Game-based Forensics Course For First Year Students

Yin Pan, Sumita Mishra, Bo Yuan
and Bill Stackpole
Department of Computing Security
Rochester Institute of Technology
102 Lomb Memorial Drive
Rochester, New York 14623
(585) 475-4645
{yin.pan; sumita.mishra; bo.yuan; bill.stackpole}@ rit.edu

David Schwartz
School of Interactive Games and Media
Rochester Institute of Technology
102 Lomb Memorial Drive
Rochester, New York 14623
(585) 475-5521
disvks@rit.edu

ABSTRACT

Identifying and attracting talented students to digital forensics programs is a crucial first step to developing professionals in this relatively young field. To respond to these challenges, we propose to develop a fun, entertaining, and yet educational forensics-course suitable for first year students in college, in an effort to identify and attract students to a forensics program.

This paper focuses on the design and development of a game-based forensics course using the game-based learning (GBL) approach building the game *in a real computing environment* that has direct access to actual forensics tools from a forensics machine and the evidence from a suspect machine. Interactive visualizations will be used to help students to understand the intangible and inaccessible abstract concepts such as deleted/hidden/encrypted/over-written digital evidence.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *curriculum, information systems education.*

K.8 [**Computing Milieux**]: Personal Computing – *games.*

General Terms

Security, Design, Legal Aspects, Experimentation.

Keywords

Computer Forensics, Game Design, Visualization, Information Assurance, IT education, Curriculum Development.

1. INTRODUCTION

Cyber security and forensics is among the most critical areas of national importance in growing need of knowledgeable professionals [17]. According to Bureau of Labor Statistics [2], Private Detectives and Investigators' job outlook for 2010-2020 will grow 21% (the number of jobs in 2010 was 34,700) with the projected main growth in the area digital forensics. In response to the increasing need for advanced studies in the areas of computer and network security and forensics, several security and forensics programs have been developed in the past 10 years [23, 24].

However, since digital forensics is a relatively young field, college freshman, especially the underrepresented groups, do not have sufficient exposure to the subject matter. Therefore, identifying and attracting students with interests, passion, and talent in forensics is crucial to the development of future forensics professionals. It would be ideal to offer an *Introduction to Computer Forensics* course in the freshman year, especially for colleges sharing a common first year experience. However, the main challenge in offering such a course so early in the program is that it requires students to have understanding of advanced concepts in a variety of areas including computer operating systems, file systems, and network traffic analysis. For example, unlike fingerprints, blood samples, and other evidence found at a traditional crime scene, digital evidence, formatted as 0's or 1's, cannot be seen by the naked eye and leaves no actual physical evidence to visually assess for relevance. Recovering digital evidence that may have been deleted/hidden/encrypted/over-written is impossible without an understanding of how operating systems and file systems work. It is therefore difficult for incoming students to grasp forensics concepts and techniques. In addition, computer forensics involves intensive hands-on exercises that require students to follow potentially tedious procedures that demand a long and focused span of attention. Due to these challenges, current forensics courses are often designed for advanced students – junior and seniors – when they are better prepared to absorb advanced abstract concepts and work on intensive investigations.

This paper proposes an innovative idea to overcome these obstacles so that the course can be offered for general education or as an introductory course for a forensics degree. We will use the Game-Based Learning (GBL) approach to attract students and to explore technologies and procedures commonly used in a forensics investigation. A game will be developed *in a real computing environment* that has direct access to actual forensics tools from a forensics machine and the evidence from a suspect machine to allow students to practice using state-of-the-art forensic technologies. Visualizations will be used to help students to understand the intangible and inaccessible abstract concepts such as deleted/hidden/encrypted/over-written digital evidence on various computer systems.

The rest of this paper is organized as follows. In Section 2, the authors introduce the game-based learning approach and visualization technology as well as how to apply these technologies in a forensics course. The game-based forensics course content and forensics game design are detailed in Section 3. In Section 4, the authors present the assessment plan to evaluate the effectiveness of this game-based approach for a forensics course, followed by conclusion and future work in Section 5.

SIGITE'12, October 11–13, 2012, Calgary, Alberta, Canada.
Copyright 2012 ACM 978-1-4503-1464-0/12/10…$15.00.

2. PREVIOUS WORK

2.1 Game-based learning

Game-based learning (GBL) has gained considerable traction since 2003 when James Gee described the impact of game play on cognitive development [12]. It usually utilizes an interesting narrative and competitive exercises to motivate students learning according to specific designed learning objectives [22]. Studies have shown that GBL can engage students with the material and make significantly improvement over those participating in learning with other educational software due to game's feature of inductive reasoning and frequent interactions with content [20, 26].

2.2 Visualization

Visualization techniques have just been introduced to security education during the past five years [8]. They are most effective in helping students to understand abstract concepts and protocols, identify patterns, monitor activities and follow complex procedures [18]. Schweitzer [19] defined Interactive classroom visualization (ICV) as a term for visualizations used in the classroom specifically designed to demonstrate concepts such as formal models, algorithms or processes. When applying visualization in teaching forensics concepts in our classroom, we will design forensics ICVs as follows:

- Abstract forensic concepts: visualizations that illustrate a general concept such as deleted data, slack data, stegnography, etc.
- Formal models: visualizations that demonstrate a forensics model such as forensics procedure and chain-of-custody.
- Forensics tools: visualizations that demonstrate how a forensic tool works. For example, the basic Unix file convert and copy utility *dd*, *Autopsy/Sleuthkit* [21], the forensic analysis tools *FTK* from AccessData [11], *EnCase* from Guidance Software [9].
- System concepts: visualizations that illustrate open files, system files such as registry/log/history files, running processes, open connections.

Even though both game-based learning and visualization techniques have been successfully used in geosciences, computer and network security [6] and other fields, based on our knowledge, the use of GBL in forensics education, especially in combination with the visualization technologies in a real computing environment, is a novel idea.

As the current generation of students grows up with computer games and television shows such as Crime Scene Investigation (CSI), the game-based forensics course utilizing visualization will harness their interests, engage and guide them to learn digital forensics concepts and practice forensics techniques in an immersive environment. Students who "play" the game will develop their forensics skills and better understand the challenges with respect to the field. This game-based approach to teaching is an innovative way to help convey knowledge about forensics and should serve to capture the interest of technologically-focused students who may then be more likely to pursue a career protecting our digital assets.

3. FORENSICS COURSE DESIGN IN A GAME-BASED ENVIRONMENT

Computer forensics involves understanding specific aspects of digital evidence and following the general forensic procedures of investigation. The field utilizes sophisticated technological tools to appropriately preserve, extract and analyze digital evidence.

This introductory course will be taught in an active learning environment involving classroom activities and in-class hands-on exercises. Visualization techniques are used to create an active learning environment that enables effective teaching of forensics principles and concepts. Specifically, we will develop a digital forensics game that includes graphical visualizations to illustrate fundamental computer forensics concepts, and interactive lab-based forensic investigation activities that allow students to practice gathering, preserving, analyzing, and reporting digital evidence in a fun and real computing environment.

3.1 Goal of the forensics course

This undergraduate introductory forensics course is designed to provide students with the ability to identify pertinent digital evidence and employ appropriate tools to gather, preserve, analyze and report admissible evidence in court. The course emphasizes both the fundamental computer forensics procedure and the hands-on experience of utilizing digital forensics technologies needed to uncover illegal activities of computer users.

3.2 Course Outcomes

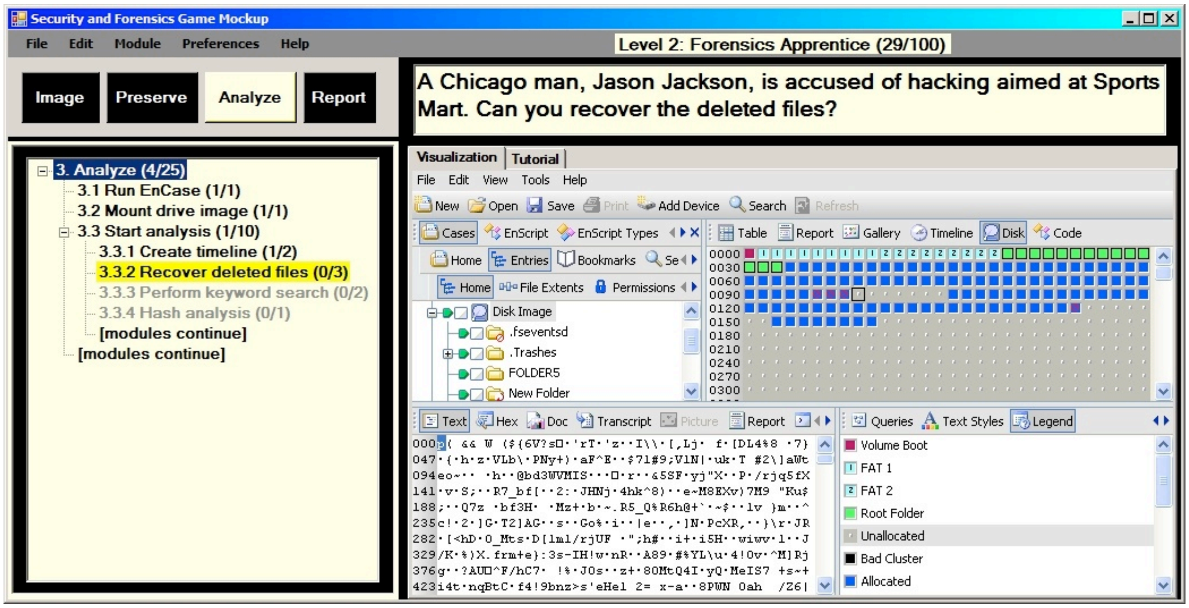
Upon completion of this course, students will be able to

1) Describe and follow basic procedures of incident response.
2) Define fundamental computer forensics concepts and procedures.
3) Apply digital forensic tools to discover, collect and preserve digital evidence.
4) Use Windows and Unix operating systems and file systems to uncover and analyze digital evidence.
5) Identify and utilize appropriate network forensics tools to detect and analyze network intruders.
6) Document and report digital evidence to court.

3.3 The digital forensics game design

The digital forensics game will be built on a Windows system that includes 1) visualizations to illustrate fundamental computer forensics concepts, and 2) interactive lab-based forensic investigation modules to allow student practice in gathering, preserving, analyzing and reporting digital evidence. All Windows-based forensics software will be directly installed in the Windows host while Linux/Unix-based software will be accessible through a Linux virtual machine installed as a guest operating system of the Windows host. This game accesses real forensics images and runs actual forensics tools from both the Windows and Linux operating systems with the following features:

- Digital Crime Scene investigations that include several real world white-collar cases such as hacking, fraud, intellectual property theft and espionage. Each case is associated with a level of difficulty to allow students to investigate different cases throughout the course, increasing in difficulty as the competence of the student increases.
- Visualizations for computer forensics concepts and tools. Players can access concepts, procedure and forensics tools using visualizations through tutorials available from the game interface.
- Sound tracks for the narrative, music, and hints, where appropriate.



Level 2: Forensics Apprentice (29/100)

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

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

- Disk Image
  - .fseventsd
  - .Trashes
  - FOLDER5
  - New Folder

```
0000
0030
0060
0090
0120
0150
0180
0210
0240
0270
0300
```

```
000p( && W ($(6V?s□·'rT·'z··I\\·[,Lj· f·[DL4%8 ·7}
047·{·h·z·VLb\·PNy+)·aF^E··$71#9;VlN|·uk·T #2\]aWt
094eo~·· ·h··@bd3WVMIS···□·r··&5SF·yj"X··P·/rjq5fX
141·v·S;··R7_bf[··2:·JHNj·4hk^8)··e~M8EXv)7M9 "Ku$
188;··Q7z ·bf3H· ·Mz+·b·~.R5_Q%R6h@+`·~$··lv }m··^
235c!·2·]G·T2]AG··s··Go%·i··|e··,·]N·PcXR,··}\r·JR
282·[<hD·0_Mts·D[lml/rjUF ·";h#··i+·i5H··wiwv·l··J
329/K·%)X.frm+e}:3s-IH!w·nR··A89·#%YL\u·4!0v·^M]Rj
376g··?AU□^F/hC7· !%·J0s··z+·80MtQ4I·yQ·MeIS7 +s~+
423i4t·nqBtC·f4!9bnz>s'eHel 2= x-a··8PWN 0ah /Z6|
```

- 🟥 Volume Boot
- 1 FAT 1
- 2 FAT 2
- 🟩 Root Folder
- ▨ Unallocated
- ⬛ Bad Cluster
- 🟦 Allocated

Figure 1: Mockup of the game, which shows an example session at "Stage 3" (Analyze) of a particular session. The player would now attempt to recover deleted files using EnCase.

The interface of the proposed game has six main displays, as shown in Figure 1:

- Menu options for running and saving a game, as well as customization and other options.
- A forensics tools and visualizations pane. This is the main panel where students will gain hands-on experiences by running various forensics tools such as *EnCase*, *FTK*, *Autopsy/Sleuthkit*, etc. Visualizations are also shown in this space, Illustrated in Figure 1 is an example disk space with allocated and deleted data visually shown with *EnCase*. The associated tutorials, which may include other visualizations, provide students with immediate help and feedback.
- A sequence of buttons: Image, Preserve, Analyze and Report. By following the four stages of Image→Preserve→Analyze→Report, the proposed game reinforces the core forensics procedure and provides hands-on experience using real forensics tools.
- A detailed set of steps for each module. For example, Figure 1 demonstrates series steps the player would need to attempt as part of the Analyze module. Note that each step indicates achieved points. For example, the current player missed part of the timeline formulation and received partial credit. This panel also keeps a running tally of module points, which the player can continue to improve by repeating previous steps and a running tally of total points for all attempted modules and their steps. As demonstrated in Figure 1, the player might have missed points in previous modules. The game will provide a series of titles as the player finishes more steps.
- A level of difficult for the current case is shown on the top of the pane.
- A narrative to help motivate the players as they progress through the steps. The narratives can also help to motivate student and provide additional explanation of the current step. Different from other simulation games, this game allows students to practice their skills in a real forensics investigation environment following the appropriate forensics procedure. The proposed interface also facilitates explanations for students with visual and/or auditory disabilities, with the ability to provide audio explanations as well as text captions.

3.4 Course Content

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 [10]. When a crime is committed today, evidence, especially digital evidence, needs to be collected from the scene. Investigators must follow an appropriate forensics procedure to insure that data is handled in a manner as free from distortion or bias as possible. Digital evidence is defined as the information in binary form that may be relied on in court [3]. Evidence might be persistent, such as data stored in non-volatile storage; for example, magnetic, solid-state, or optical. It might be non-persistent, such as over a transmission medium that has no storage. Evidence might also exist in media that is volatile but only temporarily accessible, such as random access memory on a live system or "weakly" erased disk data. Furthermore, the investigation may involve more than the subject and host machine. It could also involve routers, servers, backup storage devices, and even printers [3, 16].

As indicated in the Department of Defense Cyber Crime Center's training program [7], cyber analysts require knowledge on how network and system intrusions occur, how various logs are created, what comprises electronic evidence, how electronic artifacts are forensically gathered, and also the ability to analyze data to produce comprehensive reports and link analysis charts.

The following table ties the course content with visualization tools and hands-on exercises created in the forensics game.

Table 1: Course content, visualization and exercises

Course Outline	**Visualization Built In the Forensics Game**	**Hands-on Exercises** **Built In the Forensics Game**
Module 1: Incident response [4, 5, 15]	Link to CSI: Crime Scene Investigation Where evidence resides – RAM, hard drive compact disks, floppy disk, logs, tapes, usb, cell-phone, PDAs, …, etc.	Incident Response Lab (mock crime scene)
Module 2: Forensic Essentials and General Procedure [3, 15, 16]	What you should do? What you should avoid? Type of digital evidences	A game that students will follow the Chain-of-Custody and a correct forensics procedure sequence to receive points. Deduct points for any wrong doing actions such as destroying volatile data, altering original media, patching and updating suspect system prior to evidence seizure.
Module 3: Volatile data (processes, open files, open ports, memory) acquisition and analysis [27]	Demonstrate the tools to show users who are currently logged on, running processes, open files, open sockets/ports from a live system. Dump physical memory and identify readable information such as ip address, T*rueCrypt* keys, passwords from the memory	Collect volatile information from the game system.
Module 3: Forensics imaging techniques and tools (*dd*, *encase* and *FTK imager*) [16]	Visually show how *dd* does a bit-to-bit copy from the selected source to destination and also show the difference from cp and dd. Visually show other common Imaging formats such as *EnCase* image, E.01	Hands-on exercise to create bit-by-bit image of a usb or small partition using *dd* and *FTK imager* Use *netcat/cryptcat* to transfer data
Module 4: Forensics preservation of the image (*md5sum*, *sha1* and *sha2*) [16]	Visually show how hash function such as *MD5*, *sha1*, *sha2* works	Hands-on exercise to create and verify hashes.
Module 5: Unix Filesystem and Unix Forensic Techniques [4, 5, 15, 16]	Visually show allocated disk space vs. unallocated (deleted) disk space on the game computer. Show a Unix file system EXT2 and EXT3 in a dynamic diagram that links a filename to its inode and the data-blocks associated with this file. Show the possible indications for compromised systems • Check the passwd and shadow files for new/deleted accounts, for UID=0 • Identify wrong doing from history file and user login information • Identify hidden directory • Identify regular files in /dev • Find all SUID/SGID files • Recently modified binaries, recently created files	Examine various compromised Unix/Linux images (including honeypot projects) and identify pertinent evidence with open source *Autopsy, Sleuthkit* and *PTK*. Have hints built into the game to guide students for the investigation • Timeline Creation and analysis • Data recovery / retrieve deleted files • String/key-word search • Hash analysis • Signature analysis • Hidden data (unused partitions, unallocated space, virtual memory) • Check images, emails, internet access
Module 6: Steganography [13]	Visually show the image with	Identify images and audio file with secrets

	secrets embedded vs. a clean image.	embedded and extract the secrets from the images
Module 6: Windows Filesystems and forensics techniques [4, 5, 15, 16]	Windows FAT filesystem and NTFS filesystem. Similar to Unix, show the possible indications for compromised systems Display Windows Registry entries that is crucial to forensics investigations	Given compromised Windows images and lead students to analyze the image. Have hints built into the game to guide students for the investigation. Besides the list similar to Unix hints, additional considerations are: • Hidden data – Slack space • Registry view • Windows recycle bin • IE analysis/Internet history
Module 7: Network Forensics Essentials --Determine what happened on a system based on network traffic study [1]	IDS, router and web server logs. Captured network traffic using sniffing tools	Using *wireshark* or *snort* to capture network traffic. Post-mortem network analysis using *wireshark* and *NetworkMiner* [36] • MAC time analysis • Discover the reconnaissance, exploitation and covert operations • Which vulnerability was exploited • Recover the contents of rootkits • Where it came from • Who (ip addr) did it
Module 8: Forensics report and Forensics investigator and expert witness in reality	Video of expert witness in court. Invite a forensics professor for a talk and discussion	Play mock court

As shown in Table 1, when teaching the content the instructor uses the Interactive classroom visualization (ICV) to help students to understand advanced concepts and technologies. The corresponding game-based exercises reinforce the concepts when students are working on these specially designed games. For example, the course starts with a video clip of a crime scene investigation and shows several criminal cases that involve digital evidence stored in various media such as RAM, hard drives, compact disks, floppy disks, logs, tapes, USB drives, cell-phones, PDAs, etc. The incident response principles and procedures are covered in the lecture followed by an interactive, group-based, mock incident response game to tie the incident response principles and procedures to real-world practice. The objective of this particular game is to learn the correct procedure to respond to an incident and to answer questions such as: How to identify evidence to confirm/dispel an incident, where to collect pertinent evidence, and how to collect evidence in a forensically-sound manner. In this incident response game, students work in groups of 3~4 acting as forensics investigators called to a crime scene. A number of crime scene scenarios will be created for this project to allow students to use forensically-sound investigative techniques to 1) evaluate the scene 2) collect important data and information 3) document everything; interviewing personnel as appropriate 4) maintain chain-of-custody, and finally, 5) to write a report documenting their findings and present the report to the class.

The other game-based exercises focus on OS-specific and network forensic tools and techniques. For example, the exercise of creating a forensic image and preserving the integrity of the image with appropriate forensic tools provides students with a comprehensive understanding of the imaging and hashing (data authentication) processes. Analytical exercises focus on how to recover, categorize and analyze data from the contents of captured drive images which include building timelines based on file dates and times, performing keyword searches, and other activities. The labs are designed at varying difficulty levels. Students are able to choose the level of play, beginning at the entry level, and then move on to more advanced levels.

This fun class concludes with a video of an expert witness testifying and discussing the technical and other skills required to act as an expert witness. A forensics investigator will come to the class to discuss the challenges of the profession and the preparations needed to become an investigator.

The next table specifies how each defined learning outcome is covered in our course outline.

Table 2: Objectives vs. Course Outline

Objectives	Lecture material
Describe and follow the basic procedure of incident response	Module 1: Incident response
Define fundamental computer forensics concepts and procedure.	Module 2: Forensic Essentials and General Procedure
Apply digital forensic tools to discover, collect and preserve digital evidence	Module 3: Forensics imaging techniques and tools to collect both volatile data (processes, open files, open ports, memory) and non-volatile data Module 4. Forensics preservation of the image

Use Windows and Unix operating systems and file systems to uncover and analyze digital evidence.	Module 5: Unix File-system and Unix Forensic Techniques; Module 6: Windows File-systems and forensics techniques and Steganography
Identify and utilize appropriate network forensics tools to detect and analyze network intruders.	Module 7: Network Forensics Essential
Document and report digital evidence to court.	Module 8: Forensics Report

4. COURSE ASSESSMENT

This course will be piloted in 2013. The course assessment will be conducted to measure the effectiveness of the GBL-based Forensics course by assessing gains in student knowledge for each objective for each offering of the GBL modules. The proposed evaluation will focus on directly measuring student learning attributable to the GBL Forensics course. An experimental design will compare the GBL version of the course to an existing, non-GBL version of the course. This will allow us to examine the motivational aspects of the GBL approach along with comparing learning benefits.

5. CONCLUSION AND FUTURE WORK

This paper proposed the course design for a fun, entertaining, and yet educational forensics course suitable for first year students in college, in an effort to identify and attract students to a forensics program. The design of the GBL-based course is based on established research about game-based learning, which has been successfully used in geosciences, information security and other fields. Based on our knowledge, use of GBL in forensics education, especially in combination with the visualization technologies in a real computing environment, is a novel idea. We believe that this approach will be most effective in computer forensics and other advanced fields that involve understanding abstract concepts and hands-on practice. The future work includes implementing the game, based on this design, and conducting a thorough assessment to measure the effectiveness of this approach. Also, we plan to apply this GBL approach to other advance course development.

6. REFERENCES

[1] Buchanan, W., Introduction to Security and Network Forensics, CRC Press, 2011.

[2] Bureau of Labor Statistics, Occupational Outlook Handbook for Private Detectives and Investigators, http://www.bls.gov/ooh/Protective-Service/Private-detectives-and-investigators.htm, 2012.

[3] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd edition)*, Elsevier Science & Technology Books, (ISBN-13 9780123742681), 2010.

[4] Carvey, H., Windows Forensics and Incident Recovery, Addison-Wesley Professional, 2004.

[5] Carvey, H., Windows Registry Forensics, Syngress, 2011.

[6] CyberCiege, http://cisr.nps.edu/cyberciege/.

[7] Department of Defense Cyber Crime Center's training program, www.dc3.mil/dcita/courseDescriptions/cac.php.

[8] Dino Schweitzer, D., Baird, L., Collins, M., Brown, W., and Sherman, M., "GRASP: A Visualization Tool for Teaching Security Protocols", *Proceedings of the 10th Colloquium for Information Systems Security Education*, 2006.

[9] EnCase, http://www.guidancesoftware.com/forensic.htm.

[10] Farmer, D., and Venena, W., *Forensic Discovery*, Addison-Wesley Professional Computing Series, 2004.

[11] Forensic Toolkit (FTK), http://accessdata.com/products/computer-forensics/ftk

[12] Gee, J., *What Video Games Have to Teach Us About Learning and Literacy*, Palgrave Macmillan, NY, 2003.

[13] Katzenbeisser, S., and Petitcolas, F., Information Hiding Techniques for Steganography & Digital Watermarking, Artech House Books, 2000.

[14] Hjelmvik, E., Passive network security analysis with NetworkMiner. *Insecure.com, Issue 18, page 18-21*, 2008.

[15] Kruse, W., and Heiser, J. Computer Forensics: Incident Response Essentials. Addison-Wesley, Boston, 2002.

[16] Nelson, B., Phillips, A. and Steuart, C., *Guide to computer forensics and Investigations*, 4th Edition, Course Technology, 2010.

[17] Remarks by President on Securing Our Nation's Cyber Infrastructure, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[18] Schweitzer, D. and Brown, W., "Using Visualization to Teach Security", *Journal of Computing Sciences in Colleges*, Volume 24 Issue 5, 2009.

[19] Schweitzer, D. and Brown, W., Interactive Visualization for the Active Learning Classroom, Proceedings of the 38th ACM Technical Symposium on Computer Science Education, SIGSCE 2007.

[20] Sheldon, L., *The Multiplayer Classroom: Designing Coursework as a Game*, Cengage Learning, 2012.

[21] Sleuthkit, http://www.sleuthkit.org/.

[22] Teed, R., *Game-Based Learning*, http://serc.carleton.edu/introgeo/games/, 2012

[23] Troell, L., Pan, Y., and Stackpole, B., "Forensic Course Development – One Year Later," *Proc. of the SIGITE 2004 conference,* Salt Lake CIty, Utah, 2004.

[24] Troell, L., Pan, Y., and Stackpole, B., "Forensic Course Development," *Proc. of Conference on Information Technology Curriculum 4*. North Carolina, 2003.

[25] Van Eck, R. "Digital game-based learning: It's not just the digital natives who are restless, " *EDUCAUSE review*, vol. 41, pp16-16, 2006.

[26] Virvou, M., et al., "Combining software games with education: Evaluation of its educations effectiveness, *Educational Technology & Society*, vol. 8, 54-65, 2005.

[27] Waits, C. Akinyele, J., Nolan, R., and Rogers, L., Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis, Carnegie Mellon Technical Review, Cert Program, 2008.