Student:	Email:
Kanchan Chopde	hq0656@wayne.edu

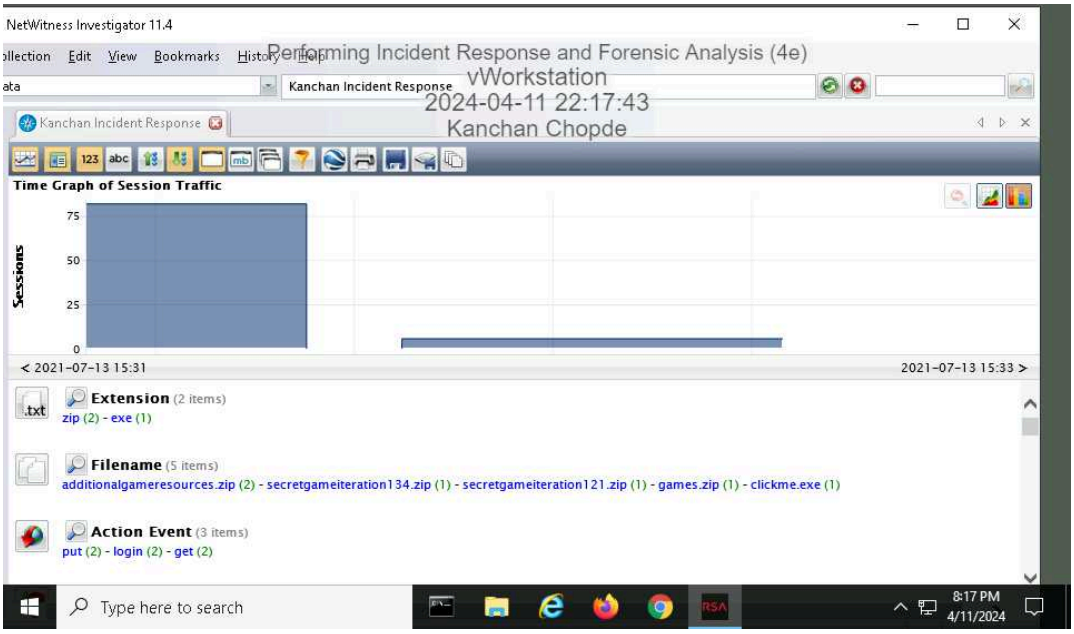
Time on Task:	Progress:
4 hours, 32 minutes	100%

Report Generated: Thursday, April 18, 2024 at 11:04 PM

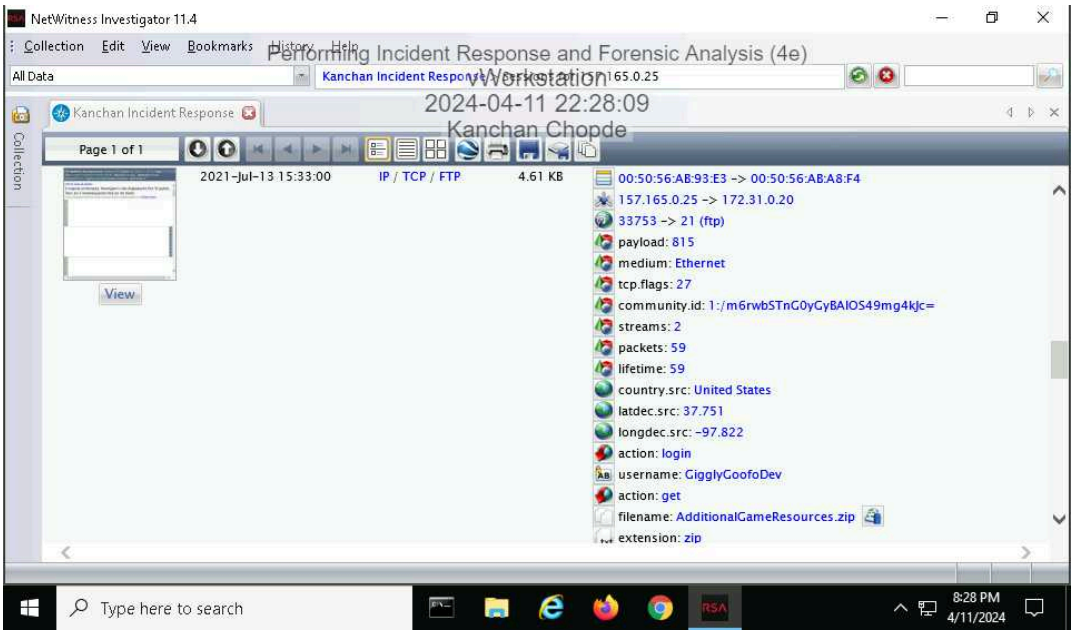
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

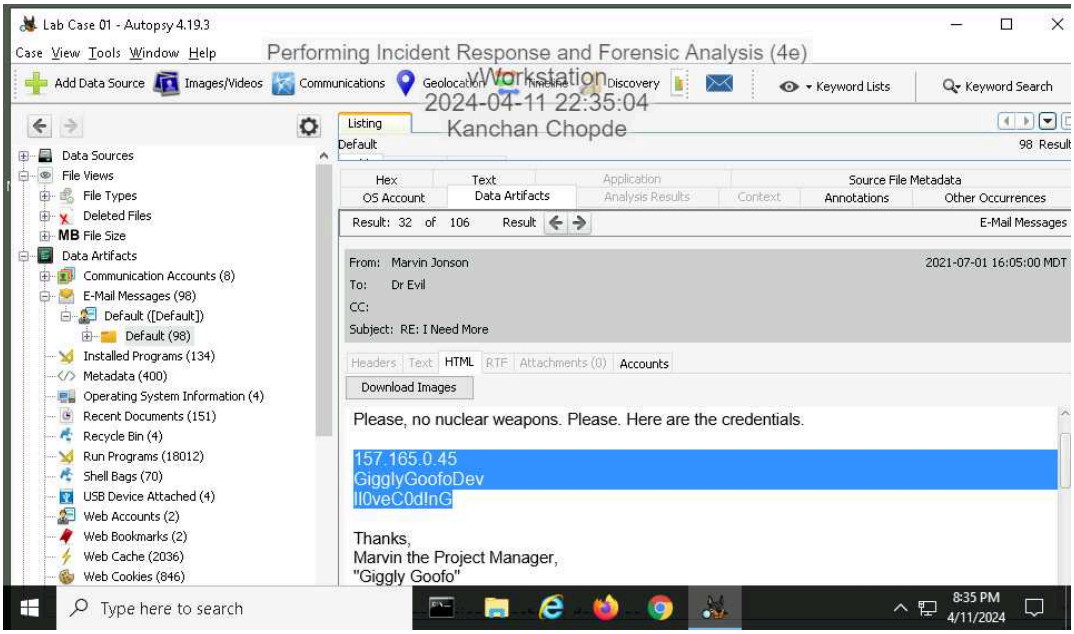


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

16th April 2024

Name
Insert your name here.

KANCHAN CHOPDE

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

As per CRR Supplemental Resource Guide, Low level cyber security incidents include suspected sharing of individually assigned accounts. Here , we can see that in Marvin's outlook we got the credentials shared to Dr. Evil. In some cases, this can lead to medium cyber security incident if not taken corrective action against it as attacker might gain access to organization's data through credentials.

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

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 when the incident was discovered: 31st July 2021, 10:30 AM Eastern Time
Date and time when the incident was reported: 31st July 2021, 10:40 AM Eastern Time
Date and time when the incident occurred: 13 July 2021 , 15:33:00
FTP transfer between 157.165.0.25 and 172.31.0.20Filename: AdditionalGameResource.zip
Credential details in email: Username: GigglyGoofoDev Password: Il0veC0d!nG

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 : System with IP 172.31.0.20 has been targeted.estimated quantity of users : Single user , The project Manager's machine seemed to be affected.
Malicious File : ClickMe.exe has been observed.

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 (e.g., IP address, port): 157.165.0.25, port : 33753
Attack destinations (e.g., IP address, port): 172.31.0.20, port:21 (ftp)Payload size: 815 bytes
Packet Count: 59

Users Affected by the Incident

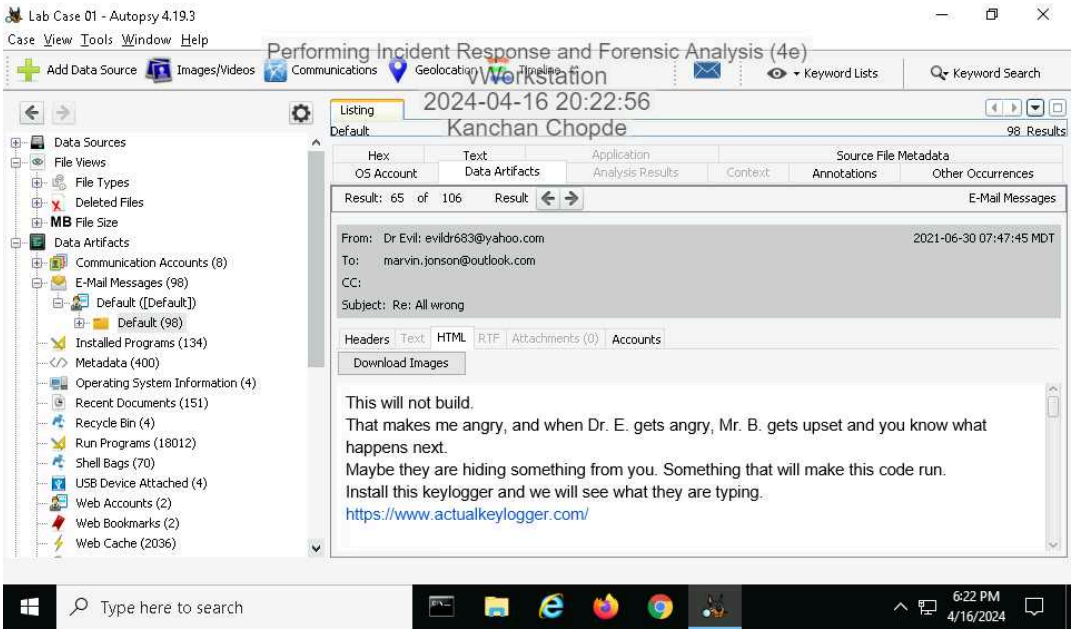
Define the following: Names and job titles of the affected users.

Names and job titles of the affected users: Marvin Jonson, Project Manager and if he shares the malicious files with other team mates they are also at risk.

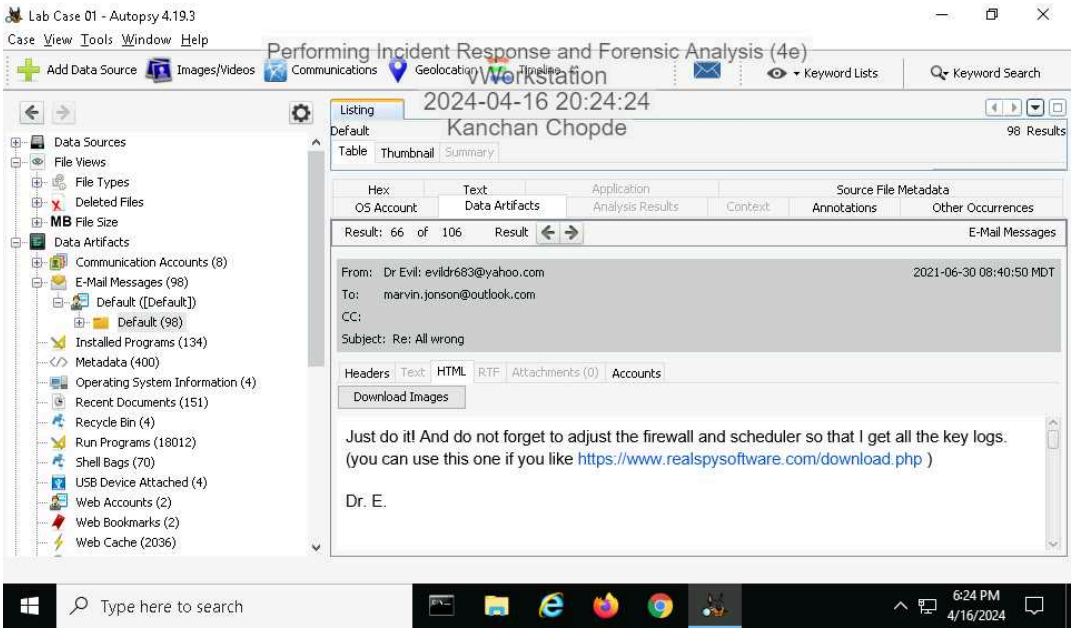
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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

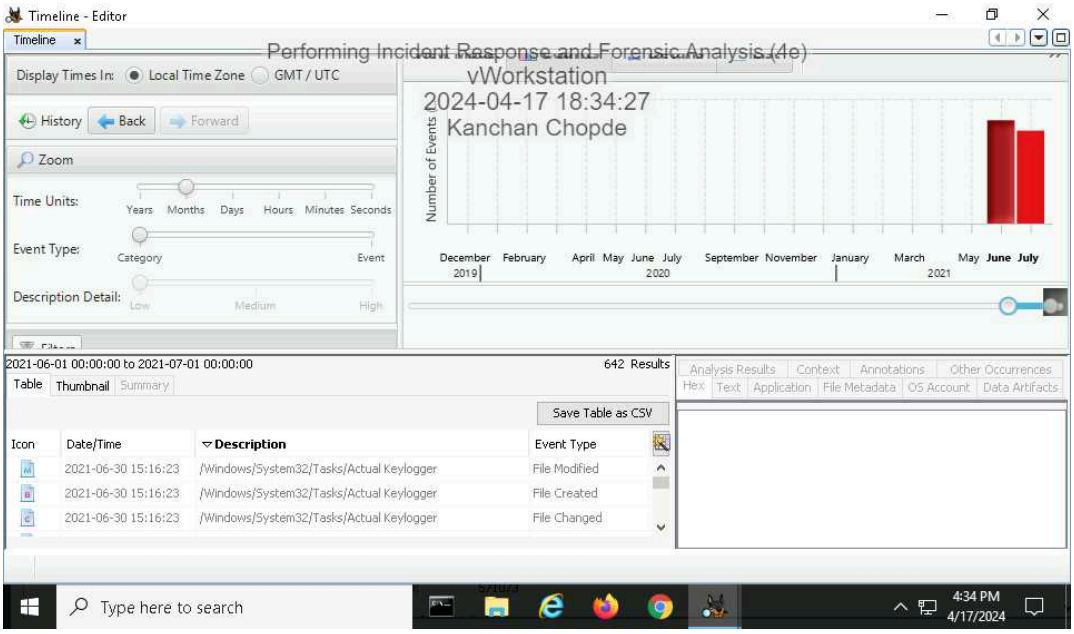


6. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.

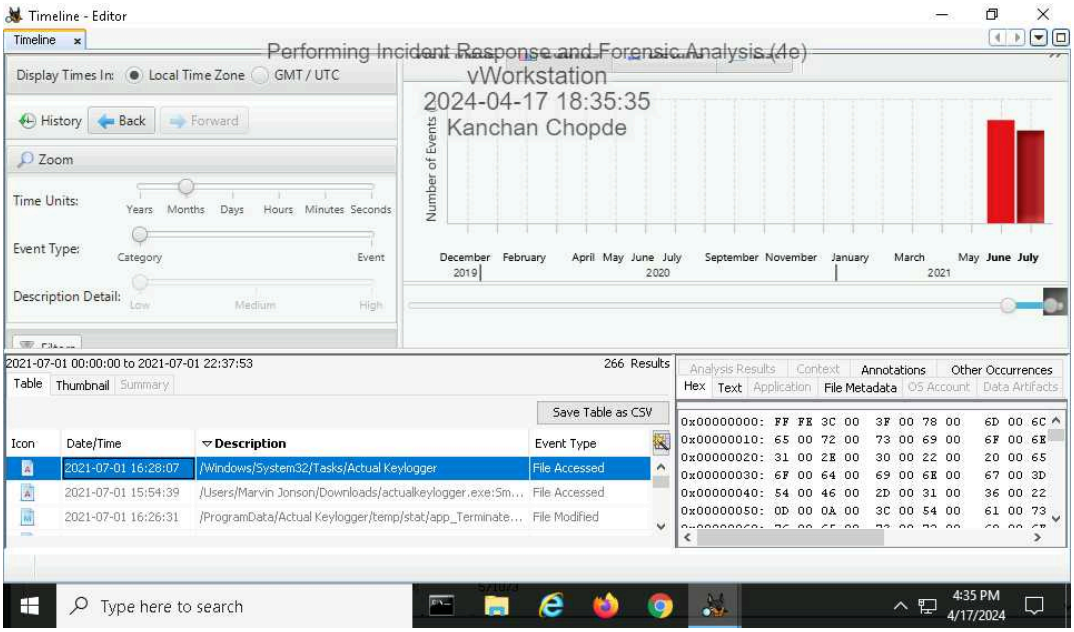


Part 2: Identify Evidence of Spyware

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.

In July, file was last accessed on 2021-07-01 at 15:54:39. So I think this evidence claims Marvin accessed the keylogger.

Part 3: Update an Incident Response Report

Date
Insert current date here.

17th April 2024

Name
Insert your name here.

KANCHAN CHOPDE

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

Yes, incident priority now has changed because Marvin was compelled by Dr Evil to install keylogger and make other unauthorized changes to his workstation. Hence , now it has medium severity.

Incident Type

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

Earlier it was Compromised User Credentials. Now the incident type has changed, it has Compromised Access as we have evidence that keylogger file was last accessed sometime in July which might have given unauthorized access by guessing keystrokes. It is also a type of Malware and spyware attack that tracks keystrokes and records them. It can also be a form of social engineering attack where user is tricked to install malware i.e. keylogger in our case through human error as Dr. Evil reminds Marvin to install and schedule the Malware.

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 and time when keylogger's executable file was created on : 2021-30-06 at 15:00:13Date and time when keylogger's executable file was last started on : 2021-07-01 at 15:54:39
Also there have been three events that related to the Actual Keylogger file in the /Windows/System32/Tasks folder and they have June 30 time stamp.
Also there is One event that related to the Actual Keylogger file in the /Windows/System32/Tasks folder that have July 1 time stamp.

Incident Scope

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

Yes the incident scope has now changed. There has been installation of a keylogger file, unauthorized changes to firewall are made, scheduled tasks are implemented.

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. Keylogger has been scheduled on Marvin Jonson's laptop.

Users Affected by the Incident

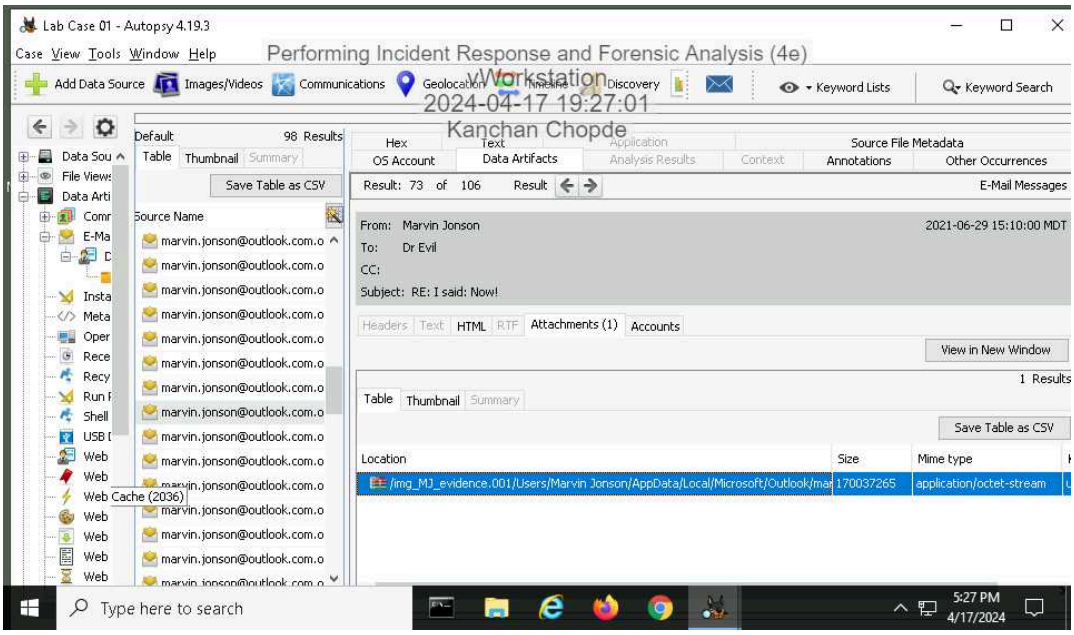
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Users affected would also be same as keylogger executable was scheduled on Marvin's laptop. And if he shared any other details related to other employees , it would also be tracked and potential data breach of other employees information is also possible.

Section 3: Challenge and Analysis

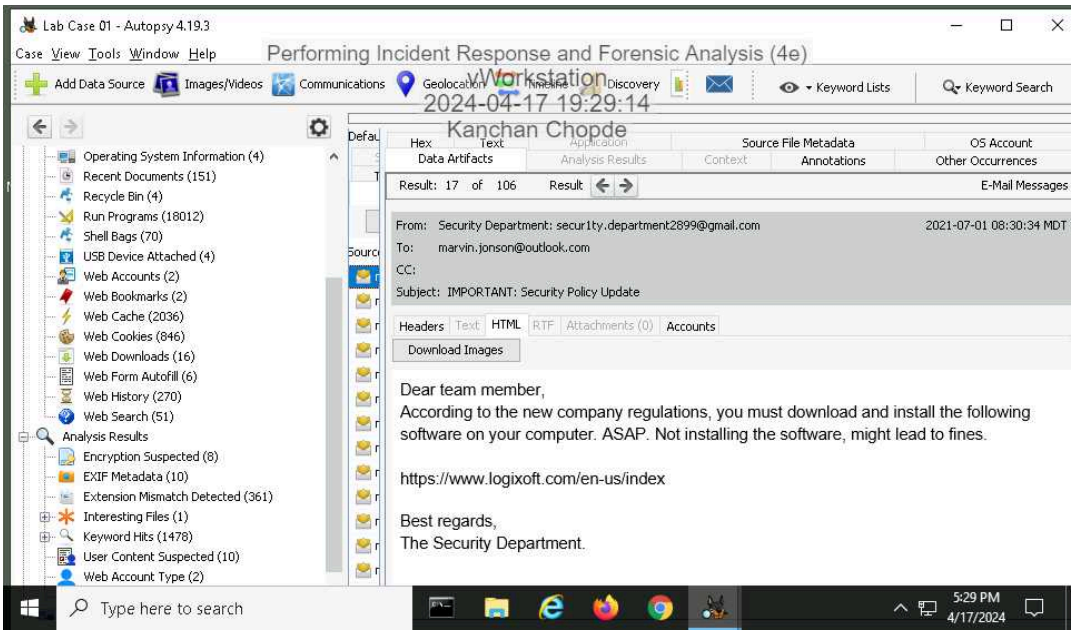
Part 1: Identify Additional Evidence of Data Exfiltration

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: secur1ty.department2899@gmail.com seems suspicious with security spelling written as secur1ty and coming not from organization domain rather gmail.com.
Also link to install software doesn't seem to be safe originating from outside organization.