Student:	Email:
Loksharan Saravanan	loksharan.soc@gmail.com

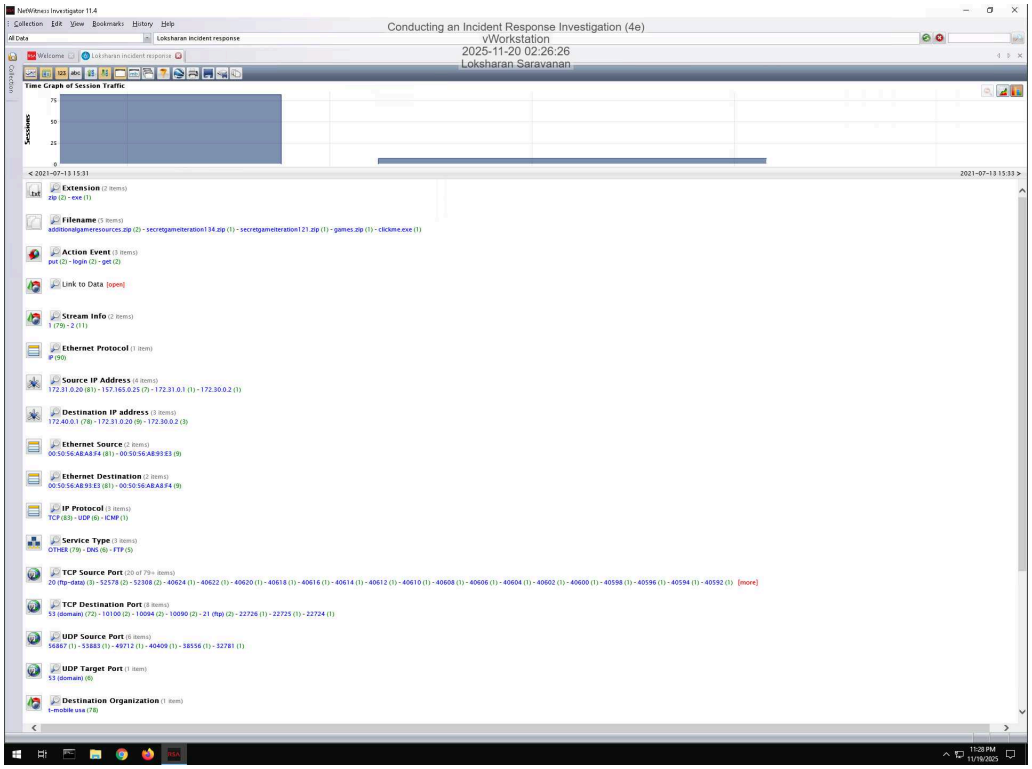
Time on Task:	Progress:
3 hours, 23 minutes	100%

Report Generated: Thursday, November 20, 2025 at 6:09 PM

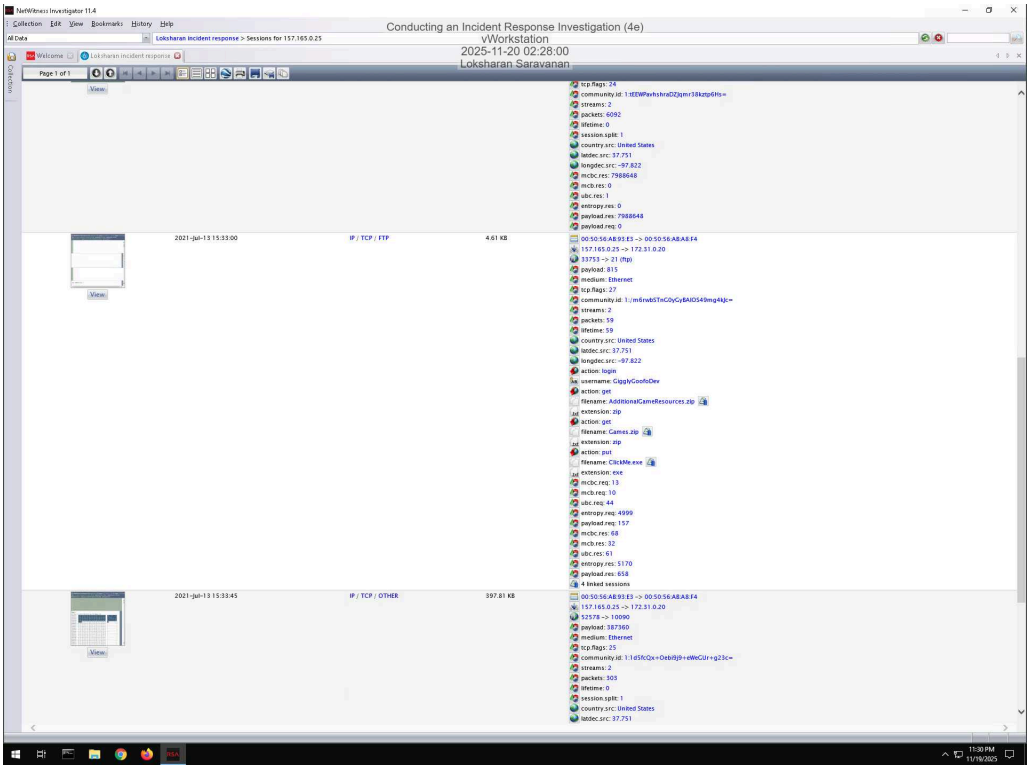
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

10. **Make a screen capture** showing the **Time Graph**.

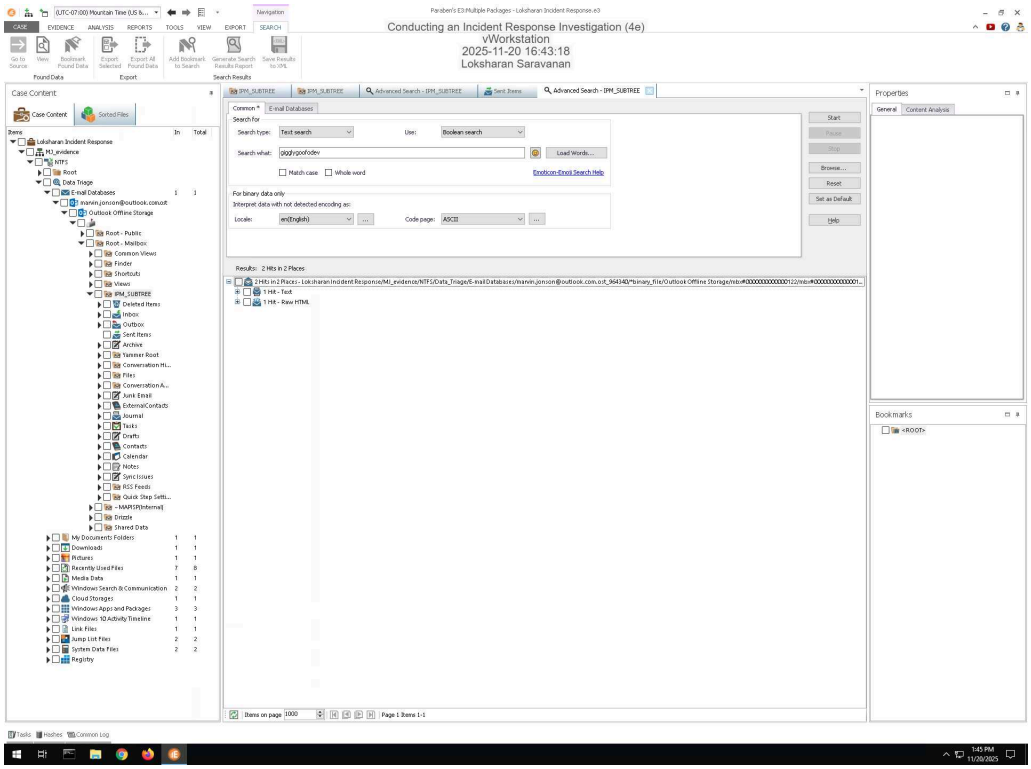


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



Part 2: Analyze a Disk Image for Forensic Evidence

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



Part 3: Prepare an Incident Response Report

Date
Insert current date here.

11/20/2025

Name
Insert your name here.

Loksharan

Incident Priority
Define this incident as High, Medium, Low, or Other.

High

Incident Type

Include all that apply: Compromised System, Compromised User Credentials, Network Attack (e.g., 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.

Other

Incident Timeline

Define the following: Date and time when the incident was discovered, Date and time when the incident was reported, and Date and time when the incident occurred, as well as any other relevant timeline details.

11/20/2025

Incident Scope

Define the following: Estimated quantity of systems affected, estimated quantity of users affected, third parties involved or affected, as well as any other relevant scoping information.

Quantity of systems

Systems Affected by the Incident

Define the following: Attack sources (e.g., IP address, port), attack destinations (e.g., IP address, port), IP addresses of the affected systems, primary functions of the affected systems (e.g., web server, domain controller).

IP Address

Users Affected by the Incident

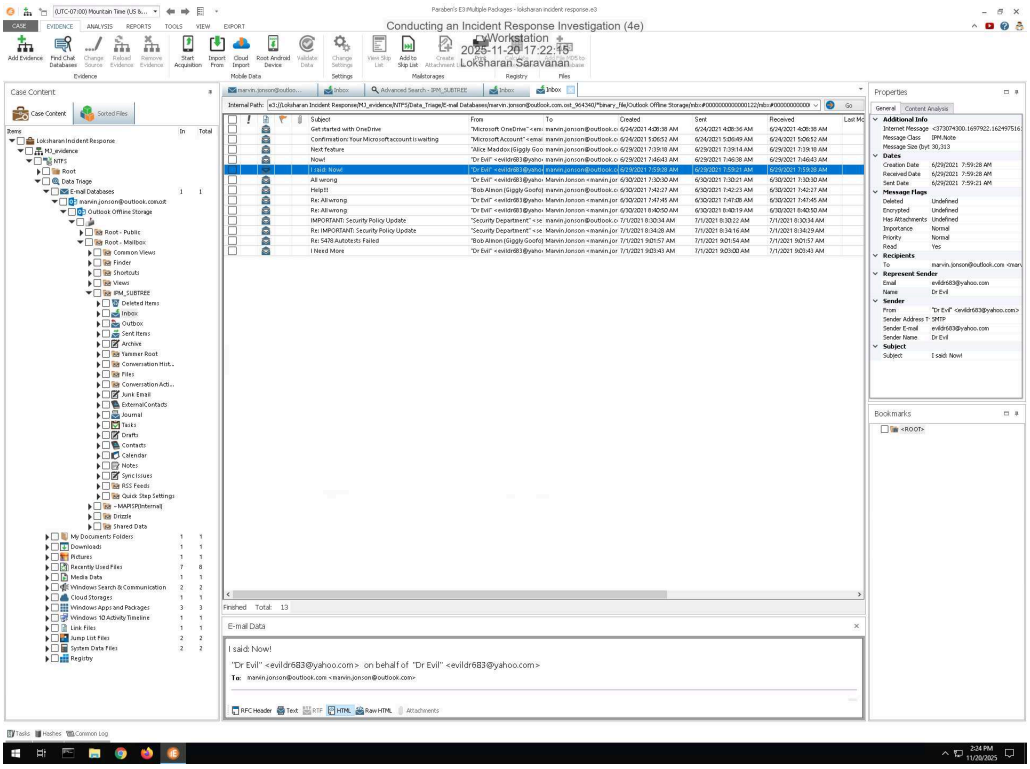
Define the following: Names and job titles of the affected users.

Marvin Jonson

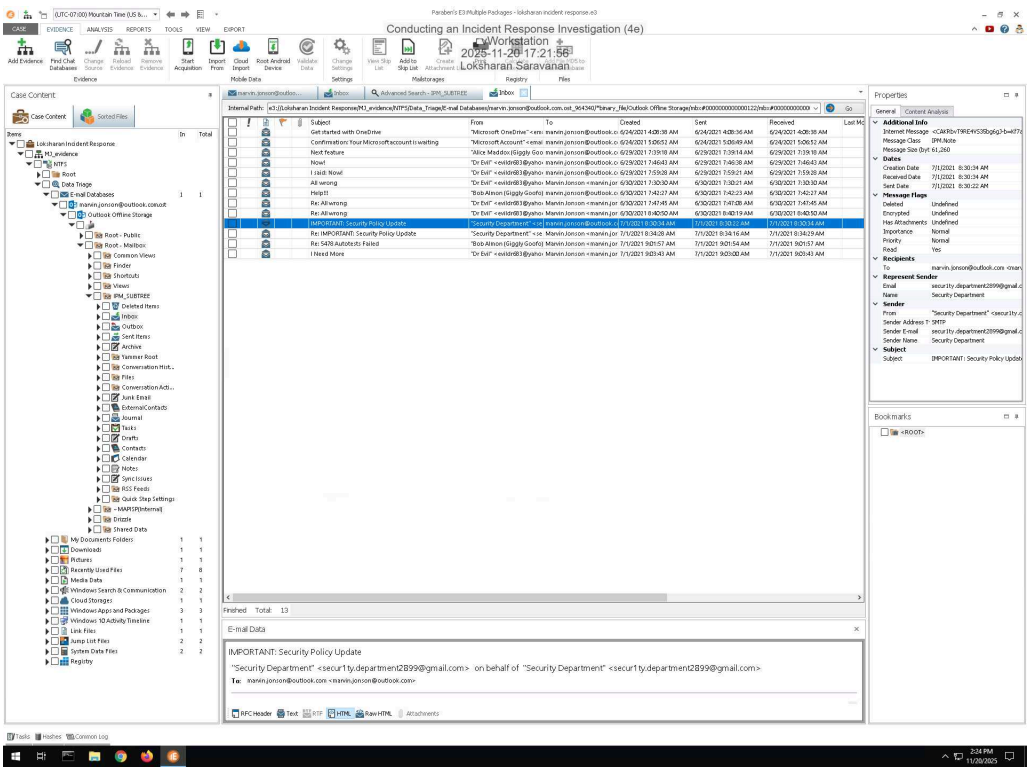
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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



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



Part 2: Identify Evidence of Spyware

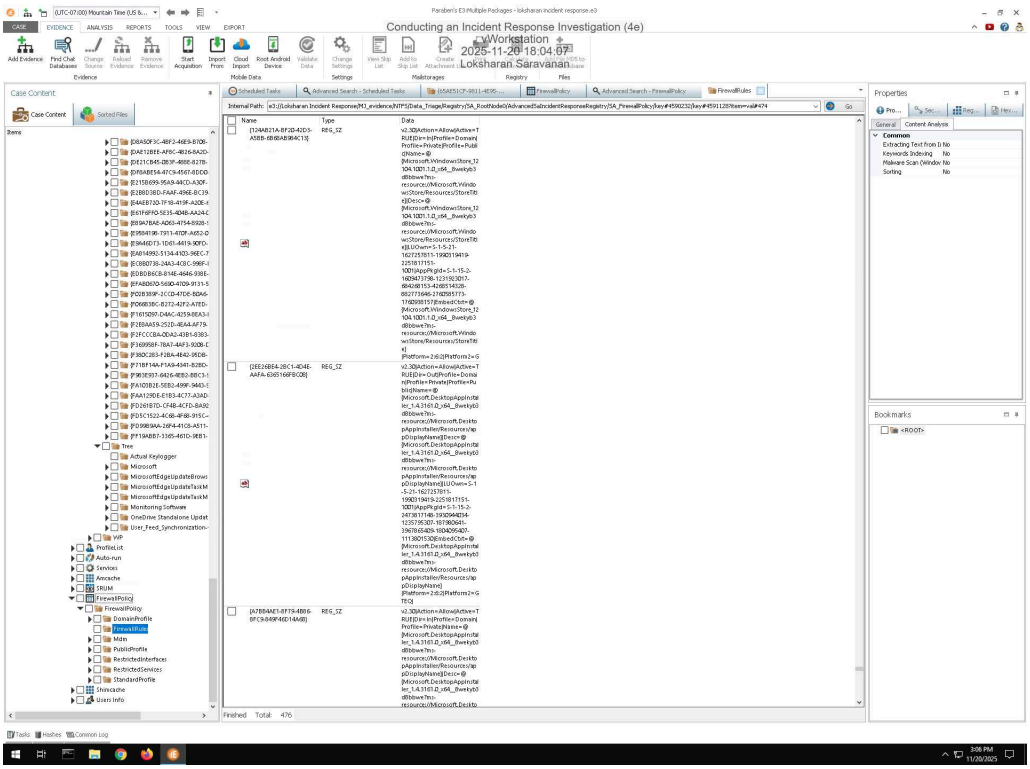
5. **Document** the Author and Date values associated with the scheduled keylogger task.

DESKTOP-CGRK7TL\Marvin Jonson

7. **Document** the port used for inbound connections to the keylogger and the name and location of the keylogger executable.

path: /actual keyloggerport 4444

9. **Make a screen capture** showing the **registry key value associated with the keylogger and the localSPM service**.



15. **Record** the first time and last time the keylogger was started.

June 14, 2023- 10:22:51 AMJune 16,2023 -4:19:33 PM

17. **Record** whether Marvin interacted with or simply opened the keylogger.

Marvin interacted with the keylogger

Part 3: Update an Incident Response Report

Date
Insert current date here.

November 20, 2025

Name
Insert your name here.

Loksharan

Incident Priority
Has the incident priority changed? If so, define the new priority. Otherwise, state that it is unchanged.

The priority increases due to confirmation that malicious software (keylogger) was intentionally installed and configured to exfiltrate data. This elevates the severity from a suspected policy violation to a confirmed malware / data compromise incident.

Incident Type
Has the incident type changed? If so, define any new incident type categories that apply. Otherwise, state that it is unchanged.

Malware Infection – A keylogger was installed and registered as a service.Unauthorized System Modification – Firewall rules and scheduled tasks were altered to support the keylogger.Potential Data Exfiltration – FirewallPolicy entries show inbound port 4444 configured for remote access.Coercion/Social Engineering – Email evidence confirms Marvin acted under pressure from Dr. Evil.

Incident Timeline
Has the incident timeline changed? If so, define any new events or revisions in the timeline. Otherwise, state that it is unchanged.

Email Evidence: Marvin received coercive emails from Dr. Evil instructing him to install a keylogger and modify system settings.Scheduled Task Creation: A scheduled task for the keylogger was created on June 14, 2023.Keylogger Activity: Windows Activity Timeline shows the keylogger was first executed at June 14, 2023 – 10:22 AM and last executed at June 16, 2023 – 4:19 PM.User Interaction: Timeline data (ActivityType = 6) confirms Marvin interacted with the keylogger application.Firewall Modification: Inbound port 4444/TCP was enabled to allow external keylogger access.

Incident Scope
Has the incident scope changed? If so, define any new scoping information. Otherwise, state that it is unchanged.

The scope now includes:Installation and persistence of a malicious keylogger.Modification of Windows Firewall and scheduled tasks to enable remote access.Creation of a Windows service to maintain persistence.Verified keylogger execution on multiple dates, suggesting active surveillance or data capture.

Systems Affected by the Incident

Has the list of systems affected changed? If so, define any new systems or new information. Otherwise, state that it is unchanged.

The affected Windows 10 Enterprise workstation now shows additional compromise indicators:Malicious executable located at:
C:\Users\Marvin\AppData\Roaming\localSPM\spm.exeRegistry modifications under:
HKLM\SYSTEM\CurrentControlSet\Services\localSPMFirewallPolicy entries allowing incoming connections on port 4444Scheduled Tasks referencing the keylogger

Users Affected by the Incident

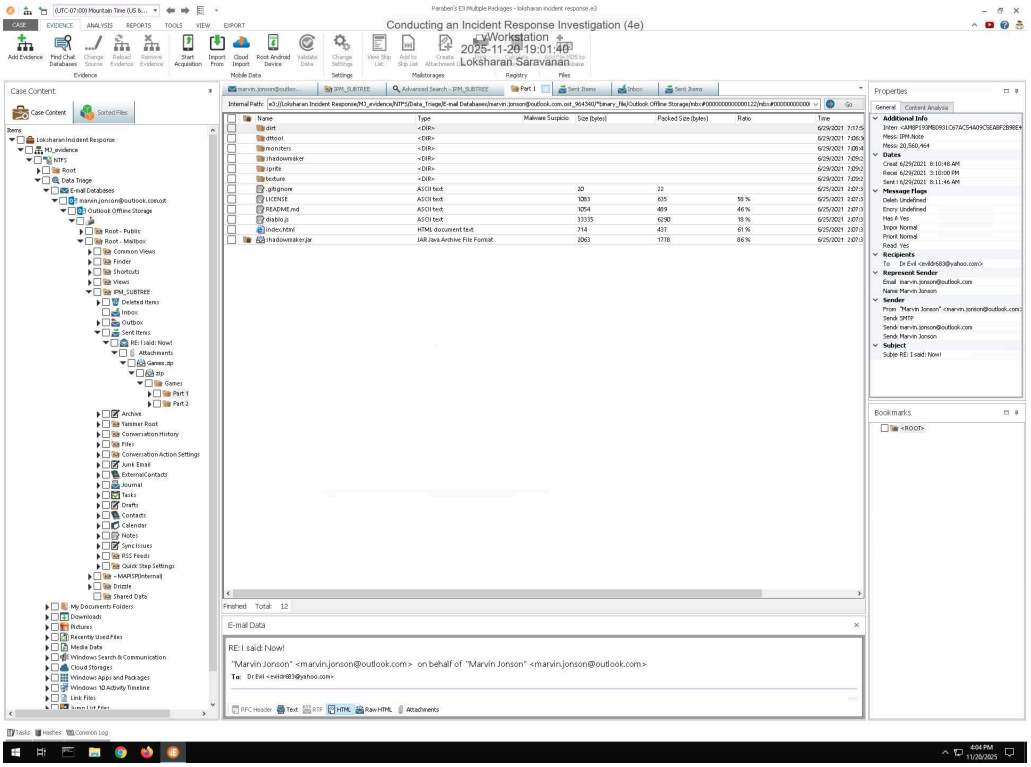
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Marvin:
Evidence now shows he not only received coercive emails but followed through with installing and interacting with the keylogger.Potential additional users:
Since a keylogger captures all system input, any user who logged into the compromised workstation during the keylogger's active period may have had their credentials recorded.

Section 3: Challenge and Analysis

Part 1: Identify Additional Evidence of Data Exfiltration

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



Part 2: Identify Additional Evidence of Spyware

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