LESSON: Introduction to DFIR

Primer

This module includes two short labs. It's imperative to thoroughly explain the second lab, "File Recovery using Photorec," as it sets the foundation for what students can expect in the class. Additionally, we highly encourage you to demonstrate how to extract EXIF data using a photo of your choice.

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 discover the fundamental concepts of digital forensics and incident response (DFIR), which integrates cybersecurity and forensic science to effectively manage digital incidents. The lesson emphasizes the critical role of DFIR in modern organizational cybersecurity, covering its continuous process and key incident-related questions. Learners will explore DFIR considerations, specific incident scenarios, and gain insights into traditional and digital forensics, along with tools like PhotoRec. The lesson concludes by highlighting the contributions of NIST and SANS to the advancement of DFIR and the significance of frameworks in ensuring legal compliance and maintaining admissibility in

legal proceedings, providing a comprehensive understanding of the investigative process from incident detection to evidence recovery.

Objectives

- Define the concept of digital forensics and incident response (DFIR).
- Describe the context in which digital forensics and incident response became popular disciplines.
- Recognize the importance of considering DFIR as an ongoing effort during an incident.
- Compare and contrast digital forensics vs. incident response.
- Outline the questions that should be asked during a cybersecurity incident.
- Analyze DFIR case studies, including a data leak, a social engineering attack, a web server defacement, and a malware infection.
- Describe the goals of digital and traditional forensics.
- Differentiate between artifacts and evidence.
- Define Locard's exchange principle and its relevance to DFIR.
- Explain how PhotoRec can help recover lost files.
- Describe the role of metadata in digital evidence analysis.
- Recognize the importance of the NIST and SANS frameworks in DFIR.

Lesson Activities and Teaching Strategies

Estimated Time	Lesson Portion	Directions
2 min	**Lesson Opener:** Introduction to DFIR	● Introduce learners to the importance of DFIR in cybersecurity.
5 min	**Real World Scenario:** Introduction to DFIR	● 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:** Introduction to DFIR	● 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:** Introduction to DFIR	● Provide a comprehensive definition of DFIR, emphasizing that it is a merger of cybersecurity and forensic science principles. ● Highlight the overall objective of DFIR in investigating incidents, examining digital evidence, and preventing future risks. ● Explore the incident response (IR) aspect of DFIR, detailing its structured methodology. ● Clarify the importance of IR in managing security incidents and its chronological relationship with digital forensics. ● Define digital forensics (DF) within DFIR, focusing on the collection, preservation, and analysis of electronic evidence. Emphasize the application of DF in various scenarios, not limited to incident handling. ● Trace the historical evolution of digital forensics from recovering lost data to investigating fraud and misconduct. ● Discuss the formalization process, including the involvement of law enforcement agencies, private sectors, and the development of methodologies. ● Examine the reasons for the rise of incident response during the 2000s. ● Discuss the adoption of an incident response mindset by organizations to manage and mitigate cybersecurity incidents in real time. ● Explore the significant maturation of DFIR from the 2010s onward. Highlight the emergence of specialized tools, techniques, and standardized practices, along with the challenges posed by new technologies. ● Emphasize that DFIR is an ongoing effort that is carried out before, during, and after an incident. ● Discuss the importance of incident response planning and the application of digital forensics once an incident is detected. ● Introduce the various aspects of incident response (IR) and digital forensics (DF). Compare their focus, goals, phases, tools, key skills, and time sensitivity. ● Discuss the concept of an incident timeline within DFIR. ● Explain its role in understanding the chronological sequence of events during and after an incident. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on introduction to DFIR. 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**	● 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:** DFIR Case Studies	● Guide learners in understanding the primary questions an organization typically asks when facing a cybersecurity incident. ● Discuss the importance of differentiating between questions that focus on the incident itself and those aimed at resolving it. ● Emphasize the significance of asking questions related to incident resolution before an incident occurs. ● Discuss key players in a response team, clarify roles and responsibilities, communication channels, and the process of preserving forensic evidence. ● Encourage learners to engage in an open discussion about typical incidents and consider the varying factors that influence considerations, recommendations, or actions. ● Explore Case 1 (the Data Leak Incident) with the learners, guiding them in identifying relevant artifacts and actions in response to the incident. ● Share a real-life example relevant to the case study ● Discuss the relevance of artifacts, such as access logs, data export logs, and configurations of the compromised server. ● Guide learners in understanding the appropriateness of actions like securing exposed data, analyzing logs for unauthorized access, and notifying affected individuals. ● Prompt learners to think beyond the mentioned artifacts and actions. What other considerations might be relevant in this context? ● Lead a discussion on the relevance of artifacts, such as employee emails, workstations, and network logs of data flow in the case of a social engineering incident. ● Discuss the appropriateness of actions, such as resetting compromised credentials, conducting employee awareness training, and reviewing email filters. ● Encourage learners to brainstorm additional actions or considerations that might be relevant.

		● Guide learners in understanding the relevance of artifacts, such as web server logs, defaced web pages, and intrusion detection system alerts. ● Discuss the appropriateness of actions like restoring original web content from backups, analyzing the intrusion vector, and hardening web server security configurations. ● Encourage learners to think creatively about additional actions or considerations. ● Discuss the relevance of the following artifacts in the context of a malware infection incident: Malware samples, registry keys, and network traffic logs. ● Explore the appropriateness of the following actions: solating affected systems, conducting malware analysis, and deleting detected executable files. ● Prompt learners to consider other potential actions or factors that could be relevant in this scenario. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on DFIR Case Study. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
15 min	**Lab:** DFIR Considerations	● 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:** Mini-Investigation	● Explain the commonalities between digital and traditional forensics. ● Emphasize the shared goal of uncovering artifacts and evidence to reveal the truth about an event. ● Define artifacts and evidence in the context of investigations. ● Highlight the distinctions between artifacts and evidence, acknowledging that these terms are often used interchangeably although they are not the same. ● Provide three examples of evidence used in a court of law. ● List three examples of digital evidence in the field of digital forensics. ● Differentiate between admissible and inadmissible evidence in a court of law. ● Explain the impact of a data leak on an organization.

		• Discuss the immediate suspicion raised by a flash drive found in a conference room and consider its potential use in proving that files were leaked. • Explain Locard's exchange principle and its significance in forensic science. • Connect Locard's exchange principle to the transfer of material or data in the case of digital forensics. • Describe what happens when data is deleted from a digital device. • Discuss the role of specialized software in recovering deleted information and its implications for digital forensics. • Introduce PhotoRec as a powerful file-recovery software in digital forensics. • Highlight the unique features of PhotoRec, such as reading data directly from storage without overwriting files. • Explain how PhotoRec can be used with physical and digital copies of devices. • Discuss aspects that should be taken into consideration before starting the file recovery process, such as specifying file system types and recovery options. • Highlight the importance of linking recovered files to the investigated event to ensure they are considered as evidence. • Discuss the role of digital fingerprints (hash values) and metadata in establishing a timeline and tracing the source of the leak. • Define metadata and explain its significance in files. • Introduce EXIF data and the specific details it provides when files are produced by cameras. • Discuss the limitations of file explorers in displaying EXIF data. • Introduce tools like ExifTool for extracting EXIF data and its potential impact on investigations. • Be prepared to discuss the implication of the real world scenario presented at the beginning of class on Mini-Investigation. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
20 min	**Lab:** File Recovery Using PhotoRec	• 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:** Significant Entities and Frameworks	• Begin the lesson by explaining the significance of contributors to digital forensics and incident response (DFIR) practices. • Emphasis on the importance of having a framework • Introduce the two main organizations that contribute to DFIR: The NIST and SANS Institutes. • Highlight that their contributions have significantly advanced techniques, tools, and best practices in the field. • Discuss NIST's role in providing authoritative guidelines and frameworks for DFIR practices.

		● Emphasize the NIST Special Publication 800-86 and its focus on integrating forensic techniques into incident response. ● Explore the content of the NIST guide, emphasizing its value in offering structured approaches and best practices for digital forensics investigations. ● Share examples on how organization adapt the framework ● Discuss practical applications and real world scenarios where NIST guidelines can be beneficial. ● Transition to the SANS Institute's contribution, focusing on frameworks like the six stages of incident response. ● Highlight SANS's primary focus on training courses and its commitment to creating platforms for knowledge-sharing and networking. ● Discuss the educational events regularly hosted by the SANS Institute, such as conferences, webcasts, and events, emphasizing their role in providing DFIR practitioners with learning opportunities and a space to connect. ● Introduce the concept of frameworks in DFIR and their role in ensuring legal compliance. ● Discuss how standardized procedures contribute to the admissibility of digital evidence in legal proceedings. ● Explore how the principles of legality and due process are upheld by standardized procedures, emphasizing their essential role in forensic investigations. ● Be prepared to discuss the implication of the real world scenario presented at the beginning of class on the “Significant Entities and Frameworks.” There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario.
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 ○ Provide the main takeaway of DFIR definition ○ Summarize the difference between Digital Forensics and Incident Response ○ Provide a summary of the incident timeline ○ Provide the key takeaway for the following use cases ■ Data Leak (artifacts, actions) ■ Social Engineering(artifacts, actions) ■ Defacement (artifacts, actions) ○ Summarize the main goals for traditional forensics and the similarities with Digital Forensics

		○ Highlight the difference between artifacts and evidences, admissible and inadmissible evidence in the court ○ Provide the key takeaway for the Locard's exchange principle and how it applies to digital forensics ○ Provide a summary of EXIF data and the metadata ○ Highlight the main contributions of NIST and SANs frameworks in DFIR
	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