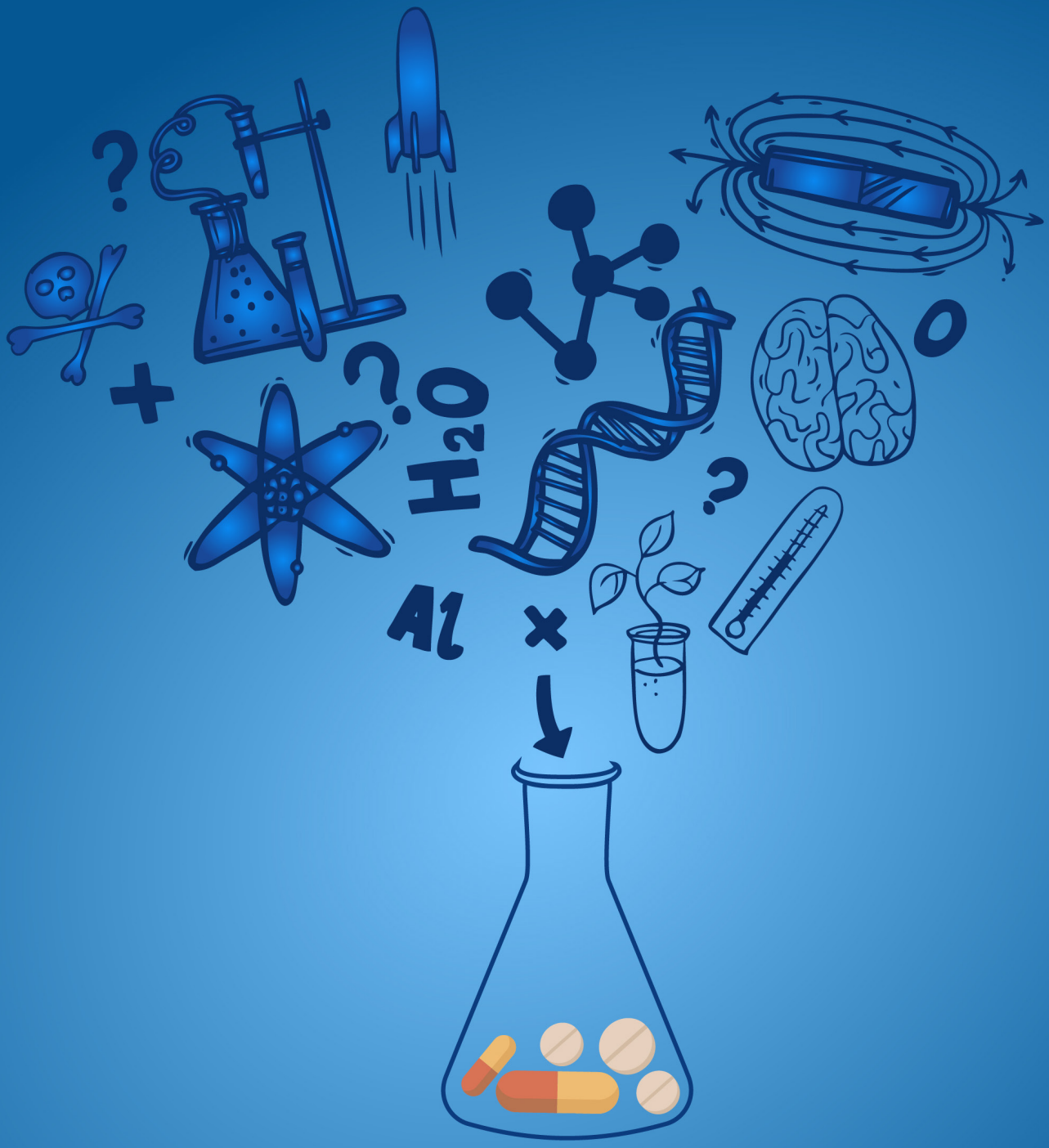
AMERICAN JOURNAL OF CHEMISTRY AND PHARMACY (AJCP)

ISSN: 2834-0116 (ONLINE)

VOLUME 1 ISSUE 2 (2022)



PUBLISHED BY: E-PALLI, DELAWARE, USA

American Journal of Chemistry and Pharmacy (AJCP)

Volume 1 Issue 2, Year 2022
ISSN: 2834-0116 (Online)
DOI: https://doi.org/10.54536/ajcp.v1i2.1077
https://journals.e-palli.com/home/index.php/ajcp

Computer Forensics Education: The Applications of Forensic Tools in Modern Education System

Samy Abdelwahab Safaan[1*]

Article Information

Received: December 15, 2022

Accepted: December 23, 2022

Published: December 29, 2022

Keywords

Computer Forensics Education, Cyber Security, Digital Forensics, Digital Forensic Tools, Encase, FTK

ABSTRACT

Cybercrime and computer-related incidents are becoming more prevalent and common, resulting in billions of dollars in damages. To address these crimes and scams, there is an urgent need to build digital forensics training programme, that will equip relevant professionals to investigate computer crime and events efficiently. There is presently no standard that governs the development of an academic program's digital forensics curriculum. This study extensively investigates prior work on curriculum design in digital forensics as well as existing computer forensics course offered at the first is the Community College in Buraidah, and the second is the Community College in Unaizah namely, "Cyber Security Diploma" The Cyber Security Diploma is offered in both colleges, the Community College in Buraidah and Unaizah, and the diploma is at the third level of the course "Computer Forensic Analysis," which is the focus of the research topic. Interviews were conducted with both digital forensic trainers and practitioners, and the findings were examined in order to identify and assess the skills and knowledge required by the industry and law enforcement agencies for their digital forensic examiners. Hands-on training may be delivered by constructing and managing a student laboratory specifically designed for digital forensic examination instruction. A laboratory can be outfitted with a wide range of software solutions, ranging from commercial investigation suites to free command line tools. Similarly, the forensic workstations that execute the software might be supplied by the vendor as stand-alone devices or assembled from separate components in-house. Building and administering a student lab successfully can be a daunting task, but it can also be done on a little budget as long as the focus stays on student achievement.

INTRODUCTION

The use of digital items has grown engrained in our professional and personal lives as computer and Internet technologies have advanced. Email and online chat, for example, have become commonplace modes of communication. Computer systems and the Internet are used by organizations and businesses for E-commerce, Corporate Communication, and Internal administration (Sindhu & Meshram, 2012)Society is so reliant on computers and Internet technology that the Internet infrastructure has become the backbone of communications, education, healthcare, transportation, and warfare, among many other things (Tsai, 2015). Because of its importance in our society, technology has become a target for cybercriminals, scammers, and terrorists (Casey, 2020). Cybercrime and device incidents continue to play a role and common, resulting in hundreds of billions in damages, highlighting the need to train a skilled workforce to limit, prevent, and prosecute these crimes, frauds, and attacks through efficient digital forensics. However, because digital technology systems are so complicated and dynamic, digital forensic investigators must have appropriate understanding as well as a diverse range of skills.

Computer Forensics is used to acquire digital evidence form a wide range of crimes such as child pornography, financial fraud, identity theft, cyberstalking, homicide, kidnapping, and rape (Harvey, 2019). During the investigation of digital devices, Computer Forensics investigators employ a number of software tools. These technologies are essential for gathering and assessing digital evidence (Tilekar). Forensic investigation in general, and especially hard disks examination, is difficult for an investigator because of the requisite technical background, such disk examinations typically have a pretty high learning curve (Garfinkel, 2013). The high learning curve is partially caused by the wide spectrum and accessibility of forensic investigative tools. There are numerous tools to consider, both commercial and open source. Increasingly popular tool, particularly free source, are becoming accessible on a regular basis. To varied degrees, these tools offer layers of information that assist forensic experts to locate and safely preserve digital evidence, as well as undertake routine examinations (Sikos, 2021). However, depending on the sort of examination, investigators are always required to know how to operate and configure/parameterize multiple tools, particularly open source types. The existence of a large number of such tools involves the expertise to address the following research questions: "How do I apply these tools properly?" and "where/when can I apply them effectively?" In fact, forensic examiners have various degrees of IT background and technical proficiency, ranging from computer security specialists to investigators with basic computer skills (Mattijssen *et al.*, 2020). As a consequence, irrespective of their computer and IT skills, investigators want practical tools that could assist them in obtaining findings quickly and with

[1] Department of Natural and Applied Sciences, Community College of Buraydah, Qassim University, Buraydah, 52571, Saudi Arabia
[*] Corresponding author's e-mail: SamyAbdelwahabSafaan@outlook.com

minimal usage complexity (Case *et al.*, 2008). Whenever we consider human participation, especially for the investigation of today's normally vast amounts of data, such tools that can reduce the investigation burden on the human investigator irrespective of their technical expertise are becoming increasingly important. When it comes to open source tools, it is usual for one software product being unable to gather all of the necessary data. As a result, the examiner must adopt a variety of methods in order to obtain useful data from the target. Due to the obvious expertise demanded by the tools, all this needs advanced training and adds to the learning curve. These tools are also not usually compatible with one another. Users of today's technologies must appropriately examine the outcomes of the tools in order to decide the next steps in performing a deeper study.

Related Work

According to the United States Government Accountability Office (GAO), preventing computer crimes and cyberattacks entails several obstacles (Fellows). Some examples include a lack of cybercrime detection and reporting technologies, a lack of education or training standards that may equip law enforcement with sufficient analytical and practical skills, and a lack of structure to enhance cybersecurity and raise public awareness. The Digital Forensics community is profoundly concerned about the industry's lacking of expertise and skills standards. So far, only a few efforts have been made to define computer forensics programme standards. The Digital Forensics Education Programs Accreditation Commission (FEPAC) published guidance for computer forensics education and skills in 2008 (Ruffell, 2010), which were bestowed upon them by the American Academy of Forensic Science (AAFS). These papers simply provide basic requirements for computer forensics training and education, such as the amount of credits required, the key forensics subjects that should be covered, and so on. The West Virginia University Forensic Science Initiative established recommendations for computer forensics training and education, which were issued by the National Institute of Standards and Technology (NIST) (Cunha *et al.*, 2017). This work may be used as a fantastic guide for developing an educational programme. However, building an educational programme based primarily on these standards would be prohibitively expensive for educational and training institutes; 24 courses is a substantial number in an academic programme. In reality, no previous educational or training programme have included such a diverse range of Computer Forensics courses (Yasinsac *et al.*, 2003). Policy Maker for Network Forensics, Computer and Network Forensics Professional, and Computer and Network Forensics Researcher are examples of topics taught in an education programme that differ significantly from those offered in a training programme. A training programme emphasizes practical skills and application, whereas an education curriculum emphasizes theory and principles. According to the designers of the approach, an undergraduate programme can ideally include themes present in both training and teaching programmers (Gottschalk *et al.*, 2005). The undergraduate course introduces students to the core tools and approaches of the subject. The undergraduate course mentioned above is necessary for the graduate course, which covers advanced issues related to evidence analysis and presentation, as well as the modification and integration of available technology into standard operating procedures. It does not give comprehensive instruction on several issues, notably the practical use of equipment and talents necessary for a forensics education programme (Digabriele, 2008). The "High Tech Crime Consortium "(HTCC) set up an online certificate program that displays the viewpoints or competence of a computer forensics degree graduate (Lee & Pagliaro, 2013). Security principles, system administration, web publishing, and two computer forensics courses were all suggested. Its central emphasis was on security and network topics, and students were not involved in the development of practical skills and technology (Gottschalk *et al.*, 2005). Erbacher and Swar stressed the need of including training and education themes in computer forensics education programme. However, their primary concentration, however, is on the management or administrative aspects of digital forensics (Fakouri & Teimouri, 2019).

LITERATURE REVIEW

Computer Forensics is a Forensic science subject with varied meanings depending on who you ask. However, it is best defined as "the application of scientifically derived and proven methods to the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of criminal events, or assisting in the anticipation of unauthorized activities shown to be disruptive to planned operations" (Taylor *et al.*, 2007).

Sub-disciplines of digital forensics include computer forensics, mobile device forensics, network forensics, and database forensics. that analyze different equipment,

Figure 1: The investigational method of digital forensics

media, or evidence (Raval, 2020b). Our study focuses on computer forensics in particular, as well as the tools utilized for training. As a result, the vast majority of the examples and explanations in this study will be provided with this goal in mind. The above description of Computer Forensics encompasses a wide variety of operations, from device seizure through evidence presented to judicial authorities. However, we would want to reduce the process phases to more basic methods, as indicated in the US Department of Justice's "A guide for first responders" (Brinson *et al.*, 2006). The suggested paradigm is divided into four stages: data collection, investigation, analysis, and reporting (See Figure. 1).

Phases of Digital Forensics

During this step, the examiner must guarantee that the copy of the media that will be used in the examination and analysis stages is correct, as well as that the original media's integrity is protected. Otherwise, the entire inquiry may be deemed illegitimate by the court (Branham, 2019). The examination phase is the stage at which detectives conduct a thorough search for evidence connected to the alleged crime. This focuses on finding and locating possible evidence, which may be in unusual areas (Mellars, 2004). This procedure should fulfil a number of goals. First and foremost, the status of the evidence must be meticulously documented. Examiners especially explore unorthodox areas for the existence of hidden or obscured data throughout the whole procedure. Because the final outcome of this procedure may be big, data reduction can be conducted after all of the information is revealed (Mellars, 2004). An investigator retrieves evidence using a variety of techniques and tools. Some of these tools will be briefly described later in this chapter. During this phase, the investigator searches for information that will help him or her answer questions about the case. An investigator, for example, has to know: "Given the reviewed files/data, might this data confirm or deny my hypothesis?" "How so?" Because they have little help from the inquiry tools, much of their work is cognitive (Casey, 2020) depending on the investigator's expertise and experience. There may be a need to gather and examine additional data that has never been covered previously. As a result, the investigative process may return from the analytical phase to the collection and inspection stages. It may also require multiple iterations of investigation and analysis to back up a criminal theory (Casey, 2020). The reporting step is the final stage of the digital forensic inquiry. A written report typically includes and summarizes the examination procedure, the pertinent data retrieved with their associated hash values, and the conclusions derived from the analysis phase (Casey, 2020). Furthermore, the tools utilized in earlier stages, as well as the reasons for their usage, are indicated in the reporting phase. Examination notes must be kept for the purposes of discovery or testifying (Casey, 2020). Some automated (particularly commercial) tools provide reports for investigators. However, nearly no single purpose tool generates such a report, hence it is important for the investigator to collect information for every activity and tool used in all of the above-mentioned phases for reporting purposes.

Digital Forensic Tools

The results of a survey conducted between both computer forensics practitioners and colleges or institutions offering a Computer Forensics programme (See Table 1). To establish the technical skills needed by Computer Forensics Practitioners, as well as the tools that should be taught in forensic analysis courses, Professionals in computer forensics both from public and private sectors were surveyed, for each group asked a variety of questions (Kessler, 2010). Teachers of digital forensics were asked what analytical tools they used in their curriculum and if they were willing to engage with digital forensics practitioners for teaching purposes. They were also polled on why they did not cooperate with Digital Forensics Practitioners for instructional purposes. The study also inquired about their thoughts on how to increase education in digital forensics. These survey questions were sent to universities and colleges that provide computer forensic degrees. This poll includes seventeen volunteers from various institutions and universities, as well as nine volunteers from the United States' Digital Forensics Practitioner Association. Sixty-seven percent of digital forensics practitioner responders had fewer than ten years of expertise in the field. The digital forensics practitioner's category had the most responses, with 44.4 percent coming from corporations or private companies. The furthermore share of respondents, 22.2 percent, came from law enforcement and non-governmental organizations. Moreover, 11.1 percent of Digital Forensics Professionals worked for government agencies, with little or no responses from of the private investigation sector.

Table.1 highlights the use of main digital forensics technologies by both professionals and digital forensics professors EnCase is the most widely used tool for both instructors and educators, with 94.1 percent of digital forensics teachers and it is used as the primary tool for computer forensics collection and analysis by 66.7 % of computer forensics professionals. FTK is the second most popular tool, with 70.6 percent of digital forensic professors and 56.6 percent of digital forensic professionals using it. WinHex, HELIX, md5sum, and MOBILedit are other handy tools. Computer forensics experts frequently employ forensics; yet, it appears that professors seldom use it. Other tools used by computer forensics professionals but not by digital forensics instructors PTK, CellDEK, VideoFOCUS, dTective, ClearID, dVelepor, and Magnifi are a few examples. Similarly, Foremost, pyFLAG, and OUTGUESS are tools used by teachers rather than specialists in digital forensics. The willingness to collaborate for the two components (e.g., the survey results are shown in Figure.2 was analyzed to establish how closely industry and allied organizations

Table 1: Use of Digital Forensics Tools (30).

Computer Forensics Tools	Results from Universities and Colleges	Results from Computer Forensics Practitioners
EnCase	94.1%	66.7%
Access Data forensics Toolkit (FTK)	70.6%	57.6
FTK Imager	70.5%	66.7%
Win Hex	64.6%	55.3%
Autopsy Forensics Tool	23.5%	11.1%
HELIX	64.7%	55.7%
SMART	0.00%	33.3%
PTK,	0.00%	11.1%
CellDEK	0.00	11,1%
Video FOCUS,	0.00	0.00%
dTective	0.00	11.1%
Clear ID	0.00	11.1%
dVelepor	0.00	11.1%
Magnifi	0.00	11.1%
md5sum	29.5%	55.7%
py FLAG	5.9%	0.00%
Foremost	17,6%	0.00%
MOBIL edit	11.8%	55.6%

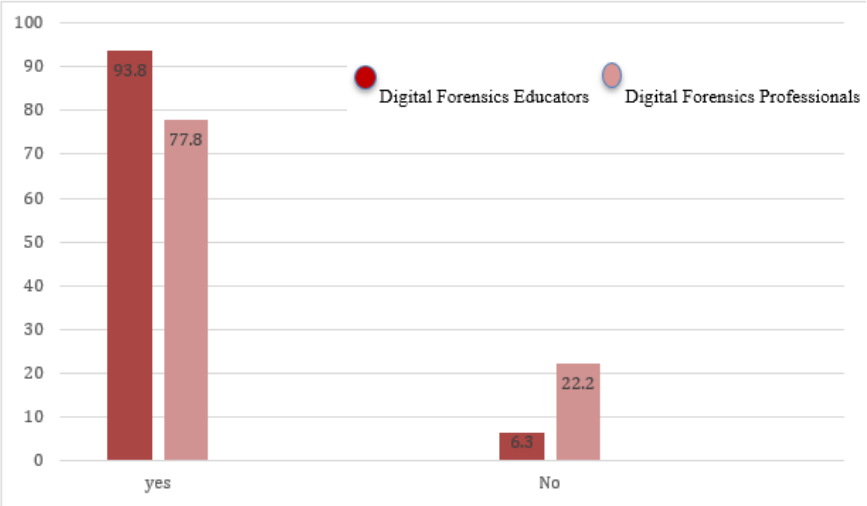


Figure 1: Digital Forensics Instructors and practitioners' desire to contribute in the progress of Digital Forensics (31).

can engage with universities for digital forensics training. According to the poll results, a digital forensics professional should be proficient in the use of the most often used tools, such as FTK and Encase. As a result, graduates of forensic institutions receive extensive training in these technologies. Furthermore, forensic training should include a comprehensive lecture on forensic tools, focusing on FTK and Encase as well as Helix, WinHex, and other open-source tools. The survey shows that the how the training of these tools helps the graduates to enter into the practical aspect of the computer forensics and how they both the educational institutes and the professionals can work together to bring a suitable learning and training environment for the students of computer forensics. Therefore, it is very important to understand that combined efforts towards the development of the computer forensics can help educational institutions and students to understand the practical aspect of the computer forensics.

Proposed Models for Digital Forensics

The most common commercial test software packages nowadays are AccessData's Forensic Toolkit (FTK) and Guidance Software's EnCase. Both commercial offers are employed by law enforcement agencies, have advantages and disadvantages, and are frequently compared and contrasted. FTK is a digital investigative tool that has been used in court. It is built for speed, stability, and ease of use, it outperforms all other products in terms of substantial pre-processing and indexing, filtering, and searching (Cantrell & Dampier, 2012). FTK is well-known for its use of front-end indexing, which results in near-instant search results. A standalone imager, registry viewer, and password recovery programme are also included in the test suite. Guidance Software describes EnCase as the global standard in digital investigative technology for forensic specialists that want rapid, forensically sound data gathering and investigations with a repeatable and defensible methodology (Cantrell

& Dampier, 2012). It also includes extra tools like an independent imager and decryption solutions in the form of modules. Both suites are also noted for their distributed processing capacity, which allows the programme to handle one case at a time using up to eight workstations. This dramatically accelerates case processing and reduces case processing durations from days to hours. While this commercial software might be rather pricey, both provide academic programme that significantly lower the cost of educational reasons. Both provide substantial training programme that may be utilized to teach new programme trainers. These advantages can help to offset some of the expense of commercial software. Another advantage of commercial suites such as FTK and EnCase is that they both provide industry-recognized certifications for their products' use and performance. AccessData Certified Examiner (ACE) eligibility is issued by FTK, and EnCase offers a comparable qualification, EnCase Certified Examiner (EnCE). Both certifications may be obtained by students at diploma level and after finishing a degree and can aid in their career search. There are several free digital forensic investigation tools available. These tools are portable and may be set up in a matter of minutes. They are frequently used in the field to gather information on the go or to conduct investigations when time is of the essence. That isn't to suggest they aren't as productive as commercial suites; in fact, commercial tools are frequently easier to use for novices. Both sorts of tools evaluate data in the same way, and a whole digital forensics programme could and is developed around free toolkits (Cantrell & Dampier, 2012).

Current Challenges for Educational Institutes

Cybersecurity", often known as information security, seems to be a rapidly expanding job sector as a result of rising and costly cyberattacks. Graduates of cybersecurity schools are often prepared for entry-level roles which includes "Cybersecurity Analysis" at "Buraydah Community College, Qassim University" and "Unaizah Community College, Qassim University". As per the "U. S. Department of Labor, Labor statistics (BLS)", workforce of cybersecurity professionals is expected to grow from 2012 to 2022, much faster than the average growth rates for all fields of work of 11 percent and 18 percent for computer-related professions (González Jaimes, 2016). There seems to be a nationwide lack of cybersecurity specialists with the necessary knowledge and expertise, and education is anticipated to become the vital solution (Tu *et al*., 2012).

As a response, there seems to be an increase in the demand for and availability of cybersecurity education and skills. Meanwhile, cybersecurity education faces significant obstacles. To excel academically and professionally in cybersecurity, students must have a solid foundation and preparedness in computer and information science and technology. However, there has been a perpetuated failure of education in the Middle East to prepare a strong and world-leading workforce in computing professions. The following are the major aspects of this catastrophe in Middle Eastern undergraduate computer programmes: The primary source of the gap among students' education as well as the real abilities required in the labor market may be outdated curricula and course material, as well as a lack of understanding practical experience. Other issues include a decline in enrolment and a failure to take advantage of service learning programmes that develop application skills. This study presents a project-based curriculum educational outreach paradigm for cybersecurity education to assist reduce the gap between college education courses and work training necessary in the real life.

To that aim, Saudi Arabia has launched two major standards that serve as principles for enhance the effectiveness of cybersecurity learning and skills for both education institutes and Employment. The first framework is (SCyWF) (Liu & Tu, 2020), which categorized 40 job positions in cybersecurity and described the required responsibilities, expertise, skills, and competencies for each position.

The second framework (SCyber Edu) (Gamlo & Bamasak, 2011), describes the minimal standards and academic units which should be provided by college cybersecurity programmes in Saudi Arabia, ranging from certificate to doctoral levels.

Some institutions have steadily incorporated one or two cybersecurity courses into academic curriculum in past few years, including "Buraydah Community College" and Unaizah Community College" Qassim University" However, introducing such courses frequently finds obstacles in teaching the practical aspect of the diplomas namely, Forensic Computer Analysis" which is one of the courses taught at the third level of the study plan for the "Diploma in Cyber Security", and the "Diploma in Cyber Security" is a two-year diploma, after secondary school, divided into four levels and teaching staff finds it difficult to teach the practical side of this course, as well as the students in understanding it. The paper will address the teaching methods to implement and make things easy for the students and teachers to understand the practical side of these courses.

The Technical Working Group on Education and Training in Digital Forensics (Tu *et al*., 2012), suggests creating a computer forensics laboratory to supply students with equipment. and software to train them in practical skills, particularly with the popular digital forensic tools featured in our findings. Individual machines are involved in the majority of white-collar crime in the public sector. The corresponding counter-investigative powers are limited to the average end-user. According to the study results, there is a considerable increase in the number of occurrences on networks, protocols/devices, and internet apps, and many of these incidents involve adversaries with skills much beyond those of typical end users (Raval, 2020b). To examine these criminal cases and their perpetrators effectively and efficiently, as well as discover relevant evidence, digital forensics specialists require more broad knowledge and abilities that introduce the discipline of

network / internet forensics.

There are currently relatively few educational programme that provide such training, and there is no agreement on what tools and subjects should be included in educational courses covering network / internet forensics. There are about three key methods to understand Cybersecurity:

(i) Incorporating one or two classroom learning into the overall

(ii) Curriculum. incorporating cybersecurity themes into other network and computer courses.

(iii) And using less formal approaches, such as training courses.

Cybersecurity modules are frequently provided throughout the latter semesters of a student's programme. In certain circumstances, a security course is an elective, which has the unintended consequence of students avoiding it during the last semester. Some students are found to fear that somehow this security course will be challenging and will damage their ability to complete their education. Under the second technique, Cybersecurity topic is introduced in other information and communication technology (ICT) curriculum such as, "Operating Systems", "Computer Networks", "Databases, and "Software Application Programming". It was frequently suggested that cybersecurity should be covered in a range of learning courses. This addition is contingent on both the teachers' understanding of the subject and their effort in addressing such topics in the curriculum. When a talented professor quits the college, this might radically alter. Cybersecurity material differs over institutions and departments including both techniques.

We therefore presented participants with a list of cybersecurity topics, such as computer security, network security, IT system security, security management, and incident response, to assist them better grasp overall competencies of colleges. The majority of interviewees felt that teaching the first three categories is more practical. The majority of interviewers felt that teaching the first three topics is more doable, and they're less convinced regarding teaching "Incident Response" in the course. The third strategy is the use of informal activities to enhance understanding about cybersecurity. Some universities host lectures, conferences, and other events to strengthen students' understanding of cybersecurity by inviting guest speakers. Such activities are said to be warmly appreciated by students and to pique their interest in the topic. Finally, certain cybersecurity topic is clearly included in professional certification material.

To meet the demand for qualified investigators, educational institutions have implemented a variety of degree and certificate programme in digital forensics. Training a student in digital forensics, or any investigative discipline, presents unique obstacles in that educators are faced with teaching a student how to analyze a case and identify evidence through discovery in the absence of an absolute definitive blueprint. Every case is unique, and there is no "recipe" or "by the numbers" way for conducting investigations. A digital forensics investigation cannot be completed by simply following a set of procedures on a reference card. A successful curriculum necessitates activities other than theoretical lectures and multiple-choice tests. A digital forensics programme must include hands-on lab work in which students execute exercises and tests on actual equipment in a lab setting. When theory can be implemented or applied, it becomes more understandable (Sánchez *et al*., 2011). This teaching technique promotes kinesthetic learning, in which students learn via physical action rather than through listening to lectures or reading PowerPoint presentations. Kinaesthetic learning happens when students actively participate in learning through hands-on activities and other ways, and students learn more as a result (Pollitt *et al*., 2008).

Modern Approach Towards Digital Forensics Education

An investigator in digital forensics must be well-versed in a wide range of operating systems. According to practitioners' experience, Windows PCs are the most prevalent in inquiry situations, whereas Unix / Linux accounts for around 20% of total systems (Tu *et al*., 2012). This implies that the digital forensics curriculum should cover a range of operating systems, with a primary concentration on Windows and a secondary focus on Unix / Linux and Macintosh. Unfortunately, while it is theoretically ideal to teach as many operating systems as possible, educational programmes have limited resources, including time, equipment, and staff resources. The difficulty for students seeking hands-on experience is to create and maintain a proper laboratory environment for instruction. The many considerations that must be taken to account for space needs, software, hardware, network concerns, and the many other varied peripherals and devices necessary for such a programme can make building and maintaining such a laboratory a daunting job. There appears to be considerable worry about how students can be prepared to fulfil the expectations of both industry and law enforcement authorities (Cummins Flory, 2016).

There are numerous options to tackling this problem; one recommended strategy is to collaborate with digital forensics specialists from both industry and law enforcement. It is impossible for digital forensics specialists to commit a significant amount of time to designing teaching programme, especially given budget and timeline restrictions. It is critical that digital forensics curriculum combine industry and law enforcement agency experiences and ideas. Specialty training for academic staff that don't have prior experience in certain fields of cybersecurity is an important component of establishing stronger curriculum. Similarly, suitable training for students in practical cybersecurity topics must be improved through the introduction of laboratories and skills acquired even outside the college.

Additional actions that should be considered include,

• Incentives for local industry to assist education programs, such as paid internships and the availability of

trainers.

• Promoting inter-temporal professional relationship among academics and governmental entities in order to boost growth.

• Obtaining assistance from global counterparts (organizations or private businesses), including the Organization of American States (in Uruguay), IBM (in Costa Rica), and Microsoft (in India).

• Creating educational programs and services, such as forensic labs.

• "Virtual Training Environments" being adopted at collage level.

• Envisioning and promoting training courses to provide students with cybersecurity relevant work experience.

• Attention on detailed practical learning and training courses.

Numerous governments have recognized the usefulness of retraining programs in enhancing practical–technical cybersecurity training. In the United Kingdom, cybersecurity training programs helped country major industries and are funded by the government (Thompson, 2019). In the United States, community college cyber job training programs also begun to appear (Thompson, 2019). Industrial cooperation help fund these and other related activities.

The cybersecurity field is incredibly dynamic and ever-changing. As the need for skilled individuals in this industry grows, education institutions are engaging in a number of ways. Advanced nations, at both the governmental and corporate levels, have begun initiatives to assist educational institutions in developing adequate cybersecurity curricula in order to meet the growing need for cybersecurity specialists. Moreover, a number of scholars have presented cybersecurity curriculum design approaches and suggestions. This research, I trust, will provide educators with a better understanding of the entire efforts undertaken in the cybersecurity field, as well as assist them in developing increasingly successful cybersecurity curriculum and instruction in future work. Professional project, internship, and/or court experience are examples of suitable courses that can be classed in this category.

Further study should be conducted to investigate the association between students who complete professional projects and internships and their competitiveness in the labor market following graduation. Anecdotal evidence suggests that students who conduct internships in this profession are more likely to obtain related work within six months of graduation than those who did not do an internship. Students must comprehend the basic principles, techniques, and procedures that skilled criminals use to perpetrate such crimes, as well as the various countermeasures that organizations and businesses may take to defend themselves, in order to successfully solve cybercrime. According to the findings made above, network forensics courses should include a wide range of subjects, including: operating systems, network and Internet protocols, malware, devices, applications, network hacking methods and tactics, as well as countermeasures and security mechanisms. To meet the demand for qualified investigators, educational institutions have implemented a variety of degree and certificate programme in digital forensics. Training a student in digital forensics, or any investigative discipline, presents unique obstacles in that educators are faced with teaching a student how to analyze a case and identify evidence through discovery in the absence of an absolute definitive blueprint. Every case is unique, and there is no "recipe" or "by the numbers" way for conducting investigations.

CONCLUSION

This study looked at the design of digital forensics curriculum and current educational programme that offered a generic list of computer forensics courses but provided no recommendations on which topics to include and which tools to teach. Both digital forensics instructors and practitioners were interviewed, and The data was evaluated in order to determine the information, methodology, and abilities required by the industry and law enforcement groups. The most often used commercial tools are Encase and FTK, and the majority deal with Windows operating systems, followed by Unix /Linux and Macintosh.

The increase in cybercrime implies the continued need for well-trained detectives. Universities may respond by offering basic and advanced digital forensics courses. Based on our findings, we propose some next research directions. We would want to first study the problems and methods for building online security and forensics courses in order to assure flexibility and cost effectiveness, as well as to enhance participation. All commercial and open source technologies should be available for use in the online courses as much as the on-campus learning environment, and the solution should be properly scalable and flexible enough to adapt to quickly developing computer and forensic technology Second, the design of digital forensics programme for both elementary and secondary school graduates should be studied to determine how they might be integrated into existing computer and network security programs. This paper has provided a high-level overview of a typical student laboratory setting. To better prepare students for a future in investigation, an emphasis on evolving technology should be maintained on a continuous basis. Of course, the focus of any programme should always be on student learning, which may be more successfully accomplished by constructing and employing a purpose-built student digital forensics laboratory.

Acknowledgments

The writer is thankful to Qassim University.

Conflict of interest

There is no conflict of interest.

Consent for publication

The author agrees to the final version submitted to the journal.

REFERENCES

Branham, R. A. (2019). Hash it out: fourth amendment protection of electronically stored child exploitation. *Akron Law Review, 53*(1), 7.

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *digital investigation, 3*, 37-43.

Cantrell, G., & Dampier, D. A. (2012). Implementing the automated phases of the partially-automated digital triage process model. *Journal of Digital Forensics, Security and Law, 7*(4), 5.

Case, A., Cristina, A., Marziale, L., Richard, G. G., & Roussev, V. (2008). FACE: Automated digital evidence discovery and correlation. *digital investigation, 5*, S65-S75.

Casey, E. (2020). Strengthening trust: Integration of digital investigation and forensic science. In (Vol. 33, pp. 301000): *Elsevier*.

Cummins Flory, T. A. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law, 11*(1), 4.

Cunha, I., Cavalcante, J., & Patel, A. (2017). A proposal for curriculum development of educating and training Brazilian police officers in digital forensics investigation and cybercrime prosecution. *International Journal of Electronic Security and Digital Forensics, 9*(3), 209-238.

Digabriele, J. A. (2008). An empirical investigation of the relevant skills of forensic accountants. *Journal of education for Business, 83*(6), 331-338.

Fakouri, R., & Teimouri, M. (2019). Dataset for file fragment classification of image file formats. *BMC research notes, 12*(1), 1-3.

Fellows, S. Immune System' Cyber-Security for SCADA Systems. *Engineering & Technology Reference, 1*(1). https://doi.org/10.1049/etr.2015.0103

Gamlo, A., & Bamasak, O. (2011). A multi-tier framework for securing e-transactions in e-government systems of Saudi Arabia. *International Journal of Electronic Finance, 5*(2), 126-149.

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

González Jaimes, E. (2016). Academic competences of university graduates and their job occupation prediction / College graduates' academic skills and their occupational employment projection. https://doi.org/10.23913 / ricsh.v5i10.78

Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005). Computer forensics programs in higher education: a preliminary study. Proceedings of the 36th SIGCSE technical symposium on Computer science education,

Harvey, D. J. (2019). *Digital Evidence Admissibility: Some Issues*. Available at SSRN 3505611.

Kessler, G. C. (2010). Judges' awareness, understanding, and application of digital evidence. Nova Southeastern University.

Lee, H. C., & Pagliaro, E. M. (2013). Forensic evidence and crime scene investigation. *Journal of Forensic Investigation, 1*(2), 1-5.

Liu, F., & Tu, M. (2020). An Analysis Framework of Portable and Measurable Higher Education for Future Cybersecurity Workforce Development. *Journal of Education and Learning (EduLearn), 14*(3), 322-330.

Mattijssen, E. J., Witteman, C. L., Berger, C. E., Brand, N. W., & Stoel, R. D. (2020). Validity and reliability of forensic firearm examiners. *Forensic science international, 307*, 110112.

Mellars, B. (2004). Forensic examination of mobile phones. *digital investigation, 1*(4), 266-272.

Pollitt, M., Nance, K., Hay, B., Dodge, R. C., Craiger, P., Burke, P., Marberry, C., & Brubaker, B. (2008). Virtualization and digital forensics: A research and education agenda. *Journal of Digital Forensic Practice, 2*(2), 62-73.

Raval, H. (2020b). Artificial Intelligence Forensics, Machine Learning Forensics and Digital Forensics. *Digital Forensics (4n6) Journal*. https://doi.org/https://doi.org/10.46293/4n6/2020.02.04.05

Ruffell, A. (2010). Forensic pedology, forensic geology, forensic geoscience, geoforensics and soil forensics. *Forensic science international, 202*(1-3), 9-12.

Sánchez, J., Salinas, A., Contreras, D., & Meyer, E. (2011). Does the new digital generation of learners exist? A qualitative study. *British journal of educational technology, 42*(4), 543-556.

Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. Wiley Interdisciplinary Reviews: *Forensic Science, 3*(3), e1394.

Sindhu, K., & Meshram, B. (2012). Digital forensics and cyber crime datamining.

Taylor, C., Endicott-Popovsky, B., & Frincke, D. A. (2007). Specifying digital forensics: A forensics policy approach. *digital investigation, 4*, 101-104.

Thompson, S. (2019). Apprenticeships as the answer to closing the cyber skills gap. *Network Security, 2019*(12), 9-11.

Tilekar, T. The Conceivability and Admissibility of Forensic Evidence from IoT Devices in Digital Forensics. *Digital Forensics (4n6) Journal.*, pp. 53–54. https://doi.org/10.46293/4n6/2020.02.02.10.

Tsai, C.-F. (2015). Dynamic grey platform for efficient forecasting management. *Journal of Computer and System Sciences, 81*(6), 966-980.

Tu, M., Xu, D., Wira, S., Balan, C., & Cronin, K. (2012). On the development of a digital forensics curriculum. *Journal of Digital Forensics, Security and Law, 7*(3), 2.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy, 1*(4), 15-23.