Performing Incident Response and Forensic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 10

Student: Patrick Kierzkowski	Email: pxk405@francis.edu

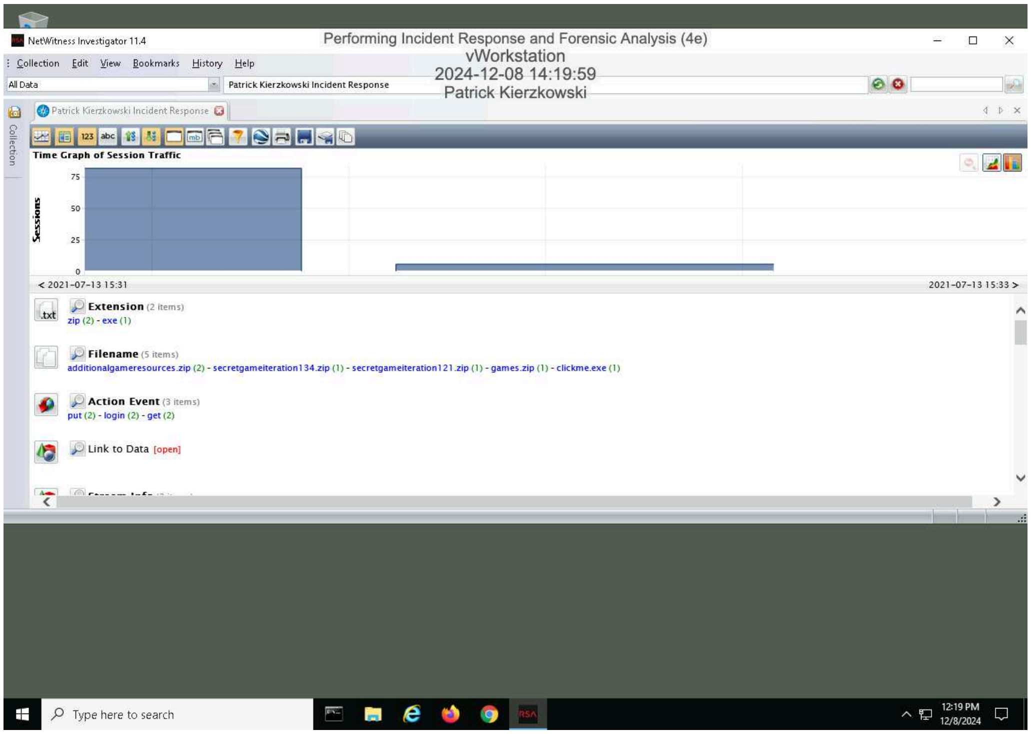
Time on Task: 8 hours, 0 minutes	Progress: 100%

Report Generated: Monday, July 7, 2025 at 9:51 PM

Section 1: Hands-On Demonstration

Part 1: Analyze a PCAP File for Forensic Evidence

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



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 14:19:59
Patrick Kierzkowski

NetWitness Investigator 11.4

All Data | Patrick Kierzkowski Incident Response

Time Graph of Session Traffic

< 2021-07-13 15:31 — 2021-07-13 15:33 >

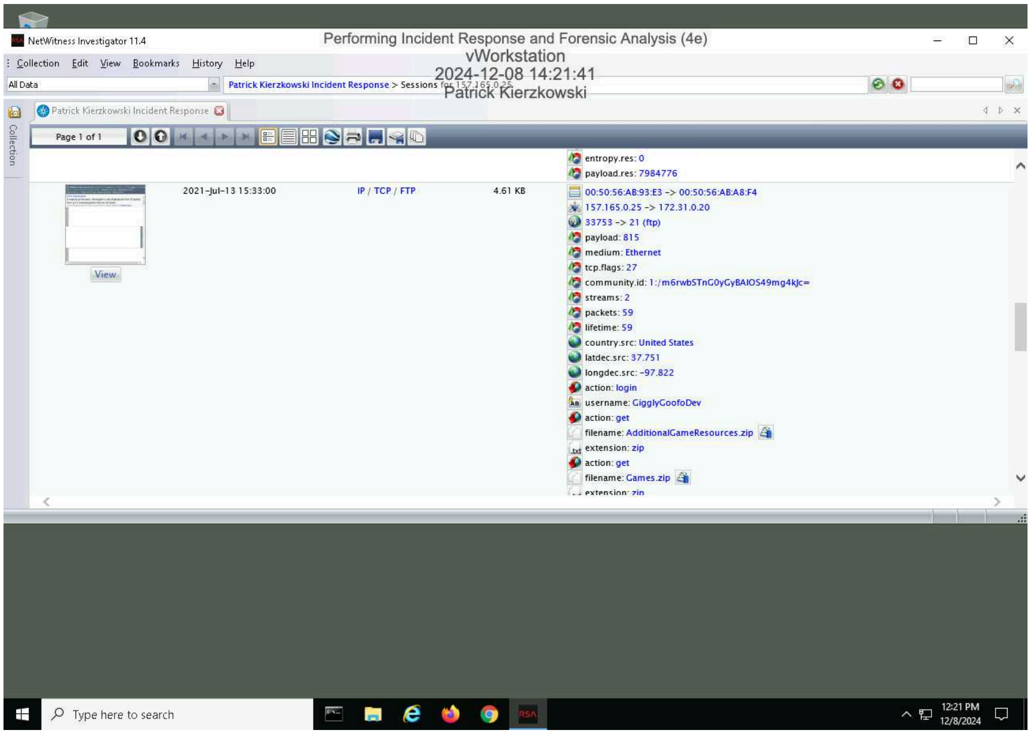
Extension (2 items)
zip (2) - exe (1)

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]

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
Patrick Kierzkowski Incident Response > Sessions for 157.165.0.25
Patrick Kierzkowski Incident Response
Page 1 of 1
Collection
View
Type here to search
12:21 PM
12/8/2024

Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 14:21:41
Patrick Kierzkowski

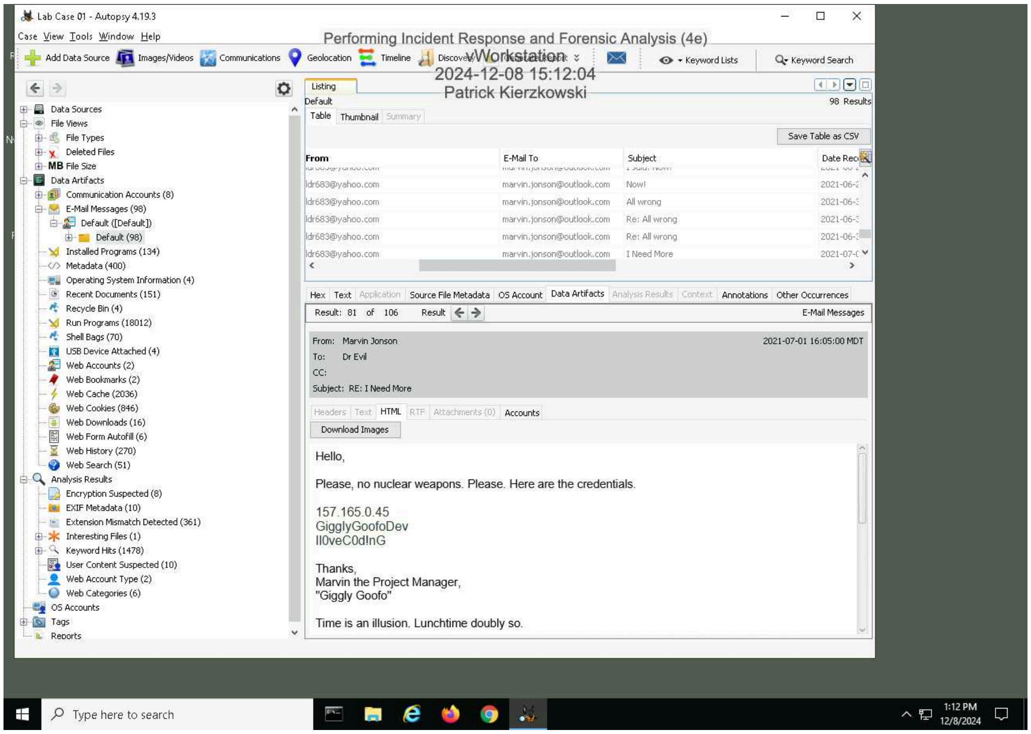
entropy.res: 0
payload.res: 7984776

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

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



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 15:12:04
Patrick Kierzkowski

From	E-Mail To	Subject	Date Rec
ldr683@yahoo.com	marvin.jonson@outlook.com	Now!	2021-06-2
ldr683@yahoo.com	marvin.jonson@outlook.com	All wrong	2021-06-3
ldr683@yahoo.com	marvin.jonson@outlook.com	Re: All wrong	2021-06-3
ldr683@yahoo.com	marvin.jonson@outlook.com	Re: All wrong	2021-06-3
ldr683@yahoo.com	marvin.jonson@outlook.com	I Need More	2021-07-0

From: Marvin Jonson 2021-07-01 16:05:00 MDT
To: Dr Evil
CC:
Subject: RE: I Need More

Hello,

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

157.165.0.45
GigglyGoofoDev
Il0veC0d!nG

Thanks,
Marvin the Project Manager,
"Giggly Goofo"

Time is an illusion. Lunchtime doubly so.

Part 3: Prepare an Incident Response Report

Date
Insert current date here.

12/8/24

Name
Insert your name here.

Pstrick Kierzkowski

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, Reconnaissance , 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.

Discovered: 2024-12-08 14:48:00 Reported: 2024-12-08 14:50:00 Occurred: 2021-07-01 16:05:00

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 - 4Estimated quantity of users affected - 1Third parties involved or affected - 0Mr. Johnson worked with Dr. Evil and released IP addresses, and account access to an FTP secured network in order to steal company information

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: 157.165.0.45Attack Destinations: 172.31.0.20 , 172.30.0.1 , 172.30.0.2 , 172.40.0.1IP addresses of the affected systems: 172.31.0.20 , 172.30.0.1 , 172.30.0.2 , 172.40.0.1Primary functions of the affected systems: Domain Controller

Users Affected by the Incident

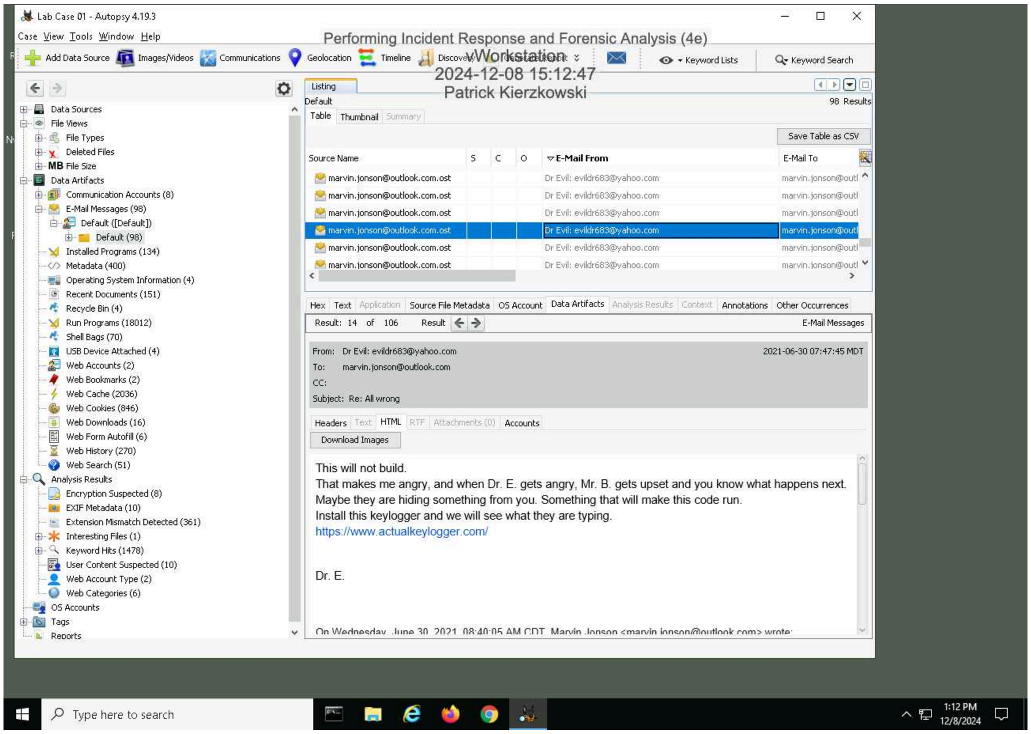
Define the following: Names and job titles of the affected users.

Marvin Johnson Project Manager

Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

5. **Make a screen capture** showing the **email from Dr. Evil demanding that Marvin install a keylogger**.



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 15:12:47
Patrick Kierzkowski

Source Name	S	C	O	E-Mail From	E-Mail To
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl

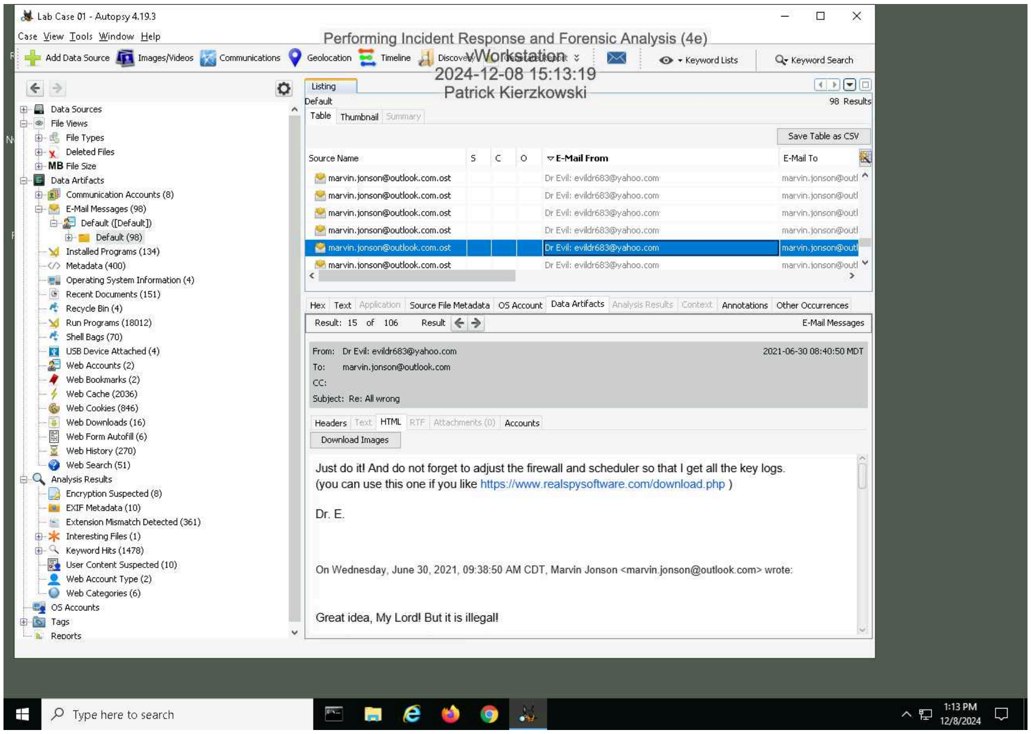
From: Dr Evil: evildr683@yahoo.com 2021-06-30 07:47:45 MDT
To: marvin.jonson@outlook.com
CC:
Subject: Re: All wrong

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/

Dr. E.

On Wednesday, June 30, 2021, 08:40:05 AM CDT, Marvin Jonson <marvin.jonson@outlook.com> wrote:

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



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 15:13:19
Patrick Kierzkowski

Source Name	S	C	O	E-Mail From	E-Mail To
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outl

Result: 15 of 106 Result   E-Mail Messages

From: Dr Evil: evildr683@yahoo.com   2021-06-30 08:40:50 MDT
To: marvin.jonson@outlook.com
CC:
Subject: Re: All wrong

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)

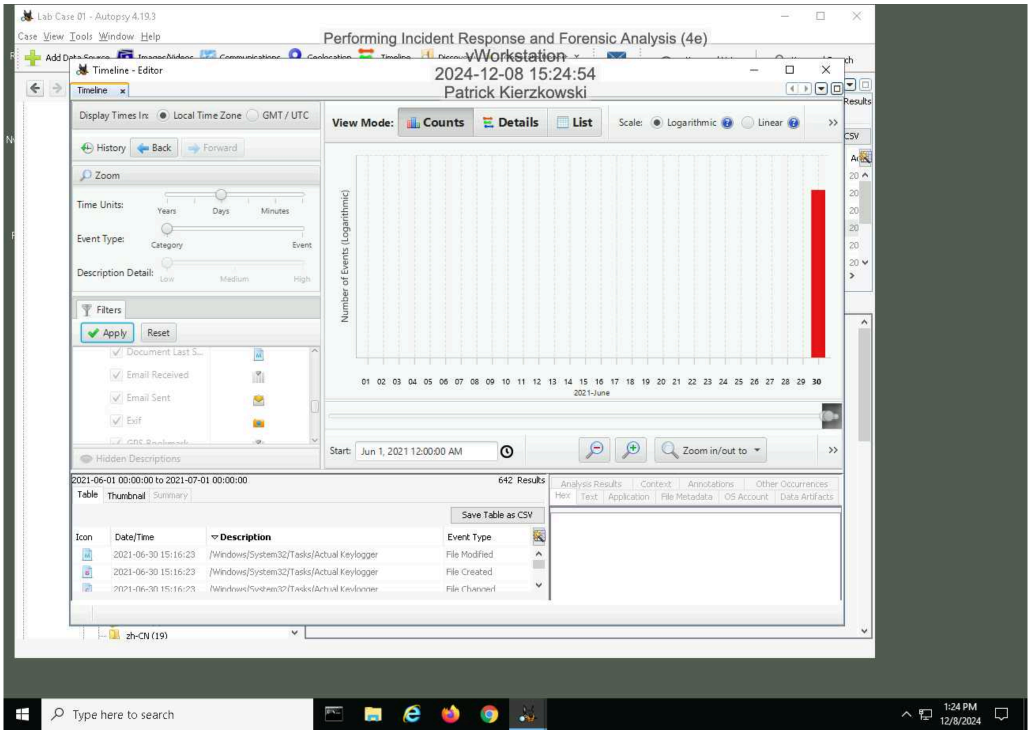
Dr. E.

On Wednesday, June 30, 2021, 09:38:50 AM CDT, Marvin Jonson <marvin.jonson@outlook.com> wrote:

Great idea, My Lord! But it is illegal!

Part 2: Identify Evidence of Spyware

12. **Make a screen capture** showing the **three events that are related to the Actual Keylogger file in the /Windows/System32/Tasks folder with a June 30 timestamp**.



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 15:24:54
Patrick Kierzkowski

Display Times In: ● Local Time Zone ○ GMT / UTC

Scale: ● Logarithmic ○ Linear

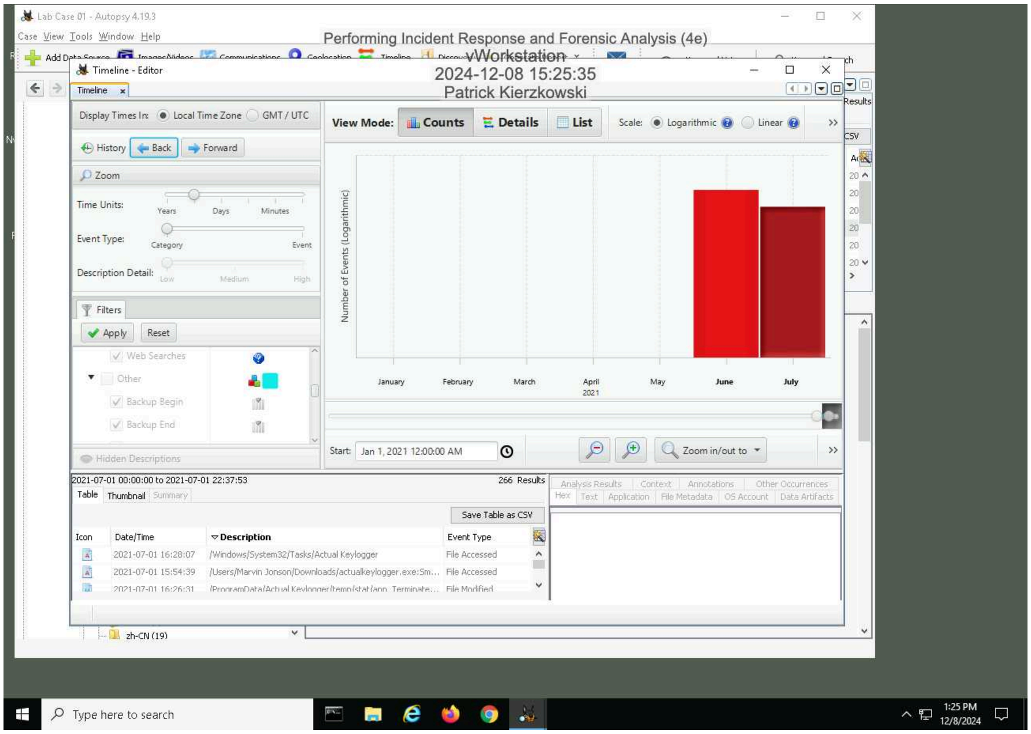
Start: Jun 1, 2021 12:00:00 AM

2021-06-01 00:00:00 to 2021-07-01 00:00:00 642 Results

Save Table as CSV

Icon	Date/Time	Description	Event Type
M	2021-06-30 15:16:23	/Windows/System32/Tasks/Actual Keylogger	File Modified
B	2021-06-30 15:16:23	/Windows/System32/Tasks/Actual Keylogger	File Created
C	2021-06-30 15:16:23	/Windows/System32/Tasks/Actual Keylogger	File Changed

15. **Make a screen capture** showing the **one event that is related to the Actual Keylogger file in the /Windows/System32/Tasks folder with a July 1 timestamp**.



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 15:25:35
Patrick Kierzkowski

Display Times In: ● Local Time Zone ○ GMT / UTC

Scale: ● Logarithmic ○ Linear

Start: Jan 1, 2021 12:00:00 AM

2021-07-01 00:00:00 to 2021-07-01 22:37:53 266 Results

Save Table as CSV

Icon	Date/Time	Description	Event Type
A	2021-07-01 16:28:07	/Windows/System32/Tasks/Actual Keylogger	File Accessed
A	2021-07-01 15:54:39	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Accessed
	2021-07-01 16:26:31	/ProgramData/Actual Keylogger/temp/stat/app_Terminate:...	File Modified

20. **Record** the date and time that the keylogger’s executable file was created.

2021-06-30 15:00:13

22. **Record** the date and time when the keylogger’s executable file was last started.

2021-07-01 15:54:39

23. **Record** whether you think you have evidence to claim that Marvin opened the keylogger.

Yes I think we have evidence to claim that Marvin opened the keylogger

Part 3: Update an Incident Response Report

Date

Insert current date here.

12/8/2024

Name

Insert your name here.

Patrick Kierzkowski

Incident Priority

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

Unchanged - still high

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, Compromised User Credentials

Incident Timeline

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

Began at 2021-06-30Keylogger accessed 2021-07-01 15:54:39

Incident Scope

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

Dr. Evil and Marvin worked together

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, but keylogger could get other users info

Users Affected by the Incident

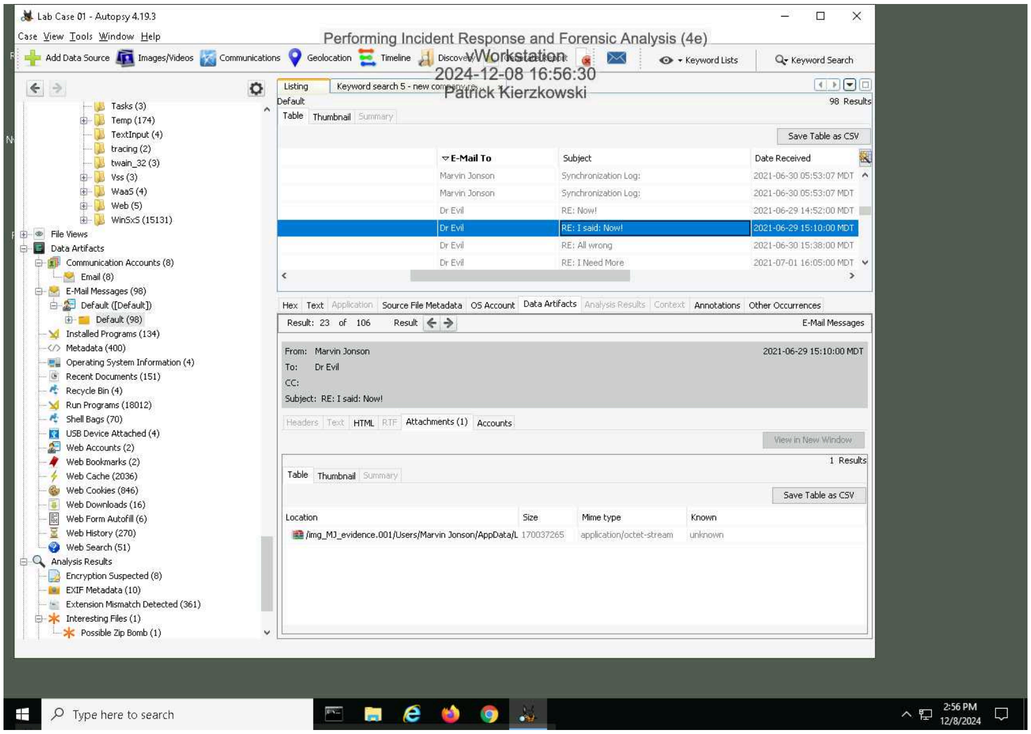
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Unchanged for now, just Marvin

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**.



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-12-08 16:56:30
Patrick Kierzkowski

Default 98 Results

E-Mail To	Subject	Date Received
Marvin Jonson	Synchronization Log:	2021-06-30 05:53:07 MDT
Marvin Jonson	Synchronization Log:	2021-06-30 05:53:07 MDT
Dr Evil	RE: Now!	2021-06-29 14:52:00 MDT
Dr Evil	RE: I said: Now!	2021-06-29 15:10:00 MDT
Dr Evil	RE: All wrong	2021-06-30 15:38:00 MDT
Dr Evil	RE: I Need More	2021-07-01 16:05:00 MDT

Result: 23 of 106 Result E-Mail Messages

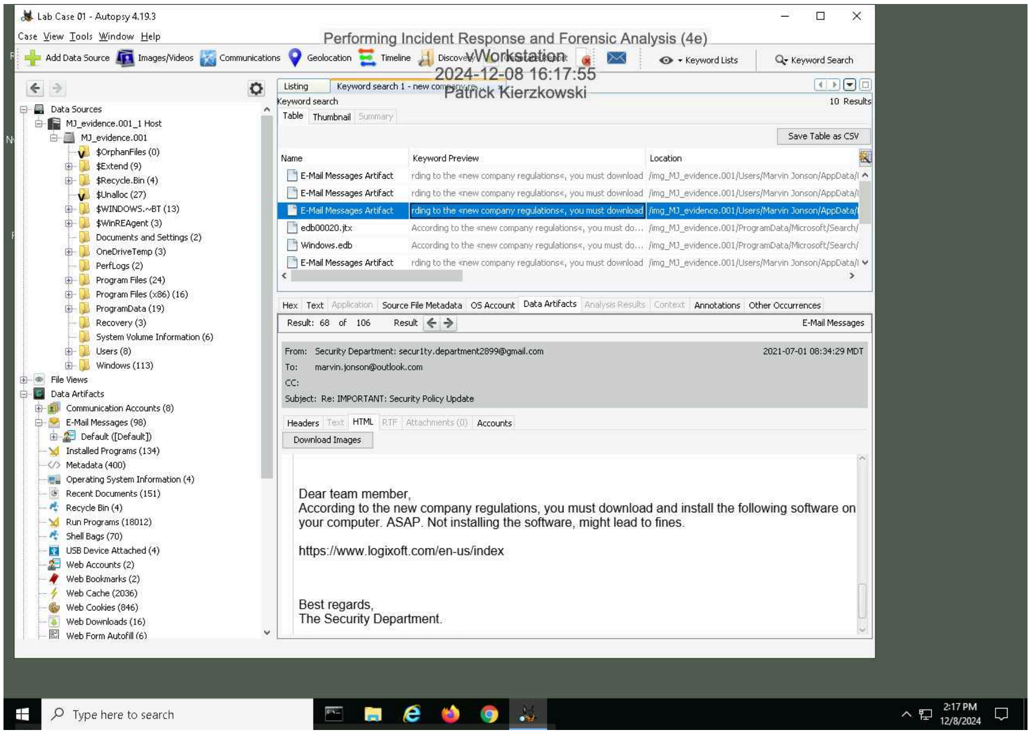
From: Marvin Jonson 2021-06-29 15:10:00 MDT
To: Dr Evil
CC:
Subject: RE: I said: Now!

1 Results

Location	Size	Mime type	Known
/img_MJ_evidence.001/Users/Marvin Jonson/AppData/L	170037265	application/octet-stream	unknown

Part 2: Identify Additional Evidence of Spyware

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



Keyword search — 10 Results

Name	Keyword Preview	Location
E-Mail Messages Artifact	rding to the «new company regulations«, you must download	/img_MJ_evidence.001/Users/Marvin Jonson/AppData/I
E-Mail Messages Artifact	rding to the «new company regulations«, you must download	/img_MJ_evidence.001/Users/Marvin Jonson/AppData/I
E-Mail Messages Artifact	rding to the «new company regulations«, you must download	/img_MJ_evidence.001/Users/Marvin Jonson/AppData/I
edb00020.jtx	According to the «new company regulations«, you must do...	/img_MJ_evidence.001/ProgramData/Microsoft/Search/
Windows.edb	According to the «new company regulations«, you must do...	/img_MJ_evidence.001/ProgramData/Microsoft/Search/
E-Mail Messages Artifact	rding to the «new company regulations«, you must download	/img_MJ_evidence.001/Users/Marvin Jonson/AppData/I

Result: 68 of 106 — E-Mail Messages

From: Security Department: secur1ty.department2899@gmail.com — 2021-07-01 08:34:29 MDT
To: marvin.jonson@outlook.com
CC:
Subject: Re: IMPORTANT: Security Policy Update

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.

Document the red flags in the email that indicate that it may be a phishing attempt.

They say to "Plz, adjust the Firewall and Scheduler and do not talk about us with others. Security, if you know what I mean. Wink." As well as the security email is spelt as secur1ty, which is a giveaway that it's not the actual security team.