Digital Forensics in the Next Five Years

Laoise Luciano
University of New Haven
West Haven, Connecticut
lluci2@unh.newhaven.edu

Ibrahim Baggili
University of New Haven
West Haven, Connecticut
IBaggili@newhaven.edu

Mateusz Topor
University of New Haven
West Haven, Connecticut
mtopo1@unh.newhaven.edu

Peter Casey
University of New Haven
West Haven, Connecticut
pgrom1@unh.newhaven.edu

Frank Breitinger
University of New Haven
West Haven, Connecticut
FBreitinger@newhaven.edu

ABSTRACT

Cyber forensics has encountered major obstacles over the last decade and is at a crossroads. This paper presents data that was obtained during the National Workshop on Redefining Cyber Forensics (NWRCF) on May 23-24, 2017 supported by the National Science Foundation and organized by the University of New Haven. Qualitative and quantitative data were analyzed from twenty-four cyber forensics expert panel members. This work identified important themes that need to be addressed by the community, focusing on (1) where the domain currently is; (2) where it needs to go and; (3) steps needed to improve it. Furthermore, based on the results, we articulate (1) the biggest anticipated challenges the domain will face in the next five years; (2) the most important cyber forensics research opportunities in the next five years and; (3) the most important job-ready skills that need to be addressed by higher education curricula over the next five years. Lastly, we present the key issues and recommendations deliberated by the expert panel. Overall results indicated that a more active and coherent group needs to be formed in the cyber forensics community, with opportunities for continuous reassessment and improvement processes in place.

KEYWORDS

Forensics, Cyber Forensics, Digital Forensics, Computer forensics, Needs analysis, Policy, Workshop, Tools, Research

ACM Reference format:
Laoise Luciano, Ibrahim Baggili, Mateusz Topor, Peter Casey, and Frank Breitinger. 2018. Digital Forensics in the Next Five Years. In *Proceedings of International Conference on Availability, Reliability and Security, Hamburg, Germany, August 27–30, 2018 (ARES 2018),* 14 pages.
https://doi.org/10.1145/3230833.3232813

1 INTRODUCTION

It is without a doubt that cyber / digital forensics has become a critical part of the cybersecurity domain. Recent events, from billions of records being hacked to potential meddling with presidential elections, has brought the importance of this domain to light. Due to increases in attacks against systems, states, and consumer products, companies like Apple have taken security more seriously. While enhancing the security of consumer products protects privacy, it has, in return, made the forensic acquisition of data from them more difficult to ascertain. The volume of digital evidence that needs to be analyzed in a short period of time has also become a major hurdle. Not only is the volume of data large, but it also comes from disparate sources, cloud systems, and a multitude of devices. The digital forensics domain is thus at a crossroads. Because of these challenges, and more, it is imperative for experts in the digital forensics community to come together and examine:

- Where we are currently
- Where we need to go
- How to achieve our goals

This paper represents the accumulated opinions of twenty-four digital forensic experts that met in May 2017 and attended both days of the National Science Foundation (NSF) funded National Workshop on Redefining Cyber Forensics (NWRCF). The individual opinions of the digital forensics experts are kept confidential, and are not directly associated with any specific expert. The goal was to set a clear agenda for the community, and reach a wide audience. Given that the domain still faces challenges and that the last exhaustive active workshop in this domain was the initial Digital Forensics Research Workshop (DFRWS) in 2001[1], it was time to reexamine the domain through an active workshop of highly notable expert panelists. Our work resulted in the following contributions:

- We hosted the first workshop to discuss and debate the domain and its challenges in detail since the 2001 DFRWS.
- We analyze and present results obtained from the exhaustive two day workshop - both by presenting survey data obtained from the experts, and by coding all the collected qualitative data from the event.
- We present agreed upon tangible steps for the community to improve the state of the domain.
- We present the biggest anticipated challenges for cyber forensics in the next five years (See Table 4).
- We present the most important research opportunities in cyber forensics in the next five years (See Table 4).

https://doi.org/10.1145/3230833.3232813

[1]The first DFRWS helped shape the field by producing the domain's primary research roadmap.

- We present the most important job-ready relevant skills that need to be addressed by higher education in the next five years (See Table 4).
- We conduct a follow-up workshop to further deliberate the findings and recommendations of this study.

In the remainder of the paper we present the related work in Section 2 and the limitations in Section 3. We then share our overarching methodology in Section 4. The pre-workshop survey is discussed in Section 5, and the agenda development for the workshop is discussed in Section 6. The core of our work is presented in Section 7 with discussions of each category and theme. We then follow up with Section 8 which summarizes our results from the post-workshop survey on the future five years of the field. The key findings and recommendations sections are then presented in Sections 9 and 10 respectively, followed by our conclusions in Section 12. Finally, the follow-up workshop topics of discussion and findings are presented in Section 11.

2 BACKGROUND INFORMATION & RELATED WORK

Cyber forensics is a field that was born out of the need to respond to incidents involving computers as they arose in law enforcement. As such, much of the early research was driven by practitioners in the field and advances were geared towards topics that affect timely investigations. This problem-solution based model did not always follow the scientific method that was prevalent in other sciences, which contributed partially to the problem of how the community should view the cyber forensics field. Although there have been numerous advances in the field, little work has been pursued to determine how the community should come together to solve some of these problems.

It was not until 2001, one month prior to the events that occurred on September 11, that fifty researchers met during the first DFRWS in Utica, New York to lay out a framework of how the community should come together [8]. This was a primary step for establishing a scientific community and defining a common discipline that was based on foundations of the scientific method.

Palmer et al. [8] explained that one of the issues that plagued researchers was that a discipline had to contain the following elements: theory, models, examples of practice, a collection of literature, and, ultimately, confidence in results. At the time, the community was still in a state of confusion and many researchers agreed that there was an unclear definition of these elements. It was noted that follow-up would be needed to not only define terms and technologies to make communication more effective but that processes would need to be re-defined and structured to accommodate operational and law enforcement perspectives in debates and discussions. They indicated that a road map should be utilized where technical challenges would be found and debated, and a process instituted where expertise would be aligned to conduct research and publish results, leading to the development of prototypes and solutions.

Almost five years later, scientists considered issues and needs of specific areas of the community. Richard III and Roussev [9] examined the tools that were utilized in investigations and noted that one of the common themes was the issue of scalability. Many of the tools lacked the ability to handle multi-threading, and the imbalance of computing resources required new approaches. It was noted that better collaboration would be necessary and that a distributed computing approach be utilized in which tools and members would pool their resources to achieve a common solution.

There were also issues that continued to plague the area of research almost a decade after the first meeting in 2001. In a workshop titled *Digital Forensics: Defining a Research Agenda* held in June 2008, it was determined that there was a need for top-down and timely research principles which stemmed from legal issues and basic principles of how evidence was collected, interpreted and conveyed to audiences [7].

A year later, Beebe [1] indicated that research in Cyber Forensics had shifted from a process as a whole to strictly the analysis phase, led by the value of digital evidence in investigations. As research was driven by these investigations, this led to the lack of standardization and formalization of procedures and resulted in lower standards due to the high learning curves of presenting information that would be understood by the community. Beebe [1] also stressed that much of the current research leaned heavily towards Microsoft Windows and that there was a long list of technical issues that had not been addressed.

In 2010, in his seminal paper, Garfinkel [3] laid out digital forensics research for the next ten years. He explained that standardization was still a large issue as it was noted that agencies should adopt standards and procedures to use abstractions in testing and validation, and that techniques should be created to make research more efficient.

As time passed, the same topics came up a number of times in discussions with no solutions. Walls et al. [11] set out to examine and define many of the key points of the digital forensics industry to ensure that research to advance the field would be highly adopted by practitioners. They determined that legal and practical constraints not only set the field apart from others, but that assumptions made about forensics in the past limited the impact of contributions.

The latest general needs analysis survey of the Cyber Forensics community was conducted by Harichandran et al. [5]. This was inspired by an older study by Rogers and Seigfried [10]. The overall results of the newer study provided 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) and; (7) more personnel and funding.

We argue that there has not been a recent, focused, active workshop with experts from the Cyber Forensics community with a purpose to debate and discuss the state of the community as a whole and to examine future needs, with the hope of solving some of the problems that the domain has been facing for almost 20 years. As many of these issues have persisted through time, the domain is at a crossroads. Therefore, an active workshop is needed to be held to obtain the opinions of Cyber Forensics leaders in greater detail to identify and address the current problems so that possible

solutions could be discussed and presented to the community at large.

3 LIMITATIONS

There are three limitations at the core of this work. The first is that the data collected at the workshop represented national presence in the United States, as the funding source was U.S. centric. Second, much of the data collected was qualitative, so the coding was manually conducted by the researchers, leaving room for some error during the coding process. To overcome this issue, the researchers validated the coding of the data through an iterative multi-review process. Thirdly, the workshop represented a limited panel of only twenty-four individuals as follows: sixteen academics, four industry professionals, two government experts, and two law enforcement experts due to funding limitations. High-impact researchers and practitioners were selected to compensate for the limited amount of experts.

4 METHODOLOGY

The workshop was developed by the University of New Haven in West Haven, Connecticut. Grant No. 1649101, which was awarded in 2016 by the National Science Foundation (NSF), served as the basis for funding, allowing for high-impact researchers and practitioners to be invited from a multitude of sectors. The overarching methodology followed is exemplified in Figure 1. As it was important to lay out an agenda for the workshop, a pre-workshop survey (Section 5) was created and contained current challenges faced by the Cyber Forensics community. After seeking Institutional Review Board (IRB) exemption, the online survey was disseminated via e-mail to the expert panelists prior to the start of the workshop to identify the top areas to later be discussed in the workshop sessions. The workshop agenda was then developed based on the feedback (Section 6), followed by hosting the workshop and qualitative data collection. A post-workshop qualitative survey was then sent to the participants to gauge where they believe the field is heading in the next five years (Section 8 and Table 4). One year following the workshop a validation session was conducted to further deliberate the findings and recommendations (Section 11). These steps were all followed by quantitative and qualitative analyses of the data, and paper writing to close the methodical loop and report the findings to the funding agency.

Figure 1: Overarching Methodology.

5 PRE-WORKSHOP SURVEY

To identify initial areas of concern to be included in the pre-workshop survey, a brainstorming session was conducted, and past literature was consulted. Five initial areas were determined as areas of high importance and were added to the pre-workshop survey for validation:

- Merger of Cyber Forensics with Other Disciplines (Psychology, Data Science, Reverse Engineering, Social Network Analysis, etc.)
- Emerging Cyber Forensics Areas: Cloud, Mobile, Internet of Things (IoT) Memory and other Areas
- Education Techniques, Technologies, Gamification and Competitions
- Cyber Forensics and Encryption
- Cyber Forensics Funding and Funding Directions

In the event topics of importance were missed, an open-ended survey question was added to allow participants to contribute additional input on areas they felt should be considered for deliberation.

5.1 Pre-workshop Data Collection and Analysis

The survey was disseminated to members that had indicated they were going to attend the workshop. Each member was asked to rate the topics by importance, with 1 being the highest and 5 being the lowest. These values were later inverted to give more weighting to items with higher importance.

Once the survey was shared, each member submitted their responses and the data was recorded. The rankings were totaled for

the question on *Topic Importance* and the results are shown in Table 1. Topics that ranked with the highest total were those of highest importance. Although there was an open-ended question, the majority of the participants agreed with the topics that were presented in the original survey so additional areas of concern were taken into consideration and were incorporated into sub-themes and other areas for discussion during the workshop.

The survey also included several questions, such as the word used to identify the discipline, in specific, Cyber V.S. Digital forensics (see Table 2). Questions pertaining to current events were also asked, such as whether backdoors should be added to secure systems (see Table 3). An additional field was added in the pre-workshop survey to provide details about expert reasoning behind their choices, which are presented in Section 7.

Table 1: Pre-workshop Survey Topic Importance

Answer	∑ Sum	% of Total
Cyber forensics funding and funding directions	73	22.5%
Emerging cyber forensics areas: Cloud, Mobile, IoT Memory and other areas	73	22.5%
Education techniques, technologies, gamification and competitions	61	18.8%
Merger of cyber forensics with other disciplines	59	18.2%
Cyber forensics and encryption	59	18.2%

Note: Each row represents one main topic. The total of the responses in points is 325. As the survey was designed with 5 being the highest concern and 1 being the least, the results of the rankings for each theme were summed up. The items with the highest total number represent those of highest overall importance.

Table 2: Cyber vs Digital Forensics, Defining the Word

Answer	# of Total	% of Total
It doesn't matter - both are OK	11	55%
Cyber Forensics	5	25%
Digital Forensics	4	20%

Note: Each row represents the opinions of how the industry should be defined: Cyber Forensics vs Digital Forensics vs Both are OK. The total of the responses is displayed on the right, with percentage of total.

6 AGENDA DEVELOPMENT

After analyzing the pre-workshop survey data, the top four themes that emerged were selected for discussion at the workshop. The themes were:

Table 3: Backdoor into encryption technologies?

Answer	# of Total	% of Total
No	11	50%
Sometimes	9	41%
No Response	2	9%
Yes	0	0%

Note: Each row represents opinions of whether there should be a backdoor into encryption technologies: Yes vs No vs Sometimes vs No Response. The total of the responses is displayed on the right, with percentages of total.

- Emerging Cyber Forensics Areas: Cloud, Mobile, IoT Memory and other Areas
- Education Techniques, Technologies, Gamification and Competitions
- Merger of Cyber Forensics with Other Disciplines (Psychology, Data Science, Reverse Engineering, Social Network Analysis, etc.)
- Cyber Forensics and Encryption

Although Cyber Forensics Funding and Funding Directions was ranked of similar importance as Emerging Cyber Forensics Areas, this discussion topic was added as a subtopic area titled Funding. Additional subtopic areas within these themes included Education, Policy & Procedures, and Technology: Tools & Testing.

The workshop was then organized into different sessions, moderated by an expert moderator, to discuss where the *discipline currently stands (where we are now), where it needs to go and how we can get there* for each of the subtopics within the identified themes. Expert panelists were initially assigned to groups based on the themes they had the most expertise in. At the end of each session, each session group would report their findings to all participants for further discussion and deliberations. Focus groups were then asked to submit their findings via online forms for data collection. This was succeeded by at least two people from each group being asked to rotate to a different theme to ensure the diversity of opinions and discussions.

At the end of the workshop, participants were individually asked to complete a follow-up *I believe* survey to provide personal feedback and opinions on various discussion points that were brought up during the workshop. They were asked to indicate *(1) what they anticipated were challenges that the digital forensics community would face in the next five years; (2) the most important research opportunities in the next five years and; (3) the most important job-ready relevant skills that need to be addressed by higher education curricula in digital forensics within the next five years* (see Table 4 for the results obtained from these open ended questions).

7 THEME DISCUSSIONS AND FINDINGS

As we present the results obtained from the active workshop, **we note that the views, opinions and positions expressed by the participants discussed in the following sections do not necessarily reflect the views, opinions or positions of the authors**. Our goal was to share aggregate findings in an unbiased manner.

Twenty-four panelists attended the workshop. Sixteen were members of academia, and were affiliated with universities. Four were from the cybersecurity/forensics industry, two were from government branches and two were from law-enforcement agencies. Nineteen participants were male, and five were female.

In response to the pre-workshop survey data collected in Section 4, participants were divided into theme-based focus groups and asked to discuss topics related to Education, Tools & Technology, Policies & Procedures and Funding within the context of the themes identified in Section 6.

The purpose of the focus groups was to identify areas of concern, discuss where the discipline currently stands, where it needs to go, and how changes should be made to get there. Responses

were categorized into statements that best identified the nature of the response and assigned to a common discussion point. The statements were then counted based on the number of times they occurred in that discussion point. The counts were totaled and assigned rankings from highest to lowest. As shown in Figure 2, areas that had the highest concern among all themes included Funding in Research and Training, Policy Standardization, Lack of Information with regards to Tools and Technology, and Specialization of Educational programs.

7.1 Backdoor Discussion

The participants discussed the topic of implementing backdoors into systems in order to recover digital evidence from them at length. Eleven of the participants agreed that placing backdoors into systems defeats security principles that systems are built upon, even though nine of participants initially agreed backdoors may sometimes be warranted as seen in Table 3. Notwithstanding, all participants agreed unanimously that in the Cyber Forensics field we focus on evidence recovery, as cybersecurity scientists and professionals, adding security holes to systems is the wrong approach. Backdoors in the case of the unanimous agreement meant that a system was purposefully built with a security hole that would allow root access to a system.

7.2 Education

Concerns in Education across all themes are shown in Figure 3. As illustrated, participants reported that programs have become too specialized, followed by the need for curriculum changes. Of equal values were the need for fundamental concepts to be incorporated, annual meetings to discuss current needs and changes, the availability of opportunities in the field including hands-on training/research, along with the need for better exchange between experts and practitioners through conferences and workshops.

7.2.1 Emerging Cyber Forensics Areas. In the theme of Emerging Cyber Forensics, the consensus of where we are now reflects a state of chaos and flux. Participants reported that fundamental concepts and abstract thinking techniques are not being adequately developed and introduced into curricula and practice. There is no coherence between syllabi and course quality, leading to program differences between organizations. Training is not currently balanced with specialization and courses that are available often do not correspond to industry needs. Although annual meetings are starting to occur to alleviate this problem, more needs to be done to discuss the needs of the field, develop solutions, and in-turn, pass these solutions onto training and educational programs.

As communication between industry and practitioners continues to improve, outreach meetings are important to discuss additional needs, identify and agree on fundamentals and transfer these needs into curricula. In addition, more needs to be conducted to expose others to current topics in the field. Universities with cyber forensics programs should conduct and publish more research while non-research based programs should participate in conferences. Practitioners should be encouraged to participate in opportunities that will grant continuing education experience, further strengthening the need to adapt to an ever-changing field.

7.2.2 Merger of Cyber Forensics with Other Disciplines. In regards to the merger of Cyber Forensics with other disciplines, participants reported that there is currently too much specialization and not enough has been accomplished to bridge disciplines together. This results in a narrow-minded focus: too many individuals are capable of thinking only in their given specialty and lack the ability to see the larger picture. Although specialization can be a good tool when used properly, programs should build a broader skill set early on in their curricula, allowing for open academic minors and the ability to choose a specialization later in the process.

In addition, merging courses in the humanities and social sciences with Science, Technology, Engineering, and Mathematics (STEM) allows students to think in more abstract ways. To get to this point, Universities need to build concentrations in other disciplines as part of their degree programs. Speakers and subject matter experts should be identified and contacted to speak to or teach students techniques that are not taught in the classroom, providing additional hands-on experiences beyond the scope of the classroom.

The panelists also reported that learning outcomes need to be clearly defined for students. As courses are developed, it is imperative that administrators and instructors pay attention to relevance and the flow of changes. If needed, course outcomes and content should be changed periodically to reflect changes in industry. Additionally, it should be encouraged for those involved in curriculum development to become members of accreditation boards, such as the Forensic Science Education Programs Accreditation Commission (FEPAC), or the Accreditation Board for Engineering and Technology (ABET), etc. to ensure that content is relevant and pedagogically robust.

7.2.3 Cyber Forensics and Encryption. In the theme of Cyber Forensics and Encryption, participants reiterated that curriculum changes are necessary. Currently, elective topics are typically voluntary and may be completed via training by outside vendors or the Internet in much shorter amounts of time than classroom training.

In terms of where we need to go, there is a definite need for programs to contain fundamentals in both forensics and fields such as encryption. For example, there is a lack of courses and course content to explain the basic elements of encryption, how to prevent it from activating, key management and the process for breaking it. To improve on this, continuing education opportunities should be provided through training and education not only for the workforce but also for students. Encryption modules should be added to database/network classes with common avenues and standards for training with materials and labs.

Another issue that was brought up involved the use of alternative means and tools to gain access to data, such as metadata surrounding encryption. These topics are generally not being addressed by curricula.

7.2.4 Education Techniques, Technologies, Gamification and Competitions. Participants agreed that many opportunities in Education Techniques, Technologies, Gamification and Competition exist for labs/education. However, more hands-on experiences need to be introduced into courses such as the examination of case studies, competitions, lifelong learning skills, and research opportunities in Cyber Forensics. These experiences need to be added at the course

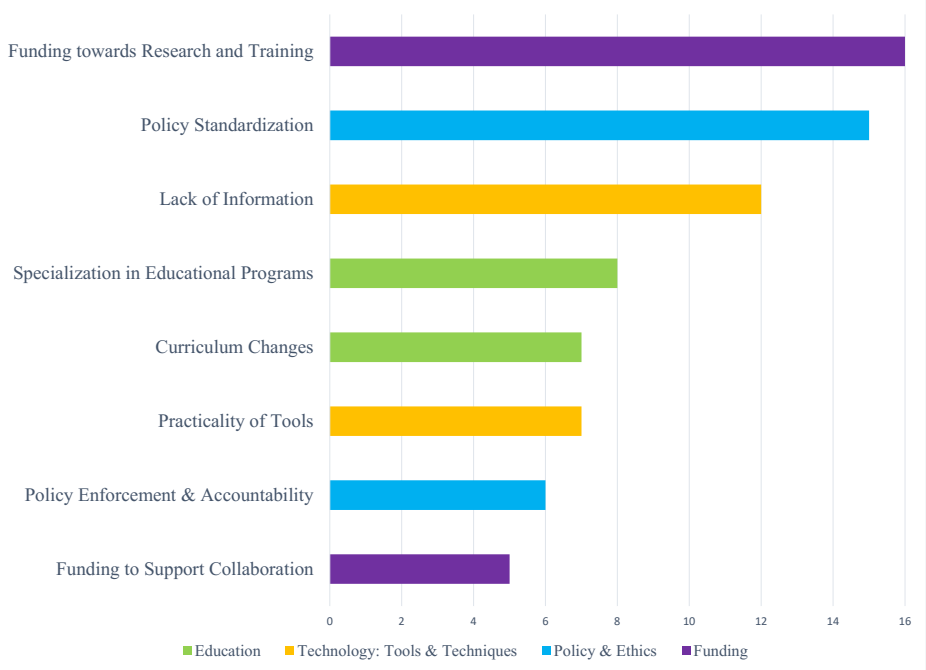

Figure 2: Top Overall Results Across All Themes. Each bar represents one main discussion point. The number of total responses across all themes is represented on the x-axis and is displayed by subtopic.

and curriculum development level. Students should be trained and taught programming and resource issues via laboratory experiences, in-person training and on-line content.

Additionally, degrees are typically not multidisciplinary and many programs are currently too focused on application/tool usage. Opportunities to create fully multidisciplinary degree programs should be encouraged. By expanding the use of student challenge groups, and adding technologies such as virtual reality into course development, it may also attract students from other disciplines.

7.3 Technology: Tools & Testing

The overall ranking of topics in Technology: Tools & Testing is illustrated in Figure 4. A lack of information in both tool usage as well as development, which includes shared data, ranked the highest. Many experts reported that tools were highly impractical, as they did not respond timely to the changes in the industry. Also of importance was the lack of collaboration in development, usage and testing.

7.3.1 Emerging Cyber Forensics Areas. Some reported that in the field of Cyber Forensics, tools currently available were impractical. There is a strong inconsistency between outputs and many are not equipped to adapt to changes and evolution of technology. A lack of shared datasets[2] to validate existing tools and techniques results in many that do not get utilized in investigations. To further complicate the matter, there is a lack of tools in areas such as IoT, encryption/decryption, multimedia, vehicle forensics, Software Defined Networks (SDNs) forensics, and emerging fields such as quantum computing.

Going forward, the community needs to improve communication between experts to determine needs and current market trends in the field. As these are identified, solutions need to be developed and avenues provided so that data and results can be passed to individuals employing them in investigations. One of the suggested solutions is to increase the number of annual competitions in open-source tool development to encourage practitioners to solve problems in emerging areas.

7.3.2 Merger of Cyber Forensics with Other Disciplines. The lack of information regarding available tools and the information they provide also continues to be a problem when merging Cyber Forensics with other disciplines. Tools are not standardized, common benchmarks do not exist to validate tools and, as discussed above, there continues to be a lack of datasets for testing and research. In order to solve this problem, tools need to have up-to-date datasets that are shared to validate both newly created tools along with existing ones that are currently being utilized to solve problems. This is not to discount the work in this area by the National Institute of Standards and Technology (NIST) [6]. The Computer Forensincs Tool Catalog provides a searchable catalog of forensics tools that meet the specific technical needs of the practitioner. Additionally, NIST's Computer Forensics Tool Catalog also tries to solve the tool

[2]The importance of datasets for cyber forensics was recently discussed by Grajeda et al. [4].

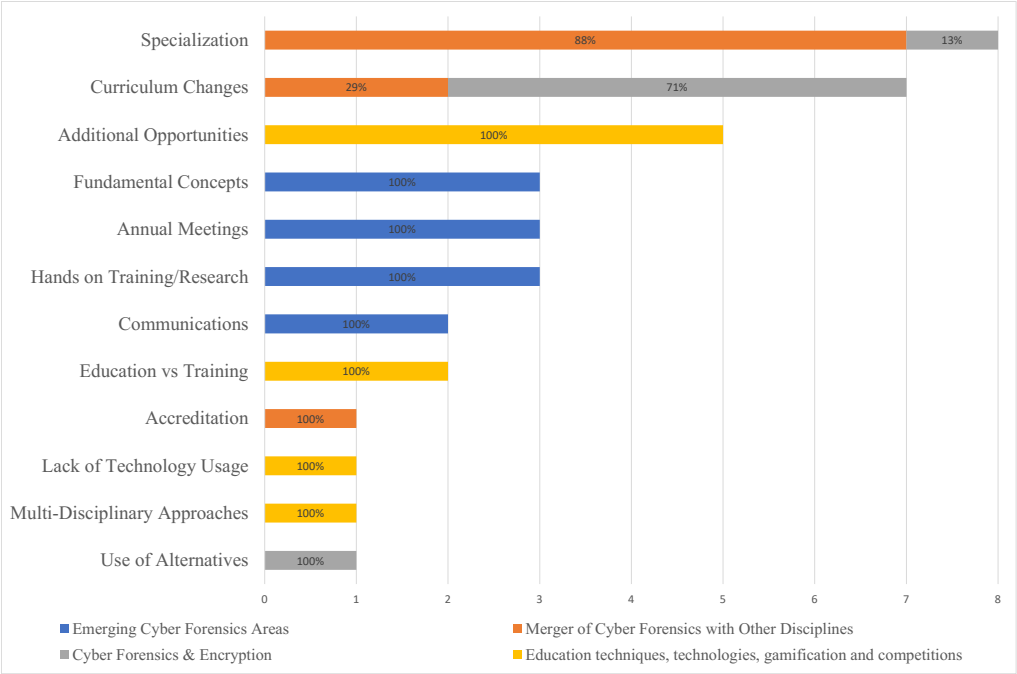

Figure 3: Education Concerns. Each bar represents one main discussion point. The number of total responses across all themes is represented on the x-axis and is displayed by subtopic.

gaps in the digital forensics landscape, and offers a tool taxonomy. But there are many open source tools that are not being tested by the NIST program, and more testing is needed.

Collaboration between individuals in multiple disciplines would allow for the creation of standardized benchmarks which could be applied to tool development and a more streamlined process for reporting bugs and flaws as they occur. This would result in more standardized tools that are not only useful to those in the field but also allows for better presentation to non-technical individuals. A centralized location for tool testing, similar to Underwriters Laboratories (UL), would ensure that standardized procedures are followed and would create a repository for tool standards, providing services to those seeking help with the application process, correspondence, or coordination of the exchange and review of data associated with the tool.

7.3.3 Cyber Forensics and Encryption. Tools that cross Cyber Forensics and Encryption are also highly impractical, existing for detection on a basic level but when utilized on computers and devices with more sophisticated users, it becomes difficult to detect and extract data. When encryption is used, it is almost infeasible to break, as resources can be quickly exhausted. The community needs to be more innovative on how to get around it, especially in the development of more forensically relevant tools. Tools should be able to determine if encryption is present and if so, use secondary attacks and side channel attacks as alternatives to be able to provide the data requested. In addition, some fields like steganography are not even on the radar when considering the nature of the tool.

7.3.4 Education Techniques, Technologies, Gamification and Competitions. The community currently faces a number of challenges in Education Techniques, Technologies, Gamification and Competitions. Software licensing continues to remain a problem for many users. Mindsets about open-source tools reflect a state that many are poor or insufficient and are not utilized at all.

There is also a strong lack of collaboration with regards to lessons learned. The industry benefits from symbiotic relationships, and exercises, challenges and the use of case studies in validation, testing, and creation help to promote more efficient tool development. In addition, tools can be developed that are more relevant for use against data hiding and anti-forensics.

Participants also agreed that the lack of information in regards to shared datasets and markets hinder the use of tools. Some repositories, such as the NIST and *digitalcorpora.org*, exist but more are necessary. A centralized marketplace also does not exist, not only to share tools that are created and validated, but also to download tools for use. Centralized marketplaces would make it more streamlined to report conflicts and provide solutions.

In terms of existing tool usage, virtual laboratory technology and other opportunities need to be utilized more as this reduces the burden on students and instructors.

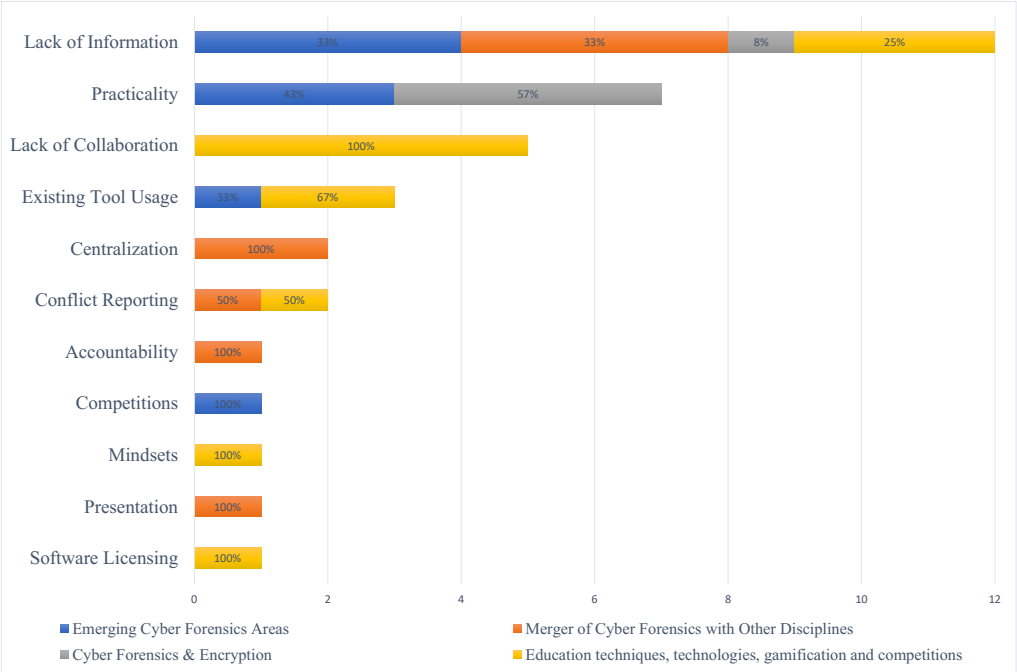

Figure 4: Tools & Testing Concerns. Each bar shows one main discussion point. The number of total responses across all themes is represented by the x-axis and is displayed by subtopic.

7.4 Policy & Ethics

Figure 5 reflects the responses in discussion topics across all themes in Policy and Ethics. Standardization, or a lack thereof, ranked the highest with comments from all groups, followed by enforcement and accountability.

7.4.1 Emerging Cyber Forensics Areas. One of the resounding issues in the area of Emerging Cyber Forensics is that technology grows and changes faster than the policies that are in effect, resulting in a lack of standardization. Policies need to be flexible so that they stay relevant to future emerging and changing technologies. However, this also raises individual privacy concerns; as technology improves and more avenues for data collection are developed, the data that is obtained becomes closer to our sense of self.

7.4.2 Merger of Cyber Forensics with Other Disciplines. Standardization was again brought up as an issue in the Merger of Cyber Forensics with Other Disciplines. The expert panelists concluded that there are way too many guidelines and different varieties of organizations and neither of them respond well to changes in technology. Going on an earlier statement, there is not much congruence between organizations and policies, leading to chaos. There needs to be more collaboration with each other; consolidating development areas and bodies that are involved in the process and creating a strong Special Interest Group (SIG) for Cyber Forensics. In addition, an oversight body can be created with professionals that requires minimum standards to be met.

A downside to a lack of standardization also involves a lack of enforcement. Without a universal set of benchmarks and guidelines for policies and procedures, there is no valid way to enforce the policies in place. Ethics are not enforced and often compliance is voluntary, leading to issues with accountability. Certification bodies need to be able to share lists of individuals that have ethic violations with each other and the public, and need to be able to request if individuals have been denied certifications for previous violations as a part of their certification process.

7.4.3 Cyber Forensics and Encryption. Policies in Cyber Forensics and Encryption are also highly inconsistent and there are disconnects between what law dictates and what people think they are able to do. For example, there are no policies that currently exist to force companies to break their encryption but there are legal precedents that exist to provide data if they are in possession of it. Companies do not want to be able to break their encryption or provide backdoors into their software as this also raises privacy issues for those that are using their software and products.

Participants also agreed that there needs to be more training for the legal system and outside users to understand how the technology works, as well as revisit existing doctrines of privacy, such as the Third-Party Doctrine. By having a better understanding of policies and technology, individuals can understand that information they believe is private is actually not and that people should not advocate to weaken security to make their lives and jobs easier.

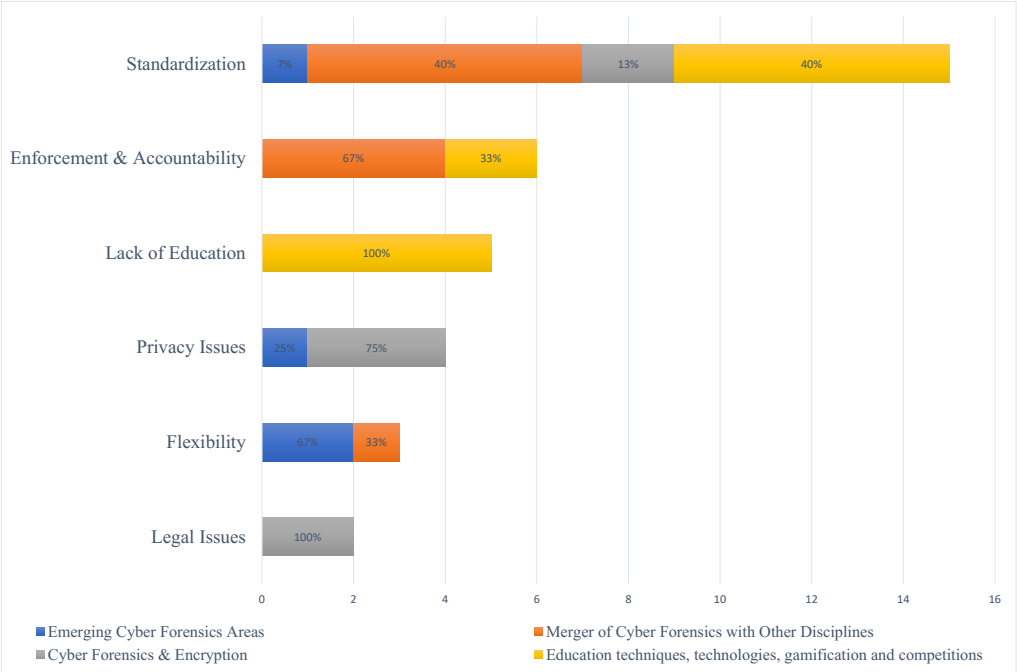

Figure 5: Policy & Ethics Concerns. Each bar shows one main discussion point. The number of total responses across all themes is represented on the x-axis and is displayed by subtopic.

7.4.4 Education Techniques, Technologies, Gamification and Competitions. There is also a lack of standardization regarding policies that are used in education. Too many different codes exist and there needs to be better organizational coherence. Common codes need to be taught in academia, and practitioners should be called in to consult with organizations and universities to develop policies. Also, collaboration with organizations such as the American Bar Association (ABA) and others are necessary to develop sustainable models that are capable of adapting to change.

Currently, there is also a lack of ethics education. Ethics needs to be taught in courses or as separate topics in digital forensics classes. Programs should teach rules of evidence, chain of custody, compliance and development. There are some universities that have adopted this model, however, participants were unsure if it is widely utilized among all avenues in Education. The industry needs to teach and train, both in higher education and continuing opportunities to develop a framework for others to follow in the workplace, as well as adding policy issues to competitions to encourage collaboration and illustrate different viewpoints so that solutions can be developed that reflect industry needs.

There also needs to be a method to enforce policies and ethics that are in place. Professional licensing should adopt standardized criteria and a framework for membership and should be utilized when enforcing ethical conduct violations to protect the credibility of members.

7.5 Funding

Overall concerns towards Funding are displayed in Figure 6. Participants reported that funding should be directed towards research and development, improving collaboration as well as changing mindsets about Cyber Forensics.

7.5.1 Emerging Cyber Forensics Areas. Currently, funding is limited for practitioners in emerging areas. Practitioners need additional resources for training and tool development in these areas. Some of these resources can include grants and incentives for participation in conferences regarding emerging areas and changes in technology, and incentives to spur competition to develop new tools. Participants also reported the need for *flash grants*, which are small, short-time grants that are awarded to tackle new projects in emerging technologies that have quick market turnarounds.

Additionally, one of the problems with providing additional funding lies in the mindsets of many individuals. As it currently stands, there needs to be better ways to establish that Cyber Forensics is a reputable discipline. This can be accomplished by providing better avenues for research and publication in reputable areas. Participants also reported consensus that the creation of dedicated NSF Cyber Forensics subsections in Secure and Trustworthy Cyberspace (SaTC), Defense Advanced Research Projects Agency (DARPA), the Federal Bureau of Investigation (FBI), as well as ARMY research laboratories would bring attention to the field and priorities could be given for funding digital forensics investigations and incident response.

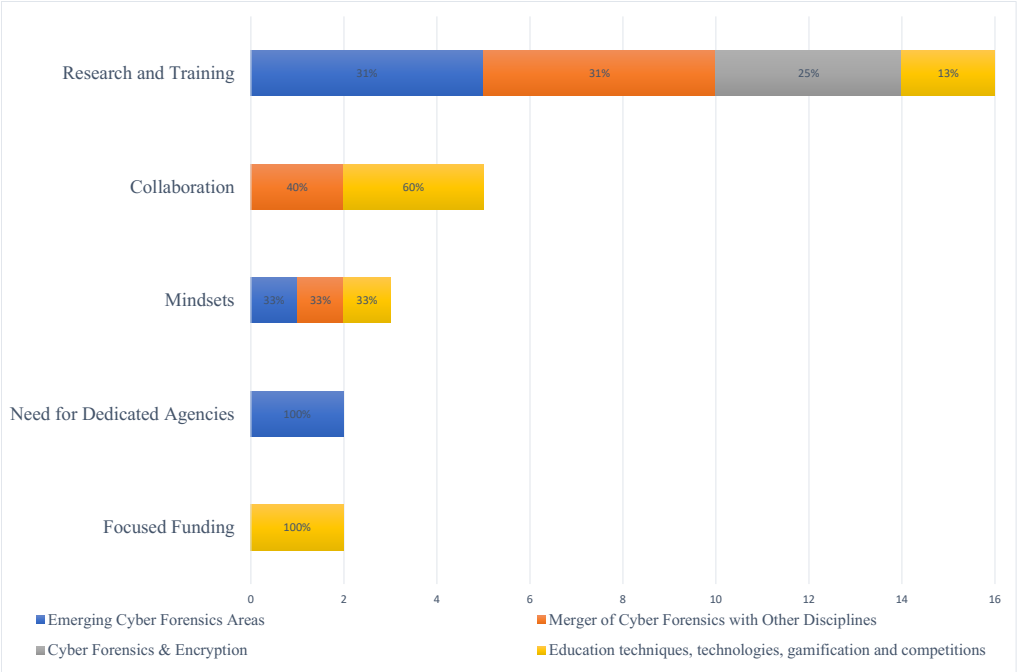

Figure 6: Funding Concerns. Each bar represents one main discussion point. The number of total responses across all themes is represented on the x-axis and is displayed by subtopic.

7.5.2 Merger of Cyber Forensics with Other Disciplines. Experts reported that in research and development areas, there is a lack of focused funding which discourages multidisciplinary collaboration. This not only prevents the community from working together, but gradually lengthens the time and resources necessary to solve large problems. Funding needs to be directed towards tool development, the education of scholars and practitioners/examiners, and should be flexible enough to keep up with development and modification as technological changes. Experts also suggested that funding agencies should also collaborate with each other if needed, to ensure that funding is directed towards the problems at hand. For example, the Department of Justice (DOJ) and NSF may collaborate together to create a joint funding effort in the area of Cyber Forensics.

Universities and departments should also work together to create and host workshops and student interest groups that bring together individuals in the field as well as throughout other disciplines, to strengthen the field's standing within the larger community.

7.5.3 Cyber Forensics and Encryption. According to the panel members, the funding that currently exists is minor and not enough to encourage research into the breaking of encryption, only better ways to improve the quality and usage of it. As such, more focused funding needs to be directed towards artifact analysis and finding evidence that is not encrypted. To encourage this, funding for the development of tutorials and labs, as well as incentives for experts to write textbooks towards finding non-traditional sources of data would go a long way.

7.5.4 Education Techniques, Technologies, Gamification and Competitions. Funding is currently too application specific and does not encourage collaboration. There is little support for community sharing of datasets, resulting in a lack of information. A substantially funded oversight program should be created with managers and staff to monitor progress towards goals and objectives of Cyber Forensics, to stay on task, and ensure that funding does not go to waste.

There also is a lack of University support to bring commercial tools into the classroom due to their cost. Funding for education needs to be directed to not only tool usage, but also research opportunities, summer camps, competitions, and collaborations, as well as programs for students in Kindergarten through 12th grade. An important example of this is the GenCyber program [2] funded by NSF and NSA, which embodies the mission of growing the number of students who study cybersecurity, by funding camps to increase interest, help correct safe online behavior, and create better teaching methods to students between Kindergarten and 12th grade. The participants are aware of the GenCyber program, but many of those summer programs are directed at the 10 principles of cybersecurity and little exposure is directed towards Cyber Forensics.

Focus and mindsets also need to be improved. Participants deliberated that the NSF encourages funding but the panels that decide funding approval may be problematic. Some panelists noted that many of the panels are not composed of digital forensics experts, leading to funding being issued towards areas that might not be

focused in cyber forensics. Additionally, although many practitioners and educational areas conduct research and publish in journals, not all of them are published in high-caliber venues to be taken seriously. This not only discourages funding recommendations but also taints the field's reputation.

8 SUMMARY OF POST-WORKSHOP SURVEY

A post-workshop survey was disseminated during the conclusion of day one to ascertain a collective understanding of the expert panelist's personal views and goals for the future. Seventeen of the twenty-four Cyber Forensics experts provided data on the path they believe needed to be taken for the future of the Cyber Forensics community. The three questions asked were as follows:

- What are the three challenges that the digital forensics community will face in the next five years?
- What are the three most important research opportunities in digital forensics for the next five years?
- What are the three most important job-ready relevant skills that need to be addressed by higher education curricula in digital forensics in the next five years?

Table 4 outlines the summary of the expert panel's opinions. Most important to the community is that the table presents an abundance of research opportunities and hard problems that could be pursued. Generally, the results were congruent to the overall findings from the workshop presented in Section 7.

Responses provided by the attendees focused around improving digital forensics of new emerging areas like IoT, cloud platforms, and artificial intelligence. This also included creating the next generation of forensic techniques to keep up with the changes in the previously listed emerging areas, realizing the growth of potential evidence in crimes, and the always-on connectivity of devices that are manufactured. Furthermore, some panelists reported that the current and future scrutiny by the legal system will have major effects on the digital forensics community. The consensus among the responses was that there should be a unification of training for professionals, a standardization of best practices with professional licenses like that of medical or law school. Another challenge expected to be faced is the major debate between the policy and ethics. How to properly balance the policies over privacy for the people and the much needed access to devices in order to conduct forensics investigations. Finally, one of the most mentioned challenge to be faced in the next five years is low funding for projects or programs suggested in future technologies.

The ideas from the individual panelists do not differ from the themes mentioned in Section 7 during the workshop about key research areas. Research into emerging areas like IoT, cloud computing, distributed storage, and autonomous vehicles was among top recurring research topics. Additionally, further study into decryption methods, improved password cracking, and identification of encrypted data is needed due to data becoming encrypted on all devices. Additionally, the creation of tools to address new fields and technologies like using machine learning to spot unusual patterns in data, understanding of uncertainty, identifying the potentials of error, and real-time forensics analysis are important research endeavours within the next five years. Other research areas of interest suggested were of human augmented digital forensics, cybercrime such as ransomware and various malware, the non-destructive analysis of live systems, and proactive forensics otherwise known as cyber threat hunting.

We also share what workshop experts agreed are the most important job-ready relevant skills needed for the future generations of workers within the next five years. Common responses among the experts were the need to teach good communications skills, problem solving, thinking outside the box, and applying life-long learning skills that can enable the next generation to be the continuous learners. Furthermore, knowledge and skills in topics such as programming, reverse engineering, computer architecture, forensic sciences, network traffic analysis, live forensics analysis, memory analysis, cybersecurity, and incident response are an additional boost to the skills needed by future practitioners. The previously mentioned skills all focus on key areas of study specific to the next generation of workers. Other skills that all future workers should have are proper tool usage skills, ability to manage projects, understand the psychology of crime, and should be able to clearly articulate information into reports.

9 KEY FINDINGS

Results from this workshop indicated that many of the issues plaguing the community in prior years are still valid. We summarize the key findings as follows:

- Limited funding towards research and development in emerging areas.
- A lack of standardization across all areas of the industry, especially regarding policies & ethics and tool development/usage.
- Too much specialization in educational programs and a lack of multidisciplinary approaches.
- A lack of shared information and collaboration with others in the community.
- Many tools and techniques are highly impractical and do not adapt rapidly to industry changes.
- The stature of cyber forensics needs to be improved to emphasize it as a reputable discipline.

10 RECOMMENDATIONS

To tackle these issues it is imperative that the following recommendations be considered and/or implemented in practice.

- Development of an emerging group as part of organizations such as the Association of Computing Machinery (ACM) to make the community a more coherent group within the computing disciplines.
- Increase the number of annual competitions in open-source tool development to encourage practitioners to solve problems in emerging areas.
- The creation of a forensic tool marketplace where tools, their issues, bugs, and tests, and testing datasets are shared with the community.
- Early identification of emerging topics so that standardized processes can be developed, leading to the possibility of more focused and timely funding being provided.
- The creation of flash granting mechanisms for applied cyber forensics research topics with short technological turnarounds.

- Improving inter-grant agency funding collaboration, such as a joint granting effort between DOJ and NSF.
- The creation of focused funding in Cyber Forensics in programs like SaTC, with review panels made up of digital forensics experts.
- Establishing mechanisms for communication channels and collaboration between stakeholders in the community should be improved and encouraged, so that standardized policies, procedures and tools can be developed, utilized and enforced with confidence in the industry.
- Hosting more frequently funded active workshops to discuss the cyber forensics community, the future of the community, and shift focus of the community to current trends.
- Re-examination of educational programs shifting the focus from a specialized approach to one that is multidisciplinary.
- Expanding cyber forensics to other areas to allow stakeholders and students to understand problems as a whole, leading to the development of more efficient solutions.
- Teaching low-level fundamentals in courses for subjects such as encryption, forensic investigations and ethics, which should be standardized and incorporated into programs.

11 FOLLOW-UP WORKSHOP

A successive workshop was held where findings were presented and topics revisited in May of 2018. The workshop was hosted as part of the IEEE Security and Privacy Systematic Approaches to Digital Forensics Engineering (SADFE) program in San Francisco, CA. Nineteen panelists attended the follow-up workshop, eighteen were members of academia and were affiliated with universities, one was from the cybersecurity/forensics industry. Fifteen participants were male, and five were female. Two panelists were present at the preceding workshop and there were several panelists representing foreign universities from Canada, Ireland, and Hong Kong.

At the follow-up workshop, the preceding topics and findings were presented to the group. Following the presentation of each topic, the group further contributed to the discussion and deliberated prior findings. Panelists were invited to introduce new concerns to the discussion. The following presents the discussions and opinions debated in the follow-up workshop.

Education. The domain of natural sciences, where researchers aim to achieve a deeper understanding of preexisting phenomena, contrasts from digital forensics, where the forefront closely tails newly developed technologies. Driving the progression of the field, real-world cases demand the need for innovation and in turn produce many of the tools and fundamentals of the modern investigator. Educators and students alike, are inherently removed from real-world cases, but only by program design.

A panelist, who currently and previously engaged in real-world cases, strongly advocated incorporating this work into the program curriculum. To stimulate student interest and provide unique problems, panelists recommend universities partnering with a local agency and offer their services. The group agreed, noting that each service learning and community engagement opportunity was a learning experience when coupled with an after action review. The discussion was concluded by a panelist noting that often universities are focused only on the prestige of published research, when in fact hands-on learning is more beneficial to the student.

Technology: Tools & Testing. Developing a partnership with a third-party organization may be difficult should viewpoints on forensic tool and intellectual property ownership resulting from an investigation differ. Where academics are bound to disseminate findings, for-profit organizations may be hesitant to publicize valuable tools and knowledge. This fear is exacerbated by the potential of such tools to be used in a malicious manner. Academics may be forced to either contribute their work in an open source forum or participate in real-world investigations in addition to weighing the cost of releasing a tool which could be misused.

Policy & Ethics: Future Directions. The academic value of real-world investigations to the forensic domain is often limited by legal and privacy doctrine. Sensitive resources and methodologies are sparingly shared between organizations, hindering the academic process and uniformity among curriculum. Panelist who had an abundance of real-world datasets were frustrated with their inability to allow students to examine the data. This is something that will be unlikely to overcome, yet the dataset problem can be addressed within the academic community. One panelist, suggested making dataset sharing mandatory.

An organization of industry experts and academics may help to facilitate the sharing of information and the standardization of the field. The prior workshops recommendation for a SIG was further deliberated, discussing the suitability of several organizations. The need for a formal cohesive group, specific to the *digital* forensic sciences was apparent, yet not fully satisfied by the American Academy of Forensic Sciences due to the organization's focus on forensic sciences, and not computing as a major discipline of focus. Although panelists suggest real-world problems drive modernization and innovation, the discussion concluded with the reiteration of the recommendation advocating for a SIG within ACM.

12 CONCLUSIONS AND FUTURE WORK

This work outlined the challenges the Cyber Forensics domain is facing through an active workshop conducted with expert panelists. The panelists deliberated many challenges that need to be addressed, but also produced some tangible steps for moving the domain forward. Panel members explained that an active national workshop like this one should be conducted at least every two years to stay ahead of the domain's challenges, and reassess the community's accomplishment towards improving the state of the art in the field.

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 1649101. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. Acknowledgement goes to the following participants in no particular order: Vassil Roussev from University of New Orleans, Nasir Memon from New York

University, Hany Farid from Dartmouth, Nitin Agarwal from University of Arkansas at Little Rock, Kathryn Seigfried-Spellar and Eugene Spafford from Purdue University, David Dampier, Nicole Beebe and Raymond Choo from University of Texas at San Antonio, Glenn Dardick from Embry-Riddle Aeronautical University, Barbara Guttman from NIST, Josiah Dykstra from National Security Agency, Michael Losavio and Adel Elmaghraby from University of Louisville, David Baker from MITRE, Cindy Murphy from Gillware Digital Forensics, Sergeant Corey Davis from Connecticut Center for Digital Investigations, Tim Vidas from Dell SecureWorks, Frank Adelstein from NFA Digital, David Miele from the Manchester Police Department, Sandip Kundu from the National Science Foundation, Stuart Sidle, Felix Anda from University College Dublin, Siuming Yiu, C.Y. Tsueng and K.P. Chow from University of Hong Kong, Corinne Rogers from University of British Columbia, Zhen Xu and Chen Shi from Iowa State University, Sujeet Shenoi from University of Tulsa, Shoufu Luo from City University of New York, Alec Yasinsac from University of South Alabama, Golika Dorai from Florida State University, Ibrahim Baggili, Frank Breitinger and Xiaolu Zhang from University of New Haven.

REFERENCES

[1] Nicole Beebe. 2009. *Digital Forensic Research: The Good, the Bad and the Unaddressed.* Springer Berlin Heidelberg, Berlin, Heidelberg, 17–36. DOI: http://dx.doi.org/10.1007/978-3-642-04155-6_2

[2] National Science Foundation. 2018. GenCyber. (2018). https://www.gen-cyber.com/about/

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

[4] Cinthya Grajeda, Frank Breitinger, and Ibrahim Baggili. 2017. Availability of datasets for digital forensics–And what is missing. *Digital Investigation* 22 (2017), S94–S105.

[5] Vikram S Harichandran, Frank Breitinger, Ibrahim Baggili, and Andrew Marrington. 2016. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security* 57 (2016), 1–13.

[6] Jim Lyle. 2012. Computer Forensics Tool Testing. *Forensics@ NIST* (2012).

[7] Kara Nance, Brian Hay, and Matt Bishop. 2009. Digital forensics: defining a research agenda. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on.* IEEE, 1–6.

[8] Gary Palmer and others. 2001. A road map for digital forensic research. In *First Digital Forensic Research Workshop, Utica, New York.* 27–30.

[9] Golden G Richard III and Vassil Roussev. 2006. Next-generation digital forensics. *Commun. ACM* 49, 2 (2006), 76–80.

[10] Marcus K Rogers and Kate Seigfried. 2004. The future of computer forensics: a needs analysis survey. *Computers & Security* 23, 1 (2004), 12–16.

[11] Robert J Walls, Brian Neil Levine, Marc Liberatore, and Clay Shields. 2011. Effective Digital Forensics Research Is Investigator-Centric.. In *HotSec.*

Table 4: Post-workshop Survey Analysis

Questions		
Biggest anticipated challenges in the next 5 years		
- Encryption	- Keeping up with technological change	- No standards for best practices
- Collaboration	- Growth of potential evidence	- Hiring shortage especially for the public sector
- Always on connectivity	- Scrutiny by the legal system	- Attribution of crime integrity of evidence
- Autonomous vehicles	- No unified curriculum/training	- Input than just from lawyers and policymakers
- Moving to the cloud	- Structured mapping of all devices	- Bridging disciplines, perspectives, and expectations
- Balancing policy over privacy	- Funding for public sector equipment	- Creating next generation forensics techniques
- Improving efficiency	- Educating judiciary on digital forensics	- Policy and ethics for the changing tech landscape
- Lack of public datasets	- Keeping practitioners current with academia	- Keeping academia current with practitioners
Most important research opportunities in the next 5 years		
- Internet of Things	- Cloud infrastructure	- Distributed storage
- Autonomous vehicles	- Decryption	- Password cracking
- Growing of datasets	- Identification of data around encryption	- Social network analytics
- Cognitive hacking	- Artificial intelligence	- Increase digital forensics analysis
- Cyber-crime	- Interoperability between tools	- Human augmentation for digital forensics
- Malware	- Encryption as it pertains to legal interests	- Data reduction within legal boundaries
- Ransomware	- Understanding of uncertainty	- Tools for spotting unusual patterns in data
- Real-time forensics analysis	- Understanding the potential for errors	- Use of virtualization for hands-on training
- Improving efficiency	- Proactive forensics (cyber threat hunting)	- Non-destructive searching of live systems
- Quantum computing	- Dissecting anonymity	- Attribution
- Automation	- Integrity of evidence	
The most important job-ready relevant skills that need to be addressed by higher education in the next 5 years		
- Communication skills	- Thinking outside the box	- Understanding legal and ethical issues
- Problem solving skills	- Solid programming skills	- Psychology of crime
- Reverse engineering	- Mathematics	- Computer architecture fundamentals
- Mobile forensics	- Life-long learning skills	- Social-cyber forensics analysis
- Live forensic analysis	- Understanding of network traffic	- Fundamentals of forensics sciences
- Memory analysis	- Incident response skills	- Project management skills
- Tool use	- Cybersecurity skills	- Cryptography skills
- Data analytics	- Writing clear reports	

Note: Bold statements represent questions. The rows show all responses in no particular order of importance. Repeated statements were excluded.