8-14-2021

Another Brick in the Wall: An Exploratory Analysis of Digital Forensics Programs in the United States

Syria McCullough
University of New Haven

Stella Abudu
University of New Haven

Ebere Onwubuariri
University of New Haven

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

Publisher Citation

Syria McCullough, Stella Abudu, Ebere Onwubuariri, Ibrahim Baggili, Another brick in the wall: An exploratory analysis of digital forensics programs in the United States, Forensic Science International: Digital Investigation, Volume 37, Supplement, 2021, 301187, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2021.301187 (https://www.sciencedirect.com/science/article/pii/S2666281721000950)

Comments

Article published in, *Forensic Science International: Digital Investigation*, volume 37, Supplement, July 2021.

Forensic Science International: Digital Investigation 37 (2021) 301187

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2021 USA - Proceedings of the Twenty First Annual DFRWS USA

Another brick in the wall: An exploratory analysis of digital forensics programs in the United States

Syria McCullough [1], Stella Abudu [1], Ebere Onwubuariri [1], Ibrahim Baggili*

University of New Haven Cyber Forensics Research and Education Group (UNHcFREG), Connecticut Institute of Technology at the University of New Haven, USA

ARTICLE INFO

Article history:

Keywords:
Digital forensics
Cybersecurity
Computer science
Education
Curriculum

ABSTRACT

We present a comprehensive review of digital forensics programs offered by universities across the United States (U.S.). While numerous studies on digital forensics standards and curriculum exist, few, if any, have examined digital forensics courses offered across the nation. Since digital forensics courses vary from university to university, online course catalogs for academic institutions were evaluated to curate a dataset. Universities were selected based on online searches, similar to those that would be made by prospective students. Ninety-seven (n = 97) degree programs in the U.S. were evaluated. Overall, results showed that advanced technical courses are missing from curricula. We conclude that most degree programs evaluated offer legal/cyber law & ethics, investigative processes, and lab & forensic operations courses. The courses offered the least were memory forensics, Internet of Things (IoT) forensics, and program & software forensics. The data shows that some universities with the Forensic Science Education Programs Accreditation Commission (FEPAC) accreditation are lacking instruction in timely digital forensics topics such as memory forensics (0%), hardware security (0%), program & software forensics (0%), and ethical hacking (0%). Investigative processes (100%), network forensics (100%), lab & forensic operations (100%), and a senior design/capstone project (100%) are offered at all FEPAC accredited universities in digital forensics and digital evidence. Undergraduate degree programs with the National Centers of Digital Forensics Academic Excellence (CDFAE) designation had over a 50% offering rate for 11 out of the 22 courses we evaluated. However, memory forensics (0%) and IoT forensics (12.5%) were largely underrepresented. Our work provides an overview of the current state of digital forensics programs and discusses the importance of these courses to educate the next digital forensics workforce.

1. Introduction

Digital devices are used in nearly every aspect of life and are becoming a staple in most industries such as in government, healthcare, and banking. As industries continue to lean heavily on digital devices for certain processes, this also leads to an increase of detrimental cyber attacks. In September of 2020, a ransomware attack on a university near the Dusseldorf University Hospital in Germany, may have caused the first death directly linked to a cyber attack (Nicole Wetsman, 2020). Cyber crimes such as this one, reinforce the need for skilled cybersecurity professionals in digital forensics. As technology advances, so does the sophistication of the attacks that are carried out with them.

The Digital Forensics market in the U.S. was estimated at $6.1 Billion in the year 2020 and $16.6 Billion by the year 2027. These estimates in the Digital Forensics Global Market Trajectory & Analytics Report highlight the importance of education in this field (Research and Markets Market Research Reports, 2020). While our work focuses on academic digital forensic programs in the U.S., it is important to note that the lack of digital forensic professionals is a worldwide challenge. In 2017, the Federal Investigation Agency (FIA)'s National Response Centre for Cyber Crime (NR3C) had a backlog of 6000 cases within a six month time range (Pakistan Daily Times Islamabad, 2017).

To tackle this workforce demand universities have incorporated digital forensics into their degree programs. Yet, past work showed that digital forensics education programs are not sufficiently preparing students to think abstractly and apply fundamental concepts

* Corresponding author.
E-mail addresses: smccu1@unh.newhaven.edu (S. McCullough), sabud1@unh.newhaven.edu (S. Abudu), eonwu1@unh.newhaven.edu (E. Onwubuariri), ibaggili@newhaven.edu (I. Baggili).
[1] Cybersecurity & Networks Graduate Student

https://doi.org/10.1016/j.fsidi.2021.301187

in the field (Luciano et al., 2018). The lack of standardization in digital forensics education means universities are offering different courses which may not fulfill the skills needed in industry.

The diversity and abundance of emerging programs in the U.S. related to cybersecurity and digital forensics makes it imperative to conduct a meta-analysis of the state of curricula to gain deeper insight into their similarities and differences. Thus, our work presents the following contributions:

- Our work provides a primary analysis on (n = 97) degree programs in the U.S. related to digital forensics.
- Our work explores courses taught in already designated National Security Agency Centers of Academic Excellence (NSA-CAE) programs, Forensic Science Education Programs Accreditation Commission (FEPAC), and National Centers of Digital Forensics Academic Excellence (CDFAE) programs to shed light on what courses exist and what courses are missing.
- Our work presents a necessary update for academia, to explore both adequacy and deficiencies in digital forensic curricula course content.

The remainder of this paper is divided into the following sections. Section 2 describes background information and related work. Section 3 details the limitations and Section 4 outlines the methodology used to categorize and make comparative analyses. Next, Section 5 discusses the results obtained from the completion of the study. Section 6 is the key findings, Section 7 is the discussion, and lastly Section 8 contains our conclusion and future work.

2. Background and related work

Digital forensics education comes with its own unique challenges such as the lack of standards in analyzing data and the lack of qualified digital forensics investigators (Eva, 2016). explains that digital forensics does not require the same standards or licenses that other professions require, such as doctors or lawyers. Additionally, digital forensics certificates are not testing to determine if the applicant is qualified, instead it merely “indicates the person has met the minimum requirements to pass the certification exam” (Eva, 2016; Huber, 2010).

The work in (Simon, 2010) noted that labs have to purchase and test each tool which is not fiscally responsible, and that some open source software is not thoroughly documented. This challenge is exacerbated by the lack of training, where organizations reported that it takes one to two years on the job before investigators are proficient (Simon, 2010). Recently, the Digital Forensic Science Strategy in the U.K. (The National Police Chiefs Council, 2020) listed one of the issues in digital forensics science as the lack of collaboration between academia and industry with the police. It would be a mutually beneficial relationship for all three fields, academia, industry, and Law Enforcement (LE) to work together.

To tackle these challenges from a workforce development standpoint, two major thrusts have been underway by academicians in (1) digital forensics program development, and (2) novel ways for digital forensics education.

2.1. Digital forensics educational program development

Several academic institutions have established two-year or four-year academic programs in digital forensics, either on their own or in conjunction with other institutions. Among these are Elgin Community College in Illinois, Erie Community College in New York, and the University of Central Florida in Florida.

Elgin Community College pursued its efforts using two major National Science Foundation (NSF) grants awards #0903090 (Adams et al., 2009) and #0802062 (Donna Kaputa and rao, 2008), to prepare undergraduate students with essential digital forensics skills via a curriculum incorporating both computer science and criminal justice.

The University of Central Florida has also been granted NSF award #1723587 (Jin and Zou, 2017), to create an online graduate program focusing on both defensive and post-attack digital forensics. In addition to introductory classes, the program includes hands-on labs to train students in the areas of networked critical infrastructures, computers, smart devices, and Internet of Things (IoT).

Union County College, New Jersey, was granted NSF award #1601060 (Hawthorne and Joyce, 2016), to create and implement a digital forensics Associates degree program curriculum combining experiential education and service learning.

From a curriculum standpoint, the University of Illinois at Urbana-Champaign was granted NSF award #1241773 (Bashir et al., 2014). Their aim was to create an interdisciplinary, standardized, digital forensics curriculum, modeled on curricula proposed by National Security Agency (NSA), Department of Homeland Security (DHS), Security Centers for Academic Excellence, Association of Computer Machinery (ACM), and the Institute of Electrical and Electronics Engineers (IEEE).

While several projects aimed to educate undergraduate and graduate students, others opted to create a curriculum to train those already working in law enforcement and law. The University of Alabama at Birmingham, for example, was granted NSF award #1723768 (Hasan and Walker, 2017) to teach the theory and practice of digital forensics to law enforcement and judicial personnel utilizing specialized courses and educational modules, designed to be scalable for nationwide use.

In 2017 (Bishop et al., 2017), the Joint Task Force on Cybersecurity Education developed a model for the development of cybersecurity programs. This model consisted of knowledge areas, cross-cutting concepts, disciplinary lens, and application areas. Digital forensics is included under the knowledge area System Security because it is needed for multiple disciplines. Also, the Accreditation Board for Engineering and Technology (ABET) Computing Accreditation Commission (CAC) accredits undergraduate computing programs. It provides fundamental topics as part of the curriculum requirement but it does not outline specific courses (ABET, 2020).

Lastly, digital forensics has been integrated into business programs. In (Wen and Yang, 2017), researchers evaluated cybersecurity curriculum to create a model at accredited business schools in the U.S. that offered Information Systems (IS) and technology programs. Even though they did not evaluate programs in computer and digital forensics, they concluded that in the twenty-seven cybersecurity programs they surveyed, 30% required a digital forensics course.

2.2. New ways for digital forensics education

Another approach to address challenges in educating current and future digital forensics students is to explore and implement novel ways of teaching in digital forensics. For example, the Naval Postgraduate School in California, recognizing the limitations of using non-realistic disk images, log files, and network packet dumps, was granted award #0919593 (Garfinkel and Dittrich, 2009), to develop and employ authentic digital forensic data for undergraduate education and research.

In another project, the University of Massachusetts at Lowell was granted award #0942113 (Fu and Liu, 2010), to design and implement an educational framework consisting of realistic cybercrime scenes and laboratory projects to teach network

forensics to undergraduate and graduate students.

Lastly, the Rochester Institute of Technology in New York, in partnership with Corning Community College and Onondaga Community College, was granted NSF award #1400567 (Pan et al., 2014) to introduce game-based modules to teach digital forensics to entry-level or lower-level undergraduate students.

While past work explored developing digital forensics programs, and novel educational approaches, it did not assess the current state of existing programs to determine digital forensics courses that need better representation in education.

3. Limitations

While our work is comprehensive, we recognize that is has the following limitations:

- **Manual Analysis**: Our data was collected and analyzed manually which leaves the potential for human error and interpretation differences. Additionally, the scope of work was conducted during the COVID-19 pandemic, making it difficult to receive additional information on course catalogs.
- **Vague Descriptions:** Some course catalogs were vague and did not provide clear descriptions for the courses they offered. For example, instead of clearly stating that students will learn C/C++, some course catalogs would state that students will learn a low-level programming language and offer a broad overview. In this case, the programming course category was marked "N/S" which means not specified, content description was unclear.
- **Catalog Updates:** Some course catalogs may not be up to date. It is possible that some universities could have added more classes to their curriculum and had not updated their course catalogs before we collected data for this study.
- **Teaching Deviation From Course Catalogs:** Instructors may deviate from the original course outline and include more or less than the descriptions available online. Thus the material taught in the classroom may be different from what is on the website.

4. Methodology

A number of universities and colleges offer digital forensics degrees and other related disciplines in computer forensics. Each has its own curriculum, some more well-rounded than others. To get better insight into the digital forensics programs available to prospective students, we accumulated a collection of courses suggested by experts that are deemed as imperative to the field and analyzed how often they are offered across all analyzed programs.

4.1. Selection criteria

The curricula for the selected universities, found on their respective websites, was used to curate our dataset. All universities were chosen based on online searches, similar to those that would be made by prospective students. Ninety-seven degree (n = 97) programs in the United States were chosen for this study. We focused on bachelors, masters, and certificate degrees offered for majors in digital forensics, cybersecurity, computer science, information technology, and other related degrees that offered digital forensic courses.

The number of universities with the National Centers of Digital Forensics Academic Excellence (CDFAE) designation at the time of writing this paper was 16. Universities with this designation are deemed by the U.S. government, academia, and standard bodies to embody the best practices for digital forensic education (DC3, 2020). Other universities included in our analysis hold designations from the National Security Agency (NSA) as National Center of Academic Excellence in Cyber Operations (CAE-CO), Cyber Defense Education (CAE-CD), or Cyber Defense Research (CAE-R). Some universities selected did not have any of these designations.

4.2. Curriculum

CDFAE designated schools are deemed to have well-rounded digital forensics curricula needed to equip students with the knowledge and skills to become digital forensic professionals. The Department of Defense Cyber Crime Center (DC3, 2020) outlined seven knowledge domains which we used within our course selection dataset. These knowledge domains are:

1. Investigative Processes
2. Lab and Forensic Operations
3. Legal and Ethics
4. Network Forensics
5. Program and Software Forensics
6. Quality Assurance, Control and Management
7. Storage Media

In addition to these seven knowledge domains, twenty-two courses were reviewed in total. These courses were chosen based on their importance in the digital forensics field today. The remaining analyzed courses were:

1. Advanced C/C++
2. Assembly Programming
3. C/C++
4. Disk Forensics
5. Ethical Hacking
6. File System
7. Hardware Security
8. Introductory Programming
9. IoT Forensics (Internet of Things)
10. Java
11. Malware and Software Analysis
12. Memory Forensics
13. Mobile Forensics
14. Python
15. Senior Design/Capstone or thesis option

4.3. Review process

The course catalog for each selected university was reviewed. Fig. 1 shows how courses were analyzed individually, by title and

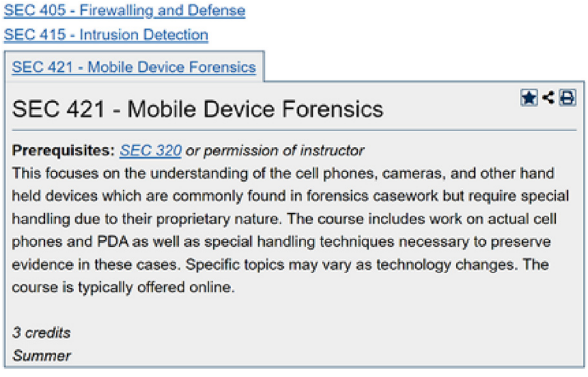

Fig. 1. Course catalog content description from Roger Williams University.

content description.

Data was only gathered from universities that have digital forensic degree programs or those which had digital forensics courses offered as part of other cyber related degrees. Other criteria that was logged and evaluated were the credit hours and whether the universities are public or private institutions. Microsoft Excel was used to log and interpret the data collected.

5. Results

We curated a dataset that is diverse and representative of the state of academic programs in the U.S (See Table 1). Overall 78 institutions and 97 programs in the U.S. between undergraduate, graduate, and certificate programs were reviewed. As shown in Table 1, there is diversity amongst the designation, program levels, regions, degree types, institutional types and the average number of credit hours of the explored academic programs. In the sections that follow, we explore the results of our granular analysis of the programs by exploring the type of courses being taught in each program.

The top ranked offered courses are investigative process, legal & ethics, and lab & forensics operations. These courses satisfy the lab component to simulate real world problems and make courses more detailed instead of introductory. For undergraduate programs 75% offered a senior design/capstone and for the graduate programs 84% offered a thesis option.

5.1. Undergraduate course rankings

The results in Fig. 2 show that most undergraduate degree programs offer introductory programming (92%), investigative processes (83%), legal/cyber law & ethics (83%), lab & forensic operations (81%), senior design/capstone (75%), quality assurance (control & management) (62%), network forensics (59%), malware & software analysis (58%), mobile forensics (60%), and storage media (56%).

The least offered courses are memory forensics (10%), advanced C/C++ (10%), IoT forensics (15%), program and software forensics (17%), disk forensics (25%), python (25%), java (25%), C/C++ (29%), assembly programming (29%), ethical hacking (32%), hardware security (44%), and file systems (50%). A related point to consider is that the course curriculum of institutions lacking relevant security and forensic courses as opposed to programming courses can be weighed differently. It is important for students to be introduced to emerging topics in security and forensics so programs not offering these courses should update their curriculum. In terms of programming courses, a student may fulfill a programming requirement with another language.

The courses with the highest not specified percentages are java (37%), python (35%), C/C++ (33%), Advanced C/C++ (30%), and assembly programming (23%). This is due to course catalogs having vague descriptions about the programming languages they require students to learn.

In Table 2 eighteen out of the twenty two courses we selected were grouped into three respective categories. Security courses included hardware security, legal & ethics, quality assurance (control & management), ethical hacking, and malware & software analysis. Next, the forensic courses included file system, network forensics, program & software forensics, mobile forensics, memory forensics, disk forensics, IoT forensics, and storage media. Programming courses included introductory programming, advanced C/C++, C/C++, python, java, and assembly programming.

Security courses were offered the most compared to the other two categories at 58%. The forensics and programming courses only had a 2% difference at 38% and 36% respectively. It is important to note that the programming courses were also among the highest "not specified" percentages.

In our dataset, we included which institutions were private or public. Fig. 3 shows the percentage of courses offered for the private and public universities/colleges. There was not a significant variation between the private and public institutions.

Table 1
Description of the collected dataset. Note: for Categories without $\sum = 97$ such as Designation, it is because some institutions had multiple designations, or because it did not apply. Data corresponds to the number of degree programs, not the number of academic institutions.

Category	Data
Designation	NSA CAE-CD = 55
	NSA CAE-R = 22
	None = 19
	CDFAE = 17
	NSA CAE-CO = 13
	FEPAC = 3
Program Level $\sum$ = 97	Undergraduate = 52
	Graduate = 25
	Certificate = 20
Region $\sum$ = 97	Northeast = 31
	Southeast = 30
	Midwest = 15
	Southwest = 10
	Online = 9
	West = 2
Degree Type $\sum$ = 97	Digital Forensics (DF) = 39
	Cyber = 23
	CS = 14
	Information Technology = 10
	DF & Cyber = 8
	Criminal Justice = 3
Institutional Type $\sum$ = 97	Public = 58
	Private = 39
Average # Credit Hours	Undergraduate = 120
	Graduate = 34
	Certificate = 16

5.2. Graduate course rankings

Similar to the undergraduate programs, investigative processes is one of the top ranked courses for the graduate degrees at 92% as shown in Fig. 2. The next highest ranked courses are legal & ethics (84%), senior design/capstone (84%), lab & forensic operations (80%), network forensics (76%), ethical hacking (68%), quality assurance (control & management) (52%), and malware & software analysis (52%).

The least offered courses are assembly programming (4%), and java, advanced C/C++, and program & software forensics all offered in 8% of the course catalogs. Followed by C/C++ (12%), python (16%), IoT forensics (20%), hardware security (20%), introductory programming (24%), memory forensics (28%), disk forensics (28%), storage media (36%), mobile forensics (40%), and file systems (40%).

5.3. Digital forensics certificates

Fig. 4 clearly shows deficiencies in the number of courses not offered. The average credit hours for digital forensic certificates offered through universities is 16–17, which means that all the courses we compiled cannot be covered. The top three courses among the certificates are similar to the undergraduate top courses which are investigative processes (100%), lab & forensic operations (75%), and legal/cyber law & ethics (65%).

The courses that were offered less frequently were quality assurance (control & management) (5%), senior design/capstone (5%), C/C++ (5%), introductory programming (10%), python (10%),

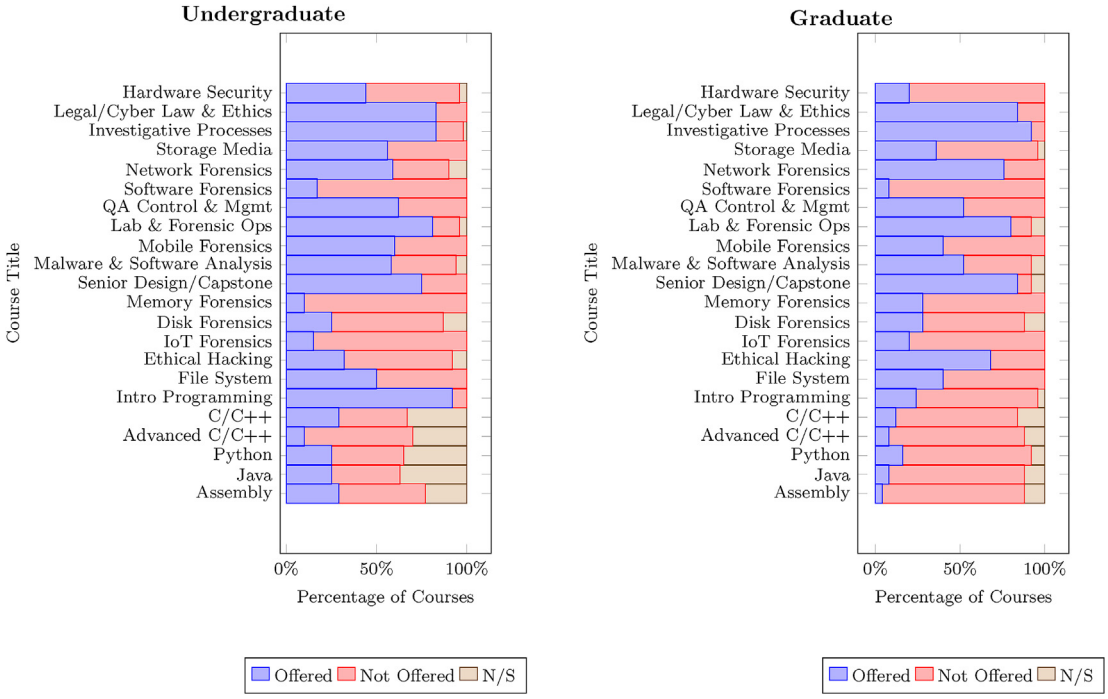

Fig. 2. Overall percentage of (n = 52) undergraduate and (n = 25) graduate courses from online course catalogs that are offered, not offered, and not specified.

Table 2
Percentage of Security, Forensic, and Programming courses offered for undergraduate degrees.

	Security courses	Forensic courses	Programming Courses
Offered	145	152	109
Total	250	400	300
% offered	58	38	36

IoT forensics (15%), storage media (25%), malware & software analysis (30%), mobile forensics (35%), file systems (40%), and network forensics (45%).

A significant percentage of the courses we selected were not offered for certificates such as hardware security, program & software forensics, memory forensics, disk forensics, ethical hacking, advanced C++, assembly programming, and java. These certificates can supplement a digital forensics education but should not be used as a replacement.

5.4. CDFAE accreditation

In Fig. 5, the academic institutions that have a National Centers of Digital Forensics Academic Excellence (CDFAE) designation were reviewed. The top programs offered at CDFAE designated schools are network forensics (100%), lab and forensic operations (87.5%), investigative processes (87.5%), legal/cyber law & ethics (87.5%), introductory programming (87.5%), storage media (75%), mobile forensics (75%), malware & software analysis (75%), senior design/capstone (75%), ethical hacking (62.5%), and file systems (62.5%).

The programs that are offered the least are memory forensics and advanced C/C++ at 0% and C++, java, assembly programming, and IoT forensics at 12.5%. Followed by program & software forensics, quality assurance (control & management), and python at 25% and disk forensics and hardware security at 37.5%.

5.5. FEPAC accreditation

For the FEPAC accreditation, the commissions goal is maintain and enhance the quality of forensic science education (FEPAC, 2019). The accreditation is for forensic science degree programs but includes natural or computer science degrees with a forensic science concentration. Currently, there are only three universities with this accreditation that are related to digital forensics.

In Fig. 5 it shows that a senior design/capstone project, network forensics, and investigative processes course are all required for these accredited universities at 100%. The courses that are not offered across the three universities are hardware security, program & software forensics, memory forensics, ethical hacking, C++, advanced C/C++, python, java, and assembly programming. Legal/cyber law & ethics, mobile forensics, IoT forensics, file systems, and introductory programming are all offered at 67% and storage media, quality assurance (control & management), malware & software analysis and disk forensics at 33%.

6. Key findings

The key findings are summarized as follows:

- The undergraduate courses that are offered 80% or more in the curriculum are introductory programming, legal/cyber law and ethics, investigative processes, and lab and forensic operations.
- The undergraduate courses that are not offered 80% or more in the curriculum are memory forensics, IoT forensics, and program and software forensics.
- The graduate courses that offered 80% or more in the curriculum are investigative processes, legal/cyber law and ethics, capstone or thesis option, and lab & forensic operations.
- The graduate courses that are not offered 80% or more in the curriculum are program and software forensics, assembly programming, hardware security, IoT forensics, advanced C/C++ and java.

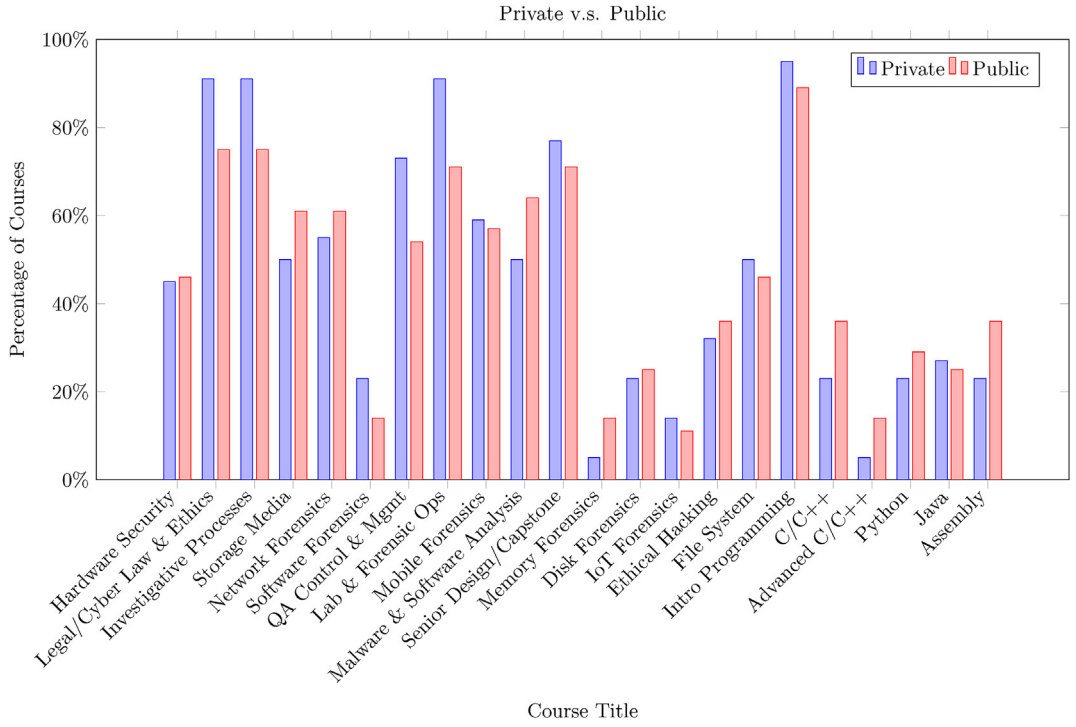

Fig. 3. Percentage of courses offered for (n = 22) private and (n = 28) public universities/colleges undergraduate degrees.

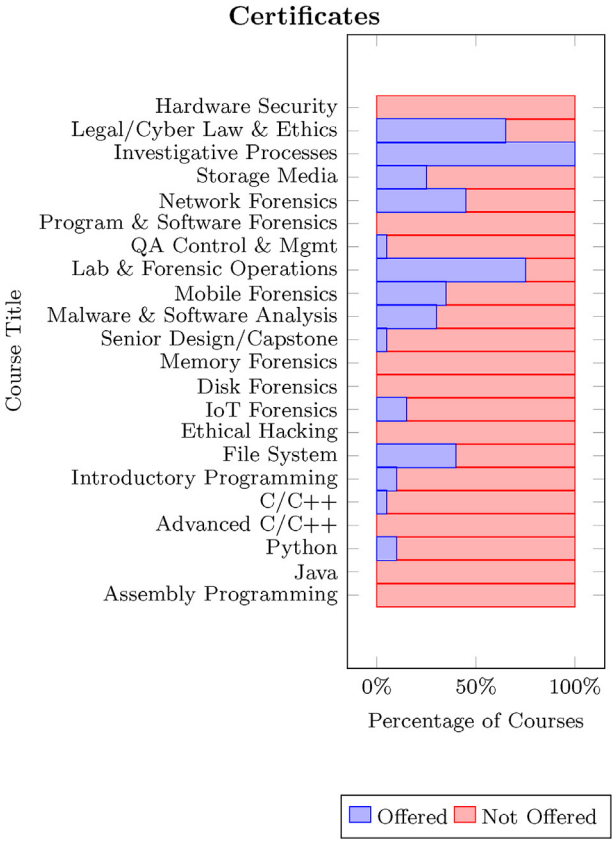

Fig. 4. Overall percentage of courses offered, not offered, and not specified for digital forensics certificates (n = 20).

- The only undergraduate and graduate certificates courses that are offered 80% or more is investigative processes, followed by lab and forensic operations at 75%.
- A significant amount of the courses are not offered 80% or more in the undergraduate and graduate certificates. These courses are hardware security, program and software forensics, memory forensics, disk forensics, ethical hacking, advanced C/C++, java, assembly programming, C/C++, python, senior design/capstone, quality assurance (control and management) and IoT forensics.
- There is a lack of standardization in digital forensics education. Standardization could solve some of the challenges that the digital forensics industry faces.

7. Discussion

Previous work in (Lang et al., 2014) identified the reasons why it is difficult to implement a digital forensics program. Among those reasons, the researchers list the lack of curriculum standards as a factor, increasing the difficulty in developing a program. This obstacle indirectly affects other challenges in creating a digital forensics program, such as finding qualified faculty and setting up lab exercises and deciding which equipment/tools to include.

Section 28.14.7 of The Global Practice of Forensic Science, labeled Digital and multimedia sciences, states “Computer and digital forensics, and cyber/information security undergraduate and graduate majors at traditional and on-line academic programs are growing in the United States. Graduates of programs may pursue positions in digital forensics, cyber security, and law enforcement positions as forensic analysts, information specialists, and forensic/criminal investigators in public and private agencies” (Ubelaker et al., 2012). This statement outlines the problems discussed in this paper. Computer and digital forensics, and cyber/information security majors, both undergraduate and graduate are

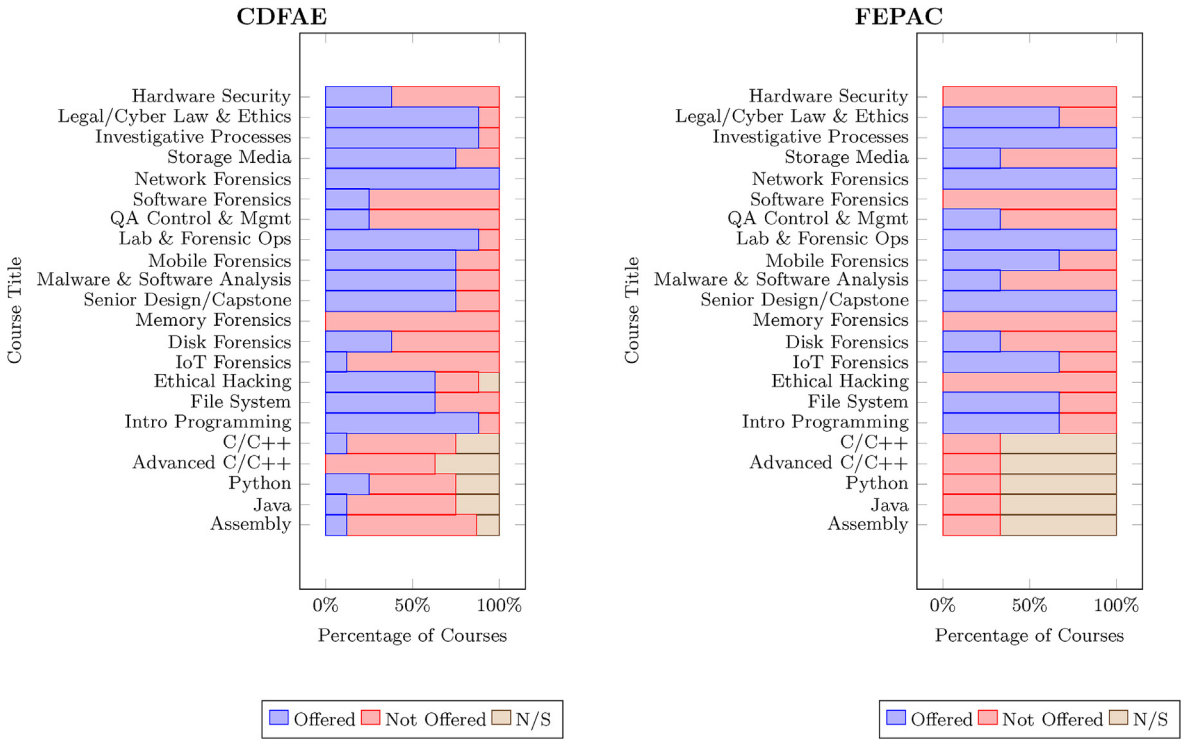

Fig. 5. Overall percentage of courses that are offered, not offered, and not specified for (n = 8) CDFAE and (n = 3) FEPAC accredited universities/colleges.

listed as viable degrees for several professions including digital forensics. Since there is a range of degrees that fall under this category, there should also be a standard digital forensics curriculum implemented in each of these majors to ensure that students are actually learning the necessary knowledge and skills to become digital forensics investigators. Sending students into the workforce under-prepared has led to the issue that has been consistently stated in the digital forensics field; a lack of qualified professionals. A direct impact of under qualified professionals is that it takes longer to complete digital forensics investigations creating a backlog of cases.

When students are searching for a digital forensics program, they should look further than the accreditation, to the course catalog and plan of study. In the FEPAC accreditation standards (FEPAC, 2020), under curriculum for Undergraduate Program Standards, it lists the requirements for specialized digital forensic science courses. These topics are acquisition of data, network/"live" forensic analysis, and exploitation of mobile devices. While these topics are important, more topics should be covered for a student looking to become a digital forensics examiner. For example, none of the FEPAC accredited universities offer memory forensics or ethical hacking. Expanding the FEPAC requirements and digital forensics curriculum at universities to include more topics that are relevant in field could cut down on the time it takes for individuals to become proficient investigators.

The CDFAE designation is focused on providing the knowledge and skills students will need in the field. As a result, half the courses we reviewed were offered at CDFAE designated universities over 50% of the time. Improvements could be made to include memory forensics and advanced C/C++ courses and increase the frequency in which the 22 courses appear on CDFAE designated university course catalogs. However, compared to the FEPAC accreditation, receiving a digital forensics degree from a CDFAE designated university, based on the courses we reviewed, is more likely to provide the necessary skills needed to pursue a career in digital forensics.

The 50 undergraduate degree programs we evaluated showed that the percentage of offered courses between public and private universities are similar, they followed the same overall trend.

Based on the results of this study, universities are on the right track by including digital forensics at their institutions, however, they need to update their curriculum to include deeper technical courses. Memory forensics is one of the courses that is not frequently offered in undergraduate, graduate, or digital forensics certificates. Memory forensics was only offered in 10% of undergraduates degrees, 33% in graduate degrees, and not in any of the university certificates we reviewed. In (Vrizlynn et al., 2010), the authors explain that digital forensics procedures need to update and include memory forensics to analyze the dynamic and volatile memory in order to have a complete investigation. Memory forensics is a vital topic in digital forensics and in high demand compared to the number of qualified professionals. Students should know how to analyze a computer that was left powered on and have the skills to retrieve the volatile data that would be lost once the machine is turned off.

85% of the universities are also not offering IoT forensics. IoT forensics should be included in a comprehensive digital forensics curriculum. The amount of IoT devices is increasing, therefore, IoT forensic courses are necessary in universities and colleges to teach students how to obtain digital evidence from a plethora of devices, especially since standard digital forensic tools and methods do not work with newer IoT devices (Servida and Casey, 2019). Furthermore, 83% of the universities are not offering program and software forensics. A course such as this one is can introduce students to another branch of science one that involves software patents and copyrights, and more importantly malware analysis (Barrett, 2012).

Lastly, there is no uniformity in which colleges within a university offer digital forensics and related degrees. In this study, we found that some universities offered the selected courses in the college of engineering while others placed it in the college of arts & sciences, the college of computer science, or the college of business.

While digital forensics spans various industries, having the same degree title offered at different colleges and departments across multiple universities can attest to the disorganized state of digital forensics education. It may also attest to the multidisciplinary nature of the domain.

It would be beneficial for universities/colleges to implement the missing courses. Teaching students during their education instead of relying on work experience after graduation will help produce more qualified digital forensic investigators, reduce the number of backlog cases due to inefficiency and hopefully lead to bridging the gap in the cybersecurity/digital forensics workforce.

8. Conclusion & future work

Based on the digital forensics programs we analyzed, it became clear that some courses have a higher priority than others. We found that investigative processes, lab & forensic operations, an legal & ethics courses appeared the most in the online course catalogs. Universities seem to be unified on this front, however, there remains discrepancies amongst other courses across institutions of higher education. Most universities did not offer a memory or IoT forensics course. It is up to the individual institution to decide on which courses to prioritize in their programs curriculum. Public and private institutions seem to be alike when compared resulting in no significant difference between the two.

Additionally, our work found that many of the online university course catalogs are not specific enough, as in, they use vague descriptions. These course catalogs should include more detail to provide prospective students a clear description of the course objectives so they can make informed decisions.

To conclude, universities need to take a deeper technical approach to digital forensics education, and to keep up with technological changes. While standards are important, and may provide a level of excellence an institution may want to attain, they need to be flexible and allow universities to create new courses that are representative of what investigators will encounter in the real world.

Future work should explore conducting surveys and interviews to explore the similarities and differences between what is taught and what is available in course catalogs. Also a similar longitudinal study could offer insight into how and if curricula are changing overtime with respect to domain and workforce needs.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 1921813. 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. We would also like to acknowledge Courtney Hassenfeldt, Sahara Fathelbab, Muna Abdelrazeq, and Tiffanie Edwards for their support and insightful feedback.

References

Abet. Criteria for accrediting computing programs, 2020 – 2021. URL. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2020-2021/. Revised by FEPAC:16-February-2020.

Adams, Jeffery Boyd Scott, Pelczarski, Mark, Davy, Laraine, 2009. Integrating internet security with law enforcement through digital computer forensic science. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=0903090&HistoricalAwards=false.

Barrett, Diane, 2012. Book review: the software ip detective's handbook: measurement, comparison, and infringement detections. The Journal of Digital Forensics, Security and Law 7 (1).

Bashir, Masooda, Applequist, Jenny A., Campbell, Roy H., DeStefano, Lizanne, Garcia, Gabriela L., Lang, Anthony, 2014. Development and Dissemination of a New Multidisciplinary Undergraduate Curriculum in Digital Forensics.

Bishop, Matt, Burley, Diana, Scott, Buck, Ekstrom, Joseph J., Futcher, Lynn, Gibson, David, Elizabeth, K., Hawthorne, 2017. Siddharth kaza, yair levy, herbert mattord, and allen parrish. Cybersecurity curricular guidelines. In: Information Security Education for a Global Digital Society (Ed.), Matt Bishop, Lynn Futcher, Natalia Miloslavskaya, and Marianthi Theocharidou. Springer International Publishing, Cham, ISBN 978-3-319-58553-6, pp. 3–13.

Dc3, 2020. National centers of digital forensics academic excellence cdfae. URL. https://www.dc3.mil/Cyber-Training/National-Centers-of-Digital-Forensics-Academic-Excellence-CDFAE/. Accessed:05-February-2021.

Donna Kaputa, Shambhu Upadhyaya, rao, Raghav, 2008. Computer Security and Investigations: an Integrative Approach to Curriculum Development in Digital Forensics. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=0802062&HistoricalAwards=false.

Eva, A., 2016. Vincze. Challenges in digital forensics. Police Pract. Res. 17 (2), 183–194.

FEPAC, 2019. Forensic Science Education Programs Accreditation Commission. URL. https://www.fepac-edu.org/. Accessed:02-February-2021.

FEPAC, 2020. Fepac Accreditation Standards. https://www.fepac-edu.org/sites/default/files/2021%200301%20FEPAC%20Standards.pdf. Revised by FEPAC:16-February-2020.

Fu, Xinwen, Liu, Benyuan, 2010. Creating Learning Materials and Strategies for Network Forensics Education. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=0942113&HistoricalAwards=false.

Garfinkel, Simson, Dittrich, Dave, 2009. Creating Realistic Forensic Corpora for Undergraduate Education and Research. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=0919593&HistoricalAwards=false.

Hasan, Yuliang Zheng Ragib, Walker, Jeffery, 2017. Digital Forensics Education for Judicial Officials. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1723768&HistoricalAwards=false.

Hawthorne, Cynthia Roemer Elizabeth, Joyce, Elizabeth, 2016. Cyber Service! Interdisciplinary and Experiential Education for Cyber Forensics Technicians. URL https://www.nsf.gov/awardsearch/showAward?AWD_ID=1601060&HistoricalAwards=false.

Huber, E. (2010). Certification, licensing, and accreditation in digital forensics. A Fistful of Dongles. URL http://ericjhuber.blogspot.com/2010/11/certification-licensing-and.html.

Jin, Yier, Zou, Cliff, 2017. Online Digital Forensics Courses and Labs for Students and Professionals. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1723587&HistoricalAwards=false.

Lang, Anthony, Bashir, Masooda, Campbell, Roy, DeStefano, Lizanne, 2014. Developing a new digital forensics curriculum. Digit. Invest. S76–S84.

Luciano, Laoise, Baggili, Ibrahim, Topor, Mateusz, Casey, Peter, Frank, Breitinger, 2018. Digital forensics in the next five years. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018. Association for Computing Machinery, New York, NY, USA, ISBN 9781450364485. https://doi.org/10.1145/3230833.3232813.

Nicole Wetsman, 2020. Woman Dies during a Ransomware Attack on a German Hospital. The Verge.

Pakistan Daily Times Islamabad, 2017. Lack of Staff Keeps Fia from Clearing Cyber Cases Backlog. Daily Times, Islamabad, Pakistan).

Pan, Sumita Mishra Yin, McCarthy, Pamela, McNett, Alicia, 2014. Gamified" Digital Forensics Course Modules for Undergraduates. URL. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1400567&HistoricalAwards=false.

Research and Markets Market Research Reports, 2020. Digital Forensics - Global Market Trajectory Analytics.

Servida, Francesco, Casey, Eoghan, 2019. Iot forensic challenges and opportunities for digital traces. Forensic Sci. Int.: Digit. Invest. 28, S22–S29.

Simon, L., 2010. Garfinkel. Digital forensics research: the next 10 years. Digit. Invest. 7, S64–S73.

The National Police Chiefs Council, N.P.C.C., 2020. Forensic capability network, association of Police & crime commissioners, and transforming forensics. Digital forensic science strategy.

Ubelaker, Douglas H., Alamade, Hugo, Alva-Rodriguez, Mario, Beh, Philip, Benomran, Fawzi, 2012. The global practice of forensic science. Forensic Science in Focus.

Thing, Vrizlynn L.L., Ng, Kian-Yong, Chang, Ee-Chien, 2010. Live memory forensics of mobile phones. Digit. Invest. S74–S82.

Wen, B., Yang, S.C., 2017. Toward a cybersecurity curriculum model for undergraduate business schools: a survey of aacsb-accredited institutions in the United States. J. Educ. Bus. 92 (1), 1–8.