8-2022

The Future of Digital Forensics, A Gamified Approach for Education.

CHUKWUEMEKA IHEKWEAZU

The Future of Digital Forensics: A Gamified Approach for Education.

by

Chukwuemeka Ihekweazu

A Thesis Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

August, 2022

Thesis Paper Committee:
Abdullah Abu Hussein, Chairperson
Akalanka Bandara Maliewa
Kasi Balasubramanian

Abstract

Digital Forensics is a 21st-century emerging field that has taken more roots than ever before in the field of information security. The growth of digital forensics can be attributed to the need for expert digital forensics analysts to respond to the increased cybercrimes currently pillaging through the Internet and its environs. Without a doubt, the field of digital forensics is by far more complex. It requires extensive knowledge of new trends and legacy systems and the extensive use of specialized tools tailored in securing convictions through properly acquired evidence that can be used in a courtroom or thereof. Due to the numerous demands of individuals in the field, it is quite shocking that the number of experts is low hence a considerable backlog of cases in law enforcement. This study's abstract is to tentatively study and meticulously understand the many reasons for the decline in the growth of Digital Forensics and Cyber Security experts in the field. The project will also provide a method to combat this problem through a gamified approach targeting high school students with the sole benefit of creating awareness about this technical field from a young age to probably foster new ideologies and critical thinkers that would see a rise in the number of experts in this field as a result of keen interest and not just for a means to ensure basic needs are met. Also, to achieve this goal, this project will provide students with an awareness of what Digital Forensics is all about at that early stage in their lives through a gaming tool that will be interactive and fun.

Table of Contents

Page

Chapter Page

Chapter Page

List of Figures

Figure Page

Figure Page

List of Tables

Chapter I: Introduction

Introduction

Digital Forensics is a continuously growing area as a proportional result of the current growth in cyber-crimes. Digital Forensics is the study of binding digital signatures or trails of electronic breadcrumbs that provide speculation or hypothesis evidence.

Digital Forensics as a tool is a branch of forensic science involved with the acquisition, preservation, identification, extraction, and documentation of digital evidence that could be used within the scope of a jurisdiction (Nelson et al., 2014). Digital Forensics and cybercrimes as professions are quite challenging and cumbersome in the number of tasks meted out for a forensics investigator. The job entails data recovery of sensitive data used in a legal case and training on evidence gathering mechanisms. The profession requires detailed reporting of evidence handling and maintaining a chain of custody to prevent evidence tampering and jeopardize a legal case's possible outcomes. According to Forensics Colleges (2020), the career path involving Digital Forensics is quite bright and would require more specialists to know how the information analyst field works.

Training, what is the training involved in the path to being a digital forensics expert? As a prospective or an established digital forensics investigator, one must have completed hours of training and re-training to access one skillset. Several organizations have already developed modules to run training and testing. Training is usually quite

useful as these companies also offer certifications to a digital forensics expert who has met the expected criteria for such certifications to be awarded. These certifications are usually not easy to get as some could require years of experience or months of career growth in a similar field. Some of these certifications also require a minimum of 40 hours and five completed well-documented forensics investigations. Furthermore, could go up to 80 hours and 20 completed well-documented forensics investigations for some advanced level. Some of the companies that offer these certifications include;

Table 1

Certifications and their costs (Nelson et al., 2014)

Certifications	Certification Body	Educational Requirements	Applicable Fees	Experience Requirements
Certified Information System Security Profession (C.I.S.S.P.)	International Information System Security Certification Consortium (ISC^2)	College degree	$700	1 – 3 years

Table 1 (continued)

Certified Cyber Forensics Professional (C.C.F.P.)	International Information System Security Certification Consortium (ISC^2)	College degree	$550	2 – 5 years
Certified Digital Forensics Examiner (C.D.F.E.).	National Initiative for Cybersecurity Careers and Studies (N.I.C.C.S.)	College degree	$400	2 – 5 years
Global Certified Forensic Analyst (G.C.F.A.).	Global Information Assurance Certification (G.I.A.C.)	College degree	$1050	1 – 5 years

Table 1 (continued)

Certified Computer Examiner (C.C.E.).	International Society of Forensic Computer Examiners (I.S.F.C.E.)	College degree	$400	1 – 2 years
Certified Forensics Computer Examiner (C.F.C.E.)	International Association of Computer Investigative Specialists (I.A.C.I.S.)	College degree	$2,995	3 – 5 years
EnCase Certified Examiner (EnCE)	EnCase Certified Examiner Certification (EnCEC)	College degree	$300	1 – 2 years

According to the U.S. Department of Labor (Statistics, 2020), Studies that shows several investigators with adequate education did not initially study computer science or cybersecurity but instead studied courses like Master of Business of Administration

(M.B.A.) in information systems and other business or computer-related courses. This means that not all investigators started from the core basics of learning digital forensics concepts from a very early stage.

Now, with the broad explanation of what digital forensics as a career entail, there are still some foundational requirements needed for a career in cyber forensics. According to the U.S. Bureau of Statistics (Labor Statistics, 2020) and Criminal Justice Degree Schools, one has to know the basics of Mathematics and Computer science (Hardware and Software) as well as having a High School Diploma and a college degree in a related field. This is quite necessary as the experience is both personally rewarding and professionally preparatory for students who wish to consider a career in digital forensics and cybercrimes.

Error! Reference source not found. shows information security analyst salary compared to other computer-related fields according to (cite). We notice that the salary remained higher than the other positions for the last three years.

Table 2

Job titles and their respective salary range (Bureau of Labor & Statistics, 2019)

	Job Title	Salary
	Information Security Analyst	$98,350
	Computer Science occupations	$86,320
	Total, Occupations	$38,640

Table 3

2018 Survey of other related fields (Bureau of Labor & Statistics, 2019)

Computer Systems design and related services	$102,620
Finance and insurance	$101,130
Information	$96,580
Management of companies and enterprises	$94,180
Administrative and support services	$94,120

Without a doubt, there is a shortage of experts in the field and, as such, is both one of the highest paying jobs in the I.T. sector and the least sort after career path. There are many reasons for this analysis, and eventually, one would break it down into key areas. However, first, Digital Forensics and Cyber Security are broad areas that require hours of attention to detail, little room for errors, and in-depth knowledge of numerous legacy systems. All these can be quite tough and scary for an indecisive mindset to consider as a career path. So, for that reason, you must ask yourself, WHY this career?

Below are some of the reasons why there are a lack of expertise in this area

1. Affordability: Due to the need for certifications, which are usually expensive and are usually paid for by companies for their employees, it is safe to assume that most individuals would instead choose a less expensive career path that does not involve graphics and text-based technical modules.

2. Self-Sufficiency: The field of digital forensics does require the least bit of experience to grasp the full knowledge of what it is all about. The field does not take anything for granted and encourages self-learning as there is a need for daily improvement due to the new ways cyber-crime occurs. As such, coming into this field requires full dedication and possible overtime in working hours due to the nature of its urgency.
3. Exhaustive: Cyber Security, Digital Forensics, Penetration Testing, Network Intrusion, Legacy systems, Virtual Machines. These are some of the areas an expert in the field is expected to be knowledgeable on. This is because attacks and crimes can occur on a network with an operating system of Windows 98, carried out in a cisco environment. As such, one must come into this field to be versatile.
4. Perception: In all fairness, the way digital forensics is being perceived is also a huge reason why there is a lack of expertise in this field. Here is why it is often viewed as challenging, complex, and often compared to its counterpart, Medical Forensics. Other times, due to the way it is portrayed in movies as this cool job, in reality, it is not all fun and games. It does require dedication and in-depth knowledge of the law to the core.
5. Current Approaches: The current delivery methods of educating individuals on Digital Forensics are perceived to be quite disinteresting and, as such, are not received with the right amount of enthusiasm. For that reason, what is the point of venturing into something that is not creating a massive buzz in society

compared to careers in Medicine, Aerospace, Digital Media, or Financial Marketing?

Problem Statement

It is without a doubt, statistically, that there is a severe shortage of experts in the field of Digital Forensics and Cybercrimes. Studies Have shown that the number of investigations that require a digital forensics expert result in a substantial digital evidence backlog that is being experienced by law enforcement agencies around the world, including the U.S.A. The number of cases that require Digital forensics is more than likely to rise as most high-profile crimes are going digital and have much more adverse effects than the average novel crimes. In 2017, the U.S. Department of Justice announced a cyber task force to investigate complex crimes in cyberspace. In addition to this, the current techniques of educating digital forensics are unexciting. As such, there will be little interest in venturing into a career that is perceived in the comparison of both being legally inclined and medically affiliated. Hence the reason why the approach to study this career path needs to be reformed and, in the case of this study, be made aware of K-12 age grade or middle and high school grade at that early stage. Also, due to the expensive nature of the certifications required to be a specialist, many people often opt out as it is mostly deemed unworthy. The hours involved in study time are also quite lasting.

Sub-Problem

Due to the severe shortage of experts, the current approaches to solving this problem are less attractive. Hence, we want to introduce the K-12 students to the

concept of forensics using a gamified approach to keep it relatively concise and challenging enough to be accepted. We will need a modified Technology Acceptance model that fits into these age groups to make them aware of this career path early enough and make it quite interesting to them for a more extended period than most existing current educational approaches. This problem's essential aim is to ensure the dwindling curve on expertise is not flattened out eventually and replaced by relatively similar programs like Cybersecurity and Ethical Hacking.

Nature and Significance of the Problem

The nature of the problem addresses the fact that there is a significantly low amount of Digital and cyber forensics currently available globally and in the U.S.A. There is a need to develop tools that relate to forensics investigations that would best be suited for developing young minds, hence the introduction of digital forensics to k-12 students.

Table 4

States with the highest employment level in Digital Forensics (Bureau of Labor & Statistics, 2019)

STATE	EMPLOYMENT	EMPLOYMENT PER THOUSAND JOBS	LOCATION QUOTIENT	HOURLY MEAN WAGE	ANNUAL MEAN WAGE

Table 4 (continued)

California	2,150	0.12	1.10	$41.92	$87,000
Florida	1,680	0.19	1.70	$26.20	$54,490
Texas	1,480	0.12	1.06	$28.87	$60,040
New York	860	0.09	0.80	$32.69	$68,000
Arizona	700	0.24	2.17	$29.72	$61,820

Table 5

States with the highest concentration of jobs and locations quotients in this occupation (May 2019) (Bureau of Labor & Statistics, 2019)

States	Employment	Employment per thousand jobs	Location quotient	Hourly mean wage	Annual mean wage
New Mexico	240	0.29	2.58	$20.85	$43,370
Kansas	400	0.29	2.54	$24.26	$50,460
Nevada	380	0.27	2.43	$30.80	$64,070
Arizona	700	0.24	2.17	$29.72	$61,820
Florida	1000	0.19	1.70	$26.20	$54,490

Table 5 (continued)

State	Employment	Employment per thousand Jobs	Location Quotient	Hourly mean wage	Annual mean wage
California	2,150	0.12	1.10	$41.92	$87,200
Illinois	410	0.07	0.60	$39.49	$82,130
Massachusetts	80	0.02	0.21	$37.00	$76,950
Alaska	50	0.16	1.43	$34.80	$72,380
Virginia	440	0.11	1.02	$33.30	$69,260

Objective of the Study

The objective of this study is to address all the significant problems detailed out earlier in the subtopics. One of which is to make this domain/career path interesting to students in the K-12 because we want to target them at this age so that when they go to college, we want them to be interested in doing cybersecurity and digital forensics and not spend a significant amount of money doing a Dual-Major in college.

We also want citizens and individuals of a region or area to be made aware of their rights, understand how and act if they see, hear, or experience a digital or cyber-crime such as cyberstalking and kidnapping. We want to create more awareness of the modes in which cybercrimes can be committed and how these cyber criminals operate on a primary and eventually advanced level.

We also want to ensure that the gaming approach we want to design should adopt specific similar scenarios that professional certified examinations would contain, just to introduce these minors into the industry required certifications gradually as well as encourage them to see the significant advantage of having these certifications and knowledge from that early stage which in turn could aid in being a huge stepping-stone to more achievements.

Study Questions/Hypotheses

1. Will the game approach help in this case? Why?
2. What game models for education are there?
3. What game models suit Digital forensic education, and why?
4. How to implement a gamified digital forensics Educator and measure its effectiveness?

Limitations of the Study

1. Time consuming: the project would be time consuming as it requires detailed research which could take weeks to months to conclude.
2. Inadequate Gaming Model: there are not enough learning models that are gamified and tailored to digital forensics out there.
3. Cost of Implementation: the cost of implementation of this project is relatively expensive due to the hardware and software aspects needed to bring the project to reality.
4. Programming Experience: One need have a knowledge of at least a programing language to understand the flowchart of the game play.

Definition of Terms

a. *Cyber Crime:* criminal activity or a crime that involves the Internet, a computer system, or computer technology

b. *T.A.M.:* The technology acceptance model (T.A.M.) is an information systems theory that models how users come to accept and use a technology

c. *Jurisdiction:* the right, power, or authority to administer justice by hearing and determining controversies.

d. *Chain of Custody:* A form used to keep track of how the evidence is being transferred from person to person.

e. *Admissible:* that may be allowed or conceded; allowable:

f. *Dongle:* a hardware device attached to a computer without which a particular software program will not run to prevent unauthorized use.

g. *Encryption:* to convert (a message, information, etc.) into code.

h. *Firewall:* an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

i. *Digital Forensics:* a branch of forensic science focused on the recovery and investigation of artifacts found on digital devices.

j. *Storage Media:* is any technology -- including devices and materials used to place, keep, and retrieve electronic data.

k. *Suspects:* a person thought to be guilty of a crime or offense

l. *Cyber-stalking:* is stalking or harassment carried out over the Internet. It might target individuals, groups, or even organizations

m. *Identity theft:* the fraudulent appropriation and use of someone's identifying or personal data or documents as a credit card.

n. *Fraud:* deceit, trickery, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.

o. *Investigations:* a searching inquiry for ascertaining facts; detailed or careful examination.

p. *Intrusion:* an illegal act of entering, seizing, or taking possession of another's property.

q. *Fourth Amendment:* The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

r. *Plain-View Doctrine:* The plain view doctrine allows a police officer to seize objects not described in a warrant when executing a lawful search or seizure if he observes the object in plain view and has probable cause to believe that it relates to criminal activities.

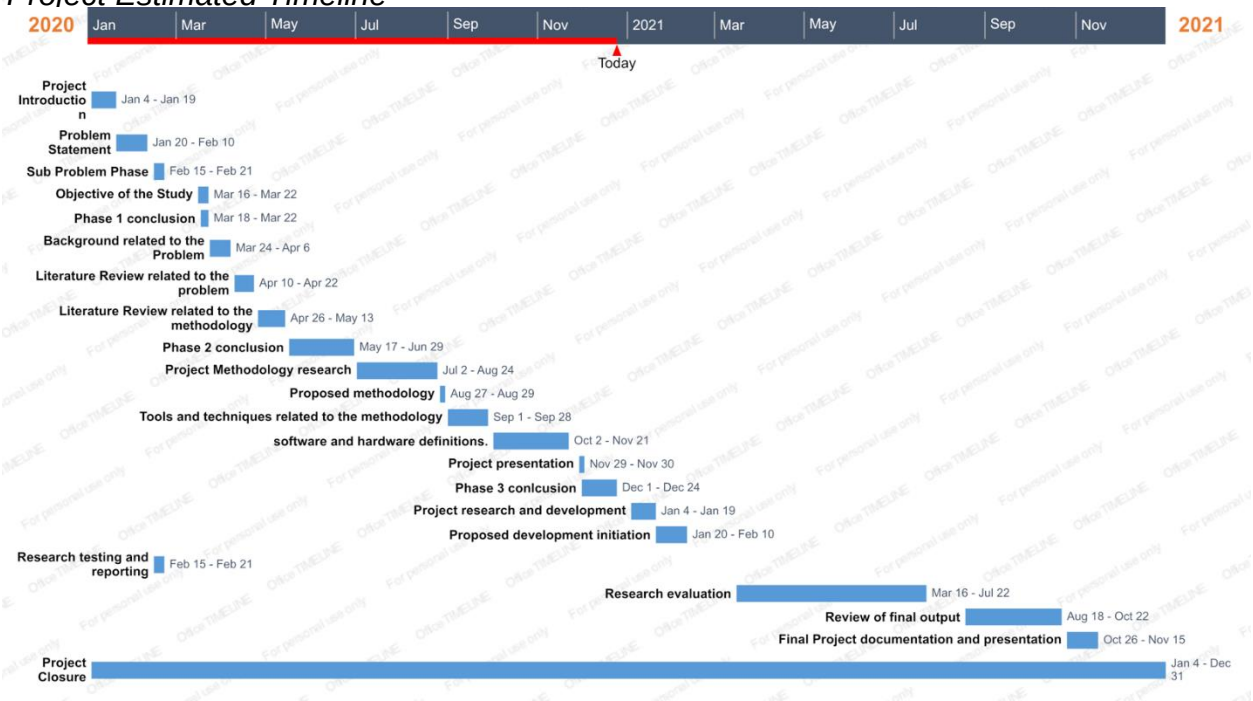
s. *Consent:* to permit, approve, or agree; comply or yield

t. *NPC:* Non-Player Character.

Project Timeline

Figure 1

Project Estimated Timeline



.

Summary

This chapter discussed the definition of digital forensics and cybercrime and some of the challenges, one of which is the shortage of expertise in the field both locally here in the U.S.A. and internationally. It also discusses why this field of study is essential and what approaches should be taken to ensure it does not gradually go obsolete. It discusses why such a profession is needed in tackling the current cyber activities currently spanning at a tremendous pace around the world. A suggestive approach calls for the immersion of K-12 students into a gamified approach to gain early

knowledge and possible future interest in the field. It looks at other approaches previously done and how this approach could be best made to ensure the continuity of interest in these young subjects. One of the critical areas of this chapter is figuring out the fundamental problems this thesis raises awareness to and how these problems can be best tackled. Essentially, it will be quite tricky to figure out all these, and the next few chapters will discuss further how this approach might just be worth the effort.

Chapter II: Background and Review of Literature

Introduction

This project aims at discussing the relevance of digital forensics and cybercrime from the perspective of what has been done, what is being done, and what could still be done. Here we will look at numerous bodies of works and comb through methodologies and proposed models that could potentially shed more insight into the need for a revised/novel model. Because we are proposing an approach that is unique in combating the problem statement, we will be looking at a combination of qualitative and quantitative methods to ensure a proper study is conducted.

Background Related to the Problem

The following subsection describes the literature review regarding why there is a need for a gamified approach to educating K-12 students in digital forensics.

Literature Related to the Problem

The aspects of k12 are linked and supported within the education system that remains rampant within the domains of the United States. This is especially true with the dawn of the new agenda and the new proposals to see the education system changed to encompass a larger direction of the state's education spectrum. It represents the education of a child from the kindergarten level to the secondary level.

Owing to the discussion of having graduated from these mentioned levels of schools. With the current systems changing, there was also the mention of the change of specific systems with the ideological fact that there is the bring-up of a more complex

yet educative and advantageous form of study (Adams, 2008). This was with the inclusion of some regions of topics and different systems when it came to the already developed curriculum—being able to encompass all aspects and give the students a chance to expound on an individual basis and given specific knowledge that would help in the shape of their future careers in a more positive domain.

With the current changes, the world is seemingly advancing when it comes to the technological aspects. Most of the individuals are switching to create specific formation on aspects of digitalization. In the same way that is being able to advance, so are the aspects of cyber-crimes performed on such a level. Students can show early signs of interest in such ideological fields. It is important to note that such students need to have this ideological fact addressed so that they may be able to assess the limitations and the extent of their abilities within the specific levels of the problematic cases.

Such a fact has resorted to having the course present when it comes to the k-12 students. This course has been disintegrated and has been a factor of discussion for quite some time. The primary concern is developing the sector and ensuring that it is also given the right amount of attention to be handled accordingly.

The cybersecurity course has been offered as a course at the high school level. The course is split into being able to handle the effects of social security and the spectrum of digital forensics on a minor level (Adams, 2008). The course gives the individuals or rather insights into the ideology of how the primary course is perceived and gives the students a basic ideology and concept knowledge on how the company is ground and the basis by which it operates.

With the world moving to a more digital conceptualized economy, this means that the central idea will shift into a digital per option and aspect. This there will be the need to ensure that the same field is advanced to expound on the same aspects of teaching digital forensics. This will inculcate the need to have specific tools for the students to get a hands-on experience and create an in-depth understanding of the matter.

It becomes quite open that the very spectrum of this field and that of cyber digital understanding is on an inclined growth rate. This is very fast and with an estimated rate of about 37% per annum. It is a topic that should be on the lookout from a very ground level of development. With the growth in the same sector, the job demand for such a sector is also expected to grow in the same ideal way. In the case that we are currently dealing with the primary input when it comes to the K-12 systems, there is a specific thing that has to be put into consideration (Adams, 2008).

It is with the basis that there are individual and specific excerpts of understanding and a set requirement by the mainboard regulating such a study. When it comes to the excerpts of digital forensic understanding, the topic can be demanding and complicated for students to understand and enact within the same ideological perspective. Such a case particularly becomes a challenge to the students' very excerpts to be able to understand.

The aspects being taught are of shallow depth and require some level of understanding. However, it should be noted that within the age bracket and the topics or rather the subjects by which such individuals or the students have been exposed means that they will have a hard time getting to grasp the content that is being discussed within

the bounds of the classroom. This is a matter that has been discussed over time, owing to the complaints that the teachers have brought forwards with the ideological avocation to have the education systems have to change such an ideological basis (Adams, 2008).

A remedy was brought out. The remedy included a set avocation not to have the specific cluster or group changed in any way possible. It revolved around the discussions that having to change the curriculum would mean that the students will have to comply with a relatively shallow exposure than what it already is. This would have more sense and would be useless when it comes to such a system. There was the avocation of various tools under digital forensics, which would ensure that the students can find such a learning procedure as one that is interesting.

The tools that are mainly incorporated in the study by these students are the ones that are regarded as those of being friendly and quite open to the spectrum of the student, with the ideological understanding that the same be easy and relatively simple to understand. However, when a higher learning standard tool has to be incorporated, this will mean that the matter will be more complicated for the student to understand.

The tools are built in the ideological wave of software. They require immense competence support to be able to manipulate the set software's and also be able to get the aspect on the whole and utterly full perspective. The main goals of having the incorporation of such a tool in the perspective of the same factor of creating interest in the specified topic as this will help create a direction of the student of having to take the

specific course when it comes to the aim of a better advancement in the course at a higher level of education.

The primary learning procedure when it comes to the bound of high school is basic. The same has been grafted and differentiated to get through a specific ideological form of ideas passed to the students without having to make such tasks a burden to them or the information too overwhelming for their case. When it comes to the teaching of digital forensic tools to these aspects, it is important to note that there is bound to be a specific system or a regulation of the same.

When such aspects come to the actual accordance and the basis of such a sequence, it will pose. The forensic tools on a digital platform on an undergraduate level will require specific software and ideological aspects as demanded by the set ideological concept, which will pose a challenge to understand, especially to a level of this kind. Therefore, there has been the inclusion of different digital tools established and introduced to handle this specific cluster of learners.

There is a particular cluster of gaming systems tags that have been introduced based on the learning procedure. This is with regards to information systems security. The established games are a particular thing now and have been in use for quite an extended period. It is also already in use within individual companies that have established trained personnel in the specific field.

The main reason for such an inclusion is to operate on the specific ideological content without being at risk in any whatsoever way as deemed possible or in threat in any form of way. When It comes to the aspects of the learning critique, it gives the

learners a better understanding process where the learners can comprehend what is being discussed and the best way to get the learners interested and have a better understanding of the same area within the field.

The significant aspect is designing a particular system that gives the student the right skills that are needed for a specific task or as a better understanding regime for what they are bound to face when it comes ok the prospects shortly. In this case, the prominent attribution is that of ensuring that the system that is being designed is bound to help the student get better information or insight into the ideological case. Not only this but also gain a certain level of understanding with regards to the ideological basis of the course.

When it comes to digital forensic bounds, the significant ideological aspect or rather the prominent distinguishable feature is that of having to l collect the relevant data from the electronic media, preserve the data and then compare the electronic data to any other forms of cases that are criminal.

The tools that have been placed under such a project should ensure that the student has all hands-on decks with such a system and be able to handle the information following the right sequence. Therefore, in developing any tool within the bounds of such a domain, these significant aspects need to be taken into concern and ideology.

To be encouraged on the same basis, there are the concepts of having to deal with the ideological basis of having to deal with the project designed to implement all the factors discussed through the domains of the course work. The aspect of a digital

forensic tool is bound to make the work more manageable when it comes to taking the route on the investigative process on developing a case (Adams, 2008).

The tool in such a case should answer such a project to its full perspective and give apparent domination over the same aspects and conclusions. The tool should be simple and gratified to complete or perform its duties to the fullest. Some may not be very sufficient but can handle the problem as an issue within the bound aspects.

It is important to note that when developing a particular forensic tool, there is the idea of noting the purpose the tool serves. In the first case, when dealing with a set of individuals who are termed as those of being in a k-12 level, then the tool must not be complicated so that the students may understand the encompass of the tool. Each tool is used for a different purpose, and the ability to know and understand the use of each is essential. In this case, the spectrum is to create a tool that is easily distinguishable from the other tools concerning the roles that each one of them plays.

When dealing with a forensic tool, some acknowledgments must be taken into explicit consideration. There is the ideological basis of having to deal with a specific set standard of having a note of how each tool is bound to operate and the context behind using any of the tools. In implementing a digital forensic tool, it is paramount to have a complete understanding of each tool's advantages and disadvantages. Once such knowledge is taken into consideration, there will be complete know-how of how to handle each perspective.

The aspects of digital forensic tools are presented in two clauses. There is the group that is constituted of those that are bound by the free packages, and then there

are the paid ones. A free package does not require any form of advancements to be made in terms of the initial payment. With the design and the same implementation, then the free domains remain the best to use. This is with the ideological aspects of having the significant customers being that of the student perspectives. A free domain will ensure that all the students have a transparent and open domain of the same. Availability is ensured, and better practice moments are guaranteed on the same levels (Boddington, 2016).

Whose primary clientele is that of the student body type and in this case, being that they fall under the domain of the k-12 students, there needs to be a creation of more multiple programs that fall under the free domain (Roussev, 2011). Mainly attributed to the fact that different software's play different roles in the digital forensic aspect. Therefore, it assumes that to be able to remit the best results, the students need to be familiarized with a set of tools. Each tool being promulgated to attend to a specific set of objectives and ideological aspects. In cases where more than one tool is used, or there is the incorporation of multiple tools, the result is bound to take a positive perspective.

Choosing the best tool or coming up with the ideological concepts remains a critical perspective when dealing with an investigative clause. The aspects must be able to specify a particular domain where one can create or implement the present best tools. In this case, the best tool is about the domain of the target users. In this case, the students need the use of tools that are in conjunction with their levels of study and that are easy to use (Roussev, 2011). A hands-on deck-form of tools will make these

clusters interested and motivated to continue in their research. However, an aspect that is limited to this fact is mainly undisclosed with the domain being thrown out.

In the development and the implementation of digital forensic tools, it should be noted that there are specific guidelines that bound or that control this particular set of domains. This is limited because there are boards that check the standards of the mode and credit such tools. Therefore, it should be noted that the tools are bound to operate following a set of domain standards to be verified to be used. It is categorically reduced or classified as those under a learning basis and those that happen to fall in the field. In both cases, the testing goes through the aspects of the N.I.S.T. (Roussev, 2011). In this case, the rules are also termed to have a copyright policy and specific standards bound by the tools developed (Boddington, 2016).

The tools for digital forensic services can also be classified under the spectrum of hardware forms. The hardware is not mainly used but remains to be an essential case study from all perspectives. (Roussev, 2011).They include having portable storage devices and cloning devices, just but to mention a few. The hardware tools have similar importance to the software tools in all criteria. At such a point, it should be noted that this is a task that befalls to have a sort of unity when it trickles down to aspects of joint operations. The hardware P.C.s are needed, and so is the software that will run in the hardware. Software tools that have been developed have ideal and specific requirements on the system they are run on. The specifications need to be met by the hardware part of the tools for such processes to be included and concluded (Roussev, 2011).

It would mean having the hardware up to standard for the students to access the specific software. Therefore, in the development of certain tools within the forensic design spectrum, then there is a need to power the standards or the hardware requirements by which it is bound to work. This is to be able to reach the minimum requirement of each student. There is also a different approach to the same. If the developing and implementation council of the tools for the school has the time and the resource, it could resort to having two versions of the module created (Zax & Adelstein, 2009). It will open a wider spectrum being able to encompass the need of all students. For example, the creation of a software tool built to suit a 32-bit operating system and be able to cater or serve a 64- bit operating system.

When designing forensic labs, the school needs to ensure that the k-12 students are presented with the best computer systems that can handle all of the objections and the sets of data that might come or follow such a path. The sets of computers must reach a minimum recommended system (Craiger et al., 2006). Such a requirement is made necessary to give a clear insight into the operation ability and give the best-practice requirement to the student. Such a case must be considered as the forensic lab acts as a tool by which the student is propelled to check on the future domains and the prospectus of having to operate on such a domain. The hardware components are supposed to have some minimum sets of requirements. These include the excerpts of the oracle database, the F.T.K. client user interface, and the client-side processing engine. Such a requirement allows the student to launch the software and operate it comfortably to obtain maximum results.

Regarding the use or coordination of the two aspects, the hardware, and the software tools, it is best to say that the minimum requirements for each hardware tool depend entirely on each component's specifications. However, the push of such an action to obtain a full set of recommended objectives for having the aspects of the hardware means no harm (Zax & Adelstein, 2009). It gives out the domain that one can be able to make advances in the future. However, it is an asset towards the school with the discussions of the tools needed for the complete aspect of the digital forensic platform. There is also the need to have a fully equipped crime kit. The significant aspect is built around the perspective of having the same needed to educate the student. A full kit should be delivered to such learners. Mainly to ensure that they understand every aspect and use of all tools (Zax & Adelstein, 2009).

In selecting or developing a tool to be used by the students, there could be two categorical aspects that could be linked to the commercially produced tools and the open-source tools that are quite openly depicted. However, the selection process should encompass the fact that there are some advantages and disadvantages. However, the basis of making such a decision can only be linked in aspects as directed by the main attributions of the cost, functionality, and the capabilities of the firm that is going ahead to make the exact presumptions (Roussev, 2011). Concerning the attributions of the open-source tool or tool that is mainly taken into common cases is the SIFT. This forensic tool kit is mainly built on the Ubuntu or the Linux operating systems. The option that makes the forensic environment much open and better is that the specific tools to objectives. Digital forensic tools have made forensic investigations take

a different and more epic illustration with the actions revolving around the domains of examinations. The specific software enables one to specifically dwell into a specific sector and get an in-depth solution for the problem. In this case, the students can understand the programs together with their operational functioning and the case sections that best befall such systems (Zax & Adelstein, 2009).

In the development and the implementation of such tools meant for the k-12 students, there needs to be a specific aspect that should be considered. This is with the follow-up of the complex domains of the tools. Given that the unit is introduced in certain stages and the general aspect revolves out a raw an essential state, then the design should follow a more open and direct state (Craiger et al., 2006). Simplicity becomes key. Complex software that revolves around coding aspects is not reliable when dealing with such a target audience. With complexity comes a total domain of having to discourage the possibility of understanding and the motivation to take the same elements at a higher education level.

There needs to be a sure tool in the necessary designing process that is entirely functional and is one without error. This is when dealing with some attributions that inked to the fundamental error or basic doubt programs. A program once issued to the students will be very hard to regulate or to assess. Therefore, there is a great need to check and ensure that the tool is well functional (Craiger et al., 2006). Giving the students a categorical chance that an error might occur during a set domain regarding the tools and the process than going in to correct such might get the students into a

form of confusion. It is necessary to have all the aspects in check before the launch, or a depicture of any attribution to the same ones as this.

When it comes to the teaching of digital forensic tools of these aspects, to students it is essential to note that is specific bound to be a particular system or a regulation of the same. When such aspects come to the actual accordance and the basis of such a sequence, it will pose. A challenge for the student to understand the concept (Zax & Adelstein, 2009). The forensic tools on a digital platform on an undergraduate level will require the use of specific software and ideological aspects as demanded by the set ideological concept, which will pose a challenge to understand, especially to this kind. Therefore, there has been the inclusion of different digital tools established and introduced to handle these specific clusters of learners.

This is a matter that has been discussed over time, owing to complaints that the teachers have brought forwards with the ideological avocation to have the education systems have to change such an ideological basis. A remedy was brought out. The remedy included a set avocation not to have the specific cluster or group changed in any way possible. It revolved around the discussions that having to change the curriculum would mean that the students will have to comply with relatively shallow exposure than what it already is. This would have more sense and would be useless when it comes to such a system. There was the avocation of the use of various tools under digital forensics, which would ensure that the students can find such a learning procedure as one that is interesting.

Literature Related to the Methodology

Gaming in Education

Gaming has been a growing part of our culture, and the interest in games in our younger generations has continued to increase over time. Three-quarters of the world's children's population play different genres of games, from computer games to outdoor games, regularly. The question is, are these games harmful or beneficial to our children, or are they learning something new as they play these games? Children have learned to love games since they were toddlers because they are fun, they have rules, and they are principal. The principal portion of this report will be an embodiment on concerning educational theory and gamification to better comprehend the parts that game academics educational environments, by presenting a classic that assimilates educational theory and game design and summarizes a methodology required to improve good educational games. The subsequent parts will test the rationality of these models in the educational systems

The Constructivist educational theory is a concept that focuses on deep understanding and growth rather than talents or conducts as the objectives of instruction. Growth and profound comprehension are edifices of dynamic learner restructuring. The main principle of constructivism is that information cannot be directly conveyed from one user to another; instead, it is something that the learner actively builds. Knowledge encompasses individual creations of learning that come about through relations with a person's environment or culture. Hence scholars are regarded as creating the peculiar learnings of their world. For education to be effective,

individuals must exclusively create knowledge through games, assessment, and social dissertation with other human beings. Objectives of learning offered in the constructivist environment need to be determinedly implanted in the milieu and should at least in one way or another represent daily experiences that people face. Students are also required to be responsible for their learning and be self-driven and inspired in exploring diverse information domains.

Contexts of formal knowledge are moderately unaccustomed when linked to real-life familiarities. They are frequently accentuating non-concrete, a decontextualized acquaintance that is challenging to transmit to real-life situations. This achieved information can then be recollected in examinations but cannot be voluntarily pragmatic in problem-solving circumstances that individuals encounter daily. In contrast, students in informal learning settings can apply factual knowledge and consistently solve their everyday challenges. Regular use of tools and knowledge helps students fully comprehend and gain more knowledge, which might help them change their perspective of life and the world in general.

The use of traditional learning designs might lead to students attaining deductive knowledge. For example, these traditional learning designs teach a concept or a law, followed by a practical and an impractical example; however, education based on inductive learning and discovery may lead to innovation, hence becoming more effective in the student's life. With this type of learning, students get to use their own experiences that make them construct concepts and rules according to what they have learned from their own experiences. This learning type encourages critical and strategic thinking,

which can be applied in the learner's future life. Education that incorporates gaming is vital for a student's growth in knowledge and understanding.

Gaming in education plays vital social, psychologically and cognitive growth, specifically throughout early infancy, and hence can be demarcated as a deliberate action that is fundamentally appealing because it involves some physical activities and mental activities that might have make-believe qualities. Games can also impact intellectual functions and inspiration that integrally encourages inquisitiveness by including challenges and elements of imaginary, intricacy, and novelty, encouraging goal formation and competition. Some of the skills that students acquire while playing games include memory, visualization, motor skills, log, i,c, and problem-solving skills, to name but a few. Hence, these skills are fundamental in attaining knowledge. Gaming in Education emboldens students to be innately motivated, metacognitively, energetic, and developmentally active, and self–evaluating.

Research that has been conducted on the use of conventional games in education is comparatively novel but promptly growing. These studies are principally apprehensive with the growth of correlated capabilities and literateness during playing games or games in the establishment of learning societies both while gaming and connected to gameplay. Many schools rarely use conventional gaming approaches to impart knowledge to their students, and hence they are dubious about being incorporated into the school curriculum. Some of the reasons include it is hard for teachers to identify the impact and relevancy of these games to the school curriculum and the exactitude and pertinence of the content within these games. There is also

exertion in coaxing other school shareholders to the potential/ definite educational advantages these mainstream games offer. Teachers do not also have time to familiarize themselves with these games and learn the methods they might use to make these games more productive to the students to acquire the best results out of them. These games might contain irrelevant content that cannot be removed or ignored; hence students and teachers lose valuable teaching time. However, parents and teachers are aware of the support and valuable skills that the students might get from these games. These skills include planning, critical thinking, strategic thinking, communication skills, number applications, negotiating skills, decision making, and handling and processing data. Incorporating these gaming models in the education system might considerably improve the students' prospects of erudition activities.

The incorporation of adventure and simulation games has been proposed as the most appropriate tools of education over the years. These games are usually used in academic environments where scholars are focused on single objectives hence leading to reduced competition among students countenancing them to discover and try out at their specific pace. Even though the concepts used in these imitation games are grounded on engaging scholars with real-world happenings and waning to recognize that playing is a fragment of their daily lives. This simulation gaming concept is concealed from the player, and hence players can only cultivate a shallow indulgence of this concept.

Scholars in support of the educational constructivism concept came up with the term micro-world, which describes scenarios where students do not learn a specific

purview but become part of the scenario, hence leading to the stimulation of interest and motivation, making students capable of interacting and exploring different complex ideas within such spaces. They also believe that simulation games might provide meaningful ways that present micro-worlds to students. Thus, games created based on sound educational theories and concepts can be used as tools that promote modern educational theories in the classroom.

Some game models used in education include the Game Object Model, which is based off on Object Orientated Programming conceptions that endeavors to generate contention amid pedagogical measurements and game rudiments and includes mechanisms that are signified by rounded squares that stimulate educational goals that are theoretical interfaces and those that sanction for the apprehension of such goals controlled in different spaces. These mechanisms either lodge solid or non-concrete edges that are characterized by circles. These components might either be self-supporting or a portion of additional mechanisms, which inherit all the parent facets. The internal elements encompass tangible interfaces, whereas the external ones are additionally abstract. Hence this game module contains four inspirational interfaces that are play, exploration, challenges, and engagement. It also encompasses the internal conception of the interstellar component.

The space visualization module consists of the storyline, analytical thinking, exploration, goal development, goal accomplishment, and practice interfaces. The components of these elements entail interfaces such as fun, graphics, technology, and sound. These components create the storyline, look, and playability of the games and

are associated with unearthing and creating goals of the visualization interstellar component and the game space component's assignation interface. This component's basics comprise the actor component that is explicitly associated with the assignation and the storyline edges and comprises a unique abstract border which is drama and two tangible connections and gesture interfaces. Other conception components that are discovery, critical thinking, goal development, goal completion, antagonism, and preparation are articulated through the glitches' literacy, communication, memory, and motorized mechanisms. Literary elements are consequently characterized by abstract interfaces and game rudiments by tangible interfaces.

This archetype is cast-off towards improvement in a qualitative methodology to identity improvement (Persona Outlining Model). The Game accomplishment Archetype is used to recognize all the existing interfaces of the Game Object Model. Software Engineering frequently buttresses the production of multifaceted software approaches that endeavor to resolve the encounter amid failures of an artifact to occur devoid of any process used in driving product production when the actual intransigent phased approach is used. Scholars projected the development of a response system that can be used to accomplish software improvement. The initial phase in the procedure is to lucid the "Situation of Concern" that defines the existing substandard condition of the domain that the software shall endeavor to solve. Afterward, the problem proclamation is demarcated to discourse the Situation of Concern

The statement of the problem in the interactive computer system comprises of four components that describe; people who will abuse the system, individual action that

the software structure will use in satisfying the condition of concern, the sustenance that the system will provide, and the tools that will be castoff in developing the system. The interaction between the individual and the computer will be well-defined in terms of a persona, which is defined as the features of a fabricated operator of the system. Descriptions of the character are more frequently than not created from existing data and do not permit necessary arithmetical implements throughout the operator assessment stages of software creation.

As much as the Game Object Model delivers a structure that connects the educational model to game design, it does not articulate how educational games are built and designed. The outmost Game Object Model interface is that of the storyline, and this interface ought to consequently be the foundation of the creation. However, if the educational software is successful, the education goals should be visibly defined. The foremost precedence of describing an educational game is defining the goals of education and the framework and settling on a storyline that encompasses these goals and ensuring that they are exhilarating adequately to deliver inherent inspiration for the students to play the game. This concept has not only been used in the higher education system. It has also been used in the K-12 system brewing many controversies (Kleman, 2013). Gamification is used for educational purposes the society, in general, society uses this methodology to improve mental activity and provoke innovation. For example, Starbucks has reward programs that encourage their consumers to set goals and compete with each other(Kleman, 2013). One of the main strategies used in educational gamification is the use of description edifices that abode learners on a path. The players

who achieve the given tasks are finally awarded (Kleman, 2013). Some of the prizes that students are awarded include education points, badges, and a progress bar's filling up. Achievement badges are given to students to offer names that represent their newly acquired competencies and provide these students with a platform that recognizes their importance (Farber, 2013). Gaming in education brings a new way that combines technology and human desire that provides learners with the best possible education (Kleman, 2013).

Most teachers create their gaming models based on the needs of their students. These games can be online games or traditional gaming systems. There are, however, free gaming platforms that can be tailor-made to fit the students' needs, for example, ScootPad, Goal Book, Socrative, Brainscape, among others. The purpose of these games in the educational system is to serve as an intervention for students' social, emotional, and mental growth (Lee, 2011). These gaming tools do not only boost the student's morale to learning. They also guide teachers on how best they can capture their students' attention and impact them with the knowledge that they need and encourage them to nurture their students' talents. Some of the positive impacts of using these gaming models in the educational system include students are exposed to technology at a very young age, and the use of these modules helps in capturing their attention and making them be more involved and engaged during lessons hence increasing their chances of attaining goals of learning and meeting their required educational standards.

Game-based learning modules also allow an individual learner or a team of students to explore their strengths and strengthen their weaknesses. These games also help students acquire a new skill; the modules also track and monitor the students' performance; hence, this helps teachers identify the subject areas that their students are struggling to understand (Holland, 2013). Gamification also encourages learners to be enthralled in the activity, which increases their attention levels. (Kleman, 2013). Gamification also endorses technical knowledge and increases students' multitasking skills since scholars are continuously diverting their attention amid the devices, screens, instructors, and their fellow students (Marquis, 2013). According to Marquis (2013), a well-set-up game encourages the spirit of teamwork by building a social component within the game. Incorporating games in the educational system also evoke creativity in students, especially when they are tackling tough challenges. This not only improves their optimism but also makes them more determined and less scared of asking for help when they are stuck.

For as much as gamification in the educational system provokes the student's interest in attaining knowledge, this learning module has its fair share of negative impact, especially for younger students. Some of the critics of this learning module argue that there has not been enough research that has been done to showcase the benefits of gamification in the education system, especially in elementary gamification (Filsecker & Hickey, 2014). Other critics argue that the meaning of learning is kicked out by the use of gamification reason being awarding students with points and badges are extrinsic motivators, students get excited about a short while, and with time the novelty

quickly wears off. The teachers are forced to keep on rewarding the students over and over again so that they do not lose interest in learning (Kleman, 2013).

The use of gaming models in school can be costly since the school incurs the cost of buying software, training teachers on how to incorporate these modules in their daily lessons, and it is also costly to implement this type of learning. This educational system can also encourage anti-social behavior whereby students might lack face-to-face interaction with their peers. Gamification might also lead to reduced attention spans. The quick speed of action and instant response they get might make students anticipate the same kind of quick immediate retort in all phases of their lives. These gamification learning modules do not always incorporate all the subjects that students need to learn. Hence, making scholars who are exceptionally inspired by these games miss out on particular areas and subjects not included (Marquis, 2013).

The use of gamification in today's classrooms always incorporates some form of technology, and multiple categories of technology are often used, such as desktops, tablets, Chromebooks, Activboards, among others. Suppose the teacher chooses to create their gaming platform in their lessons and post the leaderboard and collect data manually. In that case, they must use emerging technologies reason being students research, attain data, and compose products with the new technologies to communicate with their teachers and their school teammates.

To make gamification more effective, it needs to be differentiated. Suppose the education system plans this mode of learning correctly, different students with different skills that work at a pace that matches their individual needs, promoting growth and

development of their skills, fostering increased achievement. A relaxed way to embolden and support learners with little inspiration for education, those with lower self-esteem, or those with educational difficulties, is to implement more milestones of achievement to the gamification platform. This will give these (and all) students a chance for many small celebrations throughout their journey to mastery level. Students with disabilities also benefit from using games in the educational system, especially those who are suffering from autism, whereby digital games calm them down. Gamification might help students improve their grades, improve how they socialize and interact with one another, improve their organizational skills and make them more aware and conversant of other people's needs (Coffey, 2014). Gamification also helps teachers in capturing immediate, in-depth data about the performance of each student. Hence, these programs can assist in the assessment of students by decreasing their chances of any cheating reason being their learning is individualized.

The world has been observed to be going entirely digital over the last decade, and this has further increased the susceptibility of individual or personal data as well as information related to companies and other business organizations through the concept of cybercrime and other forms of unethical mining of data from the information presented in different databases all over the globe. According to the information presented by Eubanks (2017) in a Forbes Magazine article, there is a continuous increase in the prevalence of cybercrime throughout the globe with the complaints filed with the Federal Bureau of Investigation in the United States recorded to be 351,936 only in 2018 with the money lost found to be more than 2.7 billion dollars at the period

the information was presented. This was revealed to be due to the increasing usage of online platforms for business and personal transactions, allowing criminals to leverage this development in stealing.

This, therefore, makes the development of cybersecurity and the introduction of digital forensics important to the global environment. Many research has been conducted to determine the best way to integrate this learning among people of different ages and skill set considering the fact it is the way to go for the future due to the continuous rise in the usage of online platforms which subsequently leads to an increase in the need to secure users' information from cybercriminals. This involves the implementation of several strategies to include people of every age in the process of ensuring that interests are created in the process of digital forensics and cybersecurity, especially for children and young adults, and an example of this is the use of the gaming approach with the students in K-12 level to stimulate their interest.

According to Yerby et al. (2014) the data retrieved from the U.S. Bureau of Labor in 2014 showed that there was going to be an average growth rate of 11% for the next ten years for jobs related to private investigators and detectives with information security field including the digital forensics expected to have a growth rate of 37% over the same period which means 27,000 jobs is expected to be created in the information security sector, 700 in forensic science especially for technicians, and over 3000 for private investigators. The authors further revealed that digital forensics is a proliferating field in the information security field, and its emergence is due to the continuous cybercrime incidents throughout the globe. However, it requires having individual skills that are

exhibited using some specialized tools, which are very expensive. This has, therefore, led to the implementation of several strategies to incorporate and improve the workforce for digital forensics through the creation and expansion of new programs in educational institutions to satisfy the numbers required by the business sector as well as the law enforcement agencies and military currently and in the future (Yerby et al., 2014). In their study, these authors proposed the use of video games to ensure active participation of people as well as ensure an increment in their awareness, make the complexity in digital forensics to be fun, lively, and approachable, and to create experiences of learning and training which were supposed to be theoretical and presents a danger for learners during the process of being trained in the conventional laboratory. The authors used serious games and gamification through game-based learning to ensure students become proficient with the knowledge of digital forensics and later make them successful as professionals in the field and, by extension, information security. The authors designed a Digital Forensic Interactive (DFI) video game by using a Unity game engine and Blender as part of the efforts to make digital forensics easy to learn and applied in real life.

The study by Yerby et al. (2014) further revealed another digital forensic game that has been previously applied, and this is Mark Lane's LOGS Project H.U.M.A.N., which involves the player send a text message and retrieval information using a preferable tool. The game's design allows several players to participate at the same time without any standard to solve the case of a retired agent of the Central Intelligence Agency that was wronged. The game is more than an ordinary investigation about the

procedures involved in digital forensics. It includes a cinematic thriller with each of the players who have given zodiac diagrams to solve by getting involved with drug dealers, decoding languages considered secret, and certain riddles.

According to Jin et al. (2018), the importance of cybersecurity to national infrastructure and the military, industries, personal lives, and privacy and governments at both the federal and local levels cannot be overestimated overemphasized. They also showed the need to increase the skilled workforce required in cybersecurity, considering the possible and potential significant cybercrime and threats projected on the sectors related to the government and industries in the United States. These authors reported this to have led to the joint funding of a program known as the GenCyber to ensure the stimulation of the interest of K-12 students in the field of cybersecurity and improve their knowledge and understanding of the concept as well as to ensure safe behavior while transacting online.

The successful launching of four GenCyber summer camp programs for 181 high school students was recorded by the Purdue University Northwest in 2016 and 2017, with the students having 51.3% of African American and Hispanic students and two males to 1 female ratio. During the GenCyber summer camp, the activities were reported to be in the form of a game-based learning model and a hands-on laboratory pattern. They were found to be effective and efficient at teaching the principles of cybersecurity to the students. One of the games used was the Cyber Defense Tower Game, and this was observed to require the protection of servers from various cyber-

attack by the students. The game was observed to be well-accepted by the students, their instructors, as well as the visiting team to the site (Jin et al., 2018).

The activities involved in the game-based learning were recorded by Jin et al. (2018) to have created an "immersive and learner-centered experience" for the high school students and also proved highly effective and efficient to initiate training on cybersecurity awareness and acquisition of practical skills for beginners from different backgrounds. The results further showed that implementing the gaming method in learning activities or gamification in cybersecurity education was most effective in male high school students compared to female students.

Another study by Javidi & Sheybani (2018) showed the lack of interest in S.T.E.M. subjects by K-12 students and that this further leads to the lack of interest in cybersecurity individuals. This, therefore, means there is a need to integrate a learning approach that is considered to create a fun experience for the students to make them interested in cybersecurity. This involved training more teachers in high school to use this approach in teaching students in their classrooms with the focus on ensuring the students see I.T. security as a very attractive career path. The authors proposed the development of an unparalleled and new curriculum and scalable program focusing on cybersecurity and all its elements in such a way that robust tools will be created to make education on cybersecurity a fun experience, especially for the future generation to become interested in careers and professions directed towards protecting the cyberspace and warding off threats attached to the use of cyberspace for transactions. Javidi & Sheybani (2018) also emphasized the importance of leadership and

entrepreneurship in preparing the students for real-life experience and in solving problems.

A study by Pan et al. (2015) also highlighted the difficulties for individuals to be interested in the digital forensics field despite the importance of this field of study towards ensuring cyberspace's safety and saving the world from the attacks of cybercriminals. In their way of finding solutions to this problem associated with the lack of people's lack of interest in the field, they introduced a game framework for digital forensics which is designed to have series of fun, exciting, and at the same educational courses modules on forensics which are considered sufficient for students in their first year in college. This is directed towards the identification and attraction of students at their early stage to forensics through the use of the concept of Game-Based Learning, which has been previously and successfully applied in other fields such as information security at large, geosciences, and several other fields. The authors revealed that the application of game-based learning would be handy in the field of computer forensics and other complicated areas involving the need for concepts considered abstract and requiring active practice.

Another approach implemented in solving the problems found with the lesser number of people interested in cybersecurity is the Capture the Flag (CTF) approach (li & Kulkarni, 2015). This method is directed towards ensuring that college students, including those who are not majoring in information technology and cybersecurity, and the students in high school, become attracted to cybersecurity. The authors showed that gaming has been very useful in training and educating people in several fields, including

risk management and information assurance, and has also proved successful in training several employees.

Moreover, several approaches have also been implemented to educate people about security issues as observed in the use of security games by the United States Department of Defense's Defense Information Systems Agency (DISA) for many years. These include the use of CyberProtect as indicated by and Cyber Awareness Challenge by the Information Assurance Support Environment and Defense Information Systems Agency. Another popular gaming model introduced to integrate games into the process of educating people about cybersecurity include CyberCeige, which is a video game created by the Naval Postgraduate School Center for Information Systems Security Studies and Research as reported by Cone et al. (2007) to make the process of learning about information technology security easier for people. This model employed similar methods with the SimCity™ according to Kourtis (2020) and this involved the participant spending virtual money to buy and set up servers, operating systems, workstations, network devices, and applications towards ensuring there is a balance between security and productivity during an attack. Some firewalls can be configured, link encryptors, components to manage identity, including authentication servers and biometric scanners, and others such as VPNs and access control mechanisms in the model.

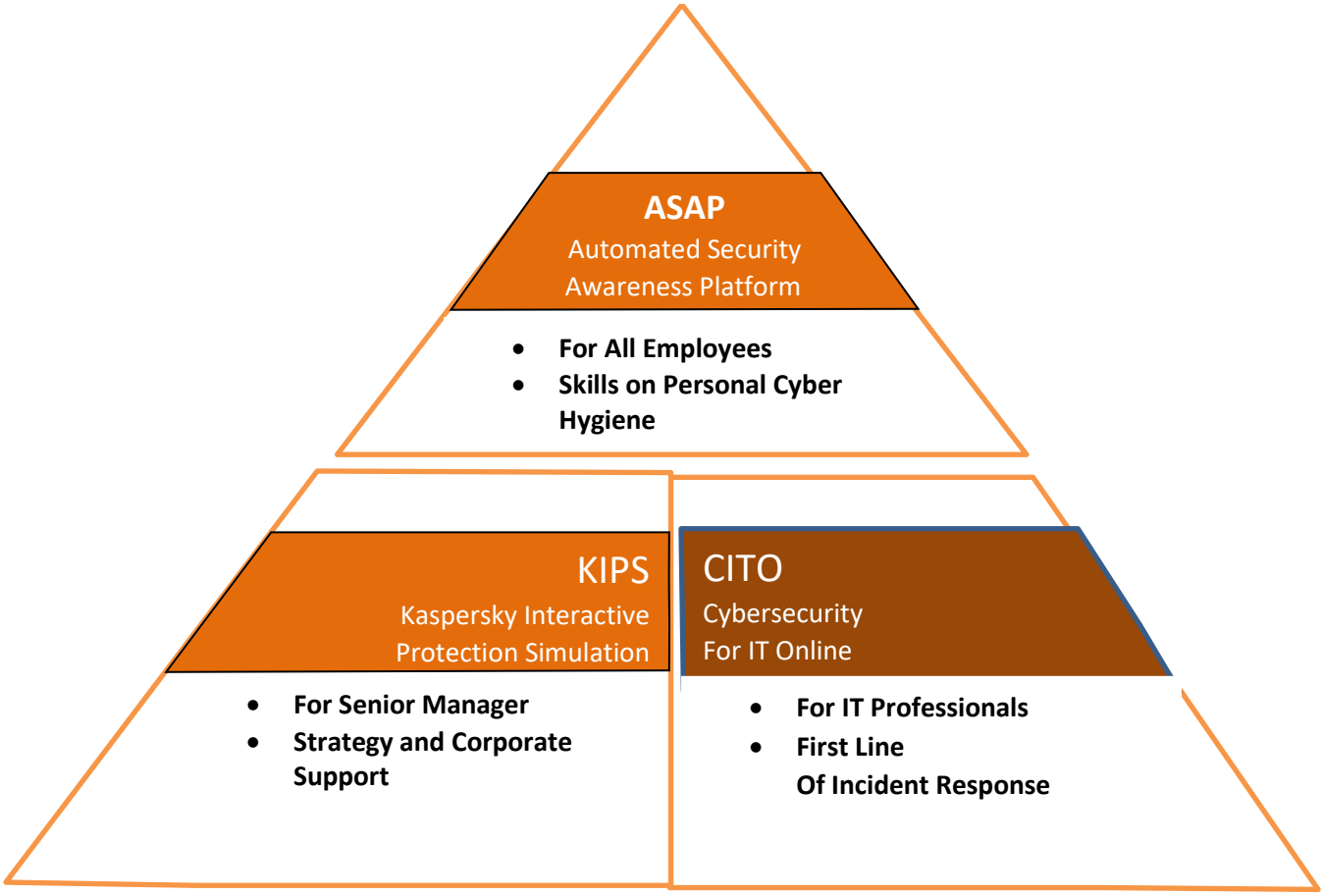
Another security game of note is the Game of Threats, which PriceWaterhouseCoopers (PwC) introduced as a digital game with the top management of a company used as the audience while the simulation is about a scenario of a real-life

security breach of a company. The participants are demanded to come up with decisions that are fast and have the potential to solve the problem significantly with little information provided (Kourtis, 2020). The security experts of PwC use the environment or interface of the game to design an experience that is real with the use of different kinds of attackers or actors who present threats to the company and the methods they prefer to use. These experts also provide the participants or players with information on ensuring effective prevention, detection, and effective response to these attacks. The game is designed to use up to three hours of play, with the maximum allowed players being 15 to ensure adequate interactivity on the platform.

Kaspersky Interactive Protection Simulation (KIPS) is another security game designed by Kaspersky Security as part of its Kaspersky Security Awareness, which is created to have three different sectors as indicated in the following figure with the remaining two being Automated Security Awareness Platform (ASAP) for all employees to understand skills on personal cyber hygiene and Cybersecurity for I.T. Online (C.I.T.O.) which is created for I.T. professionals to ensure the first line of incident response. Meanwhile, according to Kourtis (2020), the Kaspersky Interactive Protection Simulation (KIPS) makes use of the gaming method because it was created through the use of the gamified approach to improving the security consciousness and behaviors towards security towards ensuring an effective decision-making process for the senior managers.

Figure 2

Kaspersky Security Awareness. (Kourtis, 2020)



Another gamified approach to cybersecurity is the Anti-Phishing Phil, which was designed and developed by Sheng et al. (2007). The approach is focused on teaching people the protection of their e-mails and websites from phishing attacks, and this is because there are tools embedded in browsers that are used in preventing these attacks. However, there are not sufficient to function against specific attacks due to the ignorance and negligence of users in installing or heeding to the warnings from these

tools (Kourtis, 2020). Therefore, the three goals of this gamified approach in educating users are to teach them how to identify URLs related to phishing, the places to determine trustworthy or untrustworthy websites, and using search engines to search for legitimate websites. The game is divided into four different rounds, with each of them recorded to have lasted for 2 minutes.

Chen et al. (2008) discussed about a digital game-based learning model for a software engineering course that integrates pedagogical knowledge, content knowledge and technical knowledge. This model allows students learn the process of software development in a team-based environment, here they used role-playing as a strategy that lets students immerse themselves into characters such as a programmer, project leader, system analyst, or a system designer.

Another gaming model reported by Kourtis (2020) is the "2025 Ex Machina Ex Machina". This is a gamified approach attached to educating individuals on the cybersecurity attached to the use of social media platforms and the relationship between private and public life with the focus on being responsible with the use of the Internet. The scenario created for the game involves posting personal information by the people and their vulnerability to cyber-attacks through this phenomenon and when the information provided surfaces again in the future. The game player is designed to be one of the network detectives hired to retrieve information required to stop a website that is tagged "denicheur.net" from retrieving past information about people without any reason to worry about privacy protection laws.

The continuous inclusion of gamification in the cybersecurity field has led several other researchers to design different games to ensure awareness about security, as observed with the attempt made by Arachchilage & Love (2013) to design a game framework to enhance the behavior of users of the computer to encourage the prevention of phishing attacks. Another game was attempted by Adams & Makramalla (2015) towards the provision of an innovative gamified approach to educating leaders and employees of an organization to ensure the development of cybersecurity skills and to possess the ability to protect their data from breaches and threats from cybercriminals.

Furthermore, some other games have also been created, which are non-digital information assurance, and some of them include ones produced by Symantec, which is free to use d0×3d, and a flashcard game type as reported by Gondree et al. (2013). Another type is the StrikeCom, which was designed in the University of Arizona by the Center for the Management of Information and observed to be in the same design as the Digital Forensics Interactive, which was reported in Yerby et al. (2014) such that the player completes the predefined phases involved in an investigation. Meanwhile, according to Twitchell (2007), there are variations in the aspect of gameplay between these two models of gaming in computer forensic education, and this is observed in the fact that StrikeCom involves many players at a time and the focus is on operations that are related to the military.

Table 6

Methodologies employed by different authors in their research

Author	Methodologies discussed
(Yerby et al., 2014)	Digital Forensics Interactive (DFI) Mark Lane's LOGS Project H.U.M.A.N. CyberProtect Cyber Awareness Challenge CyberCeige d0x3d StrikeCom
(Jin et al., 2018)	GenCyber Cyber Defense Tower Game
Li, C. and Kulkarni, R. (2015)	Capture the Flag (CTF)
(Twitchell, 2007)	CyberProtect
(Cone et al., 2007)	CyberCeige
(Kourtis, 2020)	Game of Threats Kaspersky Interactive Protection Simulation (KIPS) Anti-Phishing Phil 2025 Ex Machina Ex Machina

Gaming in education has become a norm in recent years. This can be associated with the advancement in technology and the focus of education providers towards ensuring learners understand every aspect of the courses they are being taught. As previously stated, the cybersecurity field is considered complex, and this makes young learners lose interest in the process of acquiring the skills required to become cybersecurity experts and professionals in the offing, and this has led to the design, introduction, and implementation of gaming methods through gamified approaches toward making the process fun, easy, and learnable for students in high schools, colleges, as well as employees and senior managers in companies.

For this study's purpose, the Digital Forensics Initiatives methodology is recommended to be implemented considering that it is majorly focused on the digital forensics aspects of cybersecurity, which is the central focus of this study. The method is also considered most effective because of its elements and design, which are focused on making cybersecurity and digital forensics precisely easy for K-10 students, which are also the focus of this study. Unlike other methodologies, this method, as presented by Yerby et al. (2014), is a severe security game that is directed towards assisting students in learning the fundamental procedures of investigating issues related to digital forensics such as responding, gathering or seizing, acquiring, analyzing, and reporting data. The training was created in the form of video games to ease expanding the knowledge of cybersecurity, especially the digital forensic aspects for students in high schools or K-12 students.

Summary

In this chapter, we looked at what has been done so far in the concept of education through gaming as an approach. Here we looked at how the use of games in educational systems helps students evaluate themselves and gives them a picture of where they stand at any given time, not just during the examination period. We also looked at how education through gaming helps students develop and grow the cognitive, intellectual, psychological, and social skills that will help them make the right decisions in their next phase of life. This system helps them get insights into the areas that they need to improve and master their skills. It also helps teachers change their teaching methods by providing data that will help them improve their teaching skills. The approaches discussed in this chapter leave room for improvement as no technology is complete if there is no provision for improvements to accommodate futuristic approaches to solve a growing problem best.

Chapter III: Methodology

Introduction

Due to the lack of adequate experts in digital forensics, there is a need to create a platform that encourages awareness in this field. Hence, this project aims to channel such awareness to the younger generation with the hope of breeding young digital forensics experts that would saturate the workforce. Studies Have shown that the number of investigations that require a digital forensics expert result in substantial digital evidence backlogs that are being experienced by law enforcement agencies around the world, including the U.S.A. The number of cases that require Digital forensics is more than likely to rise as most high-profile crimes are going digital and have much more adverse effects than the average novel crimes. In 2017, the U.S. Department of Justice announced a cyber-task force to investigate complex crimes in cyberspace. In addition to this, the current techniques of educating digital forensics are unexciting, and as such, there is going to be little interest in venturing into a career that is perceived in the comparison of both being legally inclined as well as medically affiliated.

Digital forensics and cyber-crime investigation should be carried out in a legal and ethical procedure by experts or professionals. The investigators, therefore, need to investigate the cases of cybercrime handle. Analyze and interpret the digital evidence after that, record their findings, and analyze them. They also need to address the upcoming constraints in the digital forensic field inappropriate manner to solve any future challenges that could arise. The government imposes ethical obligations in cybercrime and digital forensics; they are prescribed by the national, regional, and

international law, which is stated under the cybercrime procedural law and human rights obligations in cybercrime (Holt et al., 2015).

The various human rights obligations in cybercrime include the rights of data handling, data retention, and preservation requirements in cybercrime. Therefore, the ethical code of conduct clearly defines the guidelines that cover the right and wrong conduct to informed decision-making. It mostly includes the rights and responsibilities of the cyber professionals and the behaviors demonstrated by the members. It also ensures that the results of the digital forensic processes show accuracy and trustworthiness. Members of the digital forensic and cyber should demonstrate obedience and responsibility towards the set rules and regulations by abiding by the legal orders and conducting a detailed observation and examination of evidence based on the existing and defined laws, standards, methods, and guidelines. The guideline also defines some of the prohibited acts in the digital forensic field, including withholding the evidence by profession, engagement in the biased analyses or reporting of evidence, and interpretation of the qualifications (Holt et al., 2015).

Design of the Study

Digital forensics includes obtaining, preserving, analyzing, and documenting the evidence of the study. Therefore, investigators must receive a comprehensive search method to investigate cybercrimes; they should also collect digital proofs and analyze them. In that regard, I will be developing a game design that will be built to focus on

high school students (K-12) and would include features that would be engaging, fun-filled, visual, interactive, and attractive.

1. Engaging: The game's design would be engaging enough that it should inhibit students from being distracted by external factors.
2. Fun-filled: The game would be filled with fun activities for the students to find both attractive and challenging.
3. Interactive: The game would be designed to accommodate interactive sessions that would be educationally beneficial to the students as they explore different game sections. Else, it could be labeled as being boring.
4. Attractive: This is a crucial element in the game design; without engaging content that is eye-catching, it would be difficult to lure users.
5. Visual: The game is expected to be learned by doing; hence it would provide the students with a full hands-on experience.

One of the benefits of this game would be that communications and window tabs would be disabled as soon as the game launches to prevent texting or chatting. Also, the game would be designed to follow the basics components of all games, which are.

1. Rules: The game would have rules that ought to have adhered strictly.
2. Goal: The game would have an end goal that is subjective to each player based on their keen interest or specialization.
3. Acceptance of Gaming regulations: Just as all games have policies and regulations that govern the game, this would not be an exception. It would have a user agreement banner that details the game's policies to the user.

As stated in the problem statement, this paper's primary goal is to tackle the shortage of expertise around digital forensics by producing young and vibrant digital forensics experts using non-traditional methods. We want to adopt a gamified approach to solve this issue. We would be considering so many layers of learning mechanisms to educate the target individuals, High school students.

Traditional learning methods are often perceived as being too dull, not good enough, and or obsolete; else, the need to foster up new learning methods that are both web-based could be played with a mobile device or a computer system and can be adapted to numerous operating systems. The game would also be graphically illustrated, which would be both technical and challenging enough for the students throughout the game. The game would include activities that would encourage continuous learning as they play. This could come up in the forms of quizzes, puzzles, hints, and wordplays. Because it is a learning game, it would also measure up the student's areas of strength and weaknesses and as such would penalize students who do not do great in the different stages of the game, either by having them retake that category or look for other means to achieve the required points to cross over to a new stage. Without such, the students, I believe, would have no idea how poorly or greatly they are faring, as this evaluation would be a critical element in providing the necessary motivation to boost their confidence.

The game would also have a question-based scenario where a student would be required to access a case study to the best of their knowledge and carry out investigations within the scope of the law and that of the investigation. Erring students would be required to carry out of-the-books activities to gather up points/rewards to return to those specific question-based scenarios. This will be put in place to encourage students to know how to go about investigations and how to address specific areas of the legal system as about specific case files.

For the game, a level would include investigating a public organization and a private organization. This would be so to teach the students how investigations are being carried out in government-owned businesses and privately owned businesses and the similarities in investigations between these two different institutions.

As with any other information technology implementation, this educational tool's success inevitably begins with the user; individual acceptance and usage are critical (Money & Turner, 2004). Therefore, the game would adopt some aspects of the Technology Acceptance Models proposed over the years (Lai, 2017). This would assist in providing necessary feedbacks on the Perceived Ease of Use, and Perceived Usefulness of this educational gaming system, as well as access their individual and collective knowledge capacity on how the users approach a case and also how well and effective, they solve that case using their knowledge of digital forensics.

Now, because the game leaves room for improvements and further sophistication, I will also identify the necessary skills needed for each of the game's

proposed levels based on specific metrics. These metrics would include knowledge levels, individual skills, and prerequisites, all needed in the game's fundamental stages.

Data Collection

For this research, we will be using both software and hardware alike. Mainly because the research is both technical and theoretical and, as such, requires results, graphics, and data files.

Software's needs for this research includes Autopsy, Pro-discover, EnCase, Unity game developer, Blender 3D designer, virtual machines. Hardware's required may include write blockers, laptops, desktops, hard disk drives, memory sticks—data cables, etc. Based on research conducted on numerous Highschool syllabus in the United States relating to Computer Science or Information Technology, the table below has been segmented to fit in the right order of learning approach required of high school students venturing into digital forensics.

Table 7

Components of the Game

Beginners			
	Pre-reqs	**Primary**	**Secondary**
	Basic Computer Skills	Investigations (Preparations and Conducts)	Numbering System (binary, octal, decimal, hexadecimal)

Table 7 (Continued)

	Basic computer hardware knowledge	Computer hardware and Components of a crime scene	Chain of custody
		Private/public Sectors	Identifying attack types
		4TH amendment	Understanding Steganography.
		Components of a Lab	Examining data files.
		Bad actors in crimes	Volatility.
		Recognizing graphic files	Uses of forensics tools.
		collecting data files	
		Storage types	
		Identifying forensics tools	

Game Framework

Unity is a well-known game advancement programming that has an assortment of elements. One such element is the capacity to import three-layered objects into its

gaming environment. Other parts accessible incorporate making and embedding characters also, objects, changing central focuses and outlines each second, and its utilization of physical science to make a three-layered (3D) gaming environment.

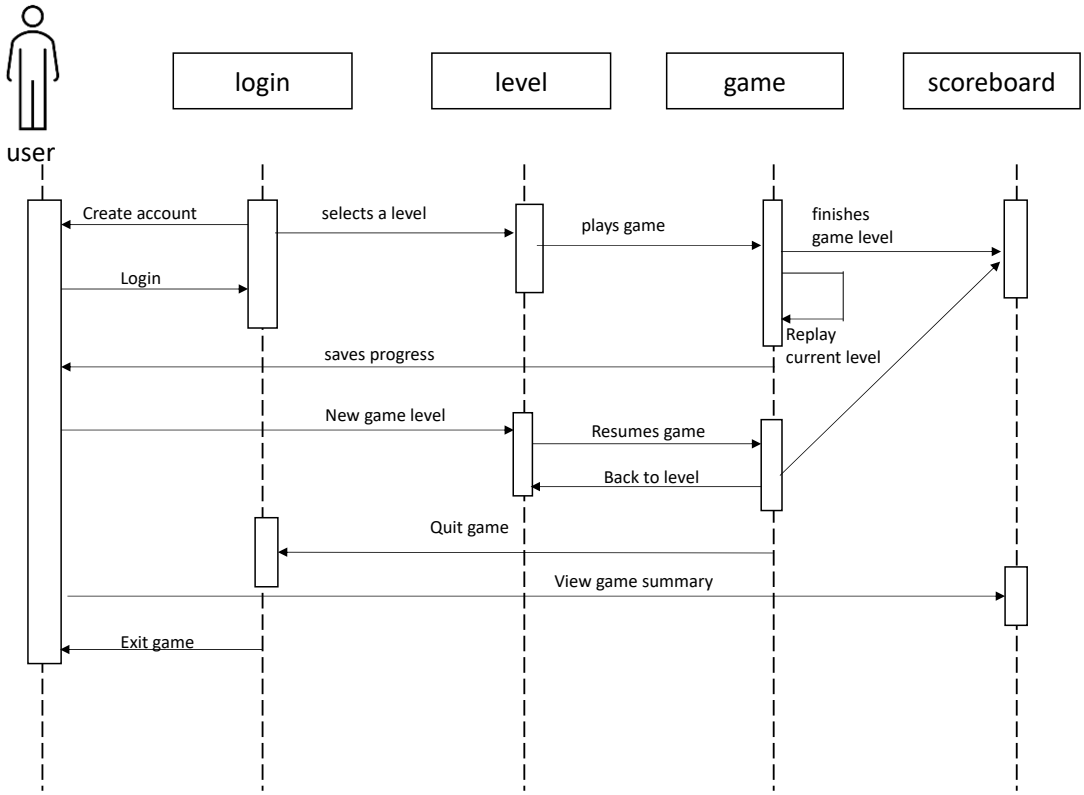
During the development of this game, we decided to use Unity software edition 2020 with the programming language C# Unity variant 2020 considers long term support (LTS) what's more, is accessible for nothing relying on the prerequisite that any incomes created stay beneath $100,000. Unity can make gaming conditions in two-layered conditions, however additionally three-layered, computer-generated simulation, and expanded reality.

This gives designers an assortment of decisions. The environment utilized in this game is three-layered. Also, Unity uses the C# programming language as it gives quick calculation times that the gaming environment needs to run without postponements or terminations to the game. The actual game has an assortment of activities which engineers can import from Unity Assets or Adobe Maximo. The two locales are online stores that have an assortment of free also, business liveliness and objects. Designers stick to the expectation that games it is not to utilize the free resources for-benefit games offered to shoppers. As this game is for research purposes, the game can use free resources from these depositaries. Structures inside the city environment come from different bundles from Unity Assets. These structures aggregate to emulate a bustling metropolitan region that holds a town hall, advanced criminology lab, and various sorts of designs.

All characters utilized in this game are from Unity Assets and Adobe Mixamo. The key character of the game is from Unity Resources, while the sounds produced and used come from Jimmy Vegas (A YouTube creator). This sound is likewise a free resource accessible to engineers and developers.

Figure 3

Sequence Diagram



Game Play Scenario

The game starts with a character appearing in front of a street with residential buildings upfront and can be seen from the camera angle. The character suddenly sees an arrow appear in front of a building a short walking distance from where his game play

begins. He walks to the tall storey building the arow is pointing on and gets in there to discover that in one of the apartments, there is a crime scene with some dead bodies and a couple of electronics such as a laptop, smart phone, hard drives and some usb flash drives and photographs in a separate room in the apartment.

When the character tries to grab the item for bagging and processing, he cannot and is shown a help icon that requires him to get a piece of document from the courthouse across the building to enable him to gather those evidence. The character goes into the courthouse to get the warrant as required by law, he gets there and is offered 2 options, a warrant to search and seize evidence in the living room or a warrant to search and seize the apartment. The character gets the warrant that stipulates the search and seizure of evidence found in the living room only. So, when the character returns to the apartment, he finds out that he cannot seize evidence found in the separate room in the apartment as he needs another warrant for that.

This time he goes back to the courthouse and gets a warrant that covers the entirety of the apartment which includes all rooms in that unit. When he goes back, he can pick up the remaining evidence in the separate room quickly with ease. Whilst, he was leaving with the evidence, he stumbled upon documents with financial records outside the apartment door, though this was outside his scope of warrant, he can retrieve this evidence which could be entered into evidence if found admissible because of the Plain view doctrine.

Now these missions are a timely based events and characters would also need to amass points to be able to buy more time as well as use points amassed to enable

them retrieve documents from the courthouse as it is a form of payment, due to the timely manner of the missions, characters are allowed to detour to allow for gathering points used for the game, without those points they cannot proceed with the mission. Also, players whilst in the game can use the littlest number of points gathered to ask for hints if they seem confused or lost. This way they are forced to gather more points as well as using those points for the mission.

To gather these points, they will be able to play side missions that includes but not limited to, puzzles, quiz, arithmetic calculations as well as basic conversions in binary or truth table conversions e.g. XOR, AND, OR Gates. For each answer failed, the question would offer an option to take away 1 wrong answer from a tablet of 4 options, to give the character a bigger chance of succeeding in the mission. For each gameplay finished, a new level unlocks which will be more challenging.

The essence of this gameplay is to teach the students the types of warrants, what the 4th amendment entails as well as the exception of the Plain View Doctrine. It also helps the students to learn about the basics of binary calculations and conversions.

Tools and Techniques

The tools and techniques required in this paper require knowledge of computer operating systems, digital forensics tools, and other imaging and auditing tools—the knowledge of the country's law where this research would be based.

Summary

In this chapter, we looked at the methodology required for this tool and proposed some important game features that would be important for the class of individuals we are focusing on in this paper. We also discussed appropriate components of the proposed tool that would encourage adherence to rules amongst other factors to consider. We tried to compare traditional learning methods to this proposed method, here we discussed some evaluation methods to encourage the students. The hardware and software environments needed for this tool were also extensively discussed with a list of components that would be attached to the game and categorized in 3 areas, namely, Pre-Requisites, Primary and Secondary areas of concentration. Also, a proposed sequence diagram was generated to guide the reader on how the gameplay would be carried out in the actual gameplay.

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, we are going to be gathering, comparing, analyzing, and interpreting the data gotten from the subjects who had a chance to test-run the proposed tool and filled out a two-part survey that covers the changes before and after using the proposed tool.

Data Presentation

Here, we have surveyed a set of twelve candidates, in a way to compare the results of the game played before and after use. For the evaluation, we targeted students who play games regularly; the reason is because they are the ones who would be enthusiastic about playing video games and can give us reliable feedback. These students are within the range of 17-21 years of age and quite familiar with a computer interface and knowledgeable as well.

We would also discuss scenes in the gameplay that reader through the first phase of the game, which includes the star and the end of the gameplay.

Pre-Game Survey

Figure 4

Survey showing number of students that play video games

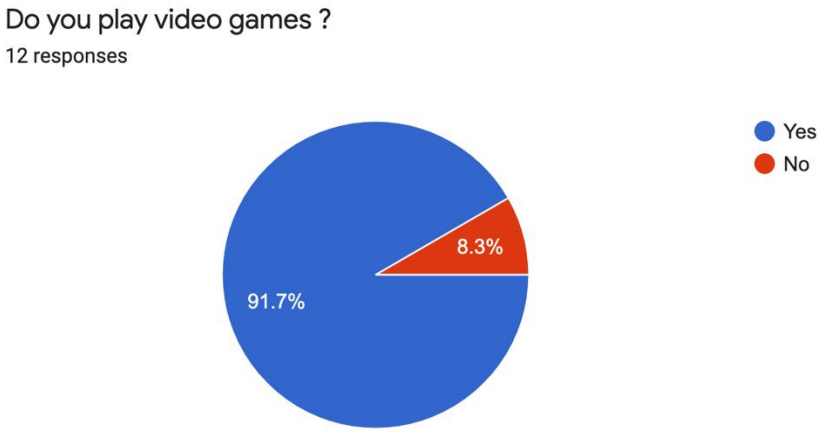


Figure 5

Survey showing number of students that has ever used video games to study

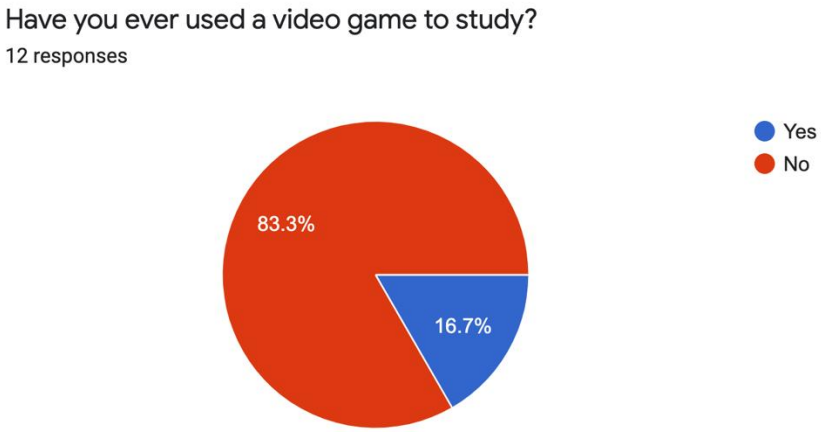


Figure 6

Survey showing number of students that know about digital crime scenes

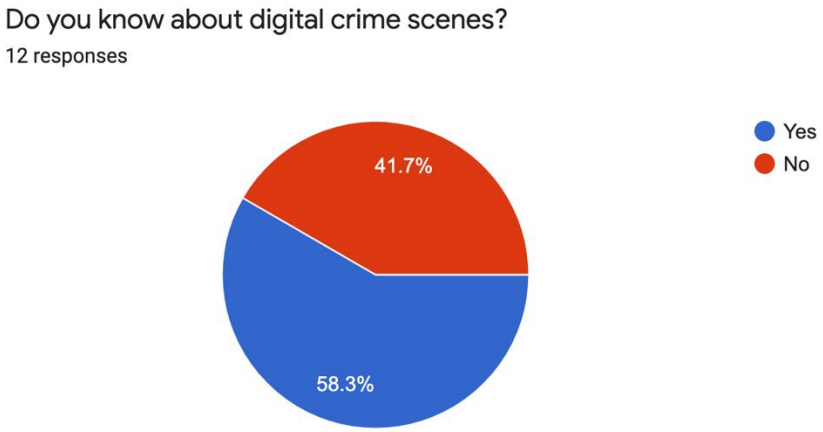


Figure 7

Survey showing number of students that know the concept of an evidence

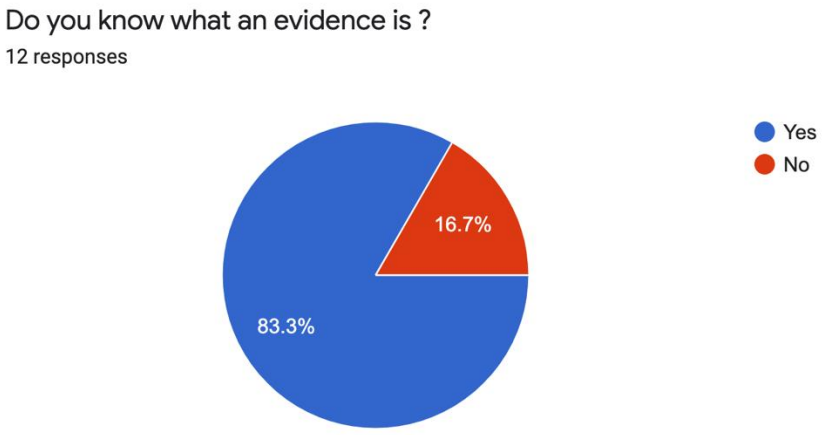


Figure 8

Survey that shows why evidence can't be touched or accessed at first glance

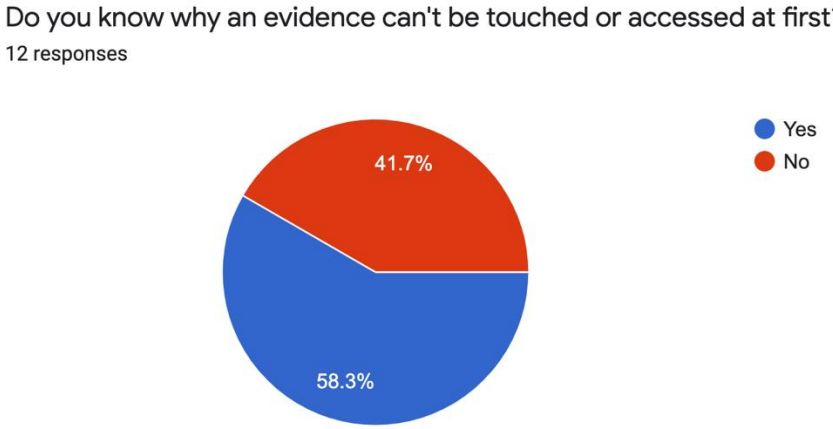


Figure 9

Survey showing the number of students that know about warrants

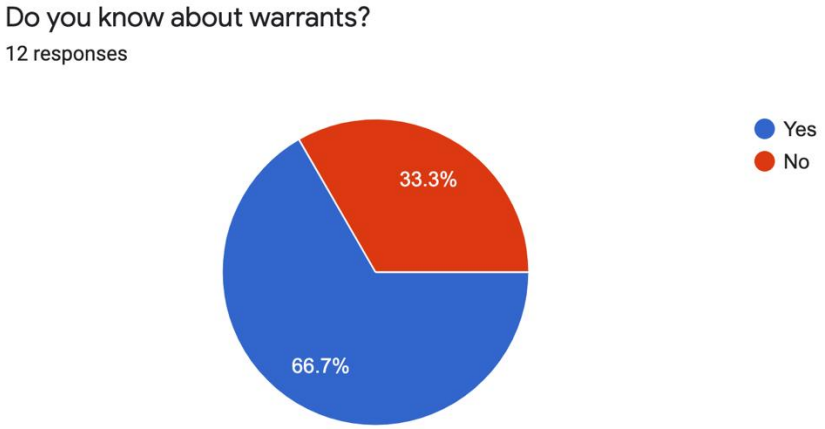


Figure 10

Survey showing number of students that know about specific types of warrant

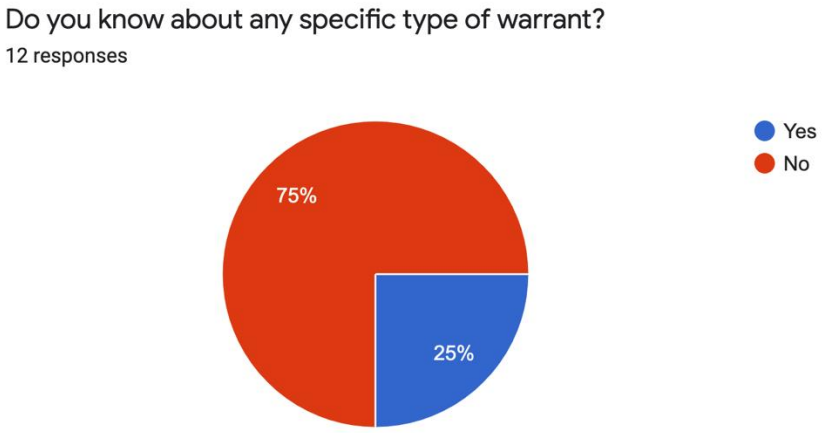


Figure 11

Survey showing number of students that know where warrants are obtained

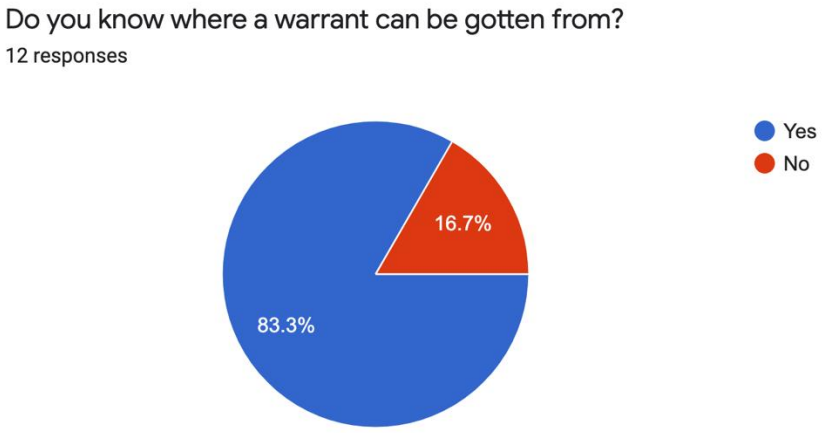


Figure 12

Survey showing number of students that know who needs a warrant

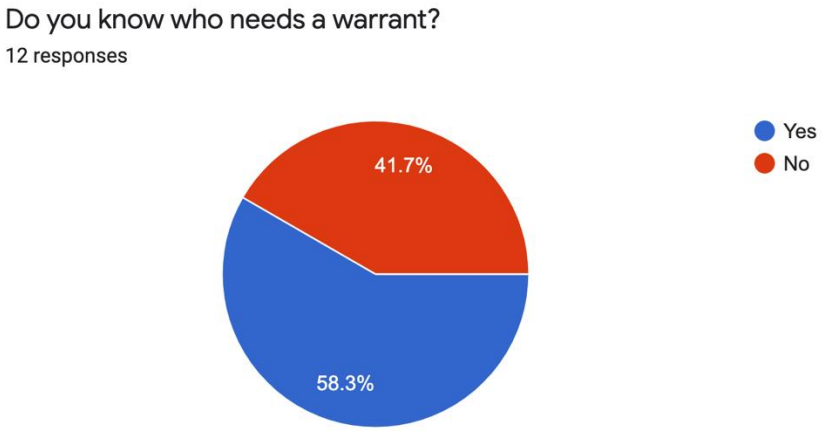


Figure 13

Survey showing number of students that know the specifics contained in a warrant

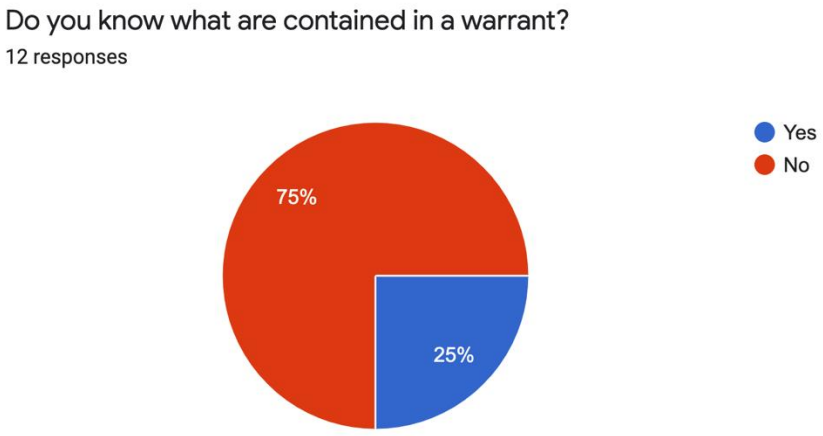
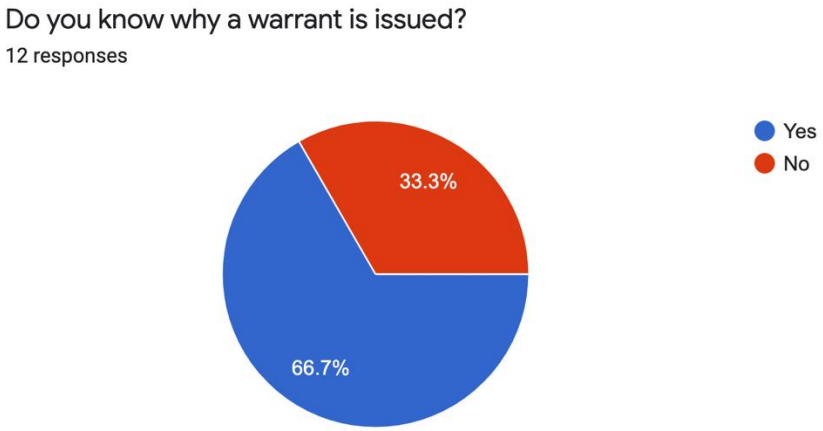


Figure 14

Survey showing number of students that know why a warrant is issued



Post-Game Survey

Figure 15

Survey showing number of students that agreed the game was interactive

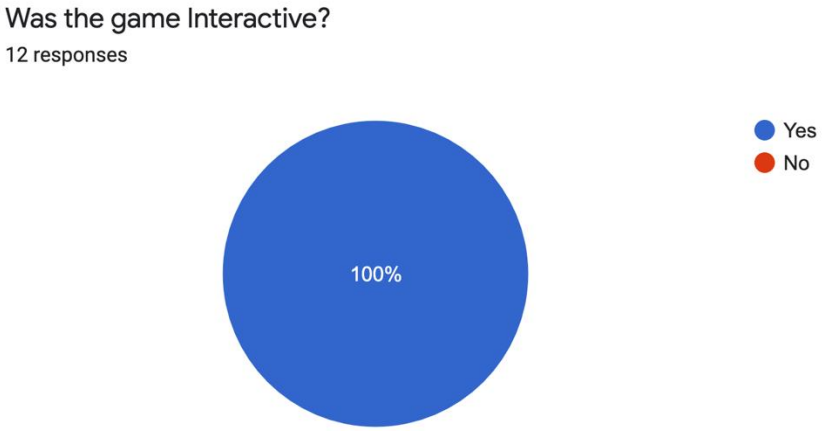


Figure 16

Survey showing number of students that now know what evidence is

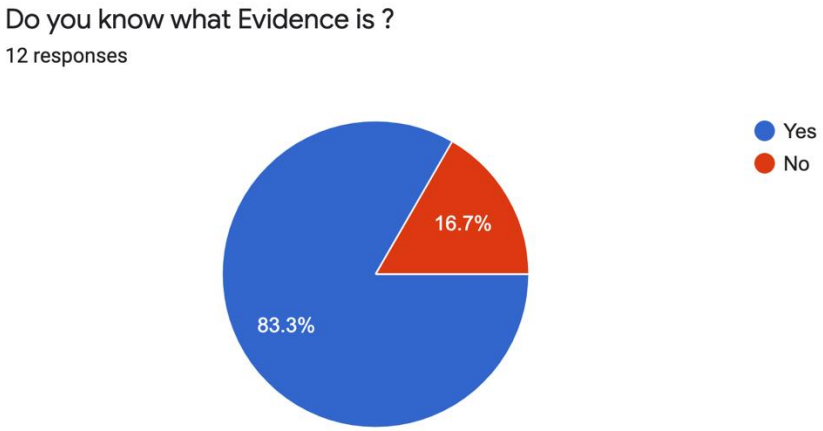


Figure 17

Survey showing number of students that now know about crime scenes

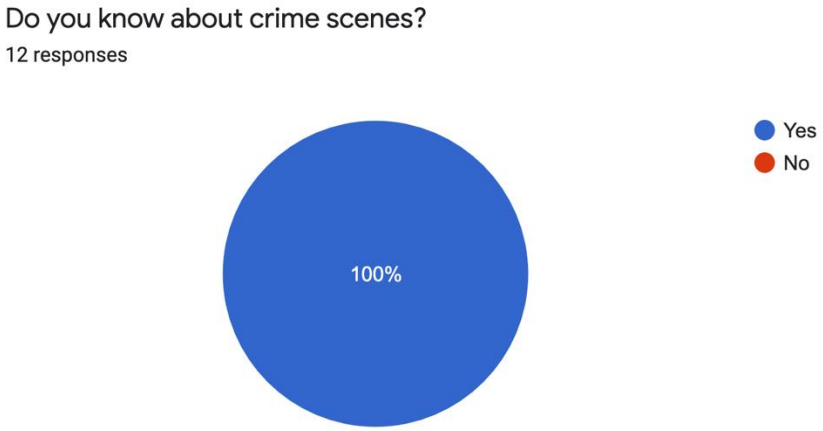


Figure 18

Survey showing number of students that now know about warrants

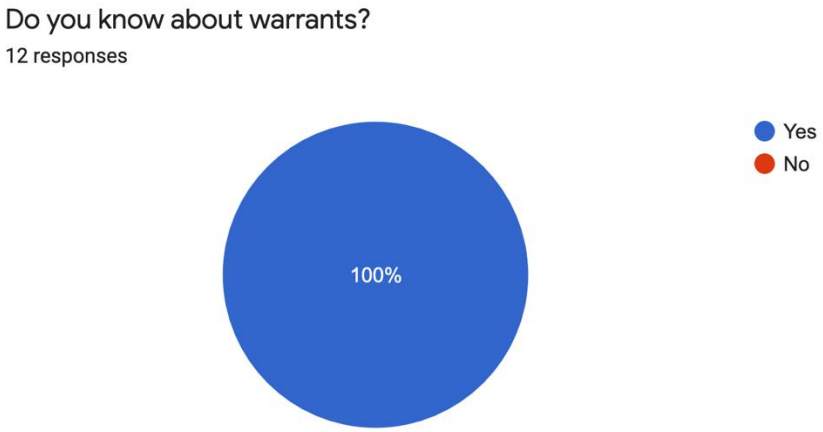


Figure 19

Survey showing number of students that now know what are contained in a court warrant

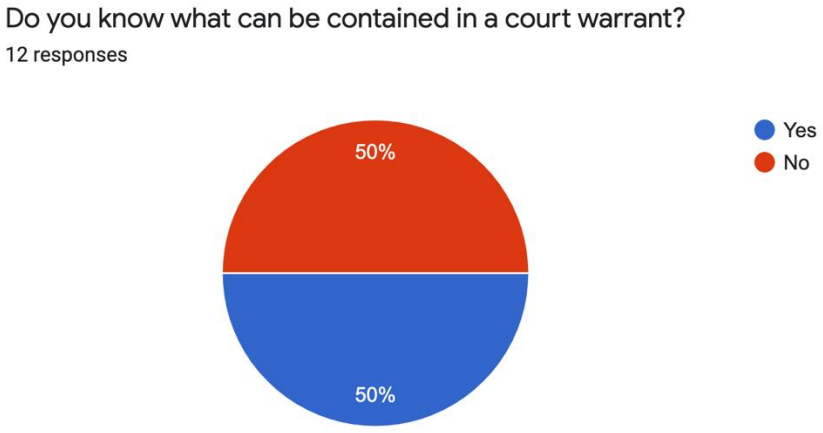


Figure 20

Survey showing number of students that agree the game was attractive

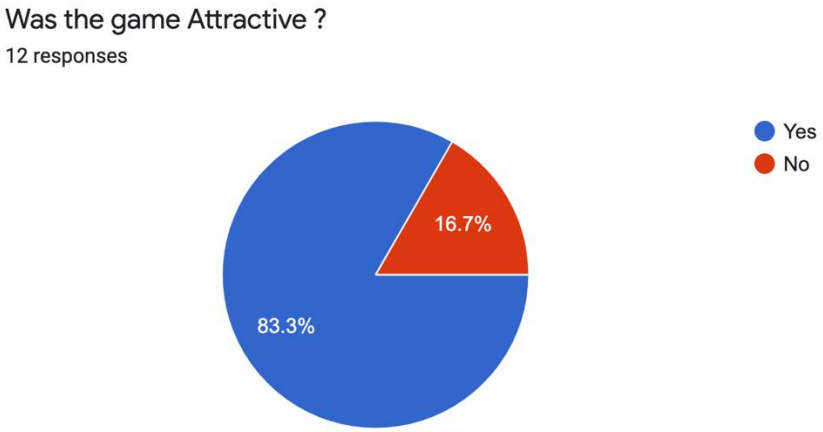


Figure 21

Survey showing number of students that admitted to gaining knowledge from the game

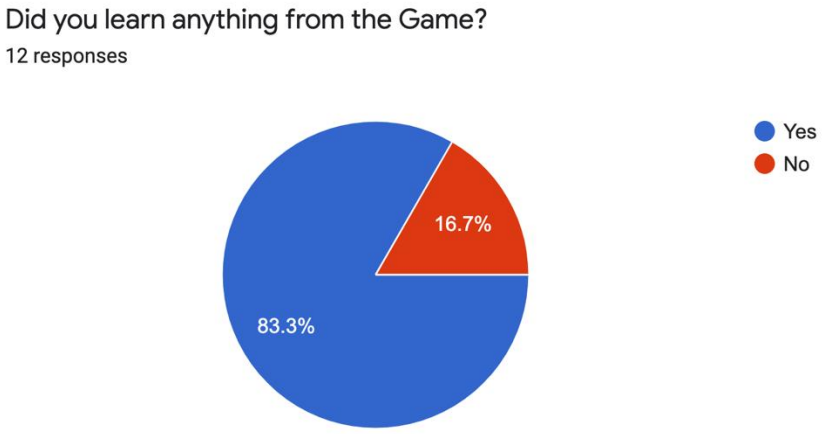


Figure 22

Survey showing number of students that agreed to achieving the goal of the game

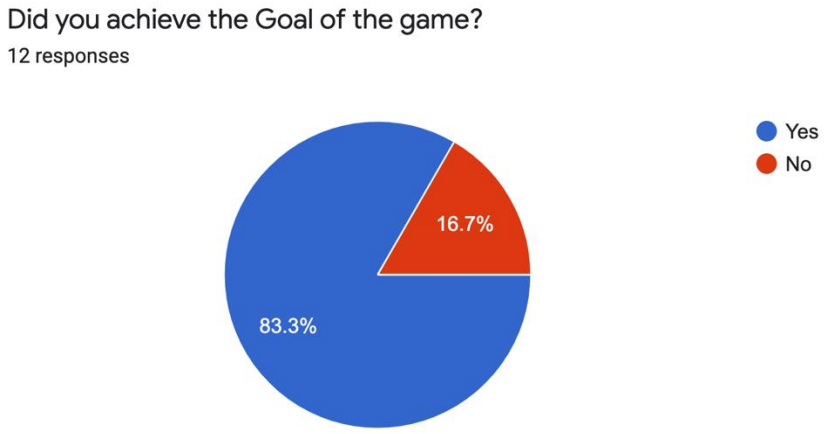


Figure 23

Survey showing number of students that agree that the rules are important in the game

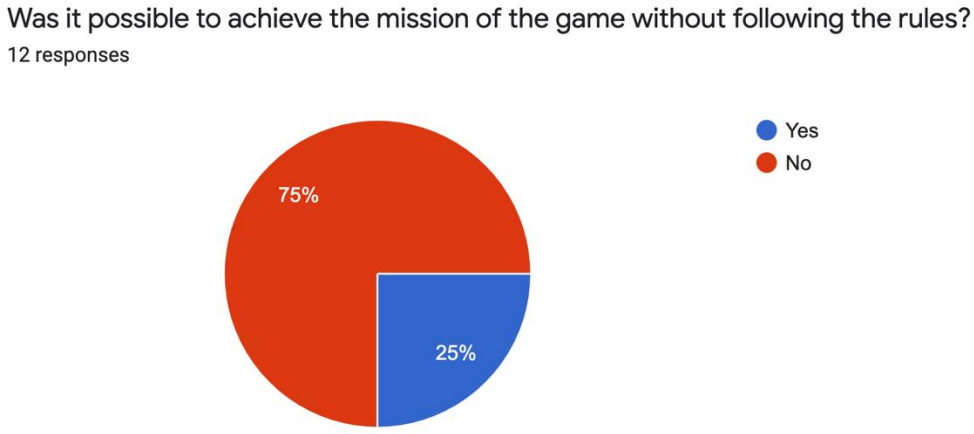


Figure 24

Survey showing number of students that now why warrants are issued

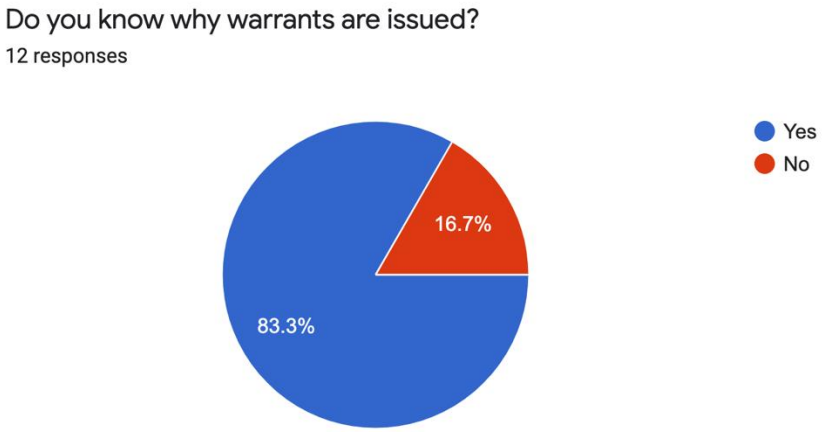


Figure 25

Survey showing number of students that now know why warrants are usually not similar

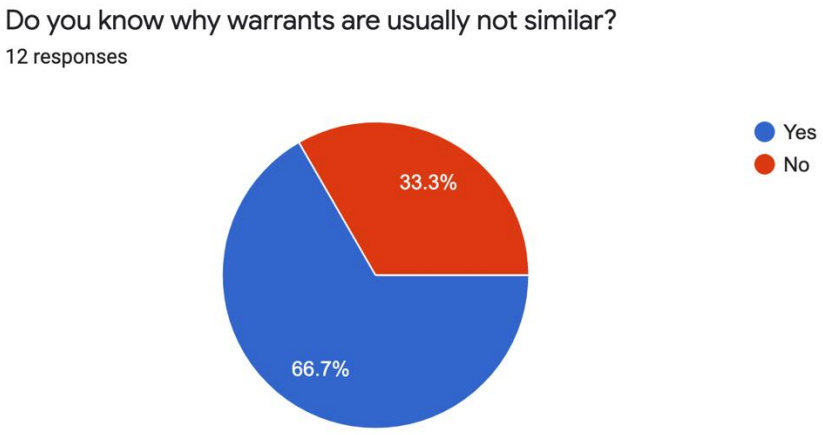


Figure 26

Survey showing number of students that now know where warrants can be obtained

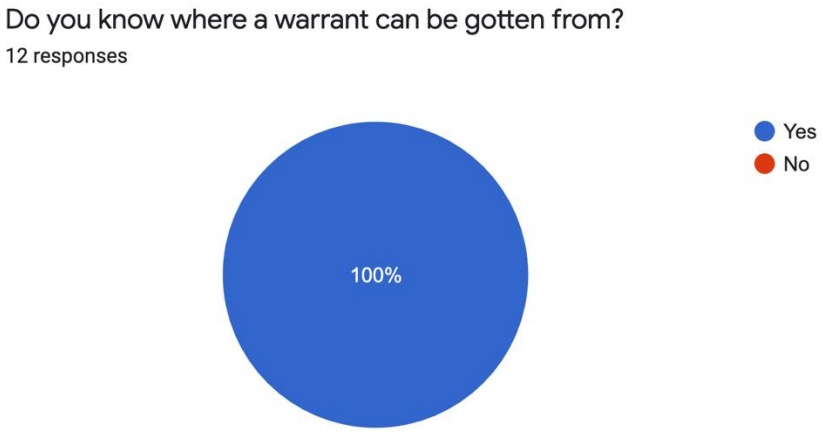
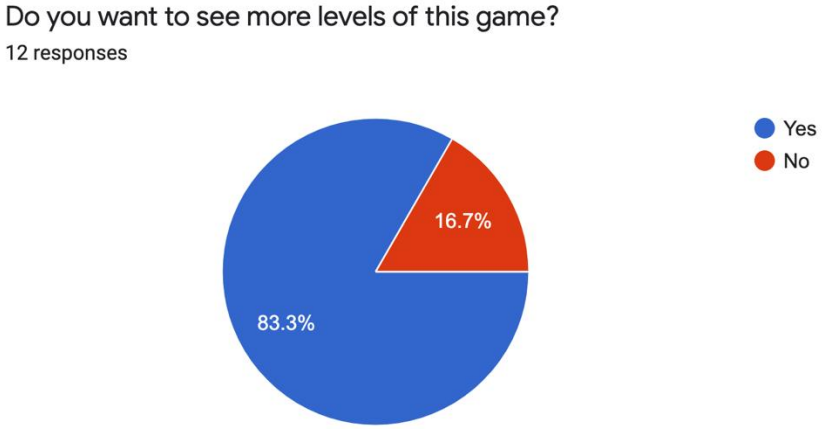


Figure 27

Survey showing number of students that want to play more levels of this game



Data Analysis

Here in this **Error! Reference source not found.** the survey analysis talks about if the student, that is, the twelve candidates who we picked, played video games and if they liked playing video games. **Error! Reference source not found.** talks about the possibility of using video games to study and if those candidates have ever used video games to study prior to this project proposal. **Error! Reference source not found.** questions if the students know about digital crime scenes and if at all they have ever heard about it or been in one before. And as you can see, the ratio of those that know about digital crime scenes are more than those who do not know.

Error! Reference source not found. talks about evidence - what is evidence, what explains evidence, what exactly do they know about evidence regarding a crime scene or a scenario that involves crime.

Error! Reference source not found. discusses why evidence cannot be touched or accessed first. Here, the candidates are being asked if they know why evidence cannot be touched or accessed at first. The question suggests that in this phase, we are going to be talking about warrants.

The question leads the students to **Error! Reference source not found.** which now talks about warrants. And in this figure, the twelve students were asked about warrants and 66.7% of them said they know about warrants, which leaves the 33.3% of students not knowing about warrants.

Error! Reference source not found. talks about if they know about a specific type of warrant regarding the list of warrants out there in a civil or criminal case. 75% of

students suggest that they do not know about any specific type of warrants. There are types of warrants that can go from search and seizure to only search warrants depending on the validity of the crime involved and the scope of jurisdiction.

The next one, **Error! Reference source not found.** talks about if the candidates have any knowledge about where warrants can be gotten from. That is, do they know where warrants are from, who issues warrants and what is the process of getting warrants in a civil or criminal case. 83% of respondents affirm that they know where a warrant can be gotten from, leaving 16% of them not knowing where a warrant can be gotten from.

Error! Reference source not found. emphasizes if the students know who needs a warrant; that is, do they know who needs a warrant, why do they need a warrant because for a warrant to be issued, someone must need it. And for someone to need a warrant, a particular crime scene must be in the process of being investigated. So, the question that suggests, “Do you know who needs a warrant?” was asked to know if the students know who needs a warrant.

Another question in **Error! Reference source not found.** is, “Do you know what are contained in a warrant? In this question, most of the students - about 75% of them say they do not know what is contained in a warrant. 25% of them affirm that they know what is contained in a warrant. This suggests that the multitude of the candidates have no idea what is contained in a warrant.

The next one **Error! Reference source not found.** states, “Do you know why a warrant is issued?” and here, the students say they do not know why. This explains that

the students have no knowledge about the issuance of a warrant. 66% of the students say they know why a warrant is issued, which means they know that a warrant exists, and they know why it is issued, they just do not know what it contains - with regards to the previous image. It is worthy to note that all these questions were being asked in a pre-game survey. For the post-game survey, the results were interestingly positive in the most part of it. 100% of the students in **Error! Reference source not found.** stated that the games that they just played were interactive which solves one of the questions in the theory.

The next one **Error! Reference source not found.**, which suggests if the students now know what evidence is. 83% of the students affirm that they now know what evidence is, and they only know about it because they have used the tool which was provided for testing to learn about what a warrant is.

The next question **Error! Reference source not found.**, “Do you know about crime scenes?” 100% of the students now know what a crime scene is. By playing the game, they were able to see about two to three crime scenes and what those crime scenes contained.

Error! Reference source not found. suggests, “Do you know about warrants?” tests the students’ knowledge of warrants as well as the components of warrants. For this question, 100% of respondents said they now know what a warrant is.

Here in **Error! Reference source not found.** the survey suggests, “Do you know what is contained in a court warrant?”- to this, some of the students still found it difficult to know what is contained in a court warrant while other students were aware. The

decision was evenly split, which means half of the respondents knew what a court warrant was as well as the components of a warrant and half of the students did not know what a court warrant contained.

The next image **Error! Reference source not found.** gives an answer to one of the questions asked, which is if the game was attractive. 83% of the students affirmed that the game was attractive, which means that they found the game to be interesting and it could be inferred that for the game to be attractive, they really liked everything that was contained in the game.

The next question that **Error! Reference source not found.** poses suggests, “Did you learn anything from the game?” 83% of the students stated yes which suggests that this is an avenue to be utilized around education because the candidates suggested that they really learnt something from the game.

Error! Reference source not found. talks about if the candidate achieved the goal of the game. 83% of the student say that they achieved the goal of the game and 16% of the student differed from this opinion.

Another question **Error! Reference source not found.** that came up was if it was possible to achieve the mission of the game without following the rules. 75% of the respondents answered in the negative which goes to show that the rules of the game are set up in a way that makes it impossible for the students to cut corners. This means the students must follow the mission play extensively to get to the goal of the game.

Another question that came up previously is in **Error! Reference source not found.** , “Do you know why a warrant is issued?” which the 12 candidates, after playing the game in **Error! Reference source not found.**, selected that they now know why a warrant is issued. 83% of them positively suggested that they now know why a warrant is issued and 16% of them suggested that they do not know why a warrant is issued. In comparison to the previous pre-game survey questions, the responses show that the students now know why a warrant is issued.

Another question that came up is in **Error! Reference source not found.**, “Do you know why warrants are usually not similar?” - the students were perplexed by the question because 63% of the students responded that they now know what warrants are not similar and that is because warrants are different given the scope of the search and the jurisdiction of the crime. And as such, a particular warrant is not issued if it does not cover extensively what areas of specification the person requesting the warrant is asking for. The person requesting the warrant must suggest what areas to be covered before a warrant is issued, which is the reason why warrants cannot be similar in different crime scenarios.

Another question is in **Error! Reference source not found.**, “Do you know where a warrant can be gotten from?” - 100% of the student say yes, they now know where a warrant can be gotten from which usually a courthouse in any is given state, city, country, or town.

The final question that **Error! Reference source not found.** displays was, “Do you want to see more levels of this particular game?” 83% of students said yes, they

would like to; this suggests that this number of students enjoyed the game play and what it had to achieve for them.

In all, the post-game result shows an increase in knowledge ability and interest as opposed to the pre-game survey that was issued to the students.

Game Play Analysis

The game play starts off with an opening scene where the Player character walks into a crime scene and then goes to meet up with his boss who asked for him to come analyze a crime scene. Here in **Error! Reference source not found.** the player is being told to “Get to work and secure the scene” which is a key knowledgeable area the student ought to know in understanding the basics of Digital Forensics investigation.

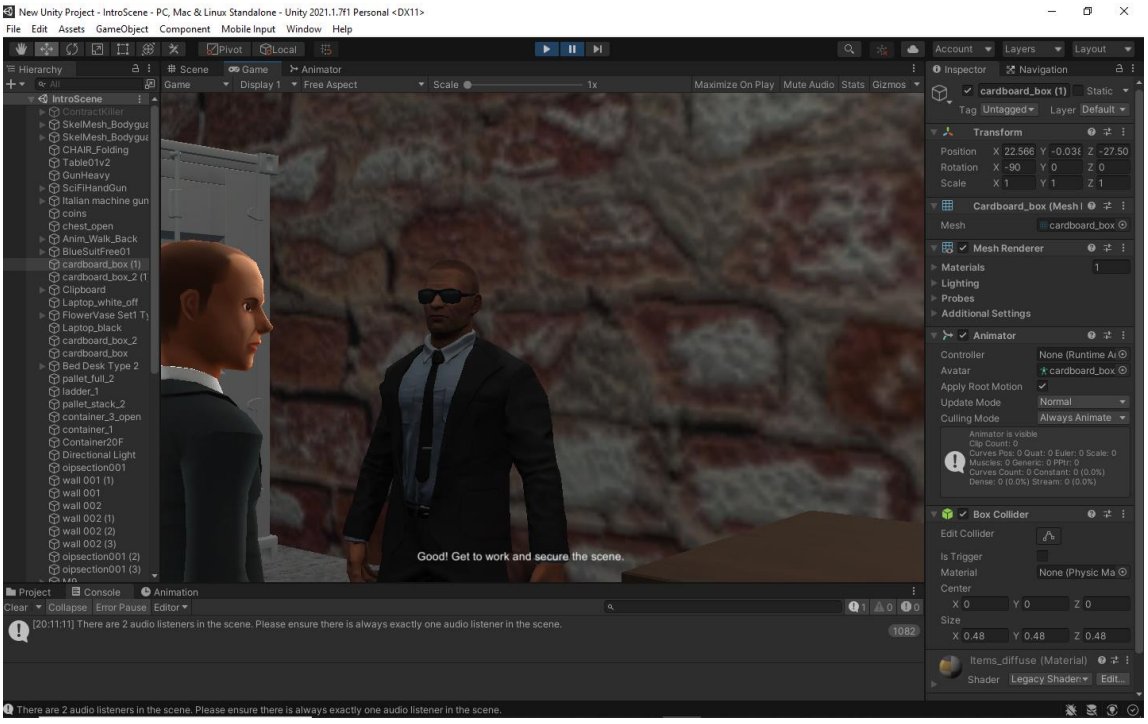
The next scene starts off with the player walking into a mission start point which is indicated by a glowing circle on the floor. It is programmed to trigger a command when the player steps into the trigger zone. The command informs the player of the need to go to the nearby courthouse to secure a warrant to begin the process of securing and bagging the evidence for investigation. In **Error! Reference source not found.** the player must get to the mission start point else they would not be able to start off the objective of the game. The mission start point is the catalyst that starts off the game and ensures that strict instructions are adhered to.

Then the player gets to the courthouse where he picks up the first available warrant there that explicitly says in **Error! Reference source not found.** that “This warrant is only for the container” which goes to explain that there are certain warrants

for certain investigations and this warrant only covers a particular place within a larger environment. This key lesson is also important for the students to know.

Figure 28

Image of the player character and his boss



Now that the player has gotten his warrant, the next objective is to go to the crime scene, upon getting to the crime scene in **Error! Reference source not found.**

an NPC which acts as a trigger point, informs the player that “His warrant does not have any jurisdiction past this point”, which ultimately means the player would have to go back and carefully go search and pick up the right warrant that covers all the necessary essential parts of the crime scene in a much larger scale.

Figure 29

Image of the Key Character prior to his mission play

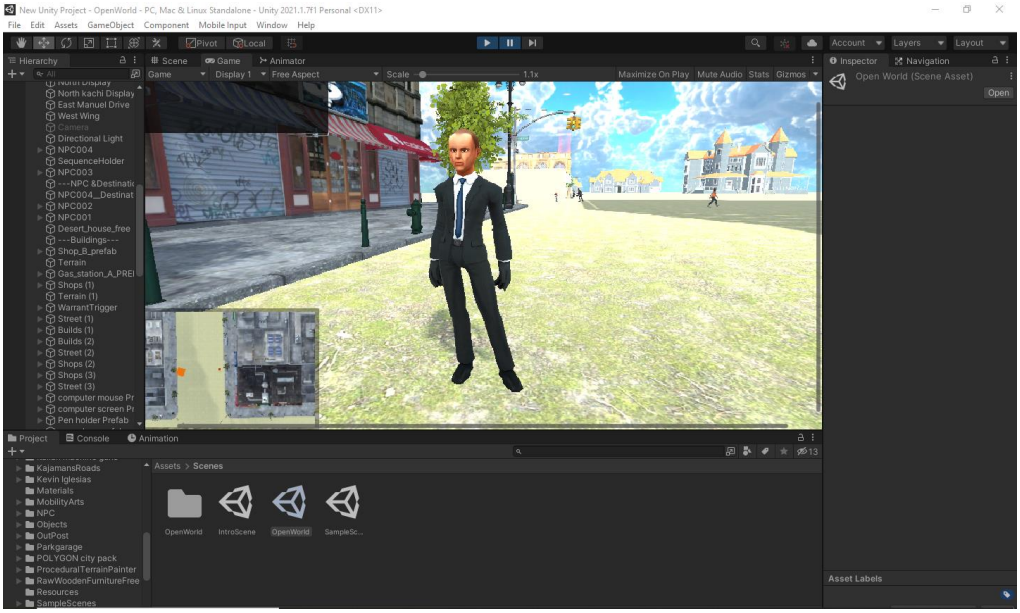


Figure 30

Image of the Key Character receiving instructions mandatory for the game play

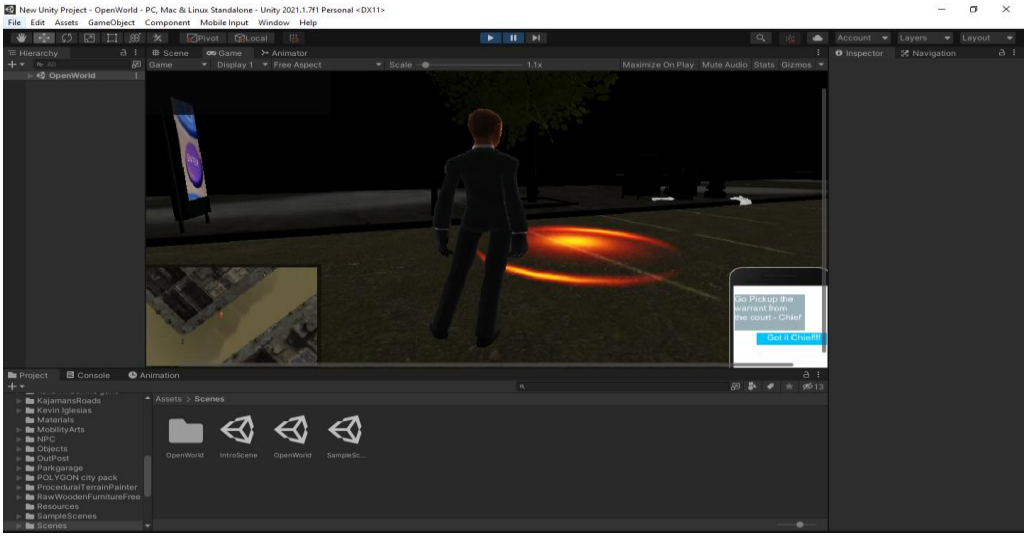

New Unity Project - OpenWorld - PC, Mac & Linux Standalone - Unity 2021.1.7f1 Personal <DX11>
File Edit Assets GameObject Component Mobile Input Window Help
Hierarchy
OpenWorld
Scene Game Animator
Game Display 1 Free Aspect Scale 1.1x Maximize On Play Mute Audio Stats Gizmos
Inspector Navigation
Go Pickup the warrant from the court - Chief
Got it Chief!!
Project Console Animation
Assets > Scenes
KajamansRoads
Kevin Iglesias
Materials
MobilityArts
NPC
Objects
OutPost
Parkgarage
POLYGON city pack
ProceduralTerrainPainter
RawWoodenFurnitureFree
Resources
SampleScenes
Scenes
OpenWorld
IntroScene
OpenWorld
SampleSc...

Figure 31

Player currently at a designated spot to pick up a warrant

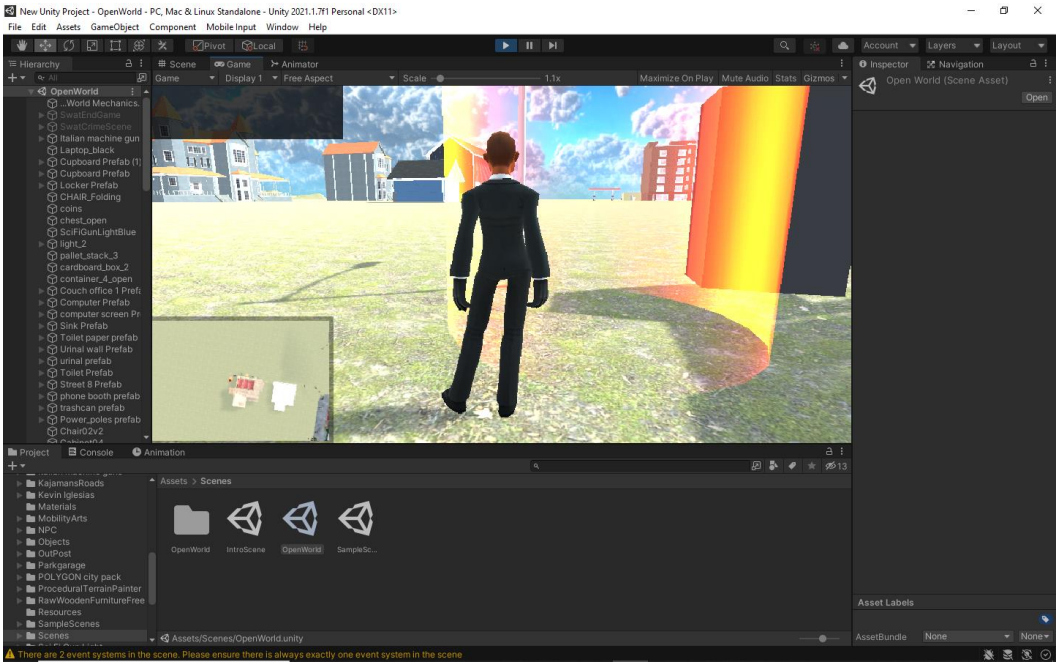


Figure 32

Player gets a warrant to a specific location only

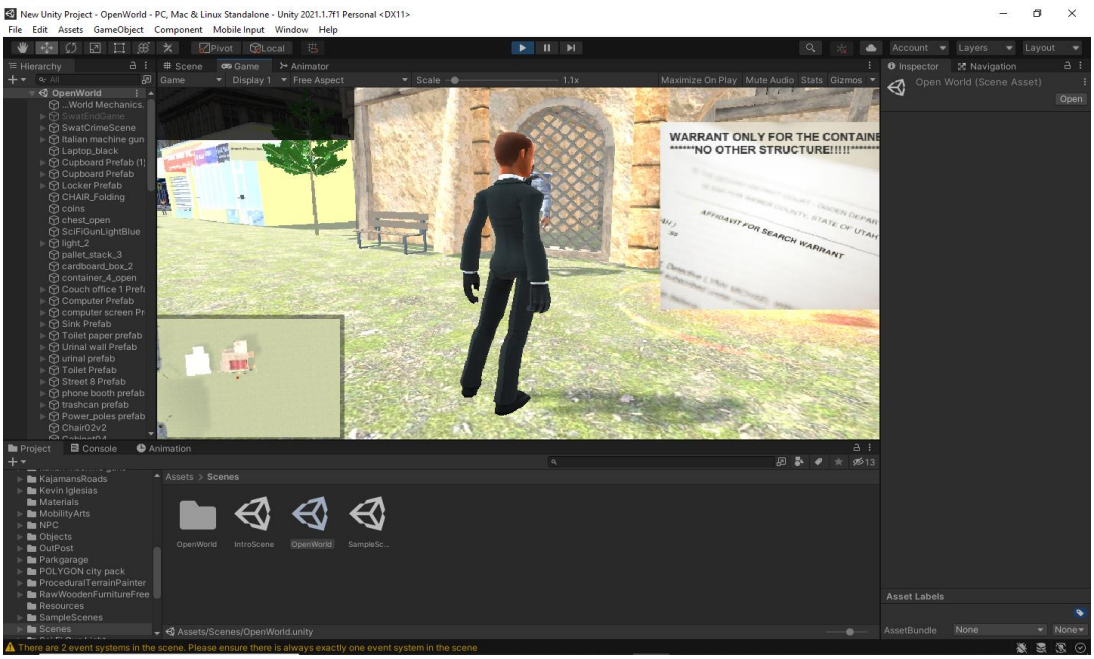


Figure 33

A non-character Player reminds player their warrant has no jurisdiction in another area of the crime scene

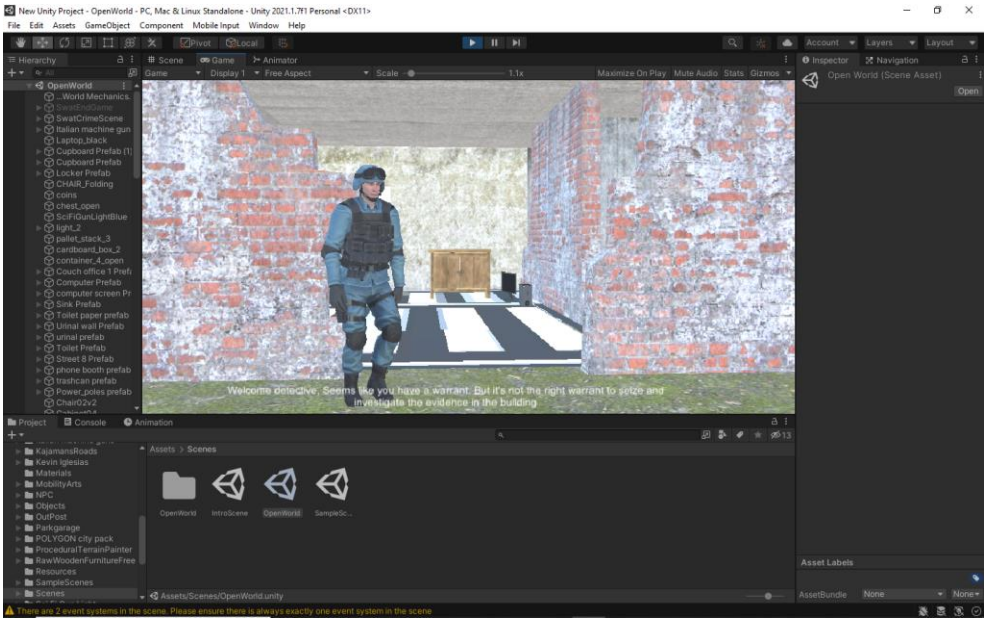


Figure 34

Player has arrived at the crime scene and are ready to start bagging the evidence

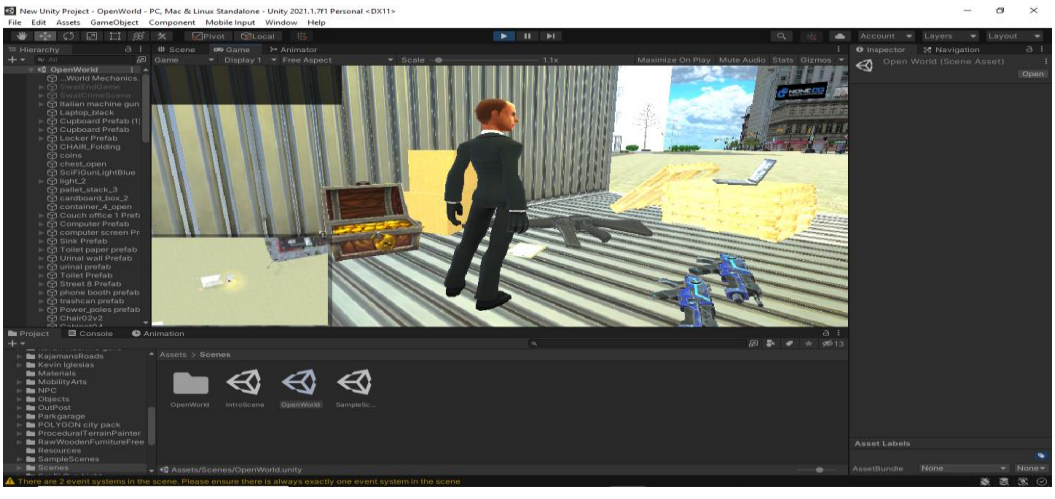
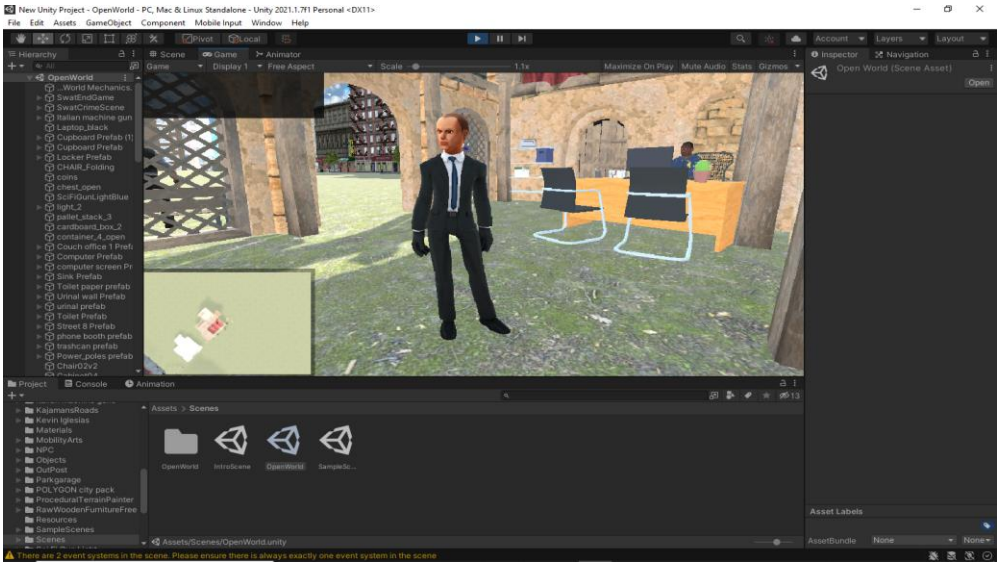


Figure 35

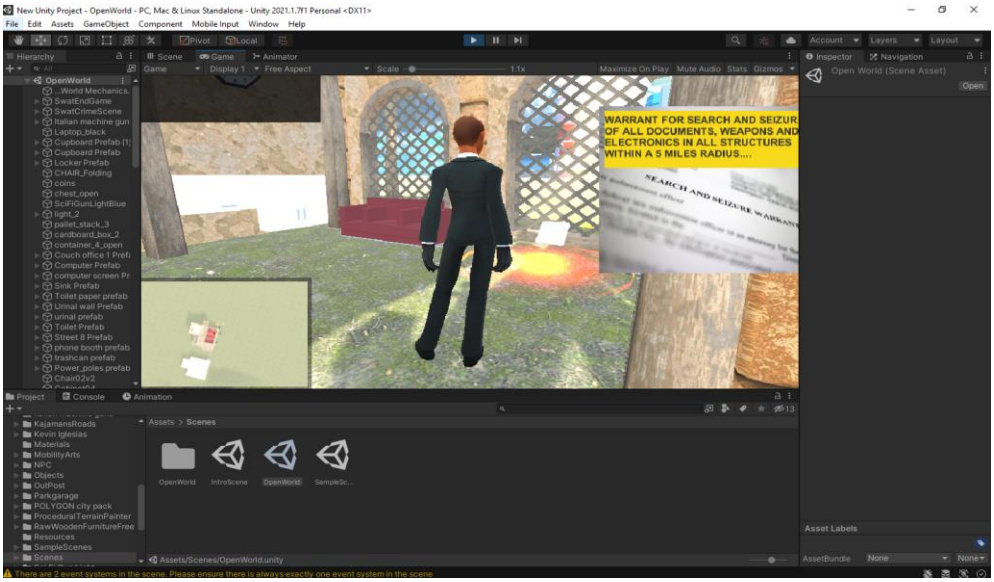
Player heads back to the courthouse to pick up another warrant



In **Error! Reference source not found.** we see the player has gone back to the courthouse to search for the right warrant to continue his mission objective of securing the evidence for analysis.

Figure 36

Player has picked up a warrant that allows for search and seizure in a larger scale



In **Error! Reference source not found.** the player is seen with a warrant that says “Warrant for search and seizure of all documents, weapons and electronics in all structures within a 5 miles radius”, this warrant essentially enables the player to go back to the crime scene just as we can see in **Error! Reference source not found.** and inspect all the evidence lying around and then bag them accordingly whilst making sure he maintains chain of custody to prevent evidence tampering. It is at this phase of the game that the current level ends with the player successfully completing the mission objective of securing the crime scene by following the instructions accordingly.

Evaluation Environment

Another point worthy of note is that the candidates chosen to play this game were 12 in number. They were gotten from several high schools within Minnesota and Texas State. These 12 students were high school students who have a very good knowledge of computers, hardware, and software for their age grade. The students

were placed in front of the proposed educational tool and were shown the buttons to use during the game play. Each of the students had about 35 minutes of game play because they did not understand some of the terminologies on the screen. Due to that, they needed some assistance navigating the game environment.

Summary

Conclusively, in this chapter, we discuss the survey questions, we also discussed how the students had a wonderful time playing this game and as the survey suggested, they want to see more levels of this game because they feel that the game has so much to offer to them and, it taught them a whole lot more than they initially anticipated. The players are penalized and rewarded in such a way that if they do not follow the rules and the mission of the game play, they would not achieve the results at the end of the game. The game is built in such a way that no one player can cut corners or go to a crime scene without first visiting the courthouse. To add to this, no player can go to the courthouse just once and get the warrant because the first time a player goes to the courthouse, he gets a warrant for only search. So, the player needs to go back to the courthouse after he has visited the crime scene to get a second warrant for search and seizure, without which the player would not finish the game play. The players are somewhat penalized by not finishing the game play if they do not follow the instructions of the game. Furthermore, we walked the readers through the game play with screenshots to guide them through the process of objectively securing the evidence by following due processes Digital Forensics expert ought to follow.

Chapter V: Results, Conclusion, and Recommendations

Introduction

The final chapter of this paper draws up the conclusion of this paper from previous chapters. It will then look at the process, testing frameworks, results or conclusions before providing any recommendations in the field of research.

Results

Earlier in this paper, in Chapter III, methodology aims, and objectives were set out; this chapter will look at the solutions on how to greatly increase the number of digital forensics field by finding more modernized way of educating young students within K-12 and above on the concepts of digital forensics as well as cybersecurity.

The main objectives at the start of the paper were to answer each of the following questions.

- Will the game approach help in this case? Why?

Yes, gaming approach has been used previously in teaching more complex concepts in other fields and has yielded good results through the result verification process of the experiments. We strongly believe this game approach would help in this case as it still has room for more additional learning modules that foster engagement and retention, these are key attributes of active learning.

- What game models for education are there?

There are numerous game models for education, a few were discussed earlier by some research authors as well as cybersecurity companies. Kaspersky Interactive

Protection Software (KIPS) is one of them, owned by Kaspersky Security firm. CyberCeige is another model proposed by the Naval Postgraduate School Center for Information Systems Security Studies and Research. Anti-Phishing Phil was developed to create awareness on email services protection as well as phishing attacks. VR-Engage is also a gaming model that functions via virtual reality environments using special Virtual Reality Headsets, this model studies difficulties in students' engagement and provides adaptive solutions to those problems.

- What game models suit Digital forensics education, and why?

Any number of the previously stated models can be adopted to provide learning modules which could be adopted for Digital Forensics. Meta, parent company for Facebook and its other subsidiaries are heavily investing in alternate worlds using Virtual Reality, so VR-Engage would be best suited as it adapts newer technology in solving existing problems whilst ensuring passive engagement is achieved.

- How to implement a gamified digital forensics Educator and measure its effectiveness?

As previously demonstrated in the last 2 chapters, we can implement these gamified digital forensics educator as a learning tool applicable within a curriculum which would be used to account for active listening as well as comprehension from the parts of the students. Also, to measure its effectiveness, the results at the end of the gameplay would allow educators to analyze and conclude what parameters of comprehension each student has difficulties on.

Conclusion

To conclude, the objective of this study is to make this domain/career path which is Digital Forensics interesting to students in the K-12 because we want to target them at this age so that when they go to college, we want them to be interested in doing cybersecurity and digital forensics. The main aim was to provide a rather unorthodox way of teaching digital forensics and cybersecurity using a gamified environment to achieve that. Further down, we looked at a detailed literature review that will be used in creating a testing framework.

In Chapter II we looked at past concept of education through gaming as an approach. We also looked at how the use of games in educational systems helps students evaluate themselves. Further down, we see how education through gaming helps students develop and grow the cognitive, intellectual, psychological, and social skills that will help them make the right decisions in their next phase of life. The academic resources incorporated on this paper are Science Direct, ACM, Research gate, IEEE Explore amongst others all had their focus on Gamified education as an alternative to teaching.

Chapter III literature review we looked at the methodology required for this tool and discussed appropriate components of the proposed tool that would encourage adherence to rules we then tried to compare traditional learning methods to this proposed method, here we discussed some evaluation methods to encourage the students. Extensively discussed were a list of components that would be attached to the game.

The final reports were presented in Chapter IV data presentation and analysis where outcomes, and we discuss the survey questions, how the students had a wonderful time playing this game and as the survey suggested, they want to see more levels of this game because they feel that the game has so much to offer to them and, it taught them a whole lot more than they initially anticipated.

After reviewing these articles related to the topic, this essay was able to identify and produce a solution that was first designed in Chapter III and then tested with the primary focus demography which yielded positive response in Chapter IV. Though the gamified tool is designed to fit other topics of fields of career that mostly involves conceptualizations and hands-on experience.

Future Work

While working on this paper with the support provided by my advisor, I was able to finally conclude my Thesis Paper by using well known research databases such as Google Scholar, IEEE Explore, ACM, Elviser to find relevant and up-to-date articles related to the main topic which is a gamified approach to teaching Digital Forensics and cybersecurity.

As we earlier discussed in Chapter I, there is a huge decline in Digital Forensics Experts in the industry. Thus, there are often mix-ups and backlogs in the legal department due to this shortage of experts. My recommendation would be to enhance this game with more detailed missions and quizzes that would both expose them to the

concepts of Digital Forensics, legal aspects of Digital Forensics as well as incorporation elements of E-Discovery as well in the game.

To make it more interesting, perhaps the game could have components that allows for multi-player online experience to allow for multiple individuals to work on a mission play together whilst learning at their own pace.

The game could essentially be improved to ensure the norm of teaching is positively tilted towards the side of adopting gamified approach in learning in curriculums.

References

Adams, C. W. (2008). Legal issues pertaining to the development of digital forensic tools. *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, 123–132. https://doi.org/10.1109/SADFE.2008.17

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1), 5–14.

Arachchilage, N. A., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706–714. https://doi.org/10.1016/j.chb.2012.12.018

Boddington, R. (2016). *Practical Digital Forensics*. Packt Publishing Ltd. Bureau of Labor & Statistics. (2019). *Information Security Analysts*. https://www.bls.gov/oes/current/oes151212.htm#st

Chen, W., Wu, W., Wang, T., & Su, C. (2008). Work in progress—A game-based learning system for software engineering education. *2008 38th Annual Frontiers in Education Conference*, T2A-12-T2A-13. https://doi.org/10.1109/FIE.2008.4720349

Coffey, H. (2014). *Non-Digital Game-Based Learning in the Teaching of Mathematics in Higher Education—ProQuest*. https://search.proquest.com/openview/dce3a3903c59e126f24d7756209d0ac6/1?pq-origsite=gscholar&cbl=396495

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

Craiger, P., Swauger, J., Marberry, C., & Hendricks, C. (2006). Validation of Digital Forensic Tools. In *Digital Crime and Forensic Science in Cyberspace*; IGI Global. https://doi.org/10.4018/978-1-59140-872-7.ch005

Eubanks, N. (2017, July 13). *The true cost of cybercrime for businesses*. Forbes. https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/?sh=3de6f12f4947

Farber, M. (2013, June). *Beyond Badges: Why Gamify?* Edutopia. https://www.edutopia.org/blog/beyond-badges-why-gamify-matthew-farber

Filsecker, M., & Hickey, D.T. (2014). A multilevel analysis of the effects of external rewards on elementary students' motivation, engagement and learning in an educational game. *Computers & Education, 75,* 136-148. https://doi.org/10.1016/j.compedu.2014.02.008

Forensics Colleges. (2020). *Computer Forensics Salary & Job Outlook—CCE, CCFE, GCFA Careers*. Forensics Colleges. https://www.forensicscolleges.com/careers/computer-forensics-examiner

Gondree, M., Peterson, Z. N. J., & Denning, T. (2013). Security through play. *IEEE Security Privacy*, *11*(3), 64–67. https://doi.org/10.1109/MSP.2013.69

Holland, B. (2013, May). *You Got Game? – EdTech Digest*. https://edtechdigest.blog/2013/05/28/you-got-game/

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Javidi, G., & Sheybani, E. (2018). K-12 Cybersecurity Education, Research, and Outreach. *2018 IEEE Frontiers in Education Conference (FIE)*, 1–5. https://doi.org/10.1109/FIE.2018.8659021

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game based Cybersecurity Training for High School Students. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 68–73. https://doi.org/10.1145/3159450.3159591

Kleman, M. (2013, May 1). *The Debate: Gamification and Education*. TechnologyAdvice. https://technologyadvice.com/blog/information-technology/debate-gamification-education/

Kourtis, A. (2020). *Raising information security awareness: The role of gamification*. https://doi.org/10/21153

Lai, P. C. (2017). The Literature Review of Technology Adoption Models and Theories for the Novelty Technology. *Journal of Information Systems and Technology Management*, *14*, 21–38. https://doi.org/10.4301/s1807-17752017000100002

Lee, J. (2011). *Gamification in Education: What, How, Why Bother?* https://www.academia.edu/570970/Gamification_in_Education_What_How_Why_Bother

Li, C., & Kulkarni, R. (2015). *Cybersecurity Education through Gamification*. https://www.asee.org/file_server/papers/attachment/file/0006/8254/CTF_Gamification_submission.pdf

Marquis, J. (2013, April). *Debates about Gamification and Game-Based Learning (#GBL) in Education – Classroom Aid*. https://classroom-aid.com/2013/04/07/debates-about-gamification-and-game-based-learninggbl-in-education/

Money, W., & Turner, A. (2004). Application of the technology acceptance model to a knowledge management system. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2004.1265573

Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations*. Cengage Learning.

Pan, Y., Schwartz, D., & Mishra, S. (2015). Gamified digital forensics course modules for undergraduates. *2015 IEEE Integrated STEM Education Conference*, 100–105. https://doi.org/10.1109/ISECon.2015.7119899

Roussev, V. (2011). Building Open and Scalable Digital Forensic Tools. *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 1–6. https://doi.org/10.1109/SADFE.2011.3

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches

people not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 88–99. https://doi.org/10.1145/1280680.1280692

Labor Statistics, L. (2020). *BLS*. Retrieved from U.S. Bureau of Labor Statistics: https://data.bls.gov/search/query/results?q=cyber+security+2020

Twitchell, D. (2007). SecurityCom: A Multi-Player Game for Researching and Teaching Information Security Teams. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2007.1029

Yerby, J., Hollifield, S., Kwak, M., & Floyd, K. (2014). *Development of Serious Games for Teaching Digital Forensics*. *15*, 9.

Zax, R., & Adelstein, F. (2009). FAUST: Forensic artifacts of uninstalled steganography tools. *Digital Investigation*, *6*(1), 25–38. https://doi.org/10.1016/j.diin.2009.02.002