4-26-2012

ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS

Francis Ripberger
ripbergerresearch@gmail.com

Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By FRANCIS MICHAEL RIPBERGER

Entitled
ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS

For the degree of Master of Science

Is approved by the final examining committee:

DR. MARCUS ROGERS
Chair

ERIC MATSON

J. ERIC DIETZ

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): DR. MARCUS ROGERS

Approved by: JEFFREY BREWER 04/24/2012
Head of the Graduate Program Date

Graduate School Form 20
(Revised 9/10)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS

For the degree of Master of Science

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22,* September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

FRANCIS MICHAEL RIPBERGER

Printed Name and Signature of Candidate

APRIL 24, 2012

Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS

A Thesis

Submitted to the Faculty

of

Purdue University

by

Francis Ripberger

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2012

Purdue University

West Lafayette, Indiana

ACKNOWLEDGMENTS

I would like to thank Dr. Marcus Rogers for the time he spent helping and directing me in this study.

I would also like to thank the Purdue IRB for taking their time to answer my questions and assisting me in filling out the right forms.

Special thanks to my committee members, Dr. Eric Matson and Dr. James Dietz, for joining my committee late in the process to help complete my degree.

Last, but not least, special thanks to all the participants who completed the research. Your time was very much appreciated.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table Page

LIST OF FIGURES

ABSTRACT

Ripberger, Francis. M.S., Purdue University, May 2012. Organizing Research in Cyber Forensics. Major Professor: Dr. Marcus Rogers.

The field of Cyber Forensics is still in its early stages of development. There are many possibilities for conducting research to progress the field, but not everyone knows what they are. This study sought to identify the general needs of the field's practitioners and discover any prevailing issues preventing the Cyber Forensic field from maintaining or establishing validity in its procedures, software, and expert witnesses. This study took volunteers from universities that offer a cyber forensic program and each state's Law Enforcement cyber crime units. All participants were given three rounds of questions in order to discover the issues of the field. From these questions, lists of categorized issues were generated. The top issues were chosen from each category, as well as the top ten issues overall.

CHAPTER 1. INTRODUCTION

1.1. Background

Technology continues to grow in our daily lives. It is in our cars, on our desks, in our pockets, on our homes, etc. Our world runs on computers and everyone is either using one or exposed to it. Cyber Forensics allows us to evaluate said technology and reveal how it is being used and by who. As technology has become dominate in our society, it is used regularly for committing crimes. Law Enforcement agencies were forced to begin conducting Cyber Forensic investigations to compensate. However, there are not many people qualified for this kind of investigation. In addition, the field is relatively new and has many aspects that need to be improved. Many individuals involved with the field know of one issue or another, but no one can know them all. Theses kinds of issues need to be identified and researched in order to establish solutions for them.

Law Enforcement agencies utilize the field in order to aid them in their investigations, Lawyers use the results discovered by the analysis of the technology during investigations to prosecute villains and exonerate the innocent, and the academics are helping research solutions to known issues; later becoming investigators themselves. Asking the opinions of those who are directly exposed to the field, and its issues, is the best staring point. The questions asked of these three groups identified the current issues in the field, elaborated on Cyber Forensic Expert characteristics, and helped evaluate the

field as a whole. From this study the groundwork has been laid for future studies and research projects in an effort to progress the field forward.

1.2. Research Question

In order to better direct research and development for Cyber Forensics, what are the top open issues in the Cyber Forensic field based on the opinions of those who are directly involved that community, and is there any research and development currently being performed in order to address those issues?

1.3. Reasons for Research

The cyber forensics field is still young and in great need of development (Dr. Marc Rogers, personal communication, January 26, 2010). Every day new issues are discovered; as well as existing issues continue to plague the field. The issues for the field range from simple regulations on how to conduct a forensic procedure, to a lack of certifications, to judicial law shortcomings to properly enforce rules and guidelines. In addition, many of the individuals who are engrossed in the field are aware of one problem or another, many do not know the underlining issues. On the other hand, some have completed research on issues in localized general regions, but no one has performed a national study (Rogers & Siegfried, 2003). In addition, research is performed based on the researcher's experience (Craiger, Swauger, Marberry, & Hendricks, 2006). Meaning, if the researcher does not experience a problem, how will they know one exists? This causes a few issues in itself. For example, if a forensic analyst has a difficult time searching systems for a specific type of file, then they might start research in order to make this task easier. Meanwhile, John Doe in a neighboring county is having the same

issue and starts to research and develop the same solution. Neither of which know what the other is doing, therefore producing redundant work. As neither are affiliated with any nationally accepted accredited program, which is part of another issue (lack of certifications and accreditation), their research is not properly dispersed or made available for others to use. Therefore, the cycle starts again in another location by another individual, more redundant work.

The redundant work does not stop at isolated individuals. Even recognized programs or groups are following the same trend of redundant work. Performing a Google search for cyber forensic procedures will yield several pages of different authors describing the same thing; the correct model for conducting a cyber forensic investigation. Many of these articles overlap, do not add any depth, or make any significant changes to their defined models. Everyone having their own opinion about the "correct" procedure and none of them being nationally accepted as a standard does not help the field.

Newcomers to the field are at a greater disadvantage, such as graduate research students. They have no idea where to start for their thesis. They may know of a few issues based on the opinion of individuals who work in their department or from what they have read, but they have no experience. In order for the forensic community to truly benefit from their research, they need to be informed of the areas in need. They need direction.

The study helped combat these issues and bring ideas together. Individuals and groups now have a better understanding of the real issues, see what projects are in development, and have a broader view of the field as a whole, regardless of experience.

The discovered results will be dispersed to the volunteers of the study, as well as made available to the public for anyone who is interested in viewing it. It was the goal of this project to broaden the perspective of the individuals in the field with the hope of better organizing research and development to address the issues that plague it.

It is vital that these discovered issues are addressed before the gab between technology/law and Cyber Forensics becomes too large to cross; analysts are already struggling to accomplish the amount of work they have, rapid developing technology is increasing the time and struggle to retrieve evidence, and as technology becomes more prominent in daily life, law will need to change in order to combat the inevitable rise of cyber crime.

1.4. Significance

The study helped to combat the concerns laid out in the *Reasons for Research*. It documented what is currently in development and what the issues of the field are. In other words, individuals and groups have a better understanding of what the real problems are, see what projects are in development, and have a broader view of the field as a whole. The research has been conducted and will be dispersed to the volunteers of the study. This will allow them to see the field outside their own point of view. In addition, the results will be made available to the public for anyone who is interested in viewing it, as well as, encourage those who received it directly, to share it among their peers. It was hoped that this study will better organize the field, spur better research and development, and inform the cyber forensic community of the major issues in the field so they may be addressed instead of possibly lost in the shuffle.

Once Cyber Forensic research institutes are made aware of this top issues, they will then have a guide to produce answers to those needs. After the directed research has begun, it is projected that the Cyber Forensic field will see a move toward being an accepted forensics science. Therefore, better tools could be developed, redundant work could be reduced significantly, researchers could engage in projects that help fix large-scale problems instead of localized issues, the law could finally start to catch up to cyber crime, and Cyber Forensic programs could be better equipped for preparing students for the challenges that will be found while practicing.

1.5. Scope

The scope of this project was limited to the United States Law Enforcement and Universities with a Cyber Forensic area of study. The State Police headquarters (HQ) were contacted for all 50 of the United States. This was the portion of the sample that pertained to Law Enforcement. Each police HQ was asked for contact(s) for their cyber forensics investigators, or the investigative company they use in the event they don't have one. In addition, they were asked for the contact of the lawyers that work with the cyber forensic investigators on their behalf. However, this did not amount to any additional participants as none of the law offices joined to the study.

The same was for academia. The universities that offered a Cyber Forensic area of study were contacted and asked if they would like to be involved in the study. Any participant could have provided contact information of additional individuals from the Cyber Forensic field they believed would like to participate in the study. These suggested participants were then contacted, either by phone or email, for recruitment.

Although the scope of this project seems broad, it was specifically chosen for the following reasons: These areas not only gave very different point of views of the field's issues, but they also contained the largest ranges of experience. These two factors provided the project with the opportunity to obtain a broader national view of the filed.

Many State Police Departments had different resources for conducting cyber crime investigations. The amount of time required to obtain participants from every resource was beyond the time constraints of the project. Therefore, one state police department's cyber investigators, whether internal or third party, was considered the sample for that particular state. As a result, the collection of samples from each state was the sample for the US Law Enforcement. The same philosophy was used for academia. There are many places to study that offer a cyber or computer forensic program. There are universities, local colleges, tech schools, training facilities, etc. As with the police departments, not every place can be questioned. From the list, universities were specifically targeted for this study because of one main reason: Universities are educating individuals in their area of choice; therefore, they offer a large range of experience spanning from the seasoned professors who instruct the classes to the beginners of the field, the students. This diversity of experience helped support a holistic view of the US's Cyber Forensic field. These large schools were considered samples of their surrounding places of study. Therefore, the collection of the universities represented the academia community.

The project boundaries could not incorporate every cyber investigator and training facility. However, as anyone or program outside the mentioned areas were still part of the community, and still affected by any national regulations or changes, the project did

allow for some flexibility in the boundaries. As stated, anyone that was recruited to participate in the study could suggest other Cyber Forensic investigators outside their unit for participation.

1.6. Definitions

All definitions were retrieved from Dictionary.com (dictionary.com, 2011).

- *Cyber Forensic Community* – anyone that practices, studies or performs research in the area pertaining to cyber forensics.
- *Cyber Forensics* – area of forensics pertaining to computers, other electronics, their communications, and how to extract specific information from such systems.
- *Descriptive Analysis* - An evaluation of acquired meta data in order to better describe the discovered results of the study.
- *Development* – anything specific to research dealing with the creating of new software forensic programs or implementation of standards, codes or regulations for forensic investigations.
- *Digital Evidence* – any data retrieved from a cyber investigation that is digital in nature.
- *DOJ* – Department of Justice
- *Drop Rate* - the number of people out of a sample size who don't fill out the questionnaire
- *External validity* – The degree of truth that a study can be generalized to make statements about a much larger population of subjects. Meaning, because this study is being conducted by specialists in the field, then it has a very high probability that it will be accurate and pertain to the Cyber Forensic Field

- *Frequency Analysis* – Evaluating and enumerating the number of times a given criteria occurred
- *Headquarters (HQ)* – location of main operations of a given group or organization.
- *NIJ* – National Institute of Justice
- *Reliability* - the degree in which the results would remain consistent over following retesting of the same subjects with the same questions.
- *Software* (AKA computer programs) – any program that is used to help with the retrieval process of digital evidence
- *Validity* – the degree to which the study's results mean what they aim to mean.

1.7. Delimitations

This section defines the delimitations of the study. The scope for the study's sample was limited to academia, state police departments and the attorney offices that represent the cyber forensic investigators of those police departments. Academia participants will include the professors of any cyber or computer forensic classes, students of the given program and any other cyber forensic investigator associated with the program. State policemen will include the individuals performing the cyber investigations and their supervisors. All participants must be 18 years of age and all three groups will be given the same questionnaires and survey.

Topics will focus on issues concerning the cyber forensic field as a whole. The official survey's questions will be close-ended and will not allow for any more additions of issues. Furthermore, participants will be asked to compare the cyber forensic field to a Daubert Test.

This research study is exploratory in nature and for the purpose of gathering data to be organized and distributed to the Cyber Forensic Community for use.

1.8. Limitations

This section defines the limitations of the study. As the questions were emailed to the participants, their timely completion of the questionnaires has the potential to be a limitation. In addition to the time limitation, past email questionnaires have a history of a response rate around 20%. Furthermore, there was no way to regulate or gage the amount of detail given for each open-ended question the participants answer.
Lastly, the entire Cyber Forensic community was not questioned for this study. Therefore, demographic and other participant specific data, from the final survey, was limited to the samples taken.

1.9. Assumptions

This section describes the aspects of the project that were believed to be true. It is assumed that all answers to the questions were 100% truthful, that participants took the time to contemplate and produce well-formed answers, that all questions were understood and the participants knew what each question was asking, and all participants were involved with Cyber Forensics through either Law, Law Enforcement, or Academia

1.10. Summary

This section was intended to describe the project as a whole and give details on the scope, significance, limitations, delimitations and assumptions. The purpose of this study was to discover the top issues plaguing the Cyber Forensic Field based on the opinions of those who were directly involved in the Cyber Forensic community, and

discover if there was any research and development being performed in order to address those issues. It was the hope of this project to confirm the issues and needs already identified from previous research, as well as, detail the reasoning of each issue and need, fill the gaps that previous research has left, and add any new items not yet listed. In addition to the confirmation and discovery of issues and needs, a list of current projects to help combat these issues were also created.

CHAPTER 2. LITERATURE REVEIW

If an individual were to investigate the issues and development needs of the Cyber Forensics field, he or she would find numerous articles of what authors believe to be the problems relative to the field. In these articles, many of the authors are discussing the same topics over and over again. They may speak about a different aspect of the issue but in the end, it is the same problem that needs to be addressed. However, after each article that is read, he or she will also find that many have the same ideas of what is wrong and how to fix them, yet the issues still remain. In addition, the research performed for the field thus far, (see Appendix B: Table of *Known Needs*) contained neglected areas where no one has spent the time to research, discuss or develop them. Though these issues exist, not everyone is aware of them because of various reasons; whether it be a lack of experience in the field or it appears to be too daunting of a task. Craiger et al. (2006) states another problem is relative to the analyst; "A good deal of forensic software is developed on a ad hoc basis, often by small labs or individuals, who recognize a need and provide a product to address it" (p. 93). Meaning, if an issue does not interfere with an analyst's work, there is no motivation to resolve it. This indicates that the problems being resolved are the symptoms of larger issues in the filed.

However, developing the field cannot happen over night, nor can it be done in one swift project, it will take many projects and many individuals. If the approach is to only fix the high level issues and not really focus on the underlining problem, the field will never catch up to today's technological crime wave. There are many who have begun narrowing down the issues in order to try to direct the field into better research and development. Appendix B: Table of *Known Needs* shows a list of examples of many papers written on certain criteria pertaining to needs in the field. Nonetheless, these are still collections of data focusing on one issue, or category of an issue. Some are even out of date, written back in 2004, nearly eight years ago. A national, three-series, multi-year research project conducted by ISTS at Dartmouth (Institute of Security Technology Studies at Dartmouth) evaluated the needs of Law Enforcement for investigations. This project ranged from September 2001 to December 2003 (Technical Analysis Group, 2004). It yielded three papers that helped identify issues Law Enforcement faced when investigating cyber attacks, a gap analysis of the identified issues, and a research agenda to help find solutions. Although very helpful in organizing research, it was eight plus years old. The last overview of the field before then was completed by the National Institute of Justice in 2001, nearly 10 years ago (Stambaugh, 2001) and it wasn't specifically targeted for Cyber Forensics. The technological world is developing too quickly for this data to be completely accurate anymore. Furthermore, the work being done today has a lot of overlap. Many different people are writing articles on the same issues, and as a result, they are still issues. Several articles referenced in this paper were written in the early 2000's where others were written more recently and they are discussing repetitively the same topics.

As shown in Appendix B: Table of *Known Needs*, there are many articles about the issues in the Cyber Forensic field. Each category has at least two different articles that mention or discuss the needs of the category. These articles are by no means the exhaustive list. Each category has many more papers that support that it is in need of improvement. For example, simply typing in "Digital Forensic Models" into Google will yield a plethora of articles written on that subject (www.google.com, 2010). Furthermore, this list is just a generalization of the needs at hand. Not every article that is written specifically says, "this needs to be improved". Multiple articles, from a multitude of different authors, all saying the "correct" way to do something proves that there is a need for improvement in that area. Evidence-gathering models, Crime Scene analysis, tool development, and certifications and standards are all examples of areas in need of improvement because they are not nationally defined or accepted. Anyone can choose to do it his or her own way. How many different models do we need? How many people need to say there needs to be a certification to ensure good and reliable work before it is created? How many bad tools need to be developed before a standard is put in place? The cyber forensic field needs results, not more opinions. There are no papers or articles that specifically say it, but the multiplicity of papers proves that there is redundant work being performed.

A few researchers have created the same type of study in the past, but were either specific to a category of needs, or the study was localized with a small sample size.

Liles and Rogers (2009) performed a study in which a diverse group ranked what given issues are the most dire to be resolved in the legal realm. This study's participants consisted of law enforcement, academia, government, industry and legal experts. This

study was performed as confirmation that the same issues found in Australia for legal issues were the same that could be found in the USA. Their paper referenced the *Brungs-Jamieson Survey* of 2005. In this survey, they gave participants a list of known issues and were asked to rank them in order of importance. The results yielded a percentage from the participants' opinions of what issues were most important. Although this was helpful, and made a good relation to the issues being the same in the US as overseas, it did not allow the participants to make comments, or add additional issues. What if the participant was dealing with a concern and knew it trumped all the other issues that were laid out for him or her? There would be no way to know. For example, Issue 17: Expert Witness Skills and Qualifications, does not elaborate on what specific skills and qualifications are in question. Is it the expert's ability to correctly extract evidence from a form of computer system, to follow the chain of custody, how they obtained their skills, how to perform well during examination/cross-examination, the knowledge on the forensic tools they are using, etc. Without detail, someone attempting to start research will still not know an exact issue or problem to target and work on. They would be trying to fix the entire field instead of the underlining issue.

Another example is Rogers and Seigfried's (2009) *The Future of Computer Forensics: A Needs Analysis Survey*. Their study helped addressed one of the problems with Brungs-Jamieson's survey. Participants in this study consisted of students, researchers, academia and private/public practitioners. They asked the participants to list what they believe to be the top five issues in the field from a dropdown menu list. This time, the topics were across the entire field instead of the just one aspect. Although it doesn't detail issues, it helps narrow down the most important areas to start concentration

of research and development. But it needs to go deeper. Where do we go from here? The same issue arises as in the above given example about expert witnesses.

In addition to giving insightful information about what general areas of the field have the highest need of improvement, the study also supported one of the underlining issues that overshadow all research so far, " The findings appear to indicate that there is a consensus regarding significant gaps or needs in the computer forensics discipline." (Rogers & Siegfried, 2009, p.15). This indicates that there research project are needed to take what they established further and deeper. This same research study went on to say, "Future research should sample a larger number of respondents, collect detailed demographics information and not only look at identifying issues, but also obtain feedback on methods for addressing these issues." (Rogers & Siegfried, 2009, p. 16). This kind of additional information will allow developers and researchers to more accurately attack specific issues, as well as have a broader view of the problem for future planning.

The National Institute of Justice (NIJ) performed a broad overview study, examining cyber crime in the nation. This study, started in 1998 and published in 2001, was able to create an overview understanding of what it would take to combat cyber crime. This was important, as cyber crime investigations had become a routine in law enforcement agencies (NIJ, 2001). It had become such an issue that the NIJ and the selected sections of the Department of Justice (DOJ), needed to assess the field to find out what was needed to combat such a rising issue. This study questioned those specifically working with cyber crime to discover the serious problems in the field. In addition, it explained why each issue was a problem and what aspect of each needed to be

addressed. The same can be said for Cyber Forensics. As Cyber Forensics continues to become more prevalent in today's society, it is a necessity to know where the issues lie so that solutions can be invented and established. Although the NIJ's study didn't specifically target Cyber Forensics, it does carry over, as cyber crime investigations will use Cyber Forensics. Some topics included tools development for cyber crime investigations, laws and regulations to help the investigators and enforcement keep up with the cyber crime population, and training / certifications on performing cyber forensics.

The previously discussed articles have shown that every paper has its usefulness and is relevant to the field. Nevertheless, they have their faults too. Many of these papers are over-viewing what needs to be addressed, but very few actually describe the exact need. Most of them, are not giving specific suggestions on how to address the issue. Furthermore, very few of the collection studies break down the results into fields of education, location, type of work and experience. None have broken down all three in a single paper. In addition, none have addressed issues of what was in development or planed for development. By knowing exactly what is being produced and developed, there is a greater chance for the field to grow substantially over the next few years. Specific issue targeted research and regional based work will be performed, as well as, a more cooperative working force will be created with a lack of redundant work plaguing the field.

Moreover, the individuals questioned for this research had their reasons for listing the issues collected. Why shouldn't they also be queried on suggestions on how to fix the issues? Or give opinions on how to improve already in-development projects or advance

"solutions" that are already in place? As technologies are constantly changing there is always room for improvement and expansion.

This research was performed in an effort to diminish the rework in the field. A goal of this study was the creation of a detailed list of needs and development projects for the field. There are many aspects of the field that are not mentioned in the Known Needs table and therefore, need to be examined. This will give everyone who reads it, a clear idea of where the Cyber Forensic field stands today and what is currently in development, so that individuals can either jump on board and work towards a common goal or start a new project concentrating on something that has not yet been addressed.

CHAPTER 3. METHODOLOGY

The goal of this study was to obtain a detailed list of top issues in the field based on the opinions of those who were directly involved in the Cyber Forensic community, as well as discover the research projects that were currently in development to address those issues. In order to obtain these opinions from across the spectrum of the field, a Delphi study was completed. This style of research was chosen because it is designed to send out more than one questionnaire, with the questions for the subsequent rounds based off the previous rounds. This study asked the participants to list the top issues they believe hinder the field as a whole, therefore, hindering them from performing their duty to the fullest. These opinions were collected and categorized and then released to the participants again for ranking and some additional questions. This is why a one-time survey could not be used and the Delphi method was chosen; the project required follow up questionnaires.

There are two main differences between a survey and a Delphi study. The first is that a survey is considered official research. A definition of a survey is the "formal or official examination of the particulars of something…" as defined by Dictionary.com (Dictionary.com, 2010). And given that surveys are official research avenues, Purdue University's Institution Review Board (IRB) requires all surveyors (researchers) to go through specific training before conducting official research (Purdue IRB, 2010).

A Delphi Study is defined as "a procedure for structuring a communication process among a group of experts to effectively deal with a complex question or problem, or reach consensus on a body of knowledge…" (Colton & Hatcher, n.d., p. 1). Meaning, that someone can collect data and ask questions of a group, whether it be a random selection or a targeted audience, in order to obtain some information, without the IRB's approval. The only down fall is that the information gathered would not be publishable. Thus, for this project, a Delphi Study was used in order to obtain the data to develop the questions to be asked in the official survey. This process, and the Delphi Study's definition, lends to the second difference between the two studies.

A Delphi study's process is done in iterations, more than one round of questioning, while a survey is designed to be given out once. For each of the rounds, the asked questions are based on the previous round's answers. So a Delphi study is essentially organized in the same fashion, with questions being asked of a sample, but it would be the equivalent of sending out multiple surveys. As mentioned above, these iterations were used for background work to develop the official survey that was sent out later. This was an attempt to ensure that the results consisted of the most in-depth and informed opinions that could be obtained.

Another similarity is the fact that the participants were not in close proximity. As surveys are usually mailed out or given to individuals as they go through a checkout line, such as those given on Wal-Mart receipts, the answers would be anonymous. This prevented others from influencing other's opinions; at least until the second round of questioning, when each participant was exposed to the other participant's answers. However, they were not told who submitted what. This also prevented groupthink and

confrontation. Groupthink often leads to faulty decisions because of group pressures; therefore, the issue at hand is not properly addressed. "…Confrontation, all too often induces the hasty formulation of preconceived notions, an inclination to close one's mind to novel ideas, a tendency to defend a stand once taken, or, alternatively a predisposition to be swayed by persuasively stated opinions of others." (Okoli & Pawlowski, 2003, p. 16). Neither of these are helpful in any way and would have greatly limited the amount of useful information retrieved from the study. This is because they could change how a participant really feels, therefore, invalidating the data. By conducting the study individually, groupthink and confrontation were eliminated.

For each round of the Delphi study, the answers to the questions were used to organize and develop the questions for the next round (Neill, 2007). This continued to be done until there was no need for additional rounds and it was believed that the participants had as much information as they needed in order to accurately list the top 10 issues in Cyber Forensics for each category that they themselves created. The number of rounds needed was two. The goal was to take a fine comb to the field's area of operations and list anything and everything that could be considered for improvement. Then from this list, the official survey was given to find the top issues for each category established and the top 10 issues overall. See Table 3.1 for the iterations used during the study.

Table 3.1: *Questionnaires Defined*

Questionnaires		Description and Goal
Delphi Iterations	Round 1	Discover issues and why they are a problem
	Round 2	Organize all responses and ask for opinions on the given issues from round 1 and previous research. Start categorizing answers.
	Round 3	*If needed:* further clarification of stated issues and grouping.
Official Survey		Top issues for each category, top 10 overall

The Delphi process is usually conducted in three phases: Phase 1 – brainstorming, Phase 2 – Narrowing Down and Phase 3 – Ranking (Okoli & Pawlowski, 2003). See Table 3.2 for an association of the project's iteration plan and the Delphi's phases.

Table 3.2: *Delphi Step Comparison*

Iteration	Phase	Description
Round 1	1 – Brainstorming	- Getting a list of issues. - Defining relative criteria
Round 2 and Round 3	2 – Narrowing Down	- Removing duplicates - Categorizing responses into like fields
Official Survey	3 – Ranking	Obtaining top issues for each category and top 10 overall

Although, the layout of the Delphi Study suited the needs of the study, it did have its limitations. Some of the issues that were raised are concerns about validity and reliability.

Validity is the proof that the study actually measures what it intends to measure. One of forms of validity used for this study was Face Validity. Face Validity means that the study appears to identify what it aims to discover. Experienced professionals that have conducted many research projects in Cyber Forensics evaluated the procedure for this study and found it be a sound approach. Also, past-published studies have used similar procedures to identify issues of a specific area. These past studies support the approach of this study to identify issues of the Cyber Forensic field. (See Appendix C for a table of these past studies)

There was also a strong sense of construct validity. Construct validity is the proof that the study will truly measure what it aims to. This study only included individuals that were engaged in the Cyber Forensic community. Therefore, their responses were developed from experience and real world situations. With the help of these individuals, obtaining a list of issues plaguing the Cyber Forensic community was accomplished.

Reliability is the proof that there is consistency of the results. Meaning, if this study was conducted again, the results would be the same. As technology changes, new programs are developed, issues are addressed, and new issues arise, the reliability of this project may seem low. To combat this, the study's results included past study's results that were looking for similar information. This allowed the study to see if progress has been made over the course of the last decade. Since high consistency was found between this study and past projects, it showed that the field has, indeed, performed redundant

work and accomplished little progress in its development as a forensic science. However, it was not 100% identical. Some new issues were discovered.

In order to organize the data retrieved from the study, frequency and descriptive analysis was performed. The frequency analysis showed what issues raised the most concerns and whether they were old or new. The descriptive analysis allowed for some correlations to be drawn between the participants, their opinions, types of electronic equipment, etc.

3.1. Participants (Sample) Defined

In order to obtain the detailed list of top issues in the field, participants for this study were volunteer expert, intermediate, and amateur investigators from the field. Historically, Delphi Studies are conducted with only experts in the field of interest (Neill, 2007; Cuhls, K, n.d.). Although, a Delphi Study can also be "characterized as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem" (Okoli & Pawlowski, 2003). This definition accurately describes this project's participant proposed sample; a pre-selected group of individuals. Using just experts was not done for this study because a full range of today's issues is required. Experts alone are not the only ones that have issues in the field; it spans from beginners just entering the field, to experienced veterans. Table 3.3 below describes the criteria for each type of investigator.

Table 3.3: *Participants Defined*

Type	Years in the field
Amateur	Student/Trainee – 2 years
Intermediate	3 – 9 years
Expert	10 - more

The investigator experience level ranges were the opinion of the research director and therefore, not affiliated to Purdue University or any other cited authors. Currently, the law considers an expert to be anyone who has "…knowledge, skill, experience, training, or education…" in the field (Cornell University Law School website, 2010). However, for this study, the amount of time spent in the field is what is believed to truly separate an expert investigator from an amateur investigator. Those with at least ten or more years of experience in the field were considered experts (Ericsson, 2006). The year lengths defined in Table 3.3 are believed to be appropriate time intervals for becoming an expert. This would have allowed for the data retrieved to be further narrowed down to exactly who needed what and the level of importance the particular issue had. However, defining a Cyber Forensic Expert was an aspect of the field that was identified as a major issue. The participants gave a large range of criteria for doing this and collectively decided that years of experience does not define an expert. So this predetermined break down of participants was not used.

As discussed previously, the questions for the second and third iteration were categorized based on the participant's responses. Furthermore, if the answers could be associated to a specific type of technology, it was again categorized within the previously mentioned areas. The types of technology were PC forensics, Mac (Apple) forensics,

Small Scale (PDAs, cell phones, iPods, etc), video game consoles and others. Since the range of participants, and area of which to obtain them was vast, time and efficiency was of most importance. Therefore, organization was key, as well as picking the correct method for obtaining the data.

The sample for this project was developed from a list of known contacts already established by professors and researchers from Purdue University's Cyber Forensic center. In addition, calls were made to police departments and the Attorney General's office for each state to try and recruit participants, as well as any college or university that offered a Cyber Forensic degree. After speaking to each potential participant, an official recruitment letter was sent to each contacted individual (refer to Appendix A.1). The letter detailed this study in its entirety, as well as laid out the rules and regulations defined by the Purdue IRB. In addition, a "thank you" and instructional letter accompanied each round of questions (refer to Appendix A.2-A.7). A total of 150 participants were needed. This number was calculated based on the hope that at least *one* individual would participate from every state police headquarters, every state attorney general's office, and at least 50 people from universities and colleges. (50 police + 50 lawyers + 50 academic individuals = 150). However, if more were acquired, it would only improved the results of the study. Also any participant could provide contact information of additional individuals from the Cyber Forensic field they believed would like to participate in the study. These suggested participants were then contacted, either by phone or email, for recruitment. However, only 85 individuals out of the intended 150 were actually recruited.

With such a large and diverse sample size, there were possibilities for biasing; one of the categories created from the participant's responses could have dominated the results. Although this may make the results seem one sided, it still generated a list of development needs of those who are truly involved in the field. This was not considered to be a negative attribute. There were more participants from the Midwest than any other US region. So the top selection lists could have been biased to the needs of the individuals from the Midwest. However, as mentioned above this was not considered negative. Their opinions still generated a list of top issues to address and will still help the majority of this study's participants.

3.2. Study Execution

Due to the size of the project, this study was conducted using email. There were several other venues that could have been taken, such as regular mail, website and interviews. However, as mail tends to take a long time and is a very slow process (Shin, n.d.), it was ruled out. Interviewing was also ruled out due to the time commitment it would require and is limited to local participants only. Email allowed for participants who are far distances from Purdue University to participate in the study.

A website based survey was initially ruled out because of the potential overhead, even though the questions would be readily available. Some of the issues included the design of a website, the programming of the data organization, and general website maintenance. In addition, a website survey would cost money for it to be hosted (Colton & Hatcher, n.d.). Last, the very nature of a website survey would allow for possible contamination due to non-cyber investigators answering the questions because the Internet is easily accessible to everyone. There are ways to avoid this, such as giving out

a password to a secured link but this would only increase the overhead of an online survey. Whereas with email surveys the participants could access it at any time, it was free, it was a controlled environment, and it allowed for follow-up questions if clarification was needed. However, due to the amount of work that was discovered during rounds one and two for sorting data and organizing the results, it was determined that a Purdue website survey service called Qualtics would significantly speed up the frequency analysis. This free service was used for the final round of this study. The survey was only accessible if a one had the link to the survey and the password to access it. This information was sent through email to the participants. This ensured that outside tampering was kept to a minimum. In addition, just as emailing allowed, the web-based survey allowed for tracking which participants had completed the study and who hadn't. Although it took significantly more time to create and set up, as was expected, it saved many hours of calculations and organizing that would have been done by hand through emails.

There was a potential setback in using email-based questionnaires: drop rate. Drop rate is the number of people out of a sample size who don't fill out the questionnaire. Email surveys have a history of low return percentage; somewhere in the 20% range (Kaplowitz, Hadlock, & Levine, 2004; Fraze, Hardin, Brashears, & Haygood, 2003). Therefore, the drop rate of email would be 80%. A study completed at Michigan State University compared mail versus email response rates to questionnaires. Their research showed that if only an email is sent, then a researcher can expect about a 21% response rate (Kaplowitz, Hadlock, & Levine, 2004). Another study completed by Texas Tech University showed that response rates to email surveys gave only a 27.37%

response rate (Fraze, Hardin, Brashears, & Haygood, 2003). For this project, a < 30% response rate was not be acceptable. Nevertheless, it was believed that this project would not fall into this category because of major differences between the examples above and this study; the participants were invested in the field, the study was conducted through email so reminder emails could be sent to those who had not yet completed the questionnaires, and the sample for this study was selectively chosen. Whereas, the aforementioned studies' samples were composed of randomly selected people. The Kaplowitz (2004) study emailed random students attending Michigan State and the Fraze (2003) study emailed all secondary agricultural instructors from the 2001-2002 school year.

The population for this project was selected from a specific classification of individuals, men and women, from the Cyber Forensic field; some of which already had a history of participating in past surveys. This aspect for participants almost doubled the response rate (Stephen, 2005; Cobanoglu, Warde, & Moreo, 2001). A study by the University of Alabama showed a 47.7% response rate with a population that was not a random selection or an entire group of people; their subjects were more strictly chosen (Stephen, 2005). The same trend was found in a study performed by Oklahoma State that received a raw 42% response rate (Cobanoglu, Warde, & Moreo, 2001). Oklahoma's study also had a more strictly chosen sample. Although, there tends to be a correlation between the response rate and the sample selection, it was not a proven fact for either; but an observation made while researching for this project. Nonetheless, they show a trend that gave a positive outlook for this project.

In addition, the study performed by Alabama State also stated that if the participants have a vested interest in the matter, then they are more likely to complete the questionnaire, increasing the response rate. As this project aimed to help direct the development of Cyber Forensics, and all the participants are directly affected by any changes to the field, the response rate should further increase. Lastly, a reminder follow-up email was sent out to those who failed to return the questionnaire after two weeks had passed.

Although the study was followed by a survey, the Delphi Study proved to be a very effective tool for gathering information in the past. Appendix C is a table of past successful Delphi Studies that were also looking for a list to help solve an issue.

Appendix C is just a small sample of many more successful Delphi Studies. These were examples of studies that were trying to gather a list of information; just as this project aimed to create. In addition to this table in its entirety (Okoli & Pawlowski, 2003), another table can be found containing specific graduate work utilizing the Delphi Study. This table can be found in *The Delphi Method for Graduate Research* (Skulmoski, Hartman, & Krahn, 2007)

Once the Delphi Study was completed, the survey was conducted. This was the official research so certain questions were added; such as demographics (geographic location), age, years working in the field, area of concentration, type of training, types of tools used during investigations, what types of electronic equipment is most often investigated by them, etc. In addition, questions surrounding the individuals learning method (training vs. education vs. self-taught) from which they got their start were also queried in the survey.

From these questions a great deal of information was discovered. Not only would the top lists help with organizing the field but the demographics, the years of training, education type, etc, is useful information and could be applicable to many other research projects.

Furthermore, the data collected, and resulting lists of top issues, would help direct academics and the rest of the field into better research and development toward solutions for the discovered issues this study identified. Once this happens, it was hoped that practitioners are able to perform their job more thoroughly, cyber crimes would become easier to track, and the field would become more standardized to help avoid unsanctioned data retrieval and investigations. This data will be readily available to the public in the hopes that others will use it in their efforts to start projects, begin research, acquire funding, etc.

CHAPTER 4. RESULTS

The final round of this study started on February 23rd, 2012 and was closed on March 20th, 2012. Out of the original 85 participants that agreed to participate in the full study, only 59 remained by the end. However, out of the 59 participants that started the final round, only 52 completed the survey in its entirety. Seven questionnaires were not completed before the deadline. At the cutoff date, the unfinished questionnaires were closed and the given answers were recorded. This yielded a 61% completion rate.

Past research discussed in the Methodology section suggested that the response rate should have been expected to be between 20% and 40%, with high emphasis on the low 20% range. It was predicted that since the participants were contacted a head of time, that the research pertained to them specifically, and that they had an interest in the topic area, it would significantly raise the response rate for this study. As the completion rate was 61% it showed an increase from the expected response rate of 40%. It is believed that the rate would have been higher if the study did not include three rounds and was not over the course of 6 months.

In order to answer the research question for this study, descriptive analysis was performed on the discovered results. The frequency of choices will indicate how items were selected and ordered.

To stay in accordance with Purdue IRB, participants were not required to answer every question. If they felt uncomfortable answering a question, they were allowed to skip it. Therefore, not every analysis will be evaluated on the 59 recorded participants, but rather the total number of the 59 participants that answered the specific question. Each table and frequency analysis from this point forward will provide the total number of participants that the percentages were calculated from.

It is also important to note that the "Law" category of this study was dropped due to the amount of time it took to contact and recruit the lawyers to participate. After three weeks of recruiting for this group, not one law office returned a phone call or responded to an email. Therefore the Law side of Cyber Forensics was dropped from the study and is not included in any of the result numbers. The only impact this had on the study was it narrowed the scope of the project. Instead of having issues identified from Law Enforcement, Academia and Court Law, it would only focused on the first two areas. Dropping the Law side does not discount or lessen the importance of the discovered results in any way.

4.1. Participants

Out of the 50 States, only 14 Law Enforcement agencies (14 different states) agreed to participate in the study. The main reason for an agency to not participate was due to a lack of time. Many of the agencies indicated interest in participating but could not spare the time due to an overwhelming number of caseloads. In additional, several agencies did not want to be associated with the research for fear of some repercussion for their opinions. Even though it was made clear that it was an anonymous study, shy of the

demographics, they were still not comfortable. Some agencies simply did not respond back after several attempts to contact them.

As for the Academia side, 14 academic programs from 12 different states agreed to participate. As was a similar case with Law Enforcement, time was an issue. In addition, several academic programs did not participate, as the head for the program did not think it would be beneficial. Last, just as with the Law Enforcement agencies, some simply never made contact.

Table 4.1 breaks down the participants into categories as to show the diversity of the subjects for this study. The participants are split into their associative US regions, then by their age, gender, and then by their classification for this study: Academia or Law Enforcement.

The frequency number indicates the number of occurrences, or votes, that a specific item had. The corresponding percentage represents the fraction of the total number of participants who answered the question associated to the data.

Table 4.1: *Demographic of the Participants*

Category	Criteria	Frequency (Percentage)
US Regions	Northeast	9 (16%)
	Mid-West	33 (58%)
	Southeast	13 (23%)
	Southwest	1 (2%)
	West	1 (2%)
	Total	57 (100%)
Age Ranges (Years)	18-25	7 (12%)
	26-33	14 (25%)
	34-41	14 (25%)
	42-49	7 (12%)
	50-57	9 (16%)
	58 or older	6 (11%)
	Total	57 (100%)
Gender	Male	46 (79%)
	Female	12 (21%)
	Total	58 (100)
Classification	Academic	31 (53%)
	Law Enforcement	27 (47%)
	Total	58 (100)

Note: US Regions' total calculations are slightly off due to rounding.

Table 4.1 shows the majority of the individuals in this study are from the Mid-West. Though this could be viewed as a biased to the Mid-west, it will not be considered as such for this study. The main focus of this study was to discover issues in the Cyber Forensic field regardless of location. An issue is still an issue whether it is in Maine or California.

In Table 4.1, the research shows that 50% of Law Enforcement examiners and students of Cyber Forensics ranged in age from 26 – 41 years. This shows that the

participants are from a younger generation. As they continue to grow in the field, they can use the data presented in this document as a guide to help develop it.

When comparing the gender of the participants, the results were as expected with a higher population of men to women. Table 4.1 shows that 46 (79%) of all participants were male. This does not change the results, nor influence the discussions.

For the classification, Only 58 of the 59 participants felt comfortable with identifying themselves as Academic or Law Enforcement. The results were very close with 31 Academics to 27 Law Enforcement participants. An Academic is anyone still in school studying Cyber Forensics, anyone who is employed by a university or teaches at one regularly. In order to fall into the Law Enforcement category, a participant must be employed by a US Law Enforcement agency working in Cyber Forensics. If a participant was involved with both sides, they were required to pick the side they felt they were more involved.

Lastly, classifying issues based on experience and education of the participants was not done due to issues with the results from the "experience" questions (which will be described in the Cyber Forensic Expert section to come) and issues with the "education" questions' design. The results collected for the "education" questions were recorded in such a way that they could not be categorized; therefore, drilling down issues based on those results was not feasible.

4.2. Issues in the Field (No grouping)

The results in this section will cover the main issues in the field of Cyber Forensics. These issues will include problems with funding, the general public, cyber

forensic labs, the field as a whole, tools, certifications, the law, technology, and training. For each question the results are displayed as a straight frequency analysis for that question and were not categorized otherwise. These are the top issues based on the opinions of the participants regardless of age, gender, or categorization. Each table focuses on a single question from the study. The frequency of the chosen answer is also included in actual number and percentage form. The results are displayed in descending order. Also, the original design of the study indicated a top 10 list of all the issues and top 5 issue lists for each category created. After the collection of data, it was discovered that some categories had a very small number of issues listed and some had many. Therefore, based on the number of responses each question received, the top number was determined. There will be lists of top 3, top 5, top 10 and in some cases the top 1 choice.

The focus of this study was to identify the issues in Cyber Forensics to help direct research and development. The goal was to create a top ten list of the most important issues the field is facing. Table D1 in Appendix D contains all the received issues from the participants during the study. From this list, the participants were to vote for the top ten issues in the field. Table 4.2 below shows the results of their selections. However, the resulting table has 11 items instead of only 10. The reason for this was because the last 3 available slots in the top ten list were to be filled by a tie between 4 items all receiving 25% of the votes. It could not be determined which of the three out of the four issues were more important to the participants. Therefore, an 11^{th} item was added to the top ten list.

Table 4.2*: Top 10 Issues Overall*

Answer	Frequency / Percentage (Total 53)
No official / accepted certifications to qualify an individual (cyber forensic analyst or not) as a cyber forensic expert	18 (34%)
Lack of funding for Training	17 (32%)
Courts, in general, are behind in knowledge for Cyber Forensic cases.	16 (30%)
Technology is constantly changing (will the old tools still work, are there any issues, does it still protect the data, etc)	15 (28%)
Ever increasing storage space	15 (28%)
Encryption for devices preventing forensic examination (examples, AES and quantum)	14 (26%)
No official characteristics or criteria that defines a Cyber Forensic Expert (everyone's definition is different)	14 (26%)
There is a knowledge gap between practitioners and courts within technology and how it operates.	13 (25%)
Lack of funding for new equipment and Software	13 (25%)
The use of "Click Button" analysts (examiners don't know the programs or their processes; they just click a button and report the results)	13 (25%)
Continuous Training (technology constantly changes = constant education of tools, equipment, and computer functions are needed)	13 (25%)

Figure 4.1 below shows a graphical representation of the top issues in the field, organized from the most popular (34%) to the least (25%).

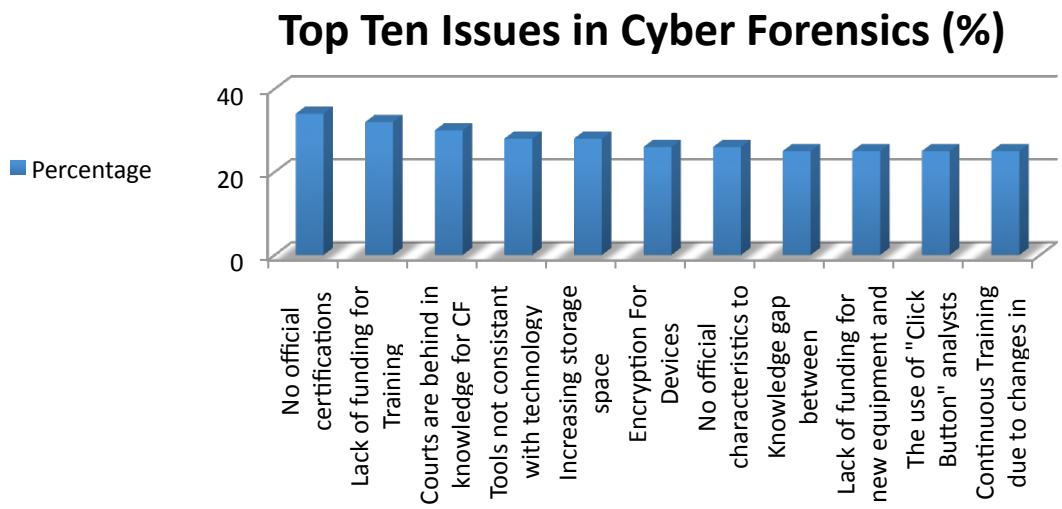

Figure 4.1: *Top 10 Issues in Cyber Forensics*

Many of these issues had follow up questions to further describe the reasons for the issue. Examples include, issues in funding, detailing Cyber Forensic Experts, issues with training, and clarifying certifications. These are just a few examples of the plethora of exploratory data that was recovered during the study. Some of the important issues will be discussed in forthcoming sections as these were hot topics in the field and are vital to its future progress. To view all the different sub questions and their responses see Tables D2-D7 in Appendix D. The tables follow the same design as described at the beginning of this section.

One important area to discuss is funding. Funding issues were identified throughout both rounds one and two. In the final round two questions were designed to narrow down the problems; what is impacted the most by a lack of funding and what is

the reason for the lack of funding. Table 4.3: *Funding Issues* contains the two questions and their analysis.

Table 4.3: *Funding Issues*

Question	Answer	Frequency (out of)	Percentage (%)
Select the area that is most impacted by a lack of funding	Training	20 (57)	35%
Select the top cause for a lack of funding	Available funds	34 (56)	61%

Note: The second entry was a follow-up to the first. This is why they are not listed descending order.

Training was ranked the highest with 20 votes (35%) out of the 57 respondents for this question. The main reason for the lack of funding for this area is due to a lack of available funds, 34 votes (61%). To see a complete breakdown of the areas impacted by funding see Table D8 in Appendix D.

The reason for a lack of funding may seem obvious, however, the alternative choice was "Upper management does not understand the complexities of Cyber Forensics, therefore it is hard to get them to buy into funding for more training, expansion, and tools."; which received the remaining 39% of the votes. Even though this choice was not selected, it was important to reveal the competing choice to prove there was no obvious answer.

4.3. Research Projects

Table 4.4 specifically answers the second half of the research question: "what research projects are currently in development." The question generated enough

responses that another top 10 list was created. This table contains the research projects that are believed to be the most impactful research projects at the time of the questionnaire. Nonetheless, many other potentially useful projects are in development. Even though they did not make the top ten list it is important they be included in this study. See Table E1 in Appendix E for a complete list of all identified research projects

Table 4.4*: Top 10 Research Projects in Progress*

Answer	Frequency / Percentage (Total 51)
Course on Mobile Device Forensics (This will combine mobile devices as well as network service provider data. There will be significant number of hands-on activities with current, state of the art tools.)	40 (78%)
Cloud Computing investigation models, tools, and methods	39 (76%)
On-site forensics and training on computer triages to increase proficiency in data extraction and time requirements.	37 (73%)
Course development on virtual/cloud-based forensics	37 (73%)
A Cell phone analysis application to interpret cell phone data-dump-report files by parsing them and providing the investigator with frequency results.	35 (69%)
Creating an information repository for cyber forensics (to be included is research conducted and published, current research in development, communication avenues for experts and analysts, info on issues in the field for possible new research topics, etc)	31 (61%)

Table 4.4 Continued.

Developing free online training modules for Law Enforcement	31 (61%)
Smart phones and pass lock options for analysis	28 (55%)
Curriculum development for a 4 year degree in CF	24 (47%)
Focusing on the legal and policy issues confronting cyber forensics and the gap that exists between what the several stakeholder groups hold to be best practice / highest need and what is actually being practiced	23 (45%)

Figure 4.2 below shows a graphical representation of the top issues in the field, organized from the most popular (78%) to the least (45%).

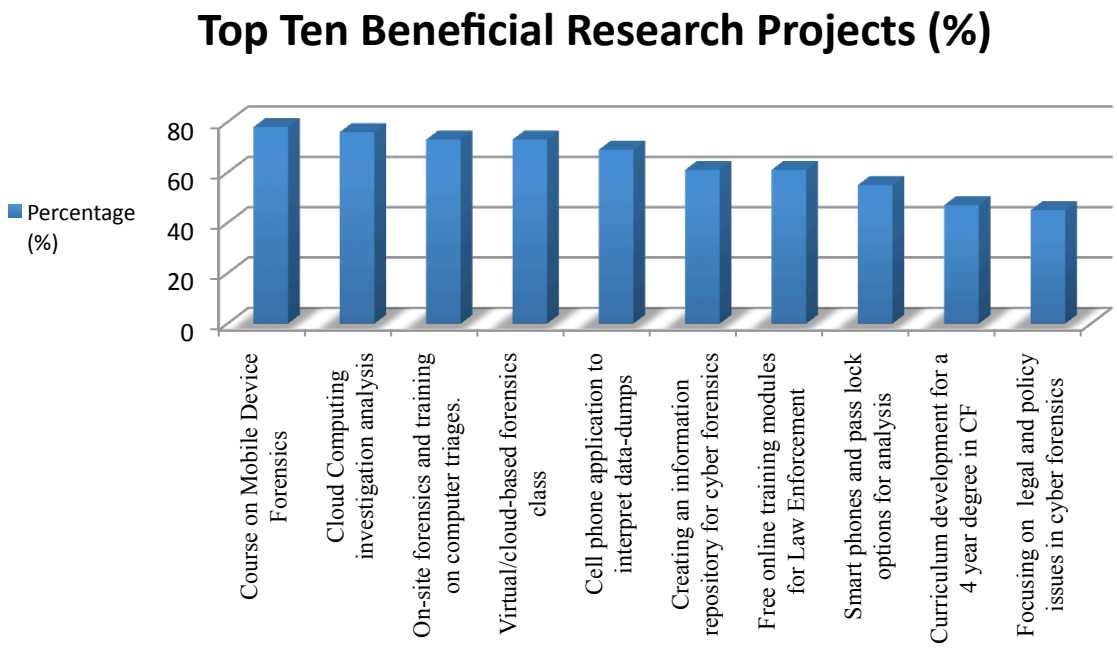

Figure 4.2: *Top 10 Research Projects*

4.4. Daubert Test

The participants were asked to comment on an existing evaluation test for scientific communities: the Dauber Test. A science, procedure or witness is often subjected to this test to ensure it is acceptable for a court of law.

The Daubert test compares against the following criteria:

--- Empirical Testing: technique or theory must be testable and refutable

--- The science or procedure must be subject to peer review

--- Potential error rates must be known

--- Standards and controls concerning its operation must be established

--- The theory or technique must be generally accepted by the relevant scientific community

Participants were then asked if the Cyber Forensic field as a whole could withstand this test. The results were surprising. Out of the 51 respondents, 32 (63%) felt that the field would *not* fail a Dauber Test Comparison. Of the 19 (37%) respondents that voted that it would fail, 18 responded to the follow-up question, which was to identify the area that the field would fail in. Table 4.5 displays the results of which areas are most likely the cause of the theoretical failure.

Table 4.5*:Voting Percentage for Failing the Daubert Test*

Criteria	Frequency / Percentage (Total 18)
Potential error rates must be known	16 (89%)
Standards and controls concerning its operation must be established	13 (72%)
Empirical Testing: technique or theory must be testable and refutable	3 (17%)
The field and its practices must be subject to peer review	3 (17%)
The theory or technique must be generally accepted by the relevant scientific community.	3 (17%)

4.5. Cyber Forensic Experts

Table 4.6 shows what the participants considered as a way to indentify someone as a Cyber Forensic Expert. This list does not imply that an expert should have everything on this list before being considered as such; but rather shows what the participants evaluated when considering an individual an expert.

Table 4.6*: Cyber Forensic Expert Identification Criteria*

Selection	Frequency / Percentage (Total 51)
Experience	38 (75%)
Training	31 (61%)
Education	23 (45%)
Peer reviewed and accepted	15 (28%)
Functional expertise is required (Cyber Forensic Experts must be competent to operate in a specific area (Law Enforcement, Info Sec, e-Discovery, etc.))	18 (35%)
Certification	16 (31%)
Federal Rules of Evidence definition of expert	10 (20%)
Active member in Cyber Forensic activities outside of employment (conferences, clubs, societies, associations, etc)	5 (10%)
Active in research and development to promote and advance the field (through associated groups or self research)	4 (8%)
Indefinable (No one can be an "expert" as technology changes too fast and there is too much of it)	3 (6%)
Involved with research (conducted and published)	3 (6%)

"Experience" was ranked at the top of the list with 75% of participants selecting this as a criterion for Cyber Forensic Experts. Figure 3 below displays the same data in a more visual summation.

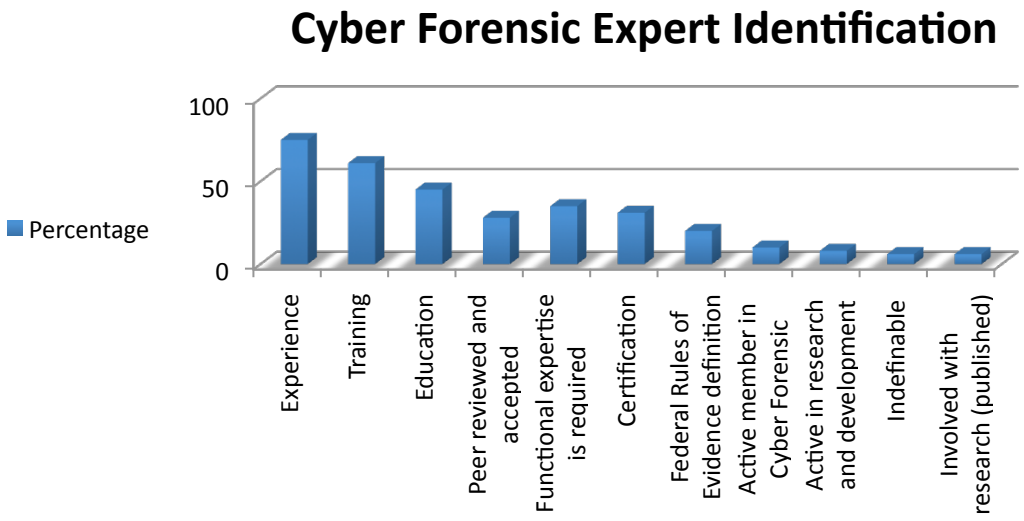

Figure 3: *Cyber Forensic Expert Identification*

During rounds one and two of the study, several of the characteristics mentioned in the previous table were identified with vague or inconsistent answers. Those responses included: not specifying the number of years an expert should have for experience, the certifications that were required, the kind of training, and level of education. Table 4.7 contains the responses to the clarification questions. Each criterion was part of a separate question, which is being displayed in one table for quick review and summation. Table 4.7: *Defined Cyber Forensic Expert Criteria* is the minimum of what the participants thought a Cyber Forensic Expert should have in order to be considered as such.

Table 4.7*: Defined Cyber Forensic Expert Criteria*

Criteria Type	Answer	Frequency (out of)	Percentage (%)
Years of Experience	None - (number of years is irrelevant, it should be based on the kind and how much experience is gained, not length of time)	27 (52)	52%
Required Certificates	Association certifications (examples: IACIS's CFCE, NW3C's BDRA , FBI's CART, or similar)	18 (48)	38%
Required Training	100 or more hours of training and/or apprenticeship to prove efficiency	16 (48)	33%
Education	Specific degree is not needed (it is what is taught and the knowledge gained during a degree that matters; whether it be a certificate, associates or PhD)	18 (51)	35%

Lastly, *Above Average Knowledge* was another vague characteristic of Cyber Forensic Experts that was mentioned multiple times during round one. In round two the participants were asked to clarify what was meant by “above average”. This yielded a

large number of responses that needed to be ranked. On the final round, participants were asked to select the top 5 aspects of Cyber Forensics that they thought were the most important for a Cyber Forensic Expert to be "above average" in. The top ranked criteria was "Knowledge must be beyond "click-button forensics (know how and why digital evidence is present)" with 43 (84%) votes out of 51. For the complete list, see Table F1 in Appendix F.

There were three other choices that received no votes:

- High Score in aptitude testing
- Must be a federal agent
- Must be a professor of Cyber Forensics

As none of these received a vote it was assumed that it was not a popular choice and that the participants that originally claimed these as an identifier were also ones that did not complete the final round.

For further clarification, another question was asked to identify the top three types of experience a Cyber Forensic Expert should have. These focused on the level of knowledge an individual would have on the field and in practicing. For these results See Table F2 in Appendix F.

During rounds one and two the issue of "a lack of qualified professionals to teach in the field" was identified. As this issue resulted in more vague responses, it required clarifying. Table F3 in Appendix F gives the top five reasons that the participants believe this issue exists.

4.6. Academic Only

This section focuses on the Academia side of this study only. During rounds one and two, there were several items that were identified as issues for Academia only. During the final round, only those that identified themselves as an Academic were allowed to contribute to ranking these identified issues. A total of 31 participants were classified as Academics.

Table G1 in Appendix G lists the top 10 issues related only to academics in Cyber Forensics. These issues were identified as items that contributed to restricting their ability to effectively learn the science. For a complete listing of all the identified issues, see Table G2 in Appendix G.

In addition to these issues, the number of years the respondents studied the field and their education level were also recorded. See Tables G3 and G4 in Appendix G for the breakdown of this information.

4.7. Law Enforcement Only

This section focuses on the Law Enforcement side of this study only. During rounds one and two, there were several items that were identified as issues for Law Enforcement only. During the final round, only those that identified themselves as a member of Law Enforcement were allowed to contribute to ranking these identified issues. A total of 27 participants were classified as Law Enforcement.

Table 4.8 is a list of the top three issues related to only Law Enforcement in Cyber Forensics. These issues were identified as factors that contributed to restricting

investigator's ability to maximize their efforts during examinations. To see the complete list of the identified issues for Law Enforcement, see Table H1 in Appendix H.

Table 4.8*: Top 3 Issues for Law Enforcement in Cyber Forensics*

Answer	Frequency / Percentage (Total 51)
Cost Effective tools for Law Enforcement	18 (69%)
Lack of manpower (more work than people)	16 (62%)
Overwhelming case workload (too much, stresses the examiner out)	13 (50%)

Figure 4.2 below shows a graphical representation of the top issues in the field, organized from the most popular (69%) to the least (50%).

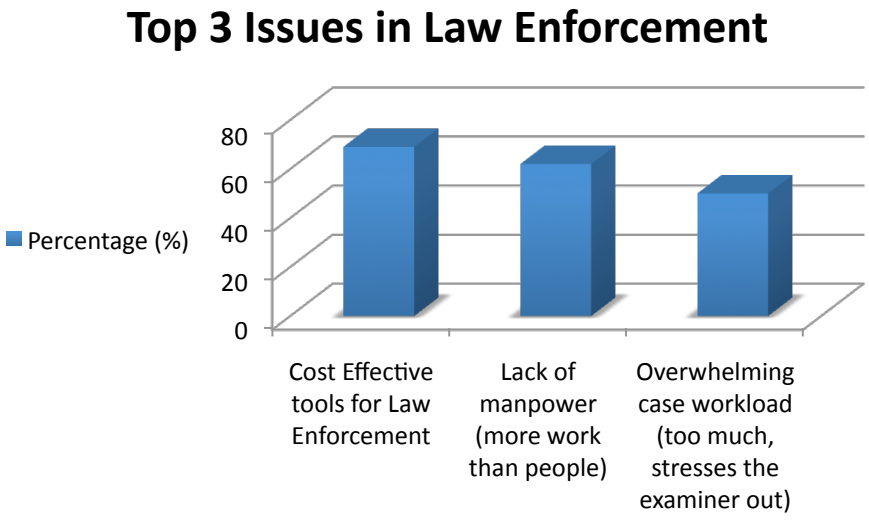

Figure 4.3: *Top 3 Issues in Law Enforcement*

The top issues for Law Enforcement consist of issues about tools and workload. To supplement this information, Law Enforcement participants were asked to list the

software they use for investigations and the systems they analyze. The respondents also indicated what systems they spend the majority of their time analyzing as Law Enforcement analysts investigate a range of systems. However, 26 (100%) of respondents said they spend the majority of their time on Windows machines. In addition, 8 (32%) participants selected a second item as their "Majority", which was identified as cell phones. Both Mac and PDAs received one vote for their secondary "Majority". To see the breakdown of systems evaluated and their evaluated time ranking, see Tables H2 and H3 in Appendix H.

Additional supplemental information was collected which included: the number of years the participants were practicing, certificates held, team vs. sole investigator comparison, and the education of the investigators. See Tables H4 – H11 in Appendix H for this information.

CHAPTER 5. DISCUSSION

This study aimed to discover the top issues in the field in order to help direct the development of it. In addition, it is aimed to discover the current research projects that were currently in development to supplement the issues list. This would help in preventing rework from being conducted by showing what issues were currently being addressed. The overview of issues and top lists gave a detailed picture of what is needed in the field of Cyber Forensics. This study was mostly directed for academics, third party companies, and R&D organizations that spend time to conduct research. However, Law Enforcement utilizes the projects that the academics and organizations develop, so it was vital to know what they felt were needs.

The results discovered in this study showed consistency with many of the issues that were previously mentioned in the literature review. Table 5.1: *Issue Comparison* shows that many of the issues identified in past issues, still exist today. This is just a partial listing of issues that were identified both past and present.

Table 5.1: *Issue Comparison*

Past Issues	Present issues
Tools (development, usefulness, accountability, metrics, etc)	• Error rates for tools used are not defined to document reliability. • Ambiguity (All the tools are doing the same thing different ways) • Tools are not keeping up with changing technology.
Certifications / Standardization	• There are no non-vender certifications to identify that a person has the qualifications required to be a Cyber Forensic Investigator. • No official / accepted certifications to qualify an individual (cyber forensic analyst or not) as a cyber forensic expert • Current vender certificates are easy to obtain. They should be more difficult (think Cisco certified).
Law (rights, search and seizure, expert witness, guidelines, etc)	• Politicians pass laws without prior knowledge of the field and how it will affect the cyber investigative process.
Training	• On-site forensics and training on computer triages to increase proficiency in data extraction and time requirements. • Lack of funding for Training
Evidence gathering (Procedure models)	• Cloud Computing investigation models, tools, and methods • There are no models or frameworks for conducting investigations. (There should be a model/framework for each type of investigation...computers, hand-helds, consoles, phones, etc)

Since many of the same issues that exist today were discussed in research projects that were conducted a few years ago, the study proves that the field is moving forward at a very slow pace. This research not only confirmed the results of past issues, but also created a more extensive list from across the field and organized lists of the top issues to aid researchers in knowing where to focus their research during the coming years of development.

Although demographics were taken, they were not specifically used to categorize or influence the results of the data. They were taken to show there was diversity in the participants and that not all the responses were from members of a single team. Although the results showed a concentration to the mid-west, it was not intended. Drilling down the responses to questions based on geographic location was not needed for this study nor was it a focus. For example, a discovered issue in California has no more weight than issues in Maine. All issues presented should have an equal chance to be selected for evaluation and the top lists regardless of who presented the issue or where it originated. This helps prevent the misrepresentation of data. Another step to prevent the manipulation of the results was to keep the participants anonymous. This prevented any kind of knowledge of the participants from influencing the answers to the questions. The issues that rose to the top did so by simple voting from across all participants.

Biases can still be conceived. Any respondent could have chosen their own answers during the questions without truly considering the other identified issues. Or if a single Cyber Forensic department had several members participating they could all vote on the same issues, pushing their ideas to the top. This would create a higher response rate compared to the other regions. Nonetheless, if either of these events were discovered

to be true, it would not be considered completely negative. The study aimed to generate a list of issues to fight the shortcomings of the field. This was accomplished. The top lists give some direction to the overwhelming number of issues that should try to be tackled first. Nevertheless, they are by no means golden lists, nor are they 100% complete. It is important to acknowledge that the issues discovered for this paper are a snapshot in time. It is feasible that new issues have arisen and issues resolved during the short time this paper was being written.

Also, just because some issues did not make it to the top of the list, their significance or impact on the field has not been diminished; they are still important issues none-the-less and need to be addressed. For example, if one were building a traffic intersection, and the traffic signal was voted as the most important part of the intersection, does that make the painted lines on the road less important? No. All it does it put an item in a list ahead of another, but it still needs to be addressed. Another analogy, during house construction, is the footer any more important than the walls that hold up the roof? No. Both need to be addressed, but one goes before the other. It does not diminish its importance, nor disregard its usefulness.

In academia, the results will give the new-coming students an overview of what is occurring in the field, as well as detailed information of where it is weak. However, it is important to note that some of the issues identified in the top lists are issues that cannot be fixed with a single research project. Does that mean it should be discarded? No. It just means that a Master's student shouldn't try to tackle that issue for their thesis. This study aimed to help direct incoming researchers to address the known issues in the field

regardless of where the motivation for the research originates. There is something for everyone to work on.

Another goal of this research was to help prevent redundant work from being conducted. Therefore, all the issues must be listed so future researches will have a much more detailed view of the field. Appendix D Table H1 has a complete list of issues that were identified during rounds one and two of the Delphi study. If the top lists do not spark an interest to research an issue, than hopefully the extended list will.

Lastly, Table 3.3 in the methodology section identified year cut-offs to classify the participants as Amateur, Intermediate, or Expert. This was originally intended to break down the responses of the participants into categories based on their experience. However, this was not done, as "defining experts" was a major point of disagreement during this study; every participant had their own definition. Since this turned out to be an issue in itself, it was decided not to categorize issues based on years of experience. Categorizing issues based on controversial criteria would not add any validity to the research, but rather cause possible rejection of the categorization.

5.1. Funding

Gaining funding for anything is always an issue. Which is why it is important to see where the funds are wanted the most. The results from this study, in Table 5.1 below, show that Training (35%) is impacted the most due to a lack funding, but it is important to see how the other areas ranked in comparison. It was surprising to see that "Equipment and Software" (25%) was ranked lower than "Training" as labs, schools, and

analysts are always trying to keep software updated and/or using out-of-date equipment: an issue that was identified in the exploratory rounds of the Delphi study.

Funding for research projects (21%) fell even further and was expected to be towards the top. As a graduate student, maintaining funding has been a point of conflict over the past couple years; and there are many other types of these cases.

Last in the list was funding for new hires with 19% of the votes. This was not a surprising outcome. In section 4.1 it stated that one of the main reasons for an agency not to participate was because of a lack of time. The agencies that did participate were able to spare the time to complete the study, therefore, it can be speculated that they were not overwhelmed with casework and did not need additional personnel to lessen the load.

However, as new technology arises, new software is developed, and new techniques are discovered, all analysts need to be taught how to function with these new aspects of the field. Lending well to the fact that training is required throughout ones career, where research projects come and go, and equipment can last long periods of time.

5.2. Research Projects Discussion

One of the issues identified in the literature review was that redundant work is being conducted. Projects are reworking old projects and not furthering the field. In addition, the same research projects are being conducted in different places. This is mostly in part due to the fact that there is no communication within the Cyber Forensic

community; no one knows what research projects are currently in development or in progress.

In order to partially address this issue, the participants were asked to list any research projects they were currently working on. Hopefully, this information can help reduce the amount of redundant work being conducted, as future researchers will have a list to reference to ensure their efforts are not wasted.

5.3. Dauber Test Discussion

It was surprising to see that the majority of the participants agreed that the Cyber Forensic Field would pass a Daubert Test Comparison. A couple of criterions that a Daubert Test compares against are in direct relation with issues in the field. In Table 4.2 *Top 10 Issues Overall* the number one issue identified in Cyber Forensics was a lack certification to identify Cyber Forensic Experts. Which has a direct relation with the number two reason that the field will fail this test, "standards and controls concerning its operation must be established".

Other issues were identified during the discovery phase that did not make the top ten list, but still contradicts the assessment that the field would pass. To name a few of these issues:

- Error rates for tools used are not defined to document reliability
- There are no standards for practicing (only best practices and personal preferences)

- There are no models or frameworks for conducting investigations. (There should be a model/framework for each type of investigation...computers, hand-helds, consoles, phones, etc)

Theses issues, and many others, show that there is a disconnect between the issues listed and how they compare to the Daubert Test criteria. The reasons for this cannot be explained from the research. It was speculated that one reason for this was because the field has not yet failed the test and it is constantly being used for crime investigations. Another reason was the participants do not believe the issues identified fall into the same categories as the Daubert Test criteria.

5.4. Cyber Forensic Experts and Certifications

This part of the research was met with a significant increase of vague responses that needed to be clarified; more so than the rest of the study. The main reason for this was that there are no official standards for identifying an expert, therefore, 51 different answers were given in response to this question. The diversity of descriptions on what "should be used" to identify an expert shows that it is completely based on individual opinion.

The federal court has a simple way of identifying an expert witness with the Federal Rules of Evidence (Cornell University Law School, 2010), but there is nothing that specifically identifies a Cyber Forensic specialist. This is a major issue as technology continues to grow and be utilized. More and more crimes are committed online and the bad guys are learning to hide their tracks better. It is imperative that the investigators have the skill set required to track the criminals or exonerate the innocent.

Practitioner's certifications were among the issues identified as a top issue to be addressed for Cyber Forensic Experts. Many certificates exist for specific skill sets, certain tools, and training completion, but it is not enough. A national standard needs to be implemented to ensure reliable Cyber Forensic Experts.

The current certifications give an overview of what skill sets are currently held in high regard for forensic examinations, what tools are most commonly used, and what scenarios to prepare for. Therefore, they arrange a starting point for developing accredited certifications that are nationally recognized. A national standard would give more focus to the kind of skills that are required to conduct Cyber Forensic Investigations. In addition, the same research for developing the national standard could lead the way to further development in tools to compensate for the gaps in skill sets and to make the investigator's work easier.

Lawyers, forensic (non cyber) examiners, police officers, and doctors all have to past nationally recognized tests before they can even begin to practice their profession. The same should be true for Cyber Forensic Experts. In order to be considered as such, an individual should have to prove that they are competent to complete the tasks. This can be done through certification or through schooling.

Today, many of the certifications that pertain to Cyber Forensic specialists do not press an individual to truly assess their knowledge base. These kinds of certificates do not help the field progress, but rather dilutes its status as a science to be taken seriously. They often focus on more "click-button" forensics and not a skill set and knowledge base.

Cisco has a certification system of ensuring that if people claim to be Cisco equipment experts, they have a way to prove it. Certifications for Cyber Forensics should look at the Cisco certification process in order to really establish experts in the field.

As mentioned, some certificates do exist that are held in higher regard, but they are still not an official test. If an individual wants to be a pilot, they need their pilot's license. Although the actual schooling may be different from organization to organization, the skill set and knowledge gained will be the same. Everyone knows what it means to have this license; there is a level of confidence and trust automatically given to those who possess it. This is the kind of evaluation the Cyber Forensics community needs to have; where the skill set and knowledge of the examiner has already been proven before their first case. (Which could also be the way professors are evaluated before teaching their first class in Cyber Forensics.)

To support this mindset, a follow-up question to the Cyber Forensic Criteria questions was given. Participants were asked to consider themselves as a hiring manager and take into account the criteria established for identifying a Cyber Forensic analyst as an expert. Then, they were asked to identify which criteria they held in the highest regard. 37 out of 51 (73%) participants that responded said that job experience was the most important; more important than training and education. Certifications were held in the least amount of regard as not 1 vote was casted for this criterion. (See Table F4 in Appendix F for the break down of the hiring manager question)

However, there was *some* support for the current certifications. In Table 4.6: *Cyber Forensic Expert Identification Criteria*, certificates were ranked 6th with 16 (31%)

votes. This completely contradicts that result from the hiring manage question as certificates did not receive one vote.

As this kind of outcome was not predicted, there was not enough time to re-question the participants to try to make this clear. Nonetheless, this contradiction supports that there are no official ways to identify a Cyber Forensic Expert, nor official testing to prove that an analyst has the skills and knowledge to be deemed as such.

As previously mentioned, the participants were asked to identify the criteria they thought would define a Cyber Forensic Expert. This led to many vague answers and required a clarification question, which yielded the results in Table 4.7: *Defined Cyber Forensic Expert Criteria* in Chapter 4.

Some aspects of the identified criteria are important to discuss. For example, the years of experience required before being defined as a Cyber Forensic Expert was voted to be "none" (52%, 27 votes from 52) as the amount doesn't matter, only the type of experienced gained from it. Someone who worked for an organization for 10 years but only worked on a case once every 6 months would not have the same skill set or level of knowledge as someone who was employed by an organization for three years and had three new cases every two months.

However, if a number of years were to be required, second in the list was "3 years experience" at 10 votes out of 52, 19%. As for certifications, association certifications (38%, 14 votes from 48) beat out tools certifications (4%, 2 total votes), non-vender certifications (27%, 13 total votes) and no certifications required at all, (27%, 13 total votes).

For training, 33% (16 votes out of 48) of respondents said that a Cyber Forensic expert should have a minimum of 100 hours of training and/or apprenticeship to prove efficiency. This kind of training was considered more important than vender training (21%), organization specific courses such as from NW3C and SANS (17%), prearrange cases for instruction (4%), and a 6-month apprenticeship with a Cyber Forensic Expert (25%). It was surprising to see that "100 hours of training" was ranked higher than the "6-month apprenticeship with a Cyber Forensic Expert". As there was not enough time to follow up on this result, it was speculated that the reason for this was that the "6-month apprenticeship" was specific and focused where the "100 hours of training" was vague and could account for any kind of training; including the apprenticeship.

Education for Cyber Forensic Experts followed the same trend as "experience". What was taught and the skill sets learned are more important then the level of education. Therefore, a specific degree was not required (35%, 18 votes from 51). Again, if a specific degree was to be required, second in the list was a Bachelor's degree with 17 votes out of 51 (33%).

To summarize, this study revealed that a Cyber Forensic Expert is defined on a case-by-case scenario. That no specific amount of education, training, certifications or years of experience can be used to identify an expert. This is unfortunate, as Cyber Forensic Experts are desperately needed in the field.

On the other hand, this kind of loose accreditation lends well to the Daubert test criterion that says it has to be peer reviewed. If every case of determining an Expert has to go though a complete review, then this aspect of the Daubert test is very much supported. However, it is unrealistic to evaluate an expert in such a manner and would

most likely take long periods of time, as no one would agree on the criteria to evaluate the expert against.

Lastly, participants were asked if Experts should have continuous schooling because technology keeps changing, 100% of participants said yes (52 out 52).

5.5. Academia

There were issues that arose outside the normal bounds of forensic practice. Learning a trade has its issues too and will often yield problems that a practitioner may not experience.

Students have a useful look on things as they see the field from a side that a day-to-day practitioner may not. As they begin to learn about a new interesting topic, they may ask many questions and inquire about why something is the way it is, or how something works, or why the field acts in a XYZ manner. This thought processes allows for more of an unrestricted examination of the field. With this mindset, their drive to understand the field will have a ripple effect on its development. Therefore, it is important to review the issues they see within the field. Table G2 in Appendix G contains the complete list of identified Academic issues from rounds 1 and 2. To see the top ten list of issues in Cyber Forensics for Academia, see Table G1 in Appendix G.

Students are a free avenue to research and development. They enter a program ready to change the world. That kind of motivation needs to be harnessed and directed. The results from this study will provide these entering students with a guide to progress the field forward.

5.6. Law Enforcement

This classification of the respondents was expected to yield the most possible ideas for research ideas, topics and projects. As they are engrossed in the field every day, they are constantly exposed to the issues that plague it.

One issue that can be identified from Table 4.2: *Top 10 Issues Overall* is a lack of error rates on used software. There is a large variety of software available for forensic examination; all of which needs to be evaluated to confirm it is forensically sound to perform an analysis. Most individuals know about the common software used such as FTK and EnCase, but what about the freeware and other smaller programs that are not widely known. How would a researcher know where to start?

The Law Enforcement participants identified the types of software they use as well as the systems they use it on. This information is vital to starting research for tool evaluations. Tables H2, H3 and H6 in Appendix H show an extensive list of software used during Cyber Forensic examinations and on what systems.

Just as in Academia, Law Enforcement participants identified issues that specifically affected Law Enforcement. The Top 3 issues (Table 4.8: *Top 3 Issues for Law Enforcement in Cyber Forensics*) identified are more corporate issues that need to be addressed rather than a research project idea. However, it depends on how it was viewed. One of the projects listed in the all-projects list in Table E1 from Appendix E discusses a project about distributing workload across multiple machines. This research project is a perfect example of how to help address the second and third issues in the Law Enforcement top 3 issues list. By distributing workload across multiple machines, it will speed up the investigations time commitment, therefore freeing up more time to address

the pilling up cases. Plus, the more the systems can do, less manpower is needed which can in turn require less funds to keep up with training for the investigators. This shows that working on a small part of a big issue can still have a staggering effect. All the issues must be carefully considered, as the ripple effect can potentially be huge.

The only problem with the results on the Law Enforcement side was the "Majority" selection question. Many of the participants selected two answers for a single-response question. There is no explanation as to why this was done, and there was not enough time to clarify the reasoning.

5.7. Conclusion

There is a great deal of information for researchers to utilize from this study. The driving force of this paper is to direct future work as opportunities arise for research projects and development funding. Although this study was geared to be a repository of information for starting new projects within Academic and third party circles, it still allows anyone to see where improvements are needed. It is unlikely that a graduate student will be able to convince the field and US court system of accepting their evaluation test to confirm someone has the skills to be a Cyber Forensic Expert, or change the mindset of the politicians into making better laws that compensate for Cyber Forensics. Nonetheless, it allows the people who do have the power to change those issues to become informed on the problem.

The top ten lists showed where the main functions of the field are struggling. But it is believed that the smaller projects and issues will most likely be researched first. This is why they are so important. Issues such as error rates for the used software, creating

programs at no cost for Law Enforcement, developing communication channels, etc. can be resolved through research projects and do not require the entire field and law system to change.

The research projects that are currently in development may not necessarily fix a discovered issue, but it does put the research on the map. By exposing the participants, and anyone else who reads these results, to all the ideas and projects from this study, redundant work can start to be reduced. Once the research has been published and made available to the public, there is no doubt that this paper will be utilized in one way, shape or form over the next few years. The only replacement for it will be another study confirming these results and discovering new ones.

A limitation was the number of participants in the study. Although 85 may have been a good number for a 3-round survey, it is hardly a great representation of the entire field and all of its issues. This study created a broad overview of the issues in the field; however, with only 14 universities and 14 different states participating out of the 50, this overview cannot be considered 100% complete. There are many others that have concerns about the field that were not able to voice their opinions. This study also generalizes the entire population to only the US. Cyber Forensics is a field that reaches across the globe. Aside for American Law downfalls, the identified issues could pertain overseas, as well as other issues could have been identified.

In addition, this project was limited to Law Enforcement and Academia only. As issues related to the Cyber Forensic Field extend into many other areas, the identified issues are still a limited collection. However, these issues were generated by the working individuals of the field as well as by those who extensively study it. As mentioned

before, this study is not a golden list or a catchall for the field, but rather a great place to start. The impact of this research has the potential to be huge as many research projects can be derived from these results. If this paper directs the research and development of the field as it intended, the next few years of Cyber Forensic practice should have a giant leap forward.

In conjunction with the study's limitations, there are some aspects of the study that could be changed in the event of a confirmation or follow-up study. First, some of the questions should have been more controlled. For example, the "What state do you reside in" question would have been more helpful for breaking down questions if a selection box was used instead of leaving it as an open text box. Although breaking down the answers based on location would not have helped explain the issues more, it would add additional supplemental information to an already large source of data. Other questions that needed more control over how the answers to the questions were recorded included: the years of studying in the field, the number of years examiners were practicing in the field, and both sets of the education breakdown questions.

Second, the recruitment phase was a huge job for one person and would be much more workable if a small team, 2 or 3 people, were in charge of this task. This would have allowed for quicker collection of responses and possibly an increase in the recruitment numbers.

Third, make cut offs for participants to meet deadlines shorter. Most wait until the last minute to finish the questionnaire so there is no reason to give them a large amount of time to do so. Which also increases the chance of them forgetting to complete it entirely. Plus, by having stricter deadlines, it would have allowed for a final follow up

to the participants to verify some of the contradicting and confusing responses that were discovered during the final round.

Last, if there were an easier way to conduct round one and two, the study would have been much easier. As the first two rounds were open-ended questions, there was a lot of data to sort through and organize. Blocks of text from a plethora of questions from 85 participants does not lend well to speedy analysis.

REFERENCES

REFERENCES

Blunden, B. (2009). Anti-forensics: The rootkit connection. Proceedings of Black Hat USA 2009. Retrieved from http://belowgotham.com/BHUSA09-Blunden-AntiForensics-PAPER.pdf.

Broucek, V., & Turner, P. (2002a). Bridging the divide: Rising awareness of forensic issues amongst systems administrators, *3rd International System Administration and Networking Conference*. Maastricht, The Netherlands. Retrieved Feb. 23, 2010 from http://bartholomewmorgan.net/resources/Maastricht_Paper.pdf.

Brown, Stephen L. (2005). E-mail versus web survey response rates among health education professionals *American Journal of Health Studies, 20*(1). Department of Health Sciences, University of Alabama.

Cobanoglu, C., Warde, B. & Moreo, P. (2001) A comparison of mail, fax, and web-based survey methods, *International Journal of Market Research, 43,*(4), pp. 441–452.

Colton, S., & Hatcher, T. *Constructing a web-based Delphi.* Unpublished manuscript, Department of Information Technology, Media Services, Monterey Peninsula College, Montgomery, CA.

Cornell University Law School. (2010). *Federal Rules of Evidence: Rule 702 – Testimony by Experts.* Retrieved from http://www.law.cornell.edu/rules/fre/rules.html#Rule702.

Craiger, P., Swauger, J., Marberry, C., & Hendricks, C. (2006). Validation of digital forensics tools. In potter, M., Roth, K., Neidig, J., Reed, S., Dean, N. (eds.) *Digital Crime and Forensic Science*. (pp91-105). Hershey, PA: Idea Group Publishing.

Cuhls, K. (n.d.). Delphi method. *Fraunhofer Institute for Systems and Innovations Research, 93-113.* Fraunhofer, Germany. Retrieved from http://www.unido.org/fileadmin/import/16959_DelphiMethod.pdf.

Dictionary.com (2010). Define Survey. Retrieved on March 20, 2010 from http://dictionary.reference.com/browse/survey.

Dictionary.com (2010). Define Groupthink. Retrieved on March 20, 2010 from http://dictionary.reference.com/browse/groupthink.

Erbacher, R. & Swart, R. (2007). Computer Forensics: Training and education. Department of Computer Science & Department of Business Information Systems,
Utah State University. Retrieved October 18, 2009 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.6123&rep=rep1&type=pd.

Ericsson, K. A. (2006). The influence of experience and deliberate practice on the development of superior expert performance. In K. A. Ericsson, N. Charness, P. Feltovich & R. R. Hoffman (Eds.), *Cambridge handbook of expertise and expert performance.*(pp. 685–706). Cambridge: Cambridge University Press.

Fraze, S. D., Hardin, K. K., Brashears, M. T., & Haygood, J. L. (2003). The effects of delivery mode upon survey response rate and perceived attitudes of Texas Agri-Science teachers. *Journal of Agricultural Educaiton, 27*(44). 27-37.

Harris, R. (2006). Arriving at an anti-forensic consensus: Examining how to define and control the anti-forensics problem. *Digital Investigations, 3S*, s44-s49. doi: 10.1016/j.diin.2006.06.005.

Jones, R. (2007) Safer live forensic acquisition. University of Kent at Canterbury. Retrieved November 02, 2009 from http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf.

Kaplowitz, M. D., Hadlock, T. D., & Levine, R. (2004). A comparison of web and mail response rates. *Public Opinion Quarterly, 68*(1). 94-101. doi: 0.1093/poq/nfh006 www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf.

Liles, S., & Rogers, M. & Hoebich, M. (2009) A survey of the legal issues facing digital forensic experts . Advances in Information and Communication Technology, 306/2009, 267-276. doi: 10.1007/978-3-642-04155-6_20.

Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence, 3*(2).

Mukasev, M. et al. (2008). *Electronic Crime Scene Investigations: A Guide to First Responders.* (NCJ 219941). Washington, D.C.: National Institute of Justice (NIJ).

Neill, J. (2007). Delphi Study: Research by Iterative, Consultative Inquiry. Retrieved from http://wilderdom.com/delphi.html.

Okoli, C., & Pawlowski, S. D. (2003). The delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42,* 15–29 doi:10.1016/j.im.2003.11.002.

PeoplePulse. (2010). Ti`ps on How to Increase Your Survey Response Rates. Retrieved on April15, 2010 from http://www.peoplepulse.com.au/Survey-Response-Rates.htm.

Purdue IRB. (2010). Obtain IRB Approval. Retrieved on March 12, 2010 from http://www.purdue.edu/research/vpr/rschadmin/rschoversight/humans/approval.php.

Reith, M., Carr. C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 4*(3).

Richard III, G. G., & Roussev, V. (2004). Next generation forensics: The digital forensic community requires new tools and strategies for the rapid turnaround of large forensic targets. *Communication of the ACM*, 49(2), 76-80.

Rogers, M. (2007) A practical approach to digital crime scene analysis. In Tipton, H. F. & Krause, M. (eds). *Information Security Management Handbook, Sixth Edition.* (pp. 2945-2966). Florida: Auerbach Publications.

Rogers, M., Goldman, J., Mislan, R., &Wedge, T. (2006). Computer forensics field triage process model. Proceedings of Digital Forensics, Security and Law. Retrieved from http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf.

Rogers, M. & Seigfried, K. (2009). The future of computer forensics: A needs analysis survey. *Computer and Security, 23,* 12-16.

Shakamui, Mayuri. (2006). *Forensic Certifications*. Unpublished manuscript. Digital Forensics, New Mexico Tech, Socorro, New Mexico.

Shin, T. (n.d.). Delphi Study at the Multi-Country Level: Gains and Limitations. Science andTechnology of Policy Institute. Retrieved from http://www.nistep.go.jp/achiev/ftx/eng/mat077e/html/mat077he.html.

Sheehan, Kim. (2001). Email survey response rates: A review. *Journal of Computer Mediated Communication,6*(2). doi: 10.1111/j.1083-6101.2001.tb00117.x Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.10836101.2001.tb00117.x/full.

Skulmoski, G., & Hartman, F. T., & Krahn, Jennifer. (2007). The delphi method for graduate research. *Journal of Information Technology Education, 6*, 1-22. Retrieved from http://www.jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2001). *Electronic Crime Needs Assessment for State and Local Law Enforcement.* (NCJ 186276). Washington, D.C.: National Institute of Justice (NIJ). Retrieved October 28, 2009 form http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.html.

Technical Analysis Group. (2004). Law enforcement tools and technologies for investigating cyber attacks: Gap analysis report. Institute for security Technology Studies (ISTS) at Dartmouth College. Retrieved on April 14th 2012 from http://www.ists.dartmouth.edu/library/215.pdf

Technical Analysis Group. (2004). Law enforcement tools and technologies for investigating cyber attacks: A national research and development agenda. Institute for Security Technology Studies (ISTS) at Dartmouth College. Retrieved on April 14th 2012 from http://www.ists.dartmouth.edu/library/214.pdf

Vatis, Michael. (2002). Law enforcement tools and technologies for investigating cyber attacks: A national needs assessment. Institute for security Technology Studies (ISTS) at Dartmouth College. Retrieved on April 14th 2012 from http://www.ists.dartmouth.edu/docs/ISTS_NA.pdf.

Wikipedia.com (2010). Delphi Method. Retrieved on February 27, 2010 from http://en.wikipedia.org/wiki/Delphi_method.

Wikipedia.com (2010). *Delphi Method*. Retrieved from http://en.wikipedia.org/wiki/Groupthink.

www.google.com (2010). Searching Digital Forensic Models. Retrieved from http://www.google.com/search?source=ig&hl=en&rlz=&q=digital+forensic+models&aq=f&aqi=g10&aql=&oq=&gs_rfai=.

www.google.com (2010). Searching Digital Forensic Models. Retrieved from http://www.google.com/search?source=ig&hl=en&rlz=&q=digital+forensic+models&aq=f&aqi=g10&aql=&oq=&gs_rfai=.

APPENDICES

Appendix A. Letters and Associated Questions

A.1 Recruitment Letter

<Date>
Purdue University, Cyber Forensics Lab

To whom it may concern,

My name is Francis Ripberger. I am a researcher at Purdue University studying for my Master's in Cyber Forensics. I contacted <Location> looking for the department that is responsible for cyber crimes, digital investigations and/or computer forensics. <contact>'s contact was given to me and in return, <he or she> gave me your email address. The reason for me contacting you is to recruit your help in my research. This project has been approved by Purdue University's Internal Review Board (IRB).

As I am sure you are aware, the Cyber Forensic field is a young, rapidly growing field; one that needs constant development. I am collecting data on the opinions of today's Cyber Forensic Specialists, Instructors, and students to discover today's issues and concerns for the Cyber Forensic field.

I am asking permission to send you three questionnaires over the course of this study to gather this data.

The first questionnaire will be to simply find out what you believe are the downfalls of the field, what needs to be improved, and if you, or someone you know, is working on a project to help improve the field. Once all the answers from this first round have been collected, those answers, and some criteria from already performed research, will be added together and categorized. This questionnaire will take approximately 15 minutes to complete.

The second questionnaire will show the opinions from all the other participants (names/organizations will not be distributed, just the collection of opinions). At this point, you will be asked to make statements on the given topics, if you agree or disagree, make changes to the categories, and/or list any research or projects that you know are in progress to help solve these issues. It is hoped that by reading the list, you may discover additional areas that are in need of development, and add those to the list. This questionnaire will take approximately 10 to 15 minutes to complete.

After the first two questionnaires have been completed and the information has been gathered, the third and final questionnaire will begin. This official survey will be made available to all the participants thus far. The study will be looking for your opinion on the top ten issues in the field overall and the top ten issues in each category that was created based on the first two rounds of questioning. This survey will also ask for

opinions on what was reported to be currently in development/researched and if you feel it will be helpful. In addition, some demographic questions will be asked including where/how you received your Cyber Forensic training. The demographic information will be used for statistical analysis and will not be linked to your specific responses. This questionnaire should take approximately 10 to 15 minutes to complete.

At the end of the study, all participating individuals will receive a copy of the finished report. As the conducting researcher, I will retain access to your contact information throughout the study. Please note, that this information will not be released to any other participant, nor will it be linked to your responses of the study's questions. Once the project has been completed, all personal information will be deleted. In addition, I will retain the original raw data in a secure fashion.

Please consider being apart of this first ever national research program in order to better the field. Remember, all research and development performed in this field affects all those who work in it; the more opinions, the greater the response, and the greater chance of the top needs getting addressed.

If you would like to participate in this study, a confirmation email is needed. Please email me at FRIPBERG@CERIAS.PURDUE.EDU, indicating that you wish to volunteer. If you have any colleagues that you believe would like to participate in this study, please pass this letter along to them. I am also looking for students who are studying the field, as they will offer a unique perspective. Please let me know if you would like to include your students. If so, please indicate how many will be participating.

If you know of any other specialists in the field, outside of your department, please forward this on to them; again, the more opinions the better. Anyone involved with Cyber Forensics is welcome.

Thank your time and willingness to help,

Francis Ripberger
Purdue University Cyber Forensics
CERIAS Student
FBI Infraguard Member
FRIPBERG@CERIAS.PURDUE.EDU
765-507-9194 (cell)

Supervising Professor:
Dr. Marcus K. Rogers
Professor/University Faculty Scholar
Fellow of CERIAS
Director - Cyber Forensics Program
College of Technology, Dept. of Computer & Information Technology
Purdue University

(765)494-2561
rogersmk@purdue.edu

Assurances and Restrictions:

This section details the assurances that are implemented in this study to protect the participant as well as list the restrictions that apply.

- This study is completely voluntary
- Non-participation will not have an effect on employment
- No addresses will be taken or recorded, only geographical region.
- You may skip any question during the two questionnaires and survey if you feel uncomfortable.
- Your name and contact will not be disclosed to any other participants and will not be linked to your responses of the study's questions.
- Only my supervising professor and I will have access to all participant's contact information. Measures will be taken to ensure that no personal or confidential information will be released. All responses will be anonymous.
- Questionnaires will be distributed through email.
- Participant must be at least 18 years of age

A.2 First Letter After Recruitment

Dear <name>,

Thank you for deciding to participate in this national study. As indicated in the first letter you received, this is the first questionnaire of three.

Please take your time and thoroughly think out your answers. The more detail you give, the better. You do not have to answer all the questions in one sitting. You may take a break at any time and come back to finish later. <just don't close the window or exit the questionnaire>

Remember, you may skip any questions that make you feel uncomfortable. But remember to hit submit at the end when you have finished.

The link below will take you to the questions. Please give your first and last name at the beginning so can follow who has finished the questions. Your answers will not be linked to your name.

<link>

Thank you for your time,

Francis Ripberger

Purdue University, Cyber Forensics

fripberg@cerias.purdue.edu

A.3 First Round of Questions

1.) What is your gender? __Male or __ Female (Check one)

2.) What is your age?
__18-25 __26-33 __ 34-41 __42-49 __50-57 __58 or older

3.) What state do you work in?

4.) What do you believe classifies someone as an expert in Cyber Forensics?

5.) Please list any, and all, issues you feel are important in the Cyber Forensic field/area of study.

   a. Please indicate why you feel these issues are important.

6.) Would you categorize yourself as Law enforcement, academia, or a lawyer?

   a. Please indicate any, and all, limitations of the field you feel hinder you from performing your job to fullest that were not listed in questions 4 and 5.

   b. Please indicate why you feel these limitations hinder you.

7.) Are you currently developing or researching any solutions for the stated items from question 1?

   a. If so, please share by giving a brief synopsis of your project(s).

8.) Is there anything else you would like to add, that wasn't mentioned on this questionnaire?

A.4 Second Letter After Recruitment

Dear <name>,

Thank you for completing the first round of questioning. As all the data has been collected and organized from the first round, we are now ready to proceed to the second round of questioning, which is based off the answers given in round one.

Please take your time in completing this questionnaire. The more detail you give, the better. You do not have to answer all the questions in one sitting. You may take a break at any time and come back to finish later. <just don't close the window or exit the questionnaire>. There will be a section at the end if you wish to add statements or ideas that were spurred from completing the second round of questioning.

Remember, you may skip any questions that make you feel uncomfortable. But remember to hit submit at the end when you have finished.

The link below will take you to the questions. Please give your first and last name at the beginning so we can follow who has finished the questions. Your answers will not be linked to your name.

<link>

Thank you for your time,

Francis Ripberger
Purdue University, Cyber Forensics
fripberg@cerias.purdue.edu

A.5 Second Round Questions

1.) What state do you reside in?

2.) What is your age?
__18-25 __26-33 __ 34-41 __42-49 __50-57 __58 or older

3.) What is your Gender? __Male __ Female (Check one)

4.) Do you agree with the organization and categorization of the results from the first questionnaire?

__ strongly agree ___agree __neutral __disagree __strongly disagree

a. If you disagree or strongly disagree, what changes would you make?

b. Why?
(this is important. As the last round of questioning will be based off the answers from this questionnaire.)

5.) After reviewing the list, do any ideas for improvement come to mind? Please write them below.

6.) Please list any additional issues for the Cyber Forensic field that come to mind.

a. For each additional item you listed in question 2 and 2A, please share why you feel that entry is important.

7.) In your opinion, do you feel the stated projects that are currently in development will be beneficial to the field?

8.) Do you believe it will be beneficial to you?

A Daubert test is a judicial assessment that can be applied to a forensic study, procedure, practice, standard or expert witness. This test is used to compare the topic in question to specific criteria for the sake of determining the topic's validity; in order for a court of law to accept the evidence discovered by it, as legitimate.
The Daubert test compares against the following criteria:

- Empirical Testing: technique or theory must be testable and refutable

- Subject to peer review
- Potential error rate must be known
- Standards and controls concerning its operation
- The theory or technique must be generally accepted by the relevant scientific community.

9.) Do you feel the forensic field as a whole could withstand a Daubert test?

a. If no, where do you think the field fails?

10.) From the criteria given on Cyber Forensic Experts, what do you believe is the bare minimum needed?

11.) Additional Comments?

A.6 Third Letter After Recruitment

Dear <name>,

Thank you for completing the second round of questioning. As all the data has been collected and organized from the first two rounds, we are now ready to proceed to the third and final round of questioning, which are based off the answers from rounds one and two.

Please take your time in completing this questionnaire. There are many choices, so please take all ideas and topics into consideration. You do not have to answer all the questions in one sitting. You may take a break at any time and come back to finish later. <just don't close the window or exit the questionnaire>. There will be a section at the end for comments on the study itself or anything else you feel needs to be shared. Please be sure to answer the demographic questions as well.

Remember, you may skip any questions that make you feel uncomfortable. But remember to hit submit at the end when you have finished.

The link below will take you to the questions. Please give your first and last name at the beginning so can follow who has finished the questions. Your answers will not be linked to your name.

<link>

Thank you for your time,

Francis Ripberger
Purdue University, Cyber Forensics
fripberg@cerias.purdue.edu

A.7 Third Round Questions (survey)

1.) Currently, would you categorize yourself as Law enforcement, academia or a lawyer?

2.) What state do you reside in?

3.) What is your gender? __Male or __Female (please check one)

4.) Are you a cyber forensic investigator?
   a. If not, what is your job title?

5.) What is your age?

__18-25 __26-33 __ 34-41 __42-49 __50-57 __58 or older

6.) From each of the categories of issues listed, please indicate the top 10 issues for each.

7.) Now, taking into account all issues listed, regardless of category, please indicate the top ten issues over all.

   a. For each, please tell how long you believe this issue has impacted the field in years.

__ 1-2 years __3-5 __6-8 __9-11 __12-14 __15-17 __18-20 __20 or more

Please read the following instructions. (Please fill out the appropriate section. If you fit more than one, please answer both section's questions.)

- ***If you are a cyber forensic investigator (a practitioner) or supervisor thereof, please answer question 8-12. Then SKIP to question 17.***
- ***If you are an academic (professor or student), please answer questions 13 & 14. Then SKIP to question 18.***
- ***If you are a lawyer, please answer questions 15 -16. Then continue with question 17.***

For Forensic Investigators only (practitioners)

8.) Are you the only cyber crimes investigator at your workplace or are you a member of a team?

   a. If you are a part of a team, how many members are in your team?

9.) How did you gain your cyber forensic skills? (Please check one)
__self taught ___school __training session ___certification ___other

   a. If school, please list which one.
   b. Please pick one of the following.
      Your school program was designed as:

__2-year associates __4-year program Bachelor's __ Master's __Doctorate

   c. Did you complete this program? __Yes ___No (Please Check one)
   d. If trained, please indicate how. (Check one)
      __ Technical School __mentor __ self-taught __other
   e. If other, please describe.

10.)If you have received a certification(s), please indicate which ones you hold.

11.)What platform do you spend your time performing cyber forensic investigations? (Check all that apply)
__Windows __Mac __Unix/Linux __cell phones __PDAs __game consoles __ipods/media player __other

   a. Which platform do you spend the **majority** of your time?
      __Windows __Mac __Unix/Linux __cell phones __PDAs __game consoles __ipods/media player __other

b. If multiple platforms are used on a regular basis, please indicate an estimated percentage of your time spent for each.
___Windows ___Mac ___Unix/Linux ___cell phones ___PDAs
___game consoles ___ipods/media player ___other

12.)What forensic software do you use?

a. Please indicate the percentage of your time you spend on each.

<u>For Academics only. (professors and students)</u>

13.)How many years have you been studying the field of Cyber Forensics?

14.)What will you graduate with? (Please check one.)

___Associates degree __Bachelor's degree __Master's degree __Doctorate
___Certification __Other

a. If other, please describe.

<u>For Lawyers only.</u>

15.)How many years have you been using cyber forensic evidence in your proceedings?

16.)How many cyber forensic cases have you worked on?

<u>General Questions Continued</u>

17.)Number of years in the field?

18.)From the criteria given on Cyber Forensic Experts, what do you believe is the bare minimum needed?

19.)Suggestions on how to maintain the Cyber Forensic field as technology is constantly changing, with new challenges rising every day. How are we to keep up?

20.)Other comments

21.)Would you use an online repository of published research pertaining to the cyber

forensic field?

a. Would you like a forum on a site so you can discuss topics with other forensic experts?
b. Would you use a site if it contained reviews of forensic software that is available at the present time?
c. Would you use a site if links to other forensic sites were listed?
d. Would you use a site if it had a designated area for developing ideas, coordination research, and recruiting for forensic projects?
e. Would you use a site if it had a contacts list of willing experts that were willing to give help if needed?

Appendix B. Table of Known Needs

Areas in need of improvement	
Tools (development, usefulness, accountability, metrics, etc)	Stambaugh, H. et al. (2001). Electronic Crime Needs Assessment for State and Local Law Enforcement. (NCJ 186276). Washington, D.C.: National Institute of Justice (NIJ). Retrieved October 28, 2009 form http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.htm Richard III, G. G., & Roussev, V. (2004). Next generation forensics: The digital forensic community requires new tools and strategies for the rapid turnaround of large forensic targets. Communication of the ACM, 49(2), 76-80
Certifications / Standardization	Shakamui, Mayuri. (2006). *Forensic Certifications*. Unpublished manuscript. Digital Forensics, New Mexico Tech, Socorro, New Mexico Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence, 3*(2).
Law (rights, search and seizure, expert witness, guidelines, etc)	Liles, S., & Rogers, M. & Hoebich, M. (2009) A survey of the legal issues facing digital forensic experts . Advances in Information and Communication Technology, 306/2009, 267-276. doi: 10.1007/978-3-642-04155-6_20. Broucek, V., & Turner, P. (2002a). Bridging the divide: Rising awareness of forensic issues amongst systems administrators, *3rd International System Administration and Networking Conference*. Maastricht, The Netherlands. Retrieved Feb. 23, 2010 from http://bartholomewmorgan.net/resources/Maastricht_Paper.pdf .
Training	Stambaugh, H., et al. (2001). *Electronic Crime Needs Assessment for State and Local Law Enforcement.* (NCJ 186276). Washington, D.C.: National Institute of Justice (NIJ). Retrieved October 28, 2009 form http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.htm Erbacher, R. & Swart, R. (2007). Computer Forensics: Training and education. Department of Computer Science & Department of Business Information Systems, Utah State University. Retrieved October 18,

	2009 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.6123&rep=rep1&type=pd
Academia	Stambaugh, H., et al. (2001). *Electronic Crime Needs Assessment for State and Local Law Enforcement.* (NCJ 186276). Washington, D.C.: National Institute of Justice (NIJ). Retrieved October 28, 2009 form http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.htm Erbacher, R. & Swart, R. (2007). Computer Forensics: Training and education. Department of Computer Science & Department of Business Information Systems, Utah State University. Retrieved October 18, 2009 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.6123&rep=rep1&type=pd
Evidence gathering (Procedure models)	Reith, M., et al. (2002). An examination of digital forensic models. *International Journalof Digital Evidence, 4*(3). Rogers, M., et al. (2006). Computer forensics field triage process model. Proceedings of Digital Forensics, Security and Law. Retrieved from http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf.
Crime Scene (securing physical evidence, live analysis, analysis)	Mukasev, M. et al. (2008). *Electronic Crime Scene Investigations: A Guide to First Responders.* (NCJ 219941). Washington, D.C.: National Institute of Justice (NIJ). Jones, R. (2007) Safer live forensic acquisition. University of Kent at Canterbury. Retrieved November 02, 2009 from http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf Rogers, M. (2007) A practical approach to digital crime scene analysis. In Tipton, H. F.& Krause, M. (eds). *Information Security Management Handbook, Sixth Edition.* (pp. 2945-2966). Florida: Auerbach Publications.
Anti-forensics	Blunden, B. (2009). Anti-forensics: The rootkit connection. Proceedings of Black Hat USA 2009. Retrieved from http://belowgotham.com/BHUSA09-Blunden-AntiForensics-PAPER.pdf.

Harris, R. (2006). Arriving at an anti-forensic consensus: Examining how to define and control the anti-forensics problem. *Digital Investigations, 3S*, s44-s49. doi: 10.1016/j.diin.2006.06.005.

Appendix C. Table of Past Studies (Partial Table)

Past Studies	Purpose
Brancheau, B.D., & Wetherbe, J. C. (1996). Key issues in information systems management: 1994–95 SIM Delphi results. *MIS Quarterly, 20*(2). 225–242. Brancheau, B. D., & Wetherbe, J. C. (1987). Key issues in information systems management. *MIS Quarterly, 11*(1). 23–45.	Identify the most critical issues facing IS executives in the coming 3–5 years
Hayne, S., & Pollard, C. (2000). A comparative analysis of critical issues facing canadian information systems personnel: A national and global perspective. *Information & Management 38*(2). 73–86.	Identify the critical issues in IS in the coming 5 years perceived by Canadian IS executives and non-management IS personnel and compare to global study rankings.
Lai, V., & Chung, W. (2002). Managing international data communications. *Information & Management 45*(3). 89–93.	Identify a prioritized list of international data communications activities vital to multinational corporations in managing information exchanges for control and implementation of global business strategies.
Viehland, D., & Hughes, J. (2002). The future of the wireless application protocol. Proceedings of the Eighth Americas Conference on Information Systems (pp. 1883–1891). Dallas	Compile a ranked list of 12 future scenarios related to the potential success of the Wireless Application Protocol (WAP).
Schmidt, R. C., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems 17*(4). 5–36.	Develop a ranked list of common risk factors for software projects as a foundation for theory building about IS project risk management.

Appendix D. Issues

This table's percentages are based on the 53 participants that voted for the top 10 issues in the field overall. They are for reference only.

Table D1: *Issues in Cyber Forensics*

Issue	Frequency	Percentage
No official characteristics or criteria that defines a Cyber Forensic Expert (everyone's definition is different)	14	26%
No official / accepted certifications to qualify an individual (cyber forensic analyst or not) as a cyber forensic expert	18	34%
Being considered an expert in all aspects of technology when the investigator is an expert in only one area.	10	19%
A lack of Cyber Forensic Experts in the field	10	19%
There are no non-vender certifications to identify that a person has the qualifications required to be a Cyber Forensic Investigator.	7	13%
Not all tools have certifications to ensure a user knows how the program functions and how to use it correctly	5	9%
Current vender certificates are easy to obtain. They should be more difficult (think Cisco certified).	6	11%

The Cyber Forensic field is young and naive, therefore reactive and not proactive.	9	17%
Policies are often well written but are often not followed	5	9%
Cyber Forensic Science is too broad when considering all the different types of technology. It needs to be broken into specialization.	6	11%
There are no standards for practioning (only best practices and personal preferences).	8	15%
There are no models or frameworks for conducting investigations. (There should be a model/framework for each type of investigation...computers, hand-helds, consoles, phones, etc)	3	6%
A lack of applying the scientific method to investigations.	6	11%
Ambiguity (All the tools are doing the same thing different ways)	4	8%
Error rates for tools used are not defined to document reliability.	3	6%
Vender restrictions prohibiting examination of source code to obtain error rate.	2	4%
There is no standardization in tool operation or creation.	4	8%
Lack of tool validation for ensuring reliable evidence	3	6%
Lack of tools to extract information from phones (such as deleted information)	5	9%
Tools are not keeping up with changing technology.	10	19%
There is a lack of understanding how the tools work and why they are used.	5	9%

Current tools cannot handle large data storage devices and large amounts of data.	5	9%
Wifi tracking - there are no tools to track / trace criminals as they can easily gain access to unsecured / poorly secured wifi connections	5	9%
There is a knowledge gap between practitioners and courts within technology and how it operates.	13	25%
Politicians pass laws without prior knowledge of the field and how it will effect the cyber investigative process.	10	19%
Limitations imposed by Courts and search warrants prohibit effective discovery tactics.	3	6%
Search warrant scopes prevent the collection of potential evidence.	0	0%
Communication - jury/judge are not technical peers and do not understand technical jargon/concepts, therefore it is difficult to explain a technical incidence	12	23%
Complexities of what constitutes a message in transit vs. one in storage	0	0%
Rapidly changing legal environment.	5	9%
Courts, in general, are behind in knowledge for Cyber Forensic cases.	16	30%
Courts need to show Practitioners the reasoning behind policies.	1	2%
Lack of funding for Research projects	10	19%
Lack of funding for Training	17	32%
Lack of funding for new equipment and Software	13	25%

Lack of funding for new hires	9	17%
The techniques taught for lab work are not evaluated.	1	2%
Labs operate with out of date equipment and tools	6	11%
Some labs are inappropriate facilities to maintain evidence integrity	1	2%
The use of "Click Button" analysts (examiners don't know the programs or their processes; they just click a button and report the results)	13	25%
Undertrained/overconfident analysts - They have only taken one class or know how to use one program and feel they are qualified to be a digital analyst.	5	9%
No Examiner Networking - so examiners can connect with other examiners for help (specialties, experience, etc)	2	4%
No Organization Networking (communication between law branches and organizations to help track down crimes over the internet)	0	0%
Lack of training for examiners.	8	15%
Lack of experts to train others	3	6%
Lack of writing skills to efficiently relay information (documenting processes, chain of evidence, findings, reports, etc)	2	4%
Communication skills - examiners need to be able to relate difficult computer concepts to the masses (jury / judge, public, etc.) as they do not understand technical jargon	4	8%
Semantics (trying to define everything)	3	6%
Examiners lack adaptability and innovation for	1	2%

changing technology		
A lack of examiner Integrity	0	0%
Lack of an ethical code (examiners have been found to operate without an ethical code to guide their work)	2	4%
Examiners don't know how to effectively use tools	5	9%
A lack of understanding of the current laws	4	8%
The lack of knowledge about digital forensics and its use in the collection and preservation of legally admissible evidence in senior management for program and IT departments	4	8%
Locating the evidence	4	8%
Classifying the evidence	1	2%
Ethically extracting evidence without errors that may harm an investigation. (finding, collecting, preserving, and/or presenting information in the Cyber Forensic field or court of law)	0	0%
Analyzing the data	7	13%
Attention to detail (ex. Meta data may change the meaning of a "first-glance and disregarded" file)	3	6%
Correct interpretation of discovered data (Is it evidence?, What does it mean?, etc.)	9	17%
Knowing how to maintain integrity and quality assurance of a hard drive and digital evidence	1	2%
Following the Chain of Custody.	1	2%
Technology is constantly changing (will the old tools still work, are there any issues, does it still protect the data, etc)	15	28%

New market trends, market motives and statistics (how tech is being used to commit crimes)	1	2%
Ever increasing storage space	15	28%
Tablets are emerging as the system to analyze	5	9%
Lack of knowledge in cellular networks and technology	4	8%
Small devices (they are everywhere and people are careless - tools and standards are needed for data extraction) phones, RFID sensors, handhelds, thumb drives, mp3 players, etc.	8	15%
OSs - many and constantly growing (proliferation of the plethora of OSs)	2	4%
Key Loggers - security threat (how to find them)	1	2%
Encryption for devices preventing forensic examination (examples, AES and quantum)	14	26%
Lack of knowledge to keep current on legacy systems	1	2%
Increased use of social networking (Is the data public, semi-private, or private?)	5	9%
Solid State Drives (current forensic tools can,Äôt recover data from unallocated space on these drives)	8	15%
Anti-forensics	11	21%
Virtualization (techniques for hard systems are unconfirmed on virtual systems -- Is all data stored the same way?, what new info can we gather?, etc.)	10	19%
Training examiners to have a Low level understanding of computers	3	6%
Lack of computer classes (example of classes that	4	8%

are need: BDRA and IDRA courses offered by the National White Collar Crime Center)		
Continuous Training (technology constantly changes = constant education of tools, equipment, and computer functions are needed)	13	25%
Lack of training options and availability	3	6%
Cost of training (technology keeps changing so more and more training is required)	12	23%
Recap training to keep lesser used skills fresh	2	4%
Limitations in training (example: a lack of time and materials for teaching)	2	4%
Training should include "how to extract information in the least intrusive form"	1	2%
The public has a lack of awareness of cyber crime, how it can effect a company and public safety, and how to prevent against it	8	15%
System admins are not keeping posted on how to protect systems, therefore, making it easier for cyber crime	1	2%
The public has a lack of sense considering Cyber Security (If they protected their data and way of life better, it would significantly limit the need for Cyber Investigators)	0	0%
The public does not know who to turn to for help when attacked or how to recoop losses	3	6%
Accountability (people storing info on systems and places that never should have contained the info)	0	0%
Cloud computing (Who owns the data?, Where does it reside?, International data centers, etc)	7	13%

Mediation between disciplines, including law, policy, academics, and enforcement	4	8%
No national organization for Cyber Forensics	3	6%
No Network Security to stop proliferation of cyber crime.	0	0%
Examiners should work on scene or/and with an experienced investigator in the beginning to understand the investigative side before working alone	0	0%
Malware (Cyber Forensics doesn't know how to track the developers, analyze what it has done, and reverse engineer it)	3	6%
Time - learning about all the past attacks and procedures, and then about the new technology takes a lot of time - hackers have a lot more free time - (we have jobs and other cases too)	4	8%
There is repetition work between research groups and agencies because of no coordination between them.	5	9%

Table D2 displays the results from 7 different questions that required only one response for each. This was done to condense similar responses together in order for the information displayed to be easier to read. Each line describes a different question, displays the answer that was voted on the most, and focuses on the top issue for a specific area within Cyber Forensics. For example, the first question refers to the top issue pertaining to Cyber Forensics and the general public. Out of 56 participants that answered that question, 34(61%) agreed the main issue was a lack of awareness of cyber crime, how it affects others, and how to prevent it.

Table D2*: Single Response (Top Issue) Questions*

Question	Answer	Frequency (out of)	Percentage (%)
Top issue pertaining to Cyber Forensics and the general public	The public has a lack of awareness of cyber crime, how it can effect a company and public safety, and how to prevent against it	34 (56)	61%
Top issue in Cyber Forensic Labs	They operate with out of date equipment and tools	29 (54)	54%
Top issue pertaining to the Cyber Forensic Field.	Cyber Forensic Science is too broad when considering all the different types of technology. It needs to be broken into specialization.	30 (56)	54%
Top issue pertaining to certifications in Cyber Forensics	There are no non-vender certifications to identify that a person has the qualifications required to be a Cyber Forensic Investigator.	26 (55)	47%
Top issue pertaining to cyber forensic examinations	Correct interpretation of discovered data (Is it evidence?, What does it mean?, etc.)	22 (56)	39%
Top issue pertaining to Cyber Forensic Experts	No official characteristics or criteria defines a Cyber Forensic Expert (everyone's definition is different)	21 (57)	37%
Top issue pertaining to Cyber Forensics	Cloud computing (Who owns the data?, Where does it reside?, International data centers, etc)	20 (57)	35%

Table D3*: Top 3 Issues with Tools in Cyber Forensics*

Selected Answers	Frequency / Percentage (Total 56)
Tools are not keeping up with changing technology.	27 (48%)
Lack of tool validation for ensuring reliable evidence	23 (41%)
Lack of tools to extract information from phones (such as deleted information)	21 (38%)

Table D4*: Top 3 Issues with Law in Cyber Forensics*

Answer	Frequency / Percentage (Total 57)
There is a knowledge gap between practitioners and courts within technology and how it operates.	48 (84%)
Courts, in general, are behind in knowledge for Cyber Forensic cases.	43 (75%)
Politicians pass laws without prior knowledge of the field and how it will affect the cyber investigative process.	35 (61%)

Table D5*: Top 5 Issues with Examiners in Cyber Forensics*

Top Selected Answers	Frequency / Percentage (Total 52)
The use of "Click Button" analysts (examiners don't know the programs or their processes; they just click a button and report the results)	40 (77%)
Lack of training	35 (67%)
Undertrained / overconfident analysts -- They have only taken one class or know how to use	31 (60%)

one program and feel they are qualified to be a digital analyst.	
Lack of experts to train others	20 (38%)
Communication skills -- examiners need to be able to relate difficult computer concepts to the masses (jury / judge, public, etc.) as they do not understand technical jargon	20 (38%)

Table D6*: Top 5 Technological Issues in Cyber Forensics*

Answer	Frequency / Percentage (Total 57)
Technology is constantly changing (Will the old tools still work?, Are there any issues?, Does it still protect the data?, etc)	45 (79%)
Ever increasing storage space	35 (61%)
Encryption for devices preventing forensic examination (examples, AES and quantum)	35 (61%)
Small devices (they are everywhere and people are careless - tools and standards are needed for data extraction) phones, RFID sensors, handhelds, thumb drives, mp3 players, etc.	26 (46%)
Virtualization (techniques for hard systems are unconfirmed on virtual systems -- Is all data stored the same way?, what new info can we gather?, etc.)	23 (40%)

Table D7*: Top 3 Issues with Training in Cyber Forensics*

Answer	Frequency / Percentage (Total 57)
Continuous Training is needed (technology constantly changes = constant education of tools, equipment, and computer functions are needed)	51 (88%)
Cost of training (tech keeps changing so more and more training is required)	71 (41%)
Lack of training options and their availability	36 (21%)

Table D8*: Areas Impacted by Funding*

Answer	Frequency / Percentage (Total 57)
Training	20 (35%)
For new equipment and software	14 (25%)
Research Projects	12 (21%)
New hires	11 (19%)
Total	57 (100%)

Appendix E. Research Projects

The percentages in Table E1 are based off the 51 participants that answered the question. They are for reference only.

Table E1: *All Identified Research Projects*

Project	Frequency / Percentage (total 51)
On-site forensics and training on computer triages to increase proficiency in data extraction and time requirements.	37 (73%)
Cloud Computing investigation models, tools, and methods	39 (76%)
Distribution of digital forensics case processing load across several machines	17 (33%)
A Cell phone analysis application to interpret cell phone data-dump-report files by parsing them and providing the investigator with frequency results.	35 (69%)
Stand alone undercover cyber CPU in order to identify and catch Internet fraud perpetrators illegally soliciting healthcare products to consumers	4 (8%)
Operational view of the cloud system (no real data capturing has been needed yet)	19 (37%)
Working with the Department of Defense to bring some of their wireless investigation tools over to Law Enforcement	22 (43%)
Smart phones and pass lock options for analysis	28 (55%)
Hands-on course that focuses on Windows Forensic Examinations using EnCase (Students analyze a current image/hard drive and extract detailed information)	17 (33%)

Course on Mobile Device Forensics (This will combine mobile devices as well as network service provider data. There will be significant number of hands-on activities with current, state of the art tools.)	40 (78%)
Course development on network penetration testing with the focus being on conducting tests and determining the observable impact from a forensics point of view.	22 (43%)
Course development on virtual/cloud-based forensics	37 (73%)
Teaching methods to help teach the conceptual methods	22 (43%)
2+2 program building off an AS/AA program with good basic tech skills and then providing the forensic, legal, and operational digital forensics	13 (25%)
Developing free online training modules for Law Enforcement	31 (61%)
Professor feedback on what is effective and not - Not national (but could be)	4 (8%)
Curriculum development for a 4 year degree in CF	24 (47%)
Focusing on the legal and policy issues confronting cyber forensics and the gap that exists between what the several stakeholder groups hold to be best practice / highest need and what is actually being practiced	23 (45%)
A comparison of smart phone searches being legally authorized or considered intrusion	9 (18%)
Research for best antivirus for Windows 7	4 (8%)
Data Breach notification for Law enforcement and Cyber Forensics	13 (25%)
Creating partnerships with two product vendors to provide discounted products to students and faculty members.	6 (12%)
Recruiting college interns to research areas of encryption and proprietary software	13 (25%)

Creating an information repository for cyber forensics (to be included is research conducted and published, current research in development, communication avenues for experts and analysts, info on issues in the field for possible new research topics, etc)	31 (61%)

Appendix F. Cyber Forensic Experts

Table F1*: 5 Areas to have "Above Average Knowledge"*

Answer	Frequency / Percentage (Total 51)
Knowledge must be beyond "click-button forensics" (know how and why digital evidence is present)	43 (84%)
An understanding of File and Operating Systems (specifically how systems create/delete files and the system changes associated with that creating and deleting)	37 (73%)
Stay current with today's changes in technology and how they effect investigations	32 (63%)
Knows where to locate digital evidence	31 (61%)
Must be comfortable with searching the registry, capable of finding remnants of old searches, and past installed programs, etc	23 (45%)

Table F2*: Top 3 Types of Experience a Cyber Forensic Expert Should Have*

Answer	Frequency / Percentage (Total 51)
Someone who knows and has the experience to find forensic evidence without the use of automated tools	32 (63%)
Variety of computer types (Mac, Windows, Linux, etc)	26 (51%)
A cyber forensic expert should versed in all topic areas (child pornography, Internet Safety, intrusion detection, data recovery, etc.)	24 (47%)

Table F3*: Top 5 Reasons for a Lack of Qualified Individuals for Teach Cyber Forensics*

Criteria	Frequency / Percentage (Total 18)
Schools don't consider the experience and specialized training, only if they possess a higher education degree. (Therefore limiting the pool of possible candidates)	29 (62%)
Organizations and companies do not offer a high enough salary compensation to pay them for their expertise (therefore the qualified candidates don't apply)	27 (57%)
Candidates lack teaching ability / experience (They need to have the knowledge and experience to pass along information to others)	22 (47%)
Cyber forensic experts don't apply for the positions (Cyber Forensic experts should only be allowed to teach)	22 (47%)

Candidates' education level is not high enough	18 (38%)

Table F4*: Hiring Manager Preferences*

Answer	Frequency / Percentage (Total 51)
Job Experience	37 (73%)
Being trained (internship and/or apprenticeships)	11 (22%)
An academic degree	3 (6%)
Having Certificates	0 (0%)

Appendix G. Academia Issues

Table G1*: Top 10 Issues in Academia Related to Cyber Forensics*

Selection	Frequency / Percentage (Total 25)
Lack of good classes, instructors and programs (Many classes are needed to teach Cyber Forensics correctly, not just one or two.)	20 (80%)
Limited resources (tools and hardware for use for teaching and training)	18 (72%)
Programs are not concentrated enough (more classes are needed that are specific to Cyber Forensics)	18 (72%)
Limited lab exposure - Different cases (fraud, cloud, corporate, etc.)	16 (64%)
Lack of a diversity of subjects (examples: the community needs classes in hacking, network forensics, etc) -- without them, and others, it limits your knowledge base	16 (64%)
No educational standard (professors teach what they want)	16 (64%)
Cyber Forensics is not seen as a science or major, but more of an area of specialization within technology or science.	14 (56%)
More educational programs (example: How to conduct Cyber Investigations)	13 (52%)

Many schools have created forensics programs based on existing information security programs. They kept the original (IS) curriculum and added a sprinkling of courses to create a new program.	13 (52%)
Lack of practical experience (internships, projects, volunteering, etc)	13 (52%)

Table G2's percentages are based from the 31 participants that categorized themselves as academia. The percentages were included to show the number of votes casted for each issue.

Table G2: *Issues in Academia*

Issues	Frequency / Percentage (Total 31)
More educational programs (example: How to conduct Cyber Investigations)	13 (52%)
Lack of good classes, instructors and programs (Many classes are needed to teach Cyber Forensics correctly, not just one or two.)	20 (80%)
Lack of a diversity of subjects (examples: the community needs classes in hacking, network forensics, etc) -- without them, and others, it limits your knowledge base	16 (64%)
Classes don't teach a mindset so examiners can think outside the box and discover the new evidence	9 (36%)
Many schools have created forensics programs based on existing information security programs. They kept the original (IS) curriculum and added a sprinkling of courses to create a new program.	13 (52%)
Lack of training to teach how to apply the software and theories to actual cases and curriculum.	9 (36%)
Programs are not concentrated enough (more classes are	18 (72%)

needed that are specific to Cyber Forensics)	
Prerequisites of math and a foundations in computers before starting a concentration in Cyber Forensics is not required	5 (20%)
No educational standard (professors teach what they want)	16 (64%)
Teaching is based on theory rather than practical experience	5 (20%)
PhD's in Cyber Forensics need to be more focused on the field	4 (16%)
Lack of education (from those who know what to do)	3 (12%)
Lack of practical experience (internships, projects, volunteering, etc)	13 (52%)
Techniques taught do not allow for adapting to changing tech.	5 (20%)
Cyber Forensics is not seen as a science or major, but more of an area of specialization within technology or science.	14 (56%)
Cyber Forensics is not completely defined as to what college it should reside under, Computer Science or Technology.	7 (28%)
Education is training (it focuses on tools and scenarios) - it is not rooted in scientific research to support its concepts and principles	7 (28%)
Lack of funding for students to conduct research	12 (48%)
Limited resources (tools and hardware for use for teaching and training)	18 (72%)
No communication between universities to discuss research topics (to collaborate and prevent rework)	11 (44%)
Limited lab exposure - Different cases (fraud, cloud, corporate, etc.)	16 (64%)
The majority of courses in academia are theoretical, not hands-on.	9 (36%)
Programs teach what has happened; they are always trying to catch up.	7 (28%)

Table G3 asked participants to identify the degrees they have acquired. If a participant was still in process for a selected degree than the participant was suppose to check "in progress" as well. This led to a confusing results table, as it cannot be determined what degrees are in progress and what percentages of participants only have lower degrees vs. the higher. For example, if a participant has a PhD, they would have selected Master's and Bachelor's in addition to PhD. Therefore, if only three people had a bachelor's out of the entire group (10 for this example), then the Bachelor's percentage would be 100%. Which is true, but now it cannot be determined who only has a Bachelor's, which should have read 30%.

This issue was identified in the conclusion as ways for improvement; it needed more control.

Table G3: Years Studying the Cyber Forensic Field

	Number of years											
	1	2	2.5	3	4	5	6	10	13	14	25+	Total
Frequency (Percentage)	1 (4%)	2 (9%)	1 (4%)	3 (13%)	6 (27%)	2 (9%)	1 (4%)	3 (13%)	1 (4%)	1 (4)	1 (4%)	22 (100%)

Table G3: *Education Table*

Degree	Frequency	Percentage
Associates	1	1 (4%)
Bachelor's	8	8 (31%)
Master's	14	14 (54%)
PhD	10	10 (38%)
Other (certificates, training, etc)	7	7 (27%)
In progress	16	16 (62%)

Note: 26 out of 31 academic participants responded to this question

Note: "Other" was an option for this question. Participants would select this if they had specific training or certifications. Some examples are (SANS, NTI, ACE, GCFA, CISP, CCE, DFC, etc.)

Table G4 contains info from a follow up questions to G3. 31 participants identified themselves as Academia but only 17 responded to the following questions.

Table G4: *Future Degrees Breakdown*

Question	Yes	No	Total
If, respondent had a Bachelor's, would they continue for their Masters?	1 (33%)	2 (67%)	3
If, respondent had a Master's would they continue for their PhD?	9 (64%)	5 (36%)	14

Note 1: It could be determined that there were only 3 participants that had a Bachelor's degree and were not working towards a higher level of education. This can be speculated since only 3 responses were recorded while asking the respondents if they were going to pursue a Master's degree after their Bachelor's. However, the number could still be inaccurate as participants could still skip any question.

Note 2: The second question is a combination of 2 questions. The first question was presented to a respondent if they selected they were working on, or had, a Bachelor's degree and did not have a higher education level selected. They were then asked if they were going to pursue a Master's degree, and if they said yes, another question displayed asking if they were going to pursue a PhD. The second question was only presented if the participant selected they were working on, or had, a Master's Degree and did not have a higher education level selected. The survey then asked if they were going to pursue a PhD. As these two questions yield the same kind of results, they were combined in Table G4.

Appendix H. Law Enforcement Issues

Table H1: *All Identified Issues Specific to Law Enforcement*

Issues	Frequency / Percentage (Total 26)
Education on Cyber Forensics	8 (31%)
More programs to focus on practical issues and law enforcement	1 (4%)
Cost Effective tools for Law Enforcement	18 (69%)
Lack of commitment (teams don't do the research beforehand - they begin investigations before the team is ready)	0 (0%)
Lack of manpower (more work than people)	16 (62%)
Overwhelming case work load (too much stresses the examiner out)	13 (50%)
Lack of prosecution for malicious behavior	2 (8%)
Limited recourses (tools and hardware)	9 (35%)
Other duties (boss says to work on XYZ, you have to stop your work on ABC)	6 (23%)
Supervisors (from other areas in department that don’t understand the process)	1 (4%)
Hard to find a position in law enforcement as Law Enforcement wants officers to fill the role as the forensic analysts, not civilians.	4 (15%)

Table H2: Types of Systems Analyzed

	Systems							
	Windows	Mac (Apple)	Unix/Linux	PDAs	Cell Phones	Game Consoles	ipods/Media Players	Other
Frequency / Percentage (Total 26)	26 (100%)	20 (77%)	14 (54%)	12 (46%)	20 (77%)	9 (35%)	13 (50%)	7 (27%)

Table H3 shows what systems are analyzed the most in cases. However, some participants picked more than one system for their "Majority". The only explanation for this, aside not following directions, is that the multiple systems selected indicate equally distributed time. No matter how unlikely that is.

Table H3: Majority of Time Spent on

System	Frequency / Percentage (Total 25)
Windows	25 (100%)
Cell Phones	8 (32%)
PDAs	1 (4%)
Mac	1 (4%)
Unix/Linux	0 (0%)
Game Consoles	0 (0%)
ipods/media players	0 (0%)
other	0 (0%)

Table H4: Years participating in the Cyber Forensic Field

Years	Frequency (Percentage)
1	1 (4%)
1.5	1 (4%)
2	4 (15%)
3	2 (8%)
4	2 (8%)
5	3 (12%)
7	3 (12%)
8	2 (8%)
10	2 (8%)
11	1 (4%)
13	2 (8%)
14	1 (4%)
16	1 (4%)
18	1 (4%)
Total	26 (100%)

Table H5: Certificates Held by Law Enforcement

ACE	Cell Phone Forensic Examiner
EnCe	Mobile Phone Repair
CFCE	UFED Mobile Device Examiner
CEECS	Microsoft MCP
IACIS	Comp TIA
Cellibrite	Cell Phone Forensic Examiner
SCERS	MDIP
CNITP	FLETC
A+	CISA
DEASTP	

Note: Be sure to see Table H11 for more certifications and classes.

Table H6*: Software Used by Law Enforcement*

EnCase	Live View	Internet Evidence Finder (IEF)
FTK	Intella	Paraben Device Seizure
SMART	Blacklight	Blackbag
TUX	Wetstone	MacMarchall
Knoppix	ImageScan	Net Analysis
Helix	RegistryViewer	Cellebrite
ProDiscover	ufed	Scalel
WinHex	Photorec	DataPilot
Device Seizure	Vmware Server	BitPim
SecureView	US-LATT	CheckBack
Oxygen	osTriage	Sand Box Tools
DaataLifter	Susteen	RegRipper

Table H7 shows if cyber crime units are typically a one-man effort or a team effort. Out of the 27 Law Enforcement respondents only 2 (8%) were the sole investigator. However, this number could be considered slightly skewed. If a member in a team agreed to participate in the study, it is feasible the rest of the team did so as well. Therefore, it is important to note that the results in Table H7 do not represent 24 different *teams* in Law Enforcement that conduct Cyber Forensic Investigations.

Table H7: *Law Enforcement Cyber Crimes Units*

	Type of Team		
	Only Investigator	Member of a Team	Total
Frequency (Percentage)	2 (8%)	24 (92%)	26 (100%)

Table H8: *Skills Acquired*

Type	Frequency / Percentage (Total 26)
Self taught	17 (65%)
Education (college, trade school, etc.)	10 (38%)
Training	25 (96%)
Certification	16 (62%)
Other	7 (27%)
In progress	4 (15%)

Table H9 was a follow-up question to the "Education" criteria from Table H8 to clarify its meaning.

Table H9: *Education Breakdown*

Type	Frequency / Percentage
High School	1 (4%)
2-year Associates	0 (0%)
Trade School completion	9 (0%)
4-year Bachelor's	13 (54%)
Masters	9 (38%)
PhD	1 (4%)
Total	24 (100%)

Table H10 was a follow-up question to the "Training" criteria from Table H8 to clarify its meaning.

Table H10: *Law Enforcement Training Types*

Type	Frequency / Percentage (Total 23)
Self-taught	14 (61%)
Some schooling (no degree)	11 (48%)
Mentor	14 (61%)
Other	12 (52%)

Table H10 had the same issues for evaluating the data as Tables G3 and G4. See their notes in Appendix G for more clarifying details.

Table H10 was a follow-up question to the "Training" criteria from Table H8 to clarify its meaning.

Table H11: Certificates Held by Law Enforcement

Category	Type	
Certifications	OTJ	BDRA
	IDRA	ADRA
	STOP	dBase III
	MS Access	FLETC
	IACIS	CFCE
Courses Offered	BlackBag (Mac)	Encase Specific
	National White Collar Crime Center	New Technologies INC
	Cell Phone	Basic DOS Forensics
	Specialized tools by SEARCH	Internet History
	Computer Forensics	Microsoft Office
	Tech. College	Professional
	Software Guidance Training	Internet Crimes Against Children (ICAC)
	Wyoming Tool Kit	Child Protection System (CPS)
	DOD training	Vendor training by Guidance Software Ver.s 3-6

Note 1: Many participants gave categorical responses that were not specific. These included: other vendor specific, vendor neutral, on the job experience, classroom, online, certifications, proficiency and competency testing, webcast, college coursework, forensic, ASCLD/LAB, laboratory, internal, external, mock, mentoring, and instructional. As there was not enough time to conduct a follow up for these answers, they could not be clarified.

Note 2: Some of these are overlapped form Table H5: *Certifications held*. They were not grouped because of the amount of difference between the two responses.