Student:	Email:
muhammad zahid	zahid1mz@cmich.edu

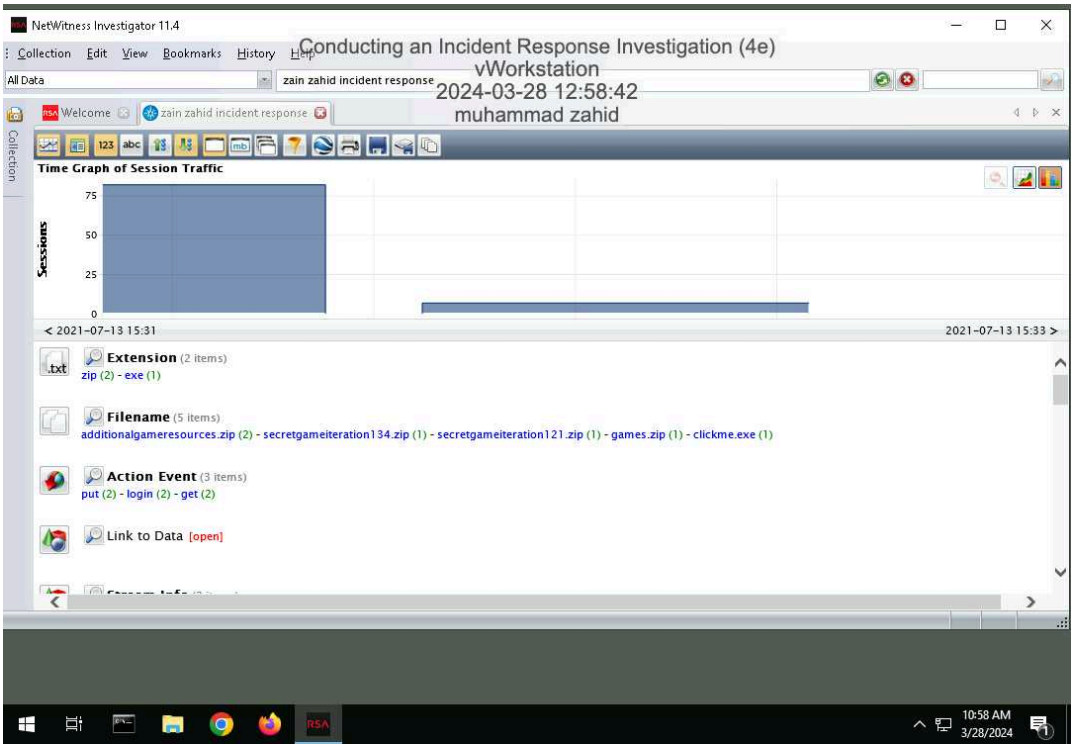
Time on Task:	Progress:
4 hours, 20 minutes	100%

Report Generated: Thursday, March 28, 2024 at 2:40 PM

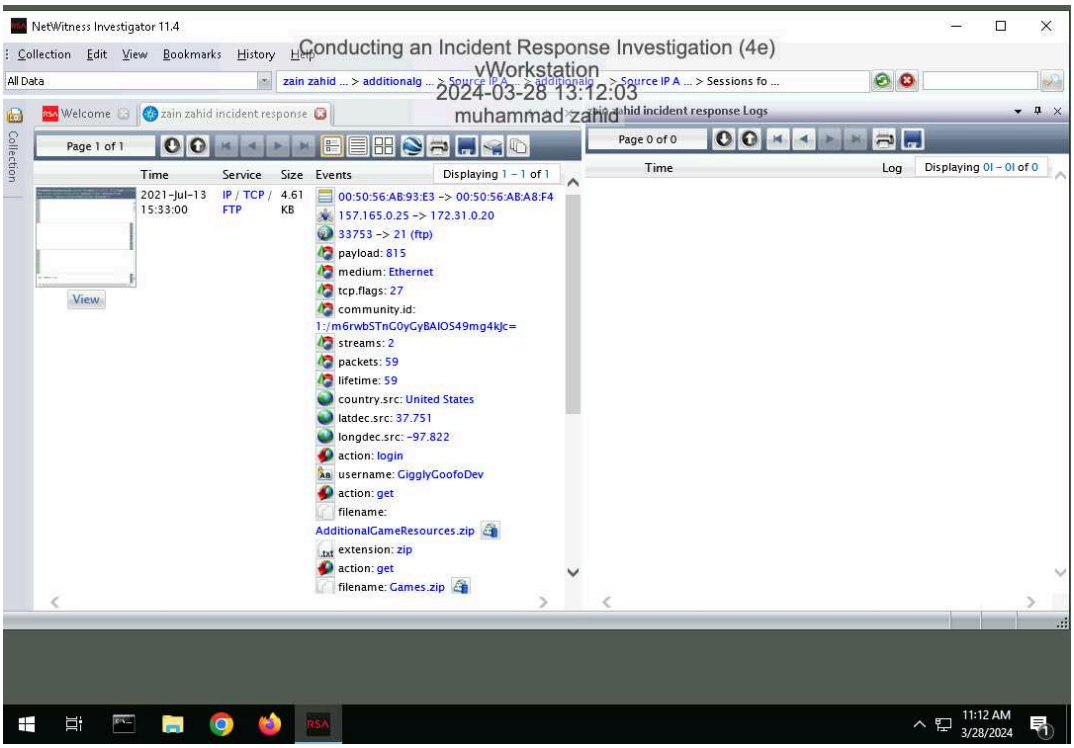
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

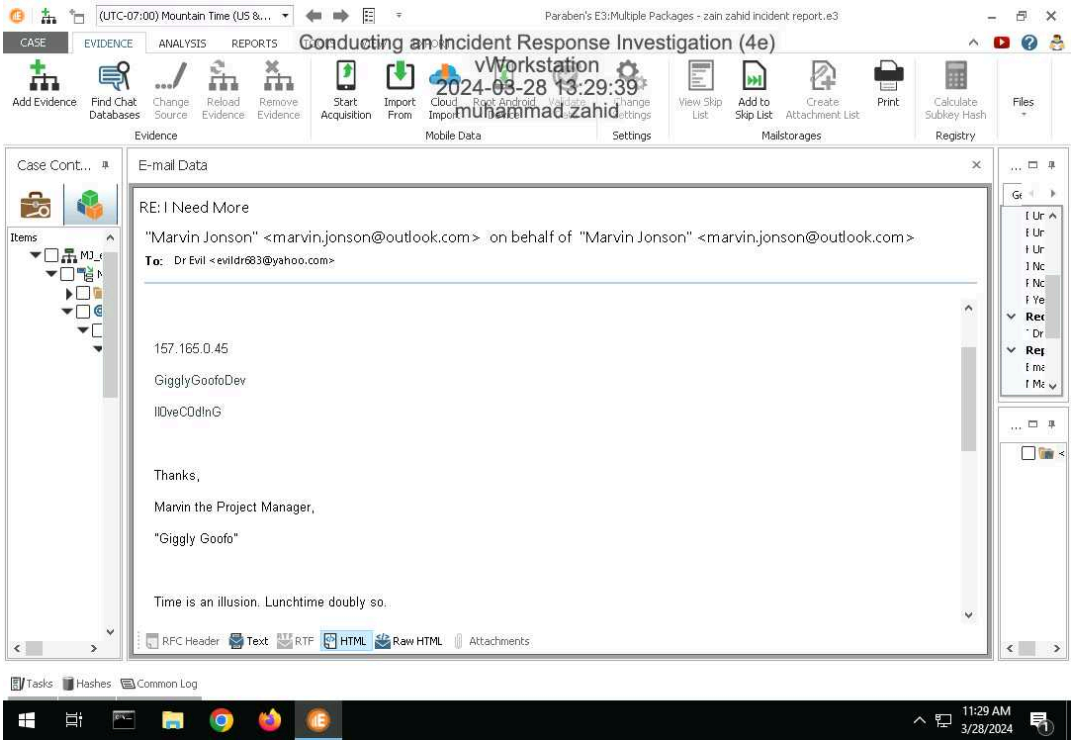


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



Part 2: Analyze a Disk Image for Forensic Evidence

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



Part 3: Prepare an Incident Response Report

Date
Insert current date here.

March 28, 2024

Name
Insert your name here.

Zain Zahid

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

Critical

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.

The incident was discovered on July 31,2021 at 10:30 EST. It was reported 10 minutes after its discovery

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.

The system that was affected 157.165.0.45. the users involved were dr.evil(evildr683@yahoo.com)(third-party), Marvin Jonson(affected party). It was disk information theft.

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 source - 157.165.0.25, Attack Destination - 172.31.0.20. IP Ports: 33753 and 21(ftp). Medium - Ethernet

Users Affected by the Incident

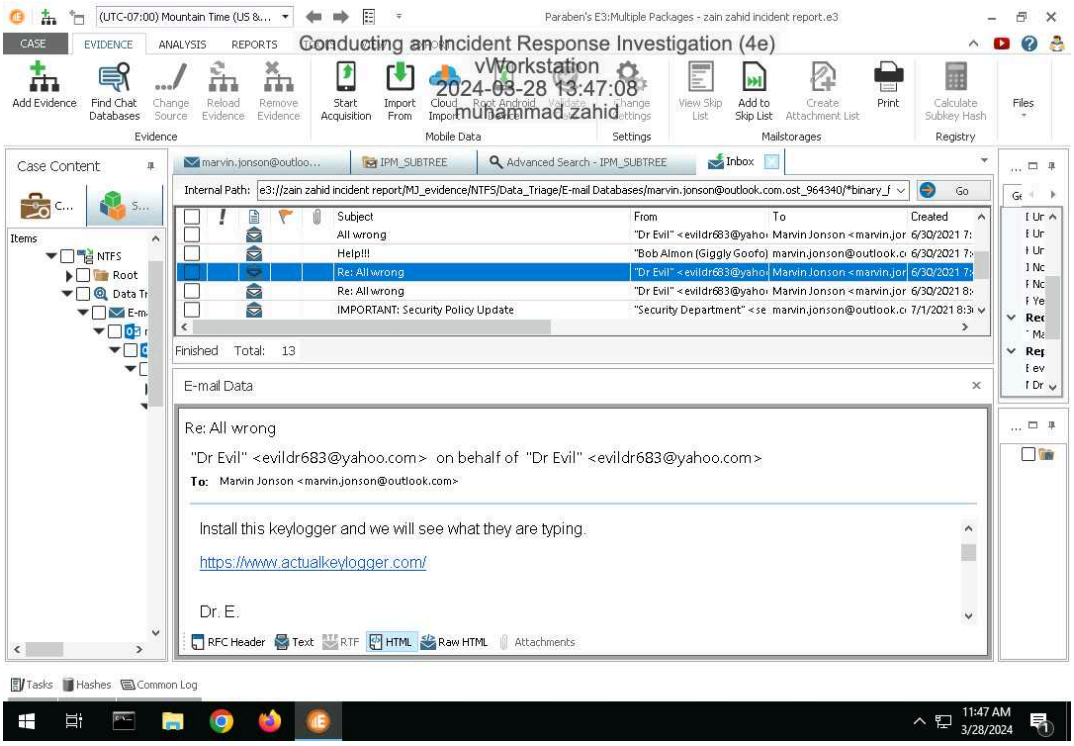
Define the following: Names and job titles of the affected users.

Marvin Jonson - Project Manager

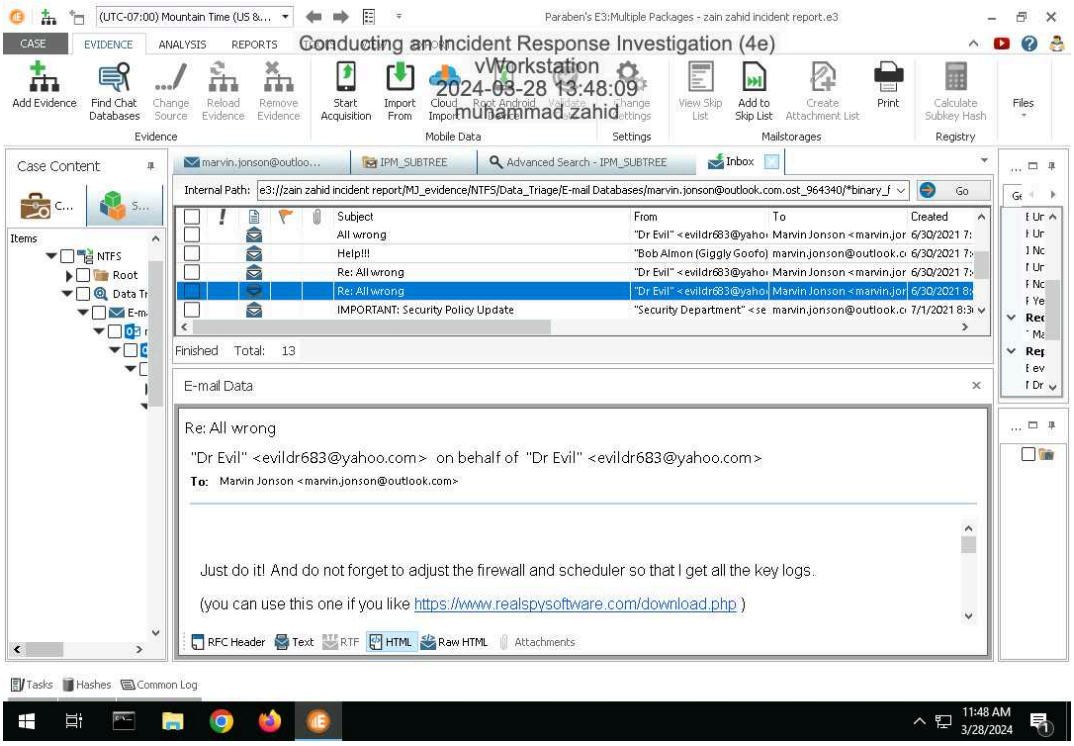
Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

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



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



Part 2: Identify Evidence of Spyware

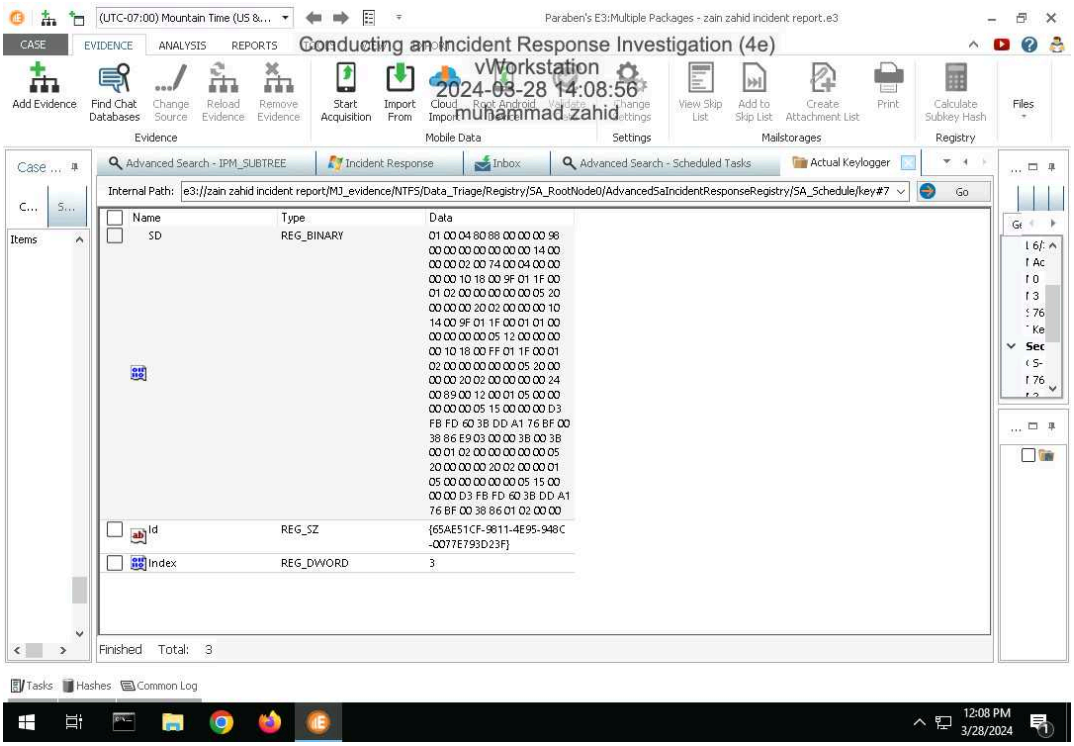
5. **Document** the Author and Date values associated with the scheduled keylogger task.

Author - DESKTOP-CGRK7LT\Marwin JonsonDate - 2021-06-30T14:16:23.2705256

7. **Document** the port used for inbound connections to the keylogger and the name and location of the keylogger executable.

Port : 666Name; Actual keyloggerLocation: C;/ProgramData/Security Monitor/{AKC34567-KCQR-WW34-AK47-INUM589023MY}\akl.exe

9. **Make a screen capture** showing the **registry key value associated with the keylogger and the localSPM service**.



15. **Record** the first time and last time the keylogger was started.

The executable file was created on 2021-06-30 at 15:00:13 The executable file was last started on 2021-07-01 at 15:54:39

17. **Record** whether Marvin interacted with or simply opened the keylogger.

In the description box it is shown that Marvin Jonson's account was used when the file was created and also it(account) was used when keylogger file was accessed

Part 3: Update an Incident Response Report

Date
Insert current date here.

March 28, 2024

Name
Insert your name here.

Zain Zahid

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

Incident priority remains unchanged

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 or Computer Virus

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 new executable file was created by the name of actualkeylogger.exe on 2021-06-30 at 15:00:13, Modified at 15:08:07, and it was last executed on 2021-07-01 at 15:54:39

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

Marvin Jonson's account was compromised by accessing the executable file by the name of actualkeylogger.exe

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.

New system affected by this incident was Marvin Jonson's account.

Users Affected by the Incident

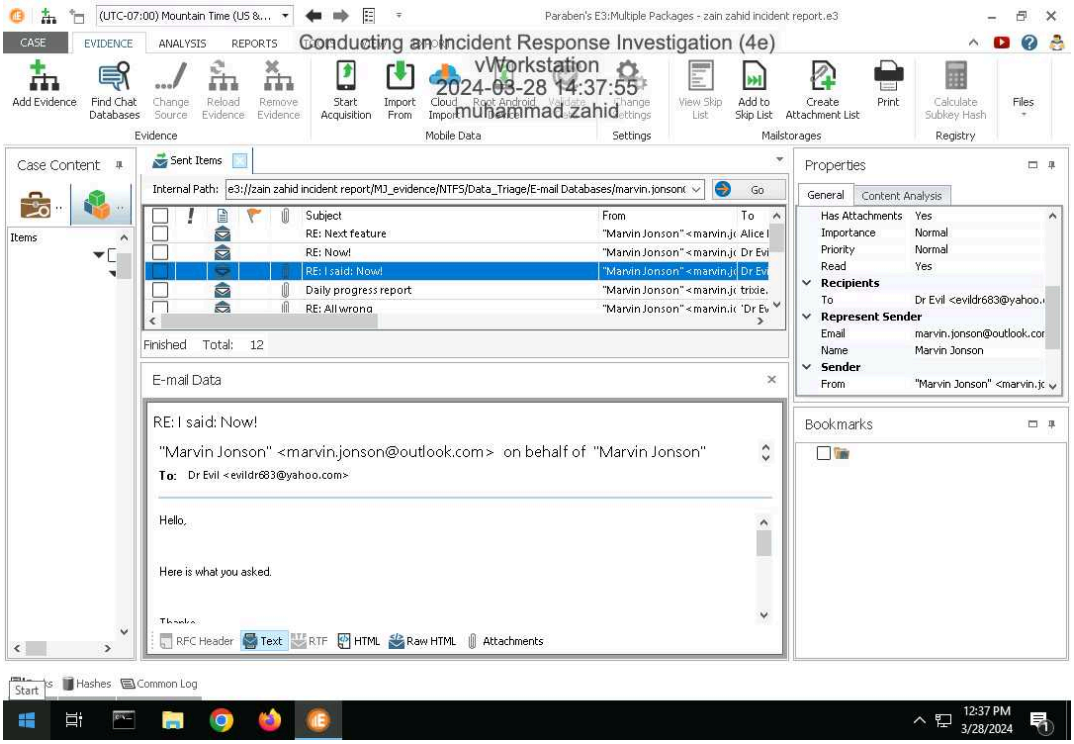
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

It remains 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**.