Conducting an Incident Response Investigation (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 04

Student: Karan Atul Vora	Email: kxv230021@utdallas.edu

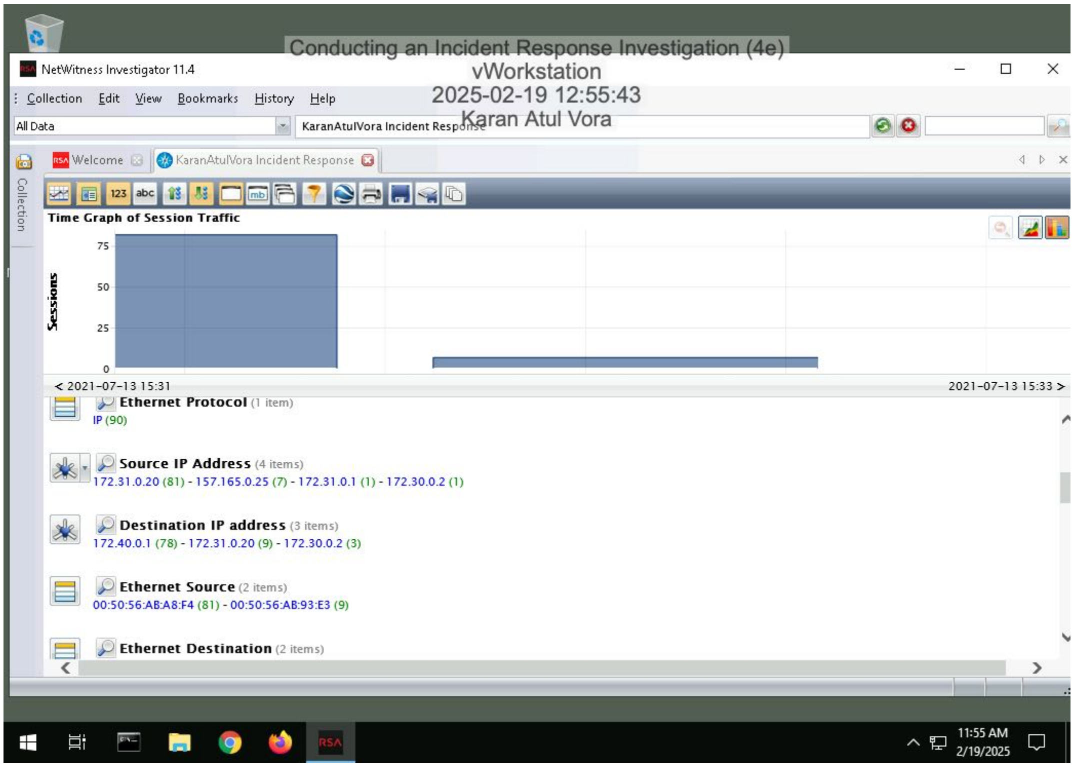
Time on Task: 3 hours, 1 minute	Progress: 100%

Report Generated: Monday, February 24, 2025 at 4:30 PM

Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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



Ethernet Protocol (1 item)
IP (90)

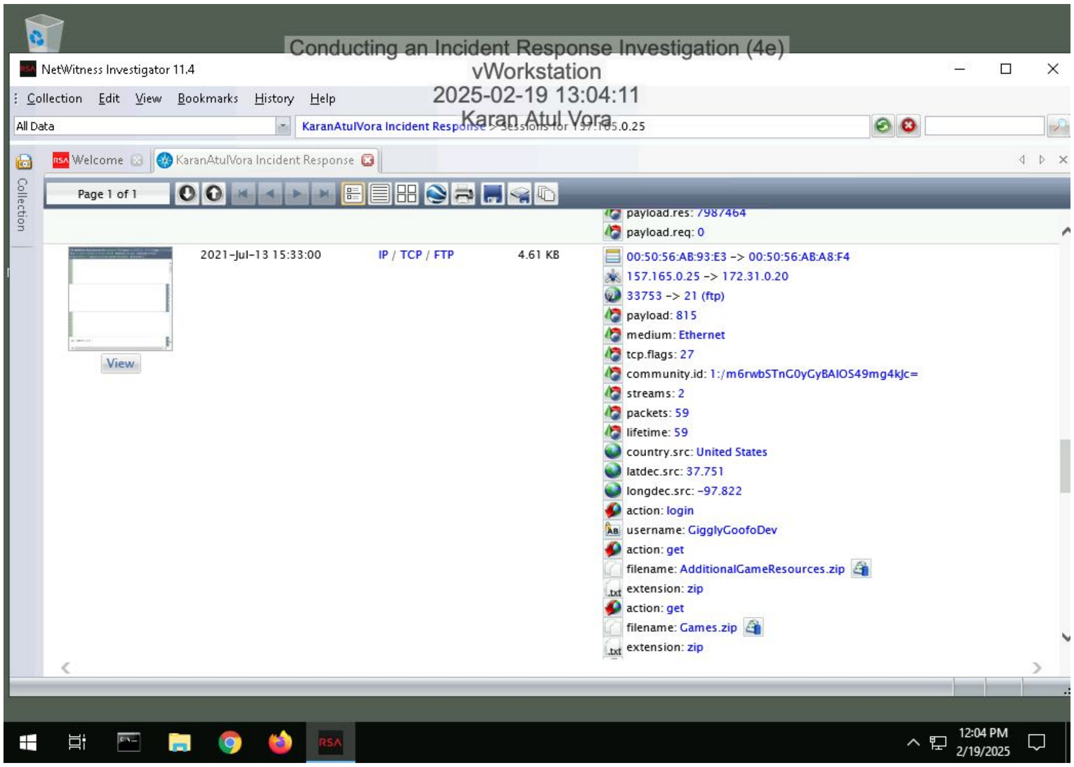
Source IP Address (4 items)
172.31.0.20 (81) - 157.165.0.25 (7) - 172.31.0.1 (1) - 172.30.0.2 (1)

Destination IP address (3 items)
172.40.0.1 (78) - 172.31.0.20 (9) - 172.30.0.2 (3)

Ethernet Source (2 items)
00:50:56:AB:A8:F4 (81) - 00:50:56:AB:93:E3 (9)

Ethernet Destination (2 items)

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



Conducting an Incident Response Investigation (4e)
vWorkstation
2025-02-19 13:04:11
Karan Atul Vora

NetWitness Investigator 11.4
Collection
Edit
View
Bookmarks
History
Help
All Data
KaranAtulVora Incident Response > Sessions for 157.165.0.25
Welcome
KaranAtulVora Incident Response
Collection
Page 1 of 1
View
12:04 PM
2/19/2025

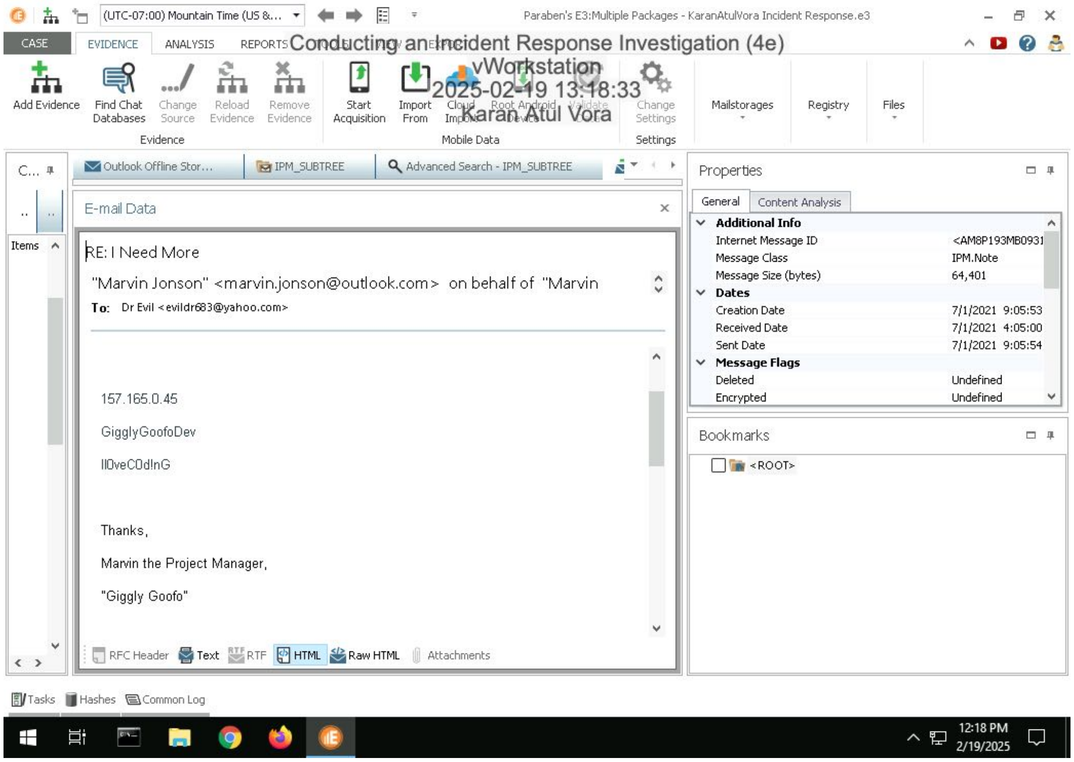
payload.res: 7987464
payload.req: 0

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

Part 2: Analyze a Disk Image for Forensic Evidence

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



RE: I Need More

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

To: Dr Evil <evildr683@yahoo.com>

157.165.0.45

GigglyGoofoDev

Il0veC0dInG

Thanks,

Marvin the Project Manager,

"Giggly Goofo"

Additional Info	
Internet Message ID	<AM8P193MB0931
Message Class	IPM.Note
Message Size (bytes)	64,401
Dates	
Creation Date	7/1/2021 9:05:53
Received Date	7/1/2021 4:05:00
Sent Date	7/1/2021 9:05:54
Message Flags	
Deleted	Undefined
Encrypted	Undefined

Part 3: Prepare an Incident Response Report

Date
Insert current date here.

February 19, 2025

Name
Insert your name here.

Karan Atul Vora

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.

Compromised system, 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.

Discovered - February 19, 2025 1:25:00 PM **Reported** - February 19, 2025 1:29:00 PM **Occurred** - July 1, 2021 9:05:54 AM

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.

systems affected - 1 estimated quantity of users affected - 1 third parties involved or affected - 1as well as any other relevant scoping information - File Transfer

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 Source (157.165.0.25,33753)Attack Destination (172.31.0.20,21)Web server

Users Affected by the Incident

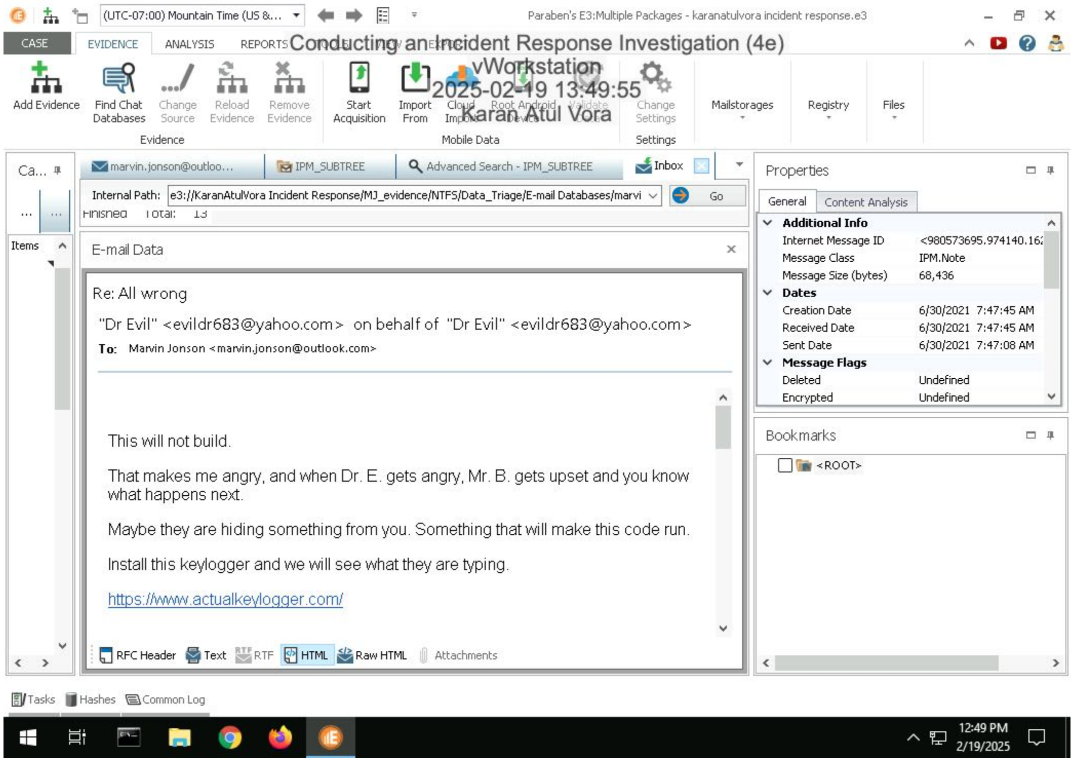
Define the following: Names and job titles of the affected users.

Marvin ,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**.



Re: All wrong

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

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

This will not build.

That makes me angry, and when Dr. E. gets angry, Mr. B. gets upset and you know what happens next.

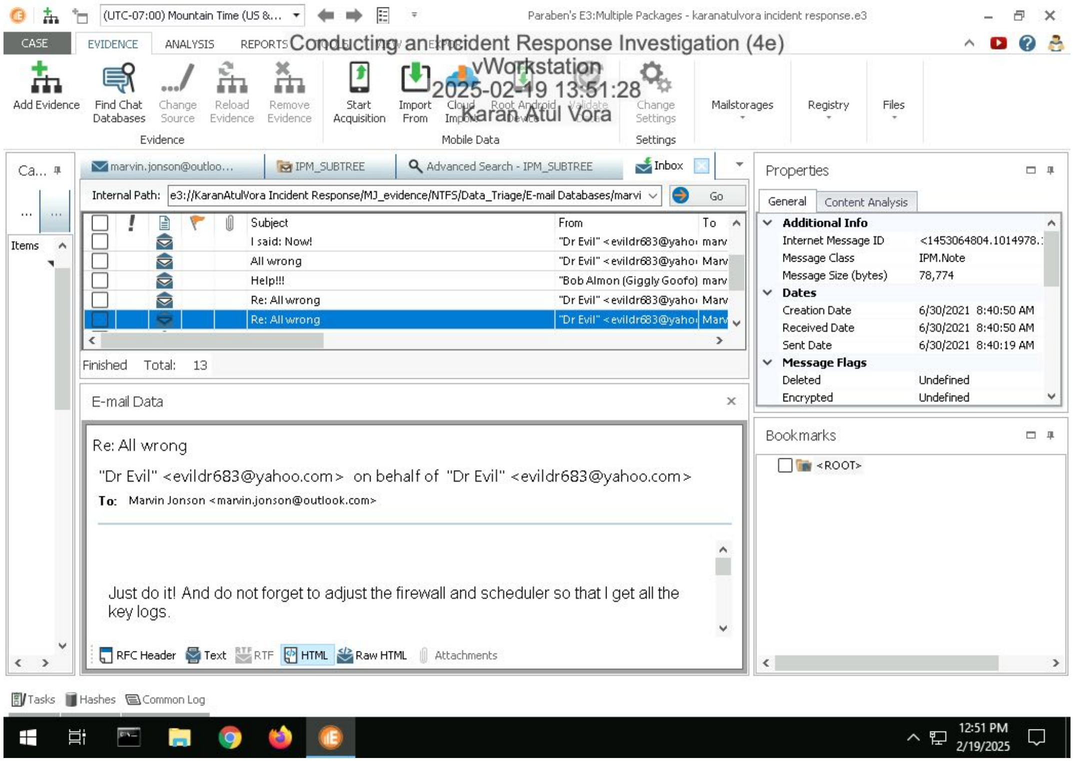
Maybe they are hiding something from you. Something that will make this code run.

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

https://www.actualkeylogger.com/

Additional Info	
Internet Message ID	<980573695.974140.162
Message Class	IPM.Note
Message Size (bytes)	68,436
Dates	
Creation Date	6/30/2021 7:47:45 AM
Received Date	6/30/2021 7:47:45 AM
Sent Date	6/30/2021 7:47:08 AM
Message Flags	
Deleted	Undefined
Encrypted	Undefined

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



Internal Path: e3://KaranAtulVora Incident Response/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvi

Subject	From	To
I said: Now!	"Dr Evil" <evildr683@yaho	marv
All wrong	"Dr Evil" <evildr683@yaho	Marv
Help!!!	"Bob Almon (Giggly Goofo)	marv
Re: All wrong	"Dr Evil" <evildr683@yaho	Marv
Re: All wrong	"Dr Evil" <evildr683@yaho	Marv

Finished Total: 13

Additional Info	
Internet Message ID	<1453064804.1014978.
Message Class	IPM.Note
Message Size (bytes)	78,774
Dates	
Creation Date	6/30/2021 8:40:50 AM
Received Date	6/30/2021 8:40:50 AM
Sent Date	6/30/2021 8:40:19 AM
Message Flags	
Deleted	Undefined
Encrypted	Undefined

Re: All wrong

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

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.

Part 2: Identify Evidence of Spyware

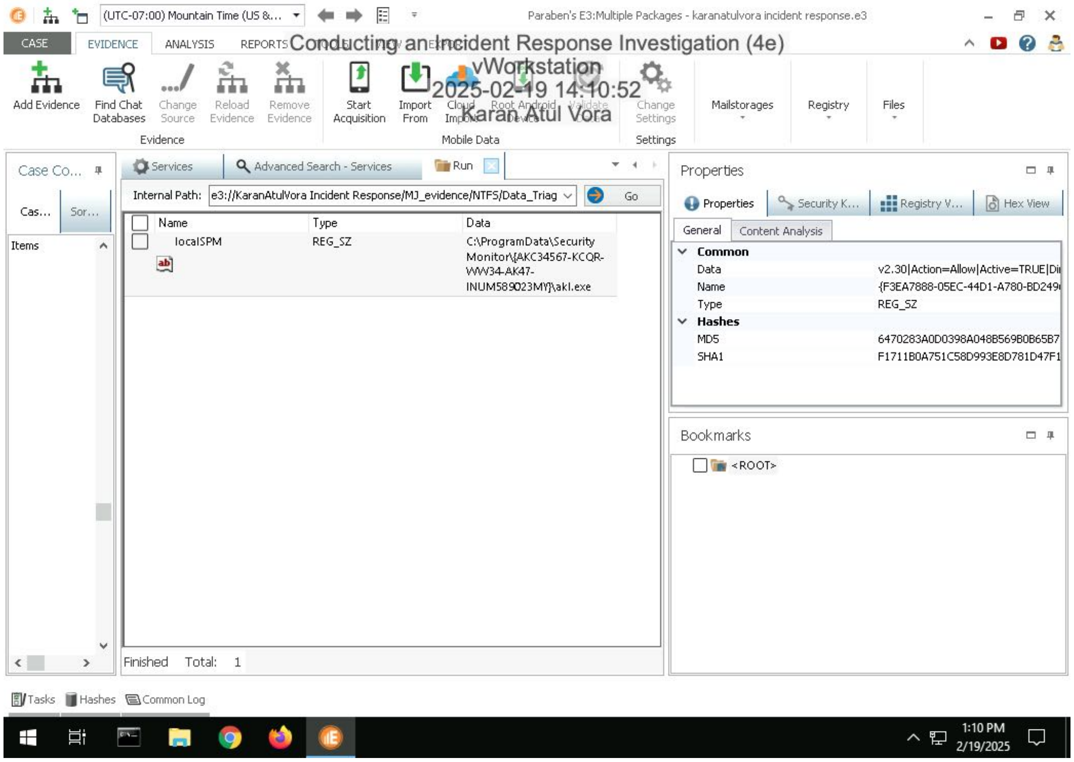
5. **Document** the Author and Date values associated with the scheduled keylogger task.

Author - DESKTOP-CGRK7LT\MarvinJonsom Date - 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=666 name=akl.exe location=C:\ProgramData\Security Monitor\{AKC34567-KCQR-WW34-AK47-INUM589O23MY}\akl.exe

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



Internal Path: e3://KaranAtulVora Incident Response/MJ_evidence/NTFS/Data_Triag

Name	Type	Data
localSPM	REG_SZ	C:\ProgramData\Security Monitor\{AKC34567-KCQR-WW34-AK47-INUM589023MY}\akl.exe

Common	
Data	v2.30|Action=Allow|Active=TRUE|Di
Name	{F3EA7888-05EC-44D1-A780-BD249
Type	REG_SZ
Hashes	
MD5	6470283A0D0398A048B569B0B65B7
SHA1	F1711B0A751C58D993E8D781D47F1

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

first time - June 30, 2021 9:11:23 PM last time - June 30, 2021 9:36:42 PM

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.

February 19, 2025

Name

Insert your name here.

Karan Atul Vora

Incident Priority

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

No

Incident Type

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

Malware Installed and Firewall Configuration opened

Incident Timeline

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

Occurred - July 30, 2021 9:11:23 PM

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.

Unchanged

Users Affected by the Incident

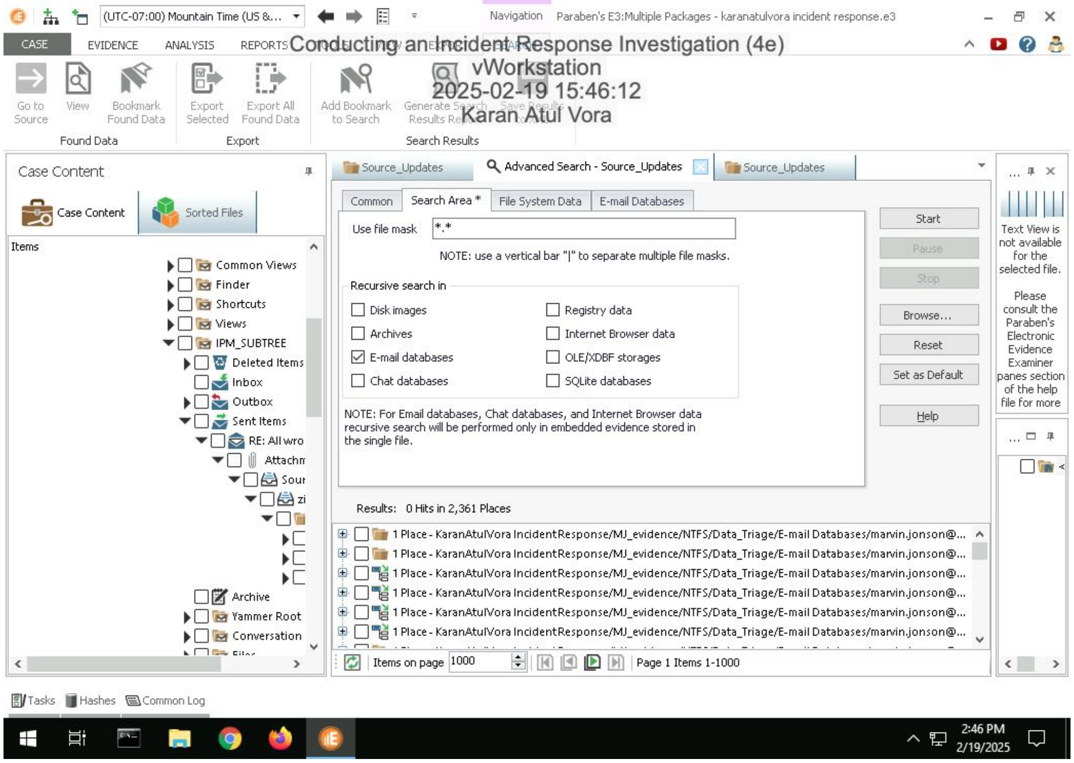
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Unchanged(All the users that might have logged in on the system that is compromised as the key logger was set on the machine)

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**.



Conducting an Incident Response Investigation (4e)
vWorkstation
2025-02-19 15:46:12
Karan Atul Vora

Use file mask: *.*

NOTE: use a vertical bar "|" to separate multiple file masks.

Recursive search in

- ☐ Disk images
- ☐ Archives
- ☑ E-mail databases
- ☐ Chat databases
- ☐ Registry data
- ☐ Internet Browser data
- ☐ OLE/XDBF storages
- ☐ SQLite databases

NOTE: For Email databases, Chat databases, and Internet Browser data recursive search will be performed only in embedded evidence stored in the single file.

Text View is not available for the selected file.

Please consult the Paraben's Electronic Evidence Examiner panes section of the help file for more

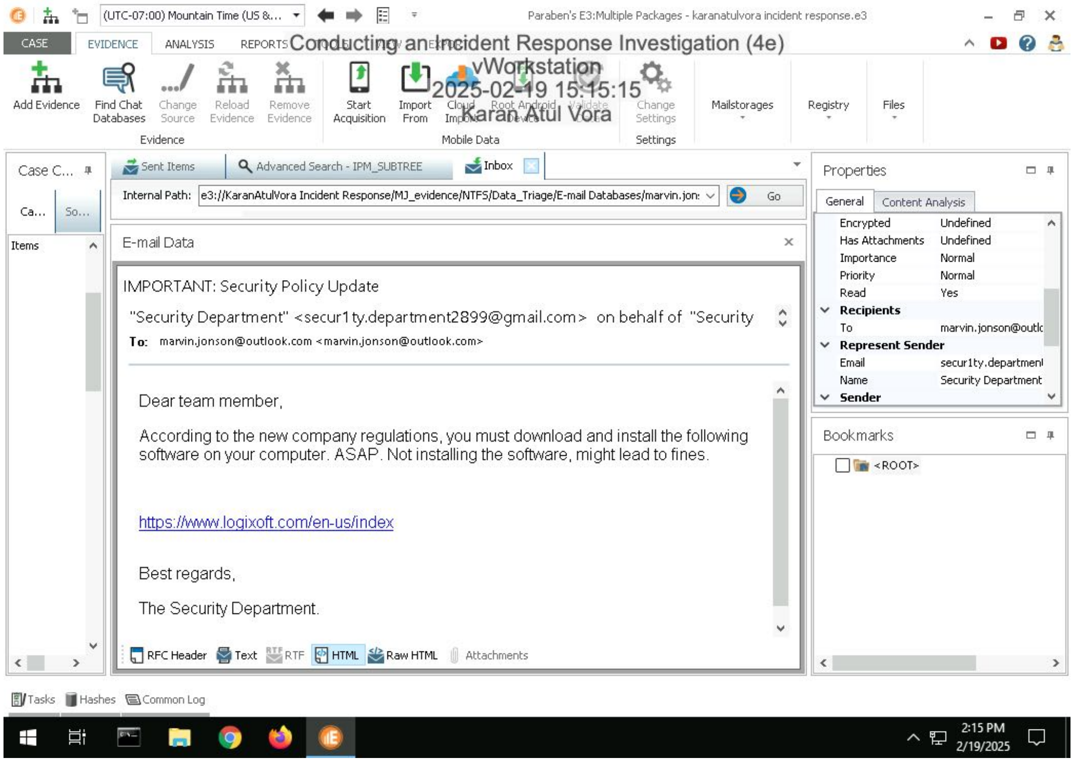
Results: 0 Hits in 2,361 Places

```
1 Place - KaranAtulVora IncidentResponse/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jonson@...
1 Place - KaranAtulVora IncidentResponse/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jonson@...
1 Place - KaranAtulVora IncidentResponse/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jonson@...
1 Place - KaranAtulVora IncidentResponse/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jonson@...
1 Place - KaranAtulVora IncidentResponse/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jonson@...
1 Place - KaranAtulVora IncidentResponse/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jonson@...
```

Items on page 1000 | Page 1 Items 1-1000

Part 2: Identify Additional Evidence of Spyware

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



Internal Path: e3://KaranAtulVora Incident Response/MJ_evidence/NTFS/Data_Triage/E-mail Databases/marvin.jon:

IMPORTANT: Security Policy Update

"Security Department" <secur1ty.department2899@gmail.com> on behalf of "Security

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

Dear team member,

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

Best regards,

The Security Department.

Encrypted	Undefined
Has Attachments	Undefined
Importance	Normal
Priority	Normal
Read	Yes
Recipients	
To	marvin.jonson@outlc
Represent Sender	
Email	secur1ty.departmen
Name	Security Department
Sender	