Student:	Email:
Matias Kun	rvh4zx@virginia.edu

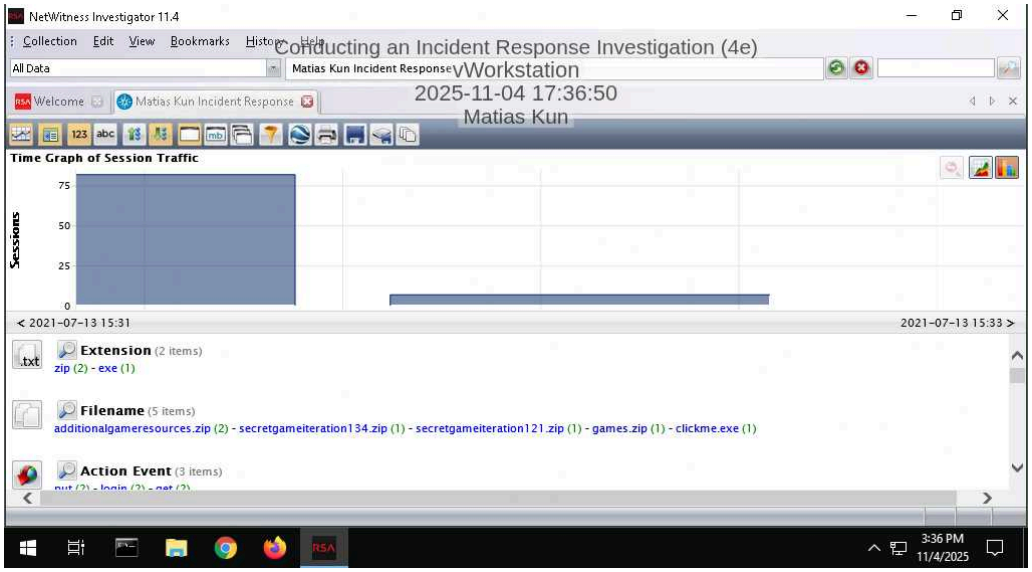
Time on Task:	Progress:
28 hours, 0 minutes	100%

Report Generated: Friday, November 7, 2025 at 12:51 AM

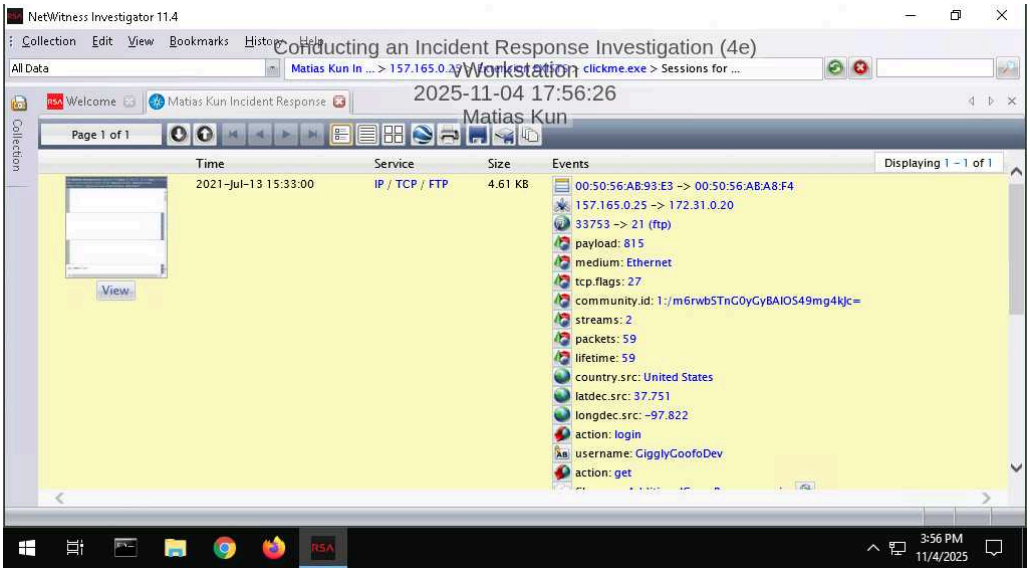
Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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

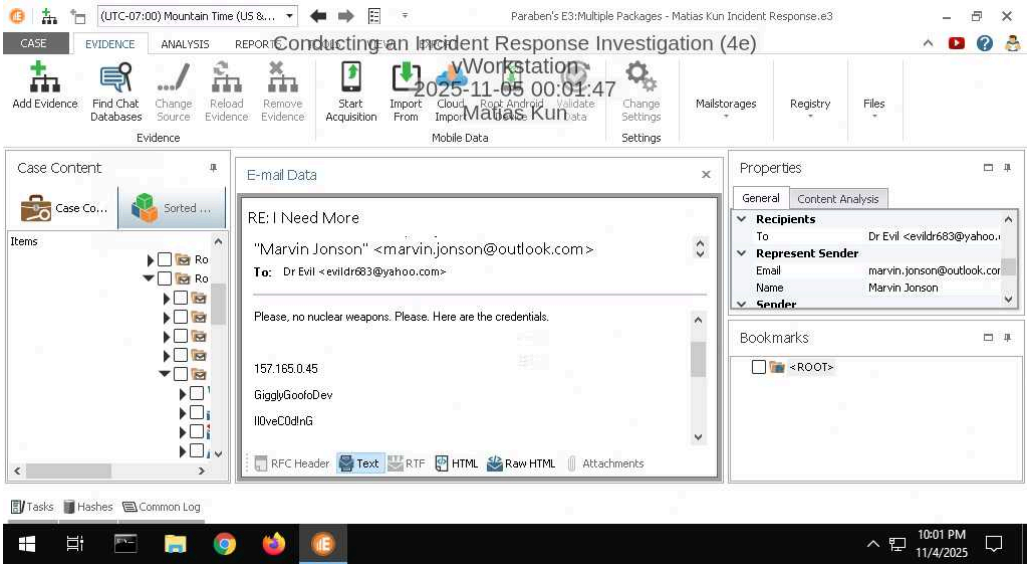


16. **Make a screen capture** showing the **details of the 2021-Jul-13 15:33:00 session**.



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.

November 4

Name
Insert your name here.

Matias Kun

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

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.

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 took place on July 13, 2021 between 3:31 PM and 3:33 PM. The incident was discovered on July 31, 2021 at approximately 10:30 AM and reported 10 minutes later.

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.

Infected systems include network locations and the credentials of the staff from Giggly Goofo. Third parties may include the email vendor and the Giggly Goofo game studio. The number of users affected is unknown, other than the employee that intercepted the email at Giggly Goofo and Dr. Evil, the individual who wrote the initial email.

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 include IP address 157.166.0.45 (source IP), and the credentials of GigglyGoofoDev and IIOveCOdlnG from the staff at Giggly Goofo. The attack destinations are likely the servers between Giggly Goofo, one of the threat actors (Dr. Evil), and the hacker who sent ransomware via email.

Users Affected by the Incident

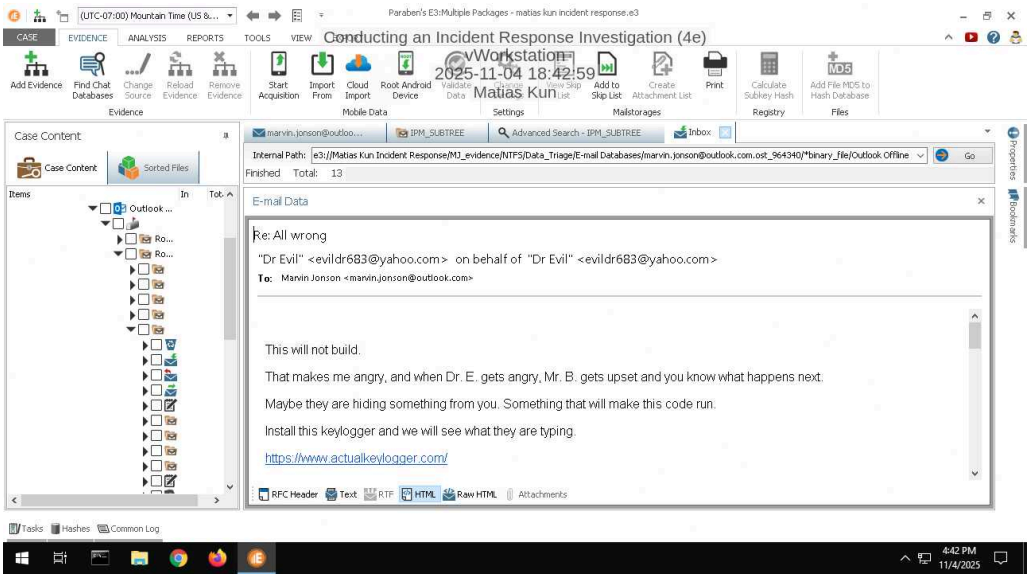
Define the following: Names and job titles of the affected users.

Marvin Jonson (Project Manager) is the only known user provided the email from the image of Giggly Goofo staff members.

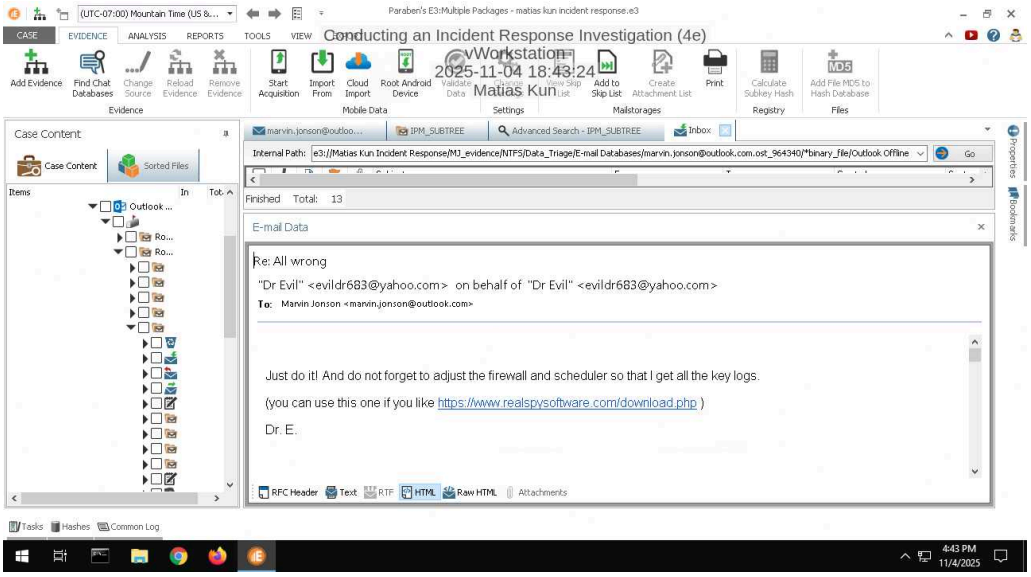
Section 2: Applied Learning

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

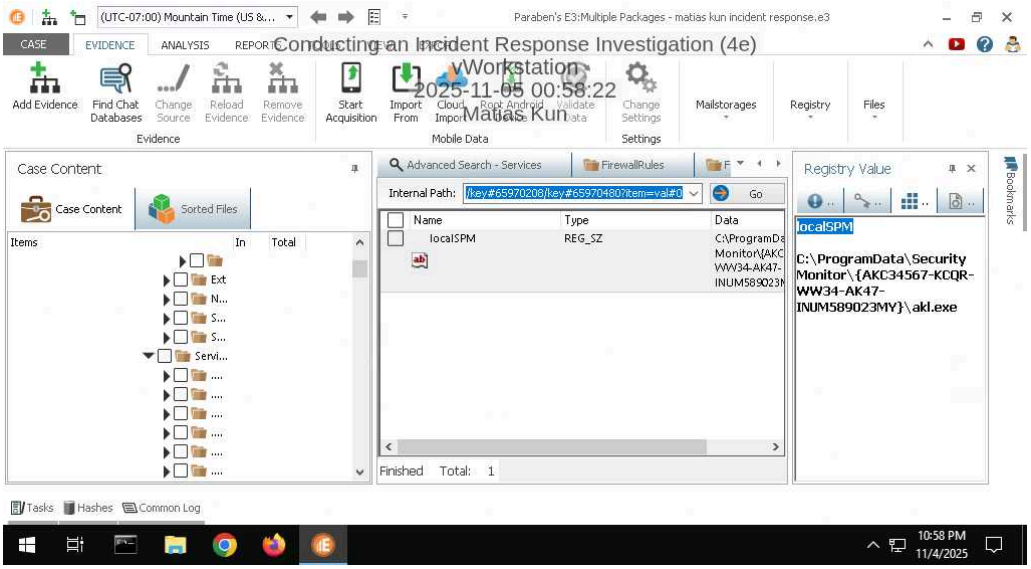
5. **Document** the Author and Date values associated with the scheduled keylogger task.

The author value associated with the scheduled keylogger task was Marvin Jonson. The date value associated with the task was 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 number = 666. Location: C:\ProgramData\SecurityMonitor\{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 first time the keylogger was started was Thursday June 24, 2021 at 2:58:35 GMT. The last start time for the keylogger is Thursday, July 1, 2021 10:25:45 PM GMT

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

Marvin has interacted with the keylogger.

Part 3: Update an Incident Response Report

Date
Insert current date here.

November 5, 2025

Name
Insert your name here.

Matias Kun

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

Priority status 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.

Compromised System and Malware. Malware installed was 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.

Interaction started with a keylogger gathering information from the company computer prior to the actual incident. Keylogger usage began on Thursday, June 24, 2021 2:58:35 PM GMT. This event happened prior to the FTP Incident.

Incident Scope

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

One user has been affected. One system has been affected.

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.

Affected System: Workstation
New Information:Attack Source: KeyloggerAttack Destination: Firewall and Scheduled Task Manager

Users Affected by the Incident

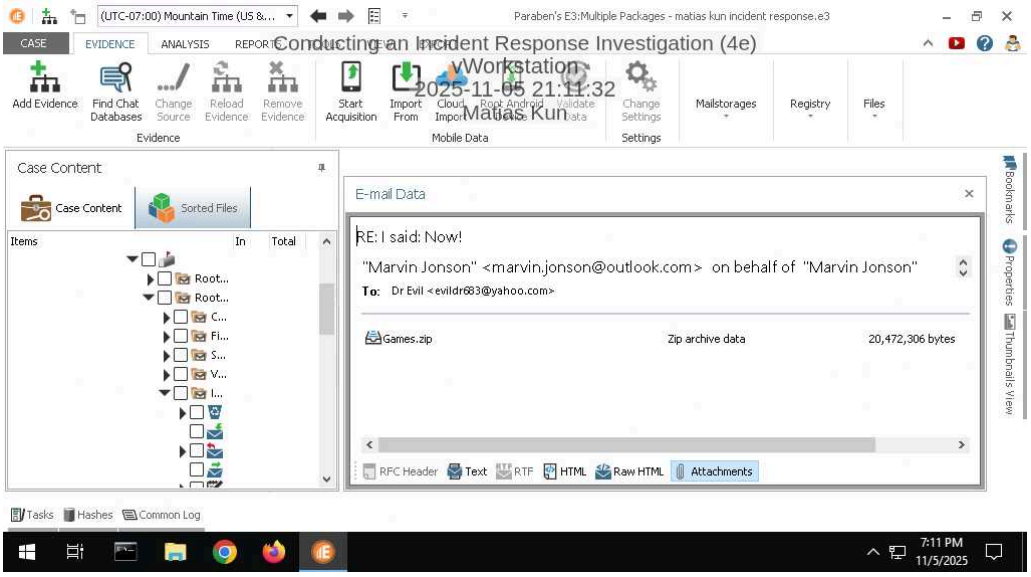
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

List of users affected were 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**.