LESSON: Digital Artifact Examination

Primer

This module includes two short labs: the first lab focuses on Autopsy Walkthrough using, while the second lab focuses on Recovery Browser Artifacts. This module also contains a short exercise where the learners get to analyze images using Google's Vision AI. 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

- 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.
- At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.

Summary

In this lesson, learners will focus on advanced digital data analysis techniques for forensic examination. Learners will explore key principles, including binary data interpretation, filesystem structures, and overcoming OS limitations like compression and encryption. Practical skills involve securely mounting disk images, searching for malicious content, and using common forensic tools like EnCase Forensic and Autopsy. Special features of forensic software, such as file carving, timeline analysis, and AI integration, will be covered. The lesson highlights Autopsy's open-source platform and powerful analytical

capabilities, emphasizing its role in browser history analysis. Learners will understand file carving, magic bytes, and the significance of indexing and classification in forensic tools. Browser forensics, anti-forensic techniques, and methods to beat them, including steganography and altering timestamps, will be explored. The lesson concludes by stressing the importance of vigilance in identifying anomalies and irregularities in digital investigations.

Objectives

- Recognize the centrality of a forensic examination in a digital investigation and define its objective.
- Describe essential computer data concepts, including partitions, sectors, and filesystems.
- Identify the methods available to overcome OS limitations in forensic analysis.
- Explain how to securely mount disk images in Windows and Linux environments.
- Review the concept of file carving.
- List popular forensic software tools and describe their unique features.
- Recognize common magic byte headers and file types.
- Explain how AI enhances the classification process in forensics.
- Recognize the need to include browser data in modern forensic investigations.
- Identify the types of artifacts stored by browsers and their location.
- Describe specialized browser forensic tools.
- Explain how to analyze browser history using Autopsy.
- Define the concepts of anti-forensics and steganography.
- Identify common anti-forensic and steganography techniques.
- Explain how alternate data streams (ADS) work.
- Describe the anomalies that forensic investigators must look for to defeat anti-forensic practices.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Digital Artifact Examination	● Introduce learners to the importance of digital artifact examination in cybersecurity.
5 min	**Real World Scenario:** Digital Artifact Examination	● 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 Artifact Examination	● 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:** Image Examination	● Emphasize the definition of examination in the context of digital forensics. Discuss its role in the analysis of digital evidence and its significance in legal cases. ● Discuss the necessity of examination in forensic investigations. Highlight the investigator's goal to distill vast amounts of information into actionable intelligence. ● Explain the representation of computer data as binary information. Describe how the operating system interprets this binary information through the filesystem. ● Explore logical concepts and structures crucial for making sense of data on a drive. Discuss partitions, sectors, and filesystems as integral components of data organization. ● Discuss storage logic, focusing on sectors overwriting. ● Discuss the concept of bypassing OS limitations in examination. Explore examples like data compression, corruption, encryption, and access control mechanisms. ● Explain the process of extracting metadata, logs, and additional artifacts during examination. Discuss the importance of these artifacts in understanding user activities and system events. ● Differentiate between mounting and examining a disk image. Discuss the factors influencing the choice between the two approaches in forensic investigations. ● Walk through the process of forensically mounting a disk image using OSFMount on Windows. Provide step-by-step instructions, emphasizing the importance of choosing the "read-only" option for data integrity. ● Explain the Linux approach to forensically mounting a disk image. Share the command-line example for mounting and discuss the significance of the "read-only" option. ● Discuss the actions a forensic investigator can take after successfully mounting a disk image. Emphasize tasks like examining directory structures, exploring system artifacts, and scanning for malicious content. ● 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:** Image Examination	● 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.
5 min Break		
20 min	**Cyber Uncovered:** Forensic Software and File Carving	● Emphasize the importance of forensic software in conducting thorough investigations. ● Highlight scenarios where forensic software is more suitable than manual methods.

		● Present the key forensic toolkits: EnCase Forensic, FTK, Autopsy, and Magnet AXIOM.
		● Briefly discuss the industry applications and capabilities of each toolkit.
		● Break down the distinctive features of forensic software:
		  ○ File Carving: Recovery based on content patterns.
		  ○ Timeline Analysis: Correlation of data to create a chronological timeline.
		  ○ Advanced Searching Capabilities: Keyword, hash, pattern, or metadata searches.
		  ○ Reporting Tools: Importance of clear, organized, and court-admissible documentation.
		● Focus on Autopsy as an open-source and accessible platform.
		● Discuss its user-friendly interface, analytical capabilities, and functionality enhancing plugins.
		● Highlight its significance for law enforcement, military, and corporate examiners.
		● Reinforce the concept of file carving as a method to recover files without relying on metadata.
		● Draw a connection to PhotoRec and the shared principle of recovering deleted files.
		● Explain the reliance on magic bytes for file carving.
		● Provide examples of magic byte sequences and their corresponding file types.
		● Explore the possibility of incomplete files in file carving.
		● Discuss the significance of incomplete data in the reconstruction process.
		● Discuss the additional benefits of file carving in forensic software like Autopsy.
		● Emphasize the contextual information provided, such as deletion location and history.
		● Explore the challenges of searching through large data sets.
		● Introduce how forensic tools like Autopsy address these challenges through indexing and sorting into categories.
		● Discuss the role of AI in forensic software, even before it became as popular and widespread as it is today.
		● Highlight how AI engines, integrated into tools like Encase and AXIOM, aid in data filtering and categorization based on patterns.
		● Draw a parallel between Google Images and forensic software.
		● Guide learners in utilizing Google's Vision AI for digital forensic analysis.
		● Discuss how image recognition in both cases enables searches based on recognized patterns rather than file names.
		● 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.

10 min	**Cyberskills:** Try it Yourself	● 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
2 min	**Real-World Scenario:** Forensic Software and File Carving	● 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	**Lab:** Autopsy Walkthrough	● 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 Break		
20 min	**Cyber Uncovered:** Browser Forensics	● Start by discussing the pivotal role web browsers play in our daily lives, emphasizing how they have become central to personal and professional activities. ● Explore the evolution of document editing, contrasting past practices with the present where cloud-based platforms like Office365 and Google Docs are more commonly used. ● Introduce the concept of browser forensics, highlighting the shift in forensic investigations from traditional artifacts on computers to the examination of browser-based data. ● Detail the types of data artifact browsers store, including browsing history, bookmarks, cookies, cache, and form data, explaining the significance of each in forensic investigations. ● Provide the file paths for locating browser artifacts in Google Chrome, Mozilla Firefox, and Internet Explorer/Microsoft Edge, ensuring students understand where to find this data. ● Introduce dedicated forensic tools like NirSoft BrowsingHistoryView and HstEx, explaining their purposes and how they aid investigators in analyzing browser history. ● Dive into the specifics of BrowsingHistoryView by NirSoft, elucidating how it aggregates browsing data across multiple browsers and simplifies the viewing and tracking of web activity. ● Walk through the steps of examining browser history in Autopsy, from case creation to data processing, highlighting the significance of web history analysis in the forensic process. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Browser Forensics. 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:**	● 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.

	Browser Forensics	
20 min	**Lab:** Recovering Browser Artifacts	● 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:** Anti-Forensics and Steganography	● Begin the lesson by explaining how adversaries obstruct forensic analysis using techniques like erasing, altering, or hiding digital evidence. Emphasize the need for forensic investigators to adapt to these challenges. ● Discuss the technique of altering timestamps and its impact on forensic investigations. Highlight the potential oversight that can occur if investigators only filter by recent dates. ● Explore the various techniques adversaries use to hide digital evidence, such as compressing executables and employing steganography. Discuss the challenges these techniques pose for investigators. ● Introduce the concept of steganography, emphasizing its purpose to conceal information within seemingly innocuous files or messages. Discuss how it remains undetectable to observers. ● Explore the idea of steganography leveraging data interpretation, especially focusing on the NTFS file system's view of files as data streams. Discuss how this makes hidden streams invisible. ● Explain the feature of alternate data streams (ADS) in the NTFS file system and its impact on file visibility in most browsers. Discuss the deceptive use of ADS by browsers. ● Discuss the intended use of ADS for computers, its invisibility in file explorers, and the simple method of accessing ADS using the command prompt. ● Explore practical scenarios involving ADS, highlighting its recognition by forensic software. Discuss more complex steganographic techniques used by adversaries, like hiding text in image files. ● Introduce publicly available steganography tools such as Steghide, OpenStego, and DeepSound. Discuss their specific applications, emphasizing the complexity of steganography tasks. ● Discuss the intricacies of steganography beyond basic concealment, involving cryptographic algorithms and complex digital structures. Highlight how these techniques evade detection.

		● Emphasize the challenges in identifying steganography and other anti-forensic techniques. Discuss the need for forensic analysts to look for anomalies, irregularities, and patterns indicating hidden information. ● Detail specific indicators that forensic analysts should consider when detecting anti-forensic techniques, including inconsistent timestamps, irregularities in data, suspicious communication patterns, and uncommon programs or software. ● 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.
25 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 for image examination ■ Perform detailed image analysis using forensics software such as Autopsy ■ Forensics imaging aims to sift through large data and identify relevant information such as deleted and hidden files ■ Forensic imaging captures a precise snapshot of digital evidence for examination without altering it. ■ Forensic imaging is vital for creating an unaltered duplicate of digital evidence for investigation ○ Highlight the key takeaway for Forensic Software and File Carving ■ Forensic software tools are essential for analyzing digital evidence, enabling investigators to uncover hidden or deleted data. This includes tools like EnCase, AXIOM, and FTK ■ Unique features of forensic software includes file carving, timeline analysis, advanced search capabilities, and sophisticated reporting tools ○ Highlight the key takeaway for Browser Forensics ■ Browser forensics is essential for retrieving crucial data such as browsing history, cookies, and cached files that can reveal user behavior.

		■ Browser history helps investigators identify visited websites, downloaded files, and online communications, aiding in digital investigations. This includes using tools like NirSoft BrowsingHistoryView ■ Nowadays the role of browser forensics is critical in legal and cybercrime investigations in providing critical evidence. ○ Highlight the key takeaway for Anti-Forensics and Steganography ■ Anti-forensics techniques aim to obstruct, hide, or destroy digital evidence, making forensic investigations more challenging. ■ Steganography involves concealing data within other files, such as images or audio, to secretly transmit information. ■ Understanding these methods is crucial for both cyber defense and forensic investigators to detect and identify the strategy used to hide data ■ ADS can be used to hide data using command prompt to access hidden data streams
	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