2-28-2015

Gamified Digital Forensics Course Modules for Undergraduates

Yin Pan

David Schwartz

Sumita Mishra

Recommended Citation
[1] Y. Pan, et al., "Gamified Digital Forensics Course Modules for Undergraduates" in Integrated STEM Education Conference (ISEC), 2015 IEEE, Princeton, NY, 2015. pp. 100-105. doi: 10.1109/ISECon.2015.7119899

Gamified Digital Forensics Course Modules for Undergraduates

Yin Pan, David Schwartz, and Sumita Mishra

Rochester Institute of Technology, yin.pan, dis, sumita.mishra@rit.edu

***Abstract* - Cyber security and forensics are among the most critical areas of national importance with a rising demand for knowledgeable professionals. In response to the increasing need for advanced studies in forensics, we propose game-based modules using the game-based learning approach that enable first-year students to learn basic digital forensics concepts without pre-requisite knowledge. This paper focuses on the design and development of an interactive game framework and the educational digital forensics modules that will be plugged into the game framework in a real computing environment. In contrast to the traditional teaching approaches, this modular approach will use game-based learning and visualization techniques to engage students to learn abstract concepts and to explore forensics investigation technologies and procedures through interactive games. The general design of the game framework can be replicated and adapted by other science education programs.**

Index Terms - Computer Forensics, Cyber Security, Game Design, Information Security, IT education.

I. INTRODUCTION

According to Bureau of Labor Statistics [1], 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. To meet workforce demands to produce more qualified forensics technicians and professionals, two-year and four-year colleges have developed several security and forensics programs in the past 10 years [2, 3]. However, due to long prerequisite chains, forensics courses taught in community colleges lack content, while these courses in four-year colleges primarily target upper-level undergraduate students who can understand abstract forensics concepts and work on intensive hands-on exercises. For example, fingerprints, blood samples, and other evidence collected at a traditional crime scene can be seen. But, digital evidence, e.g., formatted as 0s or 1s, cannot be seen by the naked eye and leaves no actual physical evidence to visually assess for relevance. The concept of recovering digital evidence that may have been deleted/hidden/encrypted/over-written is difficult for a beginner to grasp using traditional teaching approaches. 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.

This paper introduces game-based modules with intuitive designs and interactive dialogs that enable students to learn basic digital forensic content without any prior security knowledge. The Game-Based Learning (GBL) approach and visualizations aim to attract and keep students interested and engaged in exploring forensics technologies and procedures. In contrast to the traditional games, our games 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.

RIT is one of the pioneer institutions in teaching digital forensics, offering system and network forensics courses to sophomore and senior students since 2003 [4-7]. In 2012, with RIT's internal support, RIT faculty started to explore GBL approach in forensics education and presented a paper entitled "Game-based Forensics Course For First Year Students" at the ACM Information Technology Education Conference [8]. Working with our partner two-year colleges, Corning Community College and Onondaga

Community College, we are working on the design and development of multilevel plug-and-play game modules to enhance the breadth and depth of forensic content. These self-contain modules can be plugged into any existing introductory security and forensics courses offered in the freshman year, or exploratory programs that shares a common first year experience.

The rest of this paper is organized as follows. In Section II, 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 modules and the game framework design are detailed in Section III. The conclusion and future work are covered in Sections IV and V respectively.

II. RELATED WORK

A. 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 [9]. GBL usually uses an interesting narrative and competitive exercises to motivate students learning according to specific designed learning objectives [10]. Studies have shown that GBL can engage students with the material and make significant improvements over those participating in learning with other educational software, due to the game's feature of inductive reasoning and frequent interactions with content [11-13].

B. Visualization

Visualization techniques have been introduced to security education during the past five years [14]. They are most effective in helping students to understand abstract concepts and protocols, identify patterns, monitor activities, and follow complex procedures [15].

Over the last decade, both game-based learning and visualization techniques have been successfully used in Geoscience, information security, and other fields. Naval Postgraduate School developed a videogame CyberCIEGE [16] that uses GBL approach to teach computer and network security and defense.

Based on our best 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 has grown up with computer games and television shows, such as Crime Scene Investigation (CSI), the forensics games utilizing visualization will harness their interests, engage, and encourage them to learn digital forensics concepts, and practice forensics techniques in an immersive environment. Students who play the game will simultaneously develop their forensics skills and better understand the challenges with respect to the field. This game-based approach to teaching forensics is an innovative way to help convey knowledge 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.

III. FORENSICS MODULES IN A GAME-BASED ENVIRONMENT

Educational games aim to reinforce concepts and procedures by engaging student to learn and practice the same thing repeatedly through making correct choices. Computer forensics involves understanding specific aspects of digital evidence and following the general forensic procedures of investigation. It uses sophisticated technological forensic tools to appropriately preserve, extract, and analyze digital evidence.

In this paper, the authors present the design and implementation of the Digital Forensic Game Framework (DFGF) that allows students to repeatedly practice forensics tools and reinforce the forensics concepts through detective case studies. A series of forensics modules ranging from basic to advanced levels are developed to plug into this game framework. Each module associates one or more interactive forensic investigation case studies to allow students to acquire fundamental module-specific concepts and practice the latest forensic technologies in a fun and real computing environment. The game framework design is covered in section III.A below while the detailed module development will be discussed in section III.B.

A. DFGF design

The digital forensics game is built on a Windows system instead of a virtual reality-environment to interoperate with the required and commonly used forensics tools that are already installed on the system. When a module is uploaded to the game, all the module-specific material (see Table 1 in section III.B) including case images, lecture content, help document, case questions and answers will be parsed. The game player proceeds by accessing forensics case images and launching actual forensics tools from the Window system. The game framework has the following features:

- Enhance the breadth and depth of forensics course material with multilevel plug-and-play modular designs. Each module is associated with one or more digital crime scene investigation cases such as hacking, fraud, intellectual property theft and espionage. Through multiple difficulty-level modules, students can investigate different cases in system, network, mobile forensics, increasing in difficulty as the competence of the student increases. Also, the modules can be incorporated into existing courses in the curriculum without requiring any course or degree program changes and curricular approval.
- Support self-learning of the material such as tutorials and hints in visualizations format or document format for accessing concepts, procedure and forensics tools.
- Support a flexible plug-and-play structure by using a XML reader that automatically configures and sets up game interface variables, like analysis steps, narratives, questions and answers, visualization clips and hints for each digital forensics case. The use of a XML reader for the game allows dynamic changes to the case content and configuration, therefore provides more versatile case creation and future maintenance.
- Provide sound tracks for the narrative, music, and hints, where appropriate.

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

- Conspiracy Board. Each case is associated with one digital crime scene investigation, for example, “rescue your boss’s kidnapped dog.” The board is a visual representation of the tasks and/or questions to solve this particular mystery (e.g., digital evidence might give a trace to the dog’s hidden GPS tracker). Starting with a “root” (initial) task, players click on the “notes” on the board to reveal subsequent tasks/questions. Solving each task/question eventually forms a directed acyclic graph of “notes” on the board. The graph allows players to choose alternative paths/strategies when confronting more complex tasks/questions will multiple (and/or parallel) structures.

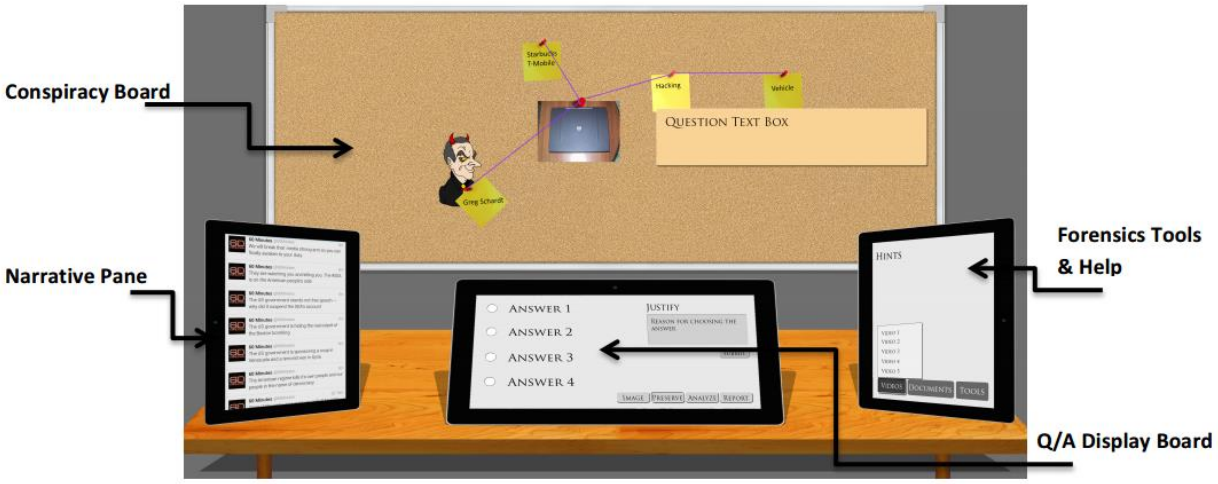

Figure 1. Proposed interface design for the Game Framework

- Narrative Pane. Each case is a self-contained story, whereby each task/question has associated dialogue that appears in this pane. The tasks/questions align to the four major forensics stages: Image → Preserve → Analyze → Report. By stepping the players through the core forensics stages, the gameplay and narrative should reinforce the required learning with real forensics tools and engage the player. If the player answers something wrong, the game framework offers the possibility of a variety of story responses to guide student to learn the concept and technology via HELP manual. The player can continue to improve by repeating previous steps.
- Question/Answer Display Board. This board allows student to input multiple choices answers or provide detailed justification for the answer. Currently, the framework supports "red, yellow, green" responses—correct (and nearly correct) responses trigger subsequent "notes" on the board, which advance the narrative to solving the case. However, incorrect responses trigger pre-determined narrative consequences, which may vary from "your boss makes you buy lunch" to "a field agent's secret identity was compromised!"
- Forensics Tools and Help. This pane allows student to launch forensics tools for investigation. The pane also includes learning material for the module. When clicking on "Help," students will access the associated tutorials and hints in visualizations format or document format via this panel.
- Menu System. The proposed interface will provide a key operation for in-lab use: load a module, save, and exit game. Because of the discrete nature of the game, whereby we associate narrative with specific tasks/questions, the framework saves "game state"—what the player already solved.

This proposed game focuses on specific and detailed technical scenarios allowing students to practice their forensics investigation skills in a real 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.

B. The digital forensics (DF) course modules

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 [17]. When a crime is committed today, investigators need to collect evidence, especially digital evidence, 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 is admissible in court [18, 19].

Evidence might be persistent, such as data stored in non-volatile storage: magnetic, solid-state, or optical devices. 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 mobile devices, cloud, routers, servers, backup storage devices, and even printers [19-21]. Our proposed digital forensics course modules will be based on the digital forensic process of using scientific technology for collecting, preserving, analyzing, and reporting digital evidence to the courts.

The course modules for the game framework form a distinct unit of course materials, for example, Linux/Unix system forensics, Windows system forensics, network forensics, as well as the emerging digital forensics areas such as mobile forensics, memory forensics, malware forensics, and steganography. Each course module, as shown in Table 1 below, contains the description of the module, level of difficulty, lecture content in visualizations format and document format, and one or more case studies including the narrative, relevant evidence, questions, question responses, and investigation results.

TABLE I. DESIGN OF A COURSE MODULE

Component	Brief Description
Overview	Description of module, prerequisite knowledge, and learning outcomes
Level of difficulty	Recommendations for the level of difficulty for college courses
Slides and visualizations	Module content for lectures or independent learning activities, graphical visualizations to illustrate fundamental computer forensics concepts using imagery and animation
Images (dd or EnCase)	Created images for the level of difficulty to be used in the forensics game.
Questions and Answers	Evidence, clues, narrative(s), possible answers, etc.—everything associated with each case
Readings	Introductory or supplementary materials required for the module
Assessment	Tools for students and instructors to measure learning and module effectiveness

Each course module will target one or more of the five the digital forensics learning outcomes as shown in the following.

Learning Outcomes:

1. *Describe digital forensics process and forensics procedures necessary for ensuring the admissibility of evidence in court.*
2. *Identify pertinent system and network information, and use court-approved forensics tools to retrieve admissible evidence.*
3. *Explain and apply emerging technologies to identify admissible evidence from memory, steganography image files, and malware.*
4. *Identify and employ forensic tools to retrieve and analyze evidence of mobile devices*
5. *Write a forensics report with findings following appropriate forensics process.*

C. Sample course modules

Level 100 Module: Introduction to digital forensics process and procedure (All levels)

This module provides students with knowledge and understanding of computer forensics. Correspondent visualization clips will be developed to help students understand the concepts, and be integrated to the game when students request for help and hint. This module covers principles of computer forensic investigation including incident responses and digital forensics process and procedure for collecting, preserving, analyzing, and reporting digital evidence to the courts [17-20]. This module would be appropriate for an introductory course in digital forensics at all levels. Prerequisites: None.

Digital forensics Learning Outcome(s): 1, 5

Level 200 Modules: example course modules for students at community colleges or 1st + 2nd year at 4-year colleges

a. Linux/Unix forensics

This module focuses on integrating Linux/Unix computer forensics essential [20, 21] concepts and exercises into the designed game. Upon successful completion of the module, students can effectively apply forensics tools and techniques for gathering, preserving and analyzing evidence on Linux/Unix systems to identify essential evidence for a trial. Students will be capable of solving low or medium difficulty level Linux/Unix cases through our game system to uncover essential evidence, including deleted files, analyze log files, scripts, permissions, timelines, etc. Prerequisites: Introduction to digital forensics process and procedure.

Digital forensics Learning Outcome(s): 1, 2, 5

b. Windows forensics

The module emphasizes both the fundamental knowledge in Windows computer forensics [22, 23, 24] and the hands-on experience. The content will be integrated to the game systems to engage student learning. Upon successful completion of the module, students can effectively apply digital forensics tools and techniques for gathering, preserving and analyzing evidence on Windows systems to identify potential evidence. Students will be capable of solving low or medium difficulty level Windows cases through our game system to uncover pertinent evidence from allocated and unallocated space, and other Windows artifacts including registry, recycle bin, Internet Explorer, emails, etc. Prerequisites: Introduction to digital forensics process and procedure.

Digital forensics Learning Outcome(s): 1, 2, 5

c. Network forensics

This module focuses on integrating network forensics essentials and practices [25] 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 the module, students can effectively apply network forensics tools, like snort and kismet to inspect and detect malicious activities, and use other network forensics tools to capture and analyze network traffic and log files. Students will be capable of solving medium difficulty level cases through our game system to uncover

network evidence from server logs, live traffic, and stored communications. Prerequisites: Introduction to digital forensics process and procedure.

Digital forensics Learning Outcome(s): 1, 2, 5

Level 300 modules: example advanced forensics modules for 3rd or 4th year students at 4-year colleges

Even through this game is targeted to the first-year and second-year students; it is also ideal to be plugged in advanced module for 3rd or 4th year students at 4-year colleges.

a. Advanced System Forensics

This module emphasizes on the advanced forensics analysis including memory forensics [26-28], steganography detect analysis [29, 30], binary and malware forensics analysis [19, 21, 23, 25]. Over the past few years, the migration of malware into memory and increasing use of encryption by adversaries caused forensics investigators to realize that they must rely on analyzing the computer RAM for examining passwords, running processes, and memory and network connections. Students will work on high difficulty level cases through our game system to analyze captured memory, binary files and digital images. Prerequisites: Introduction to digital forensics process and procedure.

Digital forensics Learning Outcome(s): 1, 3, 5

b. Mobile forensics

This module is designed to provide students with the ability to identify and employ tools used for gathering and analyzing evidence of mobile devices [31] such as cell phones, tablets, PDAs, etc. Students will learn incident response issues specific to mobile devices as well as tools used to uncover activities and information about the use of mobile devices (contact lists, sms/mms/call history, image archives, recovery of deleted and/or hidden files, etc.) The content of mobile forensics will be integrated to the game to allow students work on mobile forensics cases in medium and high difficulty. Prerequisites: Introduction to digital forensics process and procedure.

Digital forensics Learning Outcome(s): 1, 4, 5

D. Module use scenarios

We envision four ways these modules can be used:

1. *To enhance and strengthen existing forensics courses by substituting outdated forensics material.* Digital forensics classes need frequent updates to keep pace with technological advances. These modules are an excellent way to replace outdated topics to include the latest technologies. For example, modules such as Internet forensics and cloud forensics will be developed in the near future.
2. *To extend and enhance existing criminal justice and security material with new topics.* Some community colleges are only teaching courses in security and criminal justice due to lack of resources and expertise, these modules introduce new topics to introduce digital forensics concepts and technologies.
3. *To function as homework assignments or projects.* With the design of hands-on exercises, tutorials and hints presented via visualization [14], these modules could be used as homework or supplemental assignments for existing forensics courses.

4. *To concatenate into a mini-course for industrial training purposes.* These modules can provide a good forensics overview to working professionals. RIT has a long history of offering training for industry through various venues on campus.

IV. CONCLUSION

This paper introduced a digital forensics game framework: a sequence of fun, entertaining, and yet educational forensics course modules, suitable for even first college students, in an effort to identify and attract talented students to forensic field at an early stage. 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. As using an XML reader for the game allows dynamic changes of the case content and configuration, this game framework can be easily replicated and adopted by other science programs.

V. FUTURE WORK

The developed digital forensics game and forensics modules will be piloted in the summer and the fall semester of 2015 at our institution and the two partner two-year colleges. The effectiveness of the GBL-based forensics education will be measured by assessing gains in student knowledge for the defined learning outcomes of the GBL modules. Particularly, an experimental design will compare the GBL version of the course modules to an existing, non-GBL version. This will allow us to examine the motivational aspects of the GBL approach along with comparing the learning benefits.

ACKNOWLEGMENT

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 Corning Community College and Onondaga Community College for their collaborations, and RIT students Karan Sahu and William Worley for their contribution 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.

REFERENCES

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

[2] Colleges offering forensics science program, http://www.forensicpage.com/new05.htm, 2012.

[3] Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein. M, "Computer forensics programs in higher education: a preliminary study", *SIGCSE'05 Proceedings of the 36th SIGCSE technical symposium on Computer science education*, 147-1511, 2005.

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

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

[6] Pan, Y. and Stackpole, B., "Forensics Lab Development", *Secure IT 2006 Conference*, Anaheim, California, 2006.

[7] Pan, Y., and Mishra, S., Advanced Forensics Labs to Meet Computer Forensics Challenges Due to Technological Advancements, *Proc. of the 17th Colloquium for Information Systems Security Education*, Mobile, Alabama, 2013.

[8] Pan, Y., Mishra, S., Yuan, B., Stackpole, B., and Schwartz, D., Gamebased Forensics Course For First Year Students, *Proc. of 13th Annual ACM Special Interest Group for Information Technology Education (SIGITE 2012)*, Calgray, Alberta, Canada.

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

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

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

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

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

[14] 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.

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

[16] Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D., "A Video Game for Cyber Security Training and Awareness", Computers & Security 26 (2007) pp. 63-72

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

[18] National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Washington, DC, 2004.

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

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

[21] Philipp, A., Cowen, D., and Davis, C. *Hacking exposed: computer forensics secrets and solutions*, McGraw Hill, 2009.

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

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

[24] Carvey, H., *Windows Registry Forensics*, Syngress, 2011.

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

[26] 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.

[27] Carbone, R. Bean, C. and Salois, M., An in-depth analysis of the cold boot attack*, Defense R&D Canada – Valcartier*, 2011.

[28] Wade, M., *Memory Forensics: Where to Start*, http://www.dfinews.com, 2011

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

[30] Cox, I., Miller, M., Bloom, J., Fridrish, J., and Kalker, T., *Digital Watermarking and Steganography*, Morgan Kaufmann, 2008.

[31] Bennett, D., The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations, *Forensics Focus*, 2011.