Student:	Email:
Jake Simpson	jaksimps@iu.edu

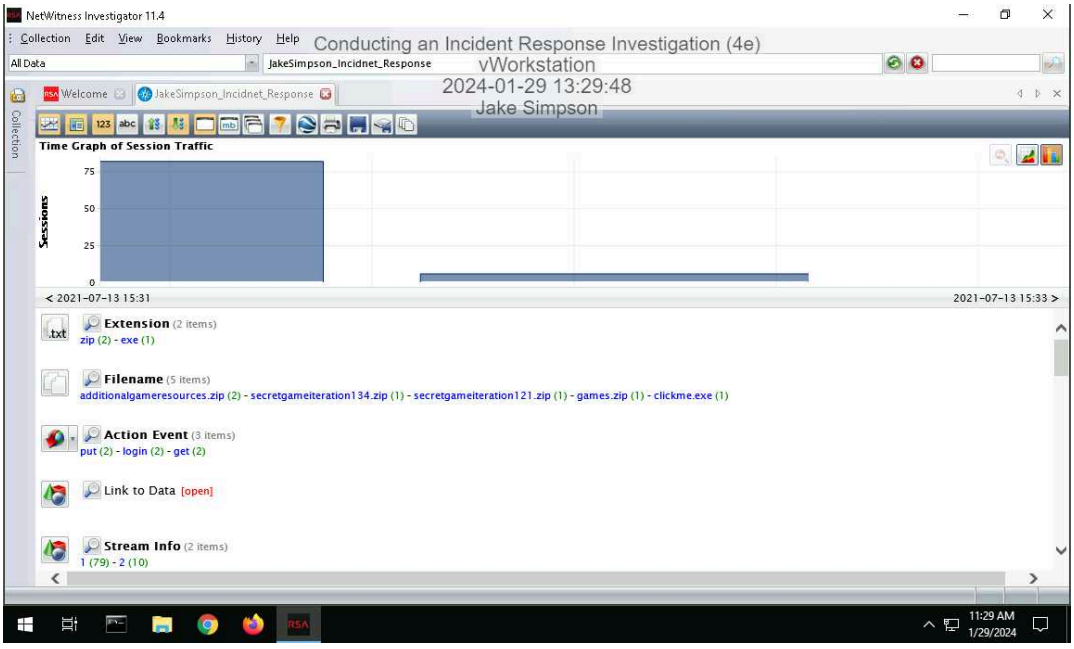
Time on Task:	Progress:
1 hour, 21 minutes	100%

Report Generated: Monday, January 29, 2024 at 2:47 PM

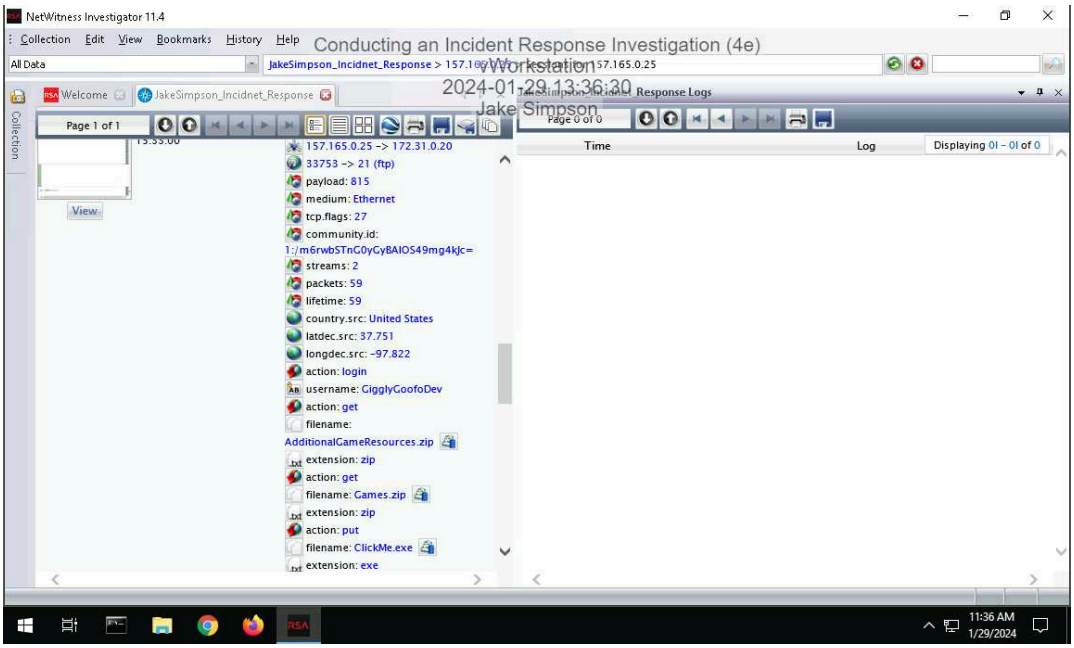
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

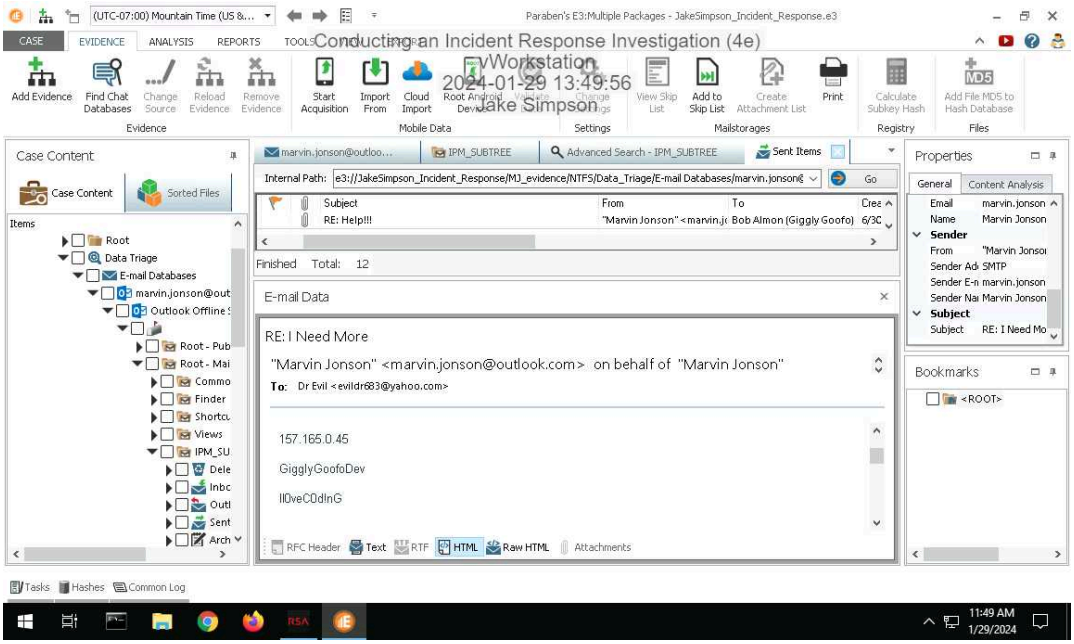


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

01/29/2024

Name
Insert your name here.

Jake Simpson

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.

Exfiltration

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 2021-Jul-13 15:33
Incident discovered 2021-Jul-31 10:30

Incident reported 2021-Jul-31 10:50

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.

1 system affected, 1 user affected
Parties involved: Marvin Johnson, Mr. Evil

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).

157.165.0.25 -> 172.32.9.20 FTP port 21

Users Affected by the Incident

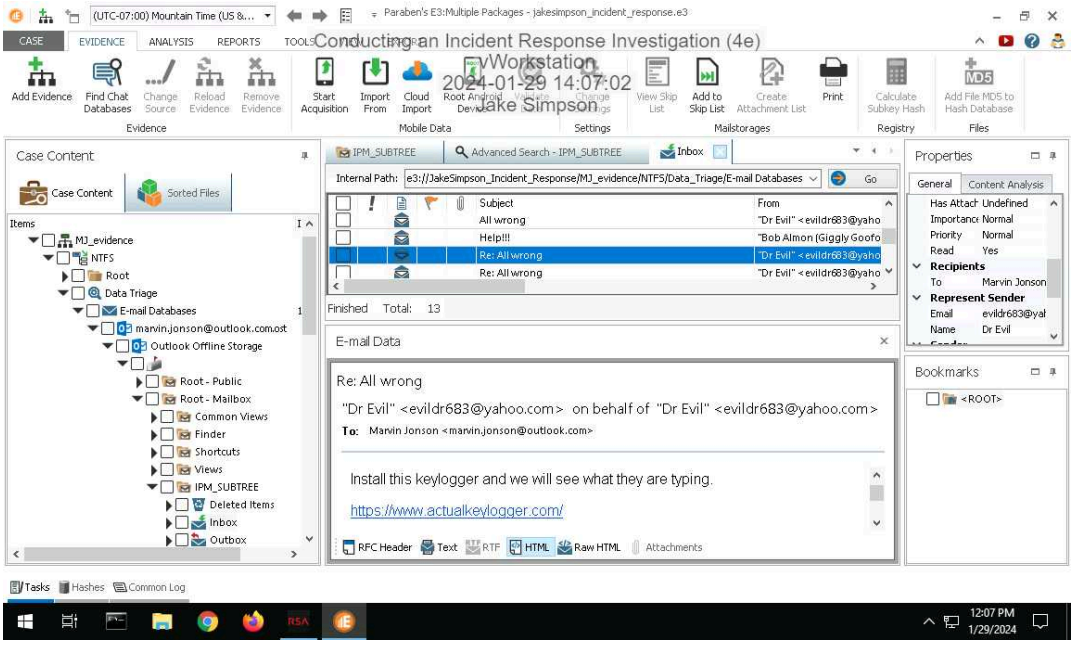
Define the following: Names and job titles of the affected users.

Giggly Goofo

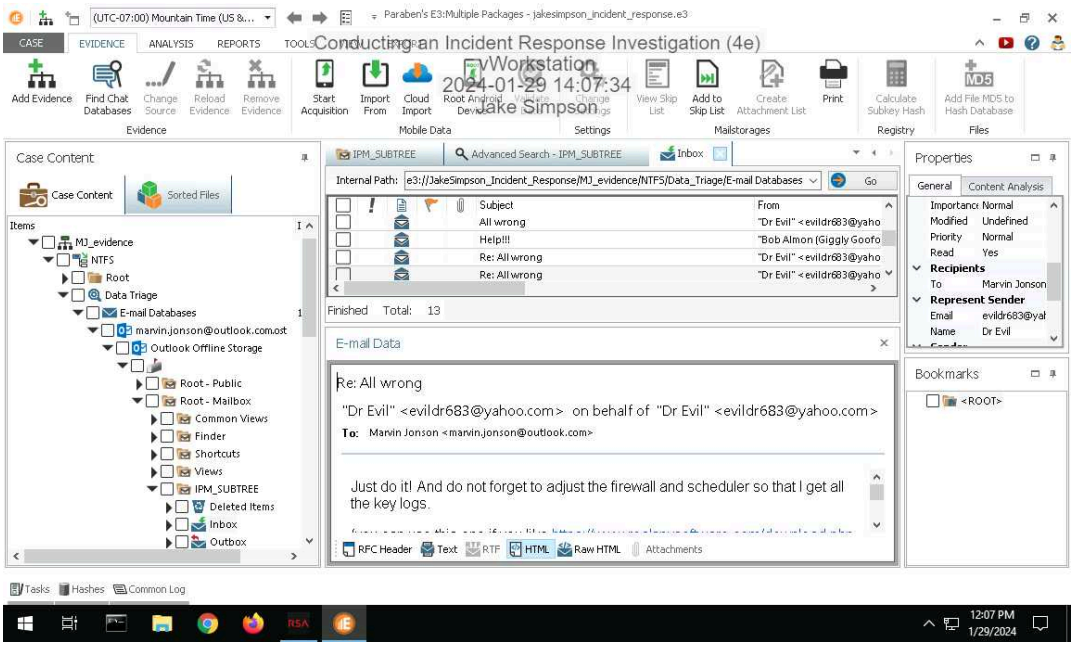
Section 2: Applied Learning

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

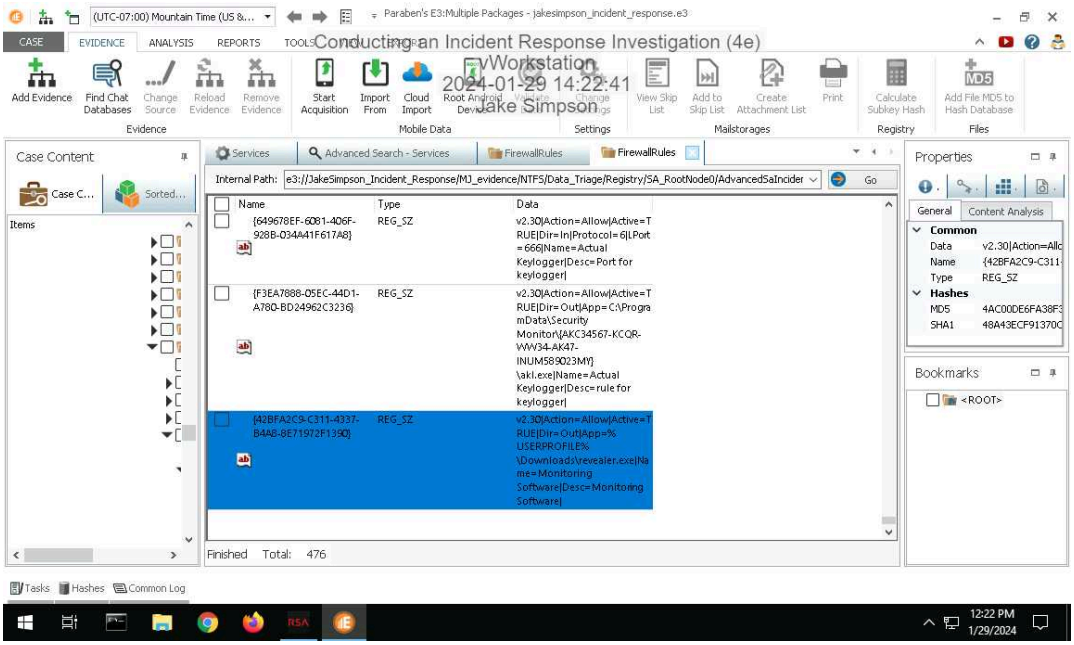
5. **Document** the Author and Date values associated with the scheduled keylogger task.

Author: DESKTOP-CGRK7LT\Marvin Johnson
Date: 2021-06-3OT14:16:23.27O5256

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

Port: 666
Location: C:\ProgramsData\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.

Start date is Wednesday, June 30, 2021 08:58:42 PM GMT
Last date is Friday, July 30, 2021 08:58:42 PM GMT

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

Since there is a 5 he only opened it

Part 3: Update an Incident Response Report

Date
Insert current date here.

01/29/2024

Name
Insert your name here.

Jake Simpson

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.

New Incident - Keylogger

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

Time Line change - June 30, 2021 - July 30, 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.

Marvin's PC

Users Affected by the Incident

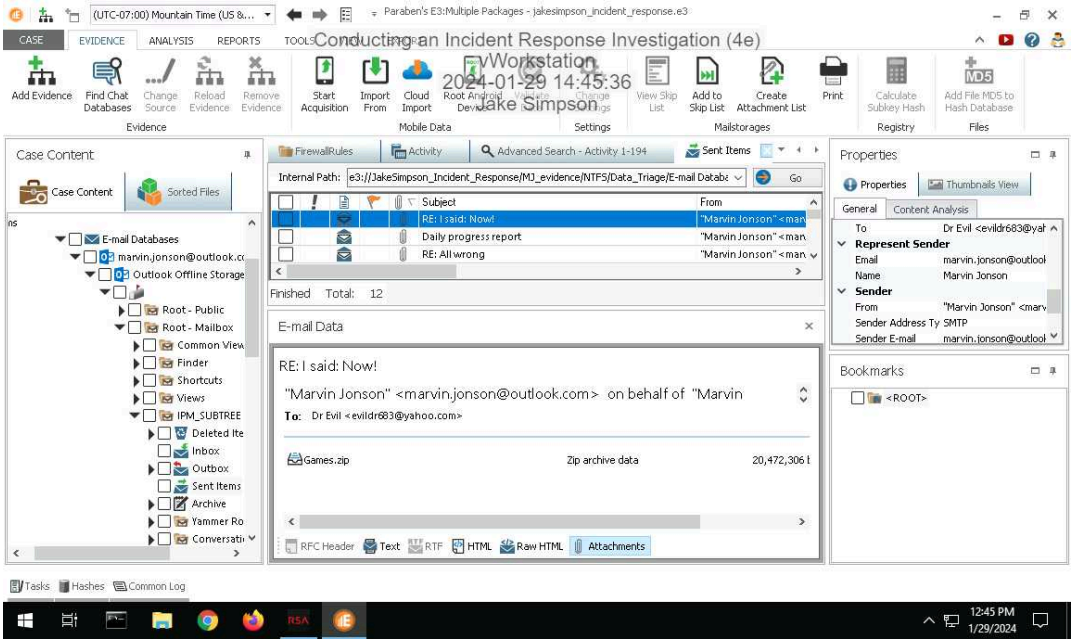
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

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**.