



Annual ADFSL Conference on Digital Forensics, Security and Law

2015
Proceedings


May 21st, 10:50 AM

Towards a Digital Forensics Competency-Based Program: Making Assessment Count

Rose Shumba

University of Maryland University College, Department of Cybersecurity and Information Assurance,
rosemary.shumba@umuc.edu

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Aviation Safety and Security Commons](#), [Computer Law Commons](#), [Defense and Security Studies Commons](#), [Forensic Science and Technology Commons](#), [Information Security Commons](#), [National Security Law Commons](#), [OS and Networks Commons](#), [Other Computer Sciences Commons](#), and the [Social Control, Law, Crime, and Deviance Commons](#)

Scholarly Commons Citation

Shumba, Rose, "Towards a Digital Forensics Competency-Based Program: Making Assessment Count" (2015). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 5.
<https://commons.erau.edu/adfsl/2015/thursday/5>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



TOWARDS A DIGITAL FORENSICS COMPETENCY-BASED PROGRAM: MAKING ASSESSMENT COUNT

Rose Shumba
University of Maryland University College
Department of Cybersecurity and Information Assurance
Largo, MD
rosemary.shumba@umuc.edu

ABSTRACT

This paper describes an approach that UMUC has initiated to revise its graduate programs to a Competency-Based Education (CBE) curriculum. The approach, which is Learning Demonstration (LD) centric, includes the identification of learning goals and competences, identification and description of the LDs, mapping of the LDs to the competences, scripting the LDs, placing the LDs into the respective courses, validating the developed materials, and the development of the open learning resources. Programs in the Cybersecurity and Information Assurance Department, including the Digital Forensics and Cyber Investigations program, are being revised. An LD centric approach to curriculum development helps align programs to the needs of employers, and standards of accreditation bodies. The rationale behind this paper is twofold: to support course development through providing reusable competency inventory, LD inventory, and open resources and to provide assessment by defining competences of an individual as a function of knowledge and skills. This is a work in progress.

Keywords: learning goal, digital forensics, competences, competency-based education, learning demonstration

1. INTRODUCTION

Competency-Based Education (CBE) has become a mainstream topic in higher education. However, CBE is not new. In the 70s, institutions including Empire State College, DePaul University and Thomas Edison State College developed systems for competency identification and validation. The basic building blocks for CBE include the identification of competences and the associated competency-based assessment.

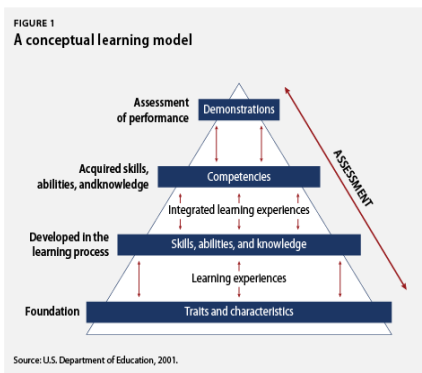
Traditional models of learning focus on what academics believe graduates need to know. These models rely heavily upon the successful completion of a series of courses, assignments, quizzes, exams, tests and time in class results in achieving the learning outcomes (Klein-Collins, 2013).

CBE is an outcomes-based approach to education where the emphasis is on what graduates know and what they can do. The learning experience is dependent upon standardized and agreed upon definitions of skills, abilities, knowledge, competences and demonstrations. Students learn at their own pace and have to demonstrate mastery of the content and associated skills required for a particular course/context, regardless of how long it takes. Competences are identified; the content, readings and assignments are then selected to support student attainment of the competences.

A competency may be defined as a combination of skills, knowledge and attitude that enable an individual to perform a task in a specific context (student and or workplace focused) to a defined level of proficiency

(Chacko, 2014). CBE measures learning rather than time spent (Mendenhall, 2012). As such, assessment of learning plays a critical role in many CBE programs and helps provide the needed support and mastery (Learning in the News, 2010, American Progress).

In a CBE model, students know the content they are expected to study and the activities to perform for assessment (Colloquium, 2008).



The above figure, from the National Postsecondary Education Cooperative report, (NPEC, 2002) describes a CBE model. The four main tiers of the model include:

- the traits and characteristics,
- skills, abilities and knowledge,
- competences, and
- demonstrations

Traits and characteristics are the foundation of learning and the natural makeup of the individuals upon which further experiences may be built. The differences in traits and characteristics help explain why people pursue different learning experiences. Through the learning experience, which includes formal education, work and participation in community affairs, skills, abilities and knowledge are acquired. The unique combination of skills, abilities and knowledge that one has acquired define the competences that an individual possesses. The

individual competences possessed by an individual are combined in carrying out different demonstrations or tasks.

CBE can be very accommodating to adult learners who have some college, but no degree but have prior learning. Competency methodology is not limited to domain knowledge of a degree but also the critical analysis and decision making capability of an individual.

To meet the professional needs of working adult learners whose responsibilities may include jobs, family and military service UMUC Graduate School is revising four graduate programs in the Cybersecurity and Information Assurance Department to CBE: Cybersecurity Technical (UMUC, 2014), Cybersecurity Policy (UMUC, 2014), Digital Forensics and Cyber Investigations (UMUC, 2014), and Information Technology with Information Assurance Specialization (UMUC, 2014).

This paper focuses on the work done so far towards the revision of the Digital Forensics and Cyber Investigations (DF) program to CBE curriculum. Section 2 gives an overview of different CBE models. Section 3 describes the UMUC Digital Forensics and Cyber Investigations program. Section 4 describes the LD centric process being used in the program revision. Section 5 presents the lessons learnt so far. This is a work in progress.

2. A BRIEF OVERVIEW OF THE CBE MODELS

There are CBE curriculum models that are evolving: assessment-based, structured instruction, and integrated models (Wax, 2014)

Elements of an assessment-based program are that the degree is based on the student demonstrating a predetermined set of competences. The students learn through a variety of modes, faculty serve as assessors, students complete assessments at their own

pace, student may start at any time, and there is competency-based assessment. There may also be an option for face to face capstone requirement. Western Governors University is an example of a university with an assessment-based program (West Governor, 2012).

The structured instruction model includes courses with modules developed around competences, a variety of learning modes, assessment embedded throughout curriculum, faculty members acting as mentors and advisors, different faculty members acting as assessors, pre-test that allows the students to skip to next module for subjects already mastered (Personalized Learning Assessment), and post-test that validates learning. Examples of colleges using this model: Capella FlexPath, Kentucky Learn on Demand, Northern Arizona PL, and Texas Affordable Bachelors's.

The integrated model, which is currently being followed by DePaul University School for New Learning, includes multiple pathways to a credential through competency-based assessment, plus on the ground traditional courses and prior learning assessment. There is also conversion of competences for credit hours. Currently UMUC has some of these elements in the undergraduate program: prior learning assessment and traditional courses.

The UMUC Graduate School is adopting the integrated model. It is not clear yet, what elements will be in the model. We envision the role of faculty changing significantly. Faculty will serve more as student guides and less as authoritarian figures setting the pace of learning and dictating grades (Krathwohl, 2002). The semester will be 11 weeks long as opposed 12 weeks. Courses will be translated into credit hours. There will be no flexi-path. Any student who finishes early must wait for the next semester. The logistics of how this will eventually work are not finalized. This is a work in progress.

3. THE UMUC DIGITAL FORENSICS PROGRAM

Digital forensic examiners are in demand to mitigate the growing vulnerabilities of the digital universe. Based on projections, the field cannot meet the demand for digital forensic professionals in the near future. The profession is expected to grow double digits with the increasing demand for cybersecurity from the public and private entities (Withycombe, 2014) (Gannett, 2012). The Bureau of Labor Statistics estimates computer forensics jobs to grow more than 13% in the next several years. The National Security Agency is planning to hire 3,000 specialists to combat the thousands of cyber-attacks in the US. The Department of Homeland Security is expected to hire about 1,000 more cybersecurity specialists (Gannett, 2012).

Many colleges and universities are adding forensics courses to their curriculum to meet the demand for forensic specialists. (CriminalJusticeSchool, 2015), (Endicott-Popovsky, Frinckle, 2006), (Nelson, Phillips, 2008).

Given the vital need for qualified digital forensic professionals and the steady rise in the number of colleges/universities offering digital forensics courses, there is a great need to align programs to the needs of employers, and standards of the accreditation bodies. There is need for programs that emphasize "doing", that is meeting higher layer objectives of Bloom's taxonomy of cognitive learning (Krathwohl, 2002).

UMUC offers an online Digital Forensics and Cyber Investigation Graduate Masters and Graduate Certificate program (UMUC graduate, 2014).

The Graduate Masters of Digital Forensics and Cyber Investigations program requires that students complete six 6-credit courses (36 credits total):

- CSEC 610: Cyberspace and Cybersecurity

- CSEC 620: Human Aspects in Cybersecurity: Ethics, Legal Issues and Psychology
- CSEC 650: Cyber Crime Investigations and Digital Forensics
- CSEC 661: Digital Forensics Investigation
- CSEC 662: Cyber Incident Analysis and Response
- CSEC 670: Capstone

The Graduate Certificate program has three courses: CSEC 650, CSEC 661 and the CSEC 662.

The majority of the students coming into the UMUC program are career changers. We therefore require that all our students take the CSEC 610 and the CSEC 620 courses. The CSEC 610 course is a study of the fundamentals of cyberspace and cybersecurity; cyber architecture, cyber services, protocols, algorithms, hardware components, software components, programming languages, various cybersecurity mechanisms, business continuity planning, security management practices, security architecture, operations security, physical security, cyber terrorism, and national security.

CSEC 620 covers an examination of the human aspects in cybersecurity; ethics, relevant laws, regulations, policies, standards, psychology, and hacker culture. Emphasis is on the human element and the motivations for cyber-crimes. Analysis covers techniques to prevent intrusions and attacks that threaten organizational data.

The CSEC 650 course covers the theory and practice of digital forensics. Topics include computer forensics, network forensics, mobile forensics, and other types of digital forensics. Discussion also covers identification, collection, acquisition, authentication, preservation, examination,

analysis, and presentation of evidence for prosecution purposes.

The CSEC 661 covers the processes and technologies used in the collection, preservation, and analysis of digital evidence in local, networked, and cloud environments. An examination of policies and procedures related to security incidents, exposures, and risks and technologies used to respond to such threats.

CSEC 662 of policies and procedures related to security incidents, exposures, and risks and technologies used to respond to such threats. Topics include dynamic vulnerability analysis, intrusion detection, attack response, evidence protection, and business continuity. Discussion also covers types and modes of computer-facilitated attacks, readiness, and evidence scope, as well as the role of computer emergency response teams.

All students within the program are required to take a Cybersecurity Capstone course, CSEC 670. The CSEC 670 course is a study of and an exercise in developing, leading, and implementing effective enterprise and national-level cybersecurity programs. Focus is on establishing programs that combine technological, policy, training, auditing, personnel, and physical elements. Challenges within specific industries (such as health, banking, finance, and manufacturing) are explored (UMUC graduate, 2014).

4. LEARNING DEMONSTRATION CENTRIC PROCESS

A key component of the new CBE curriculum is the use of authentic assessments that students employ both to learn and demonstrate learning. These are referred to as LDs in the process. Authentic assessments is based on doing and not just knowing, which is the higher order, thinking skills of Bloom's Taxonomy of learning (Learning in the News, 2014): evaluation, synthesis, analysis and application. Students advance based on their ability to master a skill or a competency.

Large skill sets are broken down into competences, which have sequential level of mastery.

The LD centric process involved the identification of the learning goals and competences, development of the LDs, scripting of the LDs, placement of the LDs into respective courses, validation of the developed materials and the development of open resources to support the developed LDs. Once again, this is a work in progress.

4.1 Identification of the learning goals and competences

A learning goal is a very broad statement of what students should know or be able to accomplish. The purpose for crafting a set of learning goals was to provide a brief and broad picture of what the program expects its students to know and be able to do upon graduation (outcomes).

The input sources for identification of the learning goals and competences included the National Cybersecurity Workforce Framework (NICE,2013)], NSA Center of Excellence in Information Assurance. Cyber Defense Knowledge Units (NSA, 2013) the Air Force Office of Special Investigations Defense Crime Center CDFAE (CDFAE, 2012), DoD 8570 (DoD,2010) and Subject Matter Experts. Five broad digital forensics specific learning goals were identified:

1. Learners interpret and utilize laws, policies, procedures, and governance in digital forensic and incident response situations.
2. Learners demonstrate the appropriate use of multiple digital forensic tools and technologies in a variety of criminal and security breach situations.
3. Learners design and implement strategies for proper seizure, evidence handling, investigation, and analysis of digital artifacts, including preparing reports and presenting findings.

4. Learners adapt proper professional, legal, and ethical frameworks to govern their forensic activities in local, national, and global environments.
5. Learners assess an Information Architecture for potential security threats and evidentiary value

In addition to the above five learning goals, the UMUC Graduate School has four learning goals which all students in the Graduate School need to master:

1. Communication: learners demonstrate ability to communicate clearly both orally and in writing.
2. Critical thinking: learners demonstrate ability to apply logical, step-by-step decision-making processes to formulate clear, defensible ideas and to draw ethical conclusions.
3. Quantitative reasoning: learners demonstrate the ability to use mathematical operations and analytical concepts and operations to address problems and to inform decision-making.
4. Leadership, facilitation, and collaboration: learners lead, facilitate, and collaborate with a variety of individuals and diverse teams to achieve organizational objectives.

The Graduate School provided the competences for the four learning goals above to all the departments revising their programs. Appendix A presents identified competences for learning goal 2 for the Digital Forensics and Cyber Investigations program.

4.2 Identifying and mapping the LDs

Once the learning goals and competences were identified, LDs were identified and described. LDs are the real tasks that someone in a given context will need to be able to do. Identifications of the LDs requires a thorough understanding of the work products that professionals in the industry are required

to produce on a daily basis. Such work products vary greatly in complexity and scope and include memos, reports, studies, oral presentations, speeches, digital/multimedia presentations, audio recordings, print or online publications, social media presence, scientific experiments, graphical models, quantitative models, and many other types of deliverables in addition to research.

Working with Subject Matter Experts (SME), 20 LDs for the Digital Forensics and Cyber Investigations program were identified and described. The LDs were arranged in a very specific order to enable students to build capacity as they progress through the program—learning something and then building on it as they move forward. The topics and content student need to master in order to complete a given LD were selected. A subset of the identified LDs, brief description and the associated content and topics for each LD is presented in Appendix B.

The next step was the mapping of the program competences to the identified LDS. The goal was to ensure that over the course of the program, the students would learn and demonstrate mastery of every competency in the program a sufficient number of times.

Appendix C presents a partial mapping grid for the competences for goal 2 for the Digital Forensics and Cyber Investigations programs to the LDs 5 to 8. The vertical axis shows the competences. The top horizontal axis has a partial list of the identified LDs (LDs 5 to 8) The highlighted yellow shading shows the mapping of the competences to the LDs.

After the mapping was completed, the next step was to assess whether any competences were over evaluated, that is, being evaluated too often. This was achieved by looking out for some gaps and overlaps in the yellow shading. Any unmapped competences were deleted. Any LDs with lower than reasonable mapping were quaranteedfor further consideration.

The identified LDs were then scripted and the placed into the courses. Scripting involved expanding what is being required for the student to demonstrate. This involved fully developing the base scenarios and details of LD for the purposes of adding to their realistic nature and context.

The Graduate School provided the elements of the scripting process:

- Describing the role the student is playing – is she/he acting or being acted upon
- Explaining what his/her is being asked to do in his/her role
- Explain the deliverable within the context of the story
- Determining the timeline; start and end dates for the story/situation – is there a crucial moment in the sequence of events
- Explaining the critical issues, events or problems under consideration and there consequences
- Providing relevant data, in appropriate format
- Suggesting where other types of relevant data might be found
- Concluding by integrating the learning demonstration into the template.

After fully scripting we will have a fully verified set of LDs, their mapping to competences, and a final set of program competences.

The fully scripted LDs will then be placed into courses. Now we will have the core blocks of the program. With the revision of the program nearing final, a focus group with three to five of adjunct faculty will be held to review and validate the placement of the LDs into the courses.

5. LESSONS LEARNT

The process has been quite an engaging experience. We have fully designed the core blocks of an academic program from a competence level, something very few Program Chairs in higher education get to do in their careers. The process has enabled us to assess the complexity and effort required in transitioning the traditional curriculum offering to a CBE one in digital forensics.

The CBE project started early March 2014. It is expected to be completed during the Spring of 2016. Implementation will immediately follow. There have been a series of workshops and a Canvas online class created to guide the Program Directors through the process. The online class also provided for submission of completed work and discussion forums for Program Director interaction. Completed products documents for learning goals and competences, LD description, and the mapping of competences to the LDs competences were submitted through the Canvas class.

Revisiting and revising programs will help make more them more relevant to the market we serve, the working adults. A CBE curriculum will provide students with a career relevant experience, and offer a practical approach to learning.

An outcome from this project will be a “knowledge cloud” containing the collection of competences, LDs, and resources that may be shared or reused by related programs.

This is a very time consuming process which requires good management and leadership. To kick off the project, roles were defined for the Program Director, coach and Subject Matter Expert. The project leadership includes the Dean and the Associate Dean. The role of the Program Director was to work with an SME to identify goals and competences, map LDs to competences, and develop the learning resources. The coaches worked with the PDs. The coach met biweekly with the Program Directors, reviewed work, and coordinated and dialogued with

departmental Chairs. SMEs were selected by the Program Chairs and assisted with content and design as specified in the contract.

6. CONCLUSION

This paper has presented the approach that UMUC is using to revise its graduate programs into a CBE curriculum. The approach which is LD centric involves the identification of the learning goals and related competences, development to the LDs, mapping of the LDs to the competences, scripting the LDs, placing the LDs into courses and validation of the developed work. We envision use of open source resources for teaching the course. The pilots of the project are planned for the Spring 2016. It is anticipated that this project will produce a “knowledge cloud” which contains a collection of competences, LDs, and open resource content that may be shared with related courses.

REFERENCES

1. Endicott-Popovsky B, Frincke D (2006). Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. In: Proceedings of the IEEE workshop on information assurance: computer forensics. West Point, NY: United States Military Academy; June 2006.
2. Nelson B, Phillips A, Enfinger F, Steuart C, (2008), Guide to Computer Forensics and Investigations, 4th Edition, Course Technology, .
3. UMUC (2014). Cybersecurity Technical Program. Retrieved from: <http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity.cfm>.
4. UMUC(2014). Cybersecurity Policy Program. Retrieved from: <http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity-policy.cfm>.
5. UMUC (2014). Digital Forensics and Cyber Investigation Program. Retrieved from: <http://www.umuc.edu/academic-programs/masters-degrees/digital-forensics-and-cyber-investigations.cfm>.
6. UMUC (2014),. Information Technology with Information Assurance Specialization Program..Retrieved from: <http://www.umuc.edu/academic-programs/masters-degrees/information-technology-with-information-assurance-specialization.cfm>.
7. Mendenhall, R (2012). What Is Competency-Based Education? Retrieved from: http://www.huffingtonpost.com/dr-robert-mendenhall/competency-based-learning-b_1855374.html.
8. Western Governors University (2014). Why WGU — Competency-Based Learning. Retrieved from: http://www.wgu.edu/why_WGU/competency_based_approach.
9. University of Wisconsin. University of Wisconsin Flexible Option FAQs. Retrieved from: http://www.wisconsin.edu/news/2012/11-2012/FAQ_FlexOption.pdf.
10. Krathwohl, D(2002). A Revision of Bloom's Taxonomy.Theory into Practice, 2002.
11. National Initiative of Cybersecurity Education (NICE). National Cybersecurity Workforce Framework. Retrieved from: http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.
12. NSA (2012). Centers of Excellence in Information Assurance and Cyber Defense Education. Retrieved

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

Formatted: Font: 12 pt

Formatted: Font: Not Italic

- from: https://www.nsa.gov/ia/academic_outreach/nat_cae.
13. CDFAE, (2012), Special Investigations Defense Crime Center, Air Force. The National Centers of Digital Forensics Academic Excellence (CDFAE) Program. Retrieved from: <http://www.dc3.mil/cyber-training/cdfae>.
14. DoD. (2010)DoD 8570, Information Assurance Support Environment. Retrieved from: <http://iase.disa.mil/Pages/index.aspx>.
15. Klein-Collins R(2013), National Institute for Learning Outcomes Assessment. Retrieved from: <http://www.learningoutcomeassessment.org/documents/Occasional%20Paper%2020.pdf>
16. Learning in the News, (2014), <http://mbmtraining.wordpress.com/2010/12/03/designing-competency-based-training-with-blooms-taxonomy/> Retrieved from: <http://mbmtraining.wordpress.com/2010/12/03/designing-competency-based-training-with-blooms-taxonomy/>
17. The Colloquium (2008). Retrieved from <http://www.thecolloquium.com/PAGE5CoreModel.htm>.
18. Wax, D (2014), When Assessment of Learning Counts: Competency-based Degree Programs in the USA. A presentation at UMUC.
19. National Postsecondary Education Cooperative (NPEC),(2002), Defining
- and Assessing Learning: Exploring Competency-Based Initiatives. Retrieved from: <http://nces.ed.gov/pubs2002/2002159.pdf>
20. Global Media Center, (2014). UMUC to Receive World Affairs Council’s “Educator of the Year” Award. Retrieved from: <http://www.umuc.edu/globalmedia/recognition-of-global-education.cfm>
21. Withycombe, C (2014), Deschutes’s Digital Forensics Lab Stretched, The Bulletin. Retrieved from <http://www.bendbulletin.com/localstate/2731689-151/digital-detectives#>.
22. Gannett, A (2012), Want CSI Without the Blood? Investigate Computer Forensics. USA Today Retrieved from: <http://usatoday30.usatoday.com/story/jobcenter/workplace/buzzese/story/2012-01-31/profession-that-hunts-cybercriminals/52909566/1>.
23. Chacko, T, (2014), Moving toward competency-based education: Challenges and the way forward, Archives of Medicine and health Science, Volume 2, Issue 2.
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic
- Formatted: Font: Not Italic
- Formatted: Font: Not Italic
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic, No underline, Font color: Auto
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic
- Formatted: Font: Not Italic, No underline, Font color: Auto
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic
- Formatted: Font: 12 pt
- Formatted: Font: Not Italic

Goal 2 for the Digital Forensics Program and Associated competences

Learners demonstrate the appropriate use of multiple digital forensic tools and technologies in a variety of criminal and security breach situations.

- 6.1 Use Forensic Tools and Techniques
 - 6.1.1 Utilize tools such as EnCase, FTK, Open Source, Imaging
- 6.2 Evaluate sources of Forensic artifacts
 - 6.2.1 Analyze computer components
 - 6.2.2 Analyze electronic devices
 - 6.2.3 Examine media
 - 6.2.4 Examine memory (RAM)
 - 6.2.5 Analyze mobile devices
 - 6.2.6 Analyze network artifacts
- 6.3 Perform Malware Analysis
 - 6.3.1 Detect unauthorized devices
 - 6.3.2 Perform static malware analysis
 - 6.3.3 Perform dynamic malware analysis
- 6.4 Investigate Mobile Technology
 - 6.4.1 Examine hardware and communication
 - 6.4.2 Evaluate 2G-5G
 - 6.4.3 Examine wireless security
 - 6.4.4 Analyze encryption
- 6.5 Investigate Multimedia Technologies
 - 6.5.1 Examine audio, pictures, video,
 - 6.5.2 Analyze digital fingerprints/device fingerprints
 - 6.5.3 Utilize various file formats
 - 6.5.4 Examine meta data
- 6.6 Analyze Social Media Artifacts
 - 6.6.1 Examine social networks
 - 6.6.2 Utilize analysis techniques (closeness, etc.)
- 6.7 Utilize Visual Analysis
 - 6.7.1 Apply link analysis
 - 6.7.2 Incorporate time analysis
 - 6.7.3 Utilize filtering
- 6.8 Use GREP
 - 6.8.1 Construct GREP searches for file headers
 - 6.8.2 Construct GREP searches for file signature analysis
- 6.9 Analyze online and console based gaming
 - 6.9.1 Identify evidence sources and challenges
 - 6.9.2 Incorporate cloud investigation techniques

Appendix B

Four of the identified LDs

	LD	Brief Description of the LD	Topics to be covered
5	Develop an Incident Response Framework	As head of the Incident Response team, you are tasked to develop an Incident Response Framework to be used as a guide in responding to various types of incidents that an organization may be faced with (Report)	Project plan, project budget, establish, execute, monitor project plan of action, incident response and management techniques, evaluating risks, risk management models, categorizing risk.
6	Incident Response: Imaging	Utilize proper procedures and tools such as Encase, FTK, and open source to image various digital artifacts. These artifacts include computer disks and RAM (for Windows, Linux and Mac systems, cloud data, RAID, SAN, NAS) Lab exercise.	Sources of forensics evidence, report writing, affidavits, investigation planning, multimedia technologies; examining audio, picture and videos, examining meta data, investigative techniques, scripting languages, file systems, data storage and transport technologies, Hexadecimal and ASCII, operating systems
7	Conduct Windows Investigations Utilizing Encase	You are presented with evidence from a crime scene and are required to carry out a number of forensics Windows investigations using Encase (Encase features, browser forensics, use of GREP, scripting, memory forensics, email forensics, GREP and file analysis, other Windows artifacts)	Sources of forensics evidence, report writing, affidavits, investigation planning, multimedia technologies; examining audio, picture and videos, examining meta data, investigative techniques, scripting languages, file systems, data storage and transport technologies, Hexadecimal and ASCII, operating systems
8	Conduct Windows Investigations utilizing FTK	You are presented with evidence from a crime scene and are required to carry out a number of forensics Windows investigations using FTK (FTK features, registry forensics and anti-forensics).	Sources of forensics evidence, multimedia technologies; examining audio, picture and videos, examining meta data, investigative techniques, scripting languages, file systems, data storage and transport technologies, Hexadecimal and ASCII, operating systems

6 Learners demonstrate the appropriate use of multiple digital forensic tools and technologies in a variety of criminal and security investigations.

6.1	Use Forensic Tools and Techniques
6.1.1	Utilize tools such as Encase, FTK, Open Source, Imaging
6.1.2	Image a live system running Windows/Linux
6.1.3	Imaging using hardware-based tools
6.1.4	Prepare collection media for compatibility with Windows, Linux and Mac
6.1.5	Acquiring a RAID
6.1.6	Acquiring and analyzing data from NAS and SAN
6.2	Evaluate sources of Forensic artifacts
6.2.1	Analyze computer components (include booting in a controlled environment)
6.2.2	Analyze electronic devices
6.2.3	Compare different SCSI/Small Computer System Interface Specifications
6.2.4	Examine media including viewing EXIF data
6.2.5	Examine memory (RAM)
6.2.6	Analyze mobile devices (Android, iOS, BlackBerry, PDAs and data from Flash Media)
6.2.7	Analyze network artifacts
6.2.7	Analyze Web artifacts
6.2.8	Collecting data in the cloud
6.3	Perform Malware Analysis
6.3.1	Detect unauthorized devices
6.3.2	Perform static malware analysis
6.3.3	Perform dynamic malware analysis
6.4	Investigate Mobile Technology
6.4.1	Examine hardware and communication
6.4.2	Evaluate 3G-5G
6.4.3	Examine wireless security (include use of wireless network scanner to identify local wireless access point)
6.4.4	Examine how to connect to encrypted wireless access point
6.4.4	Analyze encryption
6.5	Investigate Multimedia Technologies
6.5.1	Examine audio, pictures, videos,
6.5.2	Analyze digital fingerprints/devices or fingerprints
6.5.3	Utilize various file formats
6.5.4	Examine meta data
6.6	Analyze Social Media Artifacts
6.6.1	Examine social networks
6.6.2	Utilize analysis techniques (harvesting, etc.)
6.6.3	Examine IM, chat logs, configuration files, chat logs
6.7	Utilize Visual Analysis
6.7.1	Apply link analysis
6.7.2	Trace analysis
6.7.3	Utilize filtering
6.8	Use CTRIP
6.8.1	Characterize CTRIP users to a file file to access
6.8.2	Characterize CTRIP users to a file file signature analysis
6.9	Analyze online and cloud-based gaming
6.9.1	Identify evidence sources used in the program
6.9.2	Use corporate cloud investigation techniques

Learner Demonstrations

	5	6	7	8
6.1				
6.2				
6.3				
6.4				
6.5				
6.6				
6.7				
6.8				
6.9				