Student:	Email:
Vishal Singh Bhardvaj	

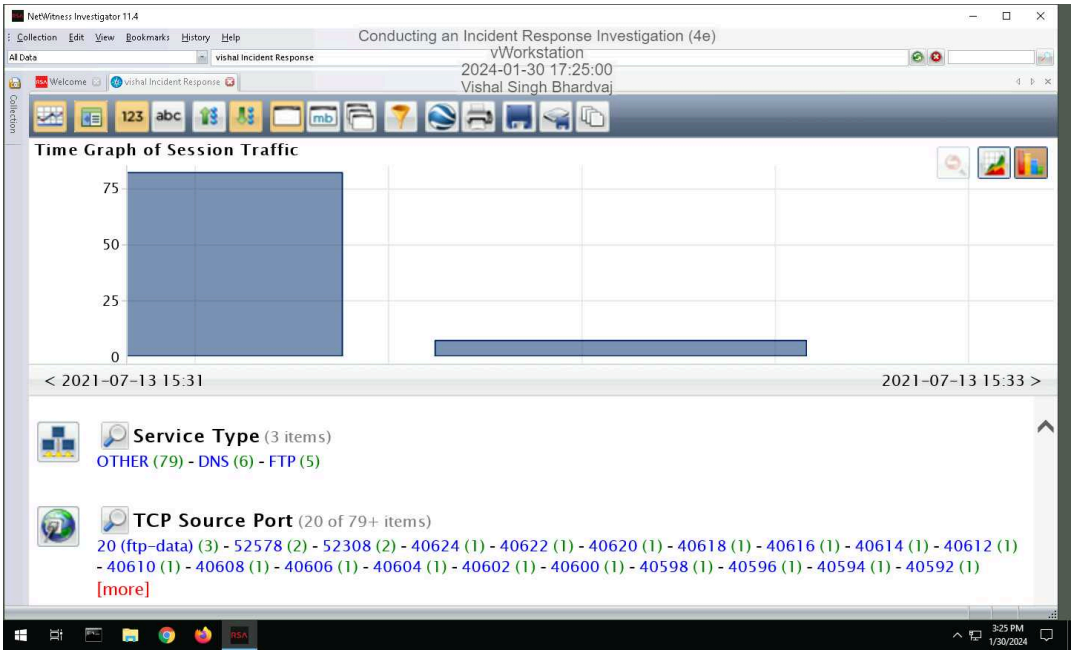
Time on Task:	Progress:
2 hours, 34 minutes	100%

Report Generated: Tuesday, January 30, 2024 at 7:50 PM

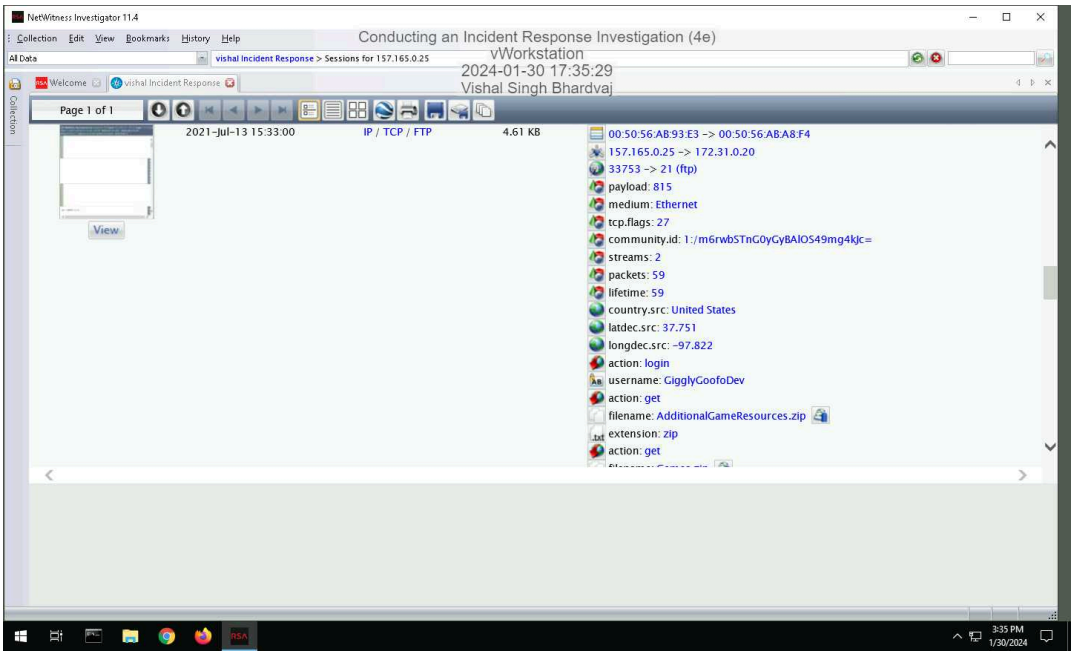
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

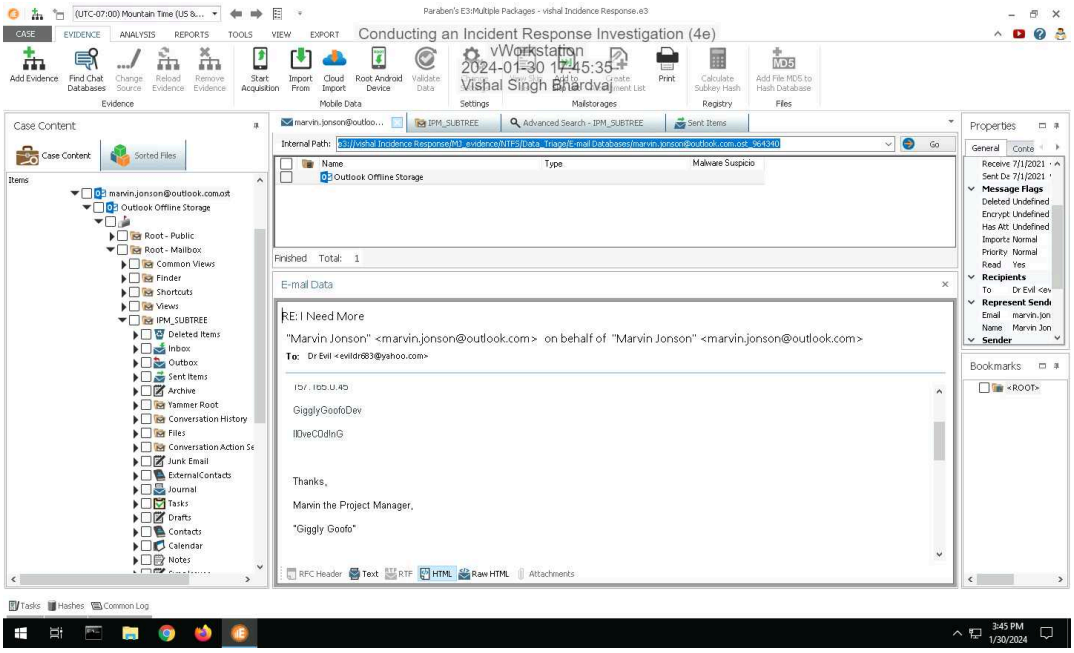


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

01/30/2024

Name
Insert your name here.

Vishal Singh Bhardvaj

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

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 Discovery Time:- July 31, 2021 at 10:30 AM
Incident Reporting Time:- July 31, 2021 at 10:40 AM

Incident Occurrence Time:- July 13, 2021 at 3:33:00 PM

Note:- There were multiple sessions established during suspected incidence but first such session was established at 3:33:00 PM on July 13,2021

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.

Number of System affected is 1. Because suspected IP 157.165.0.25 established 7 sessions with same destination IP address - 172.31.0.20.
Estimated quantity of users affected- Only 1 user who is suspected to have shared his credential using email exchange.

Third parties involved or affected- One third party having IP address 157.165.0.25 is involved.

High impact incident as Intellectual property breach is there.

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 IP address- 157.165.0.20, port 17177
Destination IP address- 172.31.0.20, port 10094

Primary function of affected system- FTP Server- File transfer of 2 suspected files.

Users Affected by the Incident

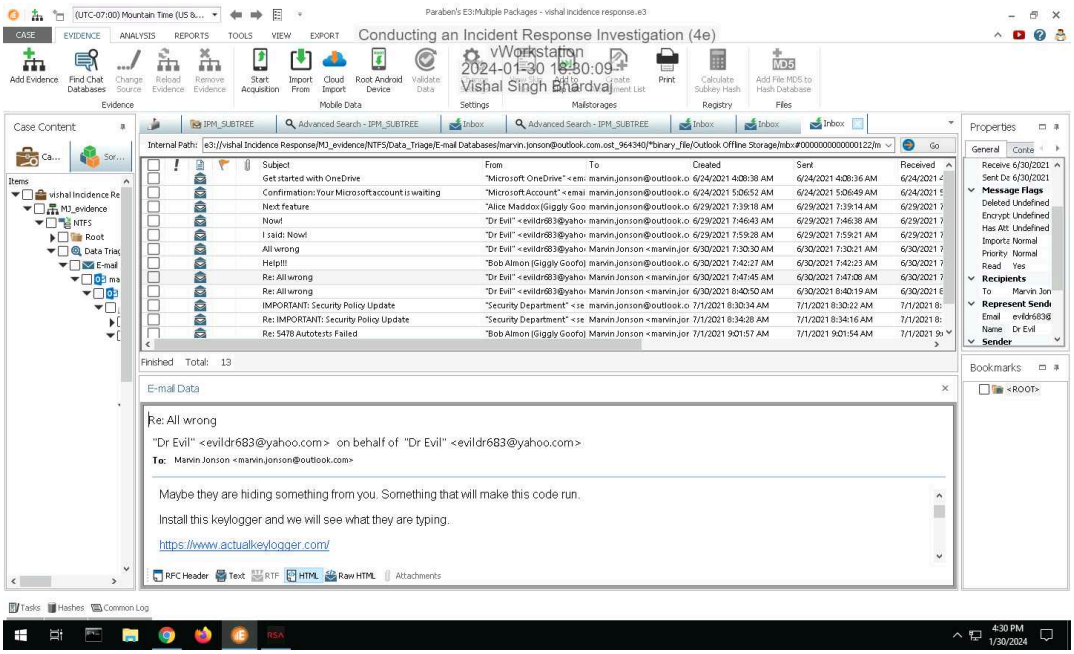
Define the following: Names and job titles of the affected users.

Names and job titles of the affected users.- Marvin Jonson, Project manager

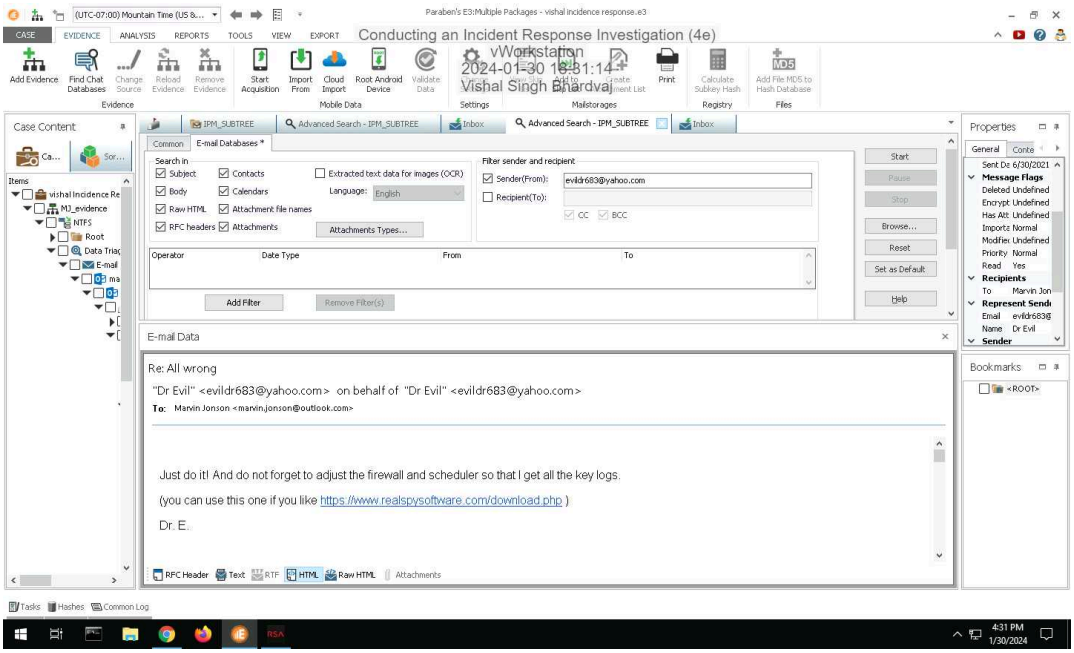
Section 2: Applied Learning

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

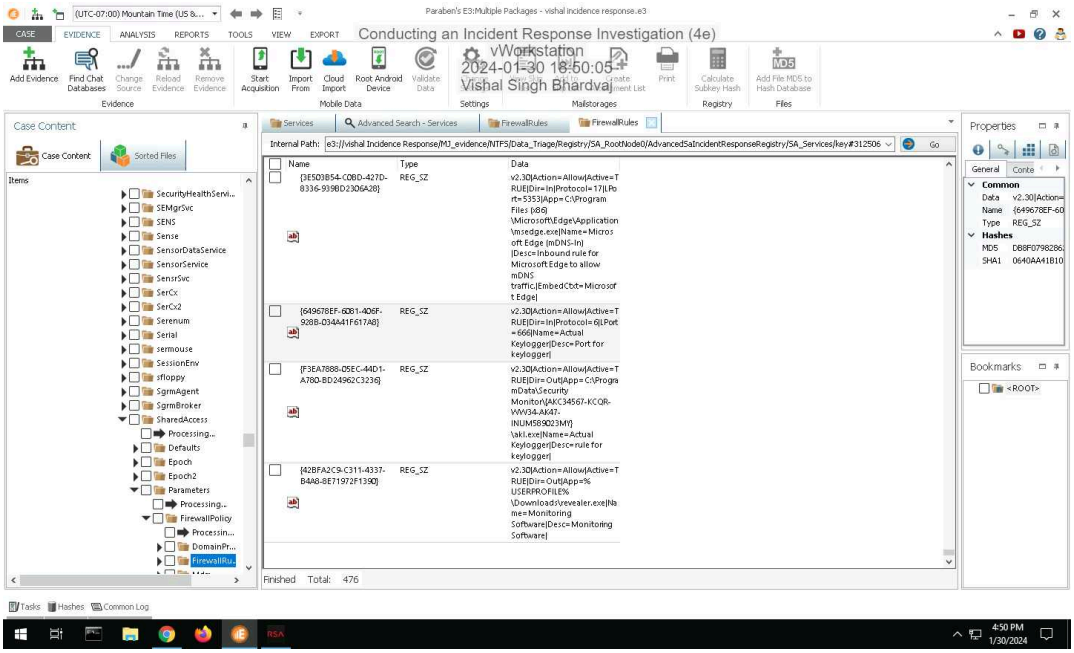
5. **Document** the Author and Date values associated with the scheduled keylogger task.

Author- Marvin Jonson
Date - 2021-06-30 (30th June 2021)

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

Port used for inbound connections to the keylogger - 666
name and location of the keylogger executable- C:\ProgramData\SecurityMonitor\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.

First Start Time - June 30,2021 9:10:20 PM
last Time Started - June 30,2021 9:10:22 PM

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

Activity type are 5,6 and 16. It means there are both interaction and opening of keylogger.

Part 3: Update an Incident Response Report

Date
Insert current date here.

01/30/2024

Name
Insert your name here.

Vishal Singh Bhardvaj

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

It is unchanged.

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

Incident type also includes Compromised System as key logger was installed along with Compromised User Credential as in the first response.

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

Incident occurrence time prepones to keylogger use timing. It is now June 30,2021 at 9:10:20 PM

Incident Scope

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

More then one user was affected as key logger was installed to a system as well. So scope changed.

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.

Keylogger was installed on a system. It increased number of affected systems.

Users Affected by the Incident

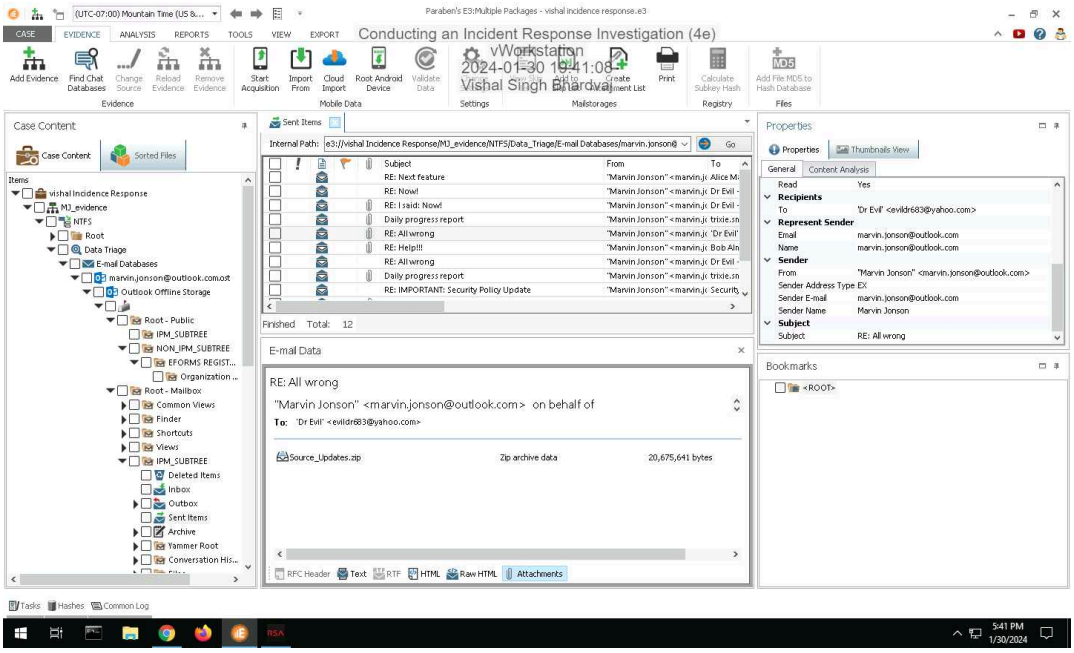
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Initially only Marvin was the affected user but since keylogger was installed on to a system it is evident that other users were also affected.

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**.