Gamifying Cybersecurity Course Content for Entry Level Students

Yin Pan, Sumita Mishra, David Schwartz
Rochester Institute of Technology
152 Lomb Memorial Drive
Rochester, New York 14623
{yin.pan; sumit.mishra; david.schwartz}@rit.edu

1. Introduction

Cybersecurity and forensics are among the most critical areas of national importance. These fields have a growing need for knowledgeable professionals. In response, many cybersecurity and forensics programs have been developed in the past ten years [15]. However, due to the requirement of prerequisite knowledge in operating systems, file systems, systems, networks, and more, cybersecurity-related courses are offered to junior and senior level college students and do not target first-year students. In an effort to identify and attract more college entry-level students to these programs, RIT faculty have been working with Onondaga Community College and Corning Community College to explore game-based learning strategies to engage students learning through interactive game scenarios. The game-based learning approach potentially shortens the prerequisite chains of advanced courses, thereby reducing the time and cost for obtaining cybersecurity knowledge and skills for students.

The Game-Based Learning (GBL) approach has gained considerable attention [10, 11, 16] since 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, 9, 12, 14]. 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 to learn abstract concepts and to explore forensics investigation technologies and procedures through interactive games [7, 8]. Supported and funded in part by the National Science Foundation under Award DUE-1400567, a modular game framework in both Windows and browser-based platforms were developed, along with a GUI-based game creator that assists in easy creation of new games.

The rest of this paper is organized as follows. In Section 2, the authors introduce the design of the modular game framework. Sample games are studied in Section 3, detailing a sequence of entertaining and engaging forensic game modules for first-year college students. In Section 4, we introduce our GUI-based game creator and demonstrate the procedure for creating new educational games in any cybersecurity subject. In fact, this framework is generalized enough that it should handle virtually any STEM education subject. The dissemination and assessment results are shared in Section 5, followed by the conclusions and future work in Section 6.

2. Game Framework Design

The game framework primarily targets problem-solving courses in digital forensics and cybersecurity, and it applies for other STEM education 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 newer 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.

We use modular design to make our game framework easily extensible to enhance the breadth and depth of existing course material. Each module is associated with one or more games, such as hacking, fraud, intellectual property theft, and espionage. It can be easily loaded into the game framework, as shown in Figure 1 below. Following narrative and storylines of each game module, students will achieve instructor-designed learning objectives and gain hands-on experience using real tools and technologies.

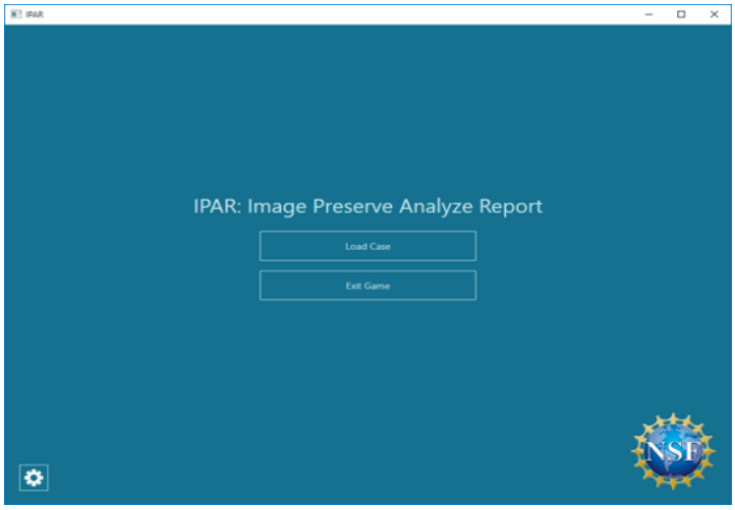

Figure 1. Load module

Through interactive real scenario cases, the player gains insight on concepts of a given subject material by making mistakes, practicing, and correcting mistakes. The game also allows students to demonstrate their capabilities to apply the knowledge to solve a realistic problem using real technical tools. The primary design goal is to make this game engaging, intuitive, interactive, extensible, and adaptive. Engagement is achieved through the design of game framework interfaces. As shown in Figure 2, a conspiracy board in a forensic game depicts the storyline and provides clues to attract students to solve a real mystery presented as a detective's case.

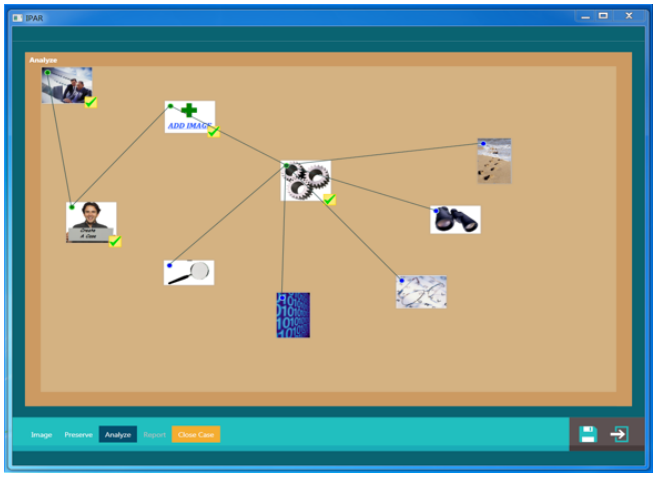

Figure 2. Conspiracy board

The educational game framework supports for multiple choice, justification, short response, and submission questions (see Figure 3 below). A GUI-based game reader allows instructors to view reports submitted by students for grading. Our module-based design makes the game framework easily extensible.

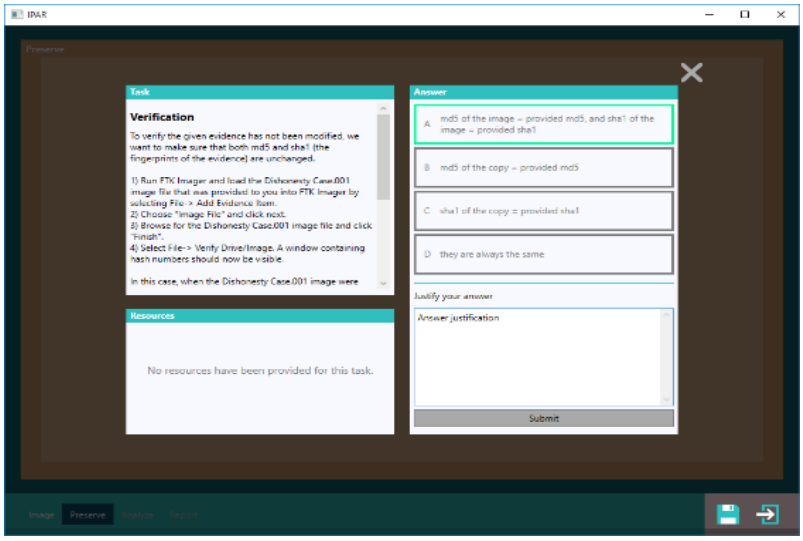

Figure 3. Game questions

To make our game easily adapted to other fields, we use 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 even developed a GUI-based game creator (Section 4) to allow users/instructors to create games without requiring XML knowledge.

3. Forensics Game Modules

We define an *educational game* as a game that has desired learning objectives and is designed to teach students specific educational contents to meet the defined learning outcomes. In this section, we introduce a sequence of forensic game modules, aimed for first year students in college, to develop students' forensic investigation capabilities through interactive play in a self-learning environment.

Digital forensics 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," as Farmer and Venema defined in 1999 [3]. When an incident is confirmed, investigators must follow an appropriate forensics procedure to ensure that data is handled in a manner as free from distortion or bias as possible. 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"). The learning modules, i.e. the *cases*, are listed below:

1. *Introduction to Digital Forensics* is a low-difficulty level module based on a storyline of investigating an academic dishonesty case. Students must follow the four-step digital forensics process of "*acquisition*, *preservation*, *analysis* and *report*" to confirm or dispel the original statement of claiming one student copying another student's work. Students use digital forensic tools such as *FTK Imager* [2], *Forensics Toolkit* [2] and *Autopsy/Sluethkit* [12] to acquire a forensic-sound evidence, analyze, and report the current case. This module would be appropriate for an introductory course in digital forensics. After loading the Dishonesty Case to the game framework, the case description/narrative is displayed, as shown in Figure 4 below. Students will follow the storyline to sequentially answer each question shown on the conspiracy board. Correctly responding to a question will advance the game by uncovering subsequent pieces of unrevealed questions, waiting for the player to solve.

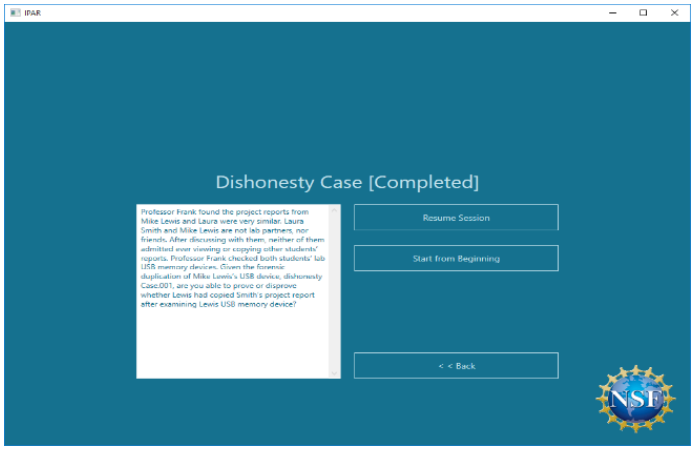

Figure 4. Case description

Tutorials and resources links are readily accessible to the player and are presented alongside of each question. The associated tutorials, which may include other visualizations, provide students with immediate help and feedback. Figure 5 below demonstrates a resource, "Evidence

Collection Document," in a PDF format, to help the player to answer a short-answer question. YouTube and Web links are commonly used resources in IPAR.

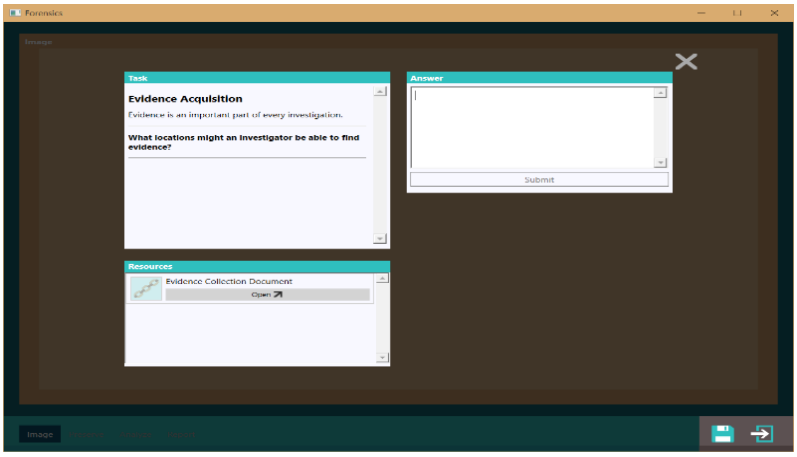

Figure 5. Resource for a short-answer question

2. Two Linux medium-difficulty level cases focus on integrating Linux/Unix computer forensics essential concepts and exercises into the designed game. The *Linux Incident Response Case* requires students to follow incident response procedure to confirm and report an incident on a compromised Linux system. Playing the *Financial Case*, students effectively apply forensics tools to analyze Linux/Unix file systems and identify crucial evidence including deleted file, timelines, permissions, and log files for a trial.

3. Two medium-difficulty level Windows forensics modules emphasize the fundamental knowledge in Windows computer forensics and the hands-on experience. Upon successful completion of the modules, students can solve Windows cases by uncovering pertinent evidence from allocated and unallocated space, and analyzing Windows artifacts including registry, recycle bin, Internet Explorer, emails, etc.

4. Two network forensics modules are developed as medium-difficulty level cases that allow players to uncover network evidence from server logs, live traffic, and stored communications. These modules focus on integrating network forensics essentials and practices to the designed game. *Network forensics* relates to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Upon successful completion of these modules, students can effectively apply network forensics tools, like *Wireshark* [16] and *NetworkMiner* [5] to capture and analyze network traffic and log files. They also practice steganography tools to detect malicious activities.

The above modules can enhance existing curriculum, e.g.

- Enhance and strengthen existing courses by substituting outdated material with latest technologies to keep pace with technological advances.
- Extend and enhance existing content with new topics, concepts, and technologies.
- Function as assignments or projects providing hands-on exercises for existing courses.
- Concatenate into a mini-course for industrial training of working professionals.

4. Game Creator Design

As we mentioned earlier, our game framework uses XML to decouple the game engine from content. Therefore, creating new games (i.e., the modules/cases) need not modify the game source-code implementation. However, instructors usually are only familiar with their subject content without knowing how to write XML. And so, we developed a GUI-based game creation interface (the IPAR editor) to assist instructors to generate new cases by focusing on the case content without worrying about the implementation 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.

As shown in Figure 6, the editor allows users to create a conspiracy board with four phases: Image Preserve, Analysis, and Report. While connected in content, each phase carries its own set of question/answers/resources representing a "chapter" of the entire game. Figure 6, below, shows the various types of questions from the Analysis phase, which are highlighted in grey. Animated relationships/connections among the questions determine a sequential order of the questions that the player solves via a visual relationship that connects all of the evidence. As the game progresses, a web of connected pieces of clues will be revealed. Clicking on each icon, instructors can generate the content for that icon. The image of the icon will visually provide players the clues for solving the case. Figure 7 demonstrates how to create the content including choosing the image for the icon, populating a question with associated answers, feedback, and helpful resources.

The editor will generate an XML file based on users' content input. The XML file can be directly loaded into IPAR for immediate play (Figure 1). The editor can also modify existing games by simply loading the module XML file. After modification, the instructor can export the updated XML file. In fact, as long as the subject matter can be explained in a hierarchical or graphical flow, IPAR and the editor provide an extremely extensible and flexible development environment for building educational detective-style games.

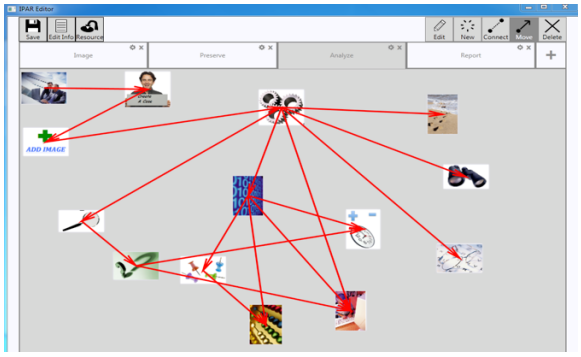

Figure 6. GUI for creating questions

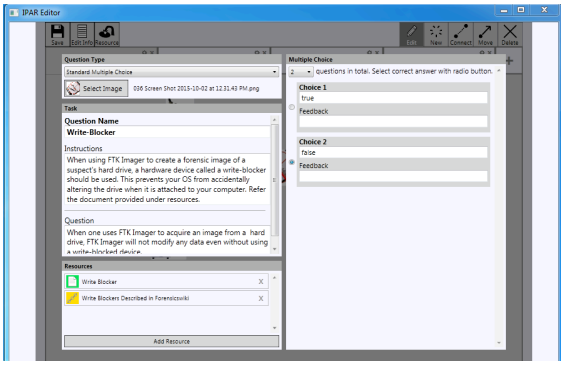

Figure 7. Generating content

5. Forensics Game Modules Assessment

The assessment of the game framework is largely determined by the quality of the module design and development. In this section, we share some assessment feedback on our digital forensics modules. 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, and the editor was introduced in a summer faculty workshop in 2016. Feedback from faculty were 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. I spent as much time traveling as I did in the classroom and it was SO worth it. Well done.
- 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 fewer other modules were also tested at the authors' institution and several other community colleges by more than 150 freshmen in Cyber Security 101 courses. A majority of the players 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. We plan to build some higher-difficulty level games in the near future to meet these students' needs.

In addition, we presented (or will present) our game and modules to communities via conferences such as NICE, ATE PI, CISSE, SIGITE, and SIGCSE. As of now, sixty-one faculty members from two-year and four-year colleges in USA have requested our modules and IPAR. After a professor at Fairleigh Dickinson University in Hackensack NJ tried our material in his graduate class in forensics administration, a retired policeman who is going to start another career in computer forensics wrote: *"I had completed both the Academic Dishonesty case and Incident Response portion of this forensic game. I was very impressed about the real life experience it gives you. Everything that you could encounter is right in front of you. But I was more impressed with using the real life tools like FTK imager and Autopsy and well as other that the game tells you to download in advance. I'm a believer in this game process of learning."*

6. Conclusions and Future Work

This paper proposed a game framework along with a sequence of fun, entertaining, yet educational game modules, in an effort to identify and attract students to cybersecurity programs. We believe that the use of game-based learning in a real computing environment, will develop students' problem solving skills. This approach will potentially shorten prerequisite chains of advanced courses, thereby reducing the time and cost for obtaining advanced knowledge. The editor provides a game creator that makes our game framework extensible and attractive by allowing instructors to develop their own game modules in cybersecurity and other STEM fields. The assessment result

for the game framework with forensics modules was very positive and encouraging. To expand our forensics modules, we plan to develop Internet forensics and cloud forensics in the near future. The main improvement suggestion 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 community.

7. 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 additional funding. The authors also thank Corning Community College and Onondaga Community College for their collaborations and module development, and RIT students Ryan McGlinn, Andrew Wetmore, Noah Ratcliff, Sarvagya Mishra, William Worley, Robin Matson, Madison Behringer, Annie Wong, Tori Bonagura, Karan Sahu, for their contributions to the game development. Finally, the authors would like to thank the anonymous reviewers for their time and valuable suggestions that contributed to the overall quality of this paper.

8. 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] NetworkMiner, http://www.netresec.com/?page=NetworkMiner.
[7] 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.
[8] Pan, Y., Schwartz, D., and Mishra, S., Gamified Digital Forensics Course Modules for Undergraduates, *IEEE Integrated STEM Education Conference*, Princeton, NJ, 2015.
[9] 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"*.
[10] Pivec, P., Game-based Learning or Game-based Teaching?, Becta 2009.
[11] Prensky, M., Digital Game-based Learning. *McGraw-Hill* 2000.
[12] Sheldon, L., The Multiplayer Classroom: Designing Coursework as a Game, *Cengage Learning*, 2012.
[13] Sleuthkit, http://www.sleuthkit.org/.
[14] Teed, R., Game-Based Learning, http://serc.carleton.edu/introgeo/games/, 2012

[15] The Horizon Report 2009 Edition, *New Media Consortium and the Educause Learning Initiative*.
[16] Van Eck, R. "Digital game-based learning: It's not just the digital natives who are restless, "*EDUCAUSE review*, vol. 41, pp16-16, 2006.
[17] Wireshark, https://www.wireshark.org/download.html.