ASHESI UNIVERSITY

THE IMPACT OF DIGITAL FORENSICS ON CYBERCRIME IN GHANA

THESIS

B.Sc. Management Information Systems

Thesis submitted to the Department of Computer Science and Information Systems, Ashesi University in partial fulfillment of the requirements for the award of Bachelor of Science degree in Management Information Systems

William Obese Gyau

May 2020

DECLARATION

I hereby declare that this thesis is the result of my original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature:

……………………………………………………………………………………………

Candidate's Name:

……………………………………………………………………………………………..

Date:

……………………………………………………………………………………………

I hereby declare that the preparation and presentation of this thesis were supervised in accordance with the guidelines on supervision of the thesis laid down by Ashesi University.

Supervisor's Signature

…………………………………………………………………………………………….

Supervisor's Name

……………………………………………………………………………………………

Date:

……………………………………………………………………………………………

Acknowledgment

I will want to say a very big thank you to Mr. David Sampah for his support, advice, and materials during the entire process of the research and writing of this paper. The CSIS Department of Ashesi University provided the environment, motivation and technical know-how for me to explore and build an application for my project and I am very grateful. I also wish to extend my sincere gratitude to my friends and family for the support and encouragement.

Finally, I want to express special thanks to my family and friends, who have supported me through my academic journey at Ashesi University.

Abstract

Ghana lost a whopping $229.9million to *recorded* cybercrime cases between 2016 and August 2018 [2]. The victims being individuals, groups and corporate bodies especially banks. The increase in cybercrime is unfortunately not being addressed by the Ghana Police service nor the Criminal Investigative department due to a lack of resources and expertise to investigate these white-collar crimes. A report from Daniel Enin on the study of cybercrime offenders in Ghana indicates that the lack of confidence in the police and their inability to investigate these crimes has boosted the confidence of cybercriminals to commit these crimes [31]. This research paper seeks to find the answer to the question, 'what opportunity does digital forensics provide in combating cybercrime in Ghana". Digital forensics refers to the uncovering and examination of evidence located on all things electronic with digital storage, including computers, cell phones, and networks[11].

A pretest-posttest experiment was used in testing the "hypothesis that the learning of digital forensics which includes crime investigation and incidence reporting can help combat cybercrime in Ghana".

This research paper should provide insight into cybercrime, some related works in this domain, application development and some recommendations that will enable future researchers in this field to conduct their research in this domain.

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION AND BACKGROUND

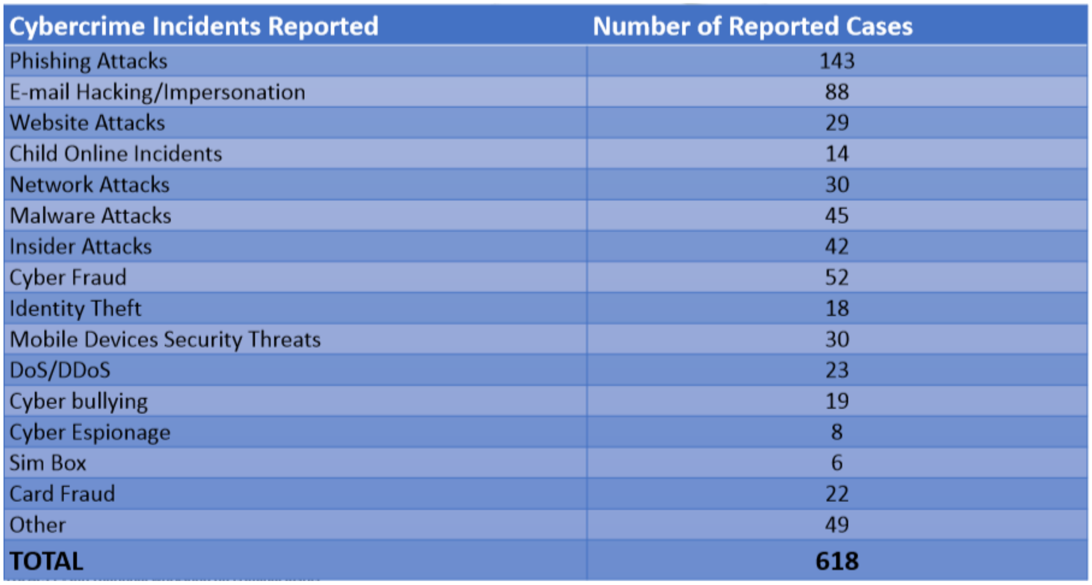
Crime refers to any act explicitly prohibited by law and is therefore considered illegal [9]. The investigation of crime has taken many forms over the centuries depending on the nature of the crime committed. For example, crimes involving arms might require fingerprints, ballistics, and firearms investigations, while crimes involving forgery of documents might require documents and photography examinations. The collection, analyses, and reports of data of criminal action are what is referred to as forensics[5]. It includes dentistry forensics, anthropology forensics, toxicology forensics, hair and fiber analysis, psychiatric forensics, biology forensics, chromatography, spectroscopy among others[13]. The use of ICT tools in recent times introduces new forms of crime popularly referred to as cybercrime or digital crime (henceforth cybercrime). The distinction between cybercrime and the traditional crimes according to Majid & Steinmetz is the role played by technology, whether it plays a mere role, or it was necessary [13]. Technology has equally capacitated crime investigators with the resources to collect and analyze data on cybercrimes. This type of forensics called Digital Forensics or Computer Forensics or Cyber Forensics is defined as the uncovering and examination of evidence located on all things electronic with digital storage, including computers, cell phones, and networks[11]. Digital forensics does not replace other types of forensics but is pursued alongside traditional forensics in most developed countries. Digital forensics is a relatively new discipline to policing and judicial ruling in developing countries like Ghana.

The Ghana Police Service which is the main law enforcing agency in the country was established in 1894. After, 27years, the Criminal Investigations Department (CID) was also established to provide technical and scientific support in criminal investigations[3]. There have been massive improvements in the CID since its inception. The department now has Commercial Unit, Homicide Unit, Anti-armed Robbery unit, Criminal Data Services, Drug Law Enforcement Unit, Forensic Science Laboratory, Central Firearms Unit, Interpol, and the Anti-human Trafficking[8]. The department in 2011 entered a 5year contract with the e-crime Bureau, a cybersecurity company to provide technical assistance to combat cybercrime due to the lack of resources in the CID to conduct digital crime investigations.[3]. This lack of expertise and unawareness of digital forensics provides a vulnerable stage for criminals to perpetuate their activities without facing the law due to the lack of evidence to incriminate them[10]. Cybercrime is an issue on the increase in Ghana which requires the implementation of a novel strategy like digital forensics for investigations. According to the head of the CID Department, Ghana lost a whopping $229.9million to *recorded* cybercrime cases between 2016 and August 2018 [2]. These cybercrimes span from individuals to groups and corporate bodies especially banks. Unfortunately, systems are not in place in Ghana to investigate and incriminate cyber fraudsters despite the admissibility of digital evidence in court[7]

The legal framework of Ghana provides a fair platform for electronic evidence to be presented in court as evidence [1]. This is included in the Electronics Act (2008) and The Evidence Act, 1975, NRCD 323 which regulates electronic transactions and allows for maps, graphs, disc, tape, soundtrack and visual images to be used as evidence in court respectively. Hence the basic requirements for establishing admissibility in court are achieved, however, these are not been utilized due to lack of expertise to gather and analyze digital evidence when there is such a crime.

1.2 Problem Statement and Motivation

Ghana has seen steady growth in technological advancements and the expansion of network infrastructures to communities and organizations around the country. For example, Ghana has acquired four additional submarine fiber optic cables: Main One Cable in 2010, GLO-1 (Globacom-1) and WACS (West Africa Cable System) in 2011, and ACE (African Coast to Europe) in 2013 which has increased the total bandwidth and reduced the cost of internet [6]. These technologies such as mobile payments, email services, mobile transactions, social media, etc. have allowed cybercriminals to engage in cybercrime, putting everyone at risk [12]. The Statistics and Information Technology Unit of the CID reported that 161 cybercrime cases were recorded by the police across the country from 2006 to 2011 [14]. About 1.2% of these cases were not pursued due to a lack of adequate information or evidence. The data also revealed that 9.3% of cases were sent to court while 7.5% of cybercriminals were imprisoned. It is very interesting to note that about 79.5% of the cases are still under investigation. Further reports have also shown a decline in the number of cases reported to the police due to their inability to investigate these cybercrimes[7]. Despite the decline in the number of cases reported to the police due to inconclusive investigations, these types of crime, however, keep increasing. E-crime, a private forensic company in Ghana, published a report in 2017 showing the increase in diverse cybercrimes in Ghana. [4].



Cybercrime Incidents Reported	Number of Reported Cases
Phishing Attacks	143
E-mail Hacking/Impersonation	88
Website Attacks	29
Child Online Incidents	14
Network Attacks	30
Malware Attacks	45
Insider Attacks	42
Cyber Fraud	52
Identity Theft	18
Mobile Devices Security Threats	30
DoS/DDoS	23
Cyber bullying	19
Cyber Espionage	8
Sim Box	6
Card Fraud	22
Other	49
TOTAL	**618**

Fig, cybercrime incidents reported to E-CRIME BUREAU 2017

Problem Statement

The increase in cybercrime, the unawareness of cybercrime among the general public, the insufficiency of expertise in the police service to conduct investigations, gather evidence, incriminate suspects, and are problems when not addressed can pose some risk to victims and the country at large.

Motivation.

The low level of understanding of digital forensics in the Ghana legal system which includes the police and the judiciary and among the general public motivated this study. The increase in cybercrime in Ghana according to reports from the Criminal Investigative Department and E-crime Bureau also contributed to the undertaking of this study.

1.3 RESEARCH QUESTIONS

1. Can digital forensics education increase the awareness of cybercrime in Ghana?
2. Can the learning of digital forensics by Intelligence Experts deter perpetrators from committing cybercrimes?
3. Can the learning of digital forensics make individuals conscious of cybersecurity?

These questions will be explored using an e-learning digital forensics platform and a set of questionnaires.

1.4 HYPOTHESIS:

Educating people security personnel and the public on digital forensics and cybercrime respectively, will bring about the better investigation, and encourage better incidence reporting which in turn will help combat cybercrime. The main objective of this project is to examine and analyze the learning of digital forensics and its effect on cybercrime in Ghana. A digital forensic e-learning platform will be developed to facilitate the learning and testing of the hypothesis.

CHAPTER 2 LITERATURE REVIEW

2.1 GLOBAL COMPUTER FORENSICS ENVIRONMENT

Digital forensics has become a critical component in the cybersecurity world and it is being patronized by security agencies and organizations[15]. According to Pollit, digital forensics might seem to be a relatively new field, however, it has a complex history to it. He describes the evolution in five phases; prehistory: where digital forensics did not exist, infancy(1985-1995); where digital forensics began to emerge, childhood(1995-2005) where there was tremendous growth in size and maturity, adolescence(2005-2010) where there was massive growth in depth and width with a lot of practitioners, and finally the future: where he predicts the introduction of powerful tools, software, educators, certifications and legal frameworks to back the field of digital forensics[19].

The USA pioneered the field of digital forensics in the early '80s with a lot of countries following and adopting this novel way to crime investigation[22]. However, all countries do not have the same level of expertise and resources in conducting digital forensics. The G8 nations which include France, Germany, Italy, the United Kingdom, Japan, the United States, Canada, and Russia are advanced in the field of digital forensics in terms of resources, personnel, and infrastructures[29]. South Africa is emerging on the scene in digital forensics in Africa, however, practitioner tends to lack training, competency, and experience to examine and analyze evidence as it is in most developing countries[35]. The International Criminal Police Organization (INTERPOL), International Organization on Computer Evidence (IOCE), International Association of Computer Investigative Specialists (IACIS) are key international bodies spearheading the course of digital forensics across the world.

Universities across the world are also pursuing some digital forensics courses, degrees and masters in the field of digital forensics. There are currently 485 Digital Forensic Science schools in the US[33]. In Pakistan, the increase in cybercrime has led to the introduction of digital forensic courses, degrees, masters and professional examinations[28]

Digital forensics is not in isolation but is performed hand-in-hand with legal precepts and regulations to ensure that the right procedures are used in digital investigations and prosecution on the basics of digital evidence. According to Monti Andrea, failing to align with legal precedents, regulations, and expectations in conducting digital forensics will prevent justice from prevailing[17].Many countries around the world have instituted regulations to facilitate digital forensics procedures. The fourth amendment protection IN THE USA, the evidence act of Ghana, the police and crime act 1997 in the United Kingdom, the electronic communications and transactions a*ct* in South Africa, and the INTERPOL regulations on digital forensics lab are all some examples of laws instituted to enhance digital crime investigations.

Digital forensics globally faces some challenges in its operations. According to the article,
*The Future of Digital Forensics: Challenges and the Road Ahead***,** some of the challenges facing the field digital forensics include, the introduction of modern and heterogeneous devices, legal issues, privacy in data collection for investigations, and the lack of standards*[27]*

2.2 COMPUTER & CYBER FORENSICS IN GHANA

Earlier works into computer forensics in Ghana explores the need for digital forensics, the increase in cybercrime, the legal framework for a forensic environment and identifies some policies and initiatives the government has undertaken to promote digital forensics. Below are some of these kinds of literature about forensics in Ghana.

The journal article *History of forensic science in Ghana*[25] by Amankwah, explores the history of forensic Science in Ghana since 1894 when the Ghana Police Service was established. It investigates the evolution of forensic science in Ghana which has been very biological and chemical while hinting on the need for digital forensics in this era. The need for digital forensics especially in the judiciary in Ghana has been investigated by Michael AdjeiFrempong & Kamal in their paper *Awareness and Understanding of Computer Forensics in the Ghana Legal System*[24]. This literature explores the legal framework of Ghana, the acceptability of digital evidence in court using digital forensics and the unawareness of digital forensics among judges. Twenty judges participated in the research exploring digital forensics in the court of law. It revealed that most judges are not exposed to digital forensics which meant that the interpretation of digital evidence by judges will be cumbersome.

The increase in cybercrime in Ghana have been studied in the paper *Cyber Crime and Criminality in Ghana*, which explores the prevalence of cybercrimes using data from the Ghana Police Service, and the criminal Investigative Department in Ghana. The research was done asking key stakeholders in Ghana these two key questions; what are forms of cybercrimes in Ghana? How is Ghana addressing reported cases of cybercrime? It further reports on the lack of expertise on the part of the Ghana Police Service to gather digital evidence which results in no or inconclusive investigations. Daniel Enin’s paper; *Cybercrime in Ghana: A Study of Offenders, Victims And the Law*[31] goes a step further to understand the motivations behind cybercrime and the experiences of victims with offenders and the police. His paper suggests that the lack of confidence in the criminal justice system has increased the confidence of criminals to continue their criminal activities.

Further research by Mohammed & Adjei titled *Computer & Cyber Forensics: A Case Study of Ghana*[16], touched on some technical aspects of cybercrime in Ghana. The study emphasizes the importance of the study of computer and cyber forensics in the fight against cybercrime while pointing to some technologies such as VPN used by cybercriminals to hide their identity on the internet.

2.3 E-LEARNING

E-Learning refers to anything delivered, enabled, or mediated by electronic technology for the explicit purpose of learning[32]. It is a web-based form of teaching and learning which over the years has outperformed the traditional classroom form of teaching and learning[30]. Several types of research have been undertaken to understand the need for e-learning, the current trend in e-learning, methodologies in e-learning among others. The number of research papers on e-learning and its importance keeps increasing after a structured search from online databases with an immense increase over the last five years[21].

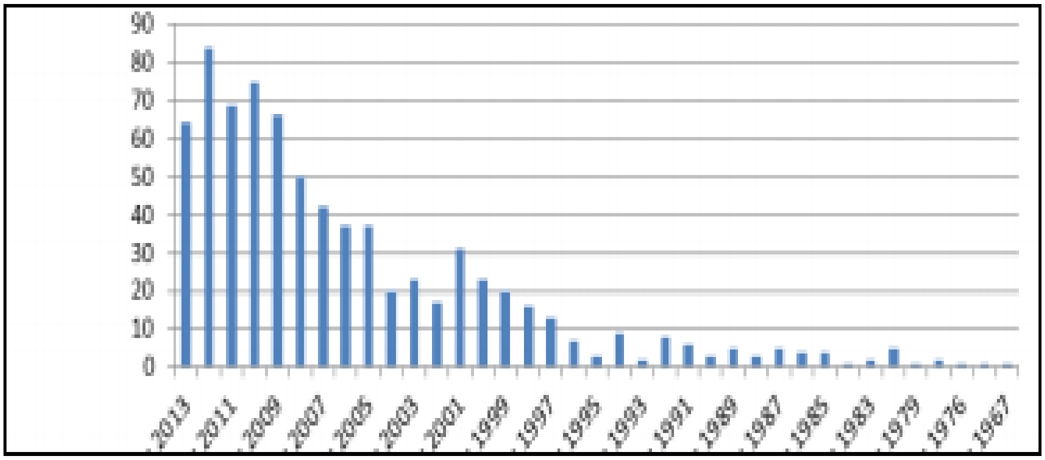


Fig 1. The trend in the number of articles published on e-learning from 1967 to 2013.

The following are some reasons e-learning has become popular and it’s been patronized by a large group of people[34];

- It engages learners who have difficulty attending conventional classroom training because they are geographically dispersed, have limited time resources to travel, busy with work or family commitments and usually located in conflict and post-conflict areas and restricted in their mobility because of security reasons,
- It engages learners limited from participating in classroom sessions because of cultural or religious beliefs, facing difficulties with real-time communication (e.g. foreign language learners or very shy learners),
- E-learning is self-paced learning, mostly with visuals, audios and kinesthetic [30] which helps to conceptualize ideas very easily.

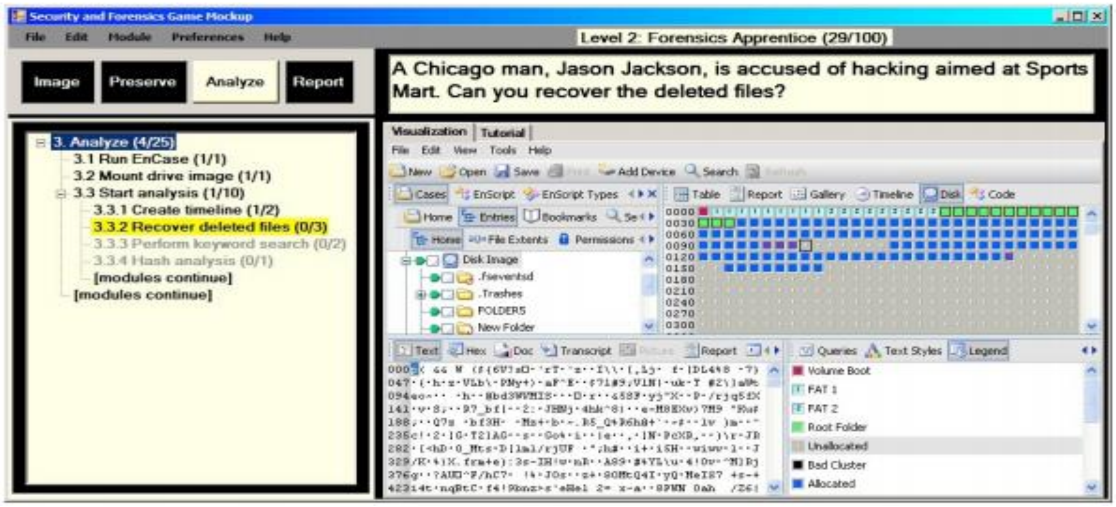
Even though e-learning is expensive in terms of development (web developers, time involved), it is relatively cheaper than putting in systems, infrastructures for face to face learning. E-Learning industry, in general, has a great future irrespective of the situation of the economy whether it be a developed economy or a developing one[36].

2.4 DIGITAL FORENSICS E-LEARNING

Education and training in digital forensics require a variety of digital experiences, technology, and realistic features to provide a better understanding and training in the field[20]. Comprehensive education of digital forensics involves both education and training. The article, *Computer Forensics Education* distinguishes education from training, suggesting the need for the two in digital forensic education. Education involves knowledge, abstraction, developing tools, establishing procedures and theory while training involves skills, application, using tools, applying procedures and practice[23].

Most digital forensics online courses tend to be visual and video-based since it involves some usage of software, and command-line scripting, etc. and a good example is explored in Kessler's paper on Online Education in Computer and Digital Forensics. This paper explores the design of introductory computer forensics courses at Champlain College, with particular attention to hands-on assignments in the online environment [37].

An interesting approach to digital forensic e-learning is also explored by Yin Pan, Sumita Mishra, Bo Yuan, and Bill Stackpole[18] in developing virtual games to engage talented young students to explore the field of digital forensics. These games involve exploring how to use open-source tools for disk imaging, data recovery, steganography, log analysis, etc. Even though this approach is very engaging and will induce young ones to gain some interest in the field, basic knowledge of operating systems, registry and file system is required for anyone who fully comprehends digital forensics concepts.



Level 2: Forensics Apprentice (29/100)

A Chicago man, Jason Jackson, is accused of hacking aimed at Sports Mart. Can you recover the deleted files?

- 3. Analyze (4/25)
  - 3.1 Run EnCase (1/1)
  - 3.2 Mount drive image (1/1)
  - 3.3 Start analysis (1/10)
    - 3.3.1 Create timeline (1/2)
    - 3.3.2 Recover deleted files (0/3)
    - 3.3.3 Perform keyword search (0/2)
    - 3.3.4 Hash analysis (0/1)
    - [modules continue]
  - [modules continue]

Fig 2. A screenshot of data recovery game

According to Austin, open-source tools like an autopsy, helix can be used in understanding basic digital forensic without buying expensive tools and equipment[26]. With a limited budget for Ghana police, implementing training sessions and developing a novel tool or infrastructure or even a laboratory to conduct digital forensics will imply more money and expenses. Hence open source tools can be utilized to achieve the same results.

2.5 SUMMARY

These papers contribute to this project in these ways;

1. Understanding cybercrime in Ghana
2. Understanding the motivations of cybercriminals and the experiences of victims
3. The current intelligence infrastructure in the police and the readiness of legal institutions in the area of digital forensics
4. The importance and application of e-learning in the field of digital forensics.

Despite the contributions of these papers to the learning of digital forensics in Ghana, there are some gaps like the insufficient evidence or research into how the learning of digital forensics can help combat cybercrime in Ghana and the complex digital forensic e-learning systems which will require some amount of experience before use.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Research Proposal

Research generally serves the purpose of exploring, describing, and explaining a phenomenon, theories, ideas or projects[3]. **This study aims to consider and analyze a digital forensics e-learning platform, its implementation feasibility and its effect on cybercrime in Ghana.** This section outlines the methodological approach, research instruments, sample size, data collection, data analysis, ethical considerations and the technical overview of this study.

3.2 Research Methodological Approach

The methodological approach to this study is an experiment. The experiment will be conducted on the victim sample and the security enthusiast sample identified above. A pretest-posttest type of experimental research approach will be adopted in this study. A pretest-posttest approach is mostly adopted in experimental research to determine if there is a difference among groups with regards to some variable of interest after the imposition of a treatment intervention[2]. Considering the research question, **"What is the impact of digital forensics on cybercrime"**, a comprehensive research study like the pretest and posttest helps to measure outcomes and results after the introduction and exposure of participants to the digital forensics e-learning platform.

3.3 Research Participants & Sampling

Sampling refers to the process of selecting participants from the whole population for research purposes. Research participants are selected because they can provide rich descriptions of their experiences. Thereby providing information that is rich and which will be able to challenge and enrich the researcher's understanding [4]. Participants for the research are students, staff and non-staff members of Ashesi University.

Victim sample: The victim sample involves a group of people prone to cybercrime attacks. This ranges from people with bank accounts, emails, mobile money accounts, e-commerce systems and some level of internet or digital presence. The population for this sample is Ashesi university staff, students, and non-staff members. The **Voluntary sample Strategy will be used to gather participants for data collection.** A voluntary sample is made up of people who self-select into the survey and have a strong interest in the main topic of the survey. A total of 20 individuals will be sampled to participate in the experimental research. The reason for sampling victims is to understand whether or not the exposure and awareness of a digital forensic platform will influence better incidence reporting practices and cybersecurity consciousness.

Security Experts/Security Conscious People: This sample involves a group of students taking cybersecurity courses in Ashesi, security enthusiasts from staff and faculty of Ashesi University. A simple random sampling will be used to sample participants for this survey. A total of 20 participants (Security Enthusiast) will participate in the experiment. The reason for sampling security enthusiasts is to assess whether or not the exposure to a digital forensic e-learning platform will influence their interest in the field, enhance their skills in crime investigation and the potential impact of a digital forensic e-learning tool on crime investigations.

Sample Size:

PARTICIPANTS	**SAMPLE SIZE**
Victim Participants	**20**
Security Enthusiasts in Ashesi	**20**

3.4 Research Instruments and Data Collection.

Research instruments are facts finding strategies or tools for data collection[1]. A pretest-posttest experiment is a tool that will be used to collect data using an e-learning digital forensics platform as an intervention.

3.5 Pretest-Posttest Experiment

Incidence Reporting Experiment: A total of 20 students/staff who self-select into this sample will be given a set of questionnaires to answer concerning an email phishing case scenario. After, they are exposed to some modules on the e-learning platform particularly on incidence reporting. They then fill the same set of questionnaires after this intervention**.** Both hard copies and online questionnaires will be administered to participants.

Crime Investigation Experiment: A total of 20 students/staff who identify as security enthusiast will be assigned practical problem sets about email phishing investigation. After, they are exposed to some modules on the e-learning platform particularly on how to solve the problem set using open source tools. After this exposure to the e-learning platform, they are assigned the same problem sets to solve.

3.6 Data Analysis

Outcomes from the pretest experiment will be compared to the outcome of the posttest experiment. **C**ritical analysis and interpretation of figures and numbers using graphs. Also, the findings in this study will be compared to the findings of the literature review.

3.7 Ethical considerations

This study has no physical risk, psychological or emotional risk to participants. Participants are assured of anonymity and confidentiality to all responses. Detailed information about the project is presented so that responses are not influenced nor bias.

3.8 E-Learning Application Overview: The e-learning system is a web application that will be hosted on an apache web server.

Design and Architecture: A three-tier architecture which involves a client/presentation tier, an application tier, and a database tier.

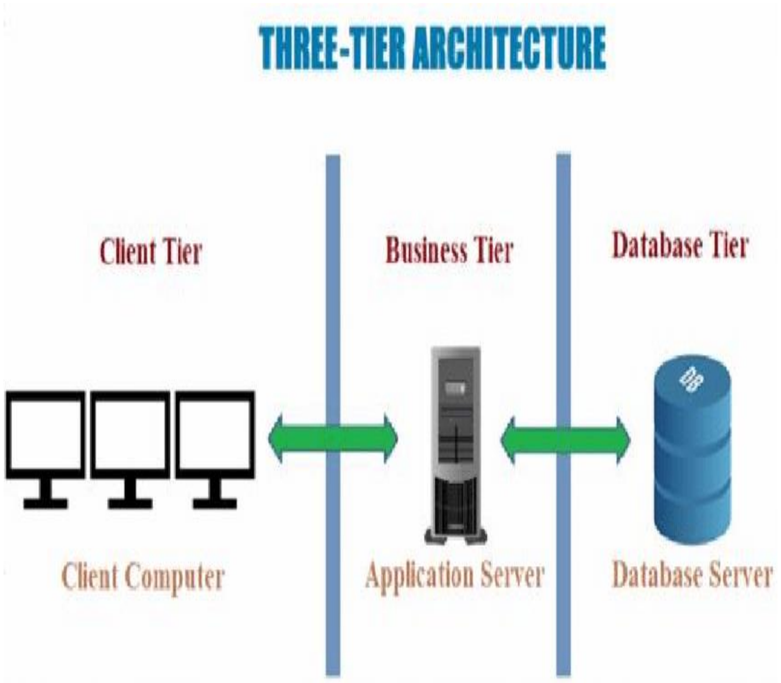


Fig 3: Three-tier architecture

Client/Presentation Layer: This is the layer of the application the user or client interacts with. Bootstrap, JavaScript, and HTML are technologies that will be explored in the presentation layer.

Application Layer: This layer is responsible for handling the core functionality and business logic of the web application. PHP Model View Controller Approach and AJAX will be used in this layer.

Database Layer: This layer handles the data storage and access system of the application. MySQL database will be utilized here.

Functional requirement:

- Cloud-based or hosted solution, Study scheduling,
- Content sharing,
- The system should allow the upload of syllabuses that are accessible through students' specific access rights.
- The possibility to create, edit and design learning content
- The possibility to integrate and embed images, presentations and video content from, YouTube, and other useful web platforms.
- The possibility to download course materials and set up to open source tools.
- Automatic notification to users about new activities, publications, assignments, examinations
- View course progress allowing the user to quickly and easily understand where s/he stands in the learning process.
- The platform must possess a built-in system for sending and receiving e-mails

Non-functional requirement:

- Attractive and easy to use interface.
- High Capacity of Data
- Modularity
- Interoperability
- Scalability
- Security
- Performance

Data Flow Diagram:

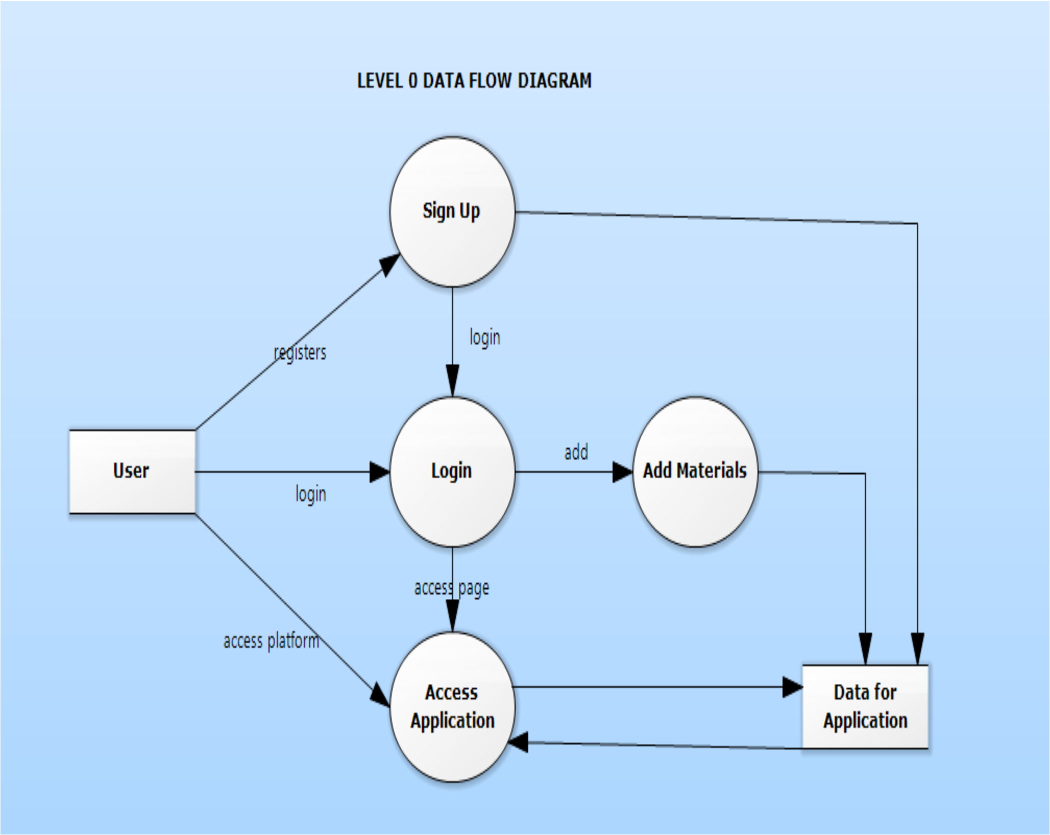


Fig 4. Data flow diagram showing how data will be flowing in the e-learning management system.

Activity diagram/Use case scenario

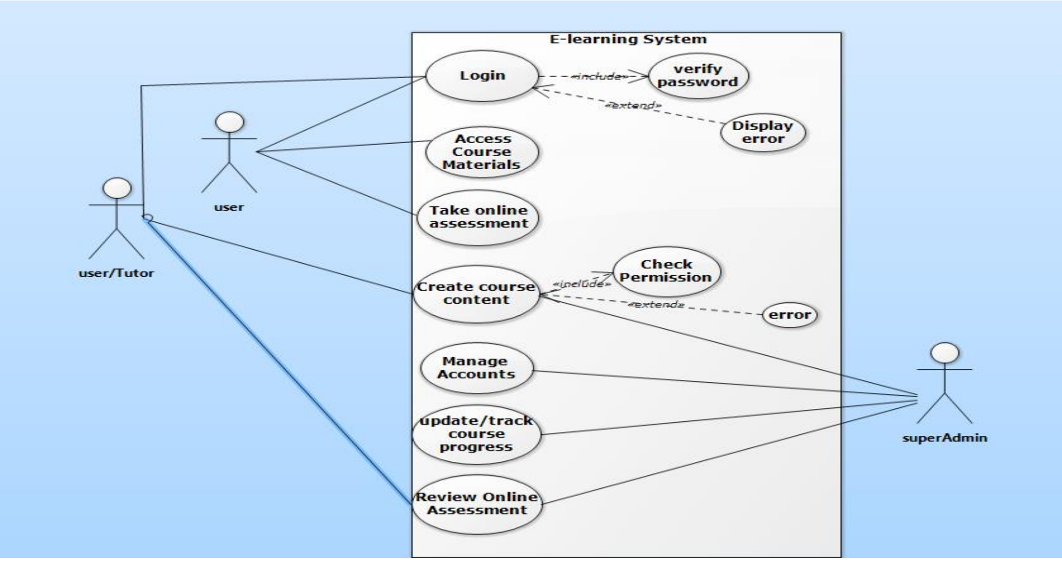
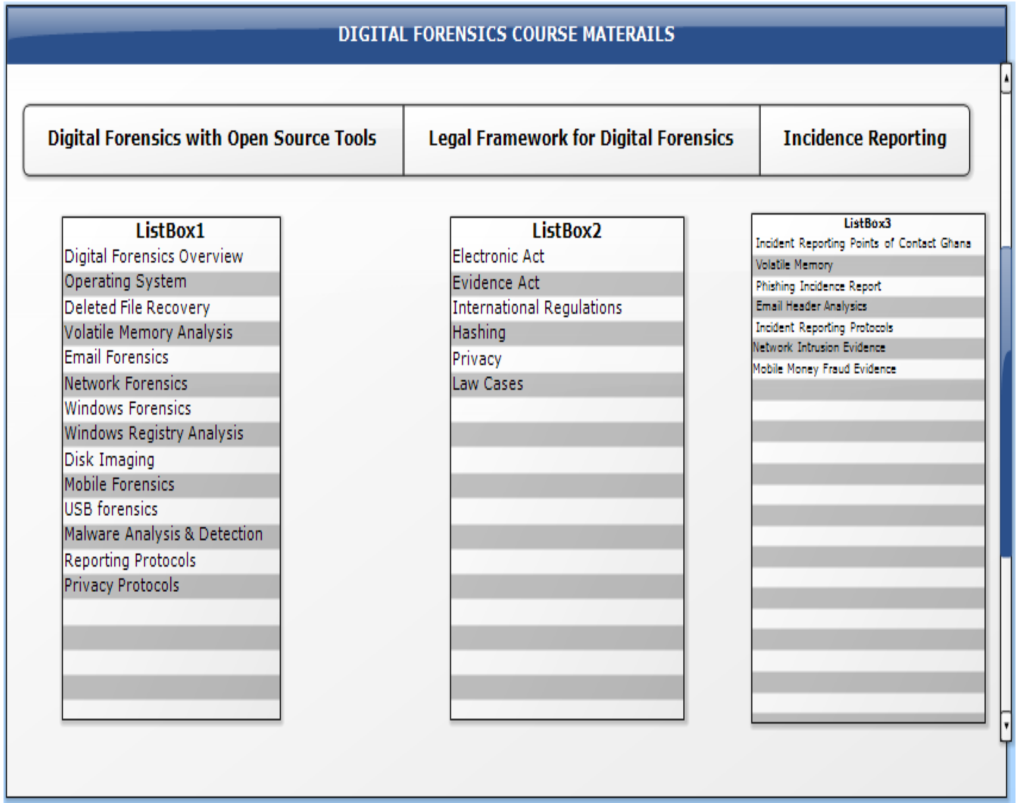


Fig 5. A use case diagram for an e-learning management system

COURSE MODULES


DIGITAL FORENSICS COURSE MATERAILS
Digital Forensics with Open Source Tools
Legal Framework for Digital Forensics
Incidence Reporting

ListBox1
Digital Forensics Overview
Operating System
Deleted File Recovery
Volatile Memory Analysis
Email Forensics
Network Forensics
Windows Forensics
Windows Registry Analysis
Disk Imaging
Mobile Forensics
USB forensics
Malware Analysis & Detection
Reporting Protocols
Privacy Protocols

ListBox2
Electronic Act
Evidence Act
International Regulations
Hashing
Privacy
Law Cases

ListBox3
Incident Reporting Points of Contact Ghana
Volatile Memory
Phishing Incidence Report
Email Header Analysics
Incident Reporting Protocols
Network Intrusion Evidence
Mobile Money Fraud Evidence

Fig 6: Course modules for the e-learning app

CHAPTER 4: EXPERIMENT AND DATA ANALYSIS

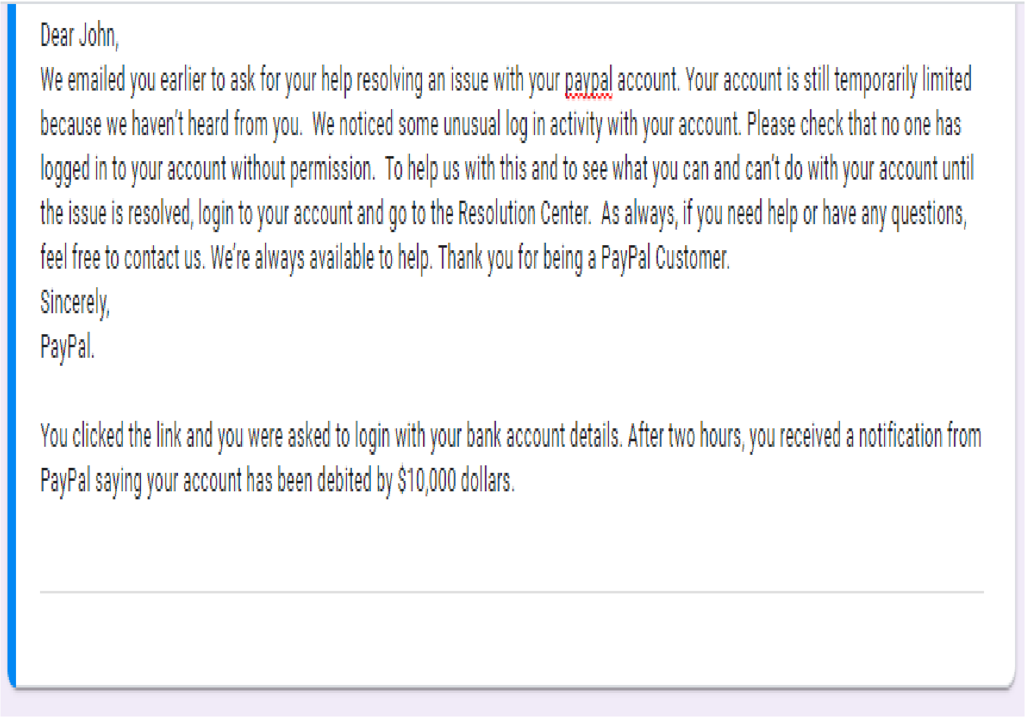
4.1 Summary

This chapter focuses on the procedures, case scenarios, observations, and data analysis of the pretest and posttest experiment about an email phishing case scenario. The results section focuses on analyzing the data that were obtained during the experiment. These results are analyzed by doing a quantitative analysis of the experiment and a conclusion will be drawn on them.

4.2 The Experiment:

The two experiments which are the incidence reporting experiment and the Cybercrime investigation took place on Ashesi Campus from the 2nd of March to the 16th of March. A google form was sent out for people to voluntarily sign up for the incidence reporting experiment. For the cybercrime investigation experiment, a sample of 20 people was randomly selected from the information security class and clubs on campus to engage in the cybercrime investigation experiment.

Case Scenario for Experiments: The case scenario was the same for both incidence reporting and cybercrime investigation experiment. It is a sample email phishing attack. Below is a snapshot of the case scenario as was in the google form.



Dear John,

We emailed you earlier to ask for your help resolving an issue with your paypal account. Your account is still temporarily limited because we haven't heard from you. We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without permission. To help us with this and to see what you can and can't do with your account until the issue is resolved, login to your account and go to the Resolution Center. As always, if you need help or have any questions, feel free to contact us. We're always available to help. Thank you for being a PayPal Customer.

Sincerely,
PayPal.

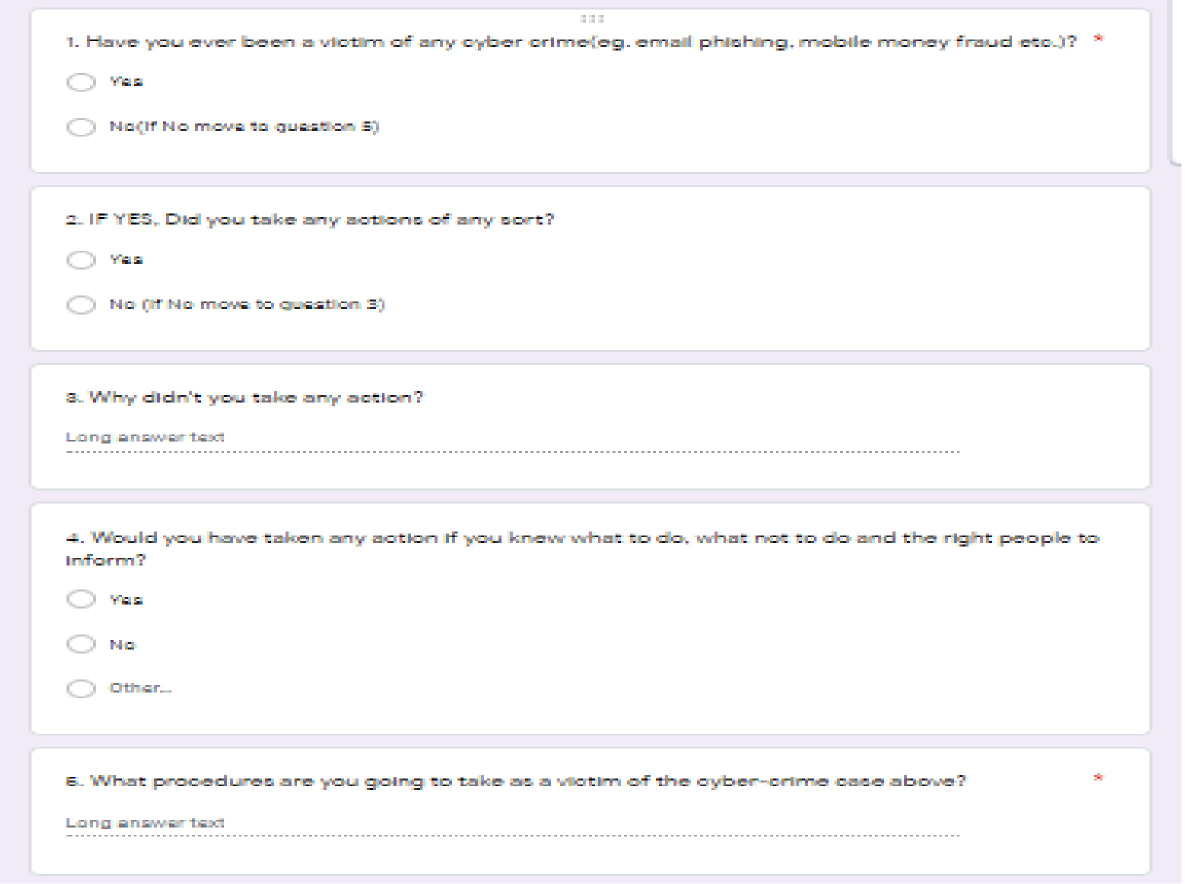
You clicked the link and you were asked to login with your bank account details. After two hours, you received a notification from PayPal saying your account has been debited by $10,000 dollars.

Fig 7: Case scenario for pretest and posttest experiment

Questionnaires were administered to participants online using google forms. For the incidence reporting experiment, the link http://bit.ly/2wpglZ8 which contains the questionnaires was sent to participants. For the cybercrime investigation experiment, the link http://bit.ly/32P89x9 was sent to participants.

4.3 Conducting Pretest Incidence Reporting Experiment and Cybercrime Investigation Experiment:

The pretest experiment involved victim participants and security enthusiast participants reading a case scenario and answering questions relating to incidence reporting and email phishing investigations respectively. It took approximately 5mins for all participants to fill the questionnaires in the pretest experiment.



1. Have you ever been a victim of any cyber crime(eg. email phishing, mobile money fraud etc.)? *

○ Yes

○ No(If No move to question 5)

2. IF YES, Did you take any actions of any sort?

○ Yes

○ No (If No move to question 3)

3. Why didn't you take any action?

Long answer text

4. Would you have taken any action if you knew what to do, what not to do and the right people to inform?

○ Yes

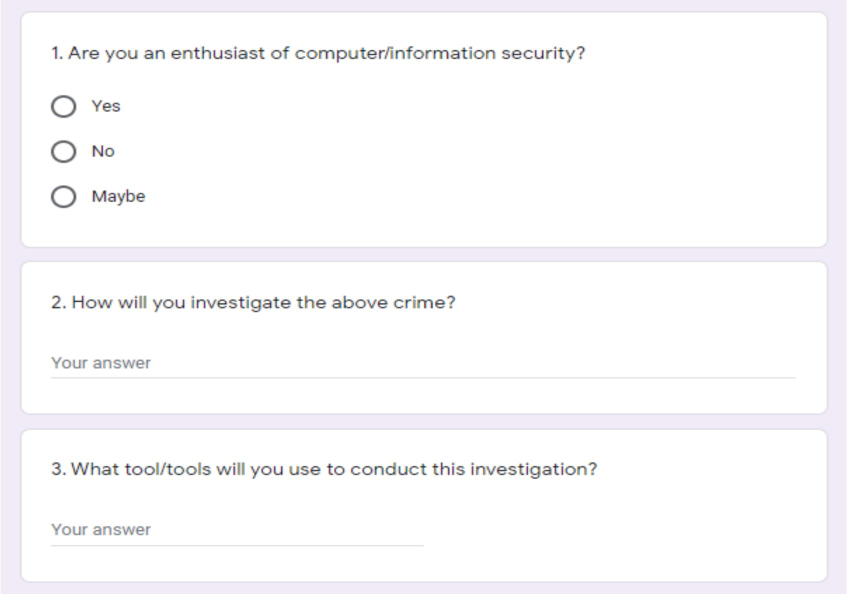
○ No

○ Other...

5. What procedures are you going to take as a victim of the cyber-crime case above? *

Long answer text

Fig 8: Pretest Questionnaires for Incidence Reporting Experiment



1. Are you an enthusiast of computer/information security?

○ Yes

○ No

○ Maybe

2. How will you investigate the above crime?

Your answer

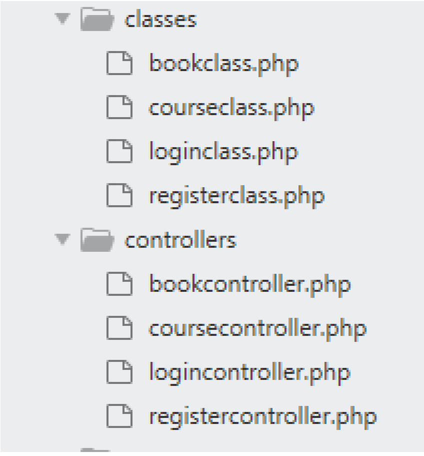
3. What tool/tools will you use to conduct this investigation?

Your answer

Fig 9: Pretest Questionnaires for Cybercrime Investigation Experiment

4.4 Implementation of E-learning Application Used for Posttest Experiment

The e-learning application with the domain name “http://learnforensicsgh.epizy.com/" was built using the Model View Controller approach which involves the use of classes, controllers, and view (user interfaces). The application has four classes namely, book class, course class, login class, and register class. It also has four controllers for the four classes.



```
classes
    bookclass.php
    courseclass.php
    loginclass.php
    registerclass.php
controllers
    bookcontroller.php
    coursecontroller.php
    logincontroller.php
    registercontroller.php
```

Fig 10: Classes and controllers directory

Classes

Book class: The book class consists of attributes/behaviours like;

- add_book
- view_book
- search_book

Course class: The course object consists of attributes like

- add_course
- add_sections
- add_images
- view_course
- view_one_course
- view_course_taught
- view_section

- view_section_content
- view_images
- Enrolled_coureses
- enrolled_view

Loginclass: The login class consists of attributes/behaviours like

- login_learner
- login_instructor
- view_instructor_information

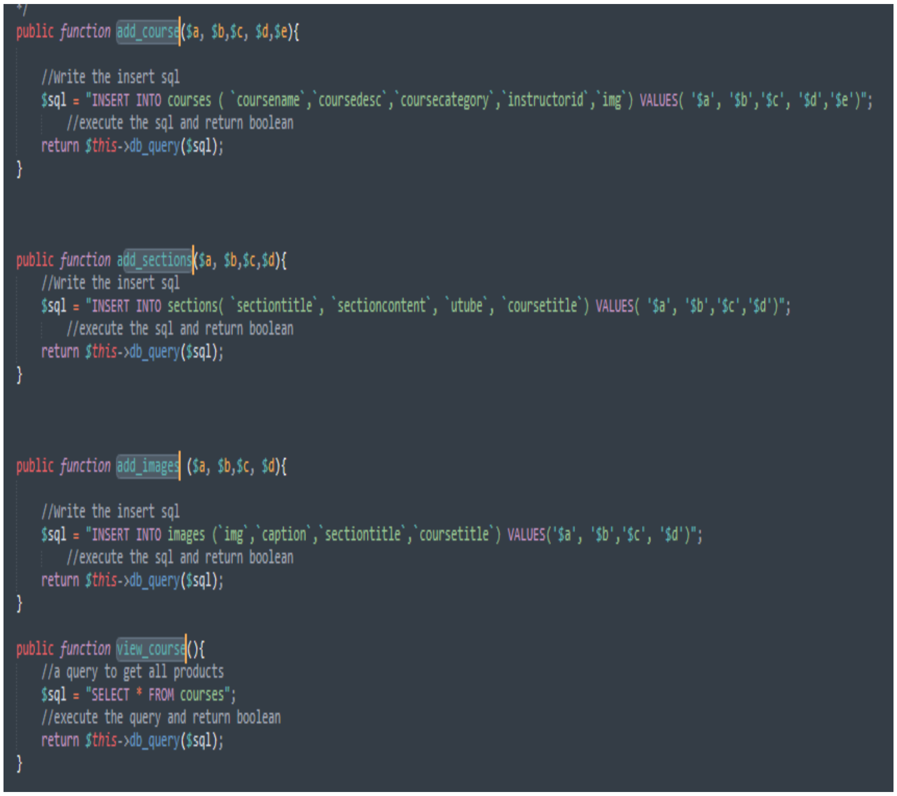
***Registerclass*:** The register class consists of attributes like

- register_learner
- register_instructor

Controllers: Every class has a controller to control/model the flow of data to the view/user.

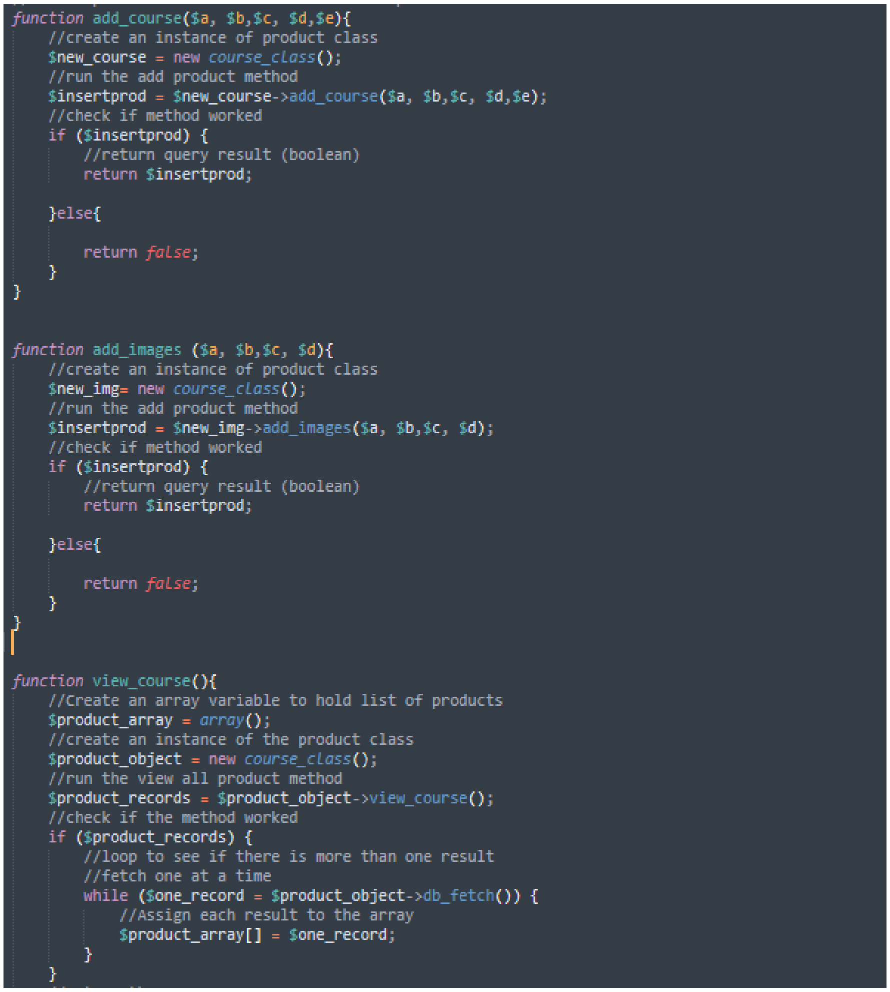
Hence all attributes respectively have their corresponding controller to channel data to the view.

Below is a snapshot of the course class and its course controller.



```
*/
public function add_course($a, $b,$c, $d,$e){

    //Write the insert sql
    $sql = "INSERT INTO courses ( `coursename`,`coursedesc`,`coursecategory`,`instructorid`,`img`) VALUES( '$a', '$b','$c', '$d','$e')";
        //execute the sql and return boolean
    return $this->db_query($sql);
}



public function add_sections($a, $b,$c,$d){
    //Write the insert sql
    $sql = "INSERT INTO sections( `sectiontitle`, `sectioncontent`, `utube`, `coursetitle`) VALUES( '$a', '$b','$c','$d')";
        //execute the sql and return boolean
    return $this->db_query($sql);
}



public function add_images ($a, $b,$c, $d){

    //Write the insert sql
    $sql = "INSERT INTO images (`img`,`caption`,`sectiontitle`,`coursetitle`) VALUES('$a', '$b','$c', '$d')";
        //execute the sql and return boolean
    return $this->db_query($sql);
}

public function view_course(){
    //a query to get all products
    $sql = "SELECT * FROM courses";
    //execute the query and return boolean
    return $this->db_query($sql);
}
```

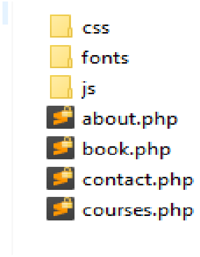
Fig 11. Implementation of course class



```
function add_course($a, $b,$c, $d,$e){
    //create an instance of product class
    $new_course = new course_class();
    //run the add product method
    $insertprod = $new_course->add_course($a, $b,$c, $d,$e);
    //check if method worked
    if ($insertprod) {
        //return query result (boolean)
        return $insertprod;

    }else{

        return false;
    }
}


function add_images ($a, $b,$c, $d){
    //create an instance of product class
    $new_img= new course_class();
    //run the add product method
    $insertprod = $new_img->add_images($a, $b,$c, $d);
    //check if method worked
    if ($insertprod) {
        //return query result (boolean)
        return $insertprod;

    }else{

        return false;
    }
}


function view_course(){
    //Create an array variable to hold list of products
    $product_array = array();
    //create an instance of the product class
    $product_object = new course_class();
    //run the view all product method
    $product_records = $product_object->view_course();
    //check if the method worked
    if ($product_records) {
        //loop to see if there is more than one result
        //fetch one at a time
        while ($one_record = $product_object->db_fetch()) {
            //Assign each result to the array
            $product_array[] = $one_record;
        }
    }
```

Fig 12. Implementation of corresponding controllers

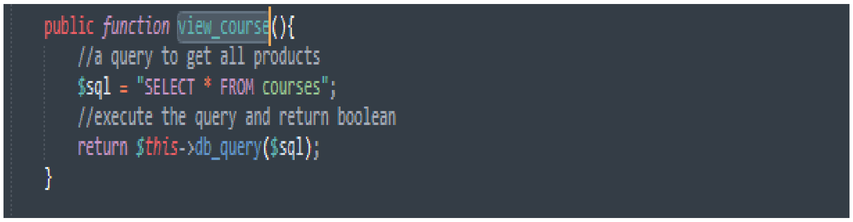
View: CSS and bootstrap were utilized for the aesthetic appeal of the web application and to also make it mobile compatible. View mainly consisted of about, book, contact, courses and index page. Controllers were called on view pages to display data from a database.



css
fonts
js
about.php
book.php
contact.php
courses.php

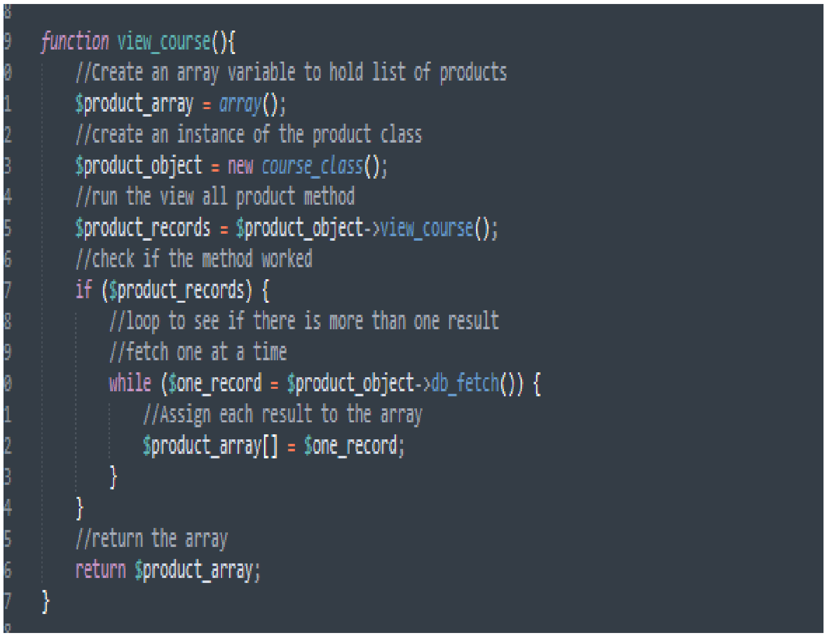
Fig 13: Directory of view classes

Below is a snippet of the view course attribute, view course controller and view showing how the MVC was used for this project



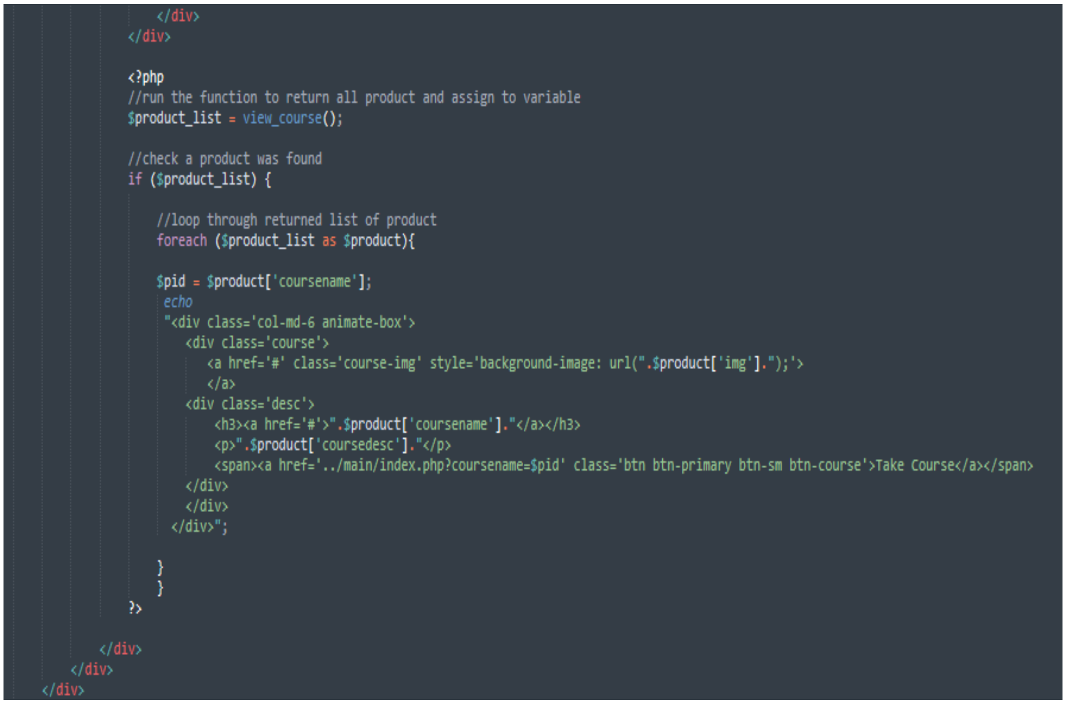
```
public function view_course(){
    //a query to get all products
    $sql = "SELECT * FROM courses";
    //execute the query and return boolean
    return $this->db_query($sql);
}
```

Fig 14. Model(view course class)



```
function view_course(){
    //Create an array variable to hold list of products
    $product_array = array();
    //create an instance of the product class
    $product_object = new course_class();
    //run the view all product method
    $product_records = $product_object->view_course();
    //check if the method worked
    if ($product_records) {
        //loop to see if there is more than one result
        //fetch one at a time
        while ($one_record = $product_object->db_fetch()) {
            //Assign each result to the array
            $product_array[] = $one_record;
        }
    }
    //return the array
    return $product_array;
}
```

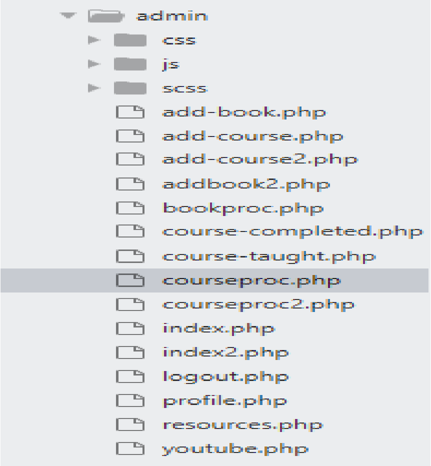
Fig 15.View Controller



```
        </div>
      </div>

      <?php
      //run the function to return all product and assign to variable
      $product_list = view_course();

      //check a product was found
      if ($product_list) {

        //loop through returned list of product
        foreach ($product_list as $product){

        $pid = $product['coursename'];
         echo
         "<div class='col-md-6 animate-box'>
           <div class='course'>
             <a href='#' class='course-img' style='background-image: url(".$product['img'].");'>
             </a>
           <div class='desc'>
             <h3><a href='#'>".$product['coursename']."</a></h3>
             <p>".$product['coursedesc']."</p>
             <span><a href='../main/index.php?coursename=$pid' class='btn btn-primary btn-sm btn-course'>Take Course</a></span>
           </div>
           </div>
          </div>";

        }
        }
      ?>

    </div>
  </div>
</div>
```

Fig 16. Code implementing the display of courses using the controller in fig. 15

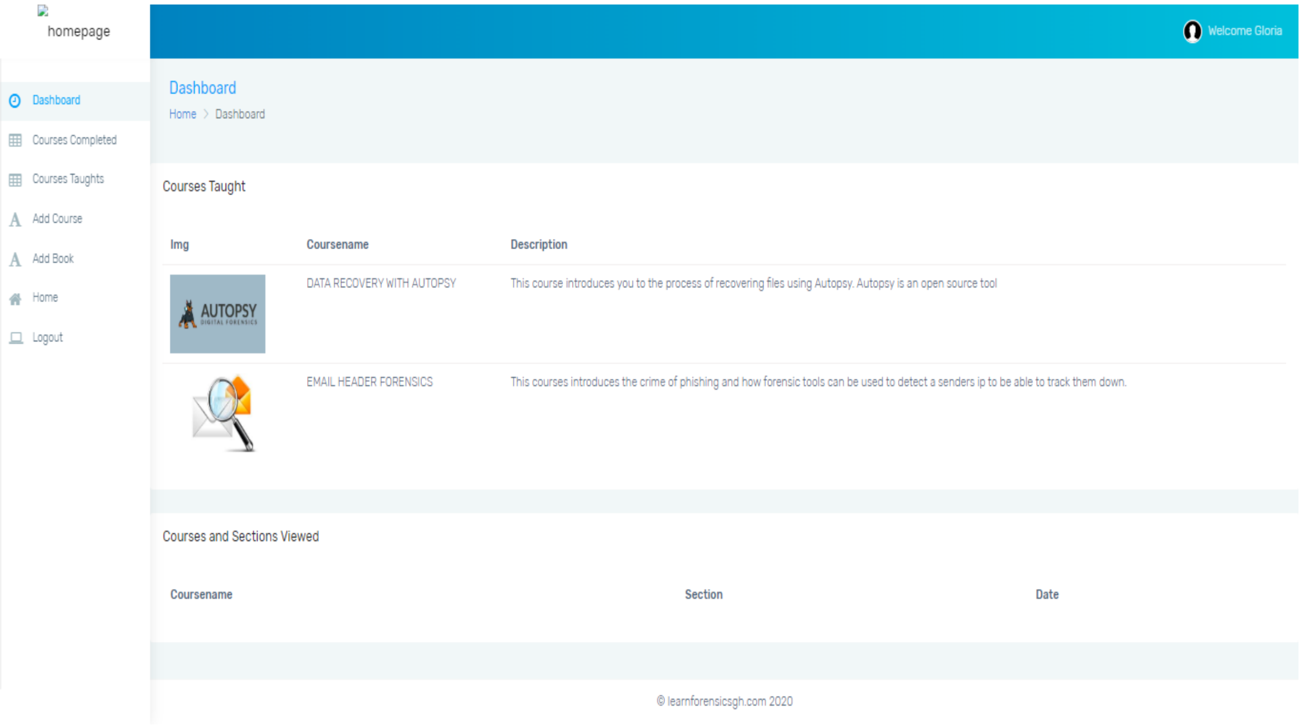
Dashboard: A dashboard was implemented for both learners and instructors to view their activities like courses taught, viewed and perform certain tasks like adding a book and creating a course. However only, instructors have the privilege to create a course after a successful login. The dashboard also required the use of the model view controller approach.



```
▾ admin
  ▸ css
  ▸ js
  ▸ scss
    add-book.php
    add-course.php
    add-course2.php
    addbook2.php
    bookproc.php
    course-completed.php
    course-taught.php
    courseproc.php
    courseproc2.php
    index.php
    index2.php
    logout.php
    profile.php
    resources.php
    youtube.php
```

Fig. 17 Below is a snapshot of the dashboard directory

Fig. 18 Below is a snapshot of a dashboard that belongs to an instructor logged in as "Gloria'.



Dashboard

Home > Dashboard

Courses Taught

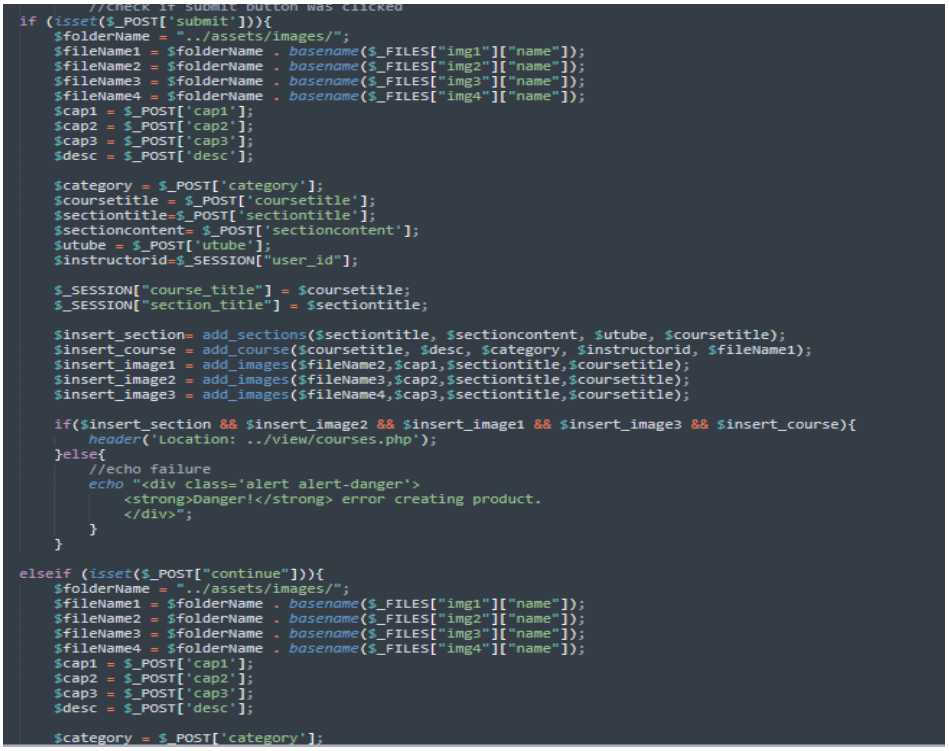
Img	Coursename	Description
	DATA RECOVERY WITH AUTOPSY	This course introduces you to the process of recovering files using Autopsy. Autopsy is an open source tool
	EMAIL HEADER FORENSICS	This courses introduces the crime of phishing and how forensic tools can be used to detect a senders ip to be able to track them down.

Courses and Sections Viewed

Coursename	Section	Date

© learnforensicsgh.com 2020

Add Course: The add course section of the dashboard consisted of forms and text areas for inputs like text, images, links, section titles, and section content. It calls on the addcourse class and controller to perform its function of adding courses. Below is a section of the code that implements the add course functionality



```
        //check if submit button was clicked
if (isset($_POST['submit'])){
    $folderName = "../assets/images/";
    $fileName1 = $folderName . basename($_FILES["img1"]["name"]);
    $fileName2 = $folderName . basename($_FILES["img2"]["name"]);
    $fileName3 = $folderName . basename($_FILES["img3"]["name"]);
    $fileName4 = $folderName . basename($_FILES["img4"]["name"]);
    $cap1 = $_POST['cap1'];
    $cap2 = $_POST['cap2'];
    $cap3 = $_POST['cap3'];
    $desc = $_POST['desc'];

    $category = $_POST['category'];
    $coursetitle = $_POST['coursetitle'];
    $sectiontitle=$_POST['sectiontitle'];
    $sectioncontent= $_POST['sectioncontent'];
    $utube = $_POST['utube'];
    $instructorid=$_SESSION["user_id"];

    $_SESSION["course_title"] = $coursetitle;
    $_SESSION["section_title"] = $sectiontitle;

    $insert_section= add_sections($sectiontitle, $sectioncontent, $utube, $coursetitle);
    $insert_course = add_course($coursetitle, $desc, $category, $instructorid, $fileName1);
    $insert_image1 = add_images($fileName2,$cap1,$sectiontitle,$coursetitle);
    $insert_image2 = add_images($fileName3,$cap2,$sectiontitle,$coursetitle);
    $insert_image3 = add_images($fileName4,$cap3,$sectiontitle,$coursetitle);

    if($insert_section && $insert_image2 && $insert_image1 && $insert_image3 && $insert_course){
        header('Location: ../view/courses.php');
    }else{
        //echo failure
        echo "<div class='alert alert-danger'>
            <strong>Danger!</strong> error creating product.
            </div>";
        }
    }

elseif (isset($_POST["continue"])){
    $folderName = "../assets/images/";
    $fileName1 = $folderName . basename($_FILES["img1"]["name"]);
    $fileName2 = $folderName . basename($_FILES["img2"]["name"]);
    $fileName3 = $folderName . basename($_FILES["img3"]["name"]);
    $fileName4 = $folderName . basename($_FILES["img4"]["name"]);
    $cap1 = $_POST['cap1'];
    $cap2 = $_POST['cap2'];
    $cap3 = $_POST['cap3'];
    $desc = $_POST['desc'];

    $category = $_POST['category'];
```

Fig. 19 code implementing add course functionality

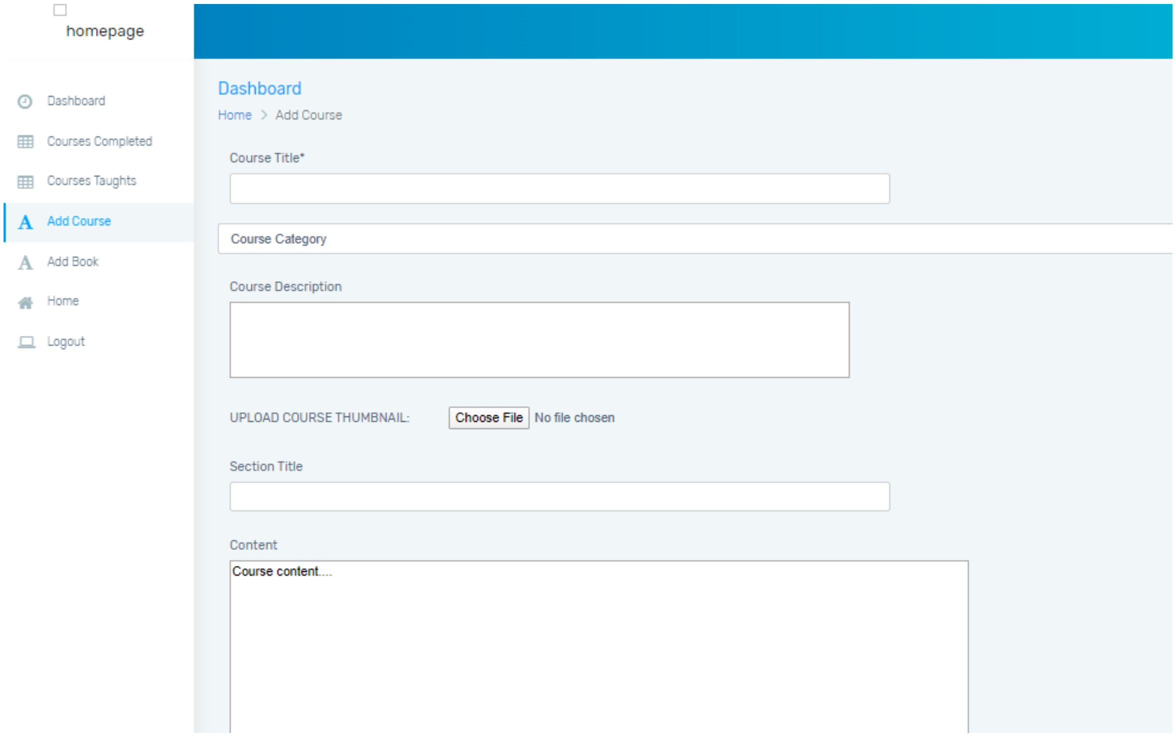
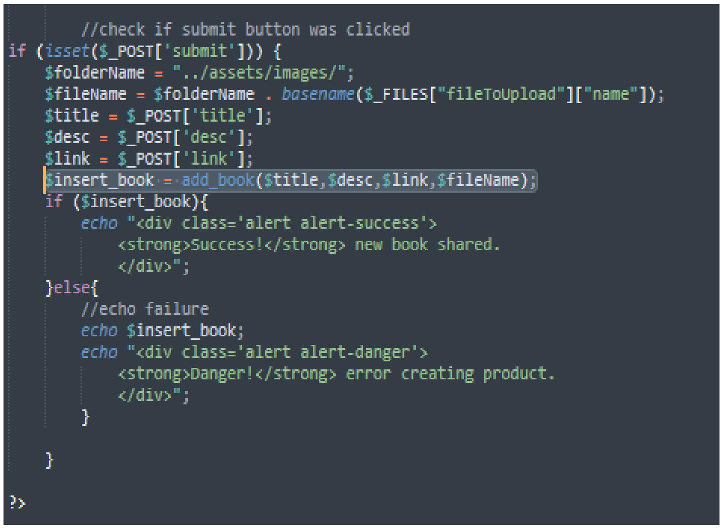


Fig 20. Add course webpage

Add Book: The add book section consisted of forms and text areas for inputs like text, images, links, etc. It calls on the book class to perform its functions.



```
        //check if submit button was clicked
if (isset($_POST['submit'])) {
    $folderName = "../assets/images/";
    $fileName = $folderName . basename($_FILES["fileToUpload"]["name"]);
    $title = $_POST['title'];
    $desc = $_POST['desc'];
    $link = $_POST['link'];
    $insert_book = add_book($title,$desc,$link,$fileName);
    if ($insert_book){
        echo "<div class='alert alert-success'>
            <strong>Success!</strong> new book shared.
            </div>";
    }else{
        //echo failure
        echo $insert_book;
        echo "<div class='alert alert-danger'>
            <strong>Danger!</strong> error creating product.
            </div>";
        }

    }

?>
```

Fig.21 code that implements the add book functionality

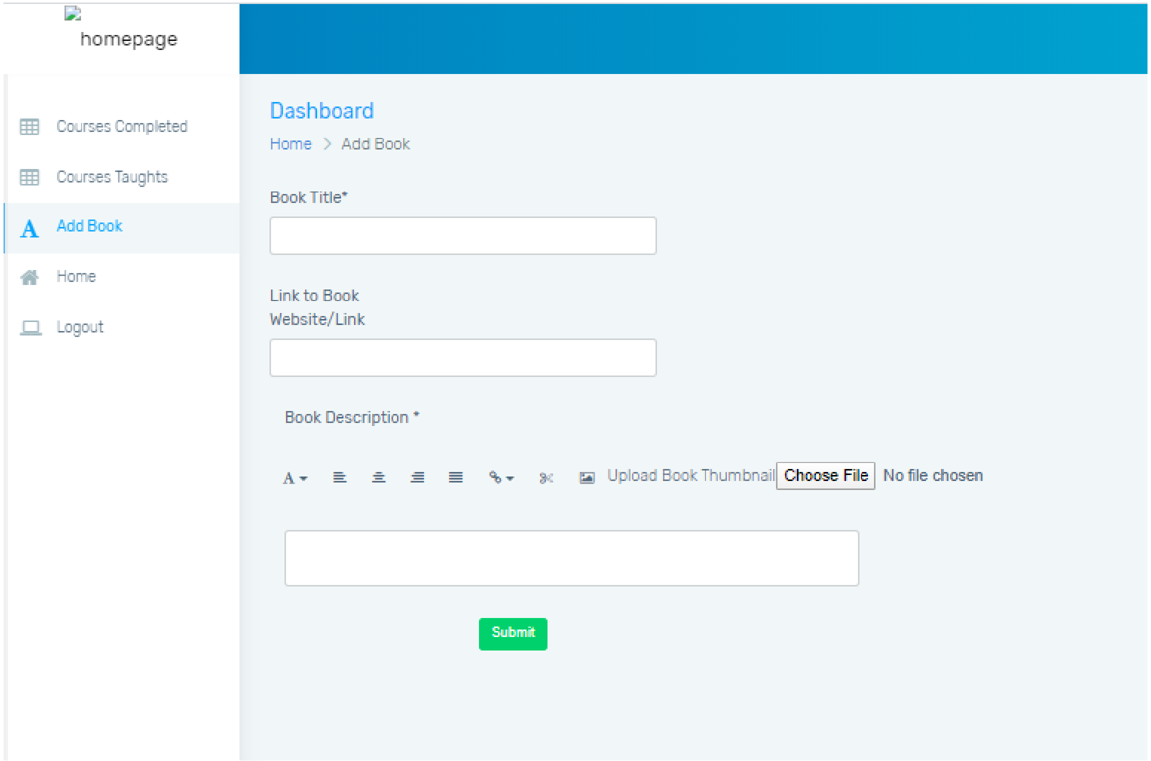
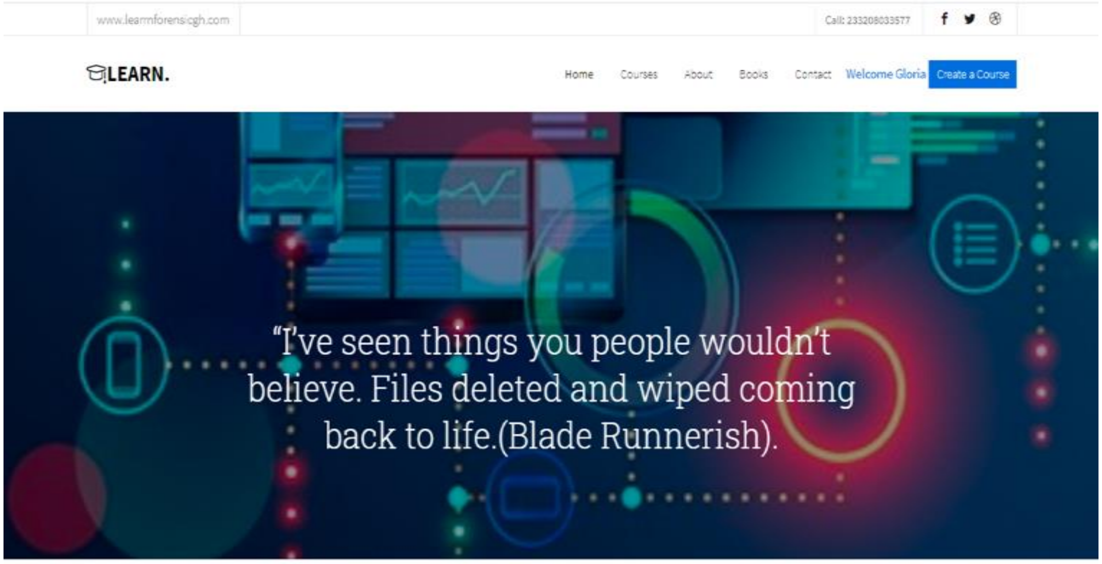


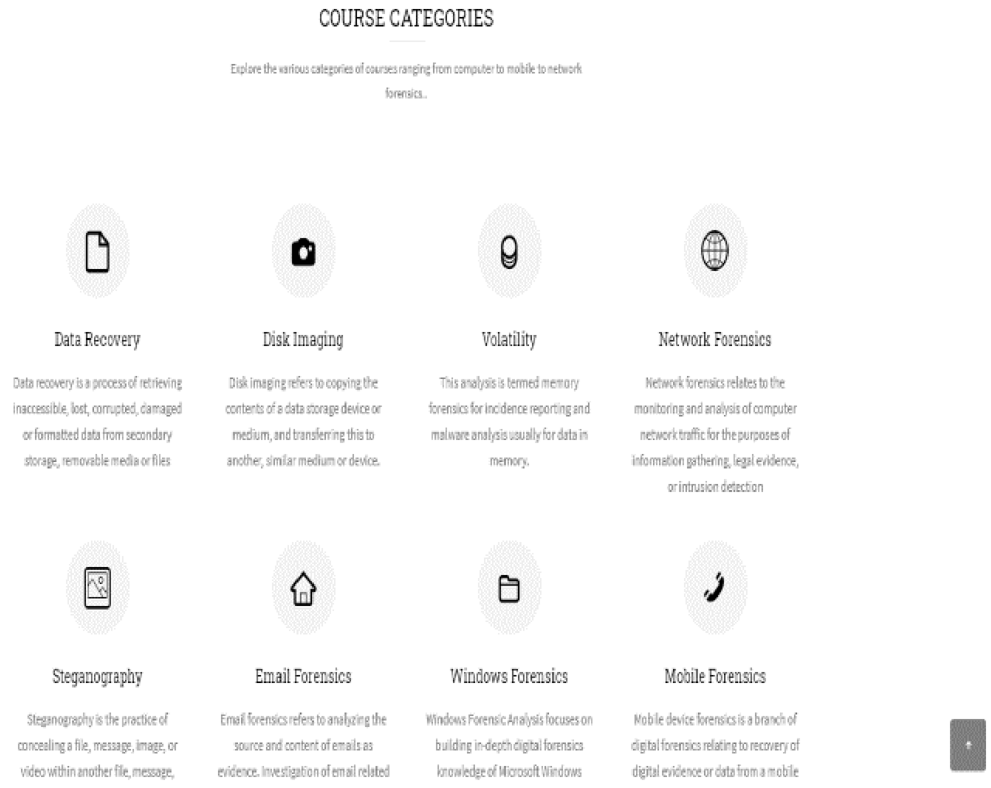
Fig.22 Add book webpage

Below are snapshots of the e-learning application used for the posttest experiment.



"I've seen things you people wouldn't believe. Files deleted and wiped coming back to life.(Blade Runnerish).

Fig.23 Homepage 1



COURSE CATEGORIES

Explore the various categories of courses ranging from computer to mobile to network forensics..

Data Recovery

Data recovery is a process of retrieving inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files

Disk Imaging

Disk imaging refers to copying the contents of a data storage device or medium, and transferring this to another, similar medium or device.

Volatility

This analysis is termed memory forensics for incidence reporting and malware analysis usually for data in memory.

Network Forensics

Network forensics relates to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message,

Email Forensics

Email forensics refers to analyzing the source and content of emails as evidence. Investigation of email related

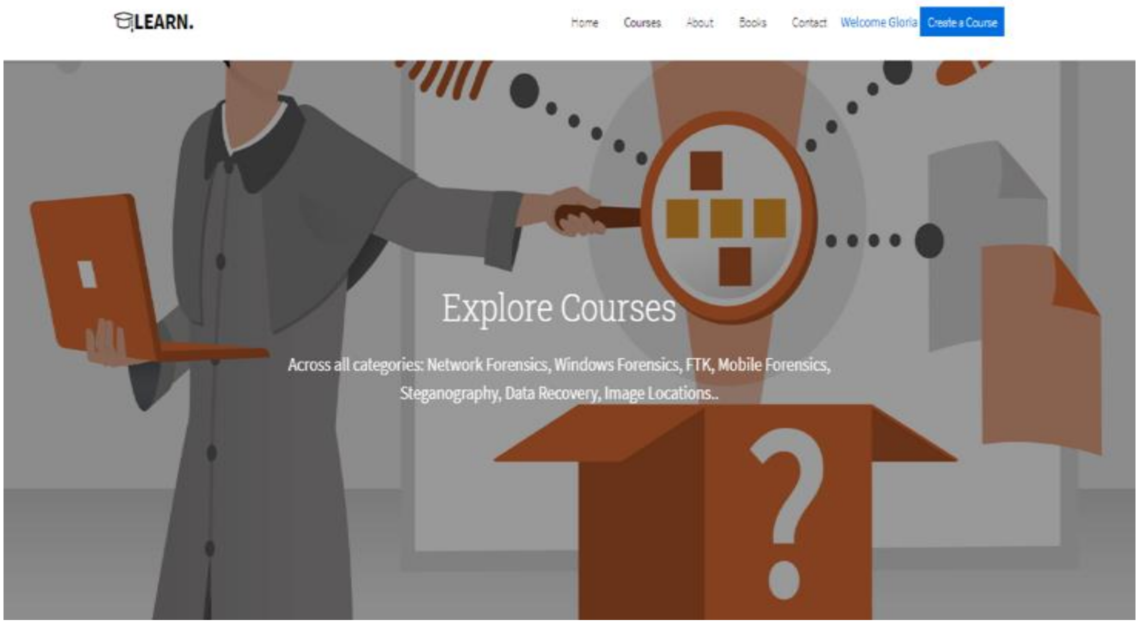
Windows Forensics

Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows

Mobile Forensics

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile

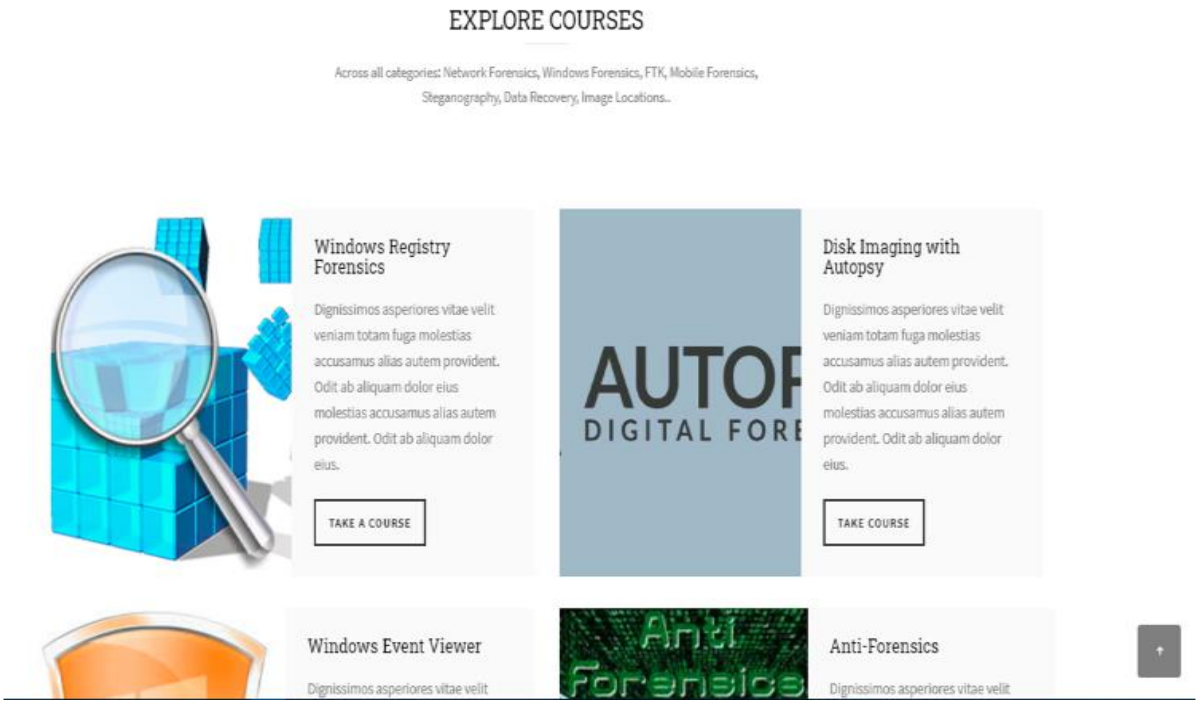
Fig.24 Homepage Extension



Explore Courses

Across all categories: Network Forensics, Windows Forensics, FTK, Mobile Forensics, Steganography, Data Recovery, Image Locations..

Fig.25 Course page



EXPLORE COURSES

Across all categories: Network Forensics, Windows Forensics, FTK, Mobile Forensics, Steganography, Data Recovery, Image Locations..

Windows Registry Forensics

Dignissimos asperiores vitae velit veniam totam fuga molestias accusamus alias autem provident. Odit ab aliquam dolor eius molestias accusamus alias autem provident. Odit ab aliquam dolor eius.

Disk Imaging with Autopsy

Dignissimos asperiores vitae velit veniam totam fuga molestias accusamus alias autem provident. Odit ab aliquam dolor eius molestias accusamus alias autem provident. Odit ab aliquam dolor eius.

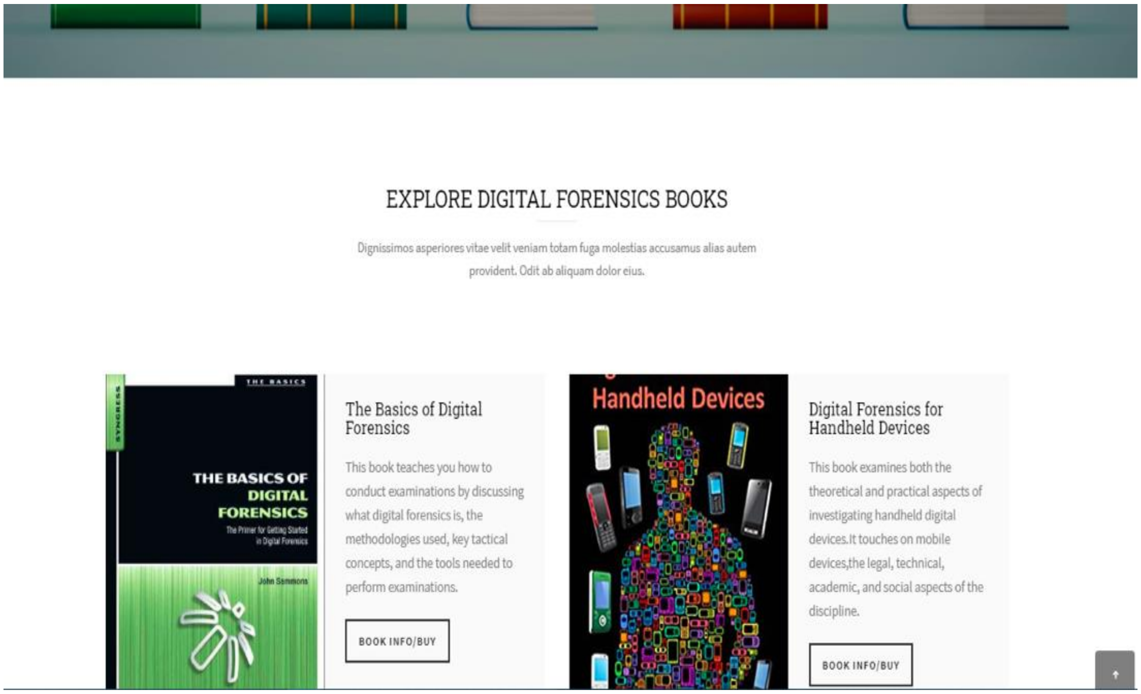
Windows Event Viewer

Dignissimos asperiores vitae velit

Anti-Forensics

Dignissimos asperiores vitae velit

Fig.26 Course page extension



EXPLORE DIGITAL FORENSICS BOOKS

Dignissimos asperiores vitae velit veniam totam fuga molestias accusamus alias autem provident. Odit ab aliquam dolor eius.

The Basics of Digital Forensics

This book teaches you how to conduct examinations by discussing what digital forensics is, the methodologies used, key tactical concepts, and the tools needed to perform examinations.

BOOK INFO/BUY

Digital Forensics for Handheld Devices

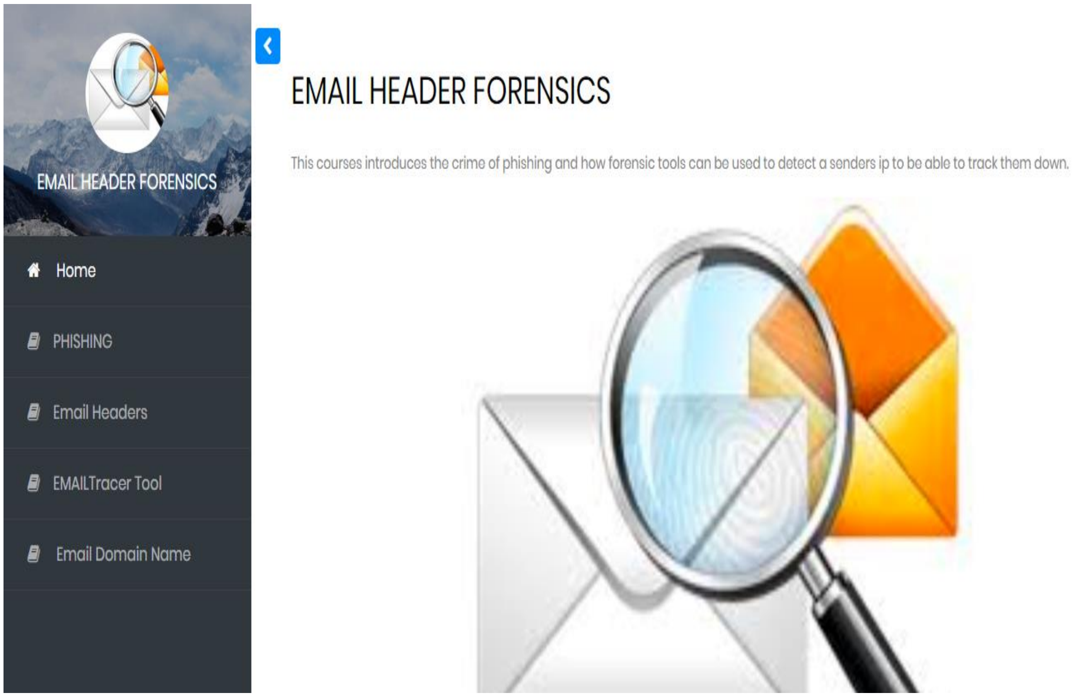
This book examines both the theoretical and practical aspects of investigating handheld digital devices.It touches on mobile devices,the legal, technical, academic, and social aspects of the discipline.

BOOK INFO/BUY

THE BASICS
THE BASICS OF DIGITAL FORENSICS
The Primer for Getting Started in Digital Forensics
John Sammons
SYNGRESS
Handheld Devices

Fig.27 Explore books page

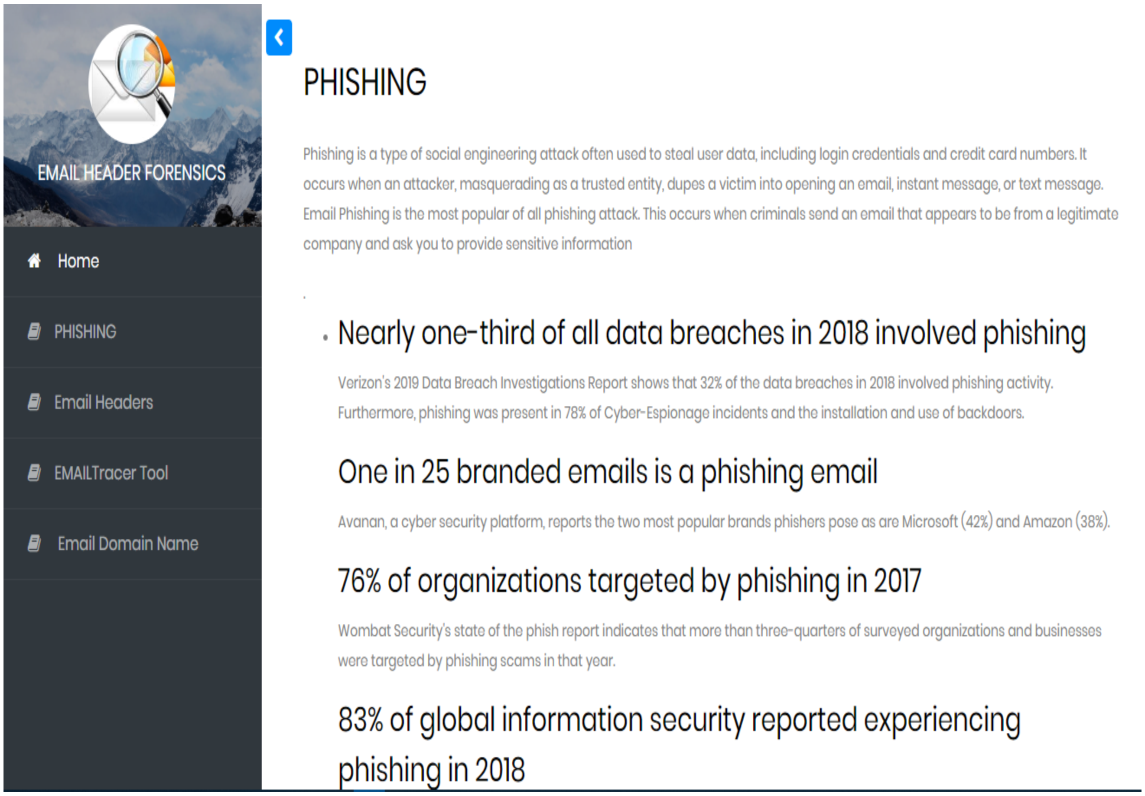
Below are the snapshots of course content for posttest experiment



EMAIL HEADER FORENSICS

This courses introduces the crime of phishing and how forensic tools can be used to detect a senders ip to be able to track them down.

Fig.28. Start page for a course(Email header forensics)



PHISHING

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. Email Phishing is the most popular of all phishing attack. This occurs when criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information

- Nearly one-third of all data breaches in 2018 involved phishing

Verizon's 2019 Data Breach Investigations Report shows that 32% of the data breaches in 2018 involved phishing activity. Furthermore, phishing was present in 78% of Cyber-Espionage incidents and the installation and use of backdoors.

One in 25 branded emails is a phishing email

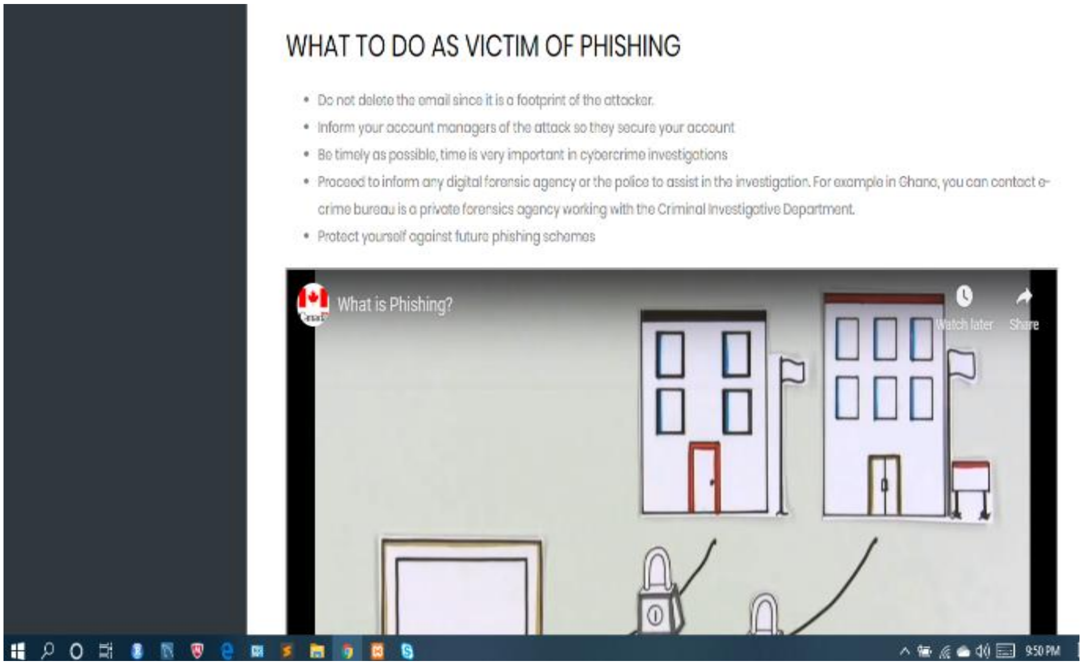
Avanan, a cyber security platform, reports the two most popular brands phishers pose as are Microsoft (42%) and Amazon (38%).

76% of organizations targeted by phishing in 2017

Wombat Security's state of the phish report indicates that more than three-quarters of surveyed organizations and businesses were targeted by phishing scams in that year.

83% of global information security reported experiencing phishing in 2018

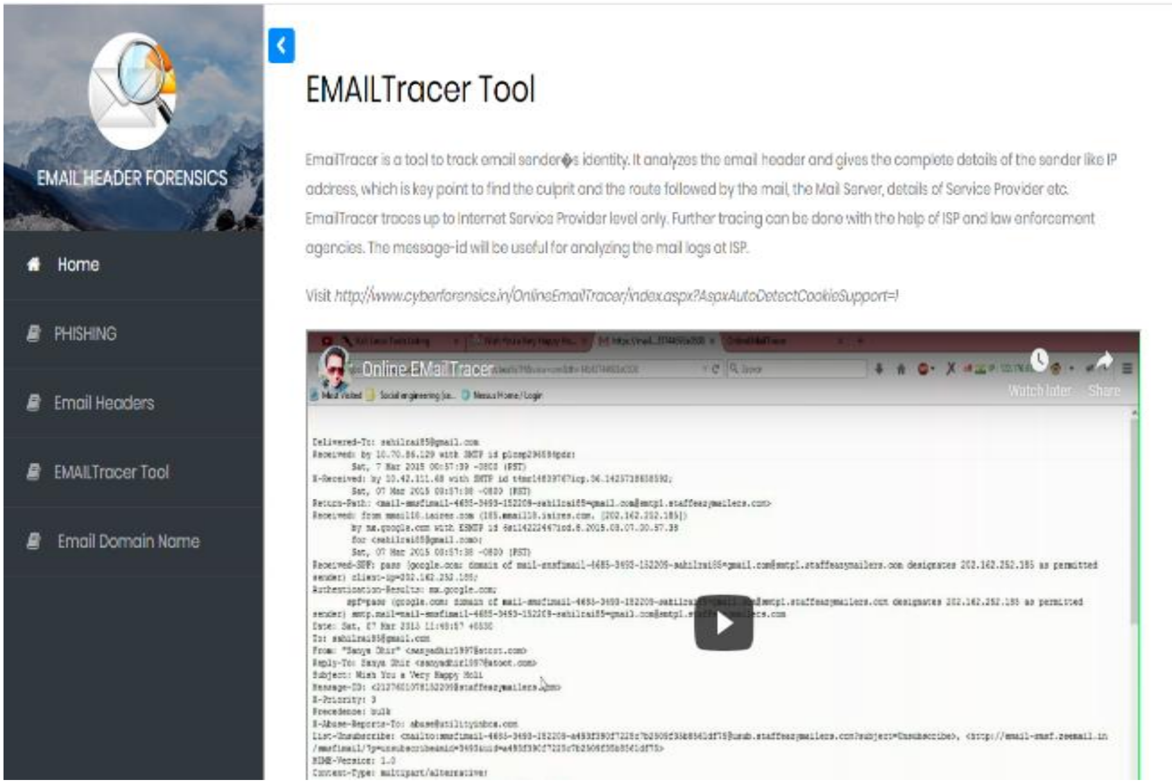
Fig.29 Course page with sections on left pane



WHAT TO DO AS VICTIM OF PHISHING

- Do not delete the email since it is a footprint of the attacker.
- Inform your account managers of the attack so they secure your account
- Be timely as possible, time is very important in cybercrime investigations
- Proceed to inform any digital forensic agency or the police to assist in the investigation. For example in Ghana, you can contact e-crime bureau is a private forensics agency working with the Criminal Investigative Department.
- Protect yourself against future phishing schemes

Fig.30 Course page with youtube plugin



EMAILTracer Tool

EmailTracer is a tool to track email sender�s identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.

Visit *http://www.cyberforensics.in/OnlineEmailTracer/index.aspx?AspxAutoDetectCookieSupport=1*

```
Delivered-To: sahilrai85@gmail.com
Received: by 10.70.86.129 with SMTP id p1csp296694pdz;
        Sat, 7 Mar 2015 00:57:39 -0800 (PST)
X-Received: by 10.42.111.68 with SMTP id t4mr14839767icp.56.1425718658592;
        Sat, 07 Mar 2015 00:57:38 -0800 (PST)
Return-Path: <mail-msfimail-4685-3493-152209-sahilrai85=gmail.com@smtp1.staffeasymailers.com>
Received: from mail18.iaires.com (185.mail18.iaires.com. [202.162.252.185])
        by mx.google.com with ESMTP id 6si14222447icd.6.2015.03.07.00.57.38
        for <sahilrai85@gmail.com>;
        Sat, 07 Mar 2015 00:57:38 -0800 (PST)
Received-SPF: pass (google.com: domain of mail-msfimail-4685-3493-152209-sahilrai85=gmail.com@smtp1.staffeasymailers.com designates 202.162.252.185 as permitted
sender) client-ip=202.162.252.185;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of mail-msfimail-4685-3493-152209-sahilrai[illegible]@smtp1.staffeasymailers.com designates 202.162.252.185 as permitted
sender) smtp.mail=mail-msfimail-4685-3493-152209-sahilrai85=gmail.com@smtp1.s[illegible]ers.com
Date: Sat, 07 Mar 2015 11:48:57 +0530
To: sahilrai85@gmail.com
From: "Sanya Dhir" <sanyadhir1997@atoot.com>
Reply-To: Sanya Dhir <sanyadhir1997@atoot.com>
Subject: Wish You a Very Happy Holi
Message-ID: <21274010781522090@staffeasymailers.com>
X-Priority: 3
Precedence: bulk
X-Abuse-Reports-To: abuse@utilityinbox.com
List-Unsubscribe: <mailto:msfimail-4685-3493-152209-a493f390f7225c7b2506f35b8561df75@unsub.staffeasymailers.com?subject=Unsubscribe>, <http://email-msf.zeemail.in
/msfimail/?p=unsubscribe&mid=3493&uid=a493f390f7225c7b2506f35b8561df75>
MIME-Version: 1.0
Content-Type: multipart/alternative;
```

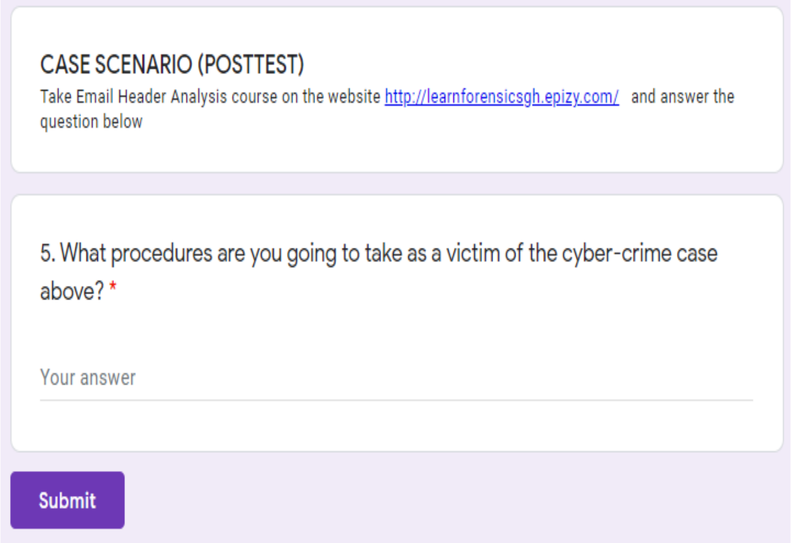
Fig.31 Course page with youtube plugin

4.5 Conducting Posttest Incidence Reporting Experiment and Cybercrime Investigation Experiment

The Posttest experiment involved the exposure of research applicants to a cyber e-learning application (http://learnforensicsgh.epizy.com/), and after, answer the same questions previously answered in the pretest experiment. The course explains email phishing, statistics over the years, characteristics, what to do as a victim of email phishing, email headers, and email tracking tool. It took 10-20mins for participants to complete the course and about 5mins to fill the questionnaires.

Posttest Questionnaires for Incidence Reporting Experiment

Below are posttest questionnaires administered to the victim category after taking the course on email phishing.



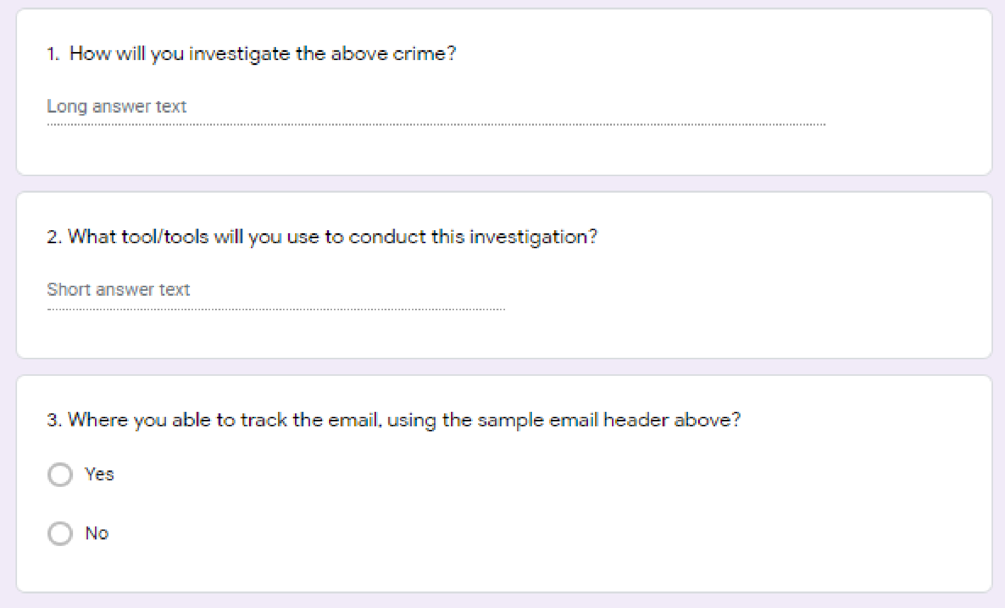
CASE SCENARIO (POSTTEST)

Take Email Header Analysis course on the website http://learnforensicsgh.epizy.com/ and answer the question below

5. What procedures are you going to take as a victim of the cyber-crime case above? *

Your answer

Fig 32. Posttest Questionnaires for Incidence Reporting Experiment



1. How will you investigate the above crime?

Long answer text

2. What tool/tools will you use to conduct this investigation?

Short answer text

3. Where you able to track the email, using the sample email header above?

○ Yes

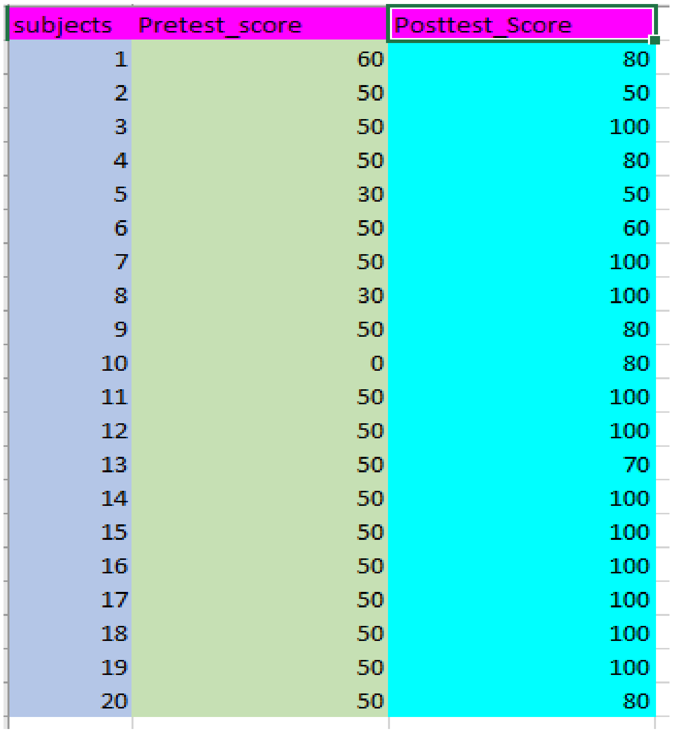
○ No

Fig 33. Posttest Questionnaires for Cybercrime Investigation Experiment

4.6 RESULTS AND ANALYSIS

4.6.1 Incidence Reporting Experiment

Below is a snapshot of the pretest and posttest scores of the 20 research participants involved in the incidence reporting experiment.



subjects	Pretest_score	Posttest_Score
1	60	80
2	50	50
3	50	100
4	50	80
5	30	50
6	50	60
7	50	100
8	30	100
9	50	80
10	0	80
11	50	100
12	50	100
13	50	70
14	50	100
15	50	100
16	50	100
17	50	100
18	50	100
19	50	100
20	50	80

Fig. 34 incidence reporting experiment scores

The boxplot below shows a significant difference in the means scores. The means score for the pretest experiment according to the boxplot below is 46 while that of the posttest experiment is 86.5, a difference of 40.5. This means that participants performed better when they were exposed to the e-learning application.

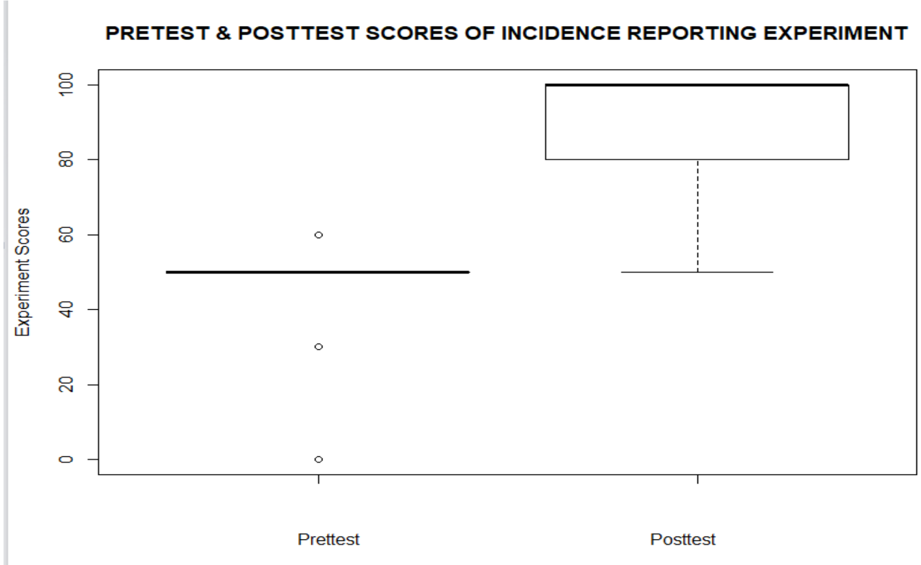


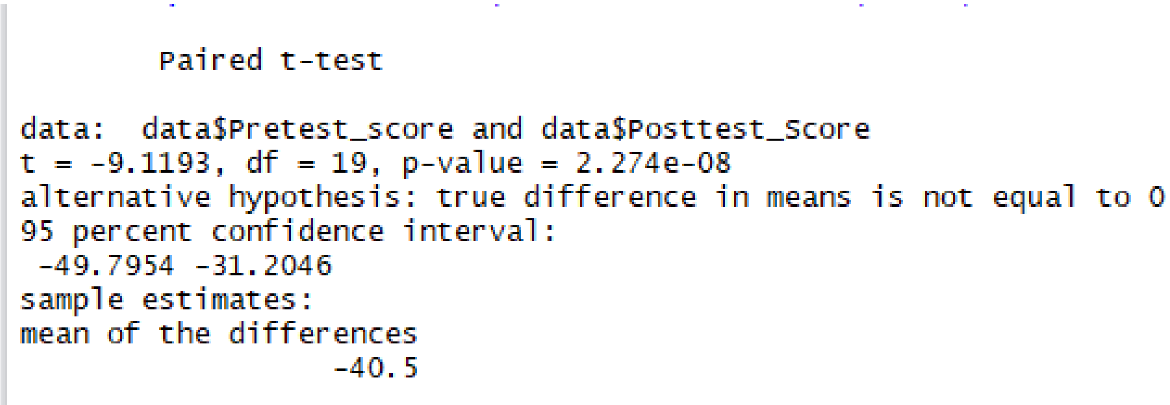
Fig 35. Boxplot for incidence report experiment scores

Paired Sample T-test

Paired Sample T-test analysis was used to analyze and measure the mean difference between the pretest results and the posttest results and understand the relationship between them. This was done under the alternative hypothesis that there exists some significant relationship between better incidence reporting and cybercrime prevention(*H1*). The null hypothesis is that, there is no significant relationship between better incidence reporting and cybercrime prevention (*Ho*). This can be illustrated statistically as.

- H0: µd = 0 (No significant difference/ impact of better incidence reporting on the prevention of cybercrime)
- H1: µd ≠ 0 (There is a significant impact of better incidence reporting on the prevention of cybercrime)

Below is a snapshot of the results from the paired t-test.



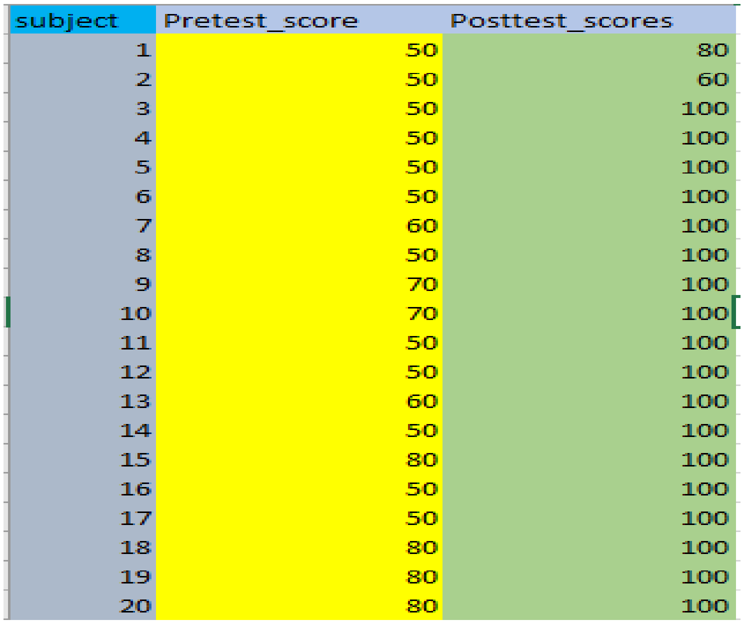
```
        Paired t-test

data:  data$Pretest_score and data$Posttest_Score
t = -9.1193, df = 19, p-value = 2.274e-08
alternative hypothesis: true difference in means is not equal to 0
95 percent confidence interval:
 -49.7954 -31.2046
sample estimates:
mean of the differences
                  -40.5
```

Fig 36. Paired sample t-test for incidence report experiment

The paired t-test showed a p-value of 2.274e-0.8 which is way lesser than the standard (0.05). This explains that there is a significant relationship between incidence reporting and cybercrime prevention. The paired t-testt was done on a 95% percent confidence level which suggests that results obtained from this experiment would match the results from the actual population 95 percent of the time. Not only is there a p-value lesser than 0.05 but also a significant mean difference of 40.5 between the pretest and posttest scores.

4.6.2 Cybercrime Investigation Experiment

Below is a snapshot of the pretest and posttest scores of the 20 research participants involved in the cybercrime investigation experiment.



subject	Pretest_score	Posttest_scores
1	50	80
2	50	60
3	50	100
4	50	100
5	50	100
6	50	100
7	60	100
8	50	100
9	70	100
10	70	100
11	50	100
12	50	100
13	60	100
14	50	100
15	80	100
16	50	100
17	50	100
18	80	100
19	80	100
20	80	100

Fig. 34 incidence reporting experiment scores

The boxplot below shows a significant difference in the means scores. The means score for the pretest experiment according to the boxplot below is 59 while that of the posttest experiment is 97, a difference of 38. This means that participants performed better investigations when they were exposed to the e-learning application.

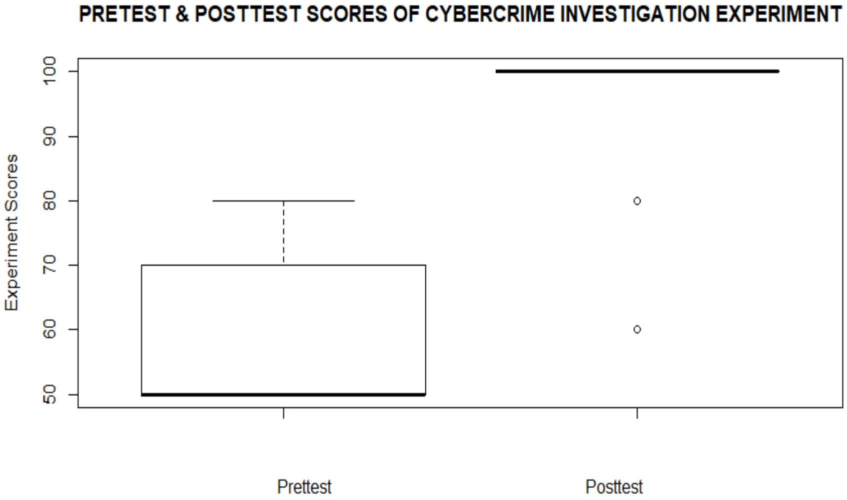


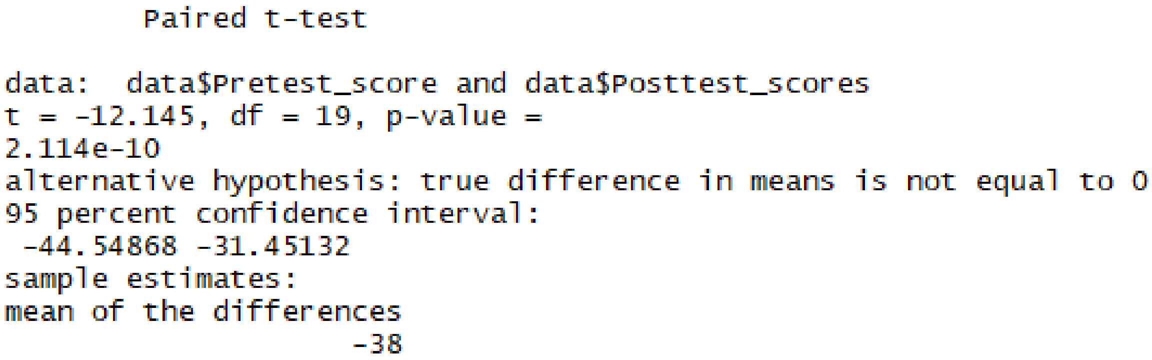
Fig 35. Boxplot for crime investigation experiment scores

Paired Sample T-test

Paired Sample T-test analysis was used to analyze and measure the mean difference between the pretest results and the posttest results and understand the relationship between them. This was done under the alternative hypothesis that there exists some significant relationship between better crime investigations and cybercrime prevention(*H1*). The null hypothesis being that, there is no significant relationship between better crime investigations and cybercrime prevention (*Ho*). This can be illustrated statistically as;

- H0: µd = 0 (No significant difference/ impact of better crime investigations g on the prevention of cybercrime)
- H1: µd ≠ 0 (There is a significant impact of better crime investigation on the prevention of cybercrime)

Below is a snapshot of the results from the paired t-test.



```
        Paired t-test

data:  data$Pretest_score and data$Posttest_scores
t = -12.145, df = 19, p-value =
2.114e-10
alternative hypothesis: true difference in means is not equal to 0
95 percent confidence interval:
 -44.54868 -31.45132
sample estimates:
mean of the differences
                    -38
```

Fig 36. Paired sample t-test for crime investigation experiment

The paired t-test showed a p-value of 2.114e-10 which is way lesser than the critical value (0.05). This explains that there is a significant relationship between better crime investigations and cybercrime prevention. The paired t-test was done on a 95% percent confidence level which suggests that results obtained from this experiment would match the results from the actual population 95 percent of the time. Not only is there a p-value lesser than 0.05 but also a significant mean difference of -38 between the pretest and posttest scores.

4.7 Conclusion

Participants performed better incidence reporting and criminal investigations on the email phishing scenario after they were exposed to the e-learning application. The average post-test scores of both incidence reporting and crime investigation experiments were higher than the average pretest scores. This explains that the awareness or teaching of incidence reporting and crime investigations to the general public and the police/information security personnel will help address the issue of cybercrime in Ghana.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Summary

The focus of this thesis was to investigate the impact of digital forensics on the prevention of cybercrime in Ghana. Digital forensics which involves cybercrime investigation and better incidence response is a field that has been adopted by a lot of advanced countries in investigating and incriminating cybercriminals [29]. The literature review on digital forensics in Ghana reported the lack of expertise in the area which has accounted for the increase of cybercrimes across the nation [16]. It also spelled out the lack of confidence in the Ghana Police and the Criminal Investigative Department when it comes to crime investigation which has led to victims not reporting cybercrimes at all [10].

A pretest-posttest experiment was conducted to access how the awareness of better cybercrime investigation and incidence reporting can help combat cybercrime. In response to the research question: "What is the impact of Digital forensics on cybercrime prevention?" and the results from the pretest-posttestt experiment, the following can be deduced.

- The awareness of incidence response procedures by individuals including victims, will promote better incidence response, and encourage crime reporting.
- The awareness of cybercrime investigation practices by security personnel including the Ghana police/Crime Investigation Department will encourage cybercrime investigations. This will help detect criminals which in turn will deter prospective cybercriminal activities.

From the study, security enthusiast participants were willing to conduct criminal investigations when they understood what crime they were investigating, and they achieved the desired results of tracking phishing emails to senders. Also, incidence reporting participants performed better incidence responses when they understood the cybercrime, digital footprint of the attacker, and the risk involved. This proves the hypothesis that better incidence response and crime investigation will help combat cybercrime in Ghana.

5.2 Limitations

There were a few limitations that were encountered during the research. The most notable limitation that was encountered during this research was the time constraint. This led to a small sample size of 40, 20 for the incidence reporting experiment and 20 for the cybercrime investigation experiment. Also, the experiment was only limited to an email attack and quite a lot of people in Ghana do not have email addresses, hence it makes it difficult to generalize the results of the experiment to suit the whole population.

5.3 Recommendation

This project has a lot of opportunities that can be explored. It presents an opportunity to look at an unexplored field in Ghana, and its impact on cybercrime prevention. In the future, other cybercrime investigative practices and incidence responses aside email phishing should be explored. Also, a large sample size that includes all classes of society including the educated and non-educated should be acknowledged in any similar research across this line.

APPENDIX

Pretest And Posttest Incidence Reporting Experiment

Case Scenario -Phishing Email

Dear,

We emailed you earlier to ask for your help resolving an issue with your paypal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, login to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always available to help.

Thank you for being a PayPal Customer.

Sincerely,

PayPal.

*You clicked the link and you were asked to login with your bank account details. After two hours, you received a notification from PayPal saying your account has been debited by $10,000 dollars.

PRETEST QUESTIONNAIRES

1. Have you ever been a victim of any cybercrime (eg. email phishing, mobile money fraud etc.)?

a. Yes
b. No(If No move to question 5)

2. IF YES, Did you take any actions of any sort?

a. Yes
b. No (If No move to question 3)

3. Why didn't you take any action?

…..4. Would you have taken any action if you knew what to do, what not to do and the right people to inform?

a. Yes
b. No
c. Other:

5. What procedures are you going to take as a victim of the cyber-crime case above?

…..

POSTTEST QUESTIONNAIRES

Take Email Header Analysis course on the website http://learnforensicsgh.epizy.com/ and answer the question below

5. What procedures are you going to take as a victim of the cyber-crime case above?

…..

PRETEST AND POSTTEST CYBCER-CRIME INVESTIGATION EXPERIMENT

*Case Scenario **Email Phishing***

Dear,

We emailed you earlier to ask for your help resolving an issue with your paypal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, login to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always available to help.

Thank you for being a PayPal Customer.

Sincerely,

PayPal.

**He clicked the link and you were asked to login with your bank account details. After two hours, you received a notification from PayPal saying your account has been debited by $10,000 dollars.*

PRETTEST QUESTIONNAIRES

1. Are you an enthusiast of computer/information security?

   a. Yes
   b. No
   c. Maybe

2. How will you investigate the above crime?

…..

3. What tool/tools will you use to conduct this investigation?

…..

POSTTEST QUESTIONNAIRES

Take Email Header course on the website http://learnforensicsgh.epizy.com/ and answer the questions below.

Below is a sample Email Header for Question 3 BELOW

(Sample Header)

1. How will you investigate the above crime?

…..

2. What tool/tools will you use to conduct this investigation?

…..

3. Where you able to track the email, using the sample email header above?

a. Yes
b. No

REFERENCES

[1]Michael AdjeiFrempong and Kamal Hiran. 2014. Awareness and Understanding of Computer Forensics in the Ghana Legal System. *Int. J. Comput. Appl.* 89, (February 2014). DOI:https://doi.org/10.5120/15752-4640

[2]Godwin Akweiteh Allotey. 2018. Ghana loses $230m to cyber criminals – CID. *Citinewsroom - Comprehensive News in Ghana, Current Affairs, Business News , Headlines, Ghana Sports, Entertainment, Politics,*. Retrieved October 5, 2019 from https://citinewsroom.com/2018/10/ghana-loses-230m-to-cyber-criminals-cid/

[3]Aaron Amankwaa. 2016. History of forensic science in Ghana-overview. *Sci. E-Mag* 1, (February 2016), A1.

[4]Albert Antwi-Boasiako. 2017. Criminal Justice Statistics on Cybercrime & Electronic Evidence. (2017), 16.

[5]Richard D. Austin. 2007. Digital forensics on the cheap: teaching forensics using open source tools. In *Proceedings of the 4th annual conference on Information security curriculum development - InfoSecCD '07*, 1. DOI:https://doi.org/10.1145/1409908.1409915

[6]Caroline Baylon and Albert Antwi-Boasiako. 2016. Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study. *Global Commission on Internet Governance*.

[7]Richard Boateng, Olumide Longe, Victor Mbarika, Innocent Avevor, and Stephen Isabalija. 2010. Cyber Crime and Criminality in Ghana: Its Forms and Implications. *J. Inf. Technol. Impact* 11, (January 2010), 85–100.

[8]CID. 2019. Criminal Inestigation Department – Ghana Police Service. Retrieved October 21, 2019 from https://police.gov.gh/en/index.php/criminal-investigation-department-cid/

[9]Tom Douglas, Douglas Thomas, and Brian Loader. 2000. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.

[10]D. Ennin. 2015. Cybercrime in Ghana A Study of Offenders, Victims and the Law. University of Ghana. Retrieved October 21, 2019 from http://ugspace.ug.edu.gh/handle/123456789/8908

[11]Simson L. Garfinkel. 2013. Digital Forensics. *Am. Sci.* 101, 5 (2013), 370–377.

[12]Alhassan Mohammed and Alexander Adjei-Quaye. 2017. Computer & Cyber Forensics: A Case Study of Ghana. Retrieved October 6, 2019 from https://www.researchgate.net/publication/314086053_Computer_Cyber_Forensics_A_Case_Study_of_Ghana

[13]Gary Palmer. 2002. Forensic Analysis in the Digital World. *Int. J. Digit. Evid.* (2002). Retrieved October 21, 2019 from /paper/Forensic-Analysis-in-the-Digital-World-Palmer/5f3f1a95a38d251ef798eb6bc4f5626c27805762

[14] Ghana Police Service: 2013 Annual Report.

[15]Laoise Luciano, Ibrahim Baggili, Mateusz Topor, Peter Casey, and Frank Breitinger. 2018. Digital Forensics in the Next Five Years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, 1–14. DOI:https://doi.org/10.1145/3230833.3232813

[16]Alhassan Mohammed and Alexander Adjei-Quaye. 2017. Computer & Cyber Forensics: A Case Study of Ghana. Retrieved October 6, 2019 from

https://www.researchgate.net/publication/314086053_Computer_Cyber_Forensics_A_Case_Study_of_Ghana

[17] Andrea Monti. 2017. Rules of (digital) evidence and prosecution's actual needs. When the law falls behind technology. *ResearchGate* (2017). Retrieved November 1, 2019 from https://www.researchgate.net/publication/334224769_Rules_of_digital_evidence_and_prosecution's_actual_needs_When_the_law_falls_behind_technology

[18] Yin Pan, Sumita Mishra, Bo Yuan, Bill Stackpole, and David Schwartz. 2012. Game-based forensics course for first year students. In *Proceedings of the 13th annual conference on Information technology education - SIGITE '12*, 13. DOI:https://doi.org/10.1145/2380552.2380558

[19] Mark Pollitt. 2010. A History of Digital Forensics. In *Advances in Digital Forensics VI* (IFIP Advances in Information and Communication Technology), 3–15. DOI:https://doi.org/10.1007/978-3-642-15506-2_1

[20] Mark Scanlon, Xiaoyu Du, and David Lillis. 2017. EviPlant: An efficient digital forensic challenge creation, manipulation and distribution solution. *Digit. Investig.* 20, (March 2017), S29–S36. DOI:https://doi.org/10.1016/j.diin.2017.01.010

[21] Noesgaard Signe Schack and Ørngreen Rikke. 2015. The Effectiveness of E-Learning: An Explorative and Integrative Review of the Definitions,... *issuu* (2015). Retrieved October 6, 2019 from https://issuu.com/academic-conferences.org/docs/ejel-volume13-issue4-article438/1

[22] Victor G. Williams and Ken Revels. 2006. *Computer Forensics: Is It the Next Hot IT Subject?* Association of Small Computer Users in Education (ASCUE), 1513 Magnolia Drive, Surfside Beach, SC 29574. Retrieved October 31, 2019 from https://eric.ed.gov/?id=ED490169

[23] A. Yasinsac, R.F. Erbacher, D.G. Marks, M.M. Pollitt, and P.M. Sommer. 2003. Computer forensics education. *IEEE Secur. Priv.* 1, 4 (July 2003), 15–23. DOI:https://doi.org/10.1109/MSECP.2003.1219052

[24] Michael AdjeiFrempong and Kamal Hiran. 2014. Awareness and Understanding of Computer Forensics in the Ghana Legal System. *Int. J. Comput. Appl.* 89, (February 2014). DOI:https://doi.org/10.5120/15752-4640

[25] Aaron Amankwaa. 2016. History of forensic science in Ghana-overview. *Sci. E-Mag* 1, (February 2016), A1.

[26] Richard D. Austin. 2007. Digital forensics on the cheap: teaching forensics using open source tools. In *Proceedings of the 4th annual conference on Information security curriculum development - InfoSecCD '07*, 1. DOI:https://doi.org/10.1145/1409908.1409915

[27] Luca Caviglione, Steffen Wendzel, and Wojciech Mazurczyk. 2017. The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Secur. Priv.* 15, 6 (November 2017), 12–17. DOI:https://doi.org/10.1109/MSP.2017.4251117

[28] Arafeen Dr. Qamar, Arifeen Najam, and Ahmed Shamim. 2016. DIGITAL FORENSICS EDUCATION IN PAKISTAN -A NEW WAY TO UNDERSTAND THE DIGITAL WORLD. (2016). Retrieved October 31, 2019 from https://www.academia.edu/25378983/DIGITAL_FORENSICS_EDUCATION_IN_PAKISTAN_-A_NEW_WAY_TO_UNDERSTAND_THE_DIGITAL_WORLD

[29]Pande Dr.Jeetendra and Prasad Dr. Ajay. 2016. *Digital Forensics*. Uttarakhand Open University, Haldwani. Retrieved October 31, 2019 from https://www.researchgate.net/publication/300474145_Digital_Forensics

[30]Samir Abou El-Seoud, Islam A. T. F. Taj-Eddin, Naglaa Seddiek, Mahmoud M. El-Khouly, and Ann Nosseir. 2014. E-Learning and Students' Motivation: A Research Study on the Effect of E-Learning on Higher Education. *iJET* 9, (2014), 20–26. DOI:https://doi.org/10.3991/ijet.v9i4.3465

[31]D. Ennin. 2015. Cybercrime in Ghana A Study of Offenders, Victims and the Law. University of Ghana. Retrieved October 21, 2019 from http://ugspace.ug.edu.gh/handle/123456789/8908

[32]Kenneth Fee. 2009. *Delivering E-Learning: A Complete Strategy for Design Application and Assessment*. Kogan Page Publishers.

[33]Isabella Franco. 2019. 7 Countries with the Best Forensic Technology. *INTROVERT*. Retrieved October 31, 2019 from http://introvertedit.com/2019/07/29/best-forensic-technology/

[34]Beatrice Ghirardini, Food and Agriculture Organization of the United Nations, Germany, and Landwirtschaft und Verbraucherschutz Bundesministerium für Ernährung. 2011. *E-learning methodologies: a guide for designing and developing e-learning courses*. Retrieved October 6, 2019 from http://www.fao.org/docrep/015/i2516e/i2516e.pdf

[35]Jason Jordaan and Karen Bradshaw. 2015. The current state of digital forensic practitioners in South Africa. In *2015 Information Security for South Africa (ISSA)*, 1–9. DOI:https://doi.org/10.1109/ISSA.2015.7335068

[36]Noah Kasraie and Esrafill Kasraie. 2010. Economies of eLearning in the 21st Century. *Contemp. Issues Educ. Res.* 3, 10 (October 2010), 57–62.

[37]G. C. Kessler. 2007. Online Education in Computer and Digital Forensics: A Case Study. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 264a–264a. DOI:https://doi.org/10.1109/HICSS.2007.407

[38]Godfred Annum. 2019. RESEARCH INSTRUMENTS FOR DATA COLLECTION (Updated). (2019). Retrieved November 6, 2019 from https://www.academia.edu/36865594/RESEARCH_INSTRUMENTS_FOR_DATA_COLLECTION_Updated_

[39]Peter Bonate. 2000. *Analysis of Pretest- Posttest Design*. Chapman & Hall/CRC.

[40]Fidelis Ifeanyi Ugwuowo. 2016. *Fundamentals of research methodology and data collection*. LAP Lambert Academic Publishing. Retrieved November 16, 2019 from https://www.researchgate.net/publication/303381524_Fundamentals_of_research_methodology_and_data_collection

[41] Crabtree Benjamin and Miller William. 1992. Doing qualitative research: multiple strategies. Thousand Oaks, CA: Sage Publications