3-1-2016

A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later

Vikram S. Harichandran
University of New Haven

Frank Breitinger
University of New Haven

Ibrahim Baggili
University of New Haven

Andrew Marrington
Zayed University

Recommended Citation

Harichandran, Vikram S.; Breitinger, Frank; Baggili, Ibrahim; and Marrington, Andrew, "A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later" (2016). *All Works*. 79.
https://zuscholars.zu.ac.ae/works/79

3-2016

A Cyber Forensics Needs Analysis Survey: Revisiting the Domain's Needs a Decade Later

Vikram S. Harichandran
University of New Haven

Frank Breitinger
University of New Haven, fbreitinger@newhaven.edu

Ibrahim Baggili
University of New Haven, ibaggili@newhaven.edu

Andrew Marrington
Zayed University

Publisher Citation

Vikram S. Harichandran, Frank Breitinger, Ibrahim Baggili, Andrew Marrington (2016). A cyber forensics needs analysis survey: revisiting the domain's needs a decade later. Computers & Security 57, March 2016, pp. 1-13. doi:10.1016/j.cose.2015.10.007

Comments

This is the peer reviewed version of the following article: Vikram S. Harichandran, Frank Breitinger, Ibrahim Baggili, Andrew Marrington (2016). A cyber forensics needs analysis survey: revisiting the domain's needs a decade later. Computers & Security 57, March 2016, pp. 1-13 which is published in final form at http://dx.doi.org/doi:10.1016/j.cose.2015.10.007. This article may be used for non-commercial purposes in accordance with the CC/BY/NC/ND license.
Dr. Ibrahim Baggili was appointed to the University of New Haven's Elder Family Endowed Chair in 2015.

A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later

Vikram S. Harichandran[a], Frank Breitinger[a,*], Ibrahim Baggili[a], Andrew Marrington[b]

[a] *Cyber Forensics Research and Education Group (UNHcFREG)*
Tagliatela College of Engineering, University of New Haven, West Haven CT, 06516, United States
[b] *Advanced Cyber Forensics Research Laboratory*
Zayed University, United Arab Emirates

Abstract

The number of successful cyber attacks continues to increase, threatening financial and personal security worldwide. Cyber/digital forensics is undergoing a paradigm shift in which evidence is frequently massive in size, demands live acquisition, and may be insufficient to convict a criminal residing in another legal jurisdiction. This paper presents the findings of the first broad needs analysis survey in cyber forensics in nearly a decade, aimed at obtaining an updated consensus of professional attitudes in order to optimize resource allocation and to prioritize problems and possible solutions more efficiently. Results from the 99 respondents gave compelling testimony that the following will be necessary in the future: (1) better education/training/certification (opportunities, standardization, and skill-sets); (2) support for cloud and mobile forensics; (3) backing for and improvement of open-source tools (4) research on encryption, malware, and trail obfuscation; (5) revised laws (specific, up-to-date, and which protect user privacy); (6) better communication, especially between/with law enforcement (including establishing new frameworks to mitigate problematic communication); (7) more personnel and funding.

Keywords: Computer forensics, Cyber forensics, Digital forensics, Mobile forensics, Needs analysis, Open source, Privacy, Research, Survey, Tools.

1. Introduction

With the rising presence of digital devices, information repositories, and network traffic, cyber forensics (a.k.a. digital forensics) faces an increasing number of cases having ever-growing complexity (Al Fahdi et al., 2013). The large volume of data and the deficit of time needed for examination have placed pressure on the development of real-time solutions such as criminal profiling systems, triage automation, and tools capable of recovery-processing parallelization. These main challenges have rippled across the field introducing and building upon obstacles related to cyber forensic resources, education/training/certification (ETC), tools & technology, research, laws, and subdomains.

Needs analysis is one type of assessment tool used for identifying areas that members of a community view as challenging. Performing them periodically is essential to adjust for fluctuating trends. Some of the benefits of needs assessment include improved resource allocation, better efficiency, informed decision-making, the generation of a professional consensus, and increased awareness of unaddressed problems and possible solutions.

The last general needs analysis survey on cyber forensics was conducted by Rogers & Seigfried (2004), titled "The future of computer forensics: a needs analysis survey." Since the publication of the original study, only subdomains have been assessed. Our study was performed to obtain an updated consensus of the cyber forensics community's opinions in order to more extensively identify and prioritize problems and solutions.

We present the feedback of 99 respondents to our 51-question survey which, among others, strongly motivates the need for more funding and personnel; better ETC, tools, and communication; updated laws; and research on cloud and mobile forensics. We further performed a direct comparison to the 2004 survey results.

This paper is divided into 6 major sections. First, we present a summary of challenges & recent findings in Section 2. In Section 3 we briefly outline the methodology, followed by a short survey section. The core of this paper is Section 5, which includes the results. Next, Section 6 discusses the implications of the results. Then the limitations are stated. Main findings and future follow-up can be found in Section 8.

2. Summary of challenges & recent findings

Despite a general public concern for cyber security, the technological response, frameworks, and support are lagging behind the escalating rate of crime. The PricewaterhouseCoopers (PwC) 2014 Global Economic Crime Survey reported 7% of U.S. organizations lost \$1 million or more due to cybercrime in 2013, and 19% of U.S. entities lost \$50,000 to \$1 million. Global equivalents of these financial ranges of loss were 3% and 8%, respectively (Mickelberg et al., 2014).

[*] Corresponding author.
Email addresses: vhari2@newhaven.edu (Vikram S. Harichandran), fbreitinger@newhaven.edu (Frank Breitinger), ibaggili@newhaven.edu (Ibrahim Baggili), andrew.marrington@zu.ac.ae (Andrew Marrington)

Accumulation of financial loss is not the only worry as recently shown with the Sony hack in which a group of hackers calling themselves the Guardians of Peace gained access to Sony systems and threatened violence on company employees if the movie 'The Interview' was released. Threat of terrorism caused the banning of the movie in nearly 20,000 theaters in North America (Dickson, 2015). As mirrored in the PwCs Annual Global CEO Survey of 2014, CEOs and executive boards must now be concerned with such risks lest denial-of-service attacks and damaged image effect company survival (Mickelberg et al., 2014). In the foreseeable future, the Internet of Things (IoT) will likely be just as much of a concern. Automobiles and other electronically enhanced devices will form new risks to individuals, businesses, and governments.

Due to such cyber incidents, the area of cyber forensics has gained ample publicity over the recent years as it becomes more important to analyze and understand breaches. In the following subsections we summarize the state of the art cyber forensics practices and research.[1] First, however, the previous general needs analysis survey is described.

2.1. *Rogers & Seigfried survey*

The first and only needs analysis survey conducted by Rogers & Seigfried (2004) consisted of a single question asking participants to list what they viewed as the top five issues in computer forensics (computer forensics was more synonymous with cyber forensics then). Responses were tallied into high-order categorizations, exhibiting the following order of frequency (from most mentioned to least):

1. Education/training/certification
2. Technologies
3. Encryption
4. Data acquisition
5. Tools
6. Legal justice system
7. Evidence correlation
8. Theory/research
9. Funding
10. Other

These categories were used in our study to directly assess how the understanding of challenges changed over the last decade. Since the time of the preliminary paper, many new challenges have emerged.

2.2. *Resource allocation & education / training / certification*

Although a variety of crimes can be committed using digital devices (violent crimes, terrorism, espionage, counterfeiting, drug trafficking, and illicit pornography to name a few) the largest driving force for cyber forensics is crime related to financial security. A survey conducted by the Ponemon Institute indicated the average cost of cybercrime for United States retail stores in 2014 ($8.6 million per company) was more than double that of 2013 (Walters, 2014). Estimations only account for publicly disclosed figures. We posit that reported numbers from surveys are likely to be underestimations because of their voluntary nature. Prevention is clearly not working, which reflects the accumulation of cases.

Consequently, the question of whether there are enough forensic practitioners arises, which can only be answered with speculation as no recent studies have attempted to quantify this; personnel, as a resource, was evaluated in our survey. General conjecture is that more cyber forensic scientists and professionals are needed to appease the amount of cases. This is partially backed by a 37% projected increase in employment of information security analysts (this category encompasses cyber forensics practice) from 2012 to 2022 (Bureau of Labor Statistics, U.S. Department of Labor, 2014). Funding may need to increase or be reallocated as these jobs are put on the market. Additionally, in part due to the variety of both cases that practitioners deal with and the methods they use to analyze the evidence, there is still no standardized certification for examiners (Srinivasan, 2013). Instead, professionals usually obtain tool-specific certifications. The same can be seen in law enforcement and judicial courts. A recent study supported by the National Institute of Justice (NIJ) indicated that first-responding officers often do not know how to properly secure digital evidence, and that prosecutors have a tendency to request all information from devices without considering their physical storage size (Goodison et al., 2015). Such a diverse and likely insufficient large pool of personnel urges the creation of faster and more efficient tools and technology to improve case processing.

2.3. *Tools & technology*

In the past, tools tended to be technology-oriented, inconveniencing non-technical users, and lacked user-friendly, intuitive interfaces (Reith et al., 2002). Today, investigating simple questions such as whether two people were in contact and which websites a person has visited still requires too much time and effort. Usually, following complex leads result in the case being handed on to more experienced, specialized investigators. Tool usability and reporting is an important issue because "misunderstanding that leads to false interpretations may impact real-life cases" (Hibshi et al., 2011). Furthermore, recent work has illustrated that tools still lack standardized reporting mechanisms, and even though research has been conducted on this front, the tools have not adopted a standard for digital evidence items (Bariki et al., 2011). The young, incompletely explored open-source landscape needs further inquiry as well because there is powerful functionality to be gained from tools tested, validated, and constantly updated via communal repositories or trusted open-sourced centers (Greek, 2013).

Two other approaches being worked on to improve tool efficiency is implementation of automation and real-time processing technology. Triage automation is considered by some to be essential for dealing with the increasing number of cases (Garfinkel, 2013). The plethora of photos created every day illustrates the need for automation. Photo doctoring is becoming commonplace yet automation of image forgery detection

[1] For more background reading on the current standards see Darnell (2012).

is still not possible (Birajdar & Mankar, 2013). Automation could be critical in the future as instances of slander and false evidence increase. Indeed, earlier this year a new Stegosploit tool demonstrated malicious, self-executing code could be hidden within pictures (Harblson, 2015). On the other hand, mobile and flash memory devices (including video game consoles and eBook readers) have resulted in quick evidence deletion. To combat this, memory forensics, real-time detection, and parallel processing research has surfaced. Parallel processing would be most beneficial in these areas: traffic generation (network models), imaging and carving processes, and development of user history timelines (Nance et al., 2009). Finally, it is unclear how to separate user/owner privacy and identification from thorough investigations, and this seems to be a topic of increasing interest (Aminnezhad et al., 2012).

2.4. Research

Research is an essential component in this period of changing focus but may not be achieving ideal output. Scientific journals within the field are relatively new, exhibiting "low ISI impact factors, circulation rates, and acceptance rates" - journals will need time to mature (Beebe, 2009). Experiments are rarely reproducible because of the lack of corpora, or standardized data sets, made available along with publications, which could also explain why mainstream journals lack interest in the domain's research (Garfinkel et al., 2009). There is a disconnect between practitioners and researchers. Despite their different roles in the field, research should support the desires of those practicing evidence recovery and examination. A survey by Al Fahdi et al. (2013) marked that practitioners were concerned with anti-forensics and encryption as future challenges while researchers worried about tool capability and social networking. Difference in opinion may be caused by the particular problems these two groups handle, but this disparity should not be present (ideally) when determining prioritization of research topics or funding. Whether this is currently the case is unclear. This disconnect can also be thought of as a failure for research to affect end users as discussed by Garfinkel (2010).

Baggili et al. (2013) studied cyber forensics research trends by analyzing 500 papers from the domain and categorizing them. The overall results indicated that the rate of publication in cyber forensics continues to increase over time. Additionally, results showed an overall lack of anti-forensics research where only 2% of the sampled papers dealt with anti-forensics. The results also showed that 17% of the samples were secondary research, 36% were exploratory studies, 33% were constructive and 31% were empirical. One important finding was the discovery of a lack of basic research, where most of the research (81%) was applied, and only 19% of the articles were categorized as basic research. Also, the results exemplified a shortcoming in the amount of quantitative research in the discipline, with only 20% of the research papers classified as quantitative, and the other 80% classified as qualitative. Furthermore, results showed that the largest portion of the research (almost 43%) from the examined sample originated from the United States. In summary, some of the identified challenges, and their associated needs, in cyber forensics research are not fully understood.

2.5. Law

Whatever the progress made in researching better solutions and improving tools, practitioners are limited by what they can and cannot do by law, and the evidence they find may not convict a criminal (Hack In The Box Security Conference, 2012; Dardick, 2010). Ransomware is a prime example of the effective means criminals now possess to anonymously and rapidly cash out (European Cybercrime Center, 2014). In the case of cloud forensics, research needs to be conducted to show the true impact of clouds on cyber forensics before frameworks and guidelines can be established (Grispos et al., 2013). However, in most cases there is ample evidence showing laws are outdated. The subdomain of cloud forensics has proven the need for new laws related to proactive collection of data and multi-jurisdiction laws (Ruan et al., 2013). A comprehensive international decree, possibly headed by the United Nations (U.N.), is imperative. According to Barwick (2014), currently "data sovereignty laws hamper international crime investigations" and although the U.N. adopted a surveillance proposal in 2013 more forensic-oriented laws are still deemed necessary.

Of course, in addition to these laws judges themselves must be educated and trained, since they are responsible for determining what types of digital evidence are allowed in their courts and how they are used for incrimination. These decisions are mostly guided by three pieces of legislation: *Daubert v. Merrel Dow Pharmaceuticals, Inc.* (1993), *Kumho Tire v. Carmichael* (1999), & FRE Rule 702. A small, yet thorough study (Kessler, 2010) involving a survey and interviews established that judicial education systems are lacking for digital evidence; judges themselves rated their knowledge of computer forensics as less than computer and Internet technology.

2.6. Communication

In response to a survey of Australia's finance and insurance industry there was a high no-incident and no-response rate (around 83%) when companies were asked about their most significant computer security incident (Choo, 2011). This suggests victims may not be aware they have been successfully attacked or that private companies are reluctant to report victimization. If the latter is true, a framework for anonymous reporting may be useful. Also, as mentioned in Section 2.4, differences in opinion between practitioners, researchers, law enforcement, and non-forensic entities may occur natively due to their different roles but little to no research has been conducted into whether this is due to faulty communication.

2.7. Urgency of closing the gaps

The end of the "Golden Age" of cyber forensics, as described by Garfinkel (2010), has quickly outdated many methods used by examiners, causing a paradigm shift with unclear direction. Some of the major concerns include standardization, researching new methods to speed up evidence recovery and analysis (proactive cyber forensics), support for non-traditional devices, and bringing about cheaper tools that support a wider variety of purposes (whether they are all-in-one or bolster a specific function). Although the field is on its way to making some changes, many obstacles such as the ones described in the above subsections prevail. Disregarding the rapidly increasing (successful) crime rate, the need to determine the direction of research, practice, and laws is vital. Cyber forensics' growth will continue to be stunted until these challenges are concretely addressed.

3. Methodology

To complete this work, the following high-level methodology was employed:

1. Performed a literature review (main findings are mentioned in Section 2) and survey design.
2. Obtained a category two exemption from the Institutional Review Board (IRB) at the University of New Haven (this meant that the survey did not record participant identification information or behavior, and posed no risk or harm to subjects not encountered in every day life).
3. Distributed the survey via list servers, LinkedIn cyber forensics groups, Twitter, and e-mail contacts.
4. Obtained data by exporting the coded responses to XLSX and CSV files from the Baseline survey system.
5. Analyzed the data using statistical probability, power tests, and crossing non-demographic questions with demographics and each other.

4. Survey design

The questions were formulated based on typical needs assessment topics, the Rogers & Seigfried (2004) survey, critical areas from the literature review that were unknown or deserved further investigation, and our interests. The survey went through three drafts, followed by a brief testing phase, in which three experts within the field were consulted to refine the wording, content, and formatting of the survey.

Needs assessment is a systematic process for determining gaps between the *status quo* and the desires of those within a community. Consequently, survey questions were designed to identify unmet desires rather than explicitly obtain statistics on the current state of the field. The survey consisted of 51 questions:

- 28 Likert scale
- 13 multiple choice
- 7 multiple selection (checkbox)
- 2 free response
- 1 ranking

According to IRB practices at our institution, participants could not be forced to answer any single question.

A general cyber forensics audience was targeted for the survey because of the researcher-practitioner discrepancies mentioned before (Section 2.4), to obtain as unbiased and wholesome a perspective as possible (for instance, if asked a group may likely blame another group rather than themselves for poor communication, or state their area is underfunded), and to understand how motivated people are to join such areas (e.g. hypothetically, if academia/research was found to be underfunded less people might find the domain desirable, which would be a problem if more employees were needed in this domain).

5. Results

The survey was available online for one month before data were exported from the system. Ninety-nine participants submitted responses. The calculated required sample size was 76 indicating that the number was large enough to make inferences from and that statistical tests were unlikely to exhibit type II errors (two-sided t-test, alpha = 0.05, using a medium effect size of 0.5 and power of 0.99). It should be noted that we aspired to obtain a higher response rate, but taking into account the relative size of the cyber forensics domain compared to cyber security in general, we deemed the sample size acceptable.

We would like to point out that although websites (e.g., the Digital Forensics Training on LinkedIn or the First Forensic Forum[2] (F3)) have hundreds or thousands of members, we do not believe citing the number provides a good estimation of the size of the domain – people in LinkedIn groups often are there to observe or self-promote, and may not be active members of the community. A reasonable approach to analyze the number of practitioners would be to count all degree holders of organizations that provide certifications. However, organizations as such do not publicly release statistics on how many professionals are trained or end up as practitioners in the domain.

This section's structure reflects that of Section 2, preceded first by an overview of the demographics and a comparison with the 2004 survey. Figures and tables related to this section using percentages may not sum exactly to 100% due to rounding error.

5.1. Demographics

The results of the demographics questions are presented in Table 1. It shows that most respondents were American (54%), 25-54 years old, had 11 years or more of experience, and had most experience in computer (disk) and mobile forensics. Albeit ages of respondents were evenly spread between age groups from 25 to 54, the years of experience participants reported were uneven, showing peaks at 2-4 years and 11 years or more. Just over half of the respondents were practitioners and most belonged to private organizations not related to the government or law enforcement. Because 28% said they work within education/training/certification (ETC) and over 50% were practitioners there is a chance some trainers and educators may be practitioners as well.

[2] https://www.f3.org.uk (last accessed 2015-08-10).

	Percentage
Region of residence	
North America	56.7
Europe	23.7
Middle East	7.2
South Asia	6.2
East Asia	2.1
Australia	2.1
Russia	2.1
Age	
18-24	6.3
25-34	25.3
35-44	24.2
45-54	25.3
55-64	14.7
65 or older	4.2
Gender	
Female	14.9
Male	85.1
Years of experience in cyber forensics	
0-1 years	11.5
2-4 years	25.0
5-7 years	16.7
8-10 years	11.5
11 years or more	35.4
Primary occupation	
Industry instructor	3.1
Law enforcement practitioner	20.8
Non-law enforcement practitioner	33.3
Professor	14.6
Researcher	16.7
Student	11.5
Occupation category	
Education/training facility/university	28.1
Federal/national law enforcement	7.3
State/local law enforcement	15.6
Military/national security	1.0
Legal system	3.1
Private organization that doesn't fit into any of the above	37.5
Public organization that doesn't fit into any of the above	7.3
Fields of expertise	
Crime scene investigation (first responding)	11.9
Cloud forensics	3.5
Computer (disk) forensics	28.8
Database forensics	1.5
Memory forensics	5.4
Mobile forensics	18.5
Multimedia forensics (audio, video, image, etc.)	5.8
Network forensics	13.5
Software/malware forensics	9.6
Non-traditional forensics (game consoles, printers, etc.)	1.5

Table 1: Not all participants answered the demographics questions but the lowest number of respondents for any one question was 94, meaning most did.

5.2. *Comparison to Rogers & Seigfried survey*

One of the main purposes of our survey was to determine how the view of future challenges within cyber forensics had changed since the Rogers study (Section 2.1). A single question asked participants to rank the categories that were formed in the 2004 survey with the results showing the following order according to calculated average rankings:

1. Education/training/certification (ETC)
2. Technologies
3. Tools
4. Evidence correlation
5. Theory/research
6. Encryption
7. Legal/justice system
8. Data acquisition & Funding (tied)

The data were analyzed via a Friedman test[3], determining that there is a significant difference among the 9 categories within a 95% confidence interval. The top two categories (ETC and Technologies) did not change when compared to the earlier survey. However, encryption moved down 3 places, while evidence correlation and theory/research moved up 3 places; this may reflect the current interest in producing automated and new technologies in the field.

5.3. *Resource allocation*

As shown in Figure 1, the types of resources having the strongest correlation to being insufficient were personnel and funding. Interestingly, in the Likert scale questions ETC and funding had similarly strong correlations while the ranked question (Section 5.2) had a clear separation of the two resources (ETC at top and funding at bottom). This may be due to the question format.

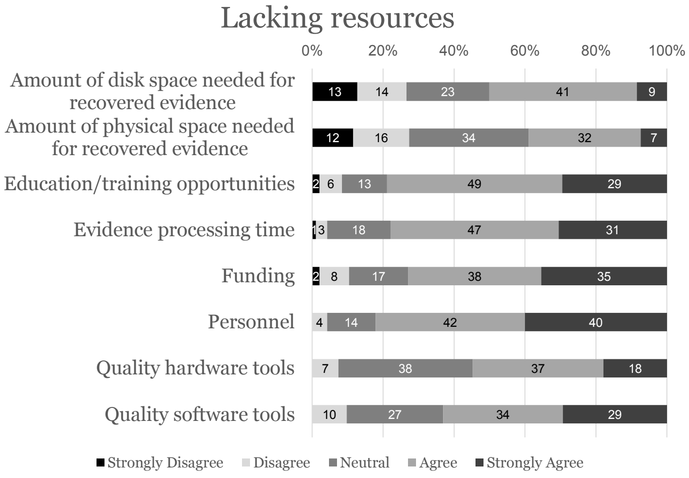

Figure 1: Each bar represents one Likert scale question. Approximate percentages are displayed for each answer selection.

Unexpectedly, 78% of those who thought public organizations needed more funding were non-law enforcement practitioners (Figure 2)[4]. About half of those who chose federal/national law enforcement were law enforcement practitioners. No bias was observed in the other categories.

[3] https://en.wikipedia.org/wiki/Friedman_test (last accessed 2015-08-10).

[4] Chi-squared test, p = 0.005.

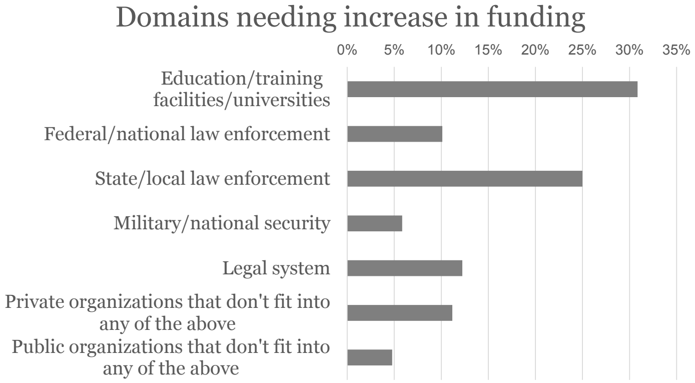

Figure 2: This multiple selection checkbox question allowed for respondents to select up to 2 of the answers shown above.

Thirty-four people responded to the practitioner-oriented free response question asking to list types of cases personally encountered that need further support/attention. Cloud/database forensics was mentioned 7 times, mobile forensics 6 times, and non-traditional devices 6 times (satellite, navigation, CCTV systems & game consoles; especially development of tools for these scenarios). Other concerns involved more support for Linux & Mac systems at law enforcement offices, timeline/profiling tools, and chip-off forensics. The concern for mobile support was echoed in another question asking which operating systems needed more support in respect to cyber forensic cases (about 24% selected each Android and iOS, while all other systems were below 12%).

5.4. *Education/training/certification*

As seen in Figure 3, the majority of respondents clearly thought state/local law enforcement needs more ETC opportunities. This was mirrored in the practitioner free response where a few respondents mentioned law enforcement & three letter agencies need more education on basics like Domain Name System (DNS) and working with Internet Service Providers (ISPs) or hosting companies.

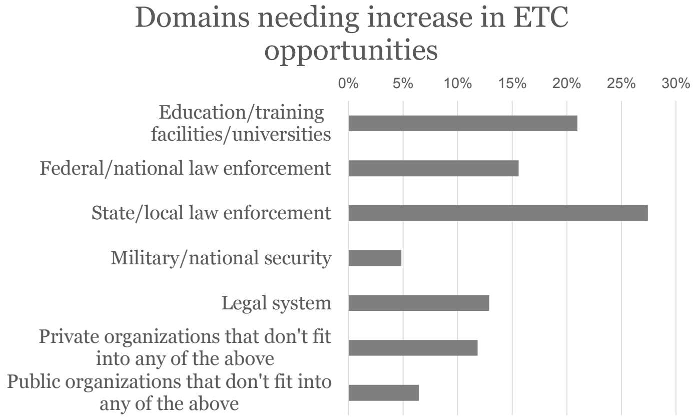

Figure 3: This multiple selection checkbox question allowed for respondents to select up to 2 of the answers shown above.

The high desire for more ETC opportunities for the education/training facilities/universities category can be interpreted as a need for more cyber forensics programs at universities and offered certifications at training facilities. This concern was less prevalent among Europeans than North Americans; the second most frequent choice for Europeans was federal/national law enforcement rather than ETC. Legal system was selected relatively frequently, which was an outstanding observation considering it was among the smallest occupational demographics.

Figure 4 implies practitioners need to know how to use tools, but this is only complementary to a thorough understanding of the forensic process/investigative skills. Reverse engineering also was expressed as a valuable skill for the future, possibly because the plethora of software being developed is increasing and may need some level of reverse engineering to help examiners gain access to evidence. This could be explained by reverse engineering being innately time intensive, thus requiring more experts to combat recovery time. Or it may be a prerequisite for mobile forensics when encountering devices that are not supported by mobile acquisition and analysis toolkits given their proprietary nature.

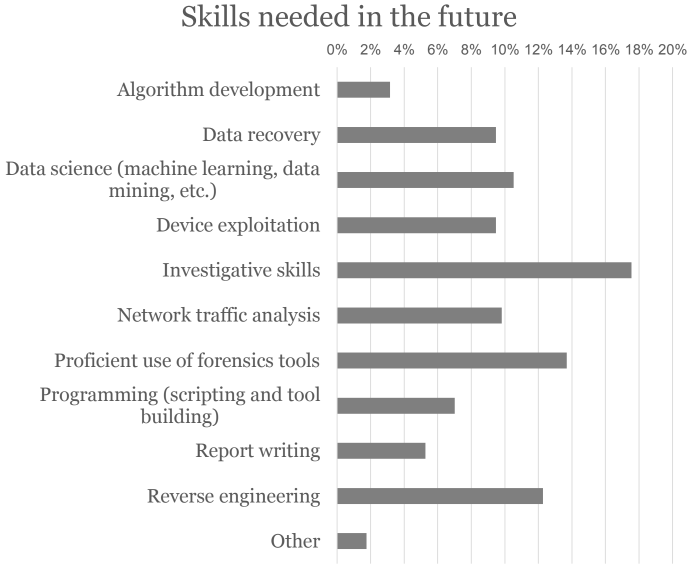

Figure 4: This multiple selection checkbox question allowed for respondents to select up to 3 of the answers shown above.

5.5. *Tools & technology*

The Likert scale questions in Figure 5 clearly show that open-source tools are not meeting the desires of professionals. They need to be both better and funded adequately. Most participants also indicated that commercial tools should be cheaper.

The checkbox question in Figure 6 shows that mobile and cloud forensic tools and technology need improvement most. North Americans were most concerned with mobile forensics while Europeans were most concerned with cloud forensics. This could be construed as a result of these domains being newer and currently experiencing rapid growth. Alternatively, it could be that in Europe there is a larger concern with cloud forensics given their typically more stringent privacy concerns when compared to the United States.

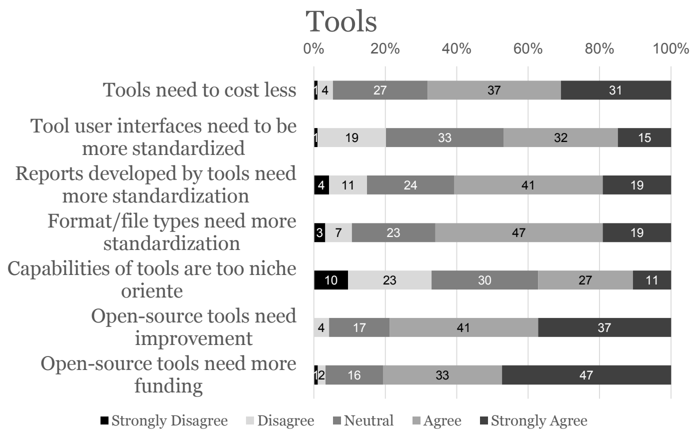

Figure 5: Each bar represents one Likert scale question. Approximate percentages are displayed for each answer selection.

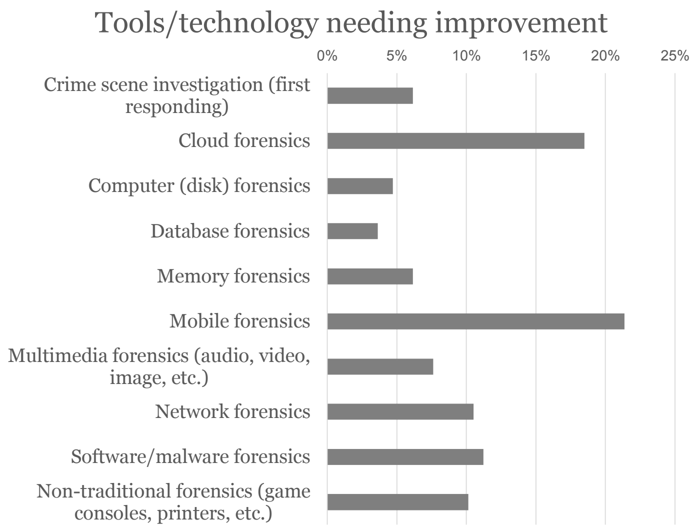

Figure 6: This multiple selection checkbox question allowed for respondents to select up to 3 of the answers shown above.

Two multiple choice questions were used to assess the use of hashing algorithms which are commonly used in digital forensics. About 42% of respondents claimed they use MD5 the most (another 40% split evenly between SHA1 and SHA-256). We noticed that older respondents were more likely to use MD5 the most. Despite being considered flawed, practitioners most likely use it because it is fast, short, and the only option in some software. However, this phenomenon could also be due to being unaware of its flaws, or not regarding MD5's flaws significant enough for their purposes or being not aware of newer developments.

To proof our statement that many people are not aware of/avoid new technologies, we asked about approximate matching, a.k.a. similarity hashing or fuzzy hashing, which is a rather new field. Although a definition was only published in 2014 (Breitinger et al., 2014), the first algorithm `ssdeep` came out eight years earlier (Kornblum, 2006). Only 13% of respondents use these algorithms on a regular basis while 34% only had used them a few times before. Thirty-one percent said they had not used them because they were not necessary for their purposes, 7% reported they are too slow for practical use, and 15% did not know what similarity hashing was. Europe is ahead in adopting this technology (68% of Europeans had used it before compared to only 40% of North Americans).[5]

5.6. Research

The Likert scale questions about research (Figure 7) indicated a strong need to research encryption, malware, and trail obfuscation countermeasures. Criminal profiling systems, data wiping, and evidence displayed opinions closer to a neutral standpoint.

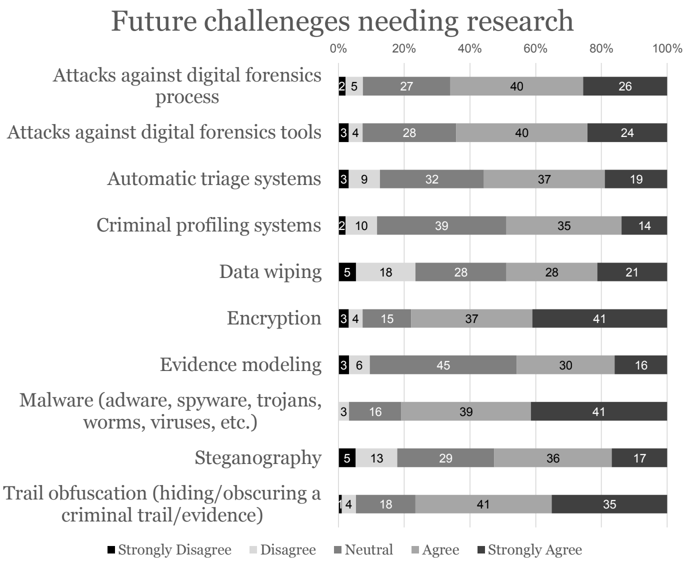

Figure 7: Each bar represents one Likert scale question. Approximate percentages are displayed for each answer selection.

A free response research-oriented question investigated what topics participants thought will be most important to research in the next 5-10 years. The 35 answers most frequently mentioned cloud forensics (10 times) and mobile forensics (6 times). Other common mentions were malware, encryption, solid state drives, and network forensics (the prior two concerns reflected in the Likert scale questions). A few respondents also expressed worry for the future of the Internet of Things/embedded devices.

5.7. Laws

There was an overwhelming consensus that laws pertaining to cyber forensics are out of date, as shown in Figure 8. The

[5] Chi-squared test, p = 0.025.

reasonably substantial evidence that user privacy needs to be protected more, along with these opinions, implies a strong need for overhaul since most of the respondents were practitioners and likely deal with legal issues more directly than non-practitioners. As mentioned in Section 2.5, laws have seen sparse attention.

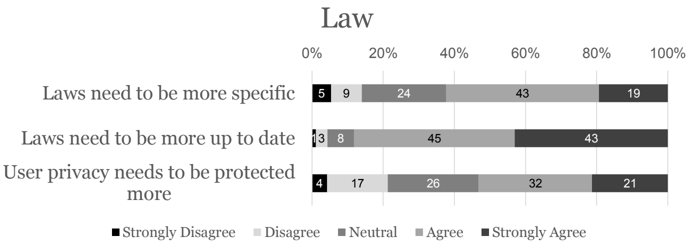

Figure 8: Each bar represents one Likert scale question. Approximate percentages are displayed for each answer selection.

5.8. Communication

The matrix in Figure 9 explicitly indicates that state/local law enforcement needs to communicate more effectively (13 occurrences where it was paired with federal/national law enforcement and 12 occurrences where it was paired with legal system). Overall federal/national law enforcement was chosen most for poor communication. Since ETC was also selected frequently, better/increased communication between practitioners and educators/researchers will need to occur.

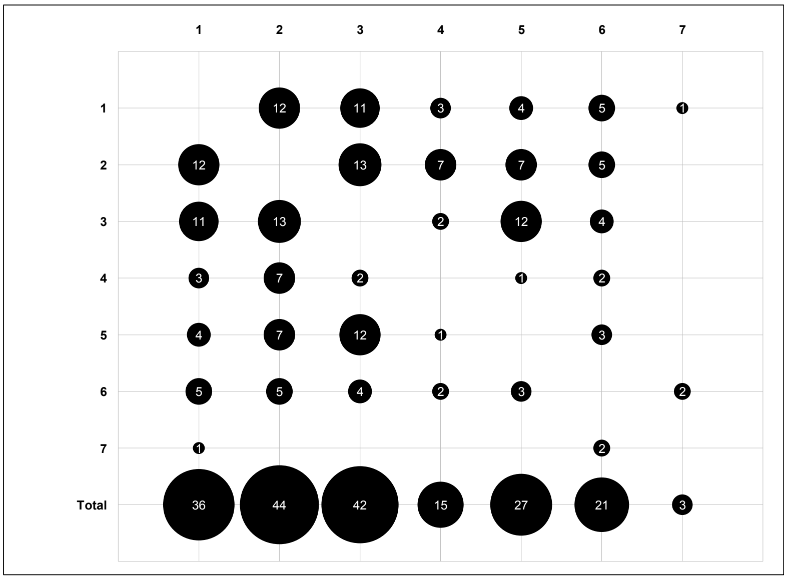

Figure 9: The matrix represents groups that need to communicate more effectively with each other (participants were asked to select a pair). The sizes of the circles are proportional to their numbers. The total in the bottom row demonstrates how much each group needs to improve on its communication, regardless of who they are communicating with. 1 = Education/training facilities/universities, 2 = Federal/national law enforcement, 3 = State/local law enforcement, 4 = Military/national security, 5 = Legal system, 6 = Other private organizations, 7 = Other public organizations.

Three yes or no questions asked respondents about communication with ISPs (e.g. AT&T, Verizon, and Comcast), online service providers (e.g. Google, Yahoo, Facebook), and computer and mobile manufacturers. In all three of these questions a unanimous call for new established frameworks for communicating with these organizations was observed (over 78% for each). Once again, the relative size of the private organization demographic and the polarized opinions of these questions may mean such frameworks are nonexistent or extremely weak.

5.9. Domain categorization

Two general questions were asked about the definition of cyber forensics. The first asked if the participants considered the field a (formal) science to which there was a resounding "yes" (77%). The second question asked whether cyber forensics is an engineering discipline. North Americans were undecided but European input tipped the scale toward an overall 63% affirmation.

6. Discussion

The results of the survey signed several things about cyber forensics. As in most technical domains, there is a relatively low number of females in the demographics; possibly the field is still unevenly gender balanced. A second eye-catching aspect was that no respondents were from Africa. This might have to do with the distribution method. Taking a closer look at the fields of expertise shows that only a few respondents had expertise in database forensics and only slightly more had cloud forensics expertise. These were top concerns for the future and although they are newer subdomains more experts must arise quickly if the field is to keep stride with criminals. Certainly, mobile forensics is extremely important as all types of cases involve mobile evidence (Saleem et al., 2014).

The upset with funding in the results can be rationalized by a low federal demographic; federal labs are more likely to "report analyzing digital evidence," implying that non-federal facilities are not equipped well enough to deal with cybercrime (Durose et al., 2012). Such lack of cohesion within the field is now leading to the call for an official governing body (Waziri & Sitarz, 2015), something that may also require a federal and non-federal delegation; a distinct difference in concerns between demographics was solidified in a 2009 survey addressing top priorities: law enforcement selected best practice issues as most critical, government selected jurisdictional issues, commercial selected access & exchange of information (Liles et al., 2009).

Since the legal system was ranked a relatively low priority in the Rogers & Seigfried followup question one would assume it is not a top priority within the field. However, the Likert scale questions advocated major amendment. Since the legal system demographic was close to non-existent we think a follow-up study would be beneficial — one that targets the judiciary viewpoint. This would be helpful to pinpoint how laws are not specific enough or could be improved upon to protect users and effectively prosecute international criminals. A similar issue could be seen in federal/national law enforcement having the poorest communication of any occupational category demographic; it was the smallest. Perhaps a follow-up study might target federal opinions on the matter.

Many of the results supported recent findings: tools need to be better (quality, usability, & price) and standardization needs to increase across the board (laws, tools, education, & communication); all of these were repeatedly found in research presented in Section 2.

7. Limitations

The Likert scale questions may have exhibited acquiescence bias (agreement with the statements as presented), because many questions observed affirmation. However, the questions were worded in a way to avoid this and this may have simply been a result of grouping questions by topic. Bias by geographic region and other demographics was not observed other than where mentioned; low count of some demographics prevented drawing further conclusions.

8. Conclusions & follow-up

A divide still exists between what professionals desire and what is currently occurring within cyber forensics. ETC and technology still remain the highest priorities for change. State/local law enforcement and ETC facilities need more ETC opportunities (whether it be newer programs or revised curricula); in Europe federal/national law enforcement is also of concern. ETC requires more funding — as an example, the Regional Computer Forensic Laboratory facilities only used 2% of their funding in 2012 on training/educational material; in 2013 the number of trained employees was even lower than the previous two years (Regional Computer Forensics Laboratory, U.S. Department of Justice, 2012, 2013). Surprisingly, reverse engineering is viewed as a skill future certified examiners should have in addition to fundamental investigative skills and ability to use tools. The most evident finding on tools was that open-source tools need much more support and improvement. Additionally, most respondents pointing out tools are too expensive.

One of the themes of the survey responses was the need to pay greater attention to cloud and mobile forensics. Not only are these subdomains in need of support (referring to technological repositories and communities useful for practitioners), but they also need more research. Cloud and mobile forensic tools are lacking when compared to other subdomains.

Another crux among the results was sluggishness to adopt newer technologies and ideas. MD5 is still used by most practitioners despite its flaws. Less than a fifth of professionals don't know what similarity hashing algorithms are; nevertheless usage is low among those who do know (especially among North Americans when compared to Europe). Laws are perceived to be out of date, not specific enough, and insufficiently protective of user privacy.

Thirdly, communication is a substantial problem. There appears to be a disconnect between educators/researchers and investigators, and ineffective communication between law enforcement and service providers/ISPs warrants the establishment of new correspondence systems. Setting this up will demand a stepwise coordinated implementation since federal/national law enforcement has problematic communication efforts at the moment (in the eyes of practitioners) and state/local law enforcement needs more funding.

Other significant results were that research has moved up in priority in the last decade (malware, encryption, and trail obfuscation now viewed as essential areas of focus) and that the domain lacks personnel. A recent survey supports this, writing that forensic departments do not have enough personnel to process the high number of cases, no matter what tools are used (Goodison et al., 2015). This study also strongly (the likelihood of incorporation was measured directly) supports the aforementioned need for ETC reform, recommending digital evidence training be incorporated into both law enforcement and judicial system curricula.

Followup Delphi-method-based studies and surveys would be extremely beneficial to target more narrow and well-defined solutions (such as those mentioned in the Discussion section).

References

Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In *Information Security for South Africa, 2013* (pp. 1–8). IEEE.

Aminnezhad, A., Dehghantanha, A., & Abdullah, M. T. (2012). A survey on privacy issues in digital forensics. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *1*, 311–323.

Baggili, I., BaAbdallah, A., Al-Safi, D., & Marrington, A. (2013). Research trends in digital forensic science: An empirical analysis of published research. In *Digital Forensics and Cyber Crime* (pp. 144–157). Springer.

Bariki, H., Hashmi, M., & Baggili, I. (2011). Defining a standard for reporting digital evidence items in computer forensic tools. In *Digital Forensics and Cyber Crime* (pp. 78–95). Springer.

Barwick, H. (2014). Data sovereignty laws hamper international crime investigations: Afp.

Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. In *Advances in digital forensics V* (pp. 17–36). Springer.

Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital Investigation*, *10*, 226–245.

Breitinger, F., Guttman, B., McCarrin, M., Roussev, V., & White, D. (2014). *Approximate Matching: Definition and Terminology*. Special Publication 800-168 National Institute of Standards and Technologies.

Bureau of Labor Statistics, U.S. Department of Labor (2014). *Occupational Outlook Handbook, 2014-2-15 Edition*. Technical Report.

Choo, K.-K. R. (2011). Cyber threat landscape faced by financial and insurance industry. *Trends & issues in crime and criminal justice*, .

Dardick, G. S. (2010). Cyber forensics assurance. In *8th Australian Digital Forensics Conference* (pp. 57–64). School of Computer and Information Science, Edith Cowan University, Perth, Western Australia.

Darnell, J. (2012). Reply: Rdt&e iwg letter to swgde. private communication (publicly documented).

Dickson, J. B. (2015). 6 ways the sony hack changes everything.

Durose, M. R., Walsh, K. A., & Burch, A. M. (2012). *Census of Publicly Funded Forensic Crime Laboratories, 2009*. Tech Report Bureau of Justice Statistics, U.S. Department of Justice.

European Cybercrime Center (2014). *Police Ransomware Threat Assessment*. Tech Report Europol.

Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *digital investigation*, *6*, S2–S11.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, *7*, S64–S73.

Garfinkel, S. L. (2013). Digital media triage with bulk data analysis and bulk_extractor. *Computers & Security*, *32*, 56–72.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the us criminal justice system, .

Greek, A. N. (2013). *Proposal to establish an Open Source Validation and Testing Center*. Ph.D. thesis UTICA COLLEGE.

Grispos, G., Storer, T., & Glisson, W. B. (2013). Calm before the storm: the challenges of cloud. *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security*, *4*, 28–48.

Hack In The Box Security Conference (2012). Hitb2012kul d2t3 - mikko hypponen - behind enemy lines. YouTube.

Harblson, C. (2015). Hacking with pictures; new stegosploit tool hides malware inside internet images for instant drive-by pwning.

Hibshi, H., Vidas, T., & Cranor, L. F. (2011). Usability of forensics tools: a user study. In *IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on* (pp. 81–91). IEEE.

Kessler, G. C. (2010). *Judges awareness, understanding, and application of digital evidence*. Ph.D. thesis Nova Southeastern University.

Kornblum, J. (2006). Identifying almost identical files using context triggered piecewise hashing. *Digital Investigation*, *3*, 91–97.

Liles, S., Rogers, M., & Hoebich, M. (2009). A survey of the legal issues facing digital forensic experts. In *Advances in Digital Forensics V* (pp. 267–276). Springer.

Mickelberg, K., Schive, L., & Pollard, N. (2014). *US cybercrime: Rising risks, reduced readiness (Key Findings from the 2014 US State of Cybercrime Survey)*. Survey PricewaterhouseCoopers LLP.

Nance, K., Hay, B., & Bishop, M. (2009). Digital forensics: defining a research agenda. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1–6). IEEE.

Regional Computer Forensics Laboratory, U.S. Department of Justice (2012). *Regional Computer Forensics Laboratory Program Annual Report*. Tech Report.

Regional Computer Forensics Laboratory, U.S. Department of Justice (2013). *Regional Computer Forensics Laboratory Annual Report for Fiscal Year 2013*. Tech Report.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*, 1–12.

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*, *23*, 12–16.

Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, *10*, 34–43.

Saleem, S., Baggili, I., & Popov, O. (2014). Quantifying relevance of mobile digital evidence as they relate to case types: A survey and a guide for best practices. *Journal of Digital Forensics, Security and Law*, *9*, 19–50.

Srinivasan, S. (2013). Digital forensics curriculum in security education. *Journal of Information Technology Education*, *12*.

Walters, R. (2014). Cyber attacks on u.s. companies in 2014.

Waziri, I., & Sitarz, R. (2015). *Cyber Forensics: The Need for An Official Governing Body*. Tech Report Center for Education and Research in Information Assurance and Security.