Student:	Email:
Samman Chouhan	schouhan1@hawk.iit.edu

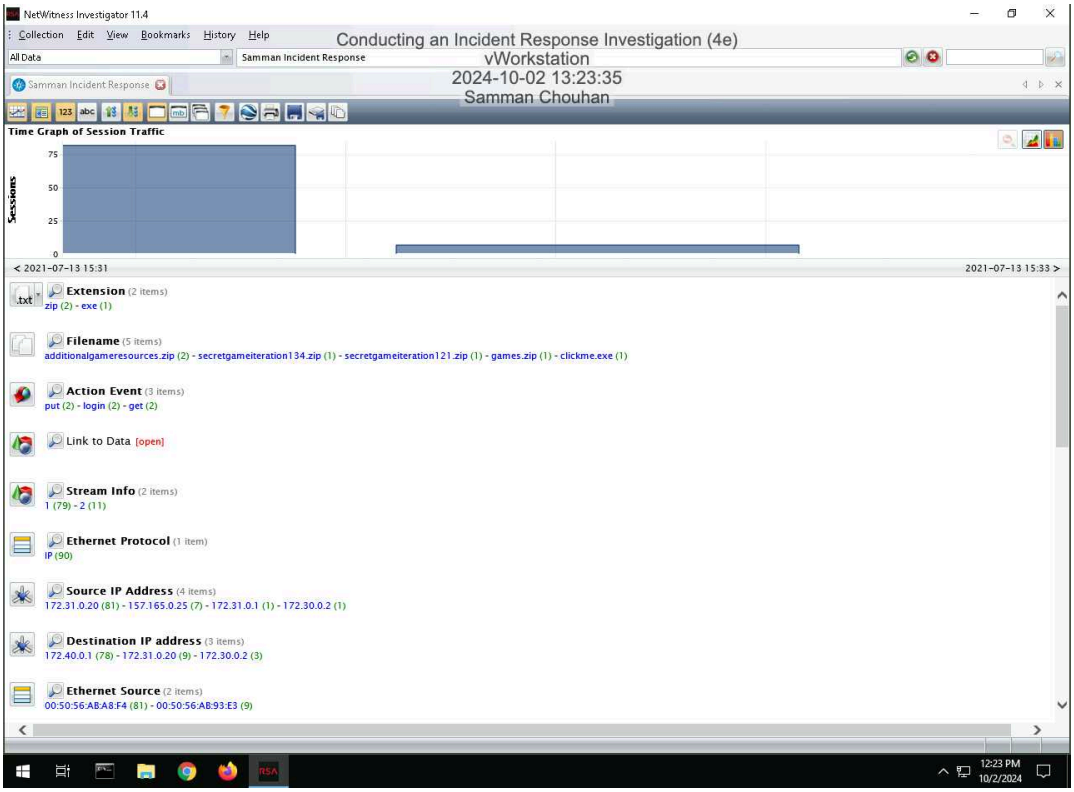
Time on Task:	Progress:
6 hours, 37 minutes	100%

Report Generated: Sunday, October 6, 2024 at 5:40 PM

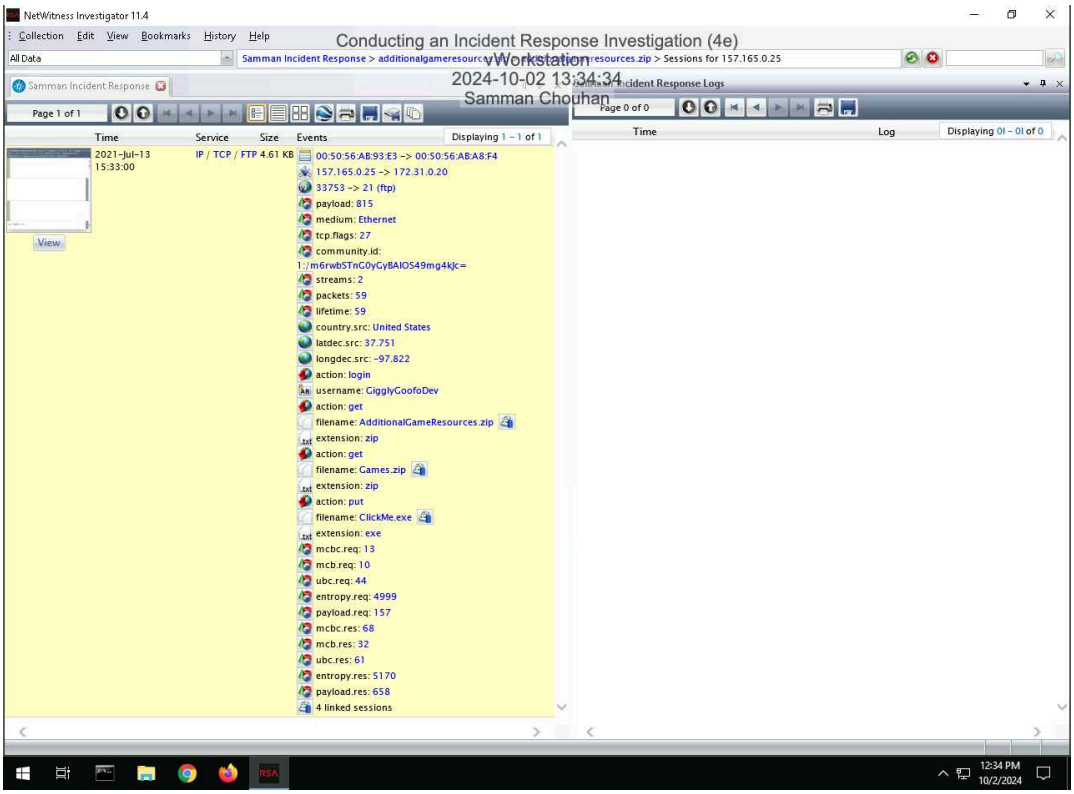
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

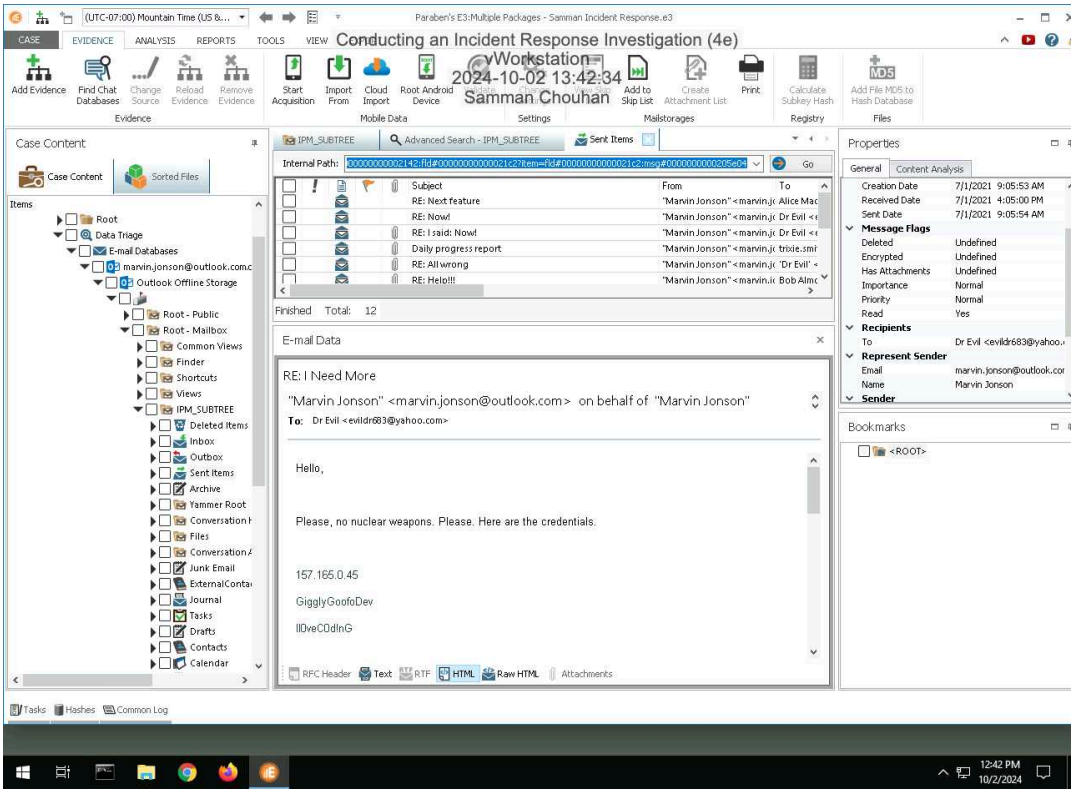


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

10/02/2024

Name
Insert your name here.

Samman Chouhan

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

The priority for this incident will be considered high as the credentials can be seen

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.

The incident type would be compromised user credentials, since data breach has occurred, both internal and external actors , wherein copies of confidential files were exfiltrated from corporate network

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 security incident was discovered on July 31 , 2021 at 10:30 AM eastern time , the same said incident was reported about 10 minutes later i.e 10:40 AM eastern time

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 Internal system seems to be vulnerable and one user was affected

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 -157.165.0.25Attack destination - 172.31.0.20ip address of the affected system-157.165.0.45Primary Function - FTP server on port 21

Users Affected by the Incident

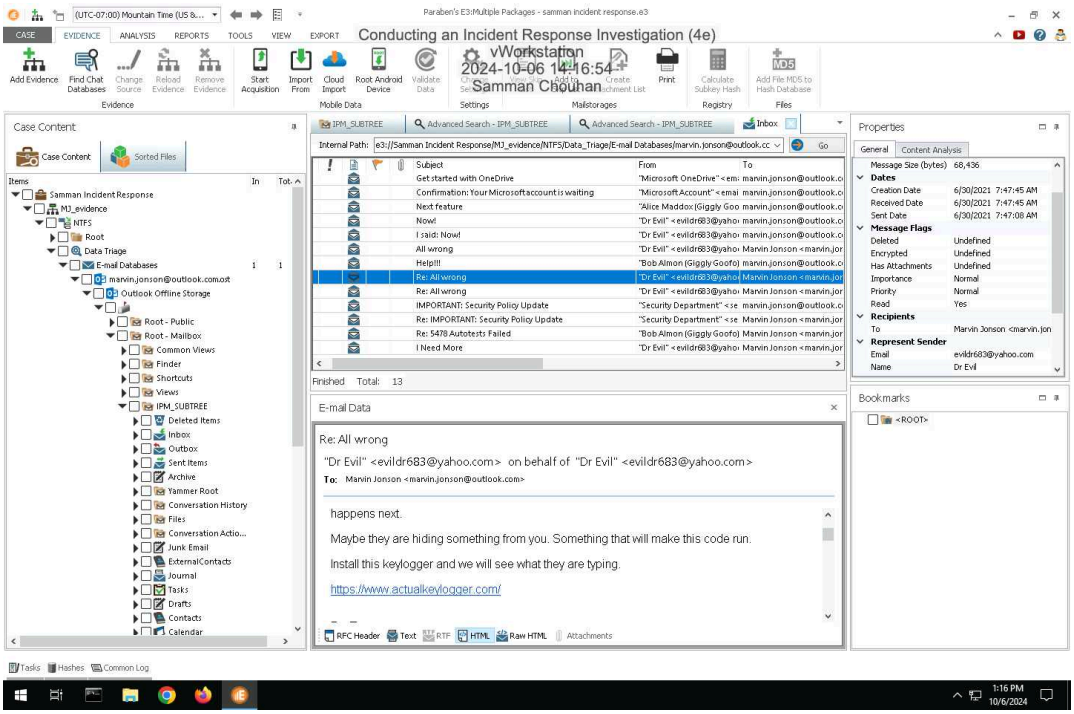
Define the following: Names and job titles of the affected users.

User - Giggly GoofoTitle - GigglyGoofoDev

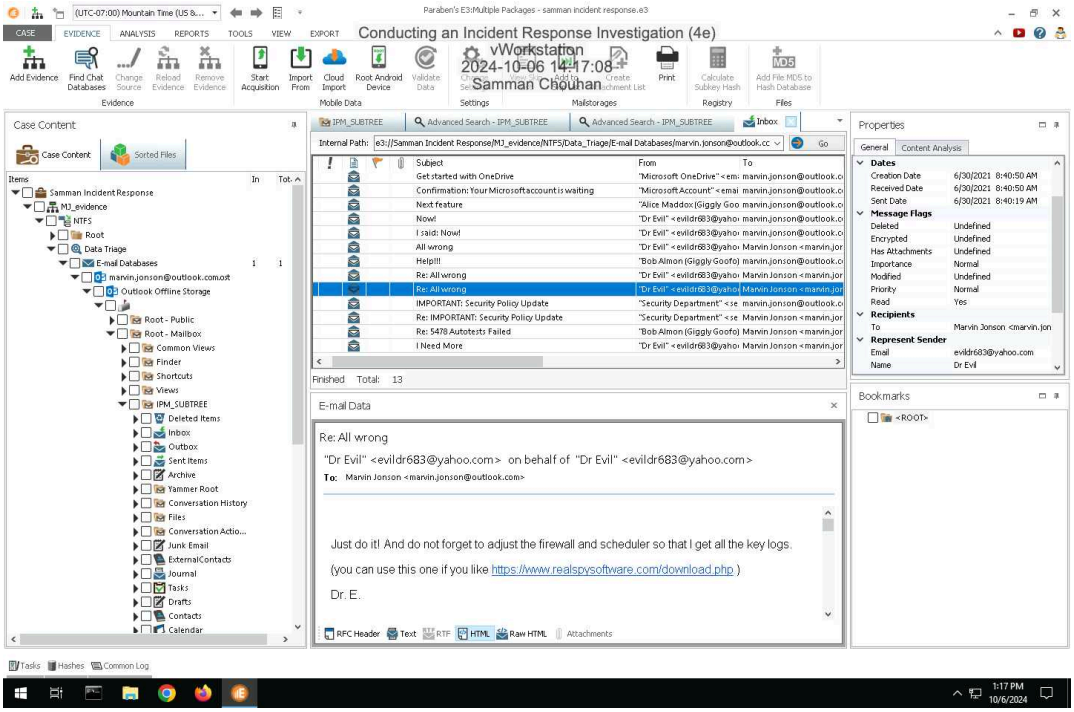
Section 2: Applied Learning

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

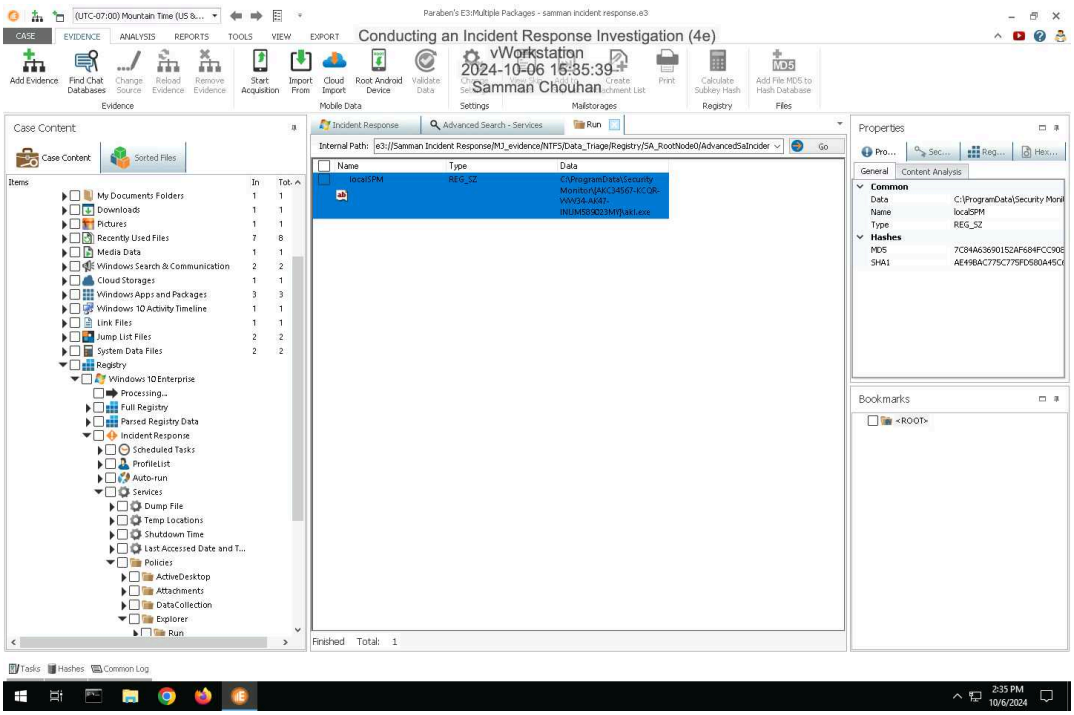
5. **Document** the Author and Date values associated with the scheduled keylogger task.

The Author seems to be :- DESKTOP-CGRK7LT\Marvin Jonson
Date - 2021-06-30 Time - 14:16:23

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

Listening Port - 666
Name - Actual Key Logger
Location- : 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.

First Start Time :- GMT ;Wednesday , June 30, 2021 8:58:42 PMLast Start Time :- GMT : Wednesday , June 30, 2021 9:10:20 PM

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

Since the value shows 6 , it means he interacted

Part 3: Update an Incident Response Report

Date
Insert current date here.

Sunday Oct 6 2024

Name
Insert your name here.

Samman Chouhan

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

Priority is still the same , unchanged

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

The incident type has been changed since the system has been compromised with the help of a 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.

yes the incident timeline has been changed ,since the starting of keylogger
time being :- First Start Time :- GMT ;Wednesday , June 30, 2021 8:58:42 PM

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

yes the incident scope has been changed , marvin is voluntarily helping Dr Evil

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.

the system affected was the one for marvin , when he installed the keylogger and started it on june 30th

Users Affected by the Incident

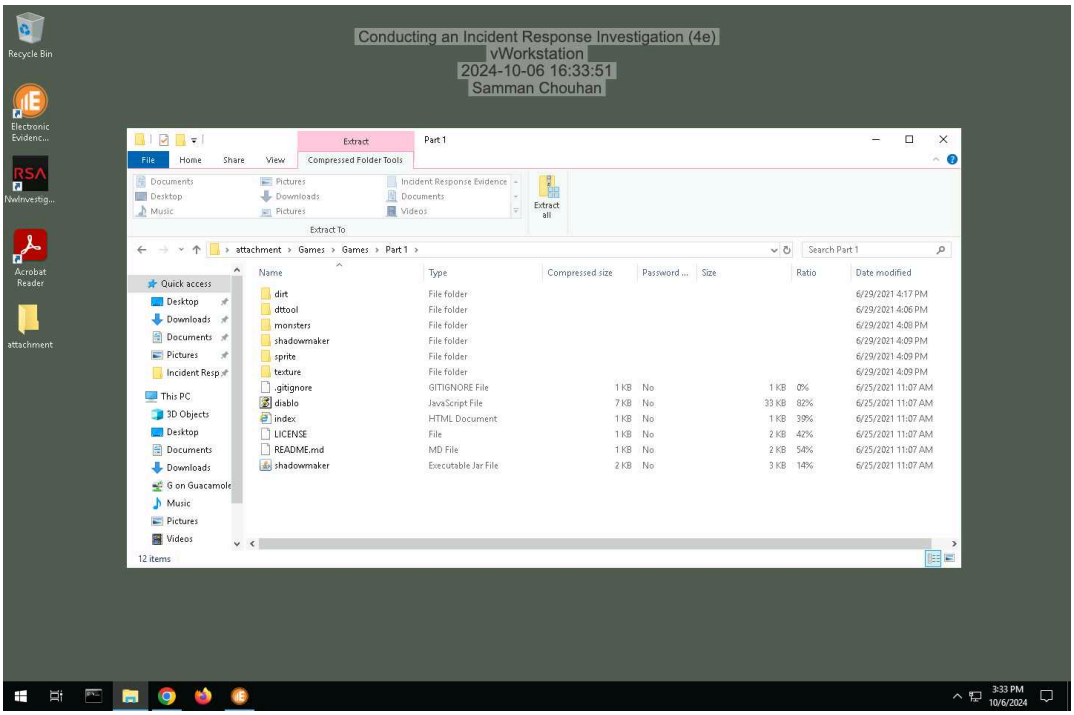
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

no the users affected will still be unchanged , marvin is still the only compromised one , the only change was the change from leaked credentials to keyloggers

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**.



As per the mail found between marvin and dr evil with the thread " i said now!!" where dr evil is requesting source code for their super secret game , here is attached file that was exported

Part 2: Identify Additional Evidence of Spyware

Make a screen capture showing the **email with instructions for installing additional spyware**.