Performing Incident Response and Forensic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 10

Student:	Email:
Andrew Sweeney	asweene8@depaul.edu

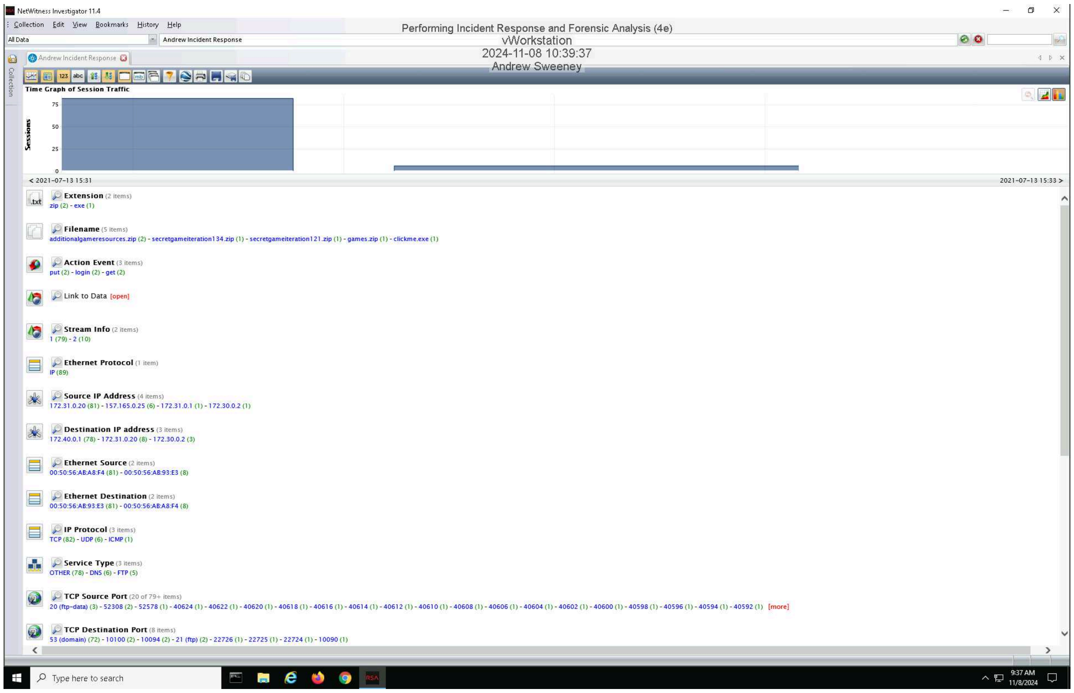
Time on Task:	Progress:
0 hours, 46 minutes	100%

Report Generated: Friday, November 8, 2024 at 1:27 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
2024-11-08 10:39:37
Andrew Sweeney

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 (10)

Ethernet Protocol (1 item)
IP (89)

Source IP Address (4 items)
172.31.0.20 (81) - 157.165.0.25 (6) - 172.31.0.1 (1) - 172.30.0.2 (1)

Destination IP address (3 items)
172.40.0.1 (78) - 172.31.0.20 (8) - 172.30.0.2 (3)

Ethernet Source (2 items)
00:50:56:AB:A8:F4 (81) - 00:50:56:AB:93:E3 (8)

Ethernet Destination (2 items)
00:50:56:AB:93:E3 (81) - 00:50:56:AB:A8:F4 (8)

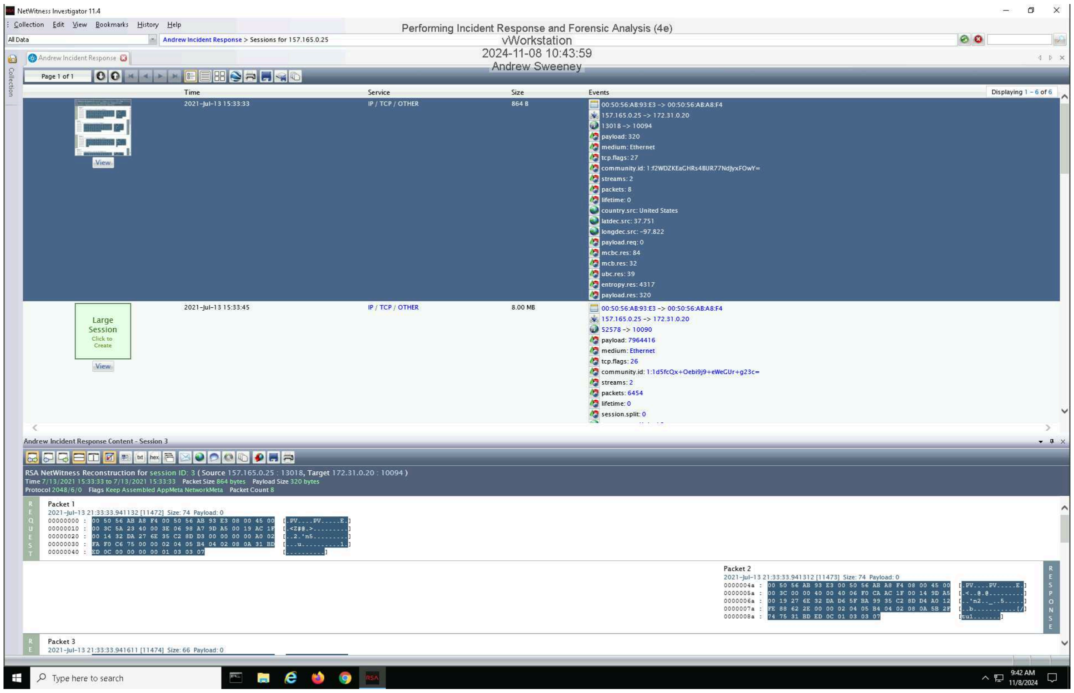
IP Protocol (3 items)
TCP (82) - UDP (6) - ICMP (1)

Service Type (3 items)
OTHER (78) - DNS (6) - FTP (5)

TCP Source Port (20 of 79+ items)
20 (ftp-data) (3) - 52308 (2) - 52578 (1) - 40624 (1) - 40622 (1) - 40620 (1) - 40618 (1) - 40616 (1) - 40614 (1) - 40612 (1) - 40610 (1) - 40608 (1) - 40606 (1) - 40604 (1) - 40602 (1) - 40600 (1) - 40598 (1) - 40596 (1) - 40594 (1) - 40592 (1) [more]

TCP Destination Port (8 items)
53 (domain) (72) - 10100 (2) - 10094 (2) - 21 (ftp) (2) - 22726 (1) - 22725 (1) - 22724 (1) - 10090 (1)

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
Andrew Incident Response > Sessions for 157.165.0.25
Andrew Incident Response
Page 1 of 1
Displaying 1 – 6 of 6
View
Large Session Click to Create
View
Type here to search
9:42 AM
11/8/2024

Time	Service	Size	Events
2021-Jul-13 15:33:33	IP / TCP / OTHER	864 B	00:50:56:AB:93:E3 -> 00:50:56:AB:A8:F4 157.165.0.25 -> 172.31.0.20 13018 -> 10094 payload: 320 medium: Ethernet tcp.flags: 27 community.id: 1:f2WDZKEaGHRs4BUR77NdJyxFOwY= streams: 2 packets: 8 lifetime: 0 country.src: United States latdec.src: 37.751 longdec.src: -97.822 payload.req: 0 mcbc.res: 84 mcb.res: 32 ubc.res: 39 entropy.res: 4317 payload.res: 320
2021-Jul-13 15:33:45	IP / TCP / OTHER	8.00 MB	00:50:56:AB:93:E3 -> 00:50:56:AB:A8:F4 157.165.0.25 -> 172.31.0.20 52578 -> 10090 payload: 7964416 medium: Ethernet tcp.flags: 26 community.id: 1:1d5fcQx+Oebi9j9+eWeGUr+g23c= streams: 2 packets: 6454 lifetime: 0 session.split: 0

Andrew Incident Response Content - Session 3

RSA NetWitness Reconstruction for session ID: 3 (Source 157.165.0.25 : 13018, Target 172.31.0.20 : 10094)
Time 7/13/2021 15:33:33 to 7/13/2021 15:33:33 Packet Size 864 bytes Payload Size 320 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 8

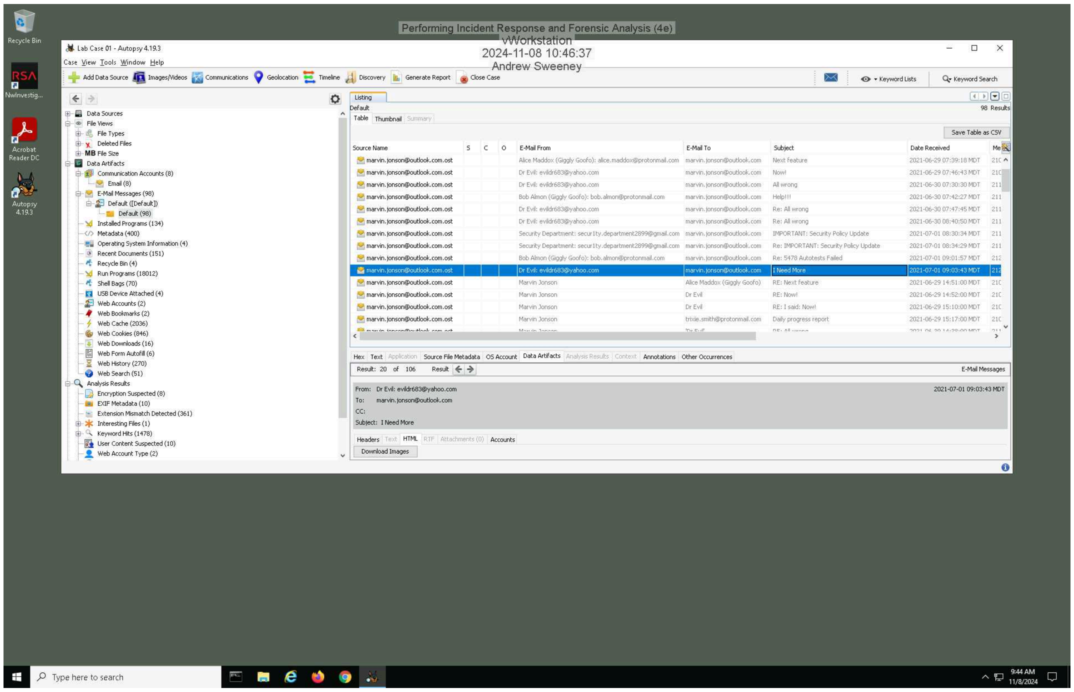
```
REQUEST
Packet 1
2021-Jul-13 21:33:33.941132 [11472] Size: 74 Payload: 0
00000000 : 00 50 56 AB A8 F4 00 50 56 AB 93 E3 08 00 45 00  [.PV....PV.....E.]
00000010 : 00 3C 5A 23 40 00 3E 06 98 A7 9D A5 00 19 AC 1F  [.<Z#@.>.........]
00000020 : 00 14 32 DA 27 6E 35 C2 8D D3 00 00 00 00 A0 02  [..2.'n5.........]
00000030 : FA F0 C6 75 00 00 02 04 05 B4 04 02 08 0A 31 BD  [...u..........1.]
00000040 : ED 0C 00 00 00 00 01 03 03 07                    [..........]

RESPONSE
Packet 2
2021-Jul-13 21:33:33.941312 [11473] Size: 74 Payload: 0
0000004a : 00 50 56 AB 93 E3 00 50 56 AB A8 F4 08 00 45 00  [.PV....PV.....E.]
0000005a : 00 3C 00 00 40 00 40 06 F0 CA AC 1F 00 14 9D A5  [.<..@.@.........]
0000006a : 00 19 27 6E 32 DA D6 5F BA 99 35 C2 8D D4 A0 12  [..'n2.._..5.....]
0000007a : FE 88 62 2E 00 00 02 04 05 B4 04 02 08 0A 5B 2F  [..b...........[/]
0000008a : 74 75 31 BD ED 0C 01 03 03 07                    [tu1.......]

RE
Packet 3
2021-Jul-13 21:33:33.941611 [11474] Size: 66 Payload: 0
```

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**.



Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Me
marvin.jonson@outlook.com.ost				Alice Maddox (Giggly Goofo): alice.maddox@protonmail.com	marvin.jonson@outlook.com	Next feature	2021-06-29 07:39:18 MDT	210
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	Now!	2021-06-29 07:46:43 MDT	210
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	All wrong	2021-06-30 07:30:30 MDT	211
marvin.jonson@outlook.com.ost				Bob Almon (Giggly Goofo): bob.almon@protonmail.com	marvin.jonson@outlook.com	Help!!!	2021-06-30 07:42:27 MDT	211
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	Re: All wrong	2021-06-30 07:47:45 MDT	211
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	Re: All wrong	2021-06-30 08:40:50 MDT	211
marvin.jonson@outlook.com.ost				Security Department: secur1ty.department2899@gmail.com	marvin.jonson@outlook.com	IMPORTANT: Security Policy Update	2021-07-01 08:30:34 MDT	211
marvin.jonson@outlook.com.ost				Security Department: secur1ty.department2899@gmail.com	marvin.jonson@outlook.com	Re: IMPORTANT: Security Policy Update	2021-07-01 08:34:29 MDT	211
marvin.jonson@outlook.com.ost				Bob Almon (Giggly Goofo): bob.almon@protonmail.com	marvin.jonson@outlook.com	Re: 5478 Autotests Failed	2021-07-01 09:01:57 MDT	212
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	I Need More	2021-07-01 09:03:43 MDT	212
marvin.jonson@outlook.com.ost				Marvin Jonson	Alice Maddox (Giggly Goofo)	RE: Next feature	2021-06-29 14:51:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	Dr Evil	RE: Now!	2021-06-29 14:52:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	Dr Evil	RE: I said: Now!	2021-06-29 15:10:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	trixie.smith@protonmail.com	Daily progress report	2021-06-29 15:17:00 MDT	210

From: Dr Evil: evildr683@yahoo.com 2021-07-01 09:03:43 MDT
To: marvin.jonson@outlook.com
CC:
Subject: I Need More

Part 3: Prepare an Incident Response Report

Date
Insert current date here.

11/08/2024

Name
Insert your name here.

Andrew

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

Medium

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 SystemCompromised User CredentialsNetwork Attack (e.g., DoS)Malware (e.g., virus, worm, trojan)Reconnaissance (e.g., scanning, sniffing)Lost Equipment/TheftPhysical Break-inSocial EngineeringLaw Enforcement Request

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 of discovery (July 31, 2021, at 10:30 AM as mentioned).Date and time of reporting. - unknownDate and time of the incident occurrence, if known. - unknown

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 detail of estimated system affected. Found in PCAP

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 (e.g., IP addresses, ports).Attack destinations (e.g., IP addresses, ports).IP addresses of affected systems.Primary functions of the affected systems (e.g., workstations, domain controllers).

Users Affected by the Incident

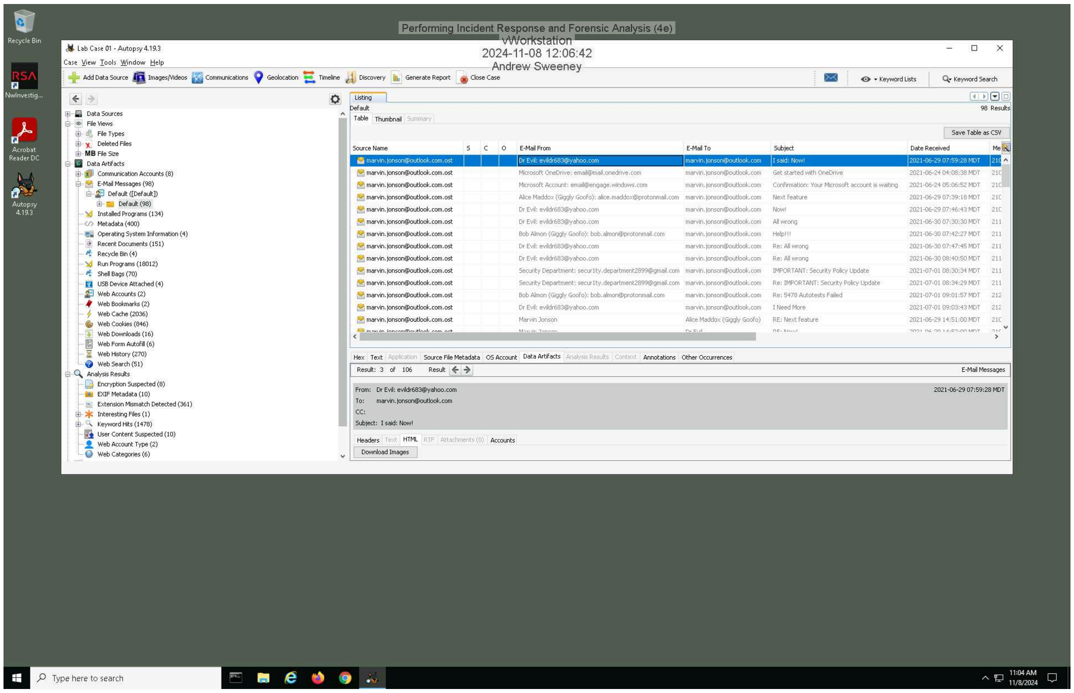
Define the following: Names and job titles of the affected users.

Marvin Jonson

Section 2: Applied Learning

Part 1: Identify Additional Email Evidence

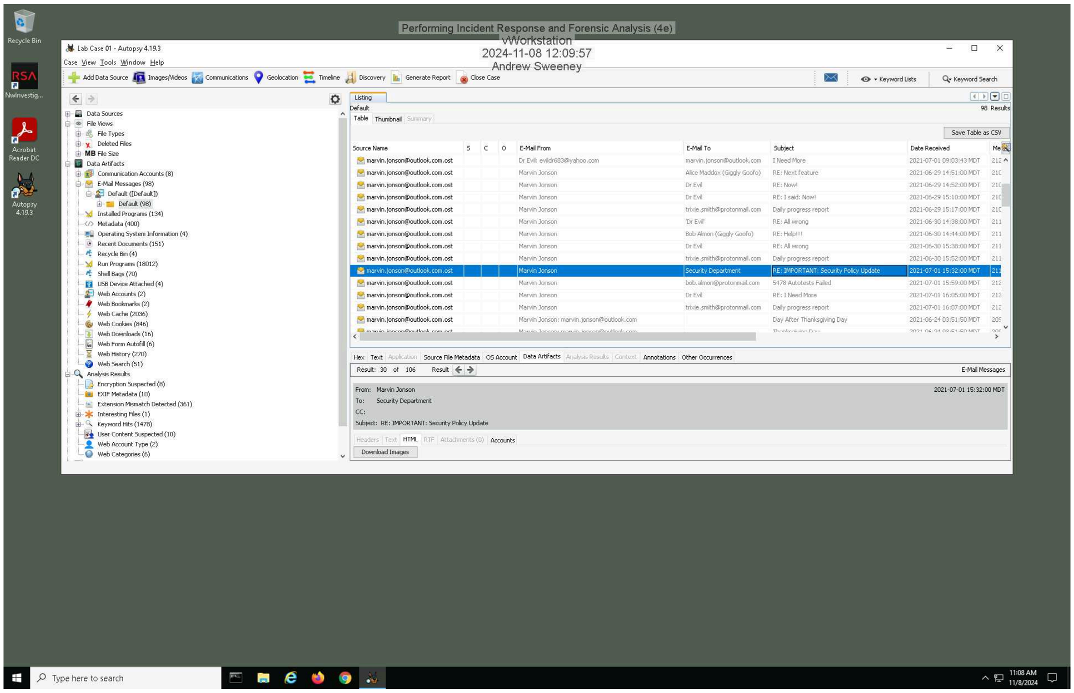
5. **Make a screen capture** showing the **email from Dr. Evil demanding that Marvin install a keylogger**.



Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Me
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	I said: Now!	2021-06-29 07:59:28 MDT	210
marvin.jonson@outlook.com.ost				Microsoft OneDrive: email@mail.onedrive.com	marvin.jonson@outlook.com	Get started with OneDrive	2021-06-24 04:08:38 MDT	210
marvin.jonson@outlook.com.ost				Microsoft Account: email@engage.windows.com	marvin.jonson@outlook.com	Confirmation: Your Microsoft account is waiting	2021-06-24 05:06:52 MDT	210
marvin.jonson@outlook.com.ost				Alice Maddox (Giggly Goofo): alice.maddox@protonmail.com	marvin.jonson@outlook.com	Next feature	2021-06-29 07:39:18 MDT	210
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	Now!	2021-06-29 07:46:43 MDT	210
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	All wrong	2021-06-30 07:30:30 MDT	211
marvin.jonson@outlook.com.ost				Bob Almon (Giggly Goofo): bob.almon@protonmail.com	marvin.jonson@outlook.com	Help!!!	2021-06-30 07:42:27 MDT	211
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	Re: All wrong	2021-06-30 07:47:45 MDT	211
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	Re: All wrong	2021-06-30 08:40:50 MDT	211
marvin.jonson@outlook.com.ost				Security Department: secur1ty.department2899@gmail.com	marvin.jonson@outlook.com	IMPORTANT: Security Policy Update	2021-07-01 08:30:34 MDT	211
marvin.jonson@outlook.com.ost				Security Department: secur1ty.department2899@gmail.com	marvin.jonson@outlook.com	Re: IMPORTANT: Security Policy Update	2021-07-01 08:34:29 MDT	211
marvin.jonson@outlook.com.ost				Bob Almon (Giggly Goofo): bob.almon@protonmail.com	marvin.jonson@outlook.com	Re: 5478 Autotests Failed	2021-07-01 09:01:57 MDT	212
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	I Need More	2021-07-01 09:03:43 MDT	212
marvin.jonson@outlook.com.ost				Marvin Jonson	Alice Maddox (Giggly Goofo)	RE: Next feature	2021-06-29 14:51:00 MDT	210

From: Dr Evil: evildr683@yahoo.com 2021-06-29 07:59:28 MDT
To: marvin.jonson@outlook.com
CC:
Subject: I said: Now!

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
2024-11-08 12:09:57
Andrew Sweeney

Lab Case 01 - Autopsy 4.19.3

Listing — Default — 98 Results

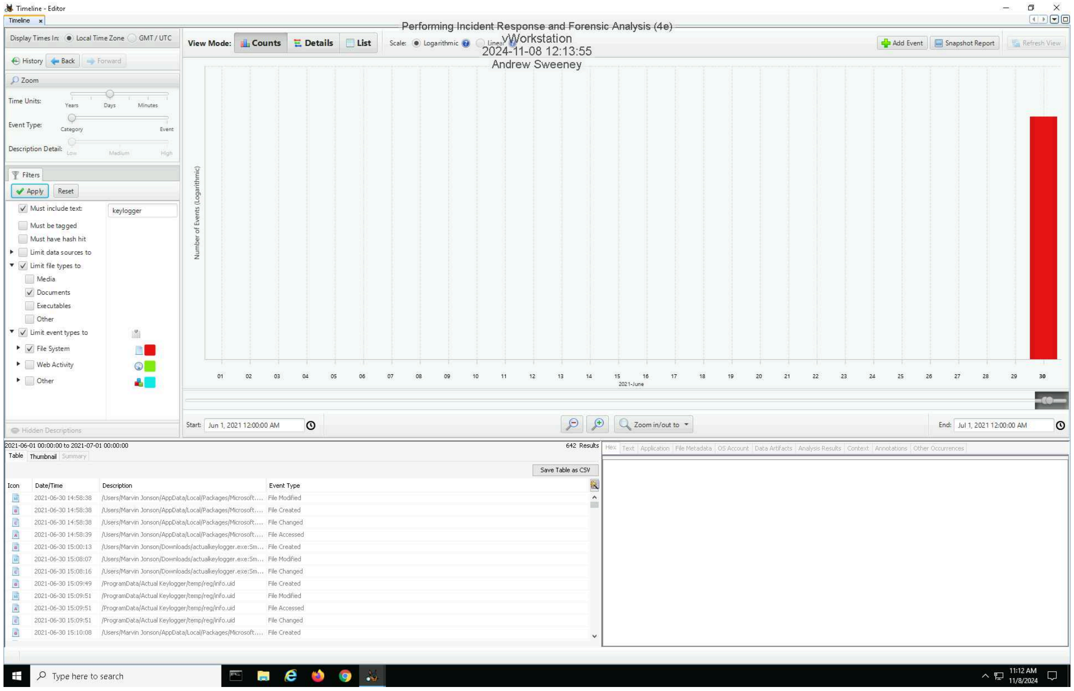
Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Me
marvin.jonson@outlook.com.ost				Dr Evil: evildr683@yahoo.com	marvin.jonson@outlook.com	I Need More	2021-07-01 09:03:43 MDT	212
marvin.jonson@outlook.com.ost				Marvin Jonson	Alice Maddox (Giggly Goofo)	RE: Next feature	2021-06-29 14:51:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	Dr Evil	RE: Now!	2021-06-29 14:52:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	Dr Evil	RE: I said: Now!	2021-06-29 15:10:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	trixie.smith@protonmail.com	Daily progress report	2021-06-29 15:17:00 MDT	210
marvin.jonson@outlook.com.ost				Marvin Jonson	'Dr Evil'	RE: All wrong	2021-06-30 14:38:00 MDT	211
marvin.jonson@outlook.com.ost				Marvin Jonson	Bob Almon (Giggly Goofo)	RE: Help!!!	2021-06-30 14:44:00 MDT	211
marvin.jonson@outlook.com.ost				Marvin Jonson	Dr Evil	RE: All wrong	2021-06-30 15:38:00 MDT	211
marvin.jonson@outlook.com.ost				Marvin Jonson	trixie.smith@protonmail.com	Daily progress report	2021-06-30 15:52:00 MDT	211
marvin.jonson@outlook.com.ost				Marvin Jonson	Security Department	RE: IMPORTANT: Security Policy Update	2021-07-01 15:32:00 MDT	211
marvin.jonson@outlook.com.ost				Marvin Jonson	bob.almon@protonmail.com	5478 Autotests Failed	2021-07-01 15:59:00 MDT	212
marvin.jonson@outlook.com.ost				Marvin Jonson	Dr Evil	RE: I Need More	2021-07-01 16:05:00 MDT	212
marvin.jonson@outlook.com.ost				Marvin Jonson	trixie.smith@protonmail.com	Daily progress report	2021-07-01 16:07:00 MDT	212
marvin.jonson@outlook.com.ost				Marvin Jonson: marvin.jonson@outlook.com		Day After Thanksgiving Day	2021-06-24 03:51:50 MDT	209

Result: 30 of 106 — E-Mail Messages

From: Marvin Jonson — 2021-07-01 15:32:00 MDT
To: Security Department
CC:
Subject: RE: IMPORTANT: Security Policy Update

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
2024-11-08 12:13:55
Andrew Sweeney

Timeline - Editor

View Mode: Counts — Scale: Logarithmic

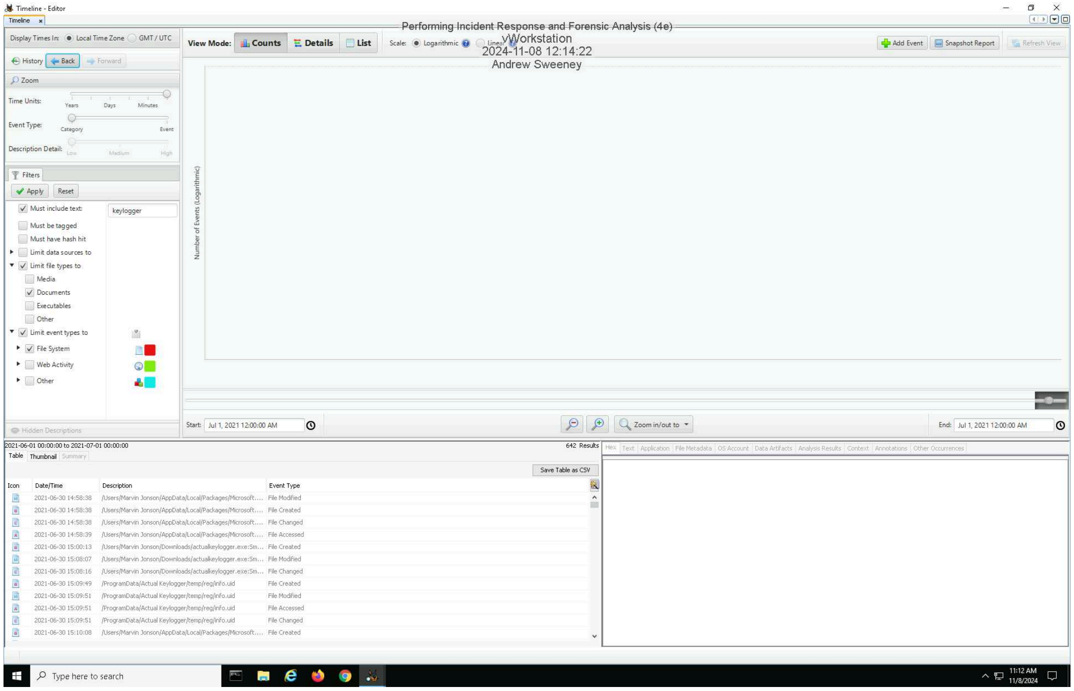
Must include text: keylogger

Start: Jun 1, 2021 12:00:00 AM — End: Jul 1, 2021 12:00:00 AM

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

Icon	Date/Time	Description	Event Type
M	2021-06-30 14:58:38	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Modified
B	2021-06-30 14:58:38	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Created
C	2021-06-30 14:58:38	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Changed
A	2021-06-30 14:58:39	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Accessed
B	2021-06-30 15:00:13	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Created
M	2021-06-30 15:08:07	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Modified
C	2021-06-30 15:08:16	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Changed
B	2021-06-30 15:09:49	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Created
M	2021-06-30 15:09:51	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Modified
A	2021-06-30 15:09:51	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Accessed
C	2021-06-30 15:09:51	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Changed
B	2021-06-30 15:10:08	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Created

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
2024-11-08 12:14:22
Andrew Sweeney

Timeline - Editor

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

View Mode: Counts Details List   Scale: ● Logarithmic ○ Linear

Filters

☑ Must include text: keylogger
☐ Must be tagged
☐ Must have hash hit
☐ Limit data sources to
☑ Limit file types to
☐ Media
☑ Documents
☐ Executables
☐ Other
☑ Limit event types to
☑ File System
☐ Web Activity
☐ Other

Start: Jul 1, 2021 12:00:00 AM   End: Jul 1, 2021 12:00:00 AM

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

Icon	Date/Time	Description	Event Type
M	2021-06-30 14:58:38	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Modified
B	2021-06-30 14:58:38	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Created
C	2021-06-30 14:58:38	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Changed
A	2021-06-30 14:58:39	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Accessed
B	2021-06-30 15:00:13	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Created
M	2021-06-30 15:08:07	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Modified
C	2021-06-30 15:08:16	/Users/Marvin Jonson/Downloads/actualkeylogger.exe:Sm...	File Changed
B	2021-06-30 15:09:49	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Created
M	2021-06-30 15:09:51	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Modified
A	2021-06-30 15:09:51	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Accessed
C	2021-06-30 15:09:51	/ProgramData/Actual Keylogger/temp/reg/info.uid	File Changed
B	2021-06-30 15:10:08	/Users/Marvin Jonson/AppData/Local/Packages/Microsoft....	File Created

11:12 AM
11/8/2024

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

2021-06-30 14:58:38

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

21-06-30 22:00:58

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

Based on the times I would say that Martin did not open the keyloggerr and it was the hacker open the keylogger on martins device

Part 3: Update an Incident Response Report

Date

Insert current date here.

11/08/2024

Name

Insert your name here.

Andrew sweeney

Incident Priority

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

Medium

Incident Type

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

Malware

Incident Timeline

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

2021-06-30

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

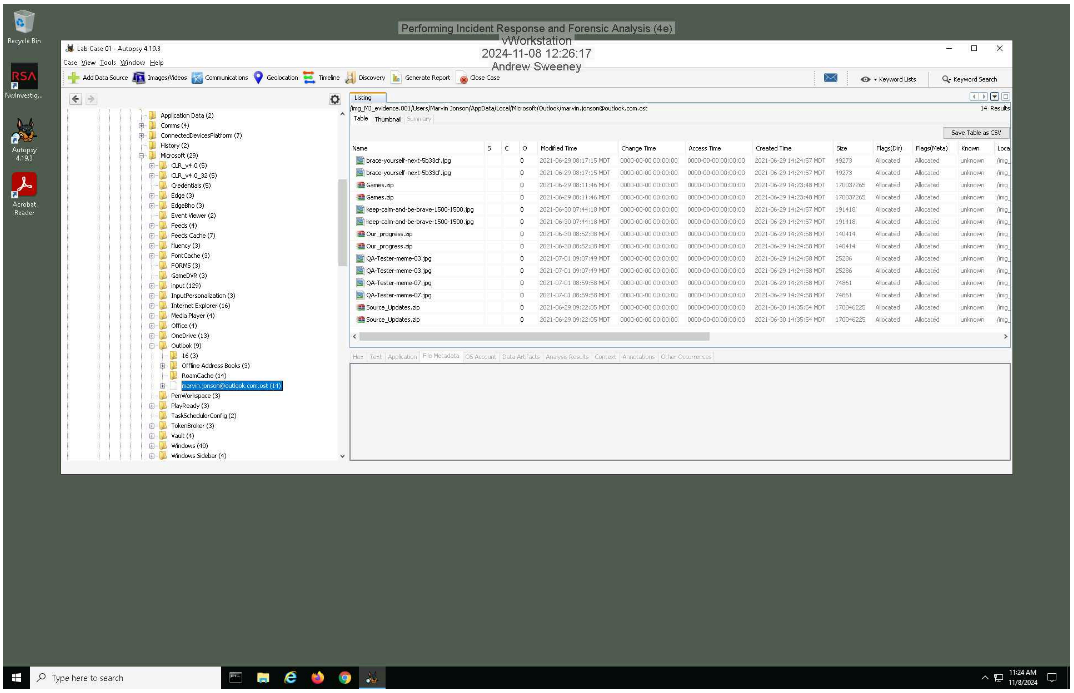
Has the list of users affected changed? If so, define any new users or new information. Otherwise, state that it is unchanged.

Marvin Jonson

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**.

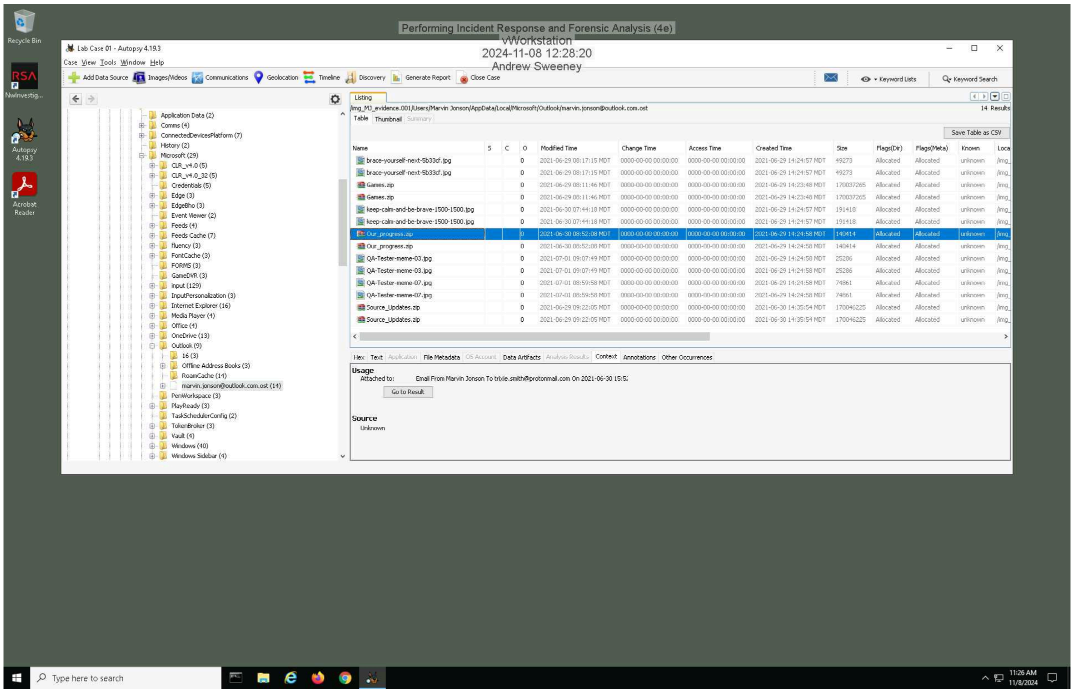


/img_MJ_evidence.001/Users/Marvin Jonson/AppData/Local/Microsoft/Outlook/marvin.jonson@outlook.com.ost 14 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loca
brace-yourself-next-5b33cf.jpg			0	2021-06-29 08:17:15 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	49273	Allocated	Allocated	unknown	/img_
brace-yourself-next-5b33cf.jpg			0	2021-06-29 08:17:15 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	49273	Allocated	Allocated	unknown	/img_
Games.zip			0	2021-06-29 08:11:46 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:23:48 MDT	170037265	Allocated	Allocated	unknown	/img_
Games.zip			0	2021-06-29 08:11:46 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:23:48 MDT	170037265	Allocated	Allocated	unknown	/img_
keep-calm-and-be-brave-1500-1500.jpg			0	2021-06-30 07:44:18 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	191418	Allocated	Allocated	unknown	/img_
keep-calm-and-be-brave-1500-1500.jpg			0	2021-06-30 07:44:18 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	191418	Allocated	Allocated	unknown	/img_
Our_progress.zip			0	2021-06-30 08:52:08 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	140414	Allocated	Allocated	unknown	/img_
Our_progress.zip			0	2021-06-30 08:52:08 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	140414	Allocated	Allocated	unknown	/img_
QA-Tester-meme-03.jpg			0	2021-07-01 09:07:49 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	25286	Allocated	Allocated	unknown	/img_
QA-Tester-meme-03.jpg			0	2021-07-01 09:07:49 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	25286	Allocated	Allocated	unknown	/img_
QA-Tester-meme-07.jpg			0	2021-07-01 08:59:58 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	74861	Allocated	Allocated	unknown	/img_
QA-Tester-meme-07.jpg			0	2021-07-01 08:59:58 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	74861	Allocated	Allocated	unknown	/img_
Source_Updates.zip			0	2021-06-29 09:22:05 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-30 14:35:54 MDT	170046225	Allocated	Allocated	unknown	/img_
Source_Updates.zip			0	2021-06-29 09:22:05 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-30 14:35:54 MDT	170046225	Allocated	Allocated	unknown	/img_

Part 2: Identify Additional Evidence of Spyware

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



Performing Incident Response and Forensic Analysis (4e)
vWorkstation
2024-11-08 12:28:20
Andrew Sweeney

/img_MJ_evidence.001/Users/Marvin Jonson/AppData/Local/Microsoft/Outlook/marvin.jonson@outlook.com.ost

14 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loca
brace-yourself-next-5b33cf.jpg			0	2021-06-29 08:17:15 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	49273	Allocated	Allocated	unknown	/img_
brace-yourself-next-5b33cf.jpg			0	2021-06-29 08:17:15 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	49273	Allocated	Allocated	unknown	/img_
Games.zip			0	2021-06-29 08:11:46 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:23:48 MDT	170037265	Allocated	Allocated	unknown	/img_
Games.zip			0	2021-06-29 08:11:46 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:23:48 MDT	170037265	Allocated	Allocated	unknown	/img_
keep-calm-and-be-brave-1500-1500.jpg			0	2021-06-30 07:44:18 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	191418	Allocated	Allocated	unknown	/img_
keep-calm-and-be-brave-1500-1500.jpg			0	2021-06-30 07:44:18 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:57 MDT	191418	Allocated	Allocated	unknown	/img_
Our_progress.zip			0	2021-06-30 08:52:08 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	140414	Allocated	Allocated	unknown	/img_
Our_progress.zip			0	2021-06-30 08:52:08 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	140414	Allocated	Allocated	unknown	/img_
QA-Tester-meme-03.jpg			0	2021-07-01 09:07:49 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	25286	Allocated	Allocated	unknown	/img_
QA-Tester-meme-03.jpg			0	2021-07-01 09:07:49 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	25286	Allocated	Allocated	unknown	/img_
QA-Tester-meme-07.jpg			0	2021-07-01 08:59:58 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	74861	Allocated	Allocated	unknown	/img_
QA-Tester-meme-07.jpg			0	2021-07-01 08:59:58 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-29 14:24:58 MDT	74861	Allocated	Allocated	unknown	/img_
Source_Updates.zip			0	2021-06-29 09:22:05 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-30 14:35:54 MDT	170046225	Allocated	Allocated	unknown	/img_
Source_Updates.zip			0	2021-06-29 09:22:05 MDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2021-06-30 14:35:54 MDT	170046225	Allocated	Allocated	unknown	/img_

Usage
Attached to: Email From Marvin Jonson To trixie.smith@protonmail.com On 2021-06-30 15:5:

Source
Unknown

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

I was unable to find this in autospy software