Student:	Email:
Alexis Cherpes	cherpea@ferris.edu

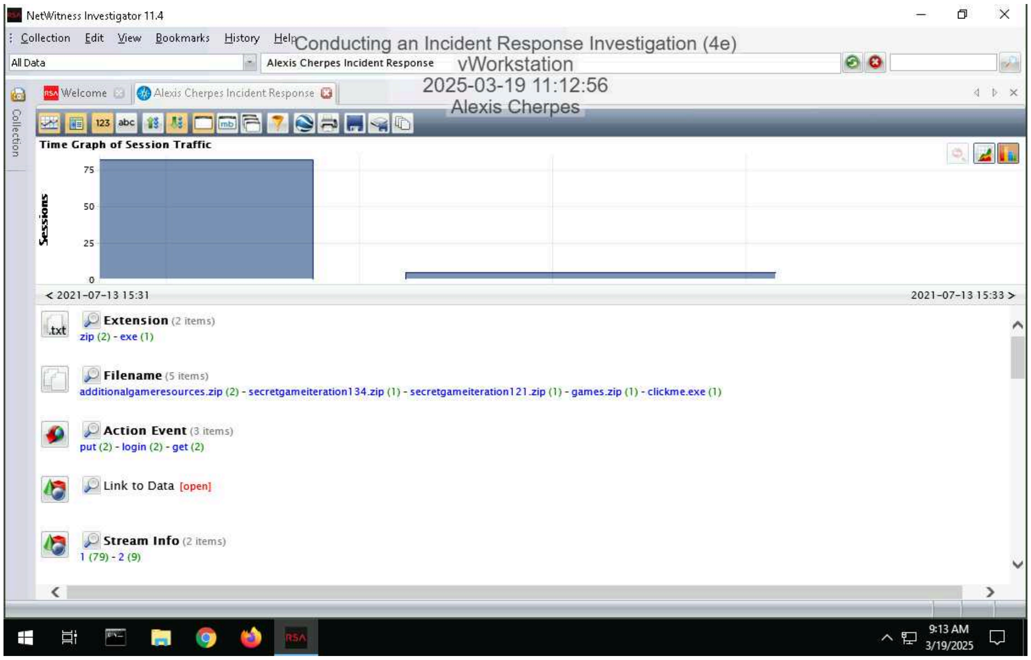
Time on Task:	Progress:
3 hours, 57 minutes	100%

Report Generated: Thursday, May 22, 2025 at 4:48 PM

Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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



Conducting an Incident Response Investigation (4e)
vWorkstation
2025-03-19 11:12:56
Alexis Cherpes

Extension (2 items)
zip (2) - exe (1)

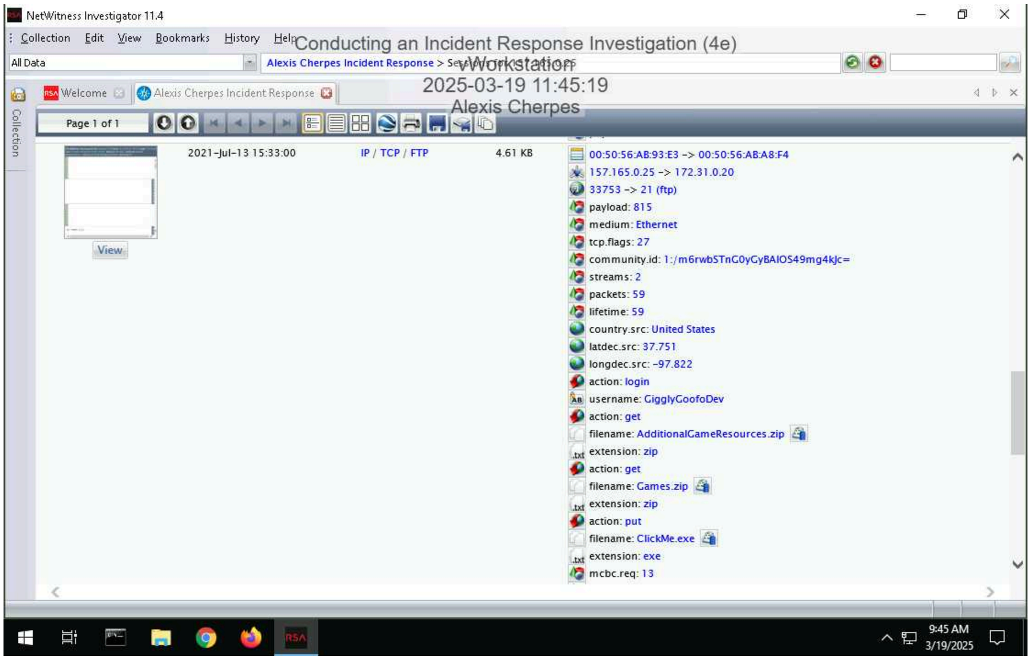
Filename (5 items)
additionalgameresources.zip (2) - secretgameiteration134.zip (1) - secretgameiteration121.zip (1) - games.zip (1) - clickme.exe (1)

Action Event (3 items)
put (2) - login (2) - get (2)

Link to Data [open]

Stream Info (2 items)
1 (79) - 2 (9)

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

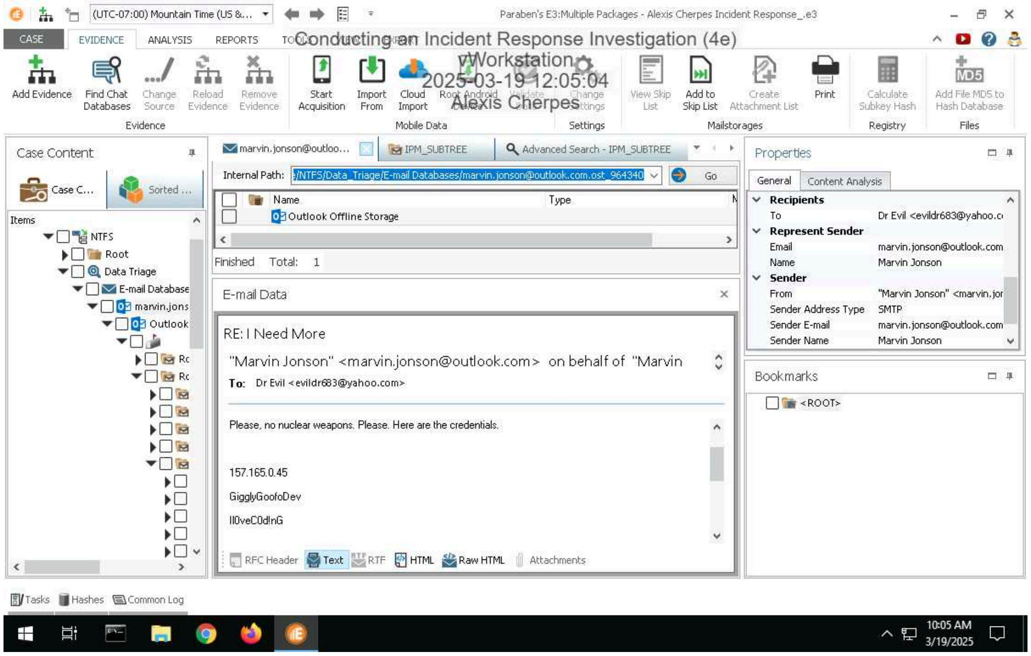

NetWitness Investigator 11.4
Collection
Edit
View
Bookmarks
History
Help
All Data
Alexis Cherpes Incident Response >
Welcome
Alexis Cherpes Incident Response
Page 1 of 1
View
Conducting an Incident Response Investigation (4e)
vWorkstation
2025-03-19 11:45:19
Alexis Cherpes
9:45 AM
3/19/2025

2021-Jul-13 15:33:00 IP / TCP / FTP 4.61 KB

00:50:56:AB:93:E3 -> 00:50:56:AB:A8:F4
157.165.0.25 -> 172.31.0.20
33753 -> 21 (ftp)
payload: 815
medium: Ethernet
tcp.flags: 27
community.id: 1:/m6rwbSTnG0yGyBAIOS49mg4kJc=
streams: 2
packets: 59
lifetime: 59
country.src: United States
latdec.src: 37.751
longdec.src: -97.822
action: login
username: GigglyGoofoDev
action: get
filename: AdditionalGameResources.zip
extension: zip
action: get
filename: Games.zip
extension: zip
action: put
filename: ClickMe.exe
extension: exe
mcbc.req: 13

Part 2: Analyze a Disk Image for Forensic Evidence

18. **Make a screen capture** showing the **email containing FTP credentials and the associated timestamps**.



Internal Path: /NTFS/Data_Triage/E-mail Databases/marvin.jonson@outlook.com.ost_964340

Name	Type
Outlook Offline Storage	

Finished Total: 1

E-mail Data

RE: I Need More

"Marvin Jonson" <marvin.jonson@outlook.com> on behalf of "Marvin
To: Dr Evil <evildr683@yahoo.com>

Please, no nuclear weapons. Please. Here are the credentials.

157.165.0.45

GigglyGoofoDev

Il0veC0d!nG

Recipients	
To	Dr Evil <evildr683@yahoo.c
Represent Sender	
Email	marvin.jonson@outlook.com
Name	Marvin Jonson
Sender	
From	"Marvin Jonson" <marvin.jor
Sender Address Type	SMTP
Sender E-mail	marvin.jonson@outlook.com
Sender Name	Marvin Jonson

Part 3: Prepare an Incident Response Report

Date

Insert current date here.

March 19th, 2025

Name

Insert your name here.

Alexis Cherpes

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.

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: July 31, 2021 at 10:30am. Date and time when the incident was reported: July 31, 2021 10:40am. Date and time when the incident occurred: started on July 13, 2021 at 3:31pm and ended on July 13, 2021 at 3:33pm.

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: 53. Estimated quantity of users affected, third parties involved or affected: 815

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: 157.165.0.25 Attack destinations: 172.40.0.1, 172.31.0.20, 172.30.0.2IP addresses of the affected systems: 157.165.0.45 Primary functions of the affected systems: FTP Server

Users Affected by the Incident

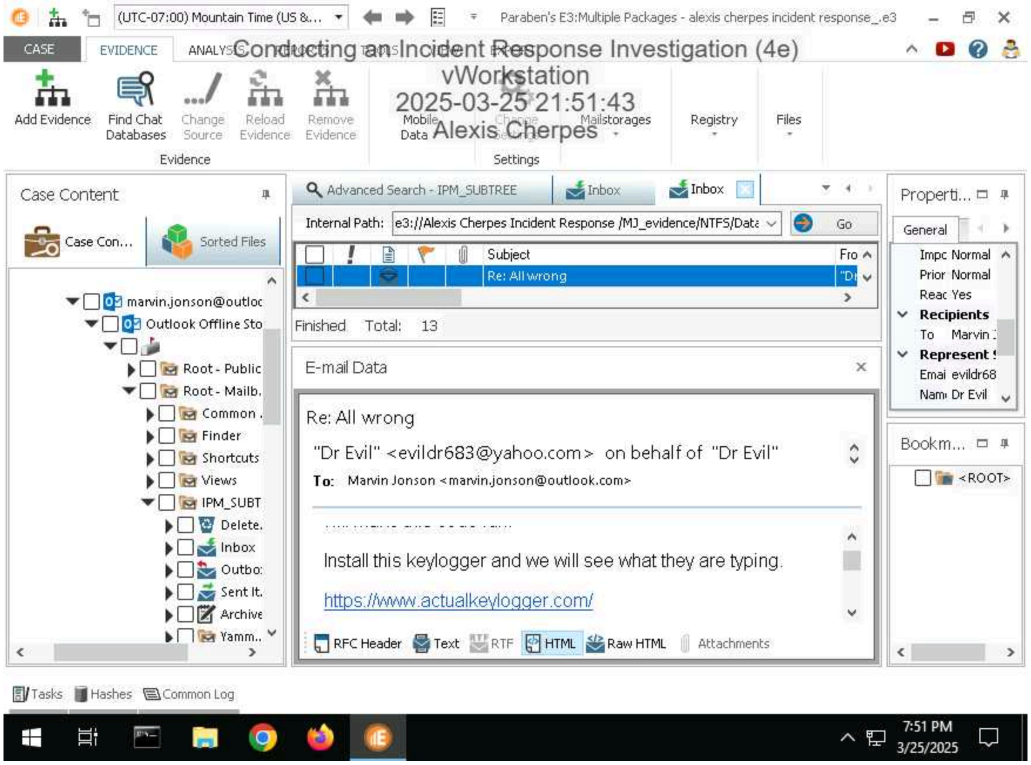
Define the following: Names and job titles of the affected users.

Name: Marvin Jonson Job Titles: 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**.



Conducting an Incident Response Investigation (4e)
vWorkstation
2025-03-25 21:51:43
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Incident Response /MJ_evidence/NTFS/Data

Finished Total: 13

Re: All wrong

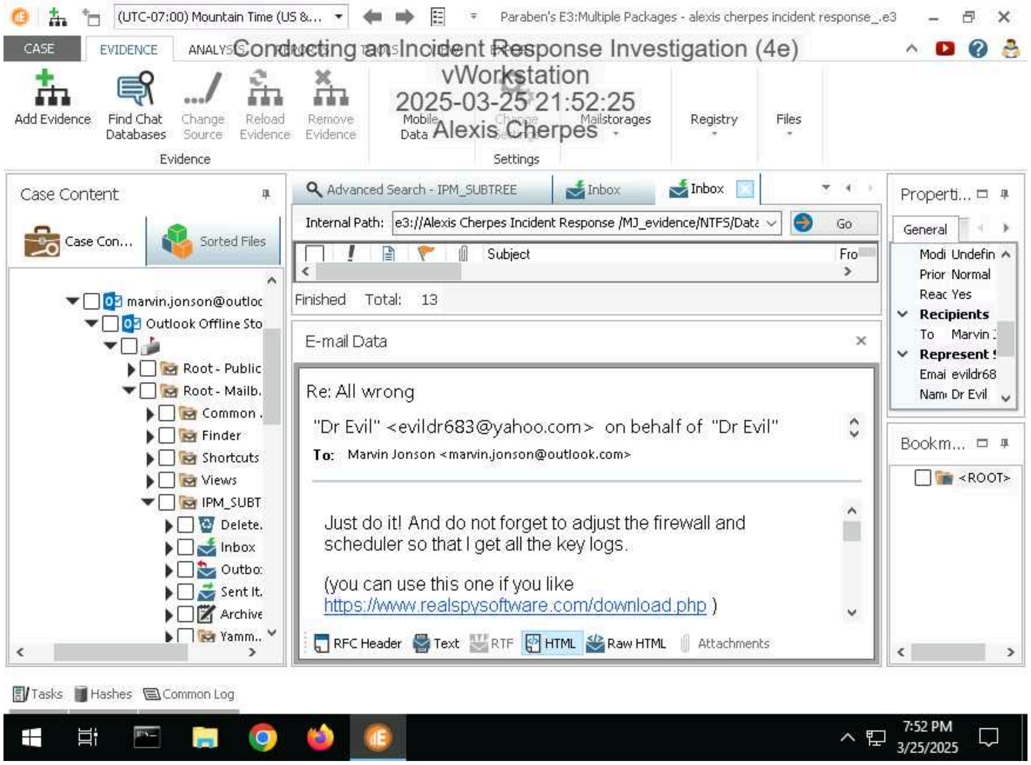
"Dr Evil" <evildr683@yahoo.com> on behalf of "Dr Evil"

To: Marvin Jonson <marvin.jonson@outlook.com>

Install this keylogger and we will see what they are typing.

https://www.actualkeylogger.com/

11. **Make a screen capture** showing the **email from Dr. Evil reminding Marvin to update the firewall and scheduler**.



Re: All wrong

"Dr Evil" <evildr683@yahoo.com> on behalf of "Dr Evil"

To: Marvin Jonson <marvin.jonson@outlook.com>

Just do it! And do not forget to adjust the firewall and scheduler so that I get all the key logs.

(you can use this one if you like https://www.realspysoftware.com/download.php)

Part 2: Identify Evidence of Spyware

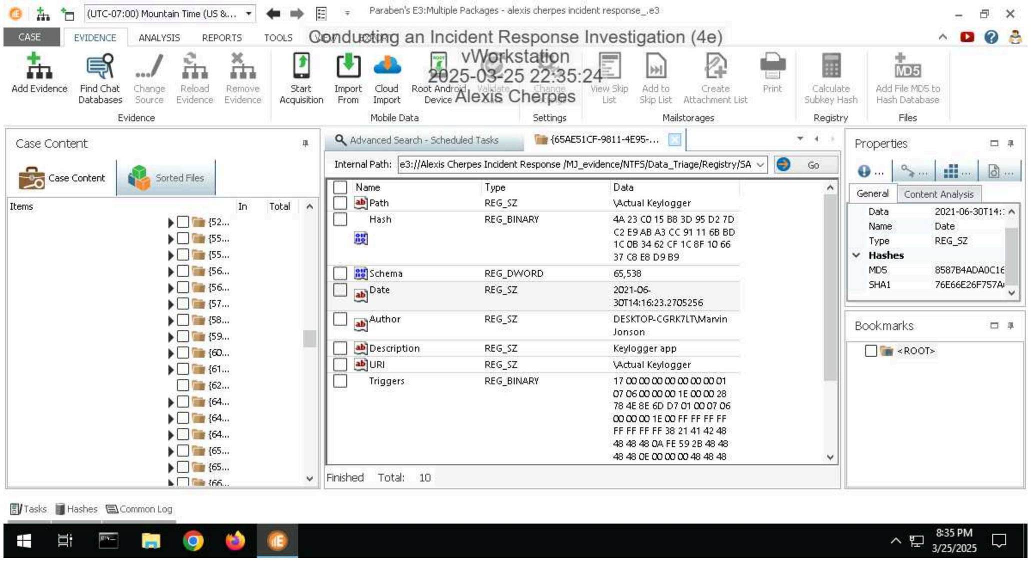
5. **Document** the Author and Date values associated with the scheduled keylogger task.

Author: Marvin Johnson. Date: June 30, 2021 at 2:16pm

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

Port: 66 Name: Actual Keylogger

9. **Make a screen capture** showing the **registry key value associated with the keylogger and the localSPM service**.



Internal Path: e3://Alexis Cherpes Incident Response /MJ_evidence/NTFS/Data_Triage/Registry/SA

Name	Type	Data
Path	REG_SZ	\Actual Keylogger
Hash	REG_BINARY	4A 23 C0 15 B8 3D 95 D2 7D C2 E9 AB A3 CC 91 11 6B BD 1C 0B 34 62 CF 1C 8F 10 66 37 C8 E8 D9 B9
Schema	REG_DWORD	65,538
Date	REG_SZ	2021-06-30T14:16:23.2705256
Author	REG_SZ	DESKTOP-CGRK7LT\Marvin Jonson
Description	REG_SZ	Keylogger app
URI	REG_SZ	\Actual Keylogger
Triggers	REG_BINARY	17 00 00 00 00 00 00 00 01 07 06 00 00 00 1E 00 00 28 78 4E 8E 6D D7 01 00 07 06 00 00 00 1E 00 FF FF FF FF FF FF FF FF 38 21 41 42 48 48 48 48 0A FE 59 2B 48 48 48 48 0E 00 00 00 48 48 48

Finished Total: 10

Data	2021-06-30T14::
Name	Date
Type	REG_SZ
Hashes	
MD5	8587B4ADA0C16
SHA1	76E66E26F757A

15. **Record** the first time and last time the keylogger was started.

First time: Wednesday, June 30, 2021 at 9:11:23 PM Last time: Friday, July 30, 2021 at 3:11:23 PM

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

Marvin opened the keylogger

Part 3: Update an Incident Response Report

Date
Insert current date here.

March 25, 2025

Name
Insert your name here.

Alexis Cherpes

Incident Priority

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

The incident priority has downgraded from high to medium. While the FTP server has been neutralized, the keylogger, firewall, and task scheduler still require further examinations.

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 changed. We have compromised system and there is malware that is installed. The malware is the 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.

The timeline has changed. The keylogger was first started on June 30th 2021.

Incident Scope

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

The incident scope has changed. The estimated quantity of systems affected is 1, and the estimates quantity of users affected is 1.

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 attack source is the keylogger installed on the workstation. The attack destination is the firewall and task scheduler. The primary function of the affected systems is the workstation.

Users Affected by the Incident

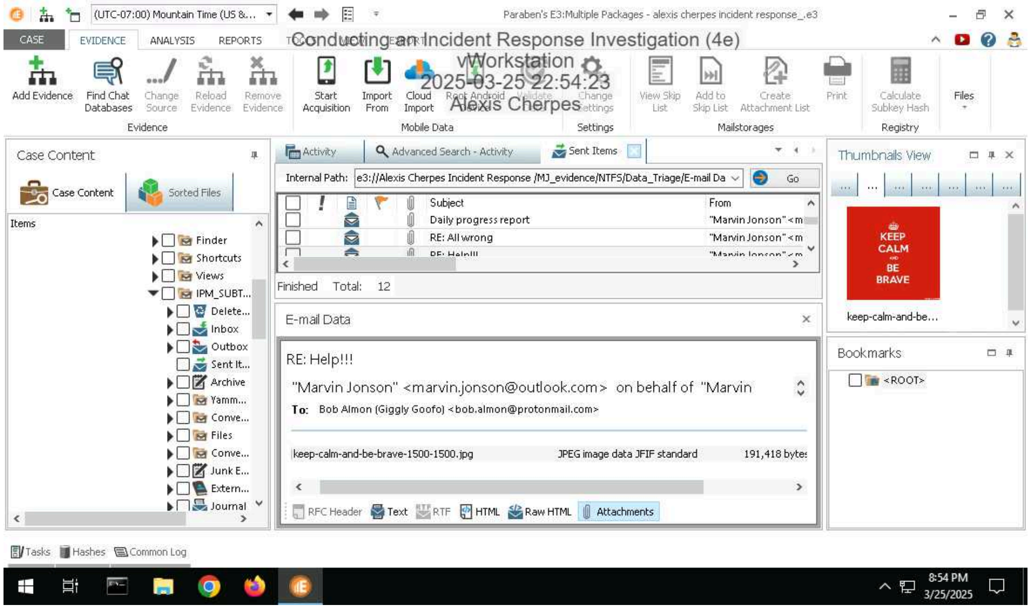
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

The user affected is Marvin Johnson.

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**.


Paraben's E3:Multiple Packages - alexis cherpes incident response_.e3

Conducting an Incident Response Investigation (4e)
vWorkstation
2025-03-25 22:54:23
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Incident Response /MJ_evidence/NTFS/Data_Triage/E-mail Da

Subject	From
Daily progress report	"Marvin Jonson" <m
RE: All wrong	"Marvin Jonson" <m
RE: Help!!!	"Marvin Jonson" <m

Finished Total: 12

E-mail Data

RE: Help!!!

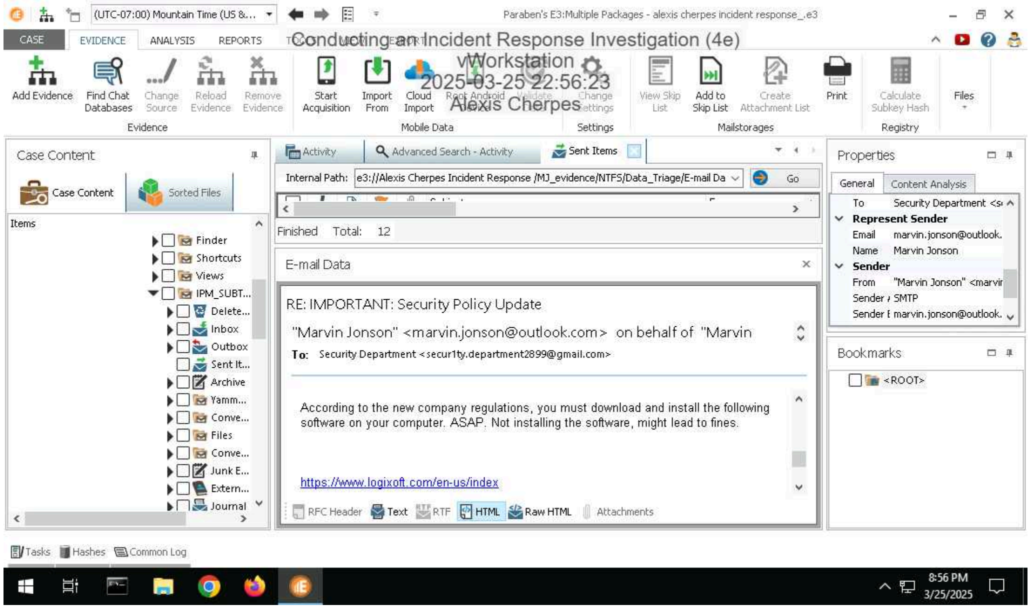
"Marvin Jonson" <marvin.jonson@outlook.com> on behalf of "Marvin

To: Bob Almon (Giggly Goofo) <bob.almon@protonmail.com>

keep-calm-and-be-brave-1500-1500.jpg	JPEG image data JFIF standard	191,418 bytes

Part 2: Identify Additional Evidence of Spyware

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


Paraben's E3:Multiple Packages - alexis cherpes incident response_.e3

Conducting an Incident Response Investigation (4e)
vWorkstation
2025-03-25 22:56:23
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Incident Response /MJ_evidence/NTFS/Data_Triage/E-mail Da

Finished Total: 12

E-mail Data

RE: IMPORTANT: Security Policy Update

"Marvin Jonson" <marvin.jonson@outlook.com> on behalf of "Marvin

To: Security Department <secur1ty.department2899@gmail.com>

According to the new company regulations, you must download and install the following software on your computer. ASAP. Not installing the software, might lead to fines.

https://www.logixoft.com/en-us/index

Properties

To	Security Department <s
Represent Sender	
Email	marvin.jonson@outlook.
Name	Marvin Jonson
Sender	
From	"Marvin Jonson" <marvir
Sender /	SMTP
Sender E	marvin.jonson@outlook.