Student:	Email:
Yengkong Sayaovong	ysayaovo@asu.edu

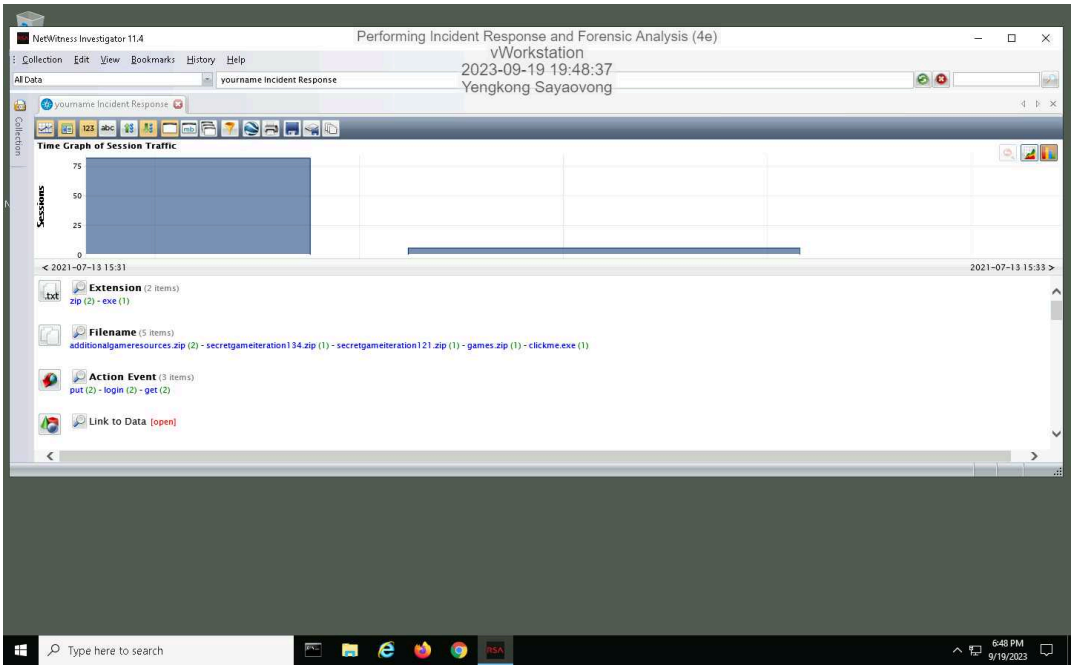
Time on Task:	Progress:
4 hours, 15 minutes	100%

Report Generated: Tuesday, September 19, 2023 at 9:49 PM

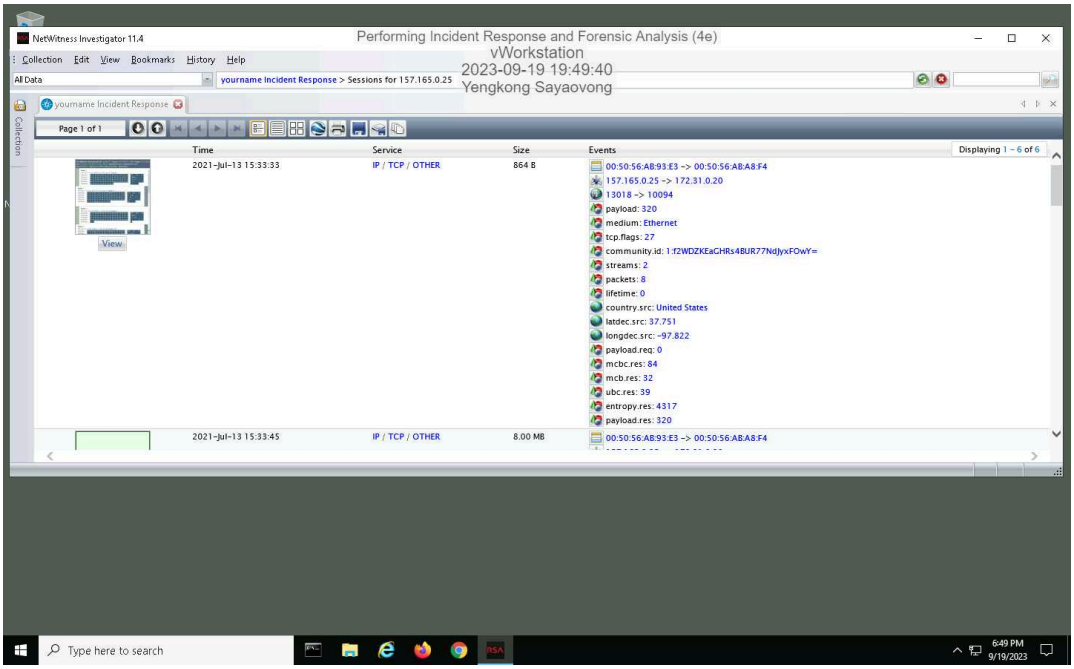
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

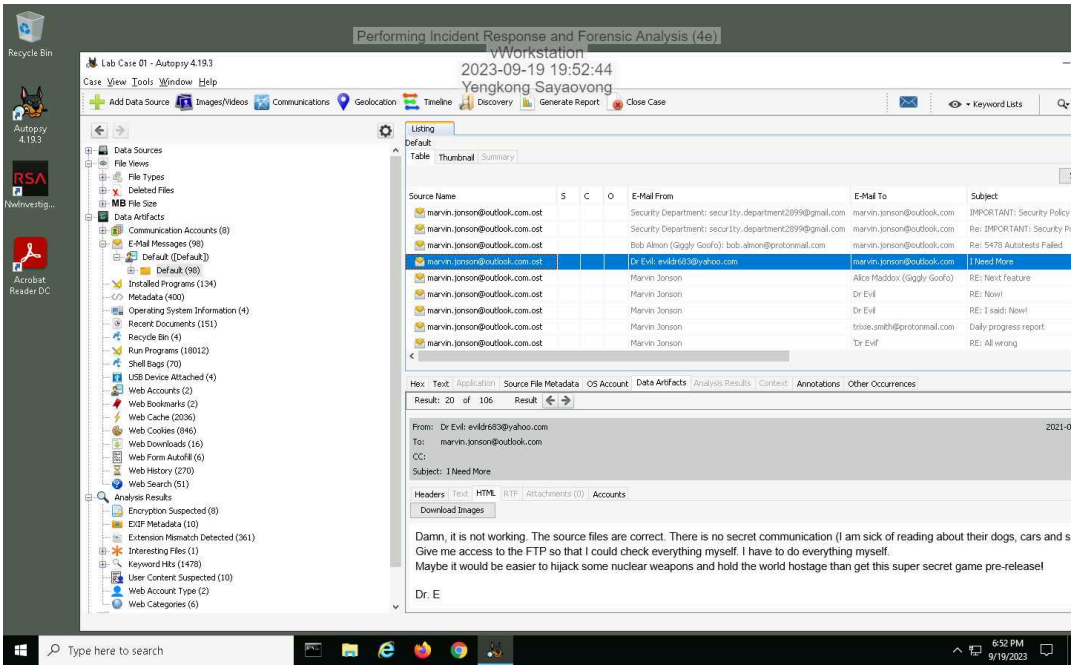


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

09/19/23

Name
Insert your name here.

Yengkong Sayaovong

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 system/information

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.

Incident Occurred: 13th July 2021 - 3:31 pm to 3:33 pm
Incident Discovered: 31st July 2021 - 10:30 am

Incident Reported: 31st July 2021 - 10:40 am (10 mins after discovering)

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 system affected - Game development
Estimated quantity of users affected - game developers, sponsors, players Third-party involved - partners

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 - 157.165.0.25
Attack destination - 172.31.0.20

IP address affected - the above 2 IP addresses
Primary functions affected - stolen game data, exfiltration

Users Affected by the Incident

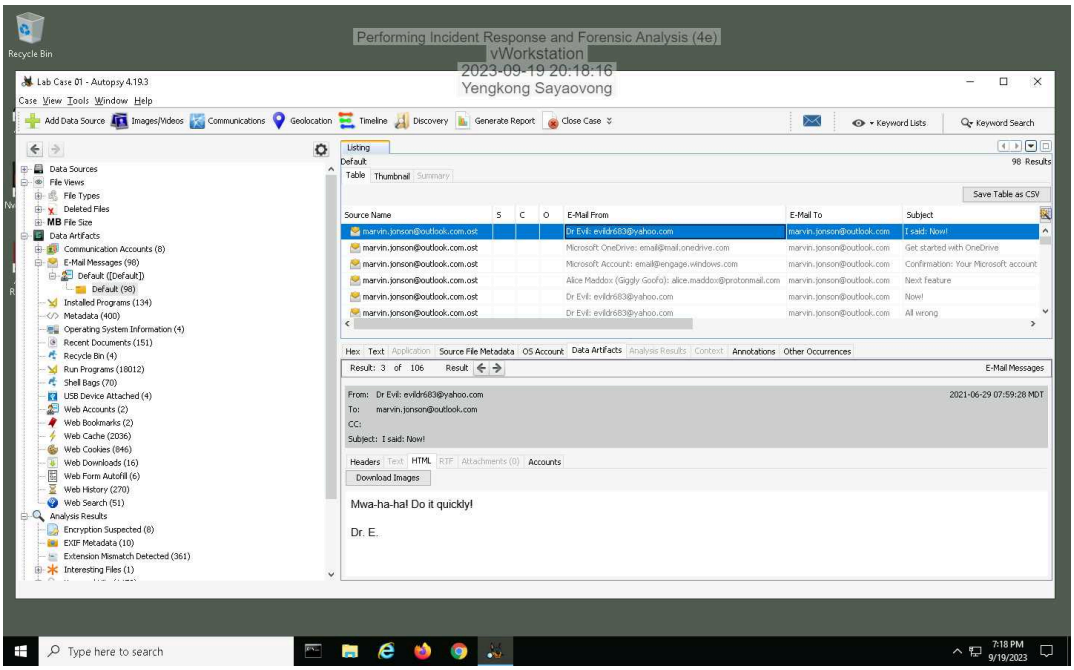
Define the following: Names and job titles of the affected users.

Name - Marvin Jonson
job - Game developer

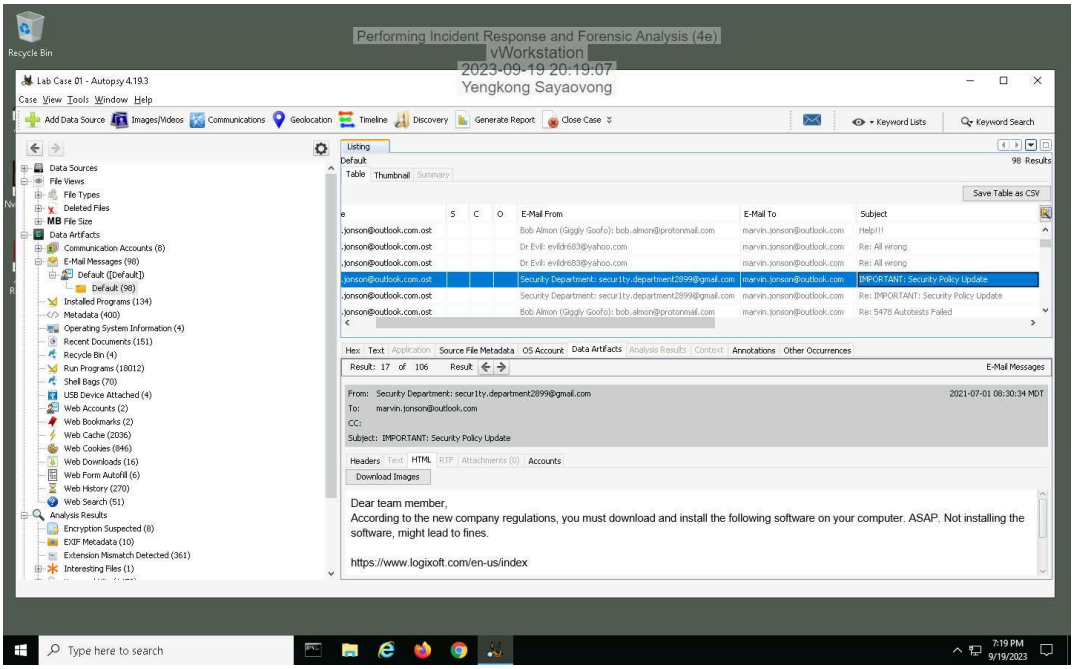
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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

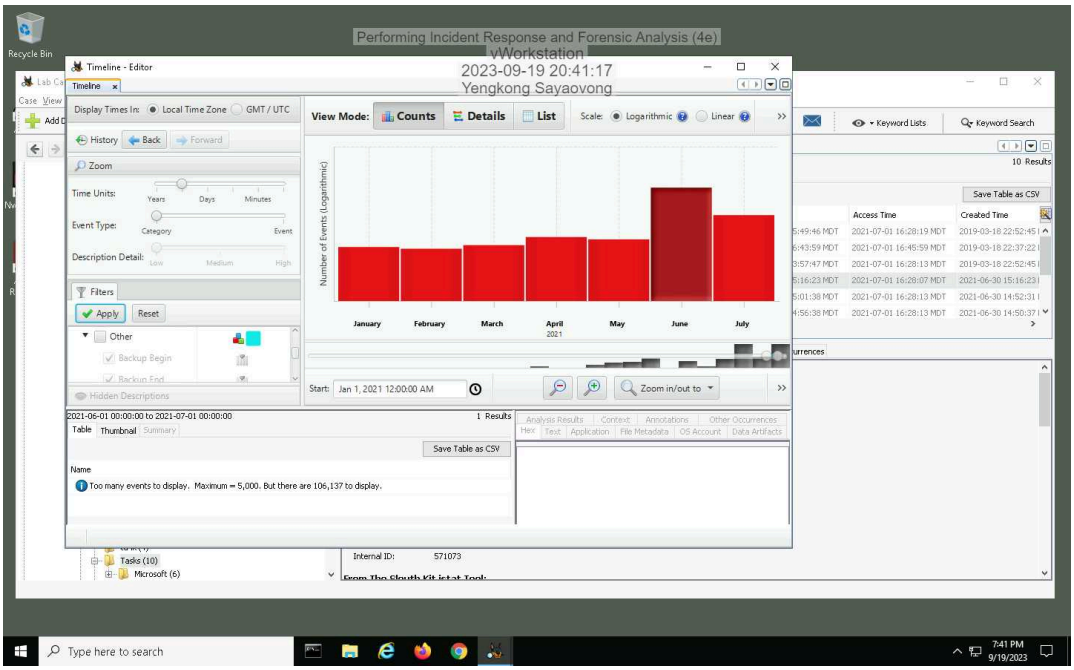


6. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.

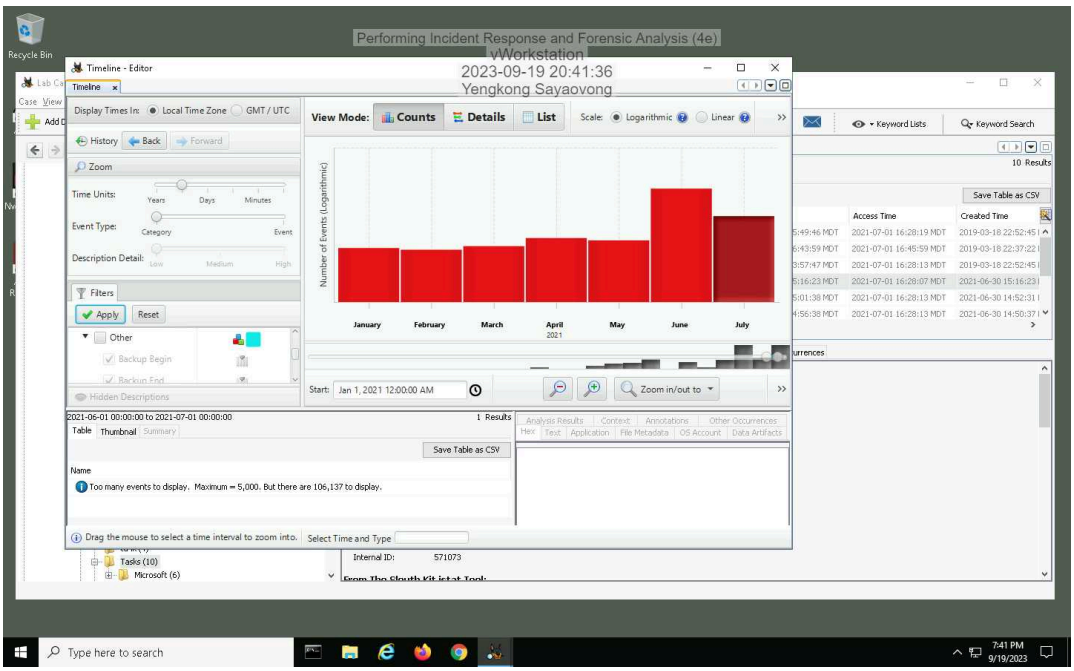


Part 2: Identify Evidence of Spyware

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.

Jan 1, 2021 12:00:00 AM

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

Jan 1, 2021 12:00:00 AM

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

Yes

Part 3: Update an Incident Response Report

Date
Insert current date here.

9/19/23

Name
Insert your name here.

Yengkong Sayaovong

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.

The incident occurred on 30th June & 1st July 2021

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

unchanged

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

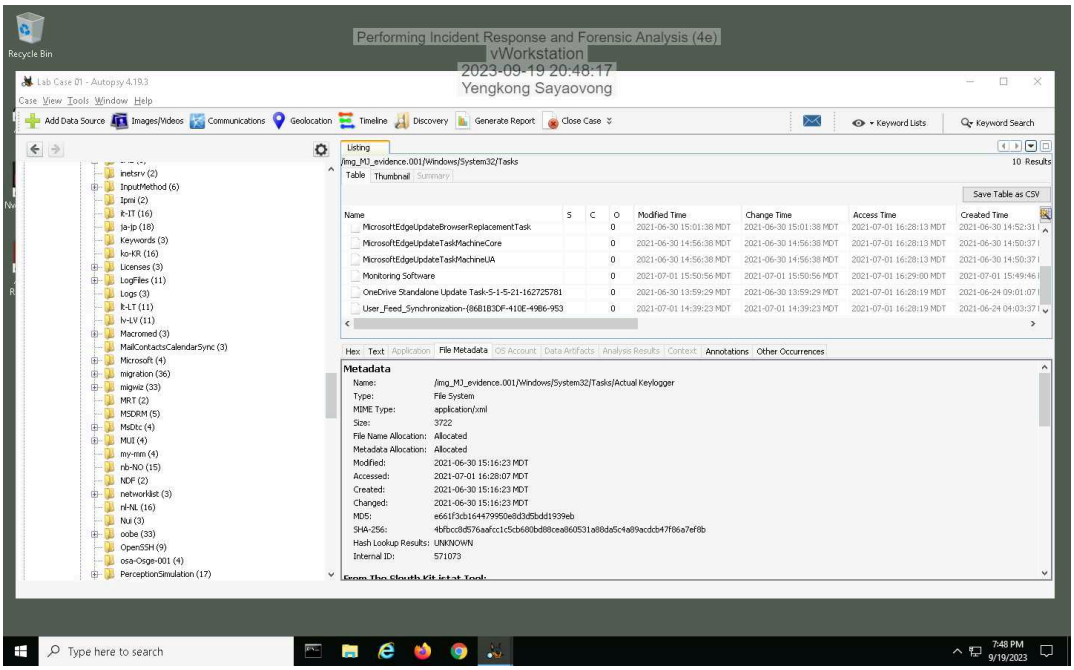
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

unchanged

Section 3: Challenge and Analysis

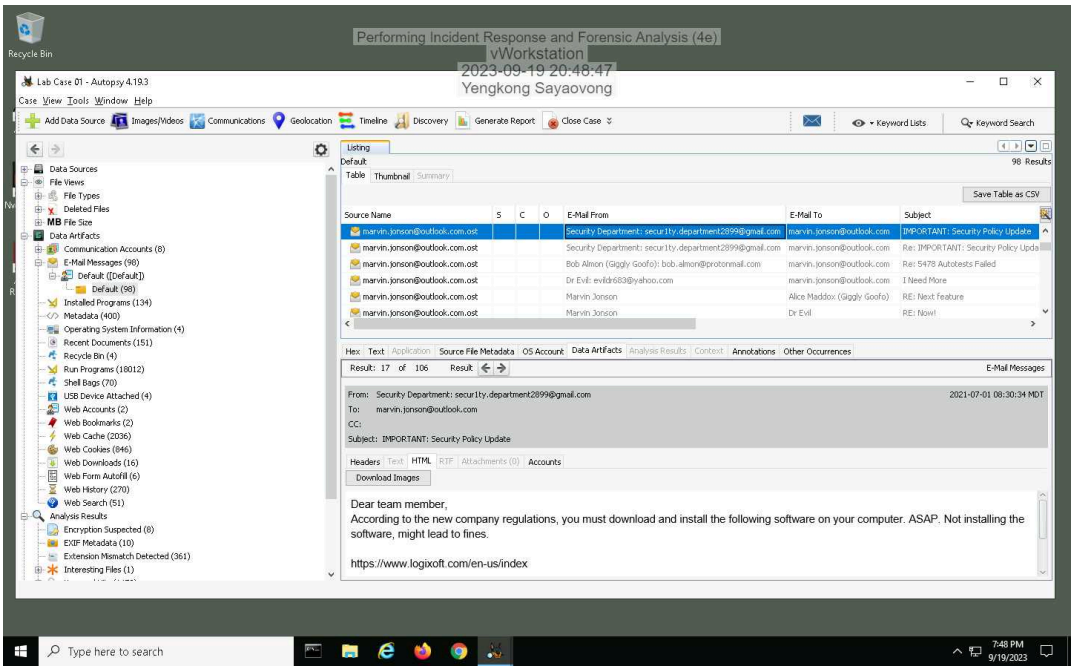
Part 1: Identify Additional Evidence of Data Exfiltration

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.

Asked Marvin to do it ASAP