Student:	Email:
Fernando Parra	fparra1@msudenve.edu

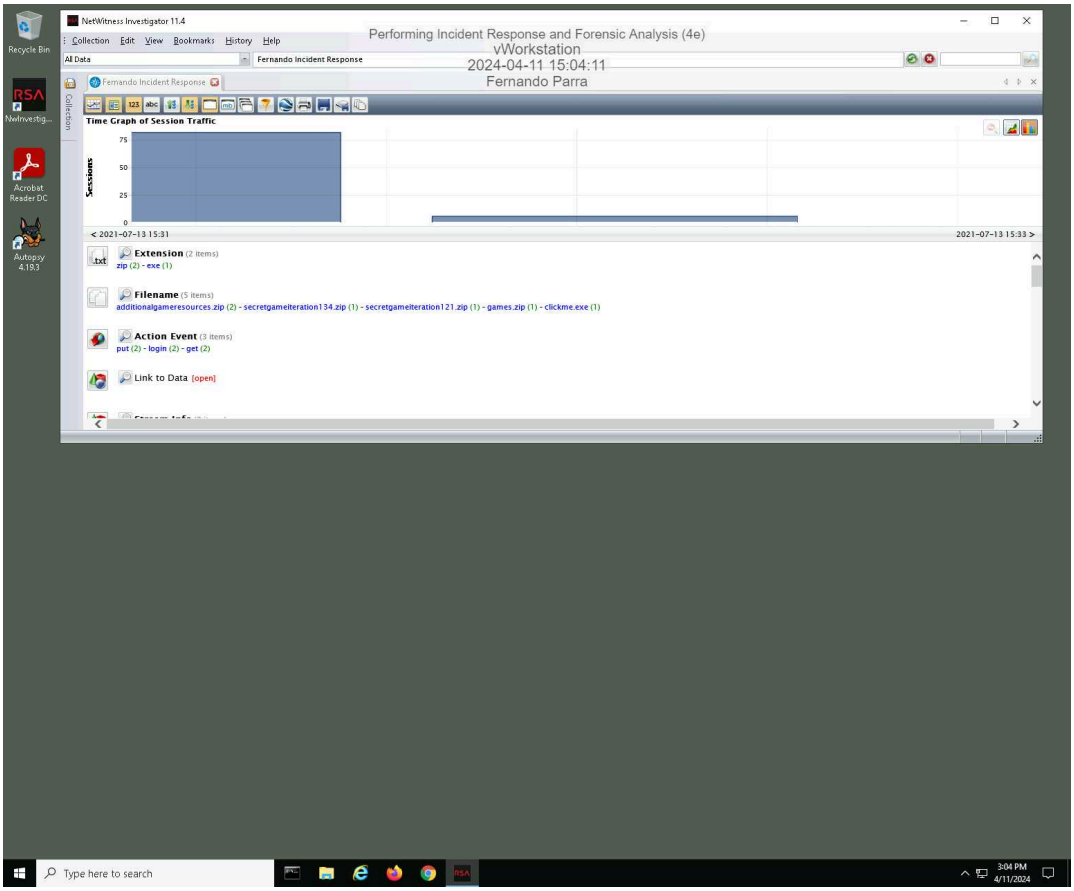
Time on Task:	Progress:
6 hours, 42 minutes	100%

Report Generated: Thursday, April 11, 2024 at 8:32 PM

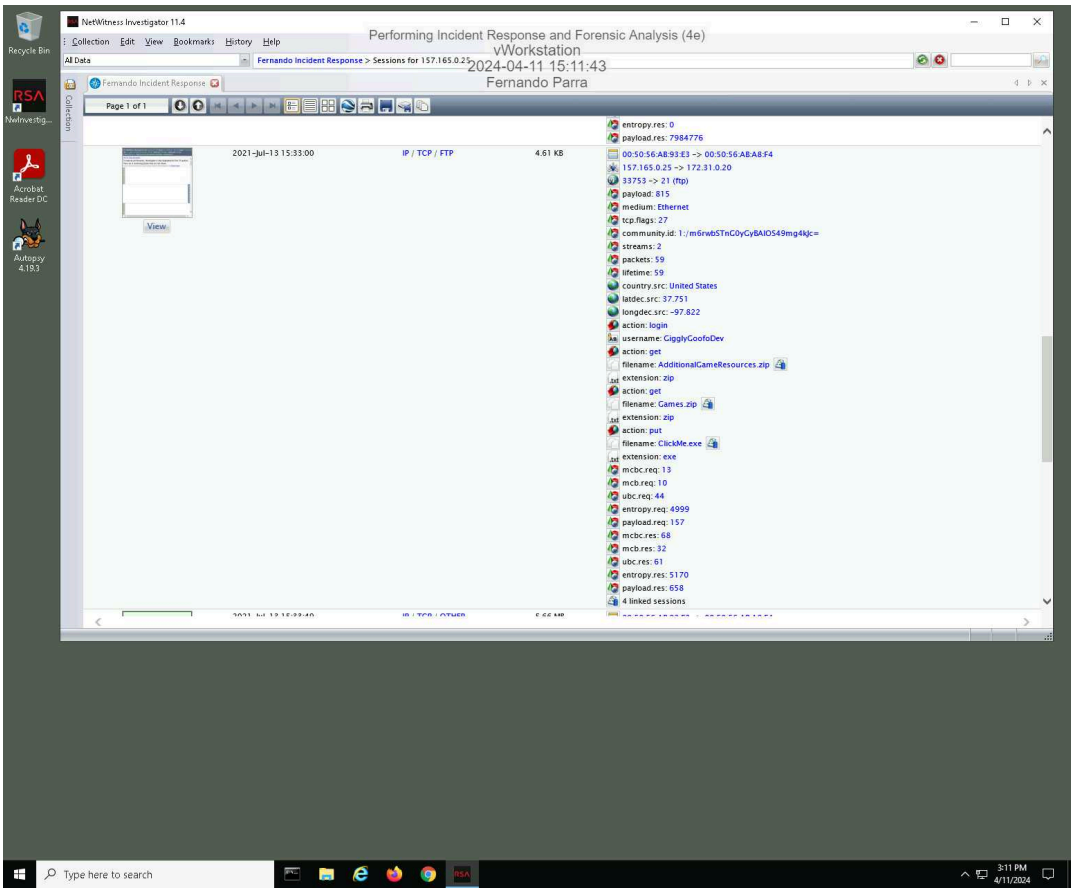
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

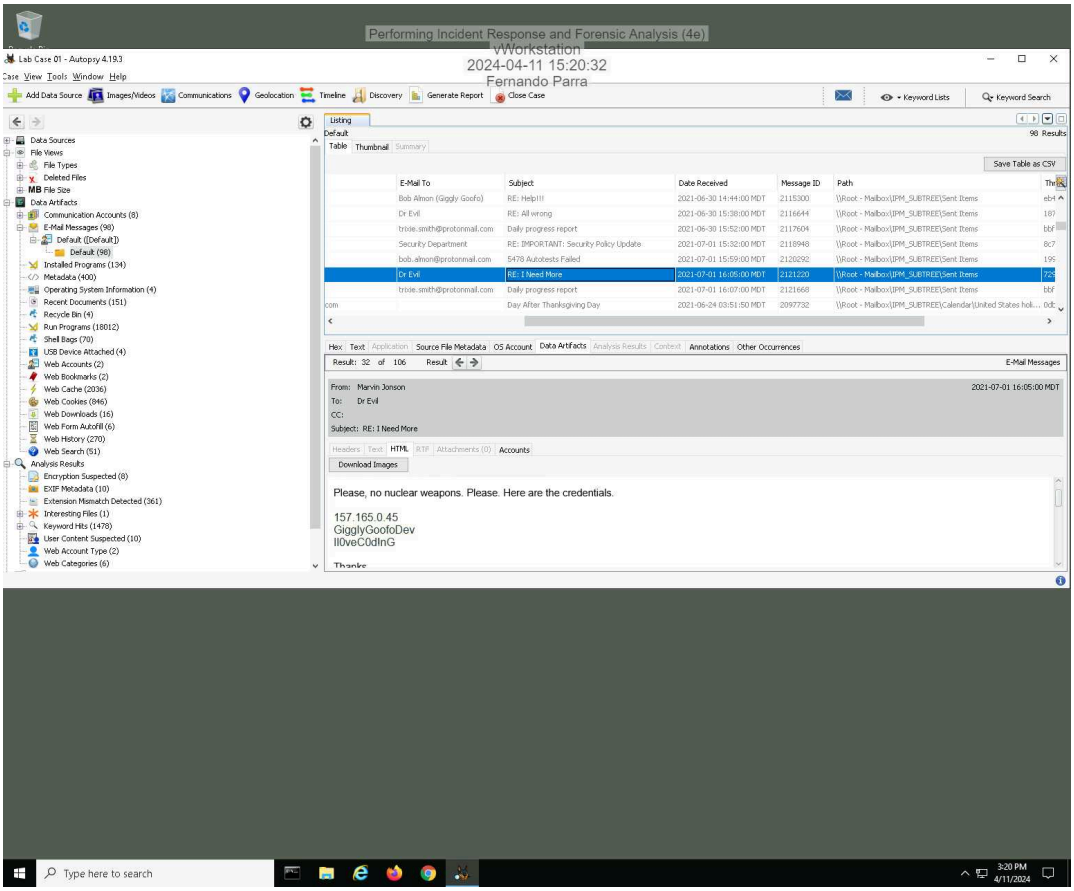


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



Part 2: Analyze a Disk Image for Forensic Evidence

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



Part 3: Prepare an Incident Response Report

Date
Insert current date here.

April 11th, 2024

Name
Insert your name here.

Fernando Parra

Incident Priority

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

Medium.
Additional Notes: The organization is facing a medium incident priority situation as the analysis demonstrates unauthorized use of a system, personal theft related to a cybersecurity incident, the tool and target of the action, and misuse of organizational services that lead to the data exfiltration. This also results in employee termination (Marvin Jonson) and means that the incident(s) are serious and should be handle that same day.

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.

Compromised System
Malware (clickme.exe)
Policy Violation
Other: Malicious Insider

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.

A. The incident was discovered on July 31st, 2021 at 10:30 AM Eastern time.
B: The incident was reported 10 minutes later, on July 31st, 2021 at 10:40 AM Eastern time.
C: The FTP exfiltration occurred on July 13th, 2021 at 3:33 PM.

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.

A. Attack sources: 157.165.0.25
B. Attack destinations: 172.31.0.20
C. IP addresses of the affected systems: 172.31.0.20

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).

A. Attack sources: 157.165.0.25

B. Attack destinations: 172.31.0.20

C. IP addresses of the affected systems: 172.31.0.20

D. Primary functions of the affected system: Company's FTP server.

E. Operating systems of the affected systems: Operating system, version, pack, patch level, or configurations are not specified for the FTP server only for Marvin Jonson's workstation, which used Windows 10 Enterprise and could be compromised by the potentially malicious file clickme.exe.

F. Security software loaded on the affected systems not specified.

G. Physical location of the affected systems: Game Development Studio Giggly Goofo.

Users Affected by the Incident

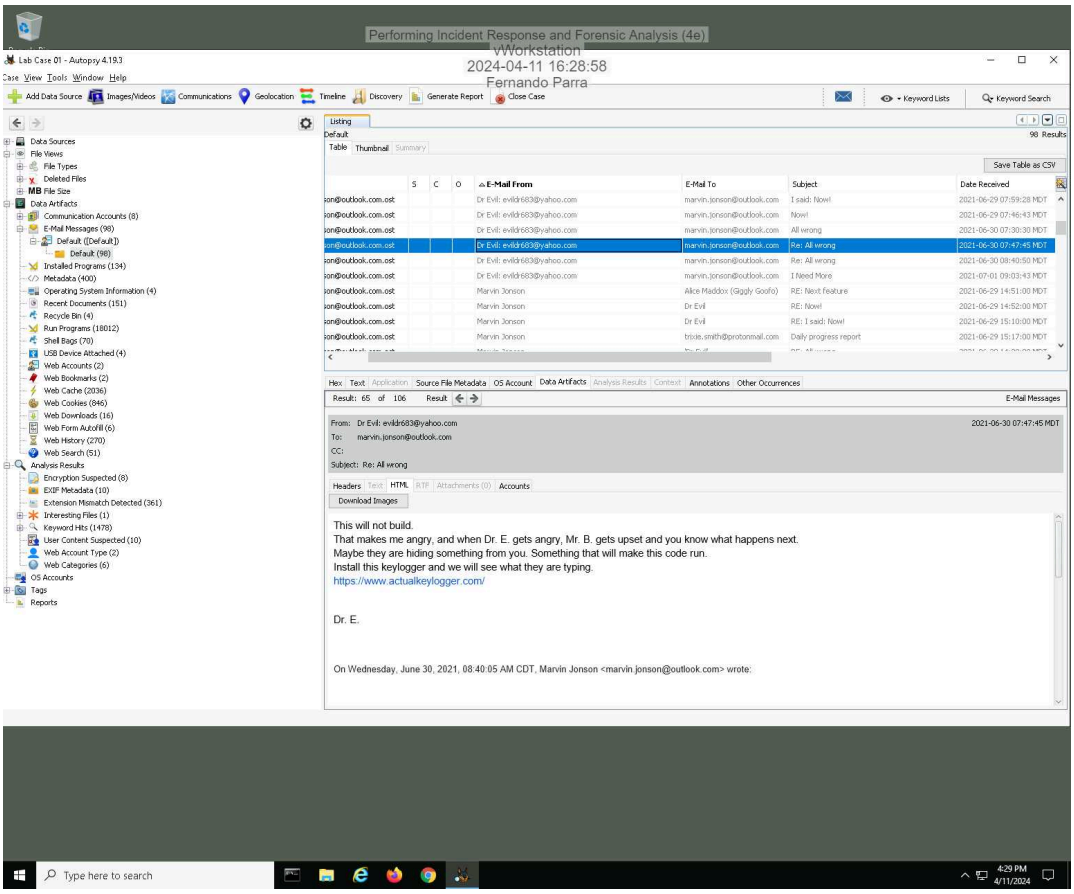
Define the following: Names and job titles of the affected users.

Potential users that could be affected by the data breach could include former developers, contractors, and players (customers). A data exfiltration might not only include intellectual property like proprietary code but also confidential information from customers such as credit card numbers, usernames, passwords, email addresses, and purchase histories.

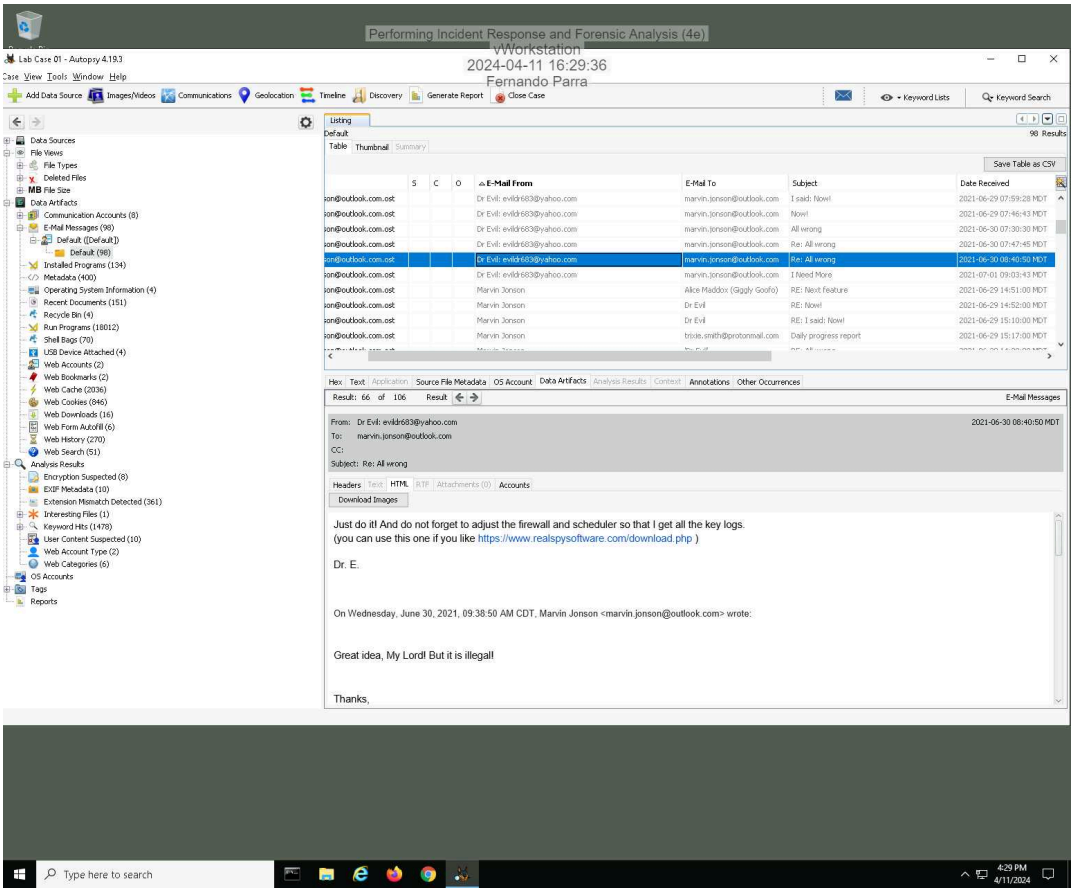
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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

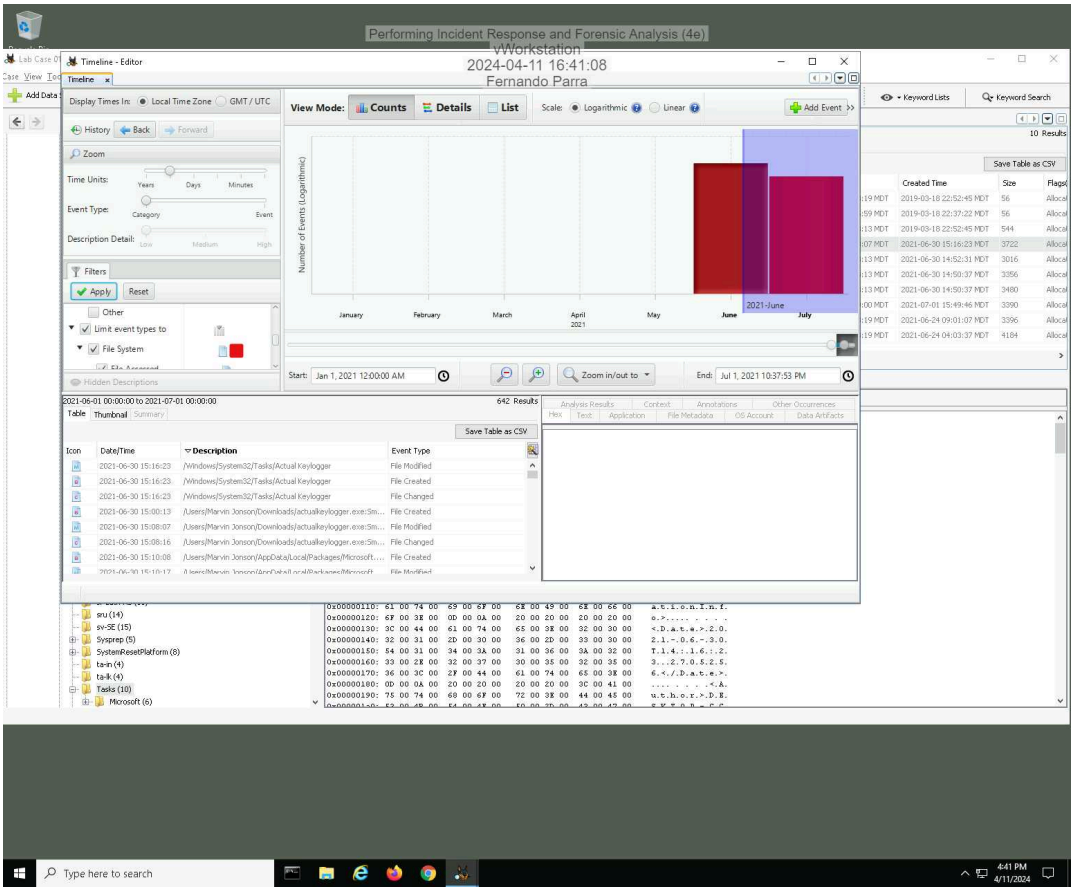


6. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.

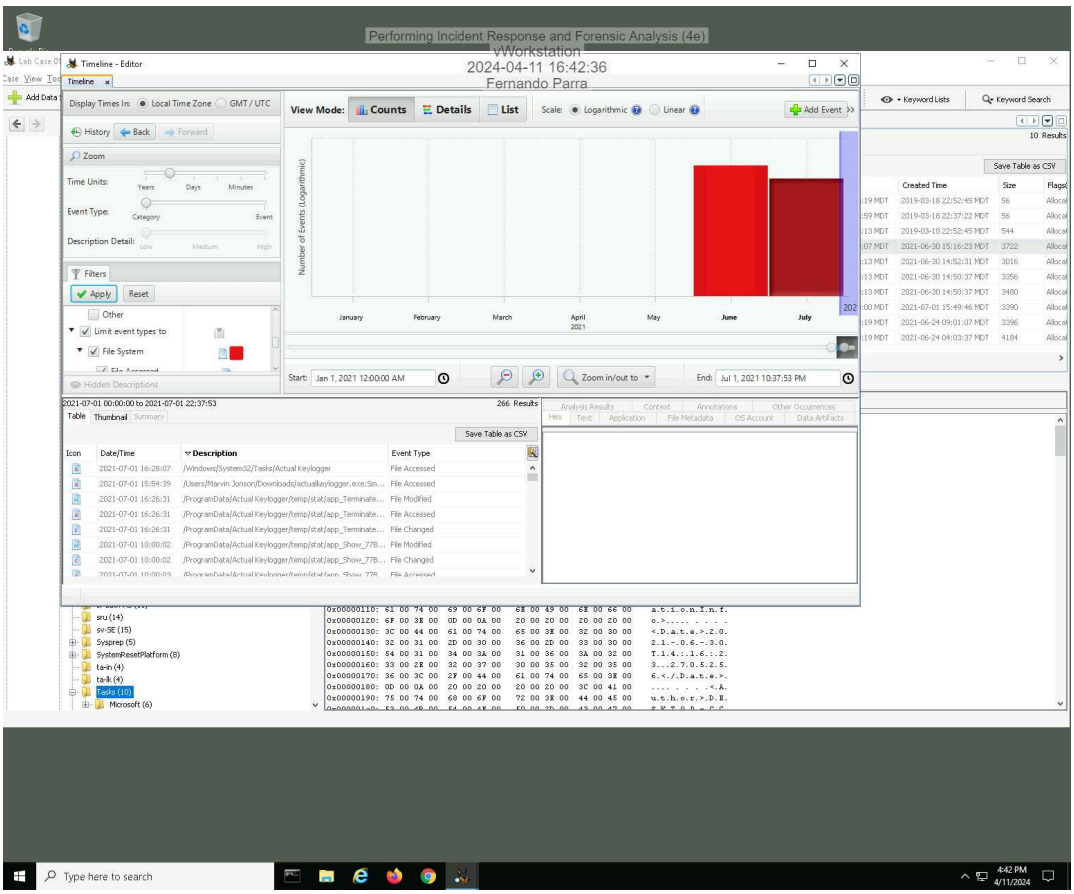


Part 2: Identify Evidence of Spyware

12. **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**.



15. **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**.



20. **Record** the date and time that the keylogger's executable file was created.

June 30th, 2021 at 3:00:13 PM

22. **Record** the date and time when the keylogger's executable file was last started.

July 1st, 2021 at 03:54:39 PM

23. **Record** whether you think you have evidence to claim that Marvin opened the keylogger.

Based on the timeline evidence, Marvin Jonson received the email from Dr Evil about installing the keylogger on June 30th in the morning, the same day in the afternoon the file was created, and then accessed on July 1st, the very next day. This evidence demonstrates that Marvin opened the keylogger.

Part 3: Update an Incident Response Report

Date
Insert current date here.

The information remains unchanged for this part of the template.

Name
Insert your name here.

The information remains unchanged for this part of the template.

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

The information remains unchanged for this part of the template.

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

Compromised System
Malware (clickme.exe, keylogger called actualkeylogger.exe)
Policy Violation
Other: Malicious Insider

Incident Timeline

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

A. The incident was discovered on July 31st, 2021 at 10:30 AM Eastern time.
B: The incident was reported 10 minutes later, on July 31st, 2021 at 10:40 AM Eastern time.
C: The FTP exfiltration occurred on July 13th, 2021 at 3:33 PM and the keylogger was installed on June 30th, 2021 at 3:16:23 PM MDT, then accessed on July 1st, 2021 at 3:54:39 PM MDT.

Incident Scope

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

A. Attack sources: 157.165.0.25
B. Attack destinations: 172.31.0.20, 172.30.0.2
C. IP addresses of the affected systems: 172.31.0.20, 172.30.0.2

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.

A. Attack sources: 157.165.0.25
B. Attack destinations: 172.31.0.20, 172.30.0.2
C. IP addresses of the affected systems: 172.31.0.20, 172.30.0.2
D. Primary functions of the affected system: Company's FTP server and the Marvin Jonson's workstation.
E. Operating systems of the affected systems: Windows 10 Enterprise on Marvin Jonson's workstation, FTP service running on a company service. (Assuming default configuration)
F. Security software loaded on the affected systems not specified. (Unchanged)
G. Physical location of the affected systems: Game Development Studio Giggly Goofo. (Unchanged)

Users Affected by the Incident

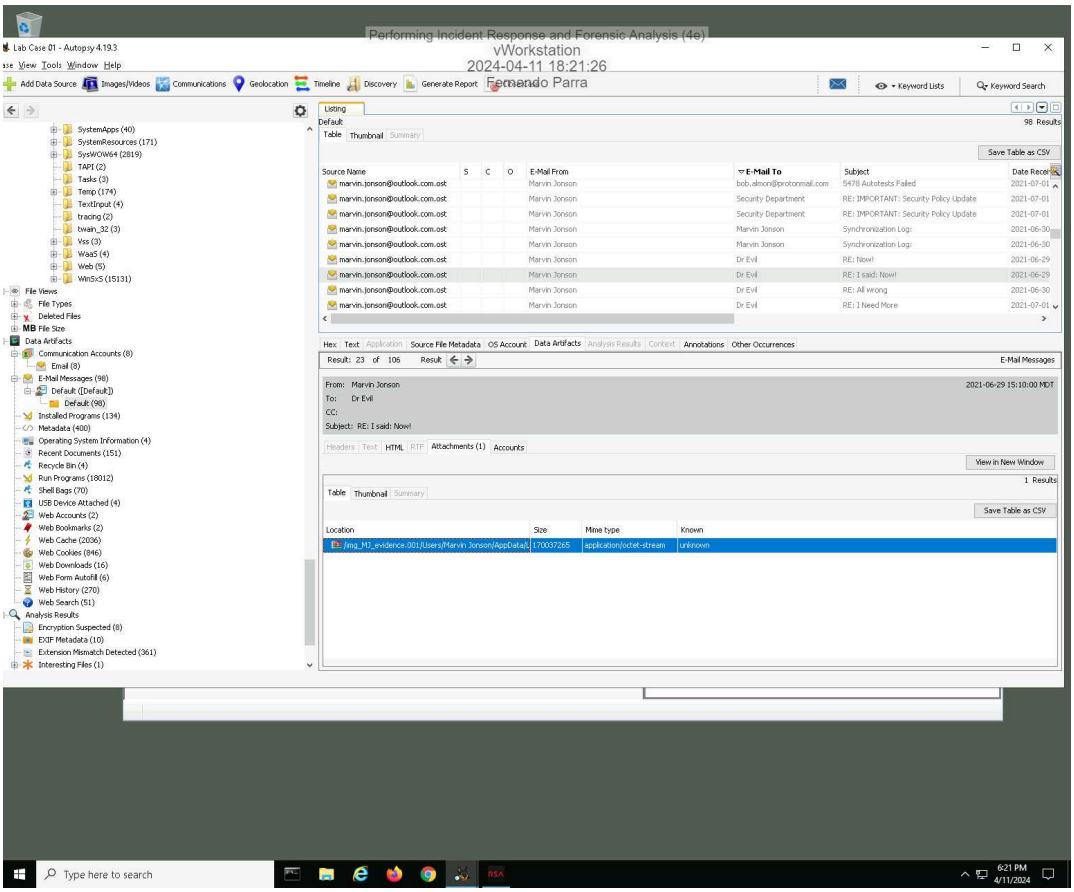
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

The information remains unchanged for this part of the template.

Section 3: Challenge and Analysis

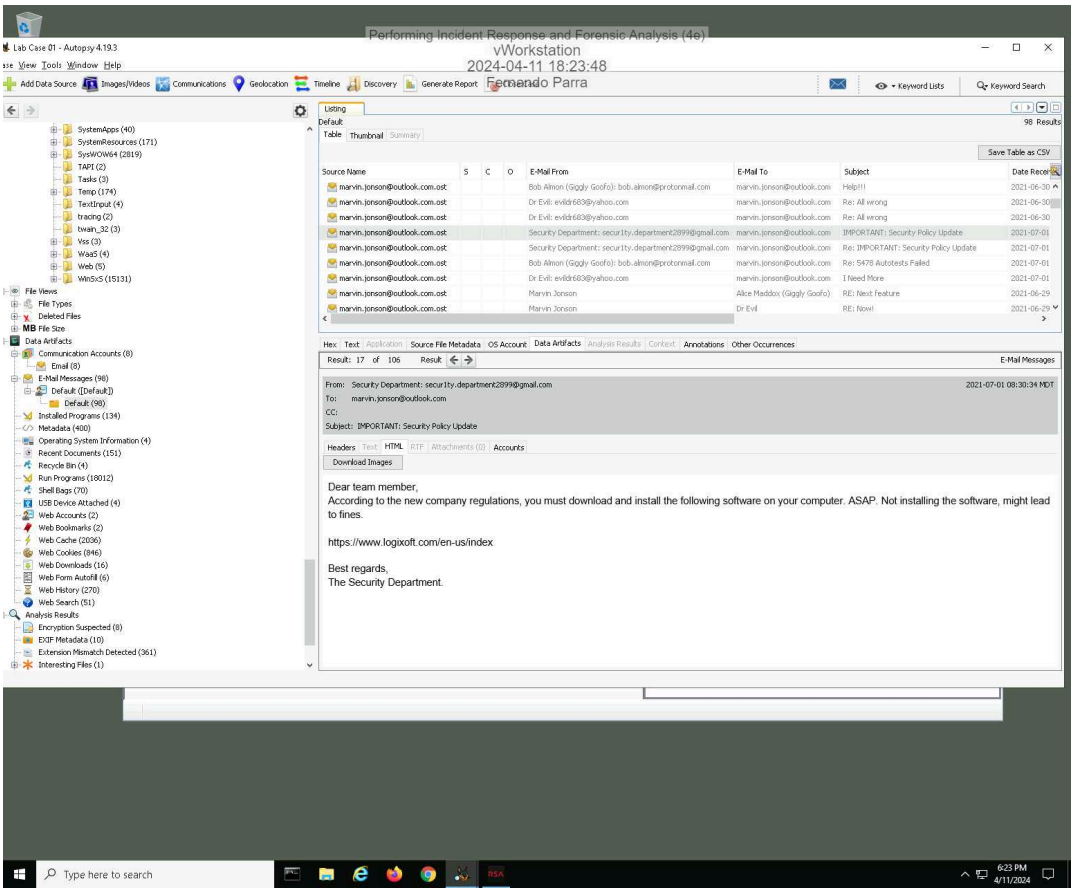
Part 1: Identify Additional Evidence of Data Exfiltration

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**.



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

This phishing attempt show a few principles that are used when performing social engineering, it shows both **consensus** and **urgency**; a group-wide decision and the "urgency" to download the software immediately. The email intends to gain **trust** by stating that the email is sent by a team member in the security department. Finally, the email uses **intimidation** by stating that not installing the software can lead to serious consequences.