LESSON: Digital Forensics

Primer

At the beginning of this lesson, please remember to remind the students about the career outcome. This module includes two short labs: the first lab focuses on Forensics Imaging Using FTK, while the second lab is related to Memory Acquisition. We highly recommend that instructors plan ahead to allocate sufficient time for these labs to ensure students have ample opportunity to practice.

For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

- Check-in with the students to see if they have any questions or need further clarification from any subject from the last class and self-study module.
- Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
- Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
- For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
- Labs are to be demonstrated live for each module. The demonstration of labs is the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.

Summary

In this lesson, learners will explore digital forensics within cybersecurity, covering the collection, analysis, and reporting of digital information to prevent breaches. The curriculum extends beyond technical aspects, exploring cybercrime investigations, fraud, and identity theft. Legal considerations, including processes, ethics, and admissible evidence, are highlighted, emphasizing strict adherence to evidence collection procedures. The scope spans live and powered-off systems, incorporating domains like live, disk, network, and memory forensics, along with advanced areas like mobile, cloud, and malware forensics. Learners will grasp the importance of preserving data integrity, following a

meticulous evidence collection process, including identification, preparation, acquisition, preservation, and documentation. Specific tools and methods for forensic imaging and memory dumping, along with associated risks, are covered, and the lesson emphasizes legal risks such as privacy breaches and jurisdictional overreach.

Objectives

- Define the concept of digital forensics.
- Discuss the legal and ethical considerations involved in digital forensics.
- Differentiate between live and powered-off systems when conducting a forensics investigation.
- Summarize the various domains of digital forensics.
- Identify the four steps of the NIST digital forensics framework.
- Explain the purpose of collecting evidence in digital forensics.
- Recognize the importance of preserving data integrity.
- Identify the steps before and during the evidence-collection process.
- Describe the forensic imaging procedure, including the existing types, tools, benefits, and drawbacks.
- Recognize the significance of volatile data and volatile memory in forensic analysis.
- Explain the process of memory dumping, including the tools and data sources used.
- Identify the different types of memory dumps.
- Describe the use of FTK Imager for memory dumping.
- Recognize the importance of documentation for evidence preservation.
- Identify the different tools used for documentation.
- Define the concept of chain of custody (CoC), including the questions it should answer.
- Describe the process of captured evidence verification.
- Discuss the technical and legal risks involved in the collection stage.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
5 min	**Career Outcomes Content Reminder**	● Remind learners about the Career Outcomes module to ensure that they know that the materials are available and to complete the assigned modules. ● This module will help the learners do the following: ○ Create a job search strategy with daily/weekly/monthly goals to help them focus on securing interviews. ○ Use referrals to tap into positions that aren't open to the public. ● Learners will receive an email inviting them to create an account for Big Interview. This platform allows them to sharpen their interviewing skills and utilize tools and resources to prepare for the technical interview. Learners who have not received an email

		should connect with their career coach. They can connect with their SSM if they do not know who their career coach is. ● The Career Outcomes module can be found at the end of Week 2 of the Digital Forensics and Incident Response module. ● Students can reach out to their SSM for questions and help if they need it.
2 min	**Lesson Opener:** Digital Forensics	● Introduce learners to the importance of digital forensics in cybersecurity.
5 min	**Real World Scenario:** Digital Forensics	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
2 min	**Lesson Companion:** Digital Forensics	● Review the lesson companion, and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
20 min	**Cyber Uncovered:** Understanding Digital Forensics	● Start by explaining the role of digital forensics in a cybersecurity incident. Emphasize its purpose in collecting, analyzing, and reporting digital information. ● Discuss how digital forensics extends beyond incident handling to include a variety of activities, such as investigating cybercrimes, fraud, and identity theft. ● Describe the legal processes, ethical considerations, and investigative techniques involved in digital forensics. ● Highlight its importance in establishing court-admissible facts.. ● Explore the legal complexities, including stringent procedures for evidence collection, chain of custody, and adherence to privacy laws. ● Discuss the significance of non-repudiation in rendering findings legally defensible. ● Explain the two main scopes of digital forensic investigations: Live and powered-off systems. ● Discuss the objectives and advantages of each approach. ● Introduce essential domains like live forensics, disk forensics, network forensics, and memory forensics. ● Explain their relevance and applicability in different scenarios. ● Explore additional domains focused on criminal misconduct, including email forensics, database forensics, and social media forensics. ● Discuss their roles in specific investigations. ● Introduce advanced domains like mobile forensics, cloud forensics, and malware forensics. ● Discuss the expertise and tools required for these specialized areas. ● Outline the digital forensics process, emphasizing the need for customization based on legal standards. ● Discuss regional variations in laws regarding evidence handling, privacy, and surveillance.

		● Provide an overview of the SANS and NIST frameworks for integrating forensic techniques into incident response. ● Focus on NIST's four-step process: Collection, examination, analysis, and reporting. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
2 min	**Real world scenario:** Understand Digital Forensics	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
5 min Break		
20 min	**Cyber Uncovered:** Evidence Collection	● Begin by emphasizing the critical role of the collection phase in digital forensics and its significance in maintaining the integrity of evidence for legal proceedings. ● Explain when collection typically occurs and the difference between initial incident-related artifact collection during incident response and systematic data gathering by a dedicated forensics team. ● Discuss the central concept of maintaining data integrity in digital forensics and its importance in distinguishing forensic investigations from non-forensic ones. ● Outline the five key steps in the evidence collection process: Identification, preparation, acquisition, preservation, and documentation. Emphasize that success starts before the actual acquisition of evidence. ● Explore how the scope of the investigation influences the necessity and relevance of evidence collection, considering factors such as data source value, priority of volatile data, and the effort required. ● Discuss the preliminary steps before evidence collection, including the identification of data sources, selection of acquisition tools, confirmation of legal authority, and preparation for documentation. ● Highlight the variability in the approach and choice of tools based on specific needs, types of devices, the nature of the incident, and the legal context. Discuss methods like volatile data collection, forensic image creation, and network device data collection. ● Explain the concept of forensic imaging as the most common collection procedure in digital forensics, emphasizing the creation of an unaltered digital clone or image for further evidence extraction.

		● Briefly describe several types of forensic imaging, including the disk-to-image file, disk-to-disk copy, logical acquisition, sparse acquisition, and remote imaging. ● Discuss industry-standard imaging software like FTK Imager and dd, the importance of write blockers, and the use of dedicated devices in professional forensic teams, such as Logicube's Falcon. ● Explain different capture formats, including raw format, proprietary formats, and Advanced Forensic Format (AFF), as well as their characteristics. ● Explore the advantages and disadvantages of forensic imaging, highlighting aspects like providing an exact copy, time consumption, artifact extraction, and potential encryption issues. ● Provide recommendations for imaging, including choosing the right capture format, using external sources, employing sterilized media, completing memory acquisition before drive acquisition, and properly documenting the capture process. ● Walk through the steps of using FTK Imager for forensic imaging, emphasizing careful review of settings before initiating the imaging process. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Evidence Collection. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
5 min	**Real world scenario:** Evidence Collection	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
20 min	**Lab:** Forensic Imaging Using FTK	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
5 min	**Pulse Check**	● Before you launch the pulse check, explain each section clearly, and encourage the learners to participate in the survey. ● After administering the survey, share the poll results with learners and ask learners to provide feedback ● Encourage learners to attend office hours with the associate instructor.
5 min Break		
20 min	**Cyber Uncovered:** Volatile Artifacts	● Emphasize the definition of volatile data and its significance in incident response and forensic analysis. ● Explain the types of information included in volatile data, such as system data, network connections, running processes, and logged-in users. ● Introduce memory imaging tools like FTK Imager and DumpIt for secure data collection in Windows systems.

		● Discuss the complexity of memory captures in Linux systems, highlighting the need for expert knowledge and specific kernel modules. ● Describe key data sources related to volatile evidence, including random access memory (RAM), swap space, hibernation file, and page file. ● Illustrate the role of each data source in preserving the system state and functionality. ● Introduce the concept of memory artifacts resulting from dumping memory. ● Define and differentiate between memory dump and crash dump, explaining their purposes and applications. ● Discuss circumstances where using memory dumping tools might be impractical and the potential use of a system crash to generate a dump as an alternative. ● Outline the steps for memory dumping when dumping tools are available. ● Stress the importance of avoiding unnecessary interaction with the target system and the verification, labeling, and documentation of the artifact. ● Provide a step-by-step guide on using FTK Imager for memory dumping. ● Include details about specifying the destination, confirming settings, and initiating the memory capture process. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Volatile Artifacts. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
20 min	**Lab:** Memory Acquisition	● Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. ● Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance.
5 min	**Real world scenario:** Volatile Artifacts	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
5 min Break		
20 min	**Cyber Uncovered:** Evidence Preservation	● Explain the significance of documenting digital evidence collection. ● Emphasize its role in maintaining evidence integrity and ensuring admissibility in legal proceedings. ● Discuss how detailed documentation provides a clear audit trail. ● Highlight the importance of transparency and how it allows other investigators to understand and replicate the forensic process. ● Introduce note-taking equipment such as digital voice recorders or note-taking apps.

		● Discuss the use of cameras or smartphones for photographing evidence and scenes. ● Present documentation templates, specifically chain of custody (CoC) forms. ● Define the chain of custody (CoC) in digital forensics. ● Emphasize its role as a chronological document that tracks evidence handling from collection to court presentation. ● Explain the importance of answering key questions in the CoC, including why, where, what, when, who, and how. ● Discuss examples for each question, such as the purpose of accessing evidence and the method used for handling it. ● Explore the critical role of isolating and preserving digital evidence. ● Introduce preservation techniques, focusing on hashing as a common method for verifying a file's authenticity. ● Discuss the risks associated with incomplete collection, loss of volatile data, alteration of evidence, data corruption, and time constraints. ● Emphasize the potential consequences of each risk on the overall investigation. ● Explore legal risks, such as breach of privacy, chain of custody issues, and jurisdictional overreach. ● Discuss the implications of these legal risks on the admissibility of evidence in legal proceedings. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Evidence Preservation. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
25 min	**Real World Scenario:** Evidence Preservation	● Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation.
2 min	**Midpoint Course Survey**	● Allocate 2 minutes to facilitate the completion of the Midpoint Survey. ● Encourage learners to provide honest and constructive feedback about their learning experience.
3 min	**Discussion Board**	● Allocate 3 minutes Review Discussion Board Slides and how it impacts students' final grades. ● Point out the new changes in the discussion board. For instance, students are not required to reply to their peers. ● The posts are only required in the first 3 weeks.
15 min	**Lesson Closure**	● Encourage learners to read ahead of time ● Provide learners additional resources to read / practice and assign homework (e.g., future labs) before you demonstrate the labs during the next class ● Spend some time to highlight what are the key takeaways from today's lesson

		● Important topics covered during the class includes: ○ Highlight the key takeaway during the digital forensics overview ■ Digital Forensics in Cybersecurity focuses on collecting, analyzing digital evidence on electronic devices and reporting the findings ■ Digital Forensics includes various activities beyond technical analysis such as cyber criminal investigations, Fraud, and identity theft ■ Legal aspect includes legal proceedings, and ensuing that the evidence collected is admissible in the court ■ The scope of the investigation includes memory forensics, power-off devices, hard drive, and network forensics ○ Highlight the key takeaway during the collection phase: ■ Identification, acquiring, and preserving the digital evidence ■ Preserving evidence and chain of custody are one of the most important steps ■ Forensic imaging creates an exact copy of the evidence without any modifications ■ Forensics imaging includes image-to-image file, disk-to-disk copy, and logical copy ○ Highlight the key takeaway for volatile artifacts ■ Volatile artifacts includes RAM or volatile memory, swap file (Linux), and page file (Windows) ■ Memory dump aims to capture the volatile memory content to a file ■ FTK image can be used to capture the windows memory including the page file ■ Memory dumping recommendation is to limit the interactions with the team ○ Highlight the key takeaway for evidence preservation ■ Documentation of the digital evidence, hashing the files to preserve/verify their integrity, and admissibility in court ■ Some of the risks includes loss of data, and potential modifications ■ Legal risk includes privacy breaches, chain of custody issue, and jurisdictional overreach
	Add Additional Time Filler	● Review using Kahoot or other similar platforms ● Conduct interview preparation conversations ● Continue discussions on real-world scenarios

		● Demonstrate how to create users in Linux and grant them permissions ● Discuss different career paths in cybersecurity and highlight the roles that require Linux skills