolen company secrets
Murder	Preparation	Jordan reads newly released legal proceedings from a murder case that used digital forensics.
Fraud	Analysis	Jordan identifies discrepancies in the financial books and data from a bank's server logs.
Theft	Reporting	Jordan shows the judge that the hashes of analyzed files are the same as the original hashes from an art heist case.
Fraud	Preparation	Jordan wins a contract to investigate fraud and decides to certify their forensics lab.
Vandalism	Acquisition	Jordan uses a script to automate the imaging of a seized web server containing a defaced website.
Drug Related	Reporting	Jordan writes down in his report that a smart home device was used to coordinate the sale of drugs.
Theft	Analysis	Jordan determines that images on a device use steganography to convey stolen trade secrets.
Drug Related	Seizure	Jordan finds a phone at a drug bust and places it into a faraday bag.
Murder	Acquisition	Jordan uses a decryption algorithm to recover lost data on the desktop of a murdered billionaire.
Vandalism	Analysis	Jordan constructs a map of the location history of a phone recovered near a defaced public building.
Drug Related	Acquisition	Jordan hashes the data from a drug lord's phone checked out from an evidence locker.
Theft	Preparation	Jordan writes a set of standard procedures for processing and copying hard drives during a theft case.
Murder	Reporting	Jordan testifies that the geolocation data of a smart watch matches the estimated time of death of a murder victim.

3.3 Collection of Data

The assessment was then tested against self-proclaimed professionals with computer forensics experience and a group of students that were in the process of taking a college level computer forensics class. The assessment was hosted on Qualtrics and was available for approximately a period of 4 weeks and over 200 results were submitted.

Students that were taking the class were offered a small portion of extra credit to take the survey. With that incentive, thirty of them participated in the assessment. Professionals were offered an incentive of winning a twenty-five dollar gift card to Amazon.

To reach the professionals, a survey link was posted on LinkedIn by a certified computer forensics professional asking other computer forensics professionals to participate in the survey. While the student's data was returned in an acceptable manner, some work was needed to clean up the professionals' data.

Unfortunately, due to the link being distributed on LinkedIn, it appears that some web crawling bots designed to take surveys were able to submit responses. There were over a hundred responses that had improbable answers to questions. For example, some had answered that they had more years of computer forensics experience than how many years they had existed. Others submitted that they had years of experience longer than the field of computer forensics has been around. Other responses indicated that they had started computer forensics as children under the age of 18. In an effort to standardize and remove inaccurate data, any response that where the years of experience exceeded the age of the responder or put them under the age of 17 were eliminated from the responses. This reduced the number of professional survey results from 200 to 109, which was a still a significant number to consider.

4 ANALYSIS, CONCLUSIONS, AND FUTURE WORK

4.1 Analysis

Using Qualtrics as a base for collecting the data, the results were downloaded into a csv format. The responses were then reformatted using a python script to extract the data, organize the situations and put each situation into the category they believed it should be in. It put each answer into a format that the algorithm was able to use to calculate the surface, deep and unexpected features.

The algorithm was then adjusted to the specifics of the survey. It determined surface, deep, and unexpected features, correlating each given situation with its surface feature and deep feature. Running the answers against the algorithm provided some statistics that could be visually graphed to show the general understanding of professionals versus the students.

Programmatically, the algorithm would look akin to a function like this. The algorithm would compare the given situation and look for a surface, deep or unexpected feature.

If Situation A = *x*:

If *x* == B then result = unexpected

If *x* == C then result = unexpected

If *x* == D then result = surface

If *x* == E then result = unexpected

If *x* == F then result = unexpected

If x == G then result = unexpected

If x == H then result = unexpected

If x == I then result = deep

Running the results through the algorithm produced the following results. Students were able to group their results by deep features on average 45.68% of the time with a 11.39% standard deviation. This is an exceptionally high rate compared to their surface feature mean of 10.14% with a standard deviation of 3.77%. These results show that the students had a decent understanding of the underlying principles of the situations and were not distracted by the surface feature parts of each scenario. Even though almost of their responses were unexpected correlations, they fared much better than the professionals.

Professionals had a much lower deep feature rate as the results showed that only 10.67% of their solutions had a related deep feature with a 5.99% standard deviation of the mean. Their surface feature correlation was only slightly higher at 12.45% with a 9.83% standard deviation. That meant that almost 80% of their responses had unexpected features in their groupings. Professionals did not seem to understand the underlying principles of each situation and grouped them in unexpected ways.

These results are depicted visually in Figure 4.1 where the results can be seen between the two groups. It was expected that professionals would have the least amount of surface features and unexpected results due to their time, training, and experience in the field. According to the sources in the literature review, professionals would have been able to identify the deep features of each scenario on a more consistent basis.

The unexpected features had much higher score than what was originally anticipated. This is an interesting data point as it was assumed that the most apparent features in scenarios was the stage the scenario took place in and the type of crime that was involved.

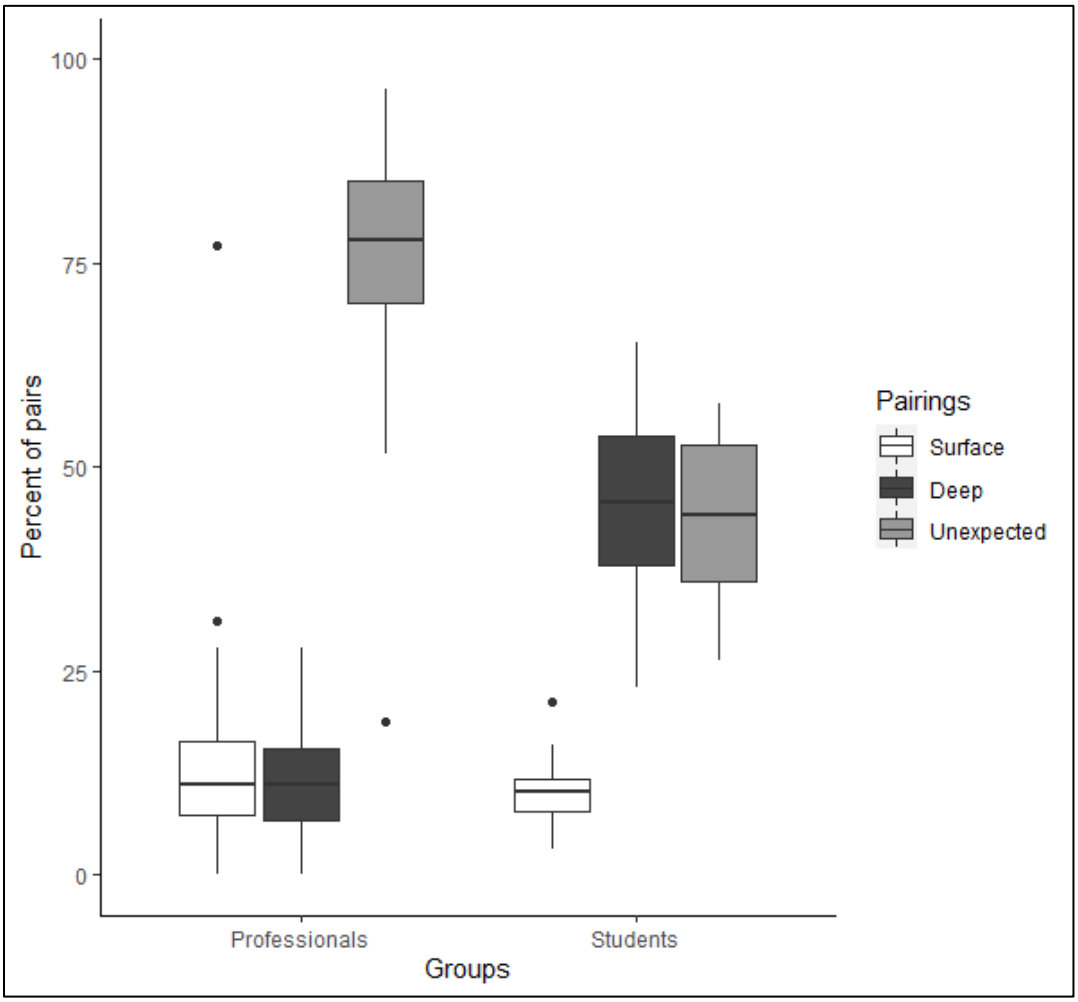


Figure 4.1: Graph of Deep, Surface, and Unexpected Features of Each Study Group

4.2 Limitations

There were some limitations that hindered the survey. The first being that the survey was published to professionals on LinkedIn without regard to who could take it. LinkedIn is an open

social media platform where there are no limitations on who can join it. Evidence of this was shown in that nearly one hundred bots or fake surveys were completed and submitted. This was also shown in most of the surveys taken in the very low deep feature grouping rate.

A second factor is that survey takers had to be trusted implicitly when stating the amount of computer forensics experience they had acquired. There was no true measure that could be enforced or implemented. One's personal view of their skills, abilities, knowledge of computer forensics may be skewed to actual true skill they may possess. More data than can be collected and used in evaluation would be the certifications a professional may hold and the grade that a student had earned in a computer forensics course and compare those to the amount of surface, deep, and unexpected features the individual creates.

Another factor could be that individuals were motivated to complete the survey only for a chance to receive the Amazon gift card. They could not have any computer forensics experience and just wanted the gift card.

It could also be that once professionals transition to working in the field, they are beset with daily tasks and that is their primary focus. This survey could be attuned towards academic learning and points of view and because professionals focus on completing tasks related to their employment, they may not immediately think of the big picture.

4.3 Discussion

Although the results were not what was predicted, there were still valuable results that were produced from this study. The original question was, "Can it be determined if a professional has more conceptual expertise than students by grouping like scenarios into the phase of computer forensics the scenario is performed in?" After performing the study, it seems

clear that professionals are more focused on tasks related to the job rather than a big picture scenario. This disproves the original hypothesis and raises some interesting questions.

Students that had the knowledge fresh in their minds from taking a class were able to show conceptual expertise in understanding the basic principles of computer forensics. They were able to show that the knowledge, skills, and areas of computer forensics they learned in a classroom setting and demonstrated their understanding in the different tasks laid out in each situation. Nearly half of their groupings contained similar deep features while only 10% of their groupings contained surface features. Coursework included introduction to different forensics tools, mock investigations, and introduction to the different the computer forensics stages and processes. Just under half of the student participants were able to use the skills, knowledge, and abilities to identify the tasks and what was required by the computer forensics professional in each of the situations.

Since novices were able to identify the deep features nearly 45% of the time, it was expected that professionals would have a similar or higher identification of deep features due to their experience, knowledge of the subject matter, and expertise. The low grouping rate, however, proves a different story.

Professionals who took the survey did not seem to understand the purpose of it. Due to the low percentage of grouped surface and deep features of approximately 10% each, their groupings seemed to be much more random. It seems that a majority of the "professionals" who had taken the survey did not have a solid understanding of computer forensics and the principles behind why each situation was performed. Citing one of the survey results from a professional computer forensics expert, they were observed to have grouped the situations by surface level features. If asked explicitly what the five stages of computer forensics were, they would have

been able to answer that question correctly and elaborate on each stage. The ambiguity of the survey seemed to throw most professionals off, much like the survey had seen some incoherence of computer forensics phases during the initial stages of the survey building process.

It is possible that professionals did not take their time during the survey to assess each situation. As mentioned previously, many computer forensics individuals have backlogs of tasks and work on their plates. They may have done the survey quickly to participate in it and then move on. The amount of time taken to complete the survey was not measured and so that could not be evaluated if that was a possible reason or not.

When Giboney performed his study on evaluating the conceptual expertise of hackers, he had referenced that individuals can often have a bias towards their own skills, abilities, and areas of knowledge (Giboney et al., 2016). It is also possible this was the case in this study as the survey was open to an indeterminate amount and unfocused group of participants. Individuals could have had a loftier and inflated view of their computer forensics skills and classified themselves as professionals to take the survey. Their lack of knowledge of the core principles of computer forensics could be a main reason why the professional group scored poorly.

Many people learn cybersecurity from personal efforts rather than an organized educational setting. One major source of learning is do-it-yourself courses and tasks hosted on the internet or through online videos hosted on platforms such as YouTube. This type of learning tends to focus on doing specific tasks and being able to complete objectives rather than learning underlying principles. Professionals who learned and entered the field this way would complete all the tasks required of a computer forensics analyst proficiently but not understand the foundational principles behind the tasks.

Some interesting future iterations of this work would concentrate on getting more focused data set of professionals rather than an open survey on the internet. A more focused method of obtaining professional data would be to solicit participation from digital forensic firms and corporations. They require their employees to be proficient, competent and perform all the daily tasks clients would require of them. If employees from these types of businesses would participate, it would eliminate much of the uncertainty of the level of expertise professionals had in this study. One can compare the results of that study with this study and can more accurately tell if professionals really do focus more on tasks than big picture principles.

Future work could also evaluate the names of the groupings that professionals use to see if they saw more complex connections between the scenario. For example, this survey would be useful in an interview and be a discussion point between an employer and a job candidate to understand the way that they think.

4.4 Conclusion

This research aimed to identify what knowledge, skills, tasks, and abilities can demonstrate conceptual expertise of computer forensics. The survey results have shown that the ability that individuals have to evaluate tasks, place them into groups based on surface features and deep features requires knowledge and skill of computer forensics. The tasks selected are fundamental in a computer forensics professional's daily work and a basic knowledge of the underlying computer forensics phases can help determine whether or not an individual comprehends them.

This study has promise to help individuals evaluate whether a professional knows the basics of computer forensics principles. While not being able to identify the exact skills, knowledge, and expertise an individual may have regarding the different stages of computer

forensics. Surveys like this could be used in job interviews, establishing expertise for a court case, or even evaluating students' learning in a computer forensics class. Furthermore, this study has confirmed that because an individual can claim to be a professional in a field, it does not mean they understand the basic phases of computer forensics.

REFERENCES

(ISC)2. (2020). *(ISC)2 Continuing Professional Education (CPE) Handbook Contents*. https://www.isc2.org/-/media/ISC2/Certifications/CPE/CPE---Handbook.ashx

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122–147. https://doi.org/10.1037/0003-066X.37.2.122

Barske, D., Stander, A., & Jordaan, J. (2010). A digital forensic readiness framework for South African SME's. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. https://doi.org/10.1109/ISSA.2010.5588281

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55–119. https://doi.org/10.5281/zenodo.22387

Center, P. R. (2021). *Mobile Fact Sheet*. https://www.pewresearch.org/internet/fact-sheet/mobile/

Cervero, R. M. (2001). Continuing professional education in transition, 1981-2000. *International Journal of Lifelong Education*, *20*(1–2), 16–30. https://doi.org/10.1080/09638280010008282

Cheney, P., & Nelson, R. R. (1997). BRIEF COMMUNICATION. *Psychological Medicine*, *27*(5), S0033291796004436. https://doi.org/10.1017/S0033291796004436

Chi, H., Dix-Richardson, F., & Evans, D. (2010). Designing a computer forensics concentration for cross-disciplinary undergraduate students. *Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10*, 52–57. https://doi.org/10.1145/1940941.1940956

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly: Management Information Systems*, *19*(2), 189–210. https://doi.org/10.2307/249688

Giboney, J. S., Proudfoot, J. G., Goel, S., & Valacich, J. S. (2016). The Security Expertise Assessment Measure (SEAM): Developing a scale for hacker expertise. *Computers and Security*, *60*, 37–51. https://doi.org/10.1016/j.cose.2016.04.001

Horsman, G. (2017). Can we continue to effectively police digital crime? *Science and Justice*, *57*(6), 448–454. https://doi.org/10.1016/j.scijus.2017.06.001

Houle, C. O. (1980). *Continuing learning in the professions* (1st ed.). Joseey-Bass.

Imam, F. (2019). *The Big List of Computer Forensics Certifications [Updated 2019]*. INFOSEC. https://resources.infosecinstitute.com/topic/big-list-computer-forensics-certifications/

IntSights Exposes Dark Side of Russia at Black Hat U.S.A. (2021). EBSCO. http://erl.lib.byu.edu/login/?url=http://search.ebscohost.com.erl.lib.byu.edu/login.aspx?direct=true&db=bwh&AN=201908080900PR.NEWS.USPR.LN36661&site=eds-live&scope=site

Lang, A., Bashir, M., Campbell, R., & DeStefano, L. (2014). Developing a new digital forensics curriculum. *Proceedings of the Digital Forensic Research Conference, DFRWS 2014 USA*, *11*, S76–S84. https://doi.org/10.1016/j.diin.2014.05.008

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly: Management Information Systems*, *35*(2), 293–334. https://doi.org/10.2307/23044045

Marcella, J., A., & Greenfield, R. S. (2002). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* (A. Marcella, J. & R. S. Greenfield (Eds.); 1st ed.). Auerbach Publications. https://doi.org/9781420000115

Nance, K., Armstrong, H., & Armstrong, C. (2010). Digital forensics: Defining an education agenda. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2010.151

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2016). National Initiative for Cybersecurity Cybersecurity Workforce Framework Education (NICE). *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*, 1–135. https://doi.org/10.6028/NIST.SP.800-181

Rawson, K. A., Dunlosky, J., & Sciartelli, S. M. (2013). The Power of Successive Relearning: Improving Performance on Course Exams and Long-Term Retention. *Educational Psychology Review*, *25*(4), 523–548. https://doi.org/10.1007/s10648-013-9240-4

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers and Security*, *23*(1), 12–16. https://doi.org/10.1016/j.cose.2004.01.003

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-based model of computer hackers' motivation. *Cyberpsychology and Behavior*, *6*(2), 171–180. https://doi.org/10.1089/109493103321640365

Wassenaar, D., Woo, D., & Wu, P. (2009). A Certificate Program in Computer Forensics. *J. Comput. Sci. Coll.*, *24*(4), 158–167. http://dl.acm.org/citation.cfm?id=1516546.1516575