Student:	Email:
Brandon Trinkle	btrinkle52@gmail.com

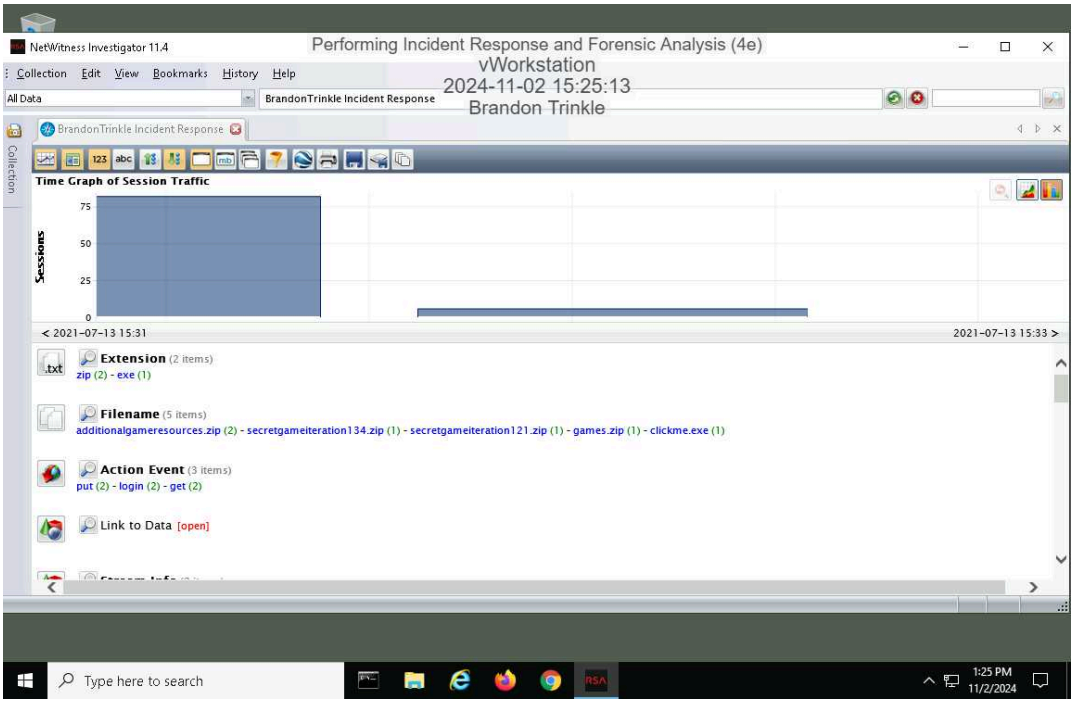
Time on Task:	Progress:
1 hour, 39 minutes	100%

Report Generated: Saturday, November 2, 2024 at 5:03 PM

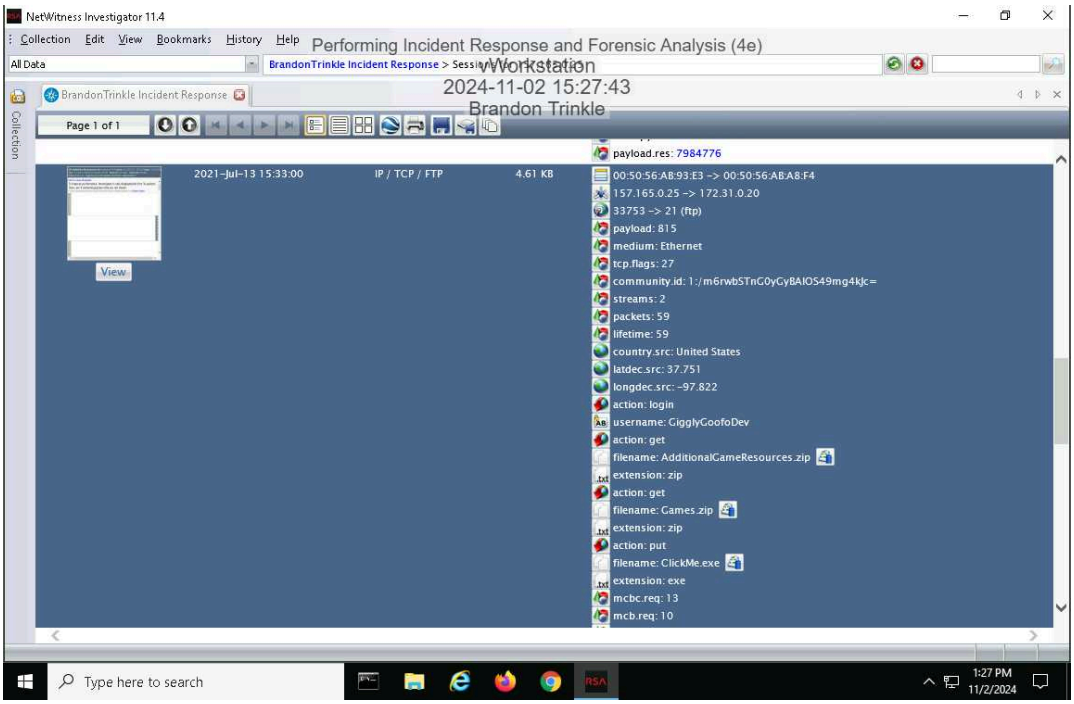
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

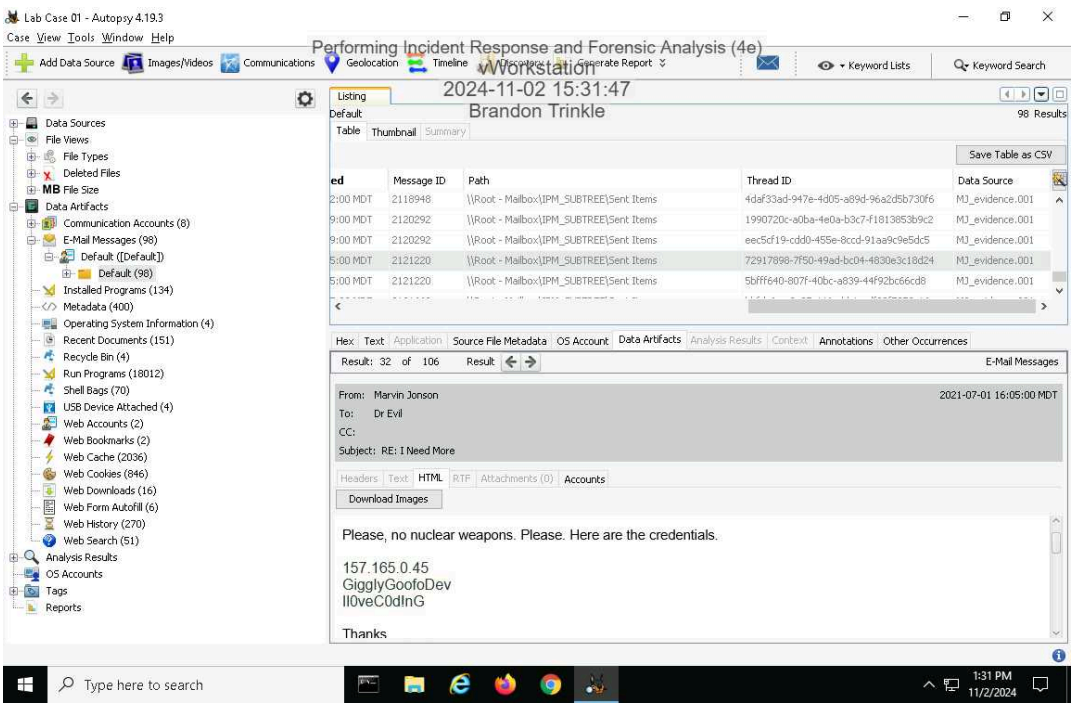


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

2024-11-02

Name
Insert your name here.

Brandon Trinkle

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

High – Compromised FTP credentials pose a direct risk of unauthorized access to sensitive data and systems.

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 User Credentials- Social Engineering- Network Attack (Unauthorized Access) – The provision of FTP credentials increases the likelihood of data exfiltration or unauthorized modification.

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.

Date and time of discovery: July 1, 2021, 16:05:00 MDT (when Marvin Jonson’s response email containing FTP credentials was sent).
Date and time reported: July 1, 2021, 08:03 AM (initial request from Dr. Evil for FTP access).
Date and time of incident occurrence: July 1, 2021, including the credential exchange at 16:05:00 MDT.

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.

Estimated quantity of systems affected: The FTP server is at risk, with potential implications for other connected systems.
Estimated quantity of users affected: At least one (Marvin Jonson), with broader exposure if FTP access is misused.
Third parties involved or affected: Dr. Evil, a suspected threat actor now in possession of FTP credentials.

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).

Attack sources: Possible IP address for Dr. Evil (157.165.0.45) may aid in tracking access attempts.
Attack destinations: The FTP server and any sensitive project resources stored there.
Primary functions of the affected systems: File storage and transfer, particularly for project-related resources and possibly sensitive pre-release game files.

Users Affected by the Incident

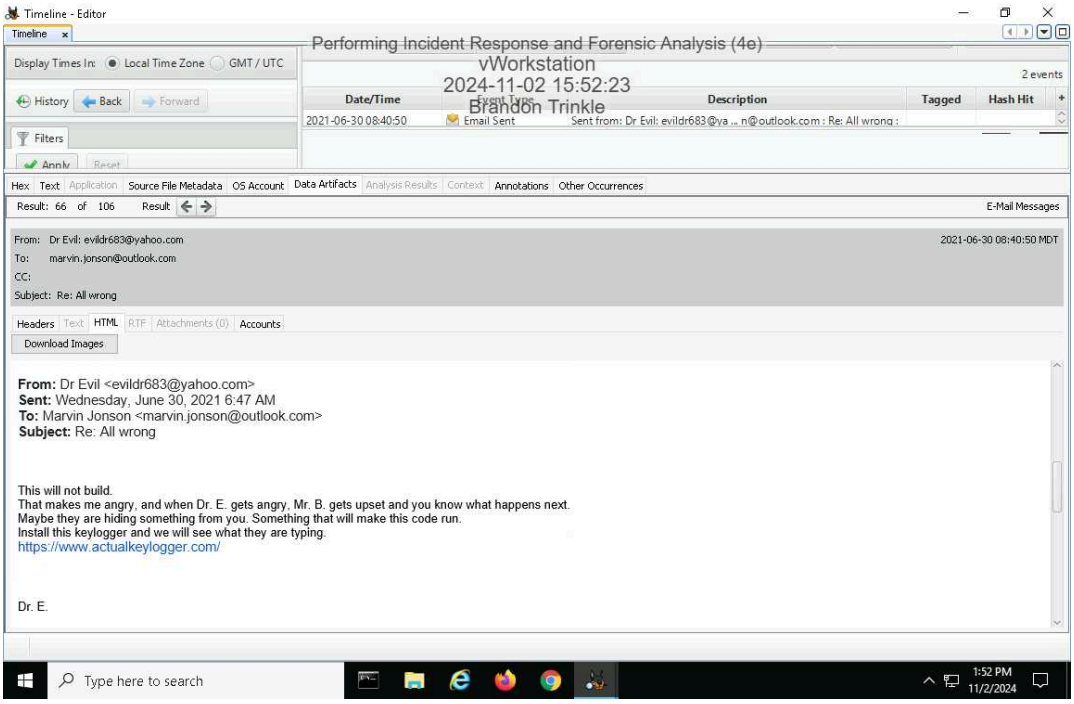
Define the following: Names and job titles of the affected users.

Marvin Jonson, Project Manager

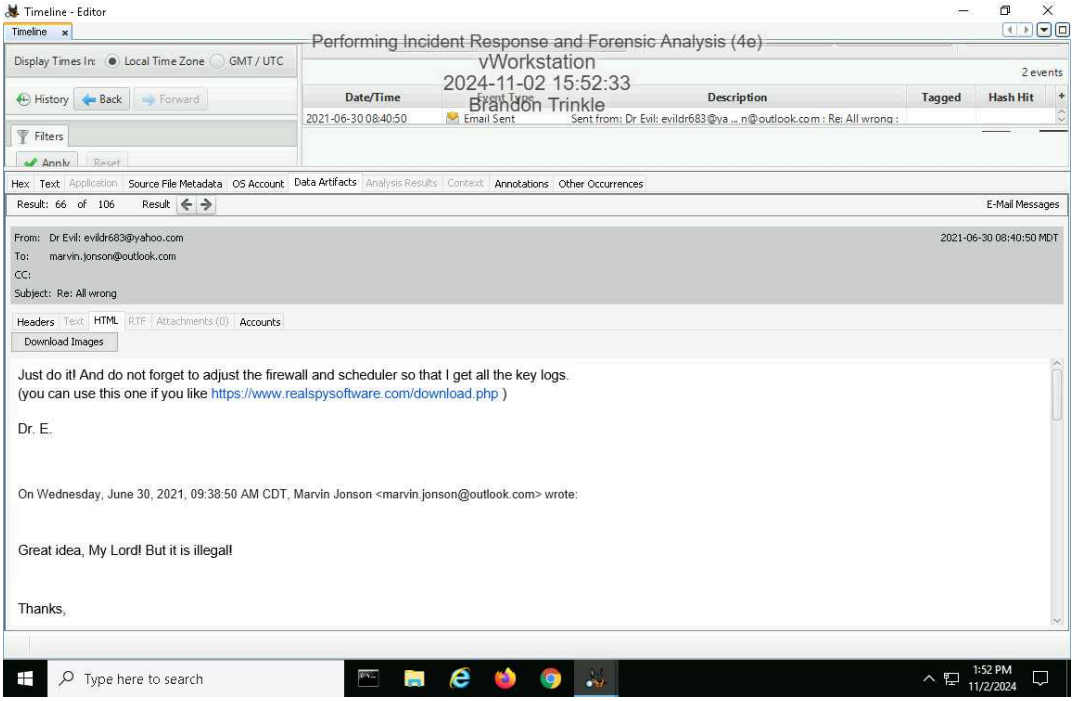
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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

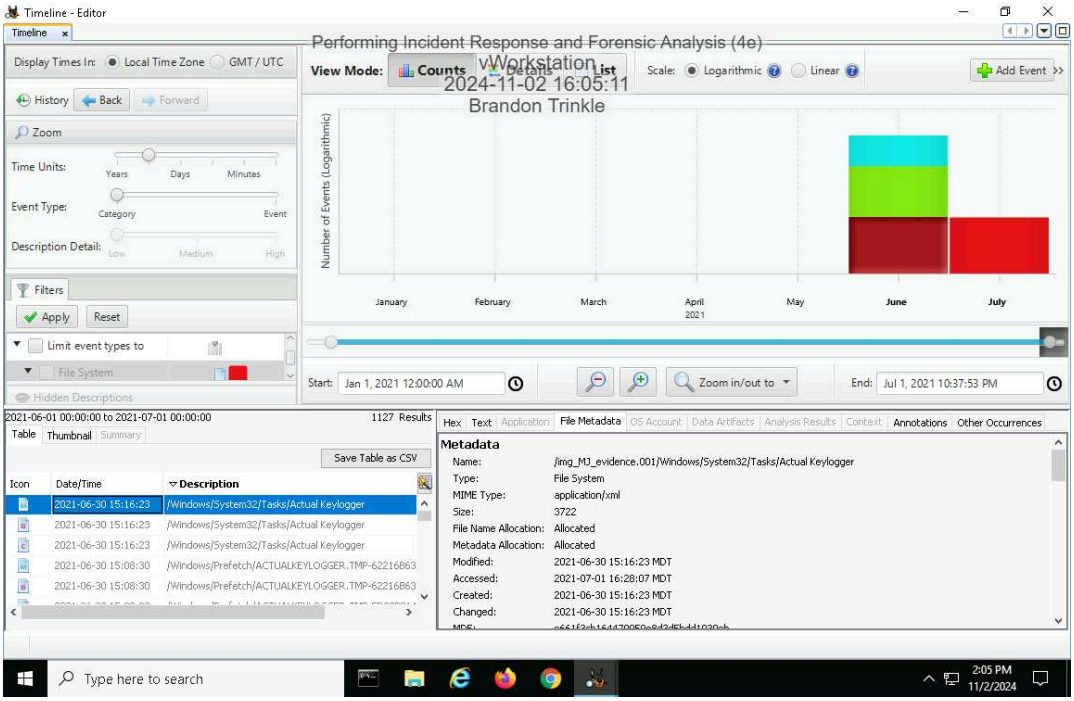


6. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.

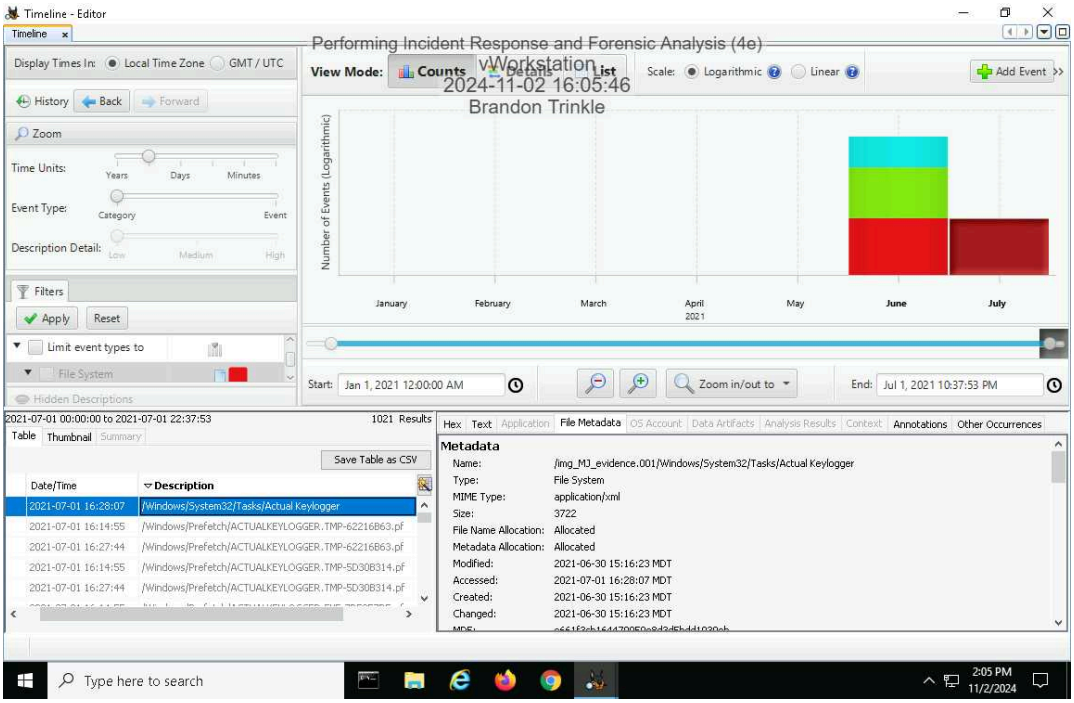


Part 2: Identify Evidence of Spyware

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.

15:00:13

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

15:54:39

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

You need more information to determine if Marvin opened the file. File accessed could mean you viewed the properties, or it was scanned with anti-virus software. So this does not definitively prove that Marvin opened the file.

Part 3: Update an Incident Response Report

Date
Insert current date here.

2024-11-02

Name
Insert your name here.

Brandon Trinkle

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

High – The keylogger installation significantly escalates the incident's severity, as it suggests potential for broader data theft and surveillance.

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

Compromised User CredentialsSocial EngineeringNetwork Attack (Unauthorized Access)Malware (Keylogger Installation)

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

June 30, 2021, 15:00:13 MDT – actualkeylogger.exe file created June 30, 2021, 15:08:07 MDT – actualkeylogger.exe file modified June 30, 2021, 15:08:16 MDT – actualkeylogger.exe file changed July 1, 2021, 15:54:39 MDT – actualkeylogger.exe file accessed

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

The keylogger affects Marvin’s workstation, with potential risk to any systems or applications he accesses, as his keystrokes and other sensitive information may be monitored and recorded.

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.

Marvin’s workstation is compromised due to the presence of the keylogger. Any system he accessed after the keylogger's installation could also be at risk if login credentials were captured.

Users Affected by the Incident

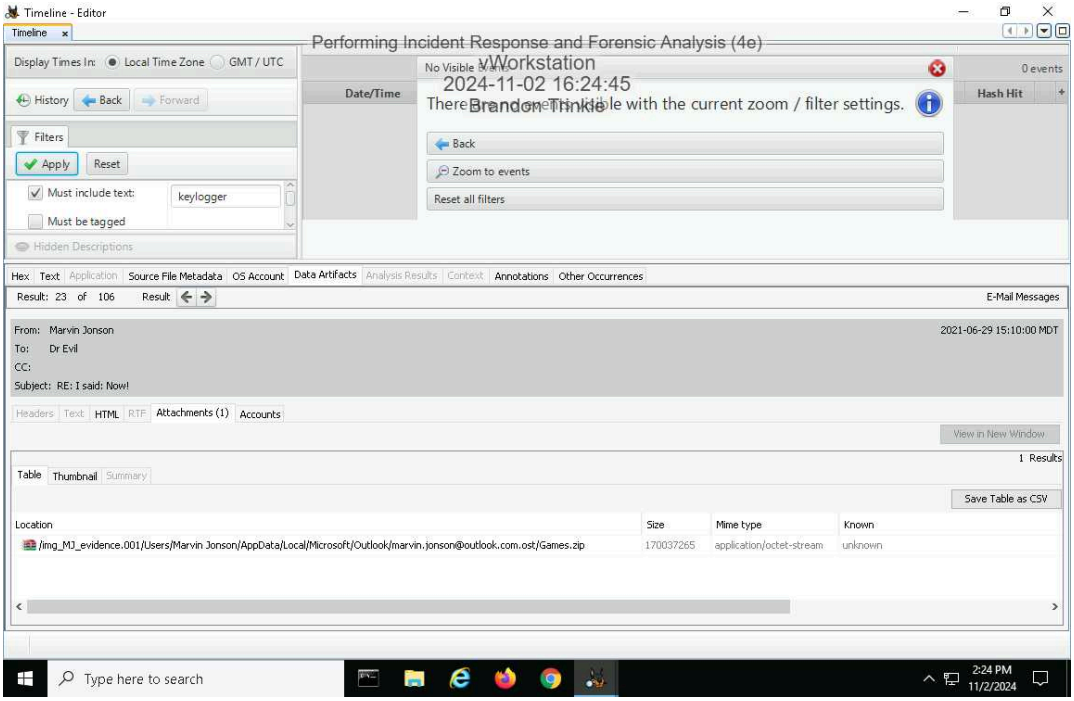
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Marvin Jonson, as the installation of a keylogger could expose his activities, passwords, and sensitive information.

Section 3: Challenge and Analysis

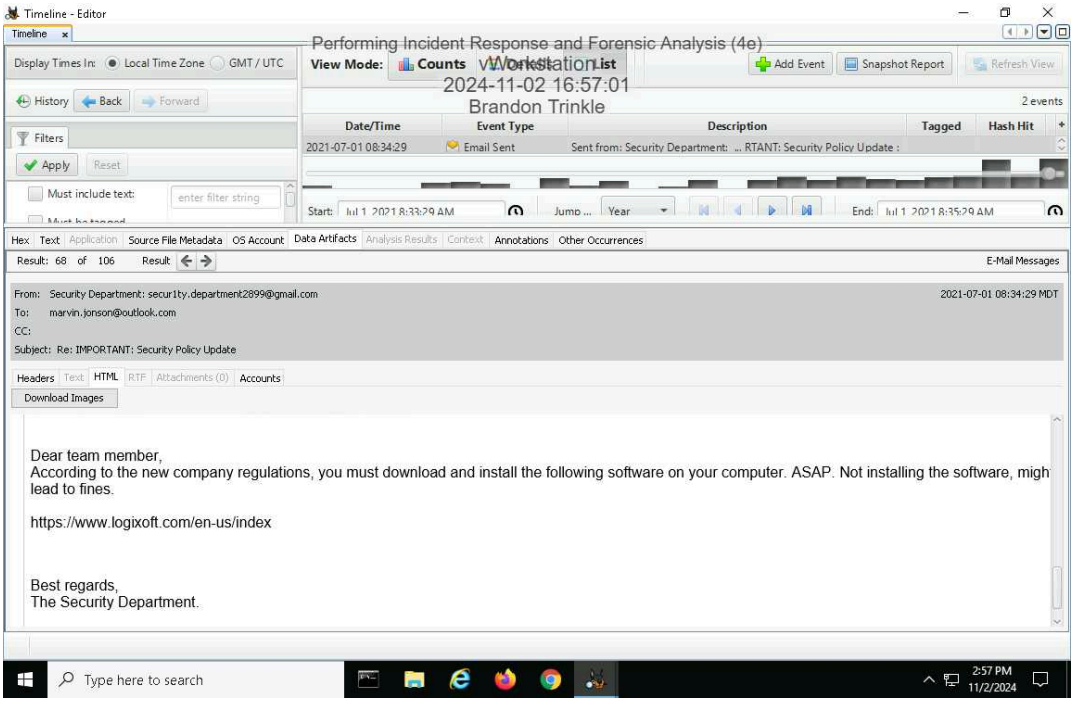
Part 1: Identify Additional Evidence of Data Exfiltration

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 email has a few signs that make it look like a phishing attempt. First, the sender’s email address, "security.department2899@gmail.com," is odd – you'd expect official security messages to come from a company email, not Gmail. The email also pushes for urgency, saying Marvin "must download and install" something ASAP. Phishing messages often try to create a sense of urgency to get people to act quickly without thinking it through.
Then, there's the mention of fines if Marvin doesn't follow the instructions, which seems like a scare tactic. The link in the email, "https://www.logixoft.com/en-us/index," could be made to look like a legit site, but it’s worth double-checking where it actually goes.
The follow-up email also has a casual tone that feels off for a security department, with phrases like "Plz" and "Wink." Security teams don’t usually talk that way in official emails. Plus, asking Marvin to adjust his firewall and scheduler settings and to keep it quiet is a big red flag. Real IT instructions wouldn't come with secrecy; they’d be straightforward and part of a standard procedure. Altogether, these details point to the email likely being a phishing attempt designed to trick Marvin into downloading something shady and making risky changes to his system.