LESSON: Live Forensics

Primer

This module includes two short labs: the first lab focuses on Windows Live Forensics using, while the second lab focuses on Linux Live Forensics. 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 discuss live forensics, a practice that focuses on investigating operational systems, particularly volatile data. The relevance of live forensics is emphasized in the context of virtualization and cloud technologies, offering benefits like quicker investigations and on-site evidence collection. Challenges, including data integrity verification and the impact of anti-forensic tools, are explored. Learners will understand decision-making nuances based on the system's state, distinguishing between virtual machines, powered-on, and powered-off systems. Key artifacts, such as running processes, network connections, and temporary files, are identified, and the relationship between live forensics and memory forensics is clarified. Essential tools for live forensics, including Sysinternals Suite

and NirSoft, are introduced, along with the importance of documentation in recording investigative actions. The lesson covers initial system information gathering, key commands for information retrieval, live acquisition techniques, and the distinctive approaches of Windows and Linux forensic investigations. The significance of scripting and automation, the selection of appropriate scripts, and the use of community scripts like PowerForensics and Kansa are highlighted. Learners will explore the adoption of an attacker's perspective, using enumeration scripts such as LinEnum and J.A.W.S for comprehensive system information gathering and security auditing.

Objectives

- Recognize the significance of live forensics in cybersecurity investigations.
- Discuss the benefits and drawbacks of employing live forensics in digital investigations.
- Analyze the decision making process that takes place in a forensic investigation.
- List key artifacts in live forensics investigations.
- Differentiate between live and memory forensics.
- Identify essential tools for live forensics investigations.
- Recognize the benefits of portable executables in reducing the interaction with a system during an investigation.
- Recognize the importance of initial system information gathering in cybersecurity investigations.
- List key commands for information gathering.
- Summarize the live acquisition process.
- Identify the most relevant commands used to retrieve artifacts, including registry hives, logged-in users, running processes, recently accessed files, network connections, and DNS cache.
- Explain how to collect a list of external devices using USBDeview.
- Compare and contrast between Windows and Linux live forensics.
- List the main artifact locations in Linux.
- Identify the built-in tools in Linux that facilitate forensic data collection.
- Define the concept of static binaries in Linux.
- Identify key commands for accessing system information in Linux.
- Explain the concept of journaling in Linux.
- Identify the risks associated with performing live forensics under pressure.
- Recognize the benefits of scripting and automation in live forensics.
- List the considerations for selecting the appropriate scripts in live forensics.
- Identify popular community scripts for forensic purposes.
- Explain the importance of adopting an attacker's perspective in forensic investigations.
- Discuss how enumeration scripts can assist in system information gathering.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Live Forensics	● Introduce learners to the importance of live forensics in cybersecurity.

5 min	**Real World Scenario:** Live 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:** Live 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:** On-Site Forensics	● Briefly define live forensics as a subfield of digital forensics. ● Emphasize its focus on conducting investigations on systems while they are still running. ● Explore the impact of virtualization and cloud technologies on live forensics. ● Discuss the evolving relationship between live forensics and incident response (IR). ● Highlight the advantages of live forensics, including its potential for a shorter investigation process. ● Emphasize its role in producing reliable, on-site, and court-admissible evidence. ● Discuss drawbacks such as the challenge of verifying the integrity of volatile data. ● Explore issues related to data consistency, evidence reproduction, and the use of anti-forensic tools. ● Outline decision-making priorities for virtual machines, powered-on systems, and powered-off systems. ● Discuss the importance of considering the integrity and chain of custody in decision-making. ● Identify key live system artifacts, including running processes, network connections, login sessions, and temporary files. ● Explain the significance of analyzing clipboard data and unsaved documents during live forensics. ● Compare the objectives of live forensics and memory forensics. ● Highlight the differences in data extraction methods and the focus of each approach. ● Introduce essential tools in the live analysis toolkit, such as memory imaging tools, network traffic analyzers, and process viewers. ● Explain the purpose of each tool and its contribution to live forensic analysis. ● Discuss the importance of versatile tool suites for unpredictable live investigations. ● Introduce Sysinternals Suite and NirSoft as examples of versatile bundles with purpose-specific utilities. ● Emphasize the need for meticulous documentation in live forensics. ● Discuss the impact of investigator interaction with the target system and tools that minimize this impact. ● Introduce the concept of "portable executables" for reducing system interaction.

		● Discuss the value of these tools in live forensic analysis and the importance of careful tool selection. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on On-Site 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:** On-Site 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.
5 min Break		
20 min	**Cyber Uncovered:** Windows Live Forensics	● Discuss why Windows live forensics is considered unique and complex. ● Highlight the role of proprietary file formats and system structures, such as the Windows Registry. ● Emphasize the importance of obtaining system information at the start of a live investigation. ● Explain how recording hardware, OS, and software details provide context and aid in tracking the system being investigated. ● Introduce three essential commands for gathering information about a Windows system. ● Discuss the specific information provided by each command (systeminfo, ipconfig /all, wmic). ● Explain the significance of live acquisition after recording system information. ● Stress the importance of saving collected artifacts to removable drives or remote storage. ● Describe the methods (query user, Get-WmiObject) used to obtain a list of logged-in or remotely accessed accounts. ● Discuss how this information can assist in determining user activities during an incident. ● Introduce commands (tasklist /svc, Get-Process) to collect information about running processes. ● Explain why identifying active programs is crucial for forensic analysis. ● Explain how to use PowerShell to list recently accessed files in a specified directory. ● Discuss the relevance of confirming recently accessed files in an investigation. ● Guide learners on acquiring a copy of the registry using the reg command.

		● Discuss the importance of exporting specific hives (e.g., SYSTEM, SOFTWARE) for forensic examination. ● Introduce commands (netstat -ano, net session) to gather information about network connections. ● Explain how this data is crucial for mapping a device's network activity in digital forensics. ● Explain how to retrieve DNS cache records using the ipconfig /displaydns command. ● Discuss the relevance of DNS cache records in tracing internet activity during digital forensics. ● Discuss the need to retrieve a list of external devices connected to a system. ● Mention the use of tools like USBDeview for simplicity in obtaining this information. ● Introduce USB device classes and their identifiers. ● Discuss examples of device classes (e.g., Audio devices, Mass storage) and their corresponding identifiers. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Windows Live Forensics. 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:** Windows Live 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.
20 min	**Lab:** Windows Live Forensics	● 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:** Linux Live Forensics	● Discuss the fundamental differences in the approach to digital forensics between Windows and Linux systems. ● Highlight the reliance on specialized APIs and handles in Windows versus the file-centric approach in Linux. ● Explain the significance of artifact locations in a Linux system for digital forensics. ● Discuss the contents of /var/log and /var/run directories and their relevance to investigations. ● Introduce the built-in tools in Linux for forensic data collection. ● Provide examples of commonly used tools, such as dd, netstat, grep, and find, and their respective purposes. ● Explain the concept of static binaries and their use in Linux forensics. ● Emphasize caution when obtaining binaries from external sources. ● Demonstrate the use of dd for file and artifact cloning in Linux. ● Walk through the process of copying a file over the network using dd, pipes, and netcat.

		● Introduce various command-line tools for obtaining system information in Linux. ● Explain the purposes of commands like uname -a, inxi -Fxz, and lsblk. ● Discuss methods for viewing logged-in users in Linux using commands like who and w. ● Highlight the importance of checking access logs, especially for remotely accessed systems. ● Explain the use of the ps command for displaying information about active processes in Linux. ● Introduce the ps aux command and its ability to provide detailed information about running processes. ● Compare the retrieval of network connections in Linux to that in a Windows operating system. ● Discuss the usage of commands like netstat -ano and net session for obtaining network connection details. ● Introduce the concept of journaling as a file system feature in Linux. ● Demonstrate the use of the journalctl command for viewing journal entries. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Linux Live Forensics. 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:** Linux Live 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.
20 min	**Lab:** Linux Live Forensics	● 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:** Automating Live Forensics	● Start by discussing the urgency associated with live forensics and the reasons behind the need for swift actions. ● Emphasize the goal of containing threats and minimizing damage during live forensic investigations. ● Explore the potential risks of rushing through live forensics, such as human errors, overlooking critical data, and contaminating evidence.

		● Discuss real world scenarios where procedural mistakes could compromise the integrity of an investigation. ● Introduce the concept of scripting and automation in live forensics. ● Highlight how automation can significantly reduce the risk of human error, ensure consistency in evidence collection, and enhance the overall reliability of investigations. ● Discuss the importance of choosing the right scripts during the preparation phase of a live investigation. ● Encourage learners to think critically about the information gathered during incident response (IR) and what might have been missed. ● Guide them in considering commands, artifacts, and the creation of bash or batch files for efficient live forensic processes. ● Introduce popular community scripts, such as PowerForensics and Kansa, emphasizing their role in forensic data collection. ● Provide insights into their functionalities, e.g., detailed file system metadata gathering using PowerShell scripts. ● Discuss the post-compromise actions of adversaries, particularly their enumeration process to discover system details. ● Draw parallels between attacker enumeration and how forensic investigators might replicate this process for understanding breaches. ● Explore publicly available enumeration scripts for both Linux and Windows systems, such as LinEnum and J.A.W.S. ● Discuss the purpose of these scripts, their role in security audits, and how they aid in system and network analysis. ● Provide hands-on scripting practice sessions using examples from the lesson. ● Guide learners in creating simple scripts or using existing ones to perform basic forensic tasks. ● Conclude the lesson with a discussion on the ethical considerations of using scripts in live forensics. ● Emphasize the importance of caution when using community scripts and the potential impact on investigation outcomes. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Automating Live Forensics. 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:** Automating Live 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.
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 onsite forensics: ■ Live forensics focuses on systems that are running while prioritizing the volatile memory data ■ One of the key benefits of live forensics is its ability to expedite investigations by revealing important information from memory artifacts. These artifacts can provide insights into attacks and data that would typically be encrypted when at rest ■ Some of the challenges of live forensics includes preserving data integrity ■ The key artifacts for live forensics includes running processes, active network connection, login sessions, temporary files, clipboard data, and unsaved documents ○ Highlight the key takeaway for Windows Live forensics: ■ The initial system gathering is one of the most important step to understand the system's capabilities and potential vulnerabilities ■ systeminfo, ipconfig /all, wmic, query user, and Get-WmObject-Class, Win32_LoggedOnUser are among the command that can be used for information gathering ■ Live acquisition involves collecting artifacts such as memory images, and registry keys ■ DNS cache records can provide insights into the online activities and interactions with the external servers ○ Highlight the key takeaway for Linux Live forensics: ■ Key artifacts in Linux includes logs, which can be found under /var/log/, /var/run also contains PID files, and /proc contains kernel details ■ Linux has built-in tools such as dd, netstat, grep, find, which can help to facilitate the investigation ■ Linux also has static binaries which can be used to reduce the system interaction and for Linux systems that may not have the tools needed for an investigation

		○ Highlight the key takeaway for automating Live Forensics: ■ Performing live forensics under urgent conditions can lead to missing or overlooking critical data, or contaminating evidence due to human error. ■ Scripting and automation in live forensics helps to reduce human error, increase efficiency, consistency, and reproducibility. ■ Some of the tools that are publicly available include LinEnum, which provide a comprehensive mechanism to perform system information gathering, security auditing, and detecting weaknesses
	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