Assessing the Modular-based Digital Forensics Game for Entry Level Students

Dr. Yin Pan, Rochester Institute of Technology

Dr. Yin Pan, Professor in the Computing Security department, received her Ph.D. in Systems Science and M.S. degree in Computer Science from Binghamton University. Dr. Pan holds four US patents in the areas of Network Quality of Services, Voice over IP and Artificial Intelligence. Since joining RIT in 2002, Dr. Pan has been actively involved in the IT security area, especially in security audits and computer forensics. Her current research interests include game-based digital forensics and memory-based malware detection using machine learning. She has published over 45 papers and presentations in research conferences and journals. She received grants from NSF, US Air Force Research Lab, and RIT. Dr. Pan teaches graduate courses in digital forensics and security audits.

Dr. Michael Yacci, Rochester Institute of Technology

Michael Yacci is the Senior Associate Dean for Academic Affairs in the Golisano College of Computing and Information Sciences at RIT.

Dr. Sumita Mishra, Rochester Institute of Technology

Sumita Mishra, professor of computing security at RIT, works on security and privacy for resource-constrained devices and networks, and cybersecurity pedagogy. Her current work focuses on the study of privacy-preserving techniques for the smart grid. She is also interested in making cybersecurity pervasive across non-computing disciplines and high school curricula.

Gamifying Cybersecurity Course Content for Entry Level Students

1. Introduction

Cybersecurity and forensics are among the most critical areas of national importance, in a growing need of knowledgeable professionals. In response, many cybersecurity and forensics programs have been developed in the past ten years [16]. However, these programs are primarily offered to only junior and senior level college students. This is due to the long list of prerequisite knowledge areas that students must obtain prior to attending these courses. In an effort to identify and attract more entry-level college students to these programs, faculty at Rochester Institute of Technology (RIT) have been working with Onondaga Community College and Corning Community College to develop a sequence of entertaining, engaging, and educational forensic games, suitable for first year students in college. We explore game-based learning strategies to engage students learning through interactive game scenarios. Following narrative and/or storylines of the game via interactive dialogs and visualized abstract concepts, we expect that students will be motivated and engaged to obtain the necessary knowledge, and to develop their problem-solving skills while playing the game. As a result, this game-based learning approach may potentially shorten the prerequisite chains of advanced courses.

The Game-Based Learning (GBL) approach has gained considerable attention [11, 12, 17] after James Gee first presented the impact of game play on cognitive development in 2003 [4]. Since then, the GBL approach has been used in geoscience, computer programing, information security, and other fields [1, 5, 10, 13, 15]. The Naval Postgraduate School developed a videogame CyberCIEGE that uses this approach to teach computer and network security and defense [1]. In 2012, the authors at RIT first proposed the idea of using game-based learning and visualization techniques to engage students in learning abstract concepts and to explore forensics investigation technologies and procedures through interactive games [6, 7]. Supported and funded in part by the National Science Foundation under the award DUE-1400567, a modular game framework in both Windows and browser-based platforms have been developed, along with a GUI-based game creator that assists in easy creation of new games [8, 9].

This paper primarily focuses on assessing our project's goals and objectives. Based on the project results over three years, the game modules appear to be effective in teaching the processes of digital forensics, while the GUI-based game creator allows educators to create and develop new educational games. Using the game creator, the game approach can be extended and applied in any STEM education field. In this paper, the authors also share their evaluation strategy and results of assessing the effectiveness of the games-based course modules via a comprehensive evaluation plan.

The rest of this paper is organized as follows. In section 2, the authors describe the project's goals and objectives, followed by a brief introduction to their module-based educational game framework and the GUI-based game creator. Section 3 describes the pilot project introduced to apply the developed game framework in digital forensics courses through a sequence of entertaining and engaging forensic game modules for first-year college students. In section 4, the authors share their evaluation strategy and comprehensive evaluation plans. The results of assessing the effectiveness of the games-based course modules are presented in section 5, followed by the conclusion and our future direction.

2. Goals and Objectives of the Game

We define an educational game as a game that has desired goals and learning objectives and is designed to teach students specific educational contents to meet the defined learning outcomes. Our game aims to develop student's problem-solving capabilities through interactive play in a self-learning environment.

2.1 What are our design goals?

- Engaging - while the main purpose of an educational game is learning, a game must be designed to inspire students and keep them interested and *engaged* in learning content and technology.
- Intuitive and interactive - the game interface should be simple and intuitive.
- Extensible - the educational game should be extensible to enhance the breadth and depth of existing course material with multi-level modular design.
- Adaptive - the game should be adaptable to various STEM fields - math, science, engineering, cybersecurity, etc.
- Real technical skills - students should be able to apply their technical skills outside the game environment.

2.2 How does the game design meet the goals?

Engaging: Engagement is achieved through the design of game framework interfaces. Since our game primarily targets STEM courses that develop a student's problem-solving capability, we designed our game to be a narrative-based game in which the player assumes the role of an investigator, a detective, or an engineer. Evocative of those seen in detective dramas, we design the main interface as a visual representation board, displaying connections and progress the player has made. New leads are gradually discovered and appear on the main interface after the students correctly complete their tasks. Animated transitions from one interface to the next keep the player interested and engaged. After all puzzle pieces in a phase are solved, the next phase unveils, presenting a new set of questions and challenges. When all phases are complete, the final main board depicts the storyline and provides clues and steps to solve a real problem; the player is prompted to create a write-up detailing their solution to be evaluated by an instructor.

Intuitive and interactive: The game interface is intuitive and self-explanatory. Designed for interactive purposes, the game uses conversational dialogues as feedback, guidance, and encouragement. Based on the player's choice, the game will provide different feedback through interactive dialogues to guide the player to find clues for solutions. For certain questions, players are also required to provide a written answer to justify their choice. The written questions allow instructor to judge whether students truly understand the problem. Instructional and informational references such as, tutorials and hints in a visual format or document format, are built in the game to support self-learning of concepts, procedure and technologies through questions, answers, and helpful feedback.

Extensible: The educational game is extensible to enhance the breadth and depth of existing course material with multi-level modular design. Examples of the developed modules are Linux forensics, Windows forensics, network forensics, memory forensics, mobile forensics, etc. Each module is associated with one or more games, such as hacking, fraud, intellectual property theft, and espionage. Playing games based on various difficulty-levels, students gradually gain knowledge as their competency increases. Also, the modules can be incorporated into existing courses in the curriculum without requiring any course or degree program changes and curricular approval. These modules can be replicated and adopted by other science programs. The game is flexible and can be used to create cases covering virtually any subject material.

Adaptive: To make our game easily adaptable by various STEM fields, we used XML to support a flexible plug-and-play structure that automatically saves game interface variables, e.g., analysis steps, narratives, questions and answers, visualization clips, and hints from each module. We also developed a GUI-based game creator [8, 9] to allow users/instructors to create games without requiring XML knowledge. Therefore, this game framework supports versatile case creation and flexible case modification, and also achieves portability of game modules.

Real technical skills: Instead of using simulation tools, our game aims to develop students' hands-on problem-solving capabilities using real tools and technologies. Therefore, students are able to apply their technical skills outside the game environment. Using the game creator described in Section 3.3.2, the

instructors can create games incorporating real-time tools and technologies, to achieve the learning outcomes predefined for a particular subject.

3. The Pilot Game for Digital Forensics Courses

In general, the game framework applies to courses in STEM in various educational disciplines. It runs on both Windows and in modern Web browsers. The Windows version uses the Windows Presentation Foundation (WPF) and is compatible with any Windows computer running Windows 7 or later with the .NET framework installed. The browser-based version uses HTML/CSS, JavaScript, and some PHP to interact with the game using any modern browser.

As mentioned in the previous sections, the game framework uses modular design to support and enhance the breadth and depth of existing course material. The lower-level modules are specifically suitable for entry-level students while the higher-level modules can be used for upper-level courses.

In the following section, we briefly introduce the pilot project - digital forensics game modules designed for first year students in college. We created a storyline of investigating an academic dishonesty case: a professor found that two students' lab reports are identical. During interviews, both students denied access to each other's work. This game seeks players' help to find out whether one student copied another student's work. If so, who did it and how did the student copy the other person's work? What is the evidence that supports the players' statement and what investigation procedure should the players follow?

The game aims for developing students' forensic investigation capabilities through interactive play in a self-learning environment. The details of this project can be found in [8,9].

3.1 Develop the objectives and content of the digital forensics game modules

Digital forensics, as defined by Farmer and Venema in 1999 [3], is the process of "gathering and analyzing data in a manner as free from distortion or bias as possible, to reconstruct data and determine what has happened in the past on a system." We designed our cases in a narrative-based, detective-themed adventure setting in which the player assumes the role of an investigator/detective following the core digital forensics process: Image, Preserve, Analyze, and Report (which inspired the game's name of "IPAR").

For the foundational lower-level module *Introduction to Digital Forensics*, we first define the objectives/learning outcomes of this module. These are a subset of the overall project student learning outcomes. After completing the module, students will be able to

1) Describe and follow basic procedures of incident response.
2) Define fundamental computer forensics concepts and procedures.
3) Apply digital forensic tools to discover, preserve, and analyze digital evidence.
4) Document and report digital evidence.

This module was developed using our game framework and game creator. Following the storyline, we decide on the number of phases for this game; each phase carries its own set of question/answers/resources representing a "chapter" of the entire game. For the storyline described above, we created a conspiracy board with four phases: Image, Preserve, Analysis, and Report, to reflect our objectives. For each phase, we designed and created a sequence of questions in the format of multiple choice, short response, or upload files. The correct answers and helpful resources were also decided. This sets the stage to create the game module.

3.2 Create a game module using the GUI-based game editor

As we mentioned earlier, our game framework uses XML to decouple the game implementation from the content. With this design, game creators only need to use XML to develop game modules. We also developed a GUI-based game creation interface, called *IPAR Editor*, to assist instructors in generating new cases or modifying existing cases by focusing on the case content without worrying about the XML details. Through the editor, instructors can create custom cases that cover content subject matter with their own graphical elements and storylines for an entertaining educational experience. The graphical elements should visually provide players the clues for solving the case.

In this pilot project, we used the editor to create a conspiracy board with four phases: *Image*, *Preserve*, *Analysis,* and *Report,* as shown on the top of board in Figure 1. Each phase carries its own set of question/answers/resources representing a section of the entire game. Figure 1 demonstrates how we populate content for the *Analysis* phase, which is highlighted in grey. Each icon with a user-selected graphical element contains a specific question along with answers and associated resources. Animated relationships/connections among the icons/questions determine a sequential order of the questions that the player solves via a visual relationship between all of the evidence, and lead players to make progress. By the end of the game, a web of connected pieces of clues will be revealed. To generate content for each icon, instructors simply use the game editor by clicking on the icon and filling in the content. Figure 2 shows how we populate the content including choosing the image for the icon, populating a question with associated answers, feedback, and helpful resources.

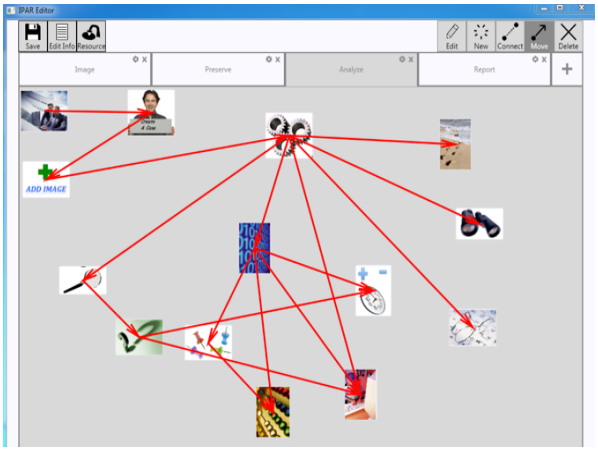

Figure 1. GUI for creating questions

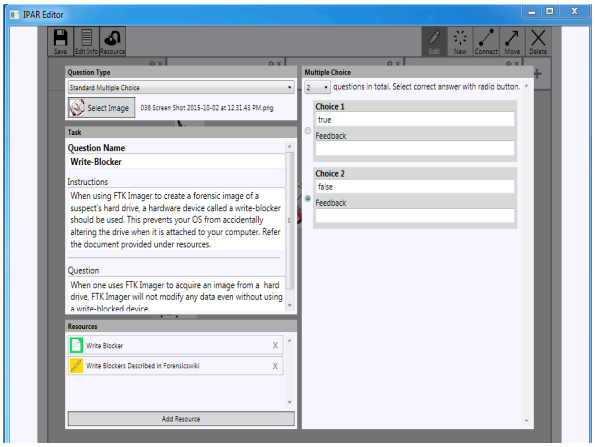

Figure 2. Generating content

After filling in all the content, the user can choose the name of the game and save it. Our example was saved as the Dishonesty case. The game is now ready to be used.

3.3 Play the game

Players will start the game by loading the Dishonesty case to the game framework. The case description/narrative is displayed, as shown in Figure 3.

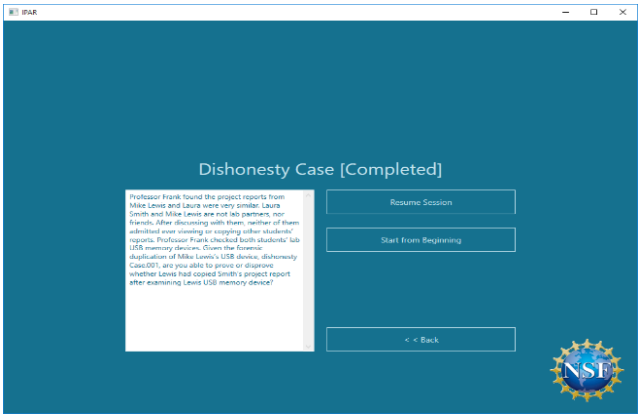

Figure 3. Dishonesty case description

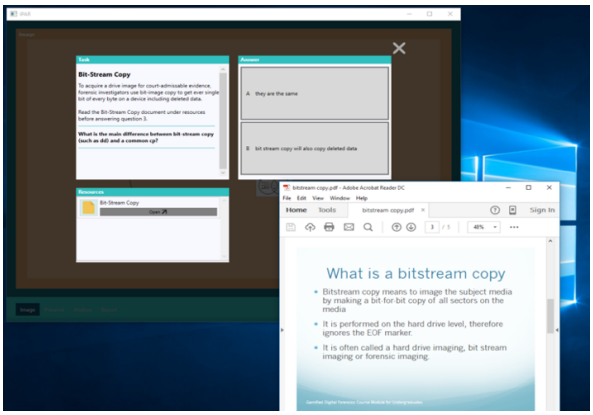

Figure 4. Open a resource link

Players will then follow the storyline to sequentially answer each question appearing on the conspiracy board. In this *Introduction to Digital Forensics* game, players must follow the objective and are required to use digital forensic tools such as *FTK Imager* [2], *Forensics Toolkit* [2] and *Autopsy/Sluethkit* [14] to acquire court-admissible evidence, analyze, and report the current case. Links for tutorials and resources are readily accessible to the players within the game and are presented alongside each question to provide students with immediate help and feedback. Figure 4 provides an example of help that a player can use to answer a particular question. YouTube and Web links are commonly used resources in our games. The game will only reveal subsequent questions and allow players to advance the game if they correctly respond to previous questions.

We also developed several medium difficulty cases to challenge students in addition to this introductory foundational game module. Two Linux cases are focused on integrating Linux/Unix computer forensics, with essential concepts and exercises built into the game design. Two Windows forensics modules emphasize the fundamental knowledge in Windows computer forensics and provide the hands-on experience. Two network forensics modules allow players to uncover network evidence from server logs, live traffic, and stored communications.

4. Evaluation Strategy and Comprehensive Evaluation Plan

The evaluation of the project was designed to follow the project through three major phases: (1) software design, (2) instructional design and effectiveness, and (3) project dissemination. These phases were expanded into seven evaluation questions that were investigated as part of the research grant.

Software Design

1. Is the game infrastructure flexible and user-friendly for plugging in additional content?
2. How can the Game-Based Learning (GBL) modules be improved?

Instructional Design and Effectiveness

3. To what extent is each of the five major learning outcomes attained?
4. Are GBL modules effective for students at each educational level?
5. What are students' attitudes toward further education and careers in Forensics?

Project Dissemination

6. How easily and effectively are modules integrated into existing curricula?
7. How supportive are experts in the field to the GBL approach?

Evaluation question #1 looked at the extensibility of the software and question #2 looked to improve the usability of the interface. These are both software usability design issues. Evaluation questions 3,4, and 5 attempted to measure overall student learning on several specific learning outcomes, and then segmented by 2-year and 4-year institutions. Finally, question #5 looked at the wider implications of GBL – the ability to create interest in the field through motivating simulated problems. For this project to succeed in a large sense, the GBL modules would need to be easily integrated into existing curricula, so questions 6 and 7 were used to look at the ease in which the existing modules could be distributed and disseminated.

Because of the range of research questions, a mixed methods evaluation approach was used, with a combination of open-ended responses and Likert-scale survey questions. Statistical analysis was used when appropriate. Additionally, all learning outcomes were tested. The following section provides some results of the first two areas of evaluation.

5. Assessing the effectiveness of the games-based course modules

The following section provides some results of the first two areas of evaluation. Note that these results came from multiple audiences, over a two-year period, so student responses vary from item to item.

5.1 Software Design and Interface: *"Is the game infrastructure flexible and user-friendly…"*

The interface, and software design aspects of GBL were initially tested iteratively during development. Faculty with expertise in game-design, cybersecurity, human-computer interaction and instructional design were consulted and did expert reviews as the GBL modules were being developed. These reviews brought forth design weaknesses and also pushed the development team towards stronger design ideas. As a more formal evaluative pilot test, the game framework and the *Introduction to Digital Forensics* module were piloted in a one-day faculty summer workshop for 18 college faculty in 2015. The following summer, the GBL editor was introduced in a similar summer faculty workshop. Survey feedback from faculty was very encouraging. Some of comments from the two summer workshops are given below:

- The workshop was very interesting. I would be interested in creating modules for my more advanced classes as well as using the game for lab assignments. I think that this would be interesting to implement within my lectures and as a way to provide my online students a more step-by-step method
- I was glad for the opportunity to work with and learn about real tools that would be used in "serious" digital forensics. Since the programs used are free (at least for training use), I can readily continue exploring what I've learned at home.
- This was very well done and very worth my time.
- As soon as I can get a copy of the editor (creator) I will start building modules of my own. I can see the value in several of my classes. I would love to be able to include in an Inventory & Logistics Class I am developing now. What a great tool to teach the way to analyze inventory breakdowns.

The *Introduction to Digital Forensics* module and a few other modules were also pilot tested at the authors' institution and several other community colleges by more than 150 freshmen in introductory Cybersecurity courses. A majority of the students considered IPAR cases/modules more interesting than other regular lab assignments. Comparing these unconventional game-based exercises with other regular lab assignments, 80% students felt the game-based labs as more interesting and engaging. 20% students liked the idea but felt some modules are not as challenging as regular labs, since they were given too much help.

5.2 Instructional Design and Effectiveness: "*To what extent is each of the five major learning outcomes attained*"

Five specific learning outcomes were listed in the original project proposal. In this article, however, we are primarily focused on two learning outcomes: 'Identify and employ forensic tools to retrieve and analyze evidence of mobile devices' and 'Write a forensics report with findings'. In Spring 2016 and Spring, 2017, the Game-Based module was used at five different schools, across more than 150 total students. The game-based modules were used in a variety of introductory computing security courses.

5.2.1 Learning Outcome: *Identify and employ forensic tools to retrieve and analyze evidence of mobile devices* The GBL itself coaches and prompts students to use the forensic tools, and the lab could not be completed without the use of the tools. After completing the labs, students were asked if they could use two of the major tools (*Autopsy* and *FTK*), essentially confirming that they were able to use the tools that were used in the lab. There was no pre-test of these skills. Students at three sites (N=94, 11, 11) were asked via survey if they were able to use the forensics tool, *Autopsy* with results shown in Figure 5.

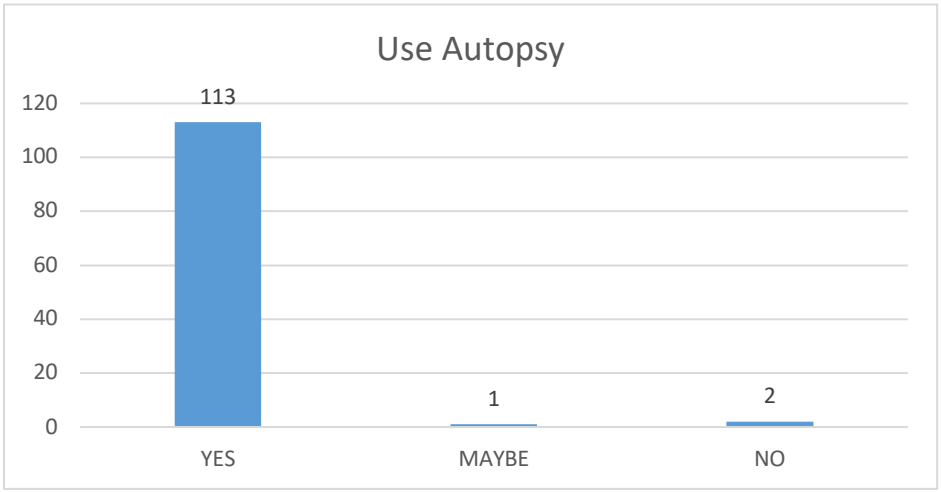

Figure 5. Use of the Forensic Tool: *Autopsy*

Students at three sites (N=94, 11, 11) were asked if they could use the tool *FTK*, with results shown in Figure 6.

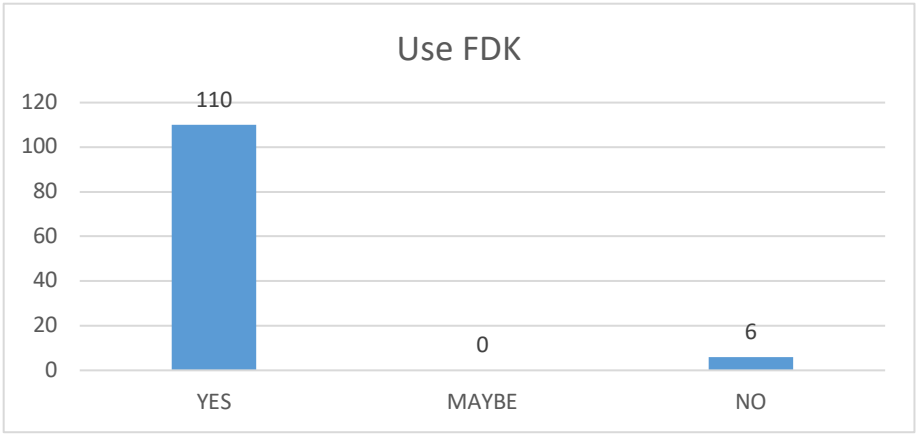

Figure 6. Use of the Forensic Tool: FTK

These results strongly suggest that students felt as though they were able to use these tools which was corroborated by their use in the completion of the labs.

In year 3, students at all sites were asked to identify the forensics tools that they used in the game-based lab, in a post-instructional survey. This is a pure recall test, with the expectation that students would recall the names of the tool they used in the GBL. A simple count of the number of tools identified by name by students is shown in Figure 5 below, with a range of 1-8 different tools that were named. Several students did not answer the question, and one student responded, "All kinds of tools" which suggested that the student did actually use the tools, but somehow failed to be able to identify the tools.

Number of Tools Identified	Count (N)
1	24
2	26
3	5
4-8	9
no answer	5

Figure 7. Use of Forensic Tools

These results strongly suggest that the majority of students did use the tools and were able to identify the tools. (Note that several students included an explanation of what each tool actually was used for. In these cases, often the student ran out of characters in answering the question, and were cut-off, so the reported count may be lower due to this.)

5.2.2 Learning Outcome: *Write a forensics report with findings*

In year two of the project, 116 students used the GBL modules and were required to write a short forensic report that summarized the key findings of the investigation. In particular, they were asked to form a conclusion about the events that transpired in this case. These were judged by evaluators using a simple rubric to determine if the basic framework of a report were included. Reports were terse but showed a comprehension of the process.

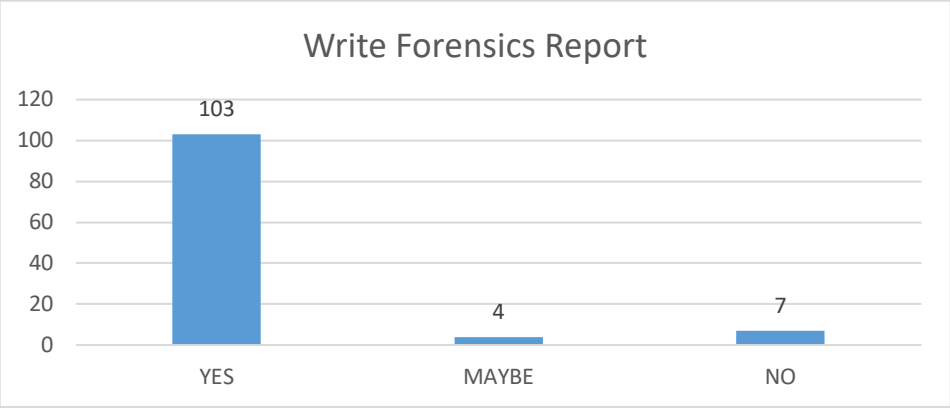

Figure 8. Understanding and Writing Findings

In the year 3 cycle of evaluation, we attempted to determine the reasoning process that students followed, rather than focus on an actual report. Students were asked "what data did you use to form your conclusion." Eight students did not answer, and one student noted that he/she was unable to form a conclusion. The remaining 66 students listed a variety of data and information that was used as they formulated their conclusion.

The following examples are typical responses:

- "We analyzed RAM, hard drives, documents, images, network logs and Wireshark captures throughout the various IPAR labs. All of which proved to be valuable information in the computer forensics process."
- "We looked at hard drive data, RAM dumps, images, logs of computers and network traffic."
- "I looked at a file that was mismatched in its data and type to see an image of the wife and the lover. I then looked at their internet history to see if there were any websites that the family used that could be suspicious and I look at a receipt that I found in the recycling bin that was made out for a vacation"

The student responses suggest that students were able to follow the logic of the particular case and were able to reason through the simulated case and form a conclusion based on the evidence that they gathered. It would appear as though students would be capable of writing a more formal report, given guidelines and report specifications.

5.3 Instructional Design and Effectiveness: "*What are students' attitudes toward further education and careers in Forensics?*"

One of the major goals of the project was to increase interest in the area of forensics and the field of computing security. Students were asked for a forced-choice response to the question: "After this module, did your interest in the field of computer forensics change?"

The results visually suggest that only 3 students' interest were moved in a negative direction. While many students (30) were unchanged, still **a majority of students' interest (38) were moved in a positive direction.** Looking at the hypothesis that responses should be uniform across the distribution, the Chi-Square goodness-of-fit test was used. The Chi-Square value is 79.6. The uniform distribution result is *not* significant at $p=\leq.0001$. Therefore, this is clearly not a uniform distribution. This suggests that overall, the project could be a factor in moving students interest in computing forensics in a positive direction.

Table 1. Change of Interest in the Forensics Field

Change in Interest	**Count (N)**
A lot more interested	3
More interested	35
Unchanged	30
Less Interested	1
A lot less interested	2
No answer	*(1)*
TOTAL	72

6. Conclusions and Future Work

This paper presents the design, development and assessment results of an educational game framework through a sequence of digital forensics game modules. Based on the project results collected over three years, we believe that the use of game-based learning in a real computing environment will help college

students, especially those at entry-level, in engaging, learning and improving their problem-solving skills through interactive games. The game editor provides a GUI-based system that makes our game framework extensible and applicable to other STEM fields, allowing instructors to develop their own game modules. The assessment results for the forensics modules were very positive and encouraging. The main suggestion for improvement that we received from students was developing more advanced and challenging game modules to inspire creativity. We will continue to disseminate our game framework to communities. In the near future, we plan to develop a repository to collect various modules developed by the community and share them with the academic and professional communities.

Acknowledgements

This material is based upon work partly supported by the National Science Foundation under Award DUE-1400567. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. The authors would like to thank RIT's B. Thomas Golisano College of Computing and Information Sciences for their funding and support. The authors also thank Corning Community College and Onondaga Community College for their collaborations and module development, RIT faculty David Schwartz for leading the game design and implementation, and students Ryan McGlinn, Andrew Wetmore, Noah Ratcliff, Sarvagya Mishra, William Worley, Robin Matson, Madison Behringer, Annie Wong, Tori Bonagura, Karan Sahu, and Nick Graca for their contributions to the game development and testing. Finally, the authors would like to thank the anonymous reviewers for their time and valuable suggestions that contributed to greatly improving the overall quality of this paper.

References

[1] CyberCiege, http://cisr.nps.edu/cyberciege/.
[2] Forensic Toolkit (FTK), http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/.
[3] Farmer, D., and Venena, W., *Forensic Discovery*, Addison-Wesley Professional Computing Series, 2004.
[4] Gee, J., *What Video Games Have to Teach Us About Learning and Literacy*, Palgrave Macmillan, NY, 2003. 2.
[5] Mathrani, A., Christian, S., and Ponder-Sutton, A., PlayIT: Game Based Learning Approach for Teaching Programming Concepts. Educational Technology & Society, 19(2), 5-17.
[6] Pan, Y., Mishra, S., Yuan, B., Stackpole, B., and Schwartz, D., Game-based Forensics Course For First Year Students, *Proc. of 13th Annual ACM Special Interest Group for Information Technology Education (SIGITE 2012*), Calgray, Alberta, Canada.
[7] Pan, Y., Schwartz, D., and Mishra, S., Gamified Digital Forensics Course Modules for Undergraduates, *IEEE Integrated STEM Education Conference*, Princeton, NJ, 2015.
[8] Pan, Y., Mishra, S., and Schwartz, D., Gamifying Course Modules for Entry Level Students, *Proc. of* the 2017 *ACM Special Interest Group for Computer Science Education (SIGCSE*), Seattle, Washington, 2017, pp.435-440
[9] Pan, Y., Mishra, S., and Schwartz, D., Gamifying Cybersecurity Course Content for Entry Level Students, *2017 ASEE Annual Conference & Exposition*, Columbus, Ohio, 2017
[10] Pivec M., Schönbacher T. (2014): E-Learning meets Game-Based Learning (GBL) – Transfer of GBL Research Results in The E-Learning Project Management Course", *the eLearning paper issue number 39 "Learning in cyber- physical worlds"*.
[11] Pivec, P., Game-based Learning or Game-based Teaching?, Becta 2009.
[12] Prensky, M., Digital Game-based Learning. *McGraw-Hill* 2000.
[13] Sheldon, L., The Multiplayer Classroom: Designing Coursework as a Game, *Cengage Learning*, 2012.
[14] Sleuthkit, http://www.sleuthkit.org/.
[15] Teed, R., Game-Based Learning, http://serc.carleton.edu/introgeo/games/, 2012
[16] The Horizon Report 2009 Edition, *New Media Consortium and the Educause Learning Initiative*.
[17] Van Eck, R. "Digital game-based learning: It's not just the digital natives who are restless, "*EDUCAUSE review*, vol. 41, pp16-16, 2006.