Lab Performing Incident Response and Forensic Analysis

Osamudiamen Eweka

Cyb-605-Z2 Principles of Cybersecurity

Utica University

Introduction

In the face of escalating cyber threats, organizations must swiftly and effectively respond to incidents that jeopardize their information systems infrastructure. An efficient incident response is essential for mitigating damage, curtailing recovery time and costs, and ensuring the admissibility of evidence in potential legal proceedings. Forensic analysis becomes pivotal in this context, with forensic analysts playing a critical role in ensuring that the evidence collected is preserved and processed according to legal standards, thus maintaining its integrity and admissibility in court (Grispos, 2015).

The incident response process involves a sequence of phases: preparation, detection, analysis, containment, eradication and recovery, and post-incident analysis, with a constant emphasis on the preservation of evidence. This structured approach not only addresses the immediate impact of cyber incidents but also bolsters the organization's defenses against future threats. Through practical exercises, such as analyzing PCAP files and disk images, participants will gain insights into the analysis phase, preparing them to draft and refine incident response reports that are both comprehensive and adaptable as new evidence emerges.

Objective

Upon the completion of this lab, participants will have acquired the ability to engage in forensic analysis as a critical component of an incident response investigation. They will gain proficiency in employing NetWitness Investigator for the forensic examination of Packet Capture (PCAP) files, enabling them to detect and analyze malicious network activities. Furthermore, participants will learn to use Autopsy for in-depth forensic analysis of disk images, uncovering vital digital evidence. A key skill developed will be the ability to correlate evidence from multiple sources, thereby enhancing their capacity to construct a comprehensive narrative of cybersecurity incidents. Finally, participants will master the formulation of detailed incident response reports, documenting their investigative process, findings, and recommendations, thereby encapsulating the essence of their forensic analysis in a coherent and impactful manner.

Lab setup

To successfully complete this lab, participants will need to utilize specific software and utilities, namely NetWitness Investigator and Autopsy. It is recommended that students familiarize themselves with these tools by exploring available resources on the Internet. This preparation will equip them with the necessary knowledge to navigate the software effectively during the lab exercises.

Section 1

Part 1: Analyze a PCAP File for Forensic Evidence

In the lab scenario involving Giggly Goofo's security incident on July 31, 2021, participants, acting as digital forensics specialists, are tasked with the analysis phase of incident response. They will use NetWitness Investigator for forensic analysis of a PCAP file to identify malicious network activity and Autopsy for examining a drive image from a potentially involved employee. The objective is to uncover evidence related to the data breach, correlating information across different sources to construct a narrative of the incident. This analysis will inform the creation of an incident response report, documenting the findings and contributing to strategies for preventing future breaches. Participants will follow a structured approach to import, organize, and analyze the evidence, utilizing the tools' features to efficiently navigate and interpret the data, ultimately aiming to piece together the sequence of events leading to the security breach Figure 1 below illustrates this practice (Jones & Bartlett, 2024).

Figure 1

Make a screen capture showing the Time Graph.

Note. The above image illustrates an effective analysis of the sessions within the PCAP file. When viewing in Bar Chart mode, placing your cursor over a particular bar reveals the number of sessions that took place during that time period.

In the investigation using NetWitness Investigator, participants identify critical evidence by first focusing on the Filename report, highlighting four .zip files and a suspicious clickme.exe file. Given the context of a game development studio's data breach, these files are scrutinized as potential exfiltrated data, with clickme.exe raising additional security concerns.

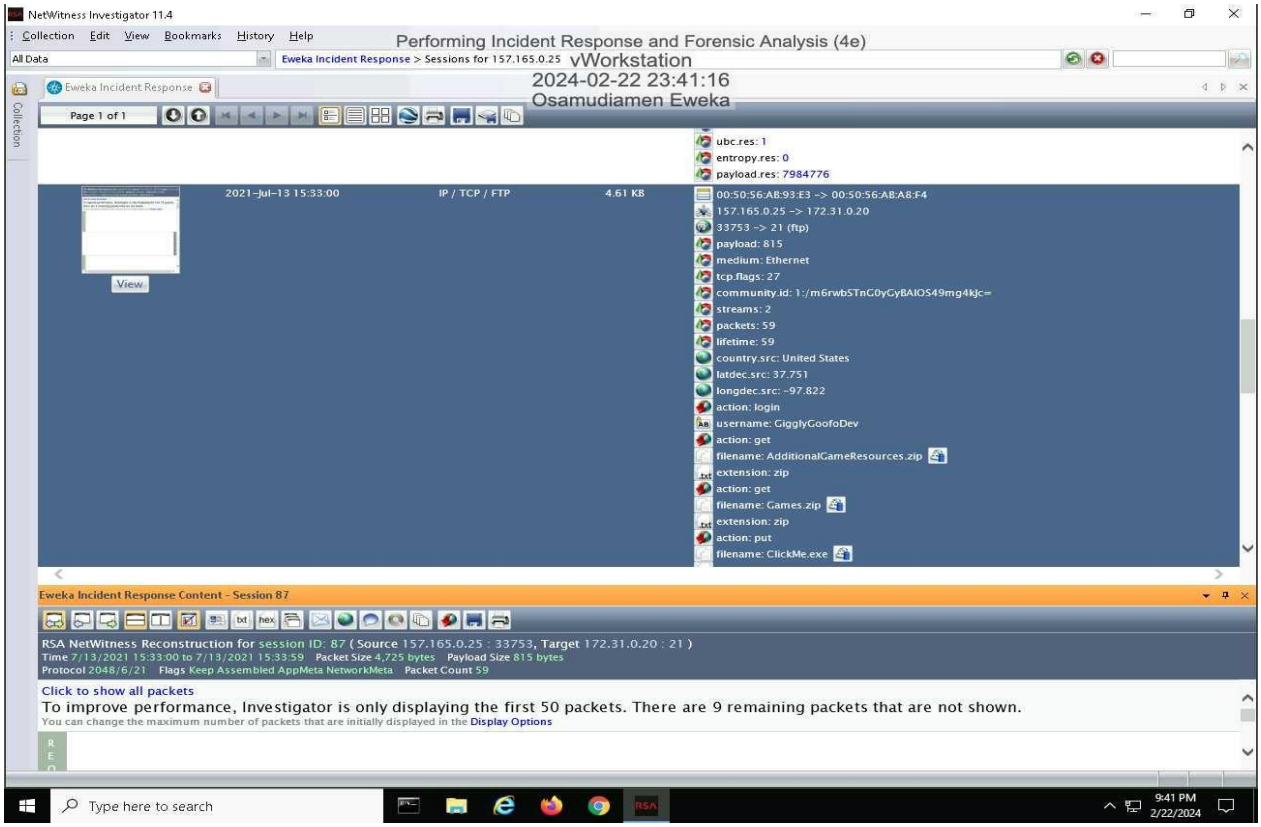
Delving into the Source and Destination IP Address reports reveals a standout external IP address, 157.165.0.25, diverging from the internal network's range. This external IP's interaction with the internal network marks it as a key suspect. A deeper examination of the sessions linked to this IP address uncovers a pivotal session dated July 13, 2021, at 15:33:00, featuring an File

Transfer Protocol (FTP) transfer of the identified .zip files using credentials associated with a legitimate user, GigglyGoofoDev.

This session's discovery, with details on IP addresses, credentials, and filenames, provides a solid lead in the breach investigation.

Figure 2

Make a screen capture showing the details of the 2021-Jul-13 15:33:00 session.



Note. Figure 2 above, captures a screenshot for the incident response report. This documented evidence forms a critical piece of the puzzle, linking specific network activities to the data exfiltration event and guiding further investigative and response efforts (Jones & Bartlett, 2024).

Section 1

Part 2: Analyze a Disk Image for Forensic Evidence

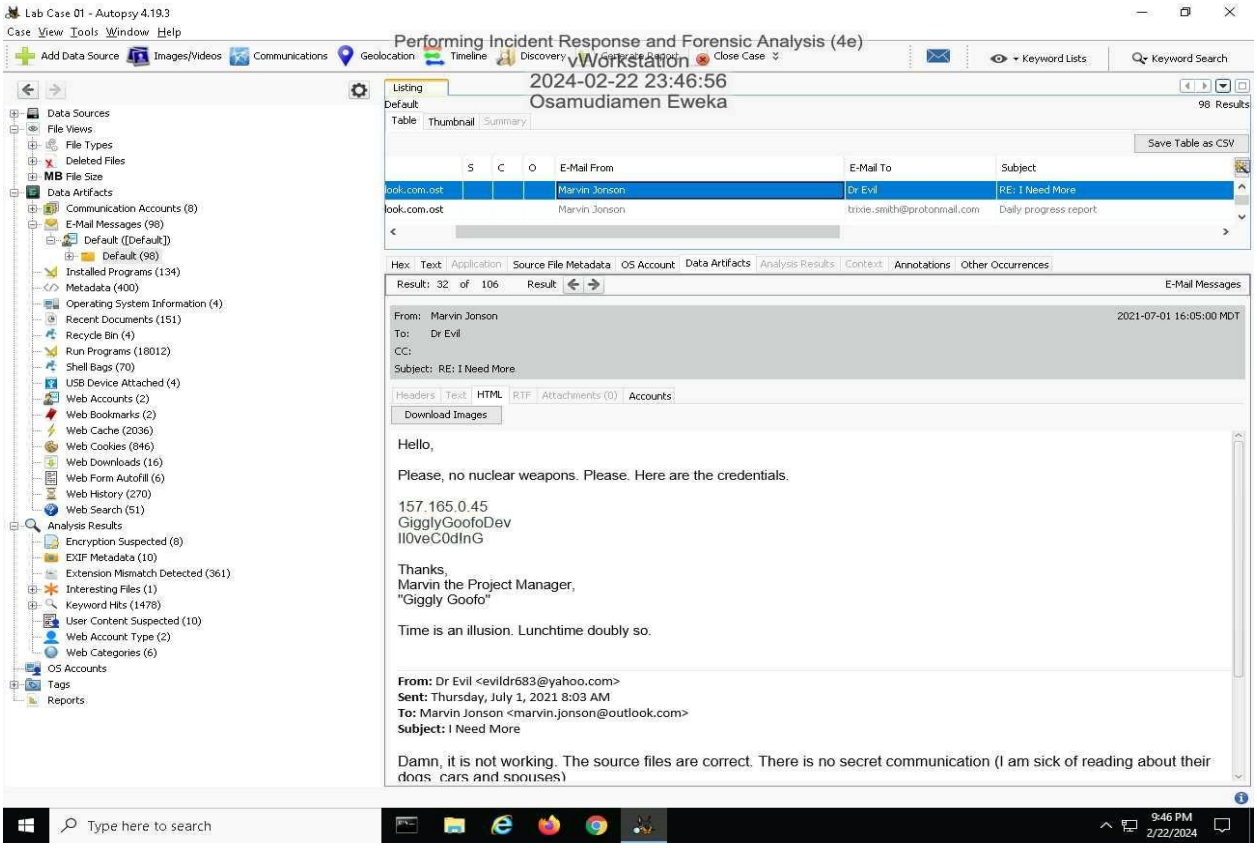
In this phase of the lab, attention shifts to analyzing the disk image from Marvin Jonson's laptop, a project manager at Giggly Goofo suspected of potential involvement in the data exfiltration incident. Utilizing Autopsy, a graphical interface for The Sleuth Kit—an open-source suite for forensic analysis—participants will examine the disk image for evidence. Autopsy's plug-in architecture allows for enhanced functionality, enabling a thorough examination of the drive image for signs of Marvin's involvement or evidence of impersonation by threat actors.

Upon launching Autopsy from the vWorkstation desktop and navigating through the case database to Marvin's email records, participants utilize the E-mail Parser module to scrutinize email messages stored in Marvin's Outlook account. This examination is crucial, given the preliminary analysis in Part 1, which identified data exfiltration from the Giggly Goofo FTP server utilizing compromised credentials. The hypothesis is that if Marvin were involved, evidence of the FTP credentials being communicated could be found in his email exchanges.

The detailed investigation leads to the discovery of an email from Marvin's account to a recipient named Dr. Evil, dated July 1, 2021, at 16:05 MDT. The email notably contains the FTP server’s IP address and valid login credentials, presenting actionable evidence that Marvin’s email account was used in the context of the data theft. However, the challenge remains in determining whether Marvin himself sent the email or if his account was compromised by an impostor. This distinction is critical for the subsequent steps in the investigation and for formulating the incident response.

Figure 3

Make a screen capture showing the email message containing FTP credentials and the associated timestamps.



Note. Figure 3 documents these findings by capturing a screenshot of the email, including the message contents and timestamps (Jones & Bartlett, 2024). This documentation is vital for the incident response report, providing a concrete link between the suspected internal actor and the security breach. The evidence uncovered through Autopsy not only advances the investigation but also emphasizes the importance of correlating data across different sources to build a comprehensive case narrative.

Section 1

Part 3: Incident Response Report and analysis

Date: February 23, 2024

Name: Osamudiamen Eweka

Incident Priority: High Priority

Incident Type: Include all that apply: Compromised System, Compromised User Credentials, Network Attack (e.g., Denial-of-Service (DoS)), Malware (e.g. virus, worm, trojan), Reconnaissance (e.g. scanning, sniffing), Lost Equipment/Theft, Physical Break-in, Social Engineering, Law Enforcement Request, Policy Violation, Unknown/Other.

Incident Timeline:

- Discovered: 2021-07-31, 10:30 AM
- Reported: 2021-07-31, 10:40 AM
- Occurred: 2021-07-13, 15:33:00 PM to 2021-07-13, 15:33:59 PM

Unusual login activities were identified during a security audit.

Incident Scope:

- Estimated quantity of system affected: Game Development
- Estimated quantity of users affected: Game developers, Sponsors, Players
- Third-party involved: Partners

Systems Affected by the Incident:

- Attack Sources: 157.165.0.25 : 33753
- Attack Destinations: 172.31.0.20 : 21
- Primary Functions of Affected Systems: Game server and developer workstation

Users Affected by the Incident: Marvin the Project Manager.

Section 2

Part 1: Identify Additional Email Evidence

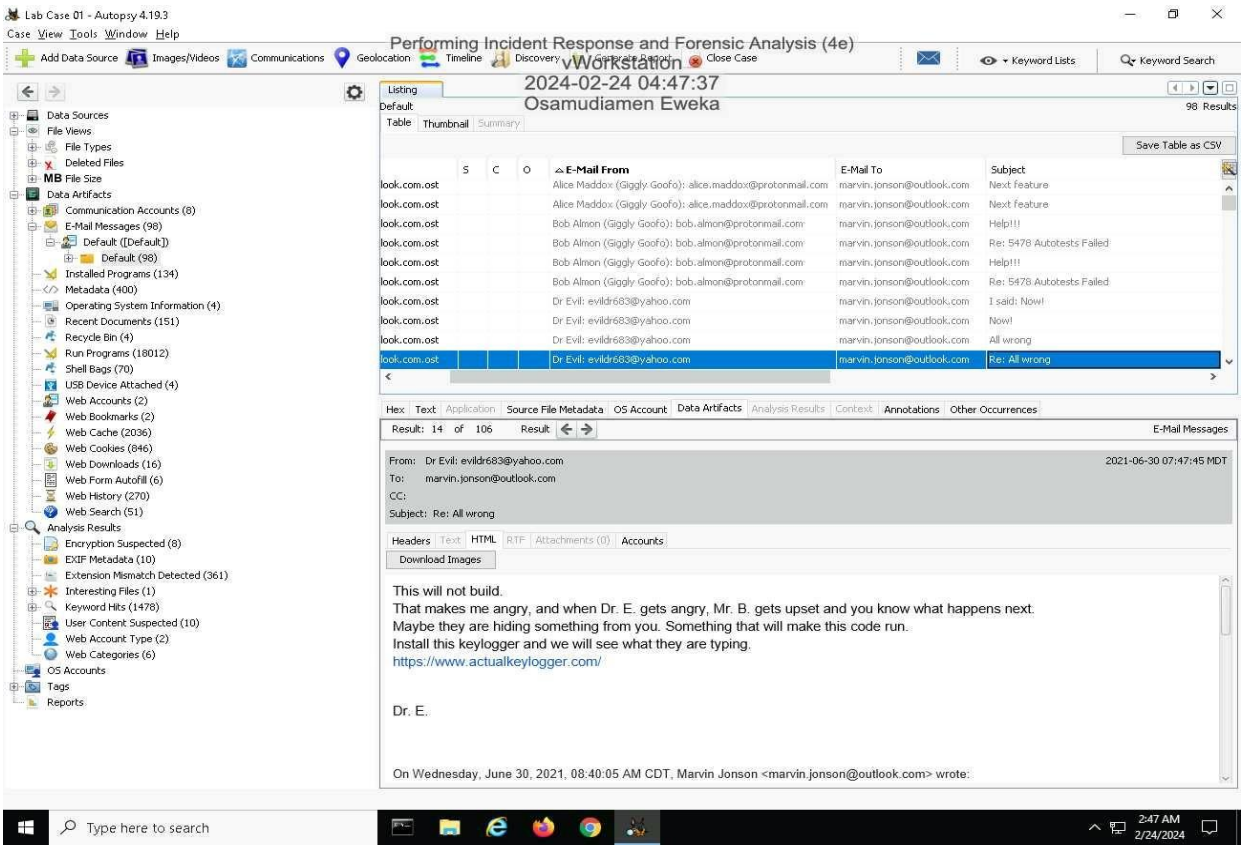
Upon submitting the initial incident response report and securing the compromised FTP server and Marvin Jonson's accounts, concerns arise about the incident's full extent not being fully captured. This worry stems from the ease with which access to the FTP server was compromised, suggesting potential further unauthorized activities.

Revisiting Marvin Jonson's email communications via Autopsy, particularly focusing on emails from Dr. Evil, reveals alarming instructions for installing a keylogger, tampering with firewall configurations, and altering scheduled tasks. These findings indicate not just data exfiltration but also ongoing unauthorized access and potential surveillance within the company's network. Such activities pose significant security risks, including the possibility of capturing sensitive information through the keylogger, creating vulnerabilities via firewall adjustments, and maintaining persistent, undetected access through changes to scheduled tasks.

These discoveries necessitate an expanded forensic analysis to understand the breach's full scope, including reviewing system logs, firewall settings, and scheduled tasks for signs of tampering. The investigation's evolution underscores the complexity of cyber incidents and the importance of a thorough and adaptable incident response strategy. Documenting these new findings will be crucial for updating the incident response report and guiding the ongoing response efforts.

Figure 4

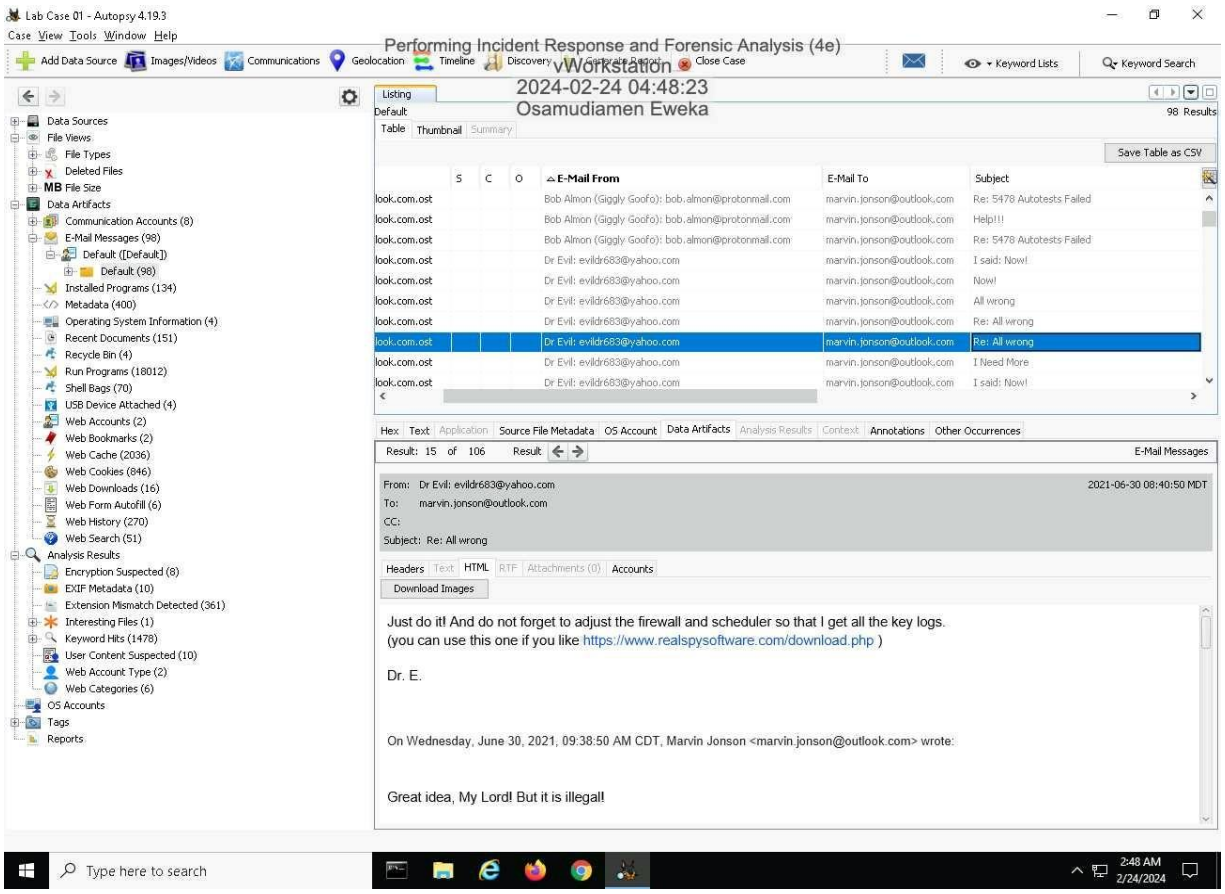
Make a screen capture showing the email from Dr. Evil demanding that Marvin install a keylogger.



Note. Figure 4 presents proof that Dr. Evil directed Marvin to implement a keylogger. Such instructions ought to trigger alarm and call for more thorough examination (Jones & Bartlett, 2024).

Figure 5

Make a screen capture showing the email from Dr. Evil reminding Marvin to update the firewall and scheduler.



Note. Figure 5 illustrates Dr. Evil's orders for Marvin to alter the firewall settings and update the scheduled tasks. These requests should raise alarms and undeniably necessitate additional probing (Jones & Bartlett, 2024).

Section 2

Part 2: Identify Evidence of Spyware

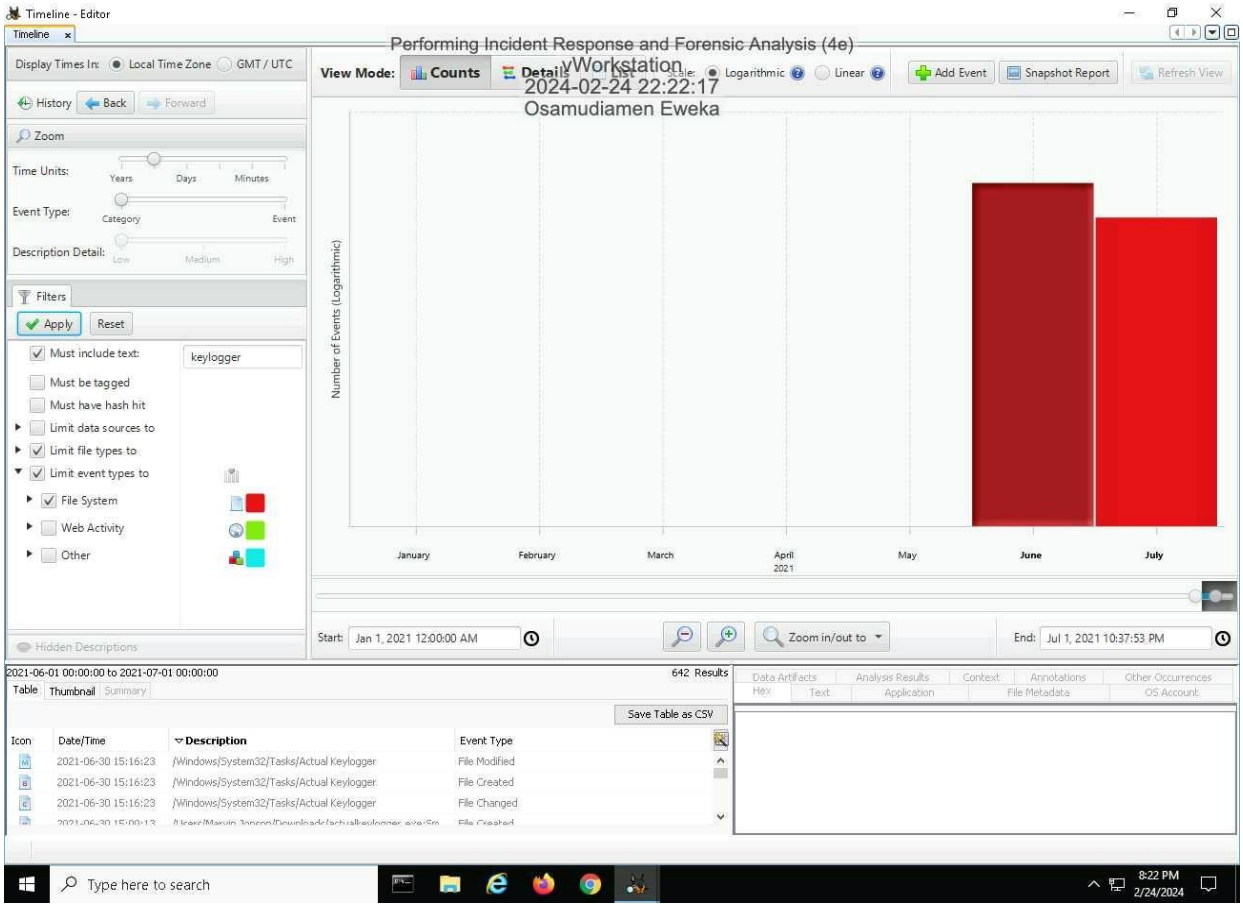
In this phase of the investigation, the focus shifts to examining Marvin Jonson's workstation for traces of a keylogger installation, unauthorized firewall changes, and newly implemented scheduled tasks. Utilizing Autopsy, participants navigate through the disk image to the System32 > Tasks directory to inspect the scheduled tasks. Here, they discover evidence of the Actual Keylogger software being scheduled, indicating potential unauthorized surveillance activities.

The investigation proceeds with the Autopsy Timeline feature to trace activities related to the keylogger. By applying filters within the Timeline Editor, participants narrow down the events to those specifically associated with keylogger activities. This process reveals significant events in June and July 2021, with a particular focus on June 30, where three events related to the Actual Keylogger indicate its scheduling.

This discovery suggests that the keylogger was indeed installed and activated on Marvin's workstation, raising questions about the purpose—whether for testing, espionage, or data exfiltration. The identification of these events underscores the necessity of further forensic analysis to understand the breach's full scope and the potential compromise of sensitive information.

Figure 6

Make a screen capture showing the three events that are related to the Actual Keylogger file in the /Windows/System32/Tasks folder with a June 30 timestamp.



Note. Figure 6 documents these findings meticulously, capturing screenshots of the timeline events, as this evidence will be crucial for updating the incident response report and guiding subsequent investigative and remedial actions (Jones & Bartlett, 2024).

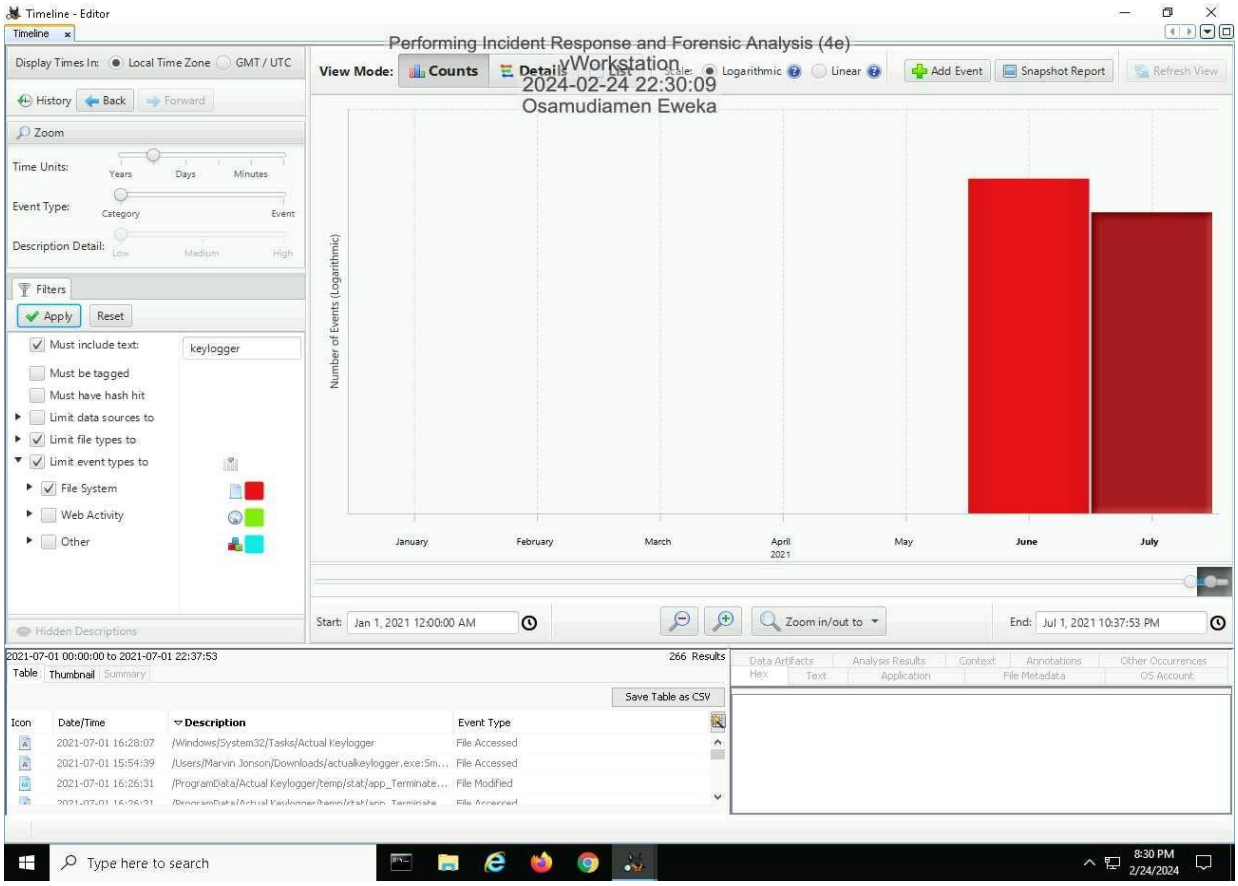
In the continued exploration of the incident involving Marvin Jonson's workstation, the investigation leverages the Timeline feature in Autopsy to pinpoint activities specifically related to the keylogger software. This meticulous approach focuses on identifying and documenting any actions executed by the keylogger, particularly looking into the sequence of events for the month of July.

Upon navigating the Timeline graph and honing in on the activities for July, a detailed examination of the events is conducted. By ensuring the Description column in the bottom-left pane is properly sorted, a critical discovery is made: a single event related to the Actual Keylogger file scheduled in the Windows/System32/Tasks folder, dated July 1. This event is pivotal as it confirms that the keylogger schedule was executed at the beginning of July, marking a significant point in the timeline of unauthorized activities on Marvin Jonson's workstation.

This finding is instrumental for the investigation, as it provides a clear indication of the keylogger being operational and potentially collecting sensitive information. The July 1 timestamp of this event could align with other unauthorized activities and data exfiltration efforts, underscoring the importance of this timeline in understanding the scope and impact of the security breach.

Figure 7

Make a screen capture showing the one event that is related to the Actual Keylogger file in the /Windows/System32/Tasks folder with a July 1 timestamp.



Note. Figure 7 above displays an event associated with the Actual Keylogger file located in the Windows/System32/Tasks folder, marked with a July 1 timestamp. This suggests that the schedule for the Actual Keylogger was executed on July 1 (Jones & Bartlett, 2024).

Result and Analysis

Question: Record the date and time that the keylogger's executable file was created.

Answer: 2021-06-30 15:16:23

Question: Record the date and time when the keylogger's executable file was last started.

Answer: 2021-07-01 16:28:07

Question: Record whether you think you have evidence to claim that Marvin opened the keylogger.

Answer: The evidence shows that Marvin Jonson at least opened the application, however it is unclear whether Marvin interacted with the application or just had it opened in the background.

Section 2

Part 3: Updated Incident Response Report and Analysis

Date: February 24, 2024

Name: Osamudiamen Eweka

Incident Priority: Unchanged, still High.

Incident Type: In addition to Compromised User Credentials and Policy Violation, a new incident type that applies is Malware because of the installation of the keyloggers.

Incident Timeline:

- (New) Keylogger Executable File Created: 6/30/2021 15:16:23
- (New) Keylogger Executable File Last Accessed: 7/1/2021 16:28:07
- Credentials Sent via Email: 7/01/2021 16:28:07 MDT
- Incident Occurred (packet capture session): 2021-07-13, 15:33:00 PM to 2021-07-13, 15:33:59 PM
- Incident Discovered: 7/31/2021 at 10:30AM EST.Incident Reported: 7/31/2021 at 10:40AM EST.

Incident Scope:

- The quantity of systems affected remains unchanged: Marvin Jonson's workstation and the Giggly Goofo Network; Attack Source, Attack Destination
- The quantity of users is affected is unpredictable, however Marvin Jonson is directly affected because of his interactions with Dr. Evil. There may be other users affected from the keylogger installed and other unauthorized changes.
- Third parties involved remains unchanged.

Systems Affected by the Incident:

- Attack Source: Source IP Address 157.165.0.25
- Attack Destination: Destination IP Address 172.31.0.20
- Primary Functions of Affected Systems: Giggly Goofo FTP Server contains confidential data files thatwere exfiltrated

Dr. Evil requested for the keylogger to be installed so they could see what they were typing.

Users Affected by the Incident: The main user impacted is Marvin Jonson, as he was pressured by Dr. Evil to install the keylogger and implement unauthorized modifications to his workstation. Based on the new evidence, there are no additional users affected by this incident.

Section 3

Part 1: Identify Additional Evidence of Data Exfiltration

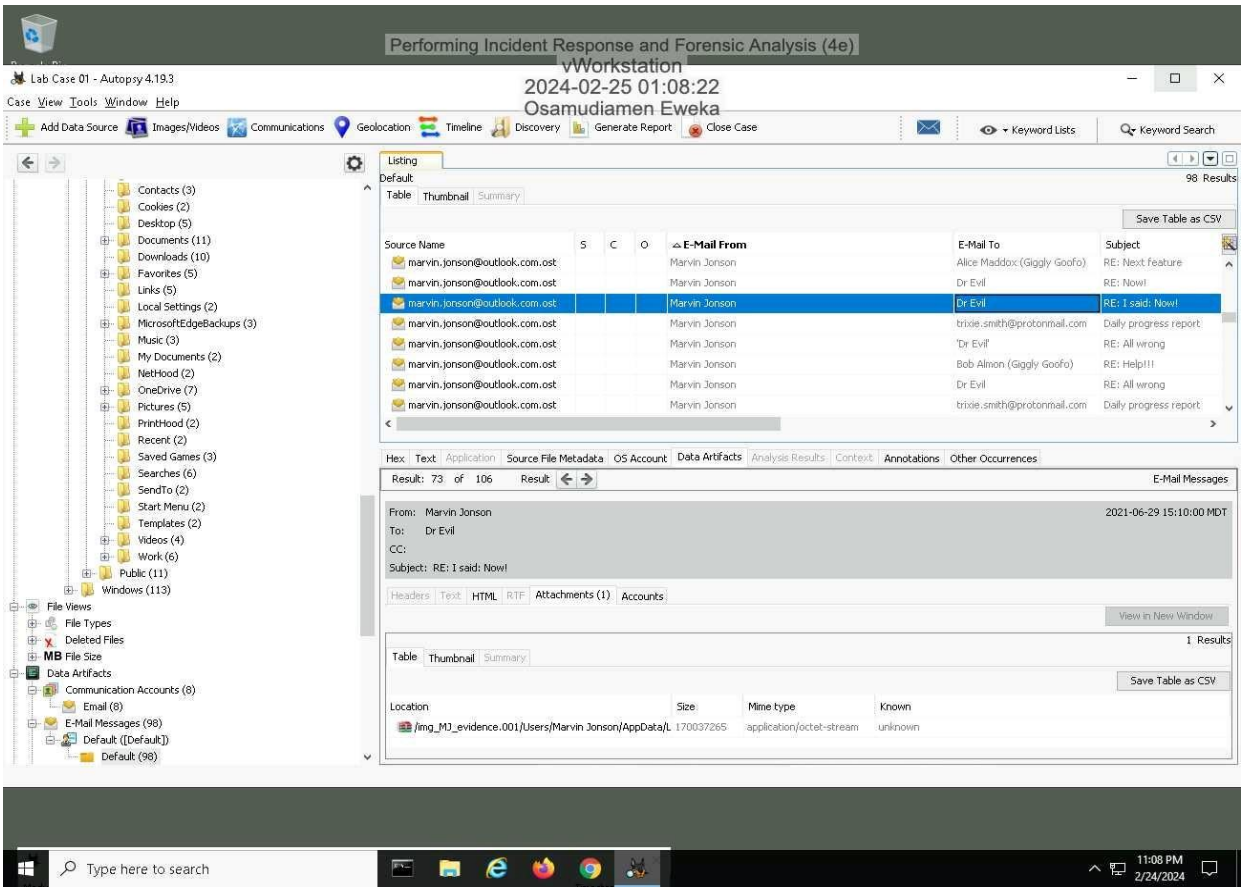
In the final phase of the investigation, lingering doubts prompt a focused review of Marvin Jonson's Outlook account for potential email-based file exfiltration to Dr. Evil. Leveraging Autopsy's E-mail parser, the investigation zeroes in on sorting and scrutinizing Marvin's emails, particularly emphasizing attachments. This targeted approach aims to uncover any smaller files that may have been discreetly sent via email, bypassing more heavily monitored data transfer methods.

Sorting through Marvin's Outlook database facilitates a streamlined identification of email attachments, enabling investigators to quickly detect any unauthorized file transfers. This crucial step is intended to reveal whether additional sensitive data was compromised, thereby broadening the understanding of the breach's extent and the methodologies employed.

Identifying further instances of data exfiltration through email attachments is key to constructing a full narrative of the incident. Any new findings will significantly enhance the incident response report, ensuring that the investigative team and leadership have a comprehensive view of the breach. This meticulous examination is essential for confirming the investigation's thoroughness and informing subsequent security enhancements to prevent similar incidents.

Figure 8

Make a screen capture showing an exfiltrated file in Marvin's Outlook database.



Note. Figure 8 sorts the data from Marvin's Outlook database to pinpoint extra files and attachments that were illicitly sent out via email (Jones & Bartlett, 2024).

Section 3

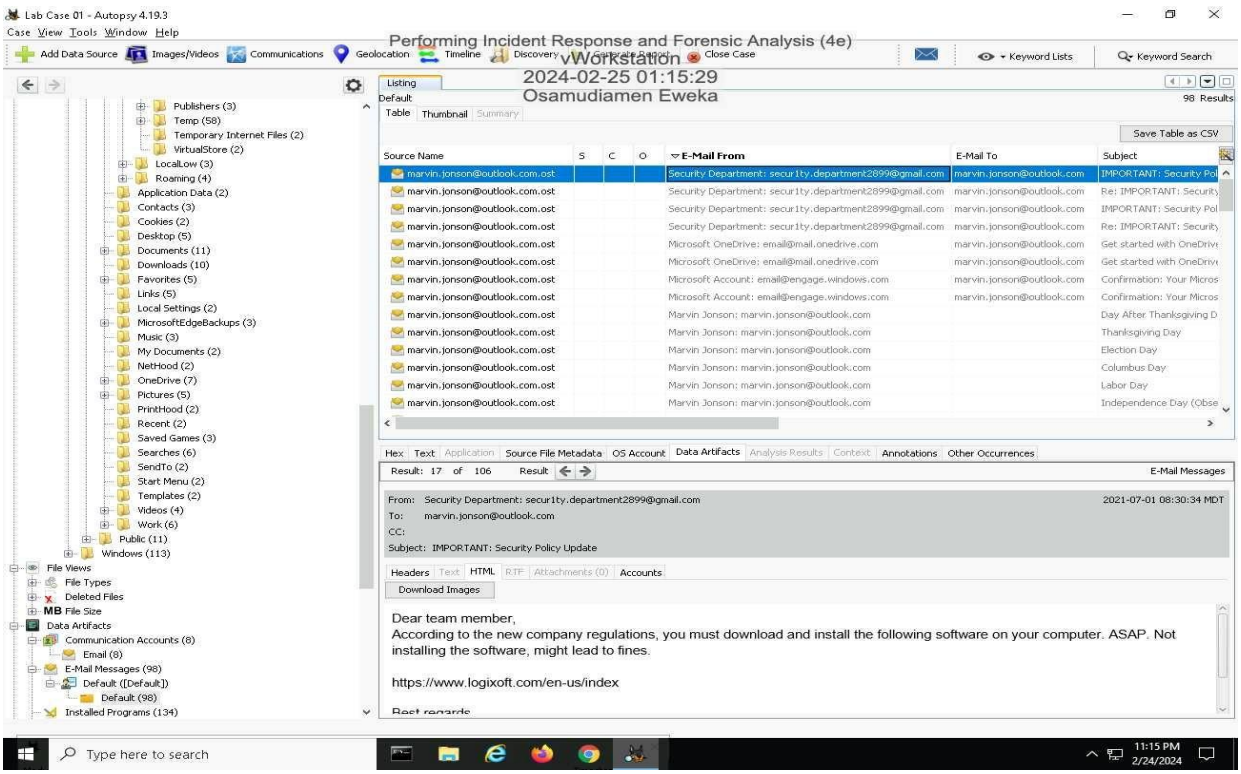
Part 2: Identify Additional Evidence of Spyware

Upon resuming the investigation, skepticism arises regarding an email within Marvin's Inbox, ostensibly from the security team, citing "new company regulations" and containing an external URL—a communication strategy uncharacteristic of the security team's protocol. To probe further into this anomaly, the Autopsy forensic tool's E-mail Parser feature is employed to sift through Marvin's email artifacts, seeking out any message bearing the phrase "new company regulations" that incorporates an external URL. This step is crucial for identifying potentially malicious attempts to install spyware under the guise of compliance with company directives. Upon identifying the email in question, it becomes apparent that this message could be part of a sophisticated attempt to compromise Marvin's workstation or to facilitate unauthorized access to Giggly Goofo’s network.

Figure 9 discovery below is crucial. By capturing a screenshot of the email, participants create tangible evidence of the phishing attempt or malicious communication. This screenshot, alongside its context and potential implications, will be instrumental in enhancing the incident response report. It not only adds another layer to the understanding of the breach’s complexity but also underscores the importance of vigilance and skepticism when dealing with unsolicited requests for software installation, especially those deviating from established security protocols.

Figure 9

Make a screen capture showing the email with instructions for installing additional spyware.



Note. Figure 9 highlights the multifaceted nature of cyber threats facing organizations and the critical role of thorough forensic analysis in uncovering and understanding these threats. By meticulously examining and documenting suspicious communications, you contribute to a broader effort to safeguard the organization's digital assets and reinforce its cybersecurity posture (Jones & Bartlett, 2024).

Question: Document the red flags in the email that indicate that it may be a phishing attempt.

Answer: The security department typically installs software automatically and would not reach out to individuals via email for such installations. In their communication, they would likely include a company phone number or the company name in their signature. The assertion

that failure to install the software could result in fines raises red flags. Additionally, the email address "secur1ty.department2899@gmail.com" is suspicious, especially given that Marvin's account is on Outlook. If the department were legitimately part of the company, they would use an Outlook account, and their username would be more professional than "secur1ty".

Conclusion

In this comprehensive lab, participants undertook a detailed incident response journey, employing forensic tools like NetWitness Investigator and Autopsy to dissect a cybersecurity incident through the analysis of a PCAP file and a disk image. This hands-on experience taught them to identify, correlate, and document evidence across multiple sources, culminating in a nuanced incident response report. Structured to mimic real-world scenarios, the lab sharpened essential digital forensic skills, from guided exercises to autonomous investigations. The resulting deliverables—meticulous lab reports and a refined incident response report—demonstrate the participants' adeptness at navigating the complexities of cybersecurity investigations, effectively preparing them to tackle similar challenges in the field with a blend of technical proficiency and critical thinking.

Reference

Grispos, G. (2015, August 11). *Security Incident Response Criteria: A Practitioner's Perspective*. arXiv.org. https://arxiv.org/abs/1508.02526

Jones & Bartlett (2024). Performing Incident Response and Forensic Analysis (Figures). *Jones and BartlettLearning Virtual Lab*. URL: https://jbl-lti.hatsize.com/startlab