DEVELOPMENT OF SERIOUS GAMES FOR TEACHING DIGITAL FORENSICS

Johnathan Yerby, Middle Georgia State College, johnathan.yerby@mga.edu
Sarah Hollifield, Middle Georgia State College, sarah.hollifield@mga.edu
Myungjae Kwak, Middle Georgia State College, myungjae.kwak@mga.edu
Kevin Floyd, Middle Georgia State College, kevin.floyd@mga.edu

ABSTRACT

Digital forensics is a rapidly growing and emerging field in information security. The need for digital forensics experts is expected to continue to grow over the next ten years to respond to ever growing incidents of cybercrime. The field of digital forensics is complex and requires a diverse set of skills through expensive specialized tools. In an effort to strengthen the digital forensics workforce, institutions of higher education are expanding or creating new programs to fill the business, military, and law enforcement needs in the upcoming years. This study proposes the use of video games as a hands-on active learning tool to increase awareness, make the complex field approachable and fun, as well as provide learning and training experiences that would otherwise be impractical or dangerous for learners to experience in a traditional laboratory setting. A review of the current literature on serious games and the Gamification of learning suggest that game-based learning can be effective at engaging students and successful in training students to become future professionals in the areas of information security and digital forensics. Finally, this paper outlines design and development of a digital forensics interactive (DFI) video game using the Unity game engine and Blender.

Keywords: Digital Forensics, Serious Games, Gamification

INTRODUCTION

According to the 2014 U.S. Bureau of Labor Statistics, the job growth for private detectives and investigators for the next ten years is average with an 11% growth rate. The field of information security, which includes digital forensics, has a job outlook for a 37% growth rate over the next decade. There are expected to be 27,400 new jobs in information security, 700 new jobs in forensic science technicians, and 3,300 new private investigators [24]. The field of digital forensics is nested within information security, but also weaves through forensic science, investigators, and criminal justice. New college programs are starting to develop to create the workforce that will meet the needs of government, business, and law enforcement. One method to engage and recruit students into this complex field of digital forensics is to use video games. The use of video games provides a training environment where players have the ability to make mistakes without the serious repercussions of botching a real investigation. Gamification of learning is a popular method in complex fields where mistakes could be very expensive or life threatening. The name of this video game is Digital Forensics Interactive (DFI). This paper describes the arguments for creating a digital forensics video game, the process and tools used to build the 3D environment, the scenario that the player will encounter, and the discussions about future research.

Gaming and simulations are great tools to allow learners to work in typically high risk situations without the serious risks. Maintaining integrity of the investigation is a crucial tenant of working in the field of digital forensics. It would not be feasible to allow novice students to begin working on a real life active investigation due to the possible risks that the learner would be exposed to. Students may encounter offensive material that students should not be exposed to such as pornography or confidential company information that an organization would not want a group of untrained investigators to have access.

There are multiple information assurance, risk management, and information security games available for free and paid versions that companies use for training, schools use for teaching, and individuals use just to enhance their skills and knowledge. A search for a game based option to learn more about digital forensics returns only two results. The first result is an idea paper to create a digital forensics game [25]. The model that Pan et. al. describe requires a connection to a real computer environment that uses real forensics tools. Their model requires the player to be on the same network and that the resources being utilized to be available for the player including expensive recurring software licensing. The second result for digital forensics games is Mark Lane’s LOGS Project
H.U.M.A.N. In Project H.U.M.A.N. the player starts by sending a text message and gathers information through any tool that they wish to use. The game is designed to be a massive multiplayer game with no right or wrong way to solve the case of a wronged retired CIA agent. Lane’s game goes beyond the process of a digital forensics investigation to more of a cinematic thriller by having players solve zodiac diagrams, becoming involved with a drug dealer, deciphering secret languages and riddles. The game was advertised to be released in September of 2013, but as of May 2014 the game is delayed and planned for a July 2014 release [20]. The model that this paper proposed was to create a stand-alone digital forensics training game that will allow players to run without being dependent on connecting to a specific network or machine. The game will be self-contained and run from several different platforms. This game will be different from Project H.U.M.A.N. in the way that this game provides guidance, feedback, and scaffolding to the learner. This serious game will be designed with a point system that will allow players to replay the single scenario multiple times while trying to solve the case and earn a higher score than their previous attempt. The game being developed in this paper is a game that can be useful for teaching, training, and increasing awareness.

The expected results from this project will be one of the first video games available for digital forensics. Educational institutions will be able to use this game to enhance security or forensics courses in an information sciences curriculum. This game will demonstrate how the field of digital forensics is not just complex and time demanding, but also interesting and fun. Gamification of learning is an increasingly popular method to teach and train users in a complex field that would otherwise be dangerous, expensive, or boring for students. This study uses gamification of learning using Unity to create the 3D environment where the digital forensics investigation is conducted.

REVIEW OF LITERATURE

Serious Games

In recent years, serious games have become a topic of interest among researchers as serious games are being used as effective tools for educating, motivating, and changing behavior [29]. According to Susi, Johanneson, and Backlund [32], serious games are digital games that are used for purposes other than entertaining. Serious games use instructional and video game elements for non-entertainment purposes. Serious games attempt to create pedagogically sound and relevant learning experiences for a wide variety of audiences and industries [9].

Serious games are an increasingly important medium with respect to education, training, and social change [23]. Research indicates that games may become more effective than other educational technologies and traditional pedagogy in engaging students and supporting active learning [28, 29]. Gee [16] reported that serious games can be effectively used to facilitate deep and sustained learning. Research conducted by Connolly, Boyle, McArthur, Hainey, and Boyle [11] found that the use of serious games had many positive impacts with respect to learning, skill enhancement, and engagement. The research also found that there was a link between playing computer games and a range of perceptual, cognitive, behavioral, affective motivational impacts and outcomes. Given the positive impacts of serious games in teaching and learning, it can be argued that such games are being increasingly used in educational settings, thus creating a gamification of learning.

Gamification of Learning

The term gamification has been broadly defined as the use of game design elements in non-game context [13]. Gamification is also used to describe the use of serious games to improve the user experience and user engagement [14]. Gamification includes using game-like elements in non-game contexts to promote learning and engagement and help an individual engage in problem solving [19]. Gamification has found its way into domains like marketing, politics, health and fitness, with analysts predicting that it will become a multi-billion dollar industry by 2015 [22].

Gamification is also making its way into education as a means of helping to motivate and engage students in the learning process. The effectiveness of games for learning or instructional games has been evaluated against the solutions available for instruction both at a college and K-12 schools. Cataloglu [8] utilized a computer simulation solution in undergraduate physics classes focusing on vector algebra. The author used pre-and post-test scores to evaluate the effectiveness of the educational software that provided several benefits for learners, including the ability to study the related topics outside of the classroom in groups. In a different study, Ljungkvist & Mozelius
The work in this study follows the framework and definitions that were created by Carrier & Spafford [7]. This study used the definitions detailed in the Carrier & Spafford as specified in the following:

- **Digital data** are data represented in a numerical form. With modern computers, it is common for the data to be internally represented in a binary encoding, but this is not a requirement.
- A **digital object** is a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a process.
- A **digital event** is an occurrence that changes the state of one or more digital objects. If the state of an object changes as a result of an event, then it is an effect of the event. Some types of objects have the ability to cause events and they are called causes.
- An object is **evidence** of an event if the event changed the object’s state. This means that the object can be examined for information about the event that occurred. However, future events could cause an object to no longer have information about past events. Every object is evidence of at least one event, because there had to be an event that created the object.
- An **incident** is an event or sequence of events that violate a policy and more specifically, a **crime** is an event or sequence of events that violate a law.
- In particular, a **digital incident** is one or more digital events that violate a policy.

Gamification has been found to foster more interaction in the classroom and leads to more student engagement. Additionally, Iosup and Epema [18] found a correlation between gamification and the percentage of students passing the course, and in the participation in voluntary activities and challenging assignments. In a study conducted by Dominguez et. al. [15], gamification led to better experiences in practical assignments and in overall assignment scores, but the students performed poorly on written assignments and participated less in classroom activities. Gamification can enhance collaborative learning environments in online learning environments by help improve the learning experience and performance for groups of students [3]. One area in the discipline of Information Technology that can benefit from the gamification of learning is information security and digital forensics.

**Games in Security and Digital Forensics**

Gaming in the area of information assurance and risk management has had recent success to train future professionals in each of the fields as well as a more interactive way to have non-security related employee’s complete training. There are numerous compliance rules and regulations that require employees in a variety of positions to complete training annually or bi-annually. Providing training through the use of gaming correlates with more engaged employees who in turn correlate with a higher awareness of information assurance policies [24, 27]. Increasing end user awareness and caring about security issues is a large part of the challenge for information security professionals. The United States Department of Defense’s Defense Information Systems Agency (DISA) has been using security games for the last couple of years. Military, federal civilians, and contractors are required to complete a security game as a part of their training and compliance. Some of the games that these employees must complete are **CyberProtect** [34], and **Cyber Awareness Challenge** [12]. Other popular security games include **CyberCeige**, which was developed by the Naval Postgraduate School Center for Information Systems Security Studies and Research [10]. There are even non digital information assurance games such as the free to use **d0x3d** and a flash card type of game from Symantec [17]. **StrikeCom**, developed by the Center for the Management of Information at the University of Arizona is similar to **Digital Forensics Interactive**, as the player completes predefined phases of an investigation [34]. **DFI** is different in the game play aspect where **StrikeCom** is a multiplayer online game dedicated to conducting military operations. With games related to network security being a popular method to teach new professionals or to increase awareness, the need for serious games in the field of digital forensics is apparent especially since there are currently zero offering available.

**Framework**

The work in this study follows the framework and definitions that were created by Carrier & Spafford [7]. This study used the definitions detailed in the Carrier & Spafford as specified in the following:
In response to an incident or crime, an investigation may begin. An investigation is a process that develops and tests hypotheses to answer questions about events that occurred. Example questions include:

- “what caused the incident to occur”
- “when did the incident occur”
- “where did the incident occur”

**DESIGN AND DEVELOPMENT OF DIGITAL FORENSICS INTERACTIVE (DFI)**

Unlike other software, games contain both rules and goals. Rules are instructions that dictate how to play and goals are particular objectives that can be achieved from playing the game [2]. The goal of the game is usually defined by the rules. The rules typically include the following items: game semiotics, game-play, sequence of play, goals of the game, and termination condition [2]. The goal of our game is to provide a training environment where players can obtain the fundamental knowledge of digital forensics through learning by doing method. Therefore, the game rules has been designed and aligned to effectively achieve the digital forensics training purpose.

Designing and developing a game is an exciting but time consuming process. Considering the objectives of our game, the game rules have been carefully designed in advance and other factors such as programming language, cost, and skills of the team also have been taken into account before moving forward into development. After the main idea and goals were decided in advance, a comprehensive storyboard was created to depict the idea of what the game should look like. As the game rules have been refined further, the in-game assets, characters, and environment has been obtained and developed.

For effective game design and development, it is important for game designers and developers to become familiar with the tools and programming language used to construct the game. For this game, Unity [35] was chosen as the game development tool since it is an extremely powerful game engine capable of creating 2-dimensional and 3-dimensional games for a nearly every gaming platform. For programming language, Unity allows for C#, JavaScript, and Boo scripts. The language chosen should be one that best fits the programmer and project at hand. For this project, C# was used because developers are most familiar with the language.

The essential building blocks of the game environment are called 3D models or assets. They could be newly developed or imported from pre-built packages. The Unity has its own online asset store where pre-built objects and scripts are available for free or for a price. For DFI, an office furniture package was bought and various other free packages including character and animation packages were used to create the office building and characters. Also the 3D assets of digital forensics tools were created by a 3D modeling tool, Blender [4], and imported into the game environment.

After the 3D models and assets were attained, actual implementation of the game-play and the sequence of the game was started according to the game rules. Unity is not easy to learn at first but the Unity site provides developers with an extremely extensive scripting guide and set of tutorials on their website, ranging from subjects such as the user interface to navigation and more. Additionally, the user base is large enough that other developers have created tutorial videos and additional resources to consult if the official documentation is not enough.

An initial version of DFI has been already constructed and the game-play and the sequence of the play are currently being tested and adjusted. The development team plans to iterate the development cycle two or three times more to enhance the game and incorporate other effective gaming features, such as various levels of challenges and actions and new user interface. Once it is fully developed, it will be tested against students majoring in digital forensics.

**GAME-PLAY**

The game-play consists of the challenges and actions the game offers players and the sequence of the game is the progression of activities that consists of the game. The challenges and actions have been carefully designed and implemented to achieve the goal of the game. The sequence of the game was devised to maximize the training effectiveness in that the player can try the tasks repeatedly until they completely obtain the fundamental knowledge.
In our game, DFI, the player is immersed in a 3D game environment in which they begin understanding the type of case they will be conducting by interviewing management that has requested the investigation [35]. The player enters the civil investigation case by clicking the begin button with their mouse and they are greeted by a character that thanks them for coming down so quickly to investigate. The character representing management of the Cheadle & Associates, is Jason Hill. Mr. Hill explains that the suspect Marsellus Wallace has just left for a one week vacation and that they suspect has committed two serious offenses. The first offense that Mr. Wallace is suspected of doing is using company resources to run his private Bed and Breakfast during work hours. The second and more serious allegation is that Wallace has copied customer information from the company owned customer relationship management system and he is preparing to leave the company to work for the competition. After the player has been given a description of the situation surrounding the investigation, the instructor will ask the player a series of questions. Questions will be used in this manner many times throughout the game to test the player’s understanding and knowledge of digital forensics practices and procedures. All inquiries will be written in a multiple choice format. Upon choosing the correct answer, the player will either be given another question or a task to perform.

This first set of questions is meant to test the player’s knowledge and memory on the purpose of this investigation. When the player answers all of them correctly, the next portion of the game will be loaded. If the player answers incorrectly, the questions will be repeated until the correct answers are chosen. Mr. Hill will give the player feedback related to the incorrect answer that was selected so that students playing the game will still be learning important concepts related to the field even when they do not select the best answer.

After the player has completed their interview with Jason Hill, the player is asked to identify the sources of possible information throughout the office the suspect works in. The office is the setting of the game and there will be objects available to select and study throughout the room. The player is able to move around the room, select, and read about these sources. As items are selected the player will be asked how they will handle this piece of media. The student will be able to: 1) leave the item and state that it would not be a part of the investigation, 2) ask Mr. Hill more questions about select items, 3) add to their list of evidence to be acquired, 4) turn on the device and begin looking for evidence. The fourth option is designed as an incorrect choice, where the player will be reminded about the tenant of integrity in an investigation. If the player were to power on the device and begin investigating it would compromise the investigation since the evident would lose nonrepudiation. As the player moves around and identifies and reads about the correct sources of information, a running count of the devices to identify will appear on the screen in a workbox area. When every device has been identified, the player will click on the button that indicates that they have completed the data identification phase. If a player has identified all of the devices that should be related to this investigation they will proceed to the next step. If the player selected items not needed for this investigation they will be presented with feedback that explains how lengthy a digital forensics investigation can...
be and that selecting items not related will lengthen their investigation. The player will be given an option to exclude some of the selected items in their workbox. If the player indicates that they have completed their data identification, but missed items they will be provided feedback that directs them to return to gather some of the missed items. Mr. Hill will test the player’s knowledge of the previously identified devices in the same multiple choice fashion as before. For the story to continue, the must answer all questions correctly.

When the player has answered these questions correctly, Mr. Hill will instruct him or her on the next step in the investigation process: preserving digital evidence. There will be some instances for the player to choose a false-positive and proceed with their investigation by just losing points. The preservation of digital evidence will include the player handling the correct tools, such as the laptop, external hard drive, and forensics field station provided, to copy all relevant data for processing. Actions inside the game may include the handling of tools such as an external hard drive and attaching it to the appropriate devices. Students will have the option of acquiring evidence using a variety of tools from a simple write blocker, to a more sophisticated unit such as the WiebeTech Ditto Forensic field-station [5]. The player will be allowed to move through the office and find the area with the investigative devices and will be required to perform the correct procedures with the correct tools to back up the data and investigate any information found. If any actions are inappropriate, an error will display and the player must repeat the action until the correct sequence is performed, or if the mistake does not halt the entire investigation points will be lost. Only when the player has accomplished all required activities will they move on to the next step of analysis.

When the use of tools and information gathering is finished, the player will once again return to Mr. Hill for another multiple choice quiz about digital forensics tools. The player will be presented with simulated digital forensics software such as Access Data Forensic Took Kit and Tech Pathways ProDiscover [1, 33]. The player will be able to click on pieces of evidence to mark as: 1) Not relevant to the investigation, 2) Flag to come back later, 3) Flag as not direct evidence, but it should still be included in the final report, 4) Indicate relevant to the investigation and add to final report. As before, if the player misses a question they will have to keep repeating them until all are correct. When this happens, Mr. Hill will reveal the next instruction.
The game will continue in this fashion until all information is collected in the proper manner and the investigation has been completed. The last phase of the game will require students to write a final report using an included template and evidence that they have selected previously. The student will indicate when they have completed their final report by clicking on submit report to management. The full paper report will be displayed to the player to review once more and they will have the option to go back to revise or confirm that the report and investigation have been completed.

If the student completed the investigation correctly, Mr. Jason Hill will return to the player and thank them for all of their hard work. The player is promoted from investigator to Chief Forensics Officer with a $10,000 bonus and a 5%
annual pay raise. The story ends with a new pending case against Marsellus Wallace. If the player missed items in the investigation or final report, Mr. Hill will return to the player with the news that the case was not put together well enough to use against Marsellus for the following reasons. With the botched investigation the player not only earns a low score for the game, but the company loses 80% of their existing customers, tarnishes the reputation of the firm and the player is laid-off.

CONCLUSIONS

The design of this digital forensics video game will provide students acting as the player a chance to become more aware of the field of digital forensics. The student will learn the basic process of an investigation including response, data gathering or seizure, acquisition, analysis, and reporting. Creation of this training as a video game will help fill the void in the burgeoning field of digital forensics to complement the existing offerings in related information assurance and network security.

The future work includes completing the game as it is designed now, then allowing colleges and high schools to use the game to increase awareness and interest in the field of digital forensics. The game also will be enhanced to provide the player with more realistic gaming and learning experiences and maximize the effectiveness of the game such as incorporating a motion detecting device (e.g., LEAP Motion controller [6]). In addition, the finished game will be evaluated against college and high school students to further enhance the game by using the feedback from actual players.

REFERENCES

4. Blender 2.70. GNU General Public License., 2014; software available at http://www.blender.org
35. *Unity 4.0 Game Engine*. 2014; software available at www.unity3d.com