Activity Led Learning as Pedagogy for Digital Forensics

[1]Shaik Shakeel Ahamad

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia

Summary

The field of digital forensics requires good theoretical and practical knowledge, so practitioners should have an in-depth understanding and knowledge of both theory and practical as they need to take decisions which impacts human lives. With the demand and advancements in the realm of digital forensics, many universities around the globe are offering digital forensics programs, but there is a huge gap between the skills acquired by the student's and the market needs. This research work explores the problems faced by digital forensics programs, and provides solution to overcome the gap between the skills acquired by the student's and the market needs using Activity led learning pedagogy for digital forensics programs.

Keywords:

Digital forensics; Activity led learning; Pedagogy; Knowledge; Skills

1. Background

Digital Forensics is an academic subject which evolved in very short span of time, but the pedagogy associated with this realm is not well defined although there are forums which seek to promote good practice and share teaching experiences. Digital forensics is the traditional forensics body of knowledge translated into the digital domain. Specialists in this area obtain electronic clues and other forms of investigative data to support investigations of crime and espionage. As a result, the knowledge base blends superb electronic capabilities with the skills of a good police detective. That includes a profound knowledge of the criminal investigative process including such things as chain-of-custody and police procedure. The general aim of the forensics process is to investigate any violation of computer or digital media for the purpose of prosecuting instances of cybercrime or fraud committed against people and property. Nonetheless, another purpose besides the criminal investigation and prosecution mandate is the development of all of the information necessary to ensure that the enterprise's networks and systems are fully and properly defended against any form of intrusion. This is done by fully scrutinizing the immediate environment in order to determine incident scope, urgency, and potential impact. [3] explains different phases, tools and research trends in the realm of cyber forensics. [4] brings minute details of cyber forensics which includes different tools which are helpful in the process of extracting evidence from the devices. [5] describes the significance of computer forensics framework and different types tools used in computer forensic tools with its usage. [6] proposes a model for investigation process for digital crime, proposed model is simple and has better performance in terms time taken for the investigation. All the research works in the literature of digital forensics education highlights the digital forensics tools and investigation process. As per our knowledge we are the first to propose an activity led learning pedagogy in the realm of digital forensics. The rest of the paper is organized as follows: Section 2 discusses about the significance of activity led learning, Section 3 highlights the problems faced by digital forensics programs, Section 4 presents cyber security education standards, Section 5 discusses about the virtual environments and tools used for digital forensics. In section 6 we proposed an activity led learning pedagogy for digital forensics, section 7 compares proposed work with the related works, section 8 provides discussion and section 9 concludes the paper.

2. Significance of activity learning led learning

Activity Led Learning is a pedagogy that motivates students to learn using simulation activity that helps them in understanding and solving real time issues. This pedagogy helps in producing graduates who are confident in their skills and abilities and capable of achieving assigned tasks. The manner in which this is achieved within undergraduate and postgraduate cohorts is supported by the concept of constructive alignment in its curriculum design, modes of delivery and use of assessment materials. Fundamental to this is the use of "industry" standards in digital forensics in order that the "Real World" relevance of the teaching and learning is consistently emphasized. The seminal paper "Computer Forensics Education" sought to develop a framework where academic programs could be developed. It focused upon curriculum as against how such a curriculum could be taught. Computer forensics is a multi-

Manuscript received April 5, 2023
Manuscript revised April 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.4.17

disciplinary discipline which has its roots in computing and law fields. Activity led learning is a pedagogy that enables students to experience "real world" problems and use acquired learning and skills in order to "solve" them, which also means that necessary multi-disciplinary practices are brought into play.

3. Problems faced by Digital Forensics Programs

Following are the list of problems faced by the universities in introducing and implementing digital forensics programs.

a) **Lack of theoretical knowledge:** There is huge demand for digital forensics education and certifications, but the training provided by the certification agencies fail to provide students in the basics and theoretical foundations in digital forensics.

b) **Lack of prescribed textbooks:** Existing digital forensics books are mostly authored by people belonging to industry, so these books lack the explanation of theoretical concepts and the underlying technologies which are very vital for the prescribing as textbooks in higher education.

c) Difficulty in recruiting qualified faculty: There is a huge demand for qualified faculty in the realm of digital forensics as there are no standard curriculum and prescribed textbooks.

d) **Difficulty in establishing digital forensics lab:** Licences for digital forensics hardware and software tools are very costly so establishing digital forensics lab in a university is very expensive.

e) **Problems in finding relevant prerequisites:** A digital forensics student needs to have a good knowledge of both computer science and law fields, so it is very difficult to find the relevant prerequisites to the courses in digital forensics.

4. Cyber Security Industry standards

This section explores some of the most popular cybersecurity education standards. There are three cybersecurity education standards, they are Information Security Common Body of Knowledge (InfoSec CBK), Certified Information Systems Security Professional (CISSP) and National Initiative for Cybersecurity Education (NICE).

a) **InfoSec CBK:** According to [1] there are ten basic domains that InfoSec CBK address, they are Security Architectures and Models, Access Control Systems and Methodologies, Cryptography, Program and Application Security, Access Control Systems and Methodologies, Cryptography, Network and Telecommunications Security , Database Security, Business and Management of Information Systems Security, Operating System Security, Physical Security and Critical Infrastructure Protection, Social, Ethical, and Legal Consideration.

b) **CISSP CBK**: CISSP CBK has ten domains they are Access Control, Application Security, Business Continuity and Disaster Recovery Planning, Cryptography, Information Security and Risk Management, Legal Regulations, Compliance and Investigations, Operations Security, Physical (Environmental) Security, Security Architecture and Design and Telecommunications and Network Security [2].

NICE (National Initiative for Cyber Security Education): NICE standards are initiated and led by the National Institute of Standards and Technology (NIST) with the main objective to motivate and advocate a robust network and an ecosystem on cybersecurity education, training, and workforce development. NICE achieves this objective by synchronizing with the government, academia, and industry. Digital Forensics is a specialized competency area of the NICE framework focused on the evidence gathering function, specifically targeted toward the collection of electronic evidence with the following goals

a) To promote Learning and Skills Development

b) To support a Diverse Learning Community

c) Guide Career Development and Workforce Planning

5. Virtual Environments and Tools used for Digital Forensics

Digital forensics investigation requires a special knowledge of the internal workings of the machine. That knowledge is always obtained by using specialized tools and hardware. These tools are utilized to ensure that every aspect of the collection and handling of virtual evidence is documented in such a way that the absolute integrity of the chain of custody is provably maintained. Also, because of the nature of digital evidence, it is almost impossible to collect and preserve it without the support of hardware and tools. This section explores some of the popular virtual environments and tools used for digital forensics.

5.1. **Virtual environments**

VMware Workstation is an industry standard desktop hypervisor for running virtual machines on Linux or Windows operating systems [7]. VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as for personal use and is freely available at [8]. It has very good features with high performance. SIFT (SANS Investigative Forensics Toolkit) is a Multi-purpose forensic operating system which is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It supports expert witness format

(E01), advanced forensic format (AFF), raw (dd) evidence formats [9]. Parrot Security Operating System is a free and Open Source GNU/Linux distribution based on debian testing which is designed for cyber security experts and developers. It includes a full portable tools for IT security, Penetration testing and Digital Forensics [10]. Kali Linux is an open-source, Debian-based Linux distribution catering the needs of various information security functions which includes digital forensics, cyber security, Penetration Testing, and reverse engineering research [11].

5.2. **Digital Forensics Tools**

i) **Hard Disks & File Systems Analyzing Tools**: The Sleuth Kit (TSK), WinHex & Autopsy Tools

ii) **Data Acquisition Tools**: AccessData FTK Imager, Encase & DiskExplorer for NTFS & Encase Tools

iii) **Computer Forensics Software:** File Viewer, P2 Commander & R-drive Image

iv) **Operating Systems Forensics**: OS Forensics, Process Explorer, Process Monitor, Event Log Explorer Tool

v) **Incident Response:** Helix Tool, ManageEngine, SolarWinds, Splunk, LogRhythm

6. Proposed Activity Led Learning Pedagogy for Digital Forensics

6.1. Underlying Knowledge, Skill, and Ability Requirements for Digital Forensics

Along with a detailed set of tasks, the NICE workforce also provides a distinctive set of KSA specifications for each specialty area. These KSAs offer much clearer elaboration and characterization of the activities that underlie each task and also help the educational community to understand the precise knowledge requirements to be used in the design of targeted training and education programs in that specific specialty area. That specification of requirements is the purpose of the KSAs enumerated by the NICE workforce model. Typical tasks and KSAs are specified within each specialty area. Each KSA has exactly one competency associated with it. Each KSA defines a specific KSA requirement. In application these requirements may be assigned to one or more specialty areas within the model.

6.2. Digital Forensics KSAs

The majority of the KSA requirements for the forensics specialty area can be factored into four distinct areas of standard application.

1. *Information systems/network security* is a classic area of cybersecurity protection.
2. *Infrastructure design* is an area, whose decision making is supported by forensics.
3. *Vulnerability assessment and risk management* is the classic risk component.
4. *Legal, government, and jurisprudence* entails the rules of evidence.

Lecture based learning pedagogy: Lectures are the most preferred way to introduce a topic to the class, since it quickly disseminates the information to a group' The two things that should be kept in mind when giving lectures are

i) **Length of the lecture**: To make the learning effective, the lecture should be short and interactive. The student's concentration and attention to the class will be less if the lectures are held for longer time.

ii) **Interactions with the students:** Instructors should make the lectures interactive in order to make the lecture interesting for the students. Instructors can maintain interest among students by including discussion, delivering jokes in between (or) at the end of the concepts and interacting with students to clear their queries. Timing is important when giving lectures; students are more interested to listen to the lecture when their energy levels are high. The instructor can include some other instructional methods to keep student's concentration in the class.

Demonstration based learning pedagogy: Demonstration is the expansion of a lecture. It is used to show a concept practically to the students rather than just teaching about a concept. Students will be able to perform the task better when the instructor explains the task through demonstrations rather than just explaining the task through lectures. Demonstrations are helpful when there is a need to explain about a procedure (or) steps in accomplishing a task. Demonstrations can be easy or difficult depending upon the concept.

Simulation-based learning pedagogy: Simulation is similar to role play since the students get ge opportunity to experience in real-life situations. The difference of simulation with role playing is that in simulation students do not act out of the script (or) situation. For example, when a student needs to learn how to land an aero plane they use flight simulators to practice the skill in a safer environment until they perfect it. Simulations are used to experience the students in a real and practical situation. Simulations should be very practical where students should be able to experience the results.

Problem-based learning pedagogy: Problem-based learning pedagogy is student-centric, which plays very important role in making the students understand the complex and multidisciplinary topics that do not have advanced solutions. Before implementing problem-based learning pedagogy students were guided about the crime scene investigation procedures. Students construct a mock crime scene and learn all the phases of investigation.

Project-based learning pedagogy: Projects are typically based on real-time problems and are a good source of learning for the students. Project based pedagogy ensures ownership, autonomy and responsibility for the students in designing and real-time implementation. The instructor should be very careful in designing the objectives of the project and should track/monitor all the phases of the project. Project-based learning pedagogy evaluates all the knowledge, skills and abilities learned from all the chapters in the courses.

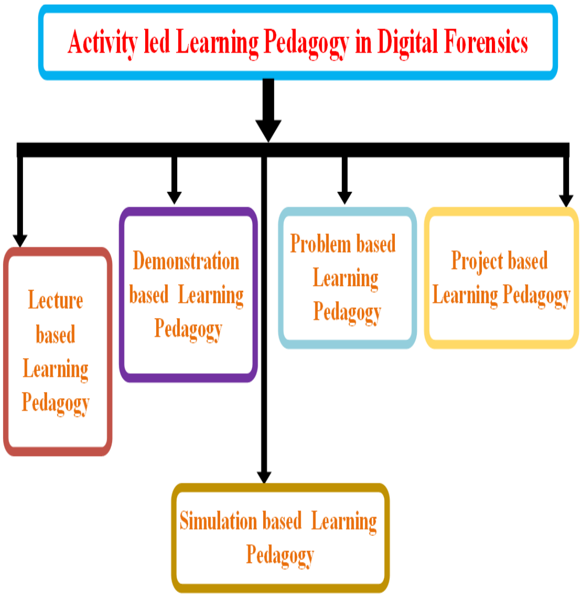
Activity led Learning Pedagogy in Digital Forensics
Lecture based Learning Pedagogy
Demonstration based Learning Pedagogy
Problem based Learning Pedagogy
Project based Learning Pedagogy
Simulation based Learning Pedagogy

Fig. 1. Proposed Activity led learning pedagogy in Digital Forensics

7. Comparative Anaysis with Related Work

This section compares our work with the related work discussed in this paper. Our proposed work out preforms the works discussed in the related work as shown in table 1.

.

Research Works Activity Name	[3]	[4]	[5]	[6]	Our's
Lecture based learning Pedagogy	×	×	×	×	✓
Demonstration based learning Pedagogy	×	×	×	×	✓
Simulation based learning Pedagogy	×	×	×	×	✓
Problem based learning Pedagogy	×	×	×	×	✓
Project based learning Pedagogy	×	×	×	×	✓

Table. 1: Comparative analysis with Related Work

8. Discussion

Integration of activity led learning pedagogy into the digital forensics courses ensures more knowledge, skill and ability to understand and implement complex topics in the real time environment. Students understand only a small part of the concepts in digital forensics from lecture based pedagogy, demonstration based learning pedagogy enables students understand the concepts in depth, simulation based learning pedagogy gives very clear picture of the crime scene, how to recognize evidence, how to secure evidence. Problem based learning pedagogy enhances the capability of a student to solve problems faced during digital forensics investigation and finally students quickly understood how project based pedagogy plays a vital role in recognizing the evidence, securing the evidence and in presenting the evidence in the court of law.

9. Conclusion

With this article's we made an attempt to explore the problems faced by digital forensics programs, and provides solution to overcome the gap between the skills acquired by the student's and the market needs using Activity led learning pedagogy for digital forensics programs. We have proposed five learning pedagogies for activity led learning pedagogy for digital forensics such as Lecture based learning Pedagogy, Demonstration based learning Pedagogy, Simulation based learning Pedagogy, Problem based learning Pedagogy and Project based learning Pedagogy.

Acknowledgments

Dr. Shaik Shakeel Ahamad would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No.

References

[1] Theoharidou, M., & Gritazalis, D. (2007). Common body of knowledge for information security. IEEE Security & Privacy, 5(2), 64–67.

[2] Tipton, H. F., & Henry, K. (2006). Official (ISC)² guide to the CISSP CBK. New York: Auerbach Publications.

[3] T. Jhansi Rani, Swathi (2017). A Review on Cyber Forensics. International Journal of Advanced Research in Education & Technology (IJARET), Vol. 4, Issue 2 (April - June 2017)

[4] Mandeep Kaur, Navreet Kaur, Suman Khurana (2016). Literature Review on Cyber Forensic and its Analysis tools. International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016

[5] B. V. Prasanthi (2016). Cyber Forensic Tools: A Review. *International Journal of Engineering Trends and Technology (IJETT) – Volume-41 Number-5 - November 2016*

[6] Seema Yadav, Khaleel Ahmad, and Jayant Shekhar (2011). Analysis of Digital Forensic Tools and Investigation Process. HPAGC 2011, CCIS 169, pp. 435–441, 2011

[7] https://www.vmware.com/mena/products/workstation-pro/workstation-pro-evaluation.html

[8] https://www.virtualbox.org/.

[9] https://www.sans.org/tools/sift-workstation/.

[10] https://www.parrotsec.org/download/.

[11] https://www.kali.org/.

Dr. Shaik Shakeel Ahamad holds a Ph.D. in Computer Science (cyber security) from the University of Hyderabad and IDRBT (Institute for Development and Research in Banking Technology), Hyderabad, India in the realm of secure mobile payment protocols and formal verification. He is currently working as an Assistant Professor in Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia. His research interests include cyber security, cloud computing, secure mobile payments, Block chain technology, secure smart grids, and security and privacy in Healthcare 4.0. He is CEI (Certified EC Council Instructor), ECSA (EC Council Certified Security Analyst), CHFI (Computer Hacking Forensic Investigator), Certified Threat Intelligence Analyst (CTIA), and Certified Application Security Engineer (CASE) – Java. He is serving as a Review Committee Member for many ISI indexed journals. He can be reached at ahamadss786@gmail.com&s.ahamad@mu.edu.sa