Student:	Email:
Jordan Calvert	jordanryancalvert@gmail.com

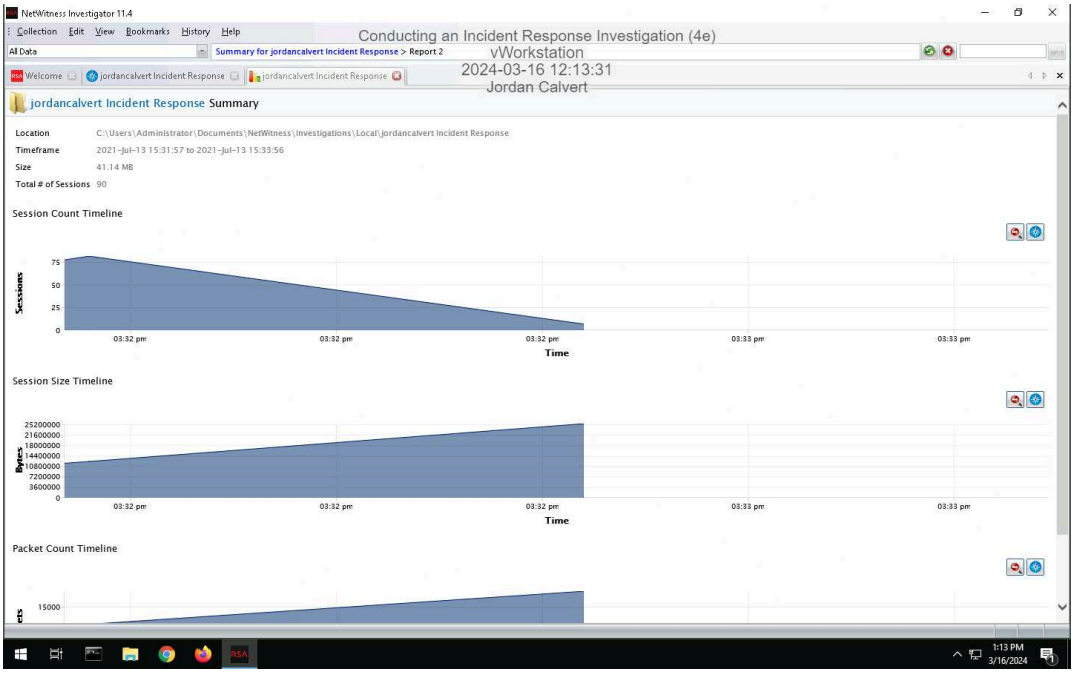
Time on Task:	Progress:
5 hours, 18 minutes	100%

Report Generated: Wednesday, May 15, 2024 at 10:44 AM

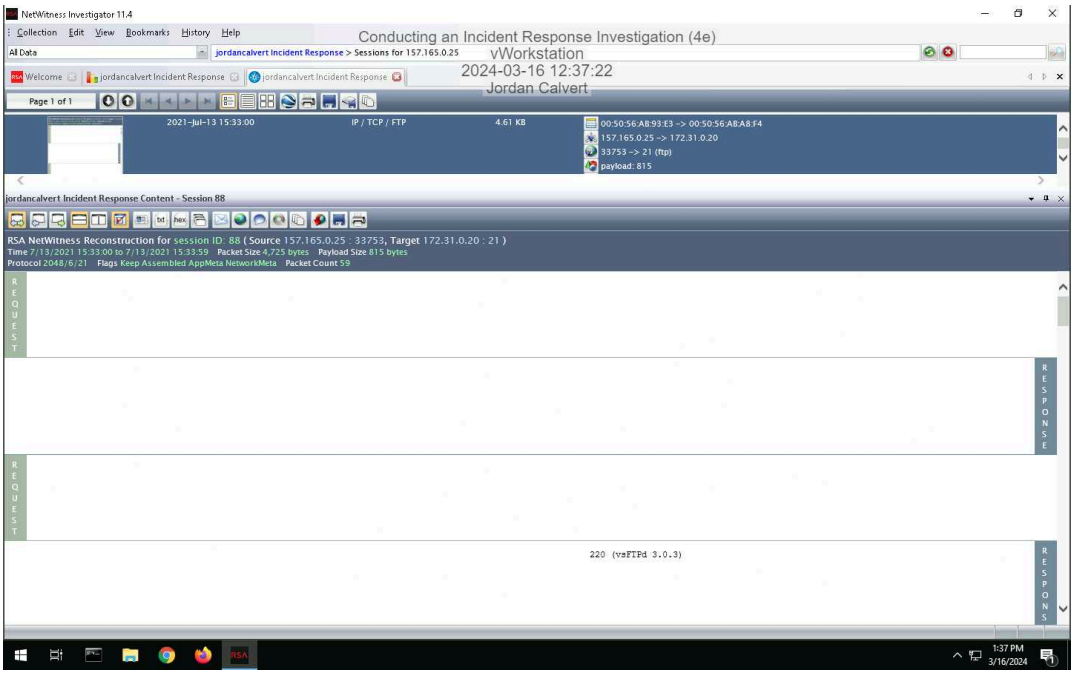
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

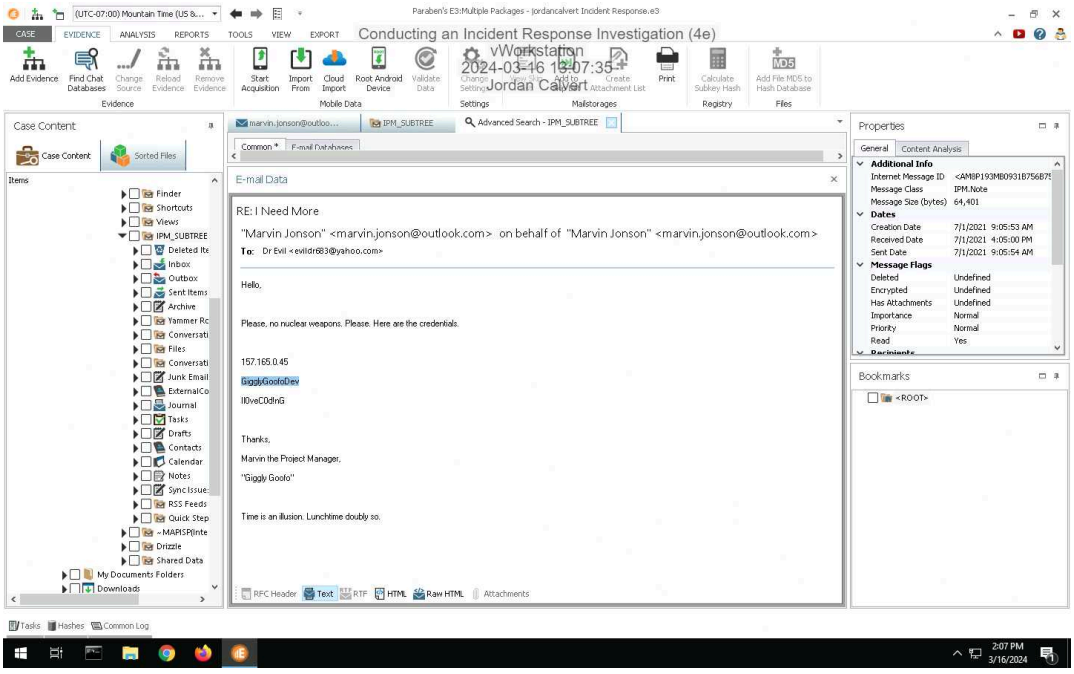


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

3/16/24

Name
Insert your name here.

Jordan Calvert

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

Incident is defined as High Priority.

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.

Incident Type can be labeled as the following: Compromised User Credentials, Policy Violation.

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: 3/16/24Date and time when the incident was reported: 3/16/24Date and time when the incident occurred: 7/13/21

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: 1Estimated quantity of users affected: 20

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).

The following systems affected by the incident are as follows: 157.165.0.25 and 172.31.0.20

Users Affected by the Incident

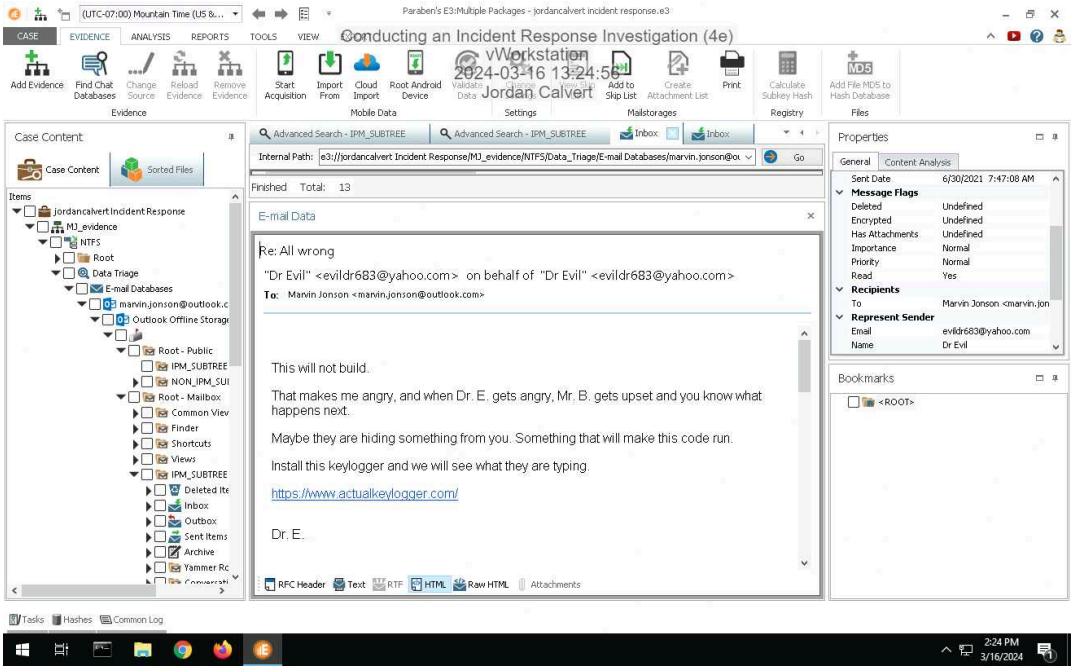
Define the following: Names and job titles of the affected users.

Marvin Johnson and Dr. Evil

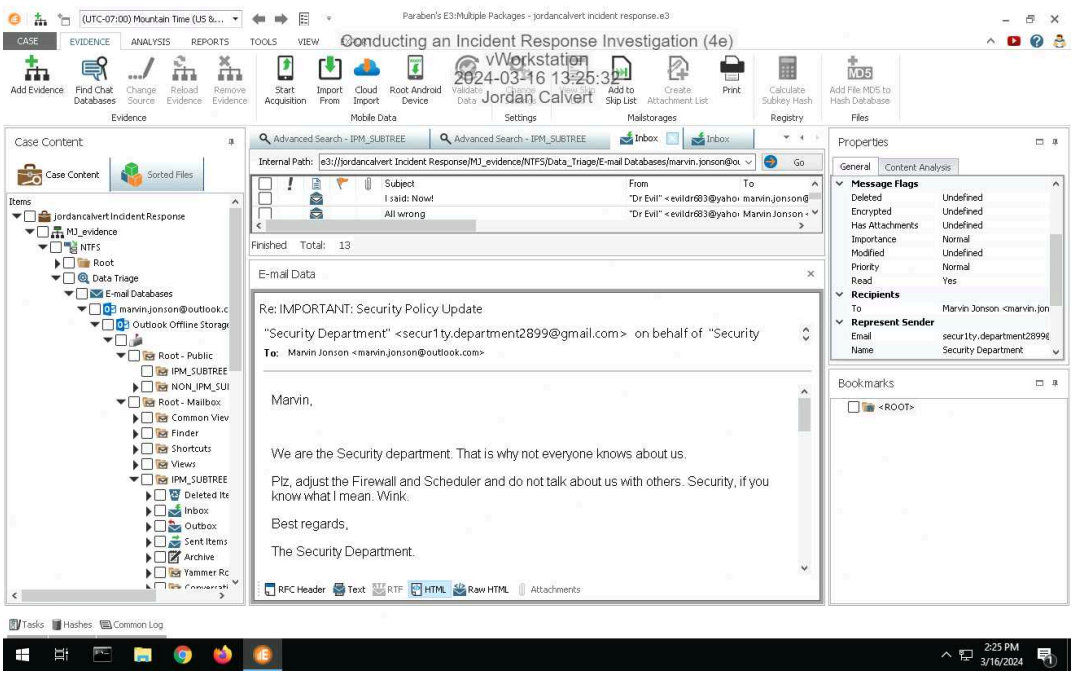
Section 2: Applied Learning

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

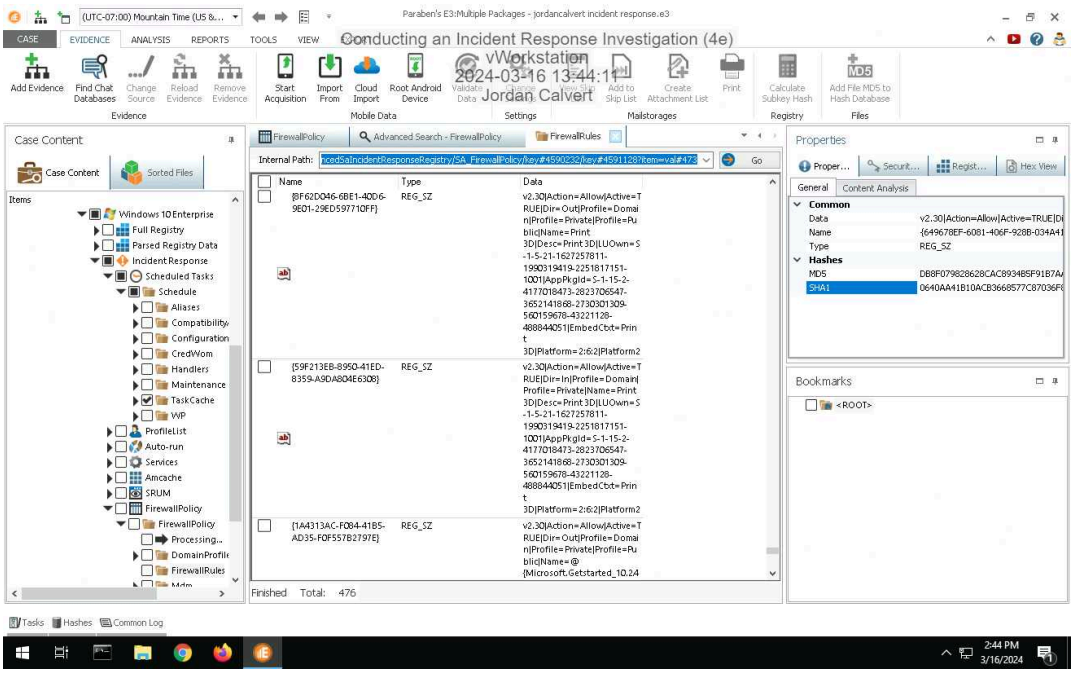
5. **Document** the Author and Date values associated with the scheduled keylogger task.

Author is Marvin Johnson. Date is 2021-06-30

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

Port 666

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.

10:00 A.M

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

Marvin interacted with the keylogger

Part 3: Update an Incident Response Report

Date
Insert current date here.

03/16/24

Name
Insert your name here.

Jordan Calvert

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

The incident remains High Priority.

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 remains 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.

Incident timeline has remained unchanged.

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

Incident scope has remained 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.

List of systems remains unchanged.

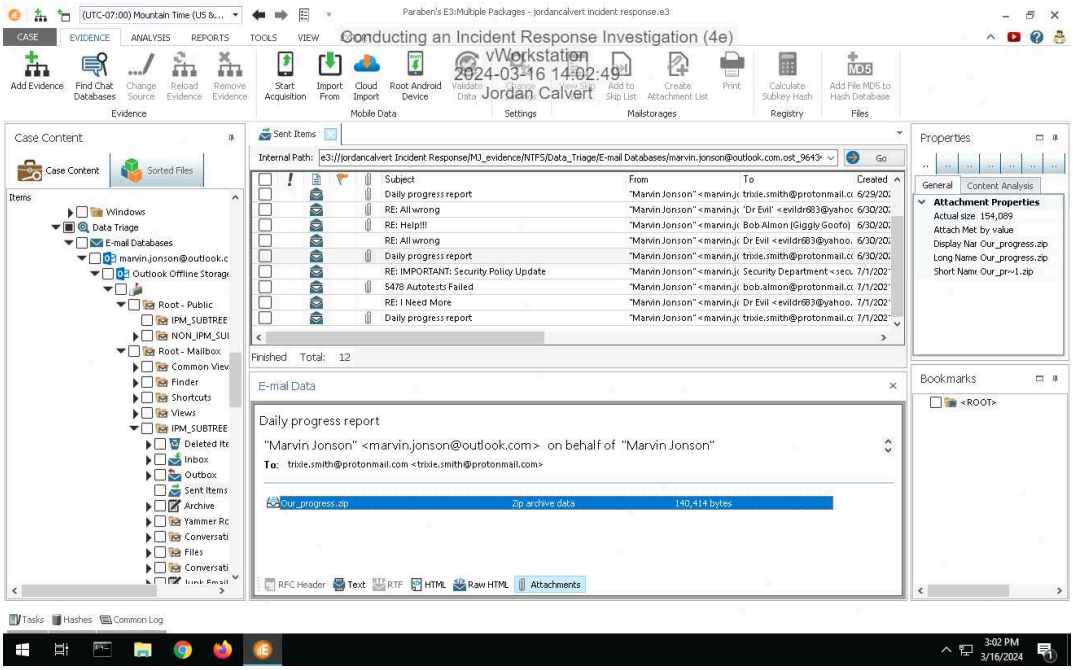
Users Affected by the Incident
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

List of affected users has not changed.

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**.