Student:	Email:
Mustafa Shah	ho3168@wayne.edu

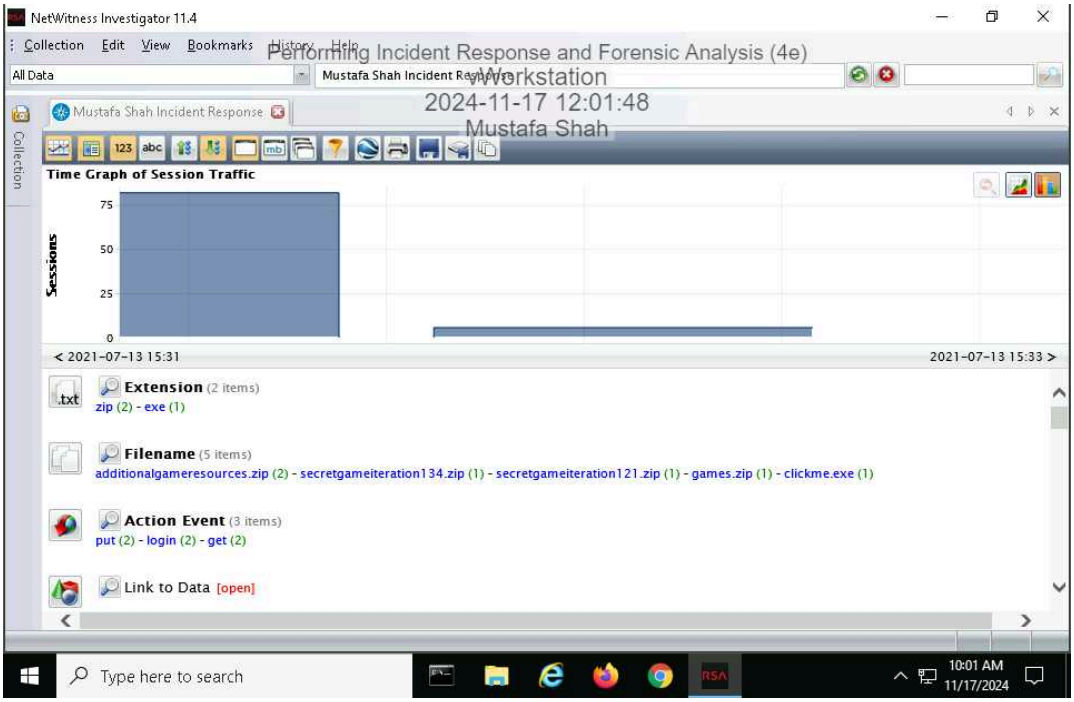
Time on Task:	Progress:
1 hour, 8 minutes	100%

Report Generated: Sunday, November 17, 2024 at 1:03 PM

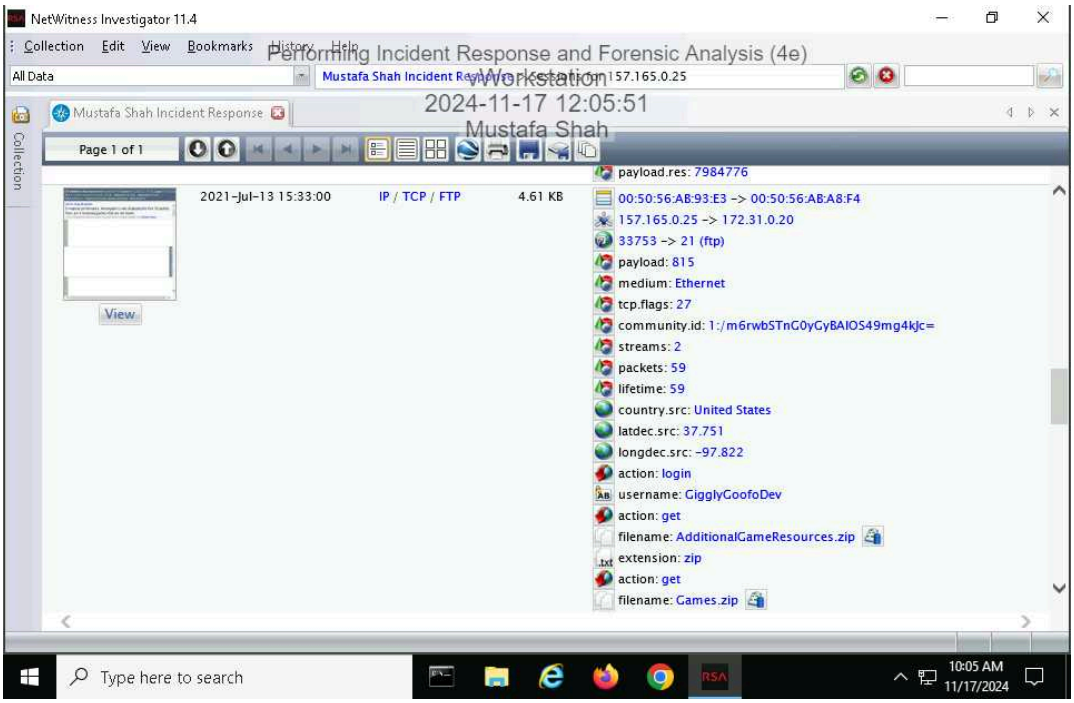
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

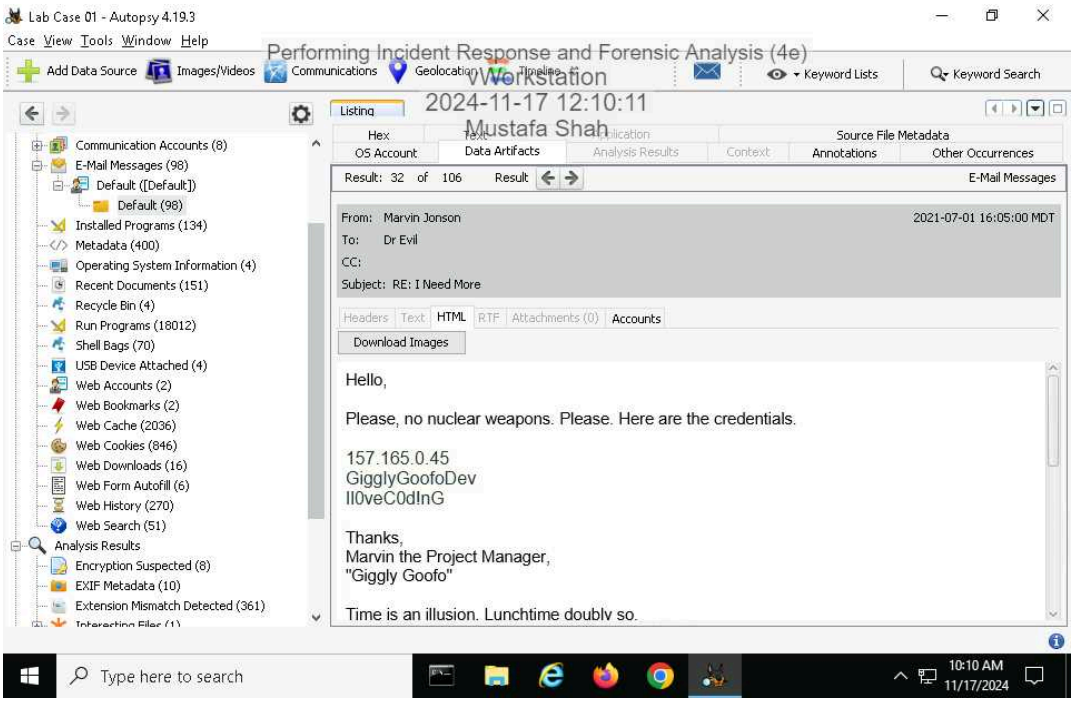


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

11/17/2024

Name
Insert your name here.

Mustafa Shah

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.

Compromised User Credentials, Compromised System, Theft

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 discovered: 07/21/2021 10:30 AM Date reported: 07/21/2021 10:30 AM Date occurred: 07/13/2021 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.

Estimated quantity of systems affected: 1Estimated quantity of users affected: 1Third parties involved: 1

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: 157.165.0.25Attack Destinations: 172.31.0.20IP Addresses of affected systems: 172.31.0.20 Primary functions of affected systems: Workstation

Users Affected by the Incident

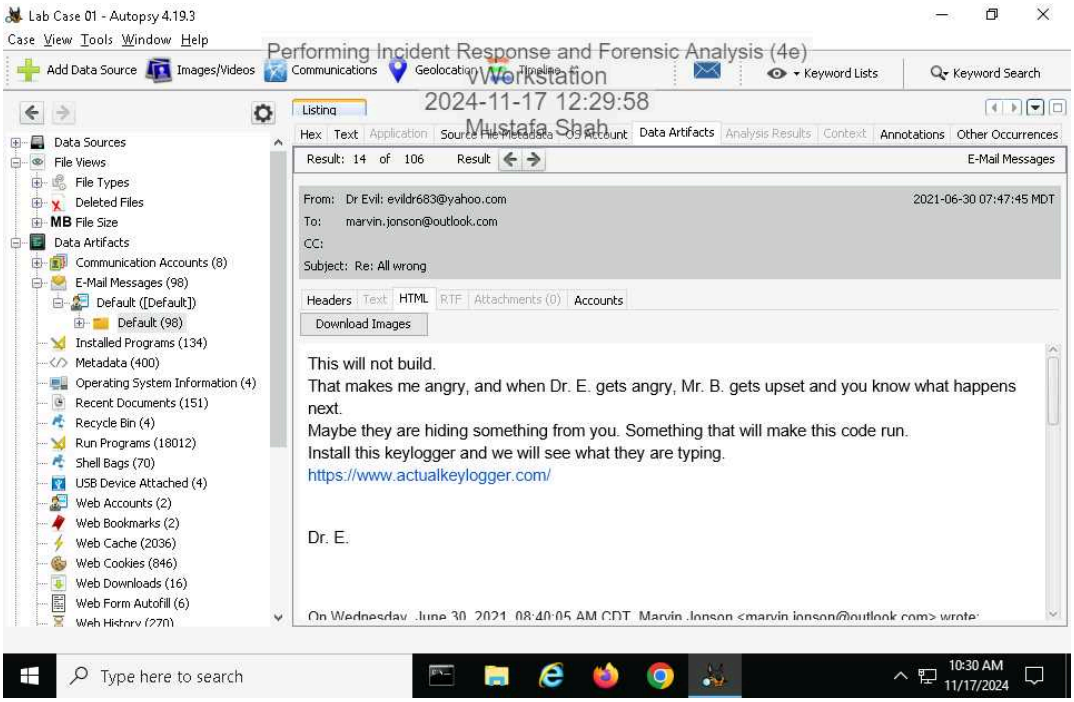
Define the following: Names and job titles of the affected users.

Marvin Jonson, Project Manager

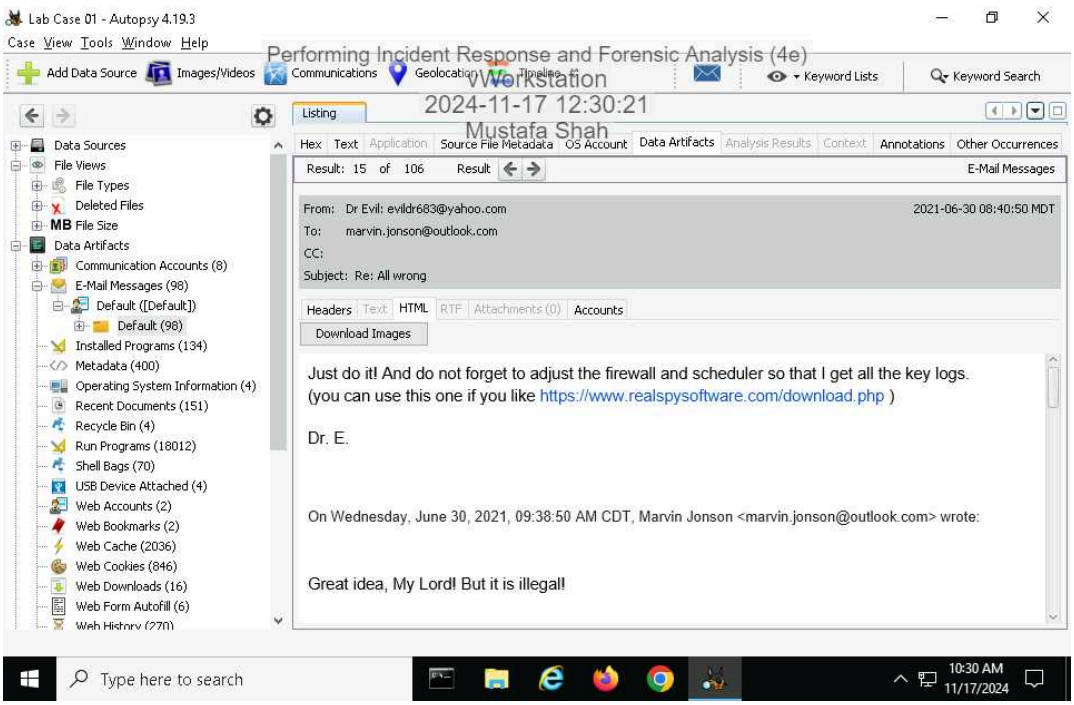
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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

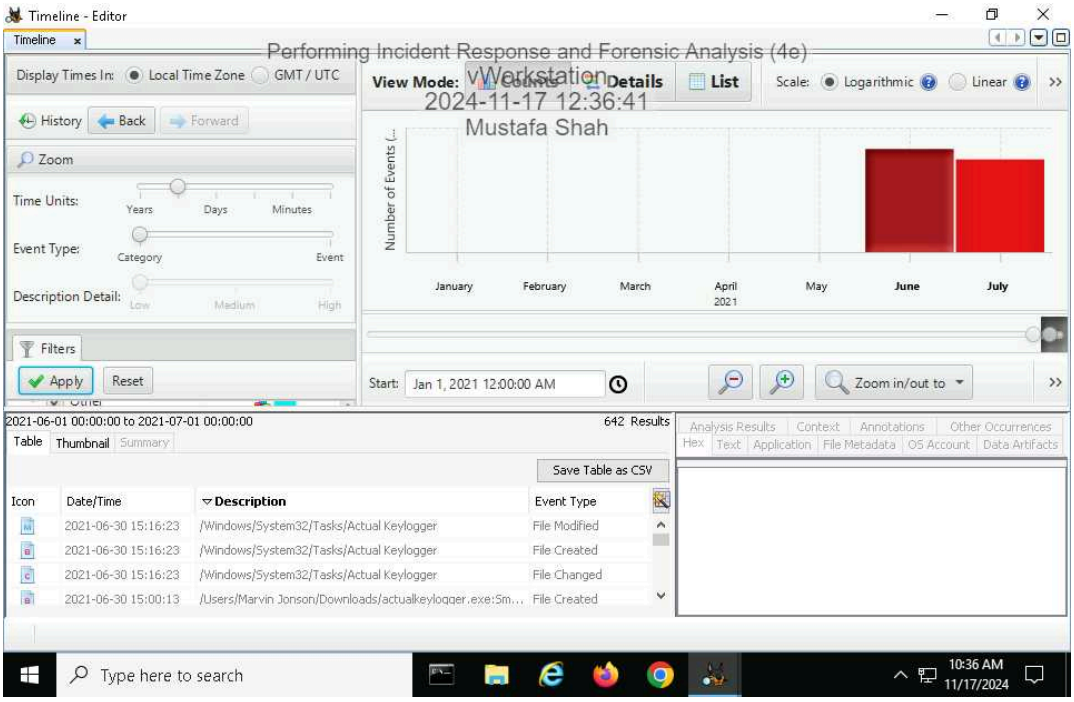


6. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.

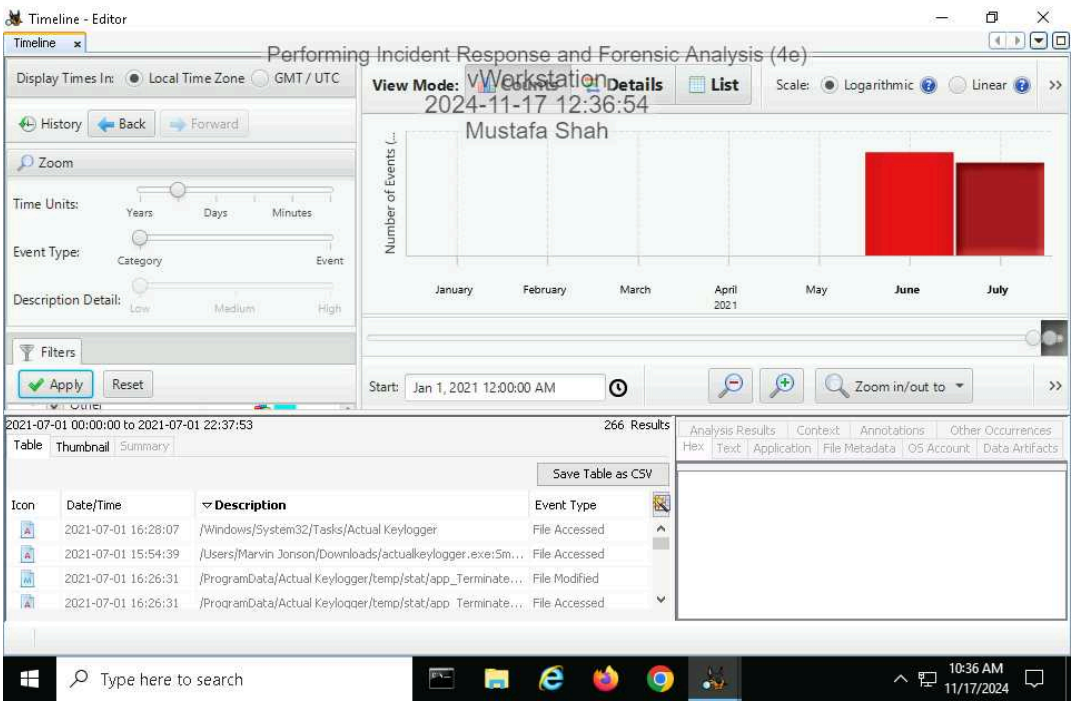


Part 2: Identify Evidence of Spyware

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.

2021-06-30 15:00:13

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

2021-07-01 15:54:39

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

Because the file was modified and accessed twice in a short span of time, there is sufficient evidence to prove that he had opened it.

Part 3: Update an Incident Response Report

Date
Insert current date here.

11/17/2024

Name
Insert your name here.

Mustafa Shah

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

Unchanged

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

Unchanged

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

Date of first interaction: 6/30/2021

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

Third parties: Employee, unidentified attacker

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.

Unchanged

Users Affected by the Incident

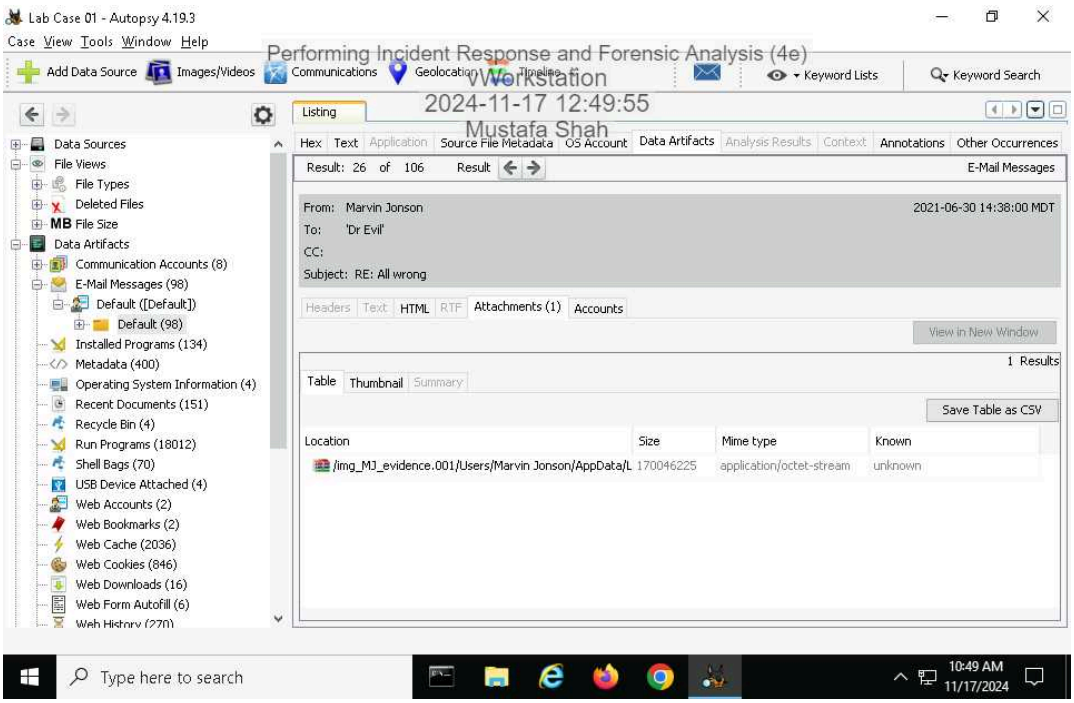
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Unchanged

Section 3: Challenge and Analysis

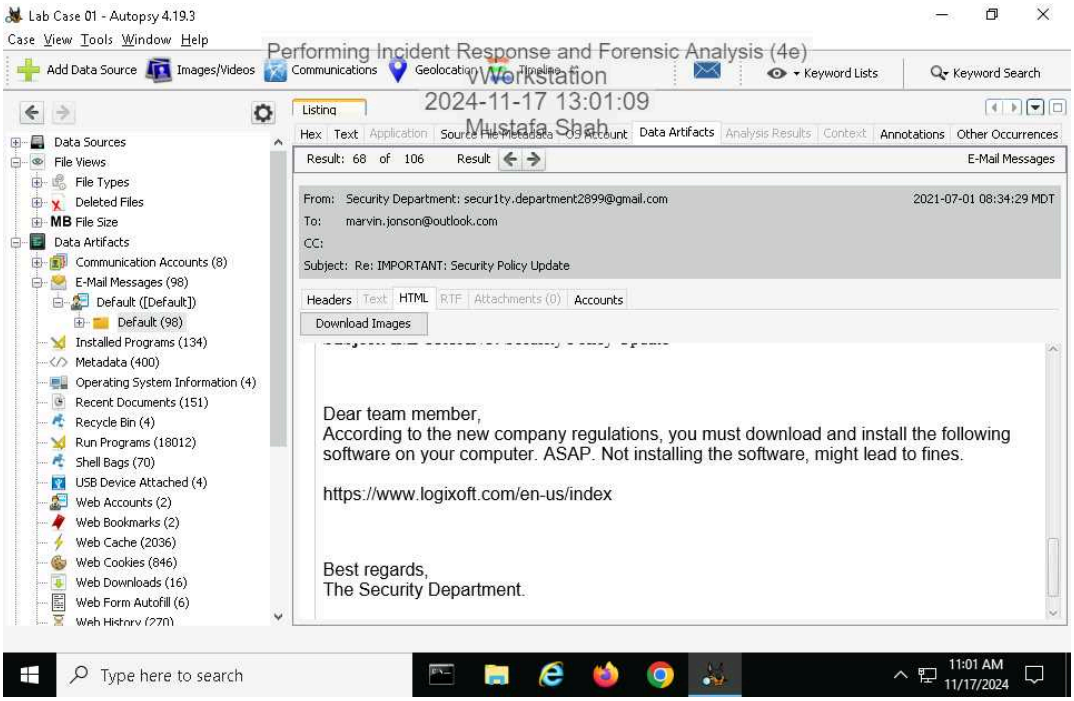
Part 1: Identify Additional Evidence of Data Exfiltration

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.

Email address having number abbreviations as well as an overall suspicious origin. Explicit mention to not discuss the conversation outside of the thread. Link placed in email with instructions to download as something it is not.