Division of Information Technology & Sciences
Department of Computer & Digital Forensics
FOR 120 – Introduction to Digital Forensics

Final Exam, 2022 Fall

Final Project

Notes:

1. The project is two parts and this document contains the first part, which is 5 pages.
2. You are required to provide screenshots of any step you have performed. Screenshots should clearly show any step used and its results. This could be done using a tool such as the “Snip and Sketch” tool, to highlight your work.
3. A thorough explanation and analysis are required to demonstrate your understanding of all steps that you performed.
4. Use any tool you like - open source or commercial.

Overview

You are helping in investigating a Windows machine of a suspect, which can be found here. We need to prove if the suspect did/didn't use the device to connect to another device.

Please analyze the provided image and answer the following questions. You are free to use any forensic (or other) software but please indicate what software you have used and provide some details about it (version, name, company, etc).

When providing answers to questions:

- You must list the file and/or forensic artifacts where you got your answers along with information about those files (metadata) such as dates & times, file size, location, etc. that will fully describe it.
- Explain how you found this information.
- The information should be precise and there must be enough information so that your work can be reproduced by another expert who may not have access to the same tool(s) you do! If you don't do this, you will lose major points!

The main investigator on this case will use your responses as is and paste them into a formal report. Answer questions professionally with full sentences, adequate explanations, and pretty tables of data (and metadata). Use proper screenshots (the text in it must be clear) and tables for the explanation.

For your deliverable, please submit a formal report that answers the client's questions (in order and numbered as such). Since this is not the Final report, you DO NOT need to include a Table of Contents, Introduction, Evidence intake, Conclusion or Signature section. However, you DO need to list your tools and then answer the questions with explanations and analysis (as described in the above paragraphs). For each question, please write out the question, then the answer. Use the exact same question numbers.

BASIC EVIDENCE INFORMATION

Please answer the following questions about the disk images:

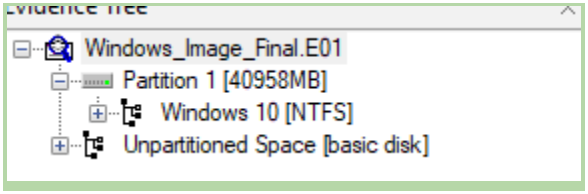
1. What is the case number of this investigation?

   This is case #008 and to find this, I used the provided txt file description of the case.

```
Case Information:
Acquired using: ADI4.7.1.2
Case Number: 008
```

2. How many partitions are present in the image?

   There is only 1 partition of this image which was found using FTK Imager.



3. What is the SHA1 hash of the forensic image given?

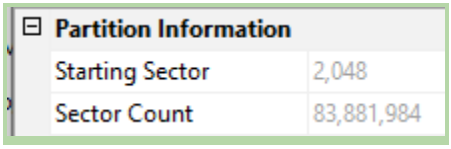
   The SHA1 hash is 2a1a01d105b64ac09d3c86801c75d3ef59381c26 and I used the provided txt file description of the case.

```
Image Verification Results:
 Verification started:  Mon Dec  5 10:52:23 2022
 Verification finished: Mon Dec  5 10:55:09 2022
 MD5 checksum:    d90029b9ccc9523fcb89051a947eb2dd : verified
 SHA1 checksum:   2a1a01d105b64ac09d3c86801c75d3ef59381c26 : verified
```

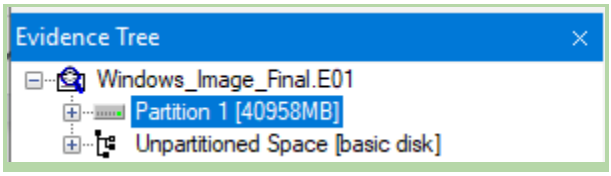
4. At what sector does the Windows partition start?

   Using FTK Imager, under properties, it shows that the sector when the

Windows partition starts is at 2,048.



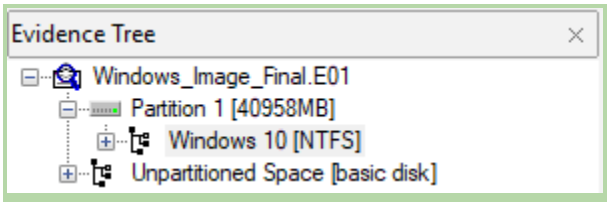
5. How large is the Windows partition in MB?



Found in FTK Imager, it displays that the size of the partition is 40,958 MB.

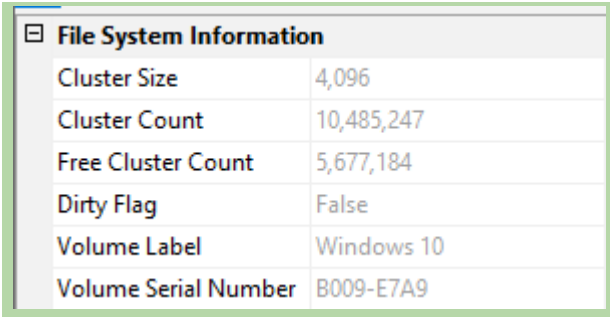
6. What file system is used for the windows partition?

Found in FTK Imager, the file system of the partition is NTFS.



7. What is the short volume serial number of the windows partition?

Using FTK Imager, under properties, it shows that the short volume serial number of the windows partition is B009-E7A9.



INVESTIGATION

Investigate the images and answer these questions.

1. What is the user name and SID of the suspect's windows user account?

   Using Axiom Examine I created a new case and began to process the image. Under the operating systems tab, I viewed the windows user accounts and found both the user name and SID of the windows account, highlighted below.

		Built-in	S-1-5-20		%systemroot%\ServicePro
		Built-in	S-1-5-18		%systemroot%\system32\
sshd	sshd	Local User	1002	1002	
DefaultAccount		Local User	503	503	
IEUser	IEUser	Local User	S-1-5-21-321011808-3761883066-353627080-1000	1000	C:\Users\IEUser
Guest		Local User	501	501	
		Built-in	S-1-5-19		%systemroot%\ServicePro
WDAGUtilityAccount		Local User	504	504	
Administrator		Local User	500	500	

   Profile Path **C:\Users\IEUser**

2. What programs were installed on the Windows machine, when were they installed, and what was the program's source? Provide a listing or a table with this information.

   Still using Axiom, I was able to navigate from Application usage to Installed programs and found 7 programs that were installed on the windows machine.

   7-Zip does not have a creation date, interestingly enough, but the last time the key was updated was the same time that google chrome was created.

   12/4/2022 12/4/2022 2:46:09 PM

   Google Chrome was created 12/4/2022. 12/4/2022

Puppet was created on 3/19/2019, which seems to be incredibly early compared to the other programs. 3/19/2019

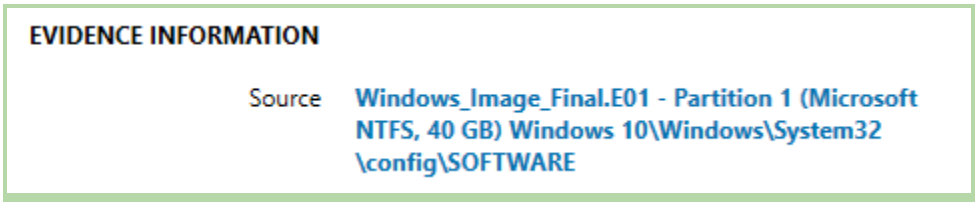
PuTTY was created 12/4/2022. 12/4/2022

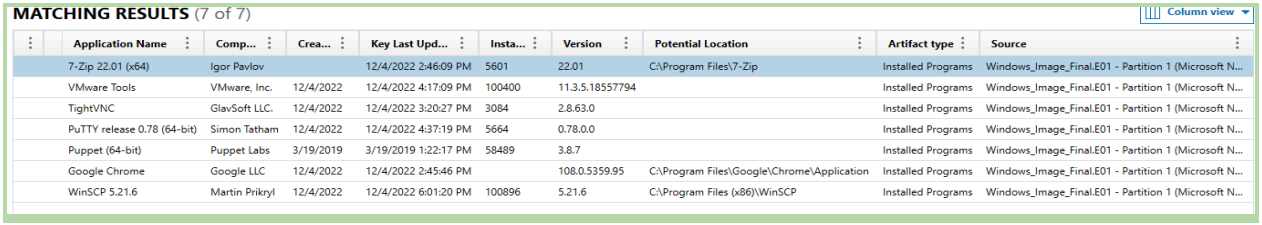
TightVNC was created 12/4/2022. 12/4/2022

VMware Tools was created 12/4/2022. 12/4/2022

WinSCP was created 12/4/2022 12/4/2022

All the sources of the programs are found under the evidence information of the applications and they are all the same as seen below.





Application Name	Comp...	Crea...	Key Last Upd...	Insta...	Version	Potential Location	Artifact type	Source
7-Zip 22.01 (x64)	Igor Pavlov		12/4/2022 2:46:09 PM	5601	22.01	C:\Program Files\7-Zip	Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...
VMware Tools	VMware, Inc.	12/4/2022	12/4/2022 4:17:09 PM	100400	11.3.5.18557794		Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...
TightVNC	GlavSoft LLC.	12/4/2022	12/4/2022 3:20:27 PM	3084	2.8.63.0		Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...
PuTTY release 0.78 (64-bit)	Simon Tatham	12/4/2022	12/4/2022 4:37:19 PM	5664	0.78.0.0		Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...
Puppet (64-bit)	Puppet Labs	3/19/2019	3/19/2019 1:22:17 PM	58489	3.8.7		Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...
Google Chrome	Google LLC	12/4/2022	12/4/2022 2:45:46 PM		108.0.5359.95	C:\Program Files\Google\Chrome\Application	Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...
WinSCP 5.21.6	Martin Prikryl	12/4/2022	12/4/2022 6:01:20 PM	100896	5.21.6	C:\Program Files (x86)\WinSCP	Installed Programs	Windows_Image_Final.E01 - Partition 1 (Microsoft N...

3. Mention any suspicious executable that was downloaded on this machine? Explain why they are suspicious.

Firstly, I looked through Axiom's walware/phising urls and was able to find these 7 links. Although these were not executables, these links each contain between 100 and 1000 malicious files which would be executables then.

MATCHING RESULTS (7 of 7)

Column view

Site...	URL	Date...	Artifact	Artif...	Artifact type	Source
	http://fewfwe.net/		Potential Browser Activity	40	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa
	http://blufda.com/		Potential Browser Activity	85	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa
	http://cts.hotbar.com/trackedevent.aspx		Potential Browser Activity	109	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa
	http://ad.eltext.com		Potential Browser Activity	120	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa
	http://www.drgeorges.com/info/sh		Potential Browser Activity	137	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa
	http://rep4.upseek.org/?r2=launc1|http://		Potential Browser Activity	143	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa
	http://ge.tt/		Potential Browser Activity	176	Malware/Phishing URLs	Windows_Image_Final.E01 - Pa

Looking a little deeper, I went back to the installed programs found on this windows image and looked at the actual programs themselves.

MATCHING RESULTS (7 of 7)

Application Na...	Comp...
7-Zip 22.01 (x64)	Igor Pavlov
Google Chrome	Google LLC
Puppet (64-bit)	Puppet Labs
PuTTY release 0.78 (64-bit)	Simon Tatham
TightVNC	GlavSoft LLC.
VMware Tools	VMware, Inc.
WinSCP 5.21.6	Martin Prikryl

Looking into Puppet, it seems to be an application used by system admins that installs and configures servers. Maybe a little suspicious, unless the company works with that.

Looking at more of the executables that this windows machine has, it seems as though they were downloading executables that dealt with file transfers. As in file transfers from one server to another as if they were trying to transfer file/s away from a windows machine off to another domain. That would describe why they have applications like PuTTY and WinSCP, which is definitely suspicious.

4. List out all web browser searches conducted by the suspect, and highlight any relevant ones. Don't forget to list out the dates and times of the searches.

   By looking at the suspect's web searches, I am able to discover that they seem to prefer using Google over any other browser unless it was to install PuTTy, which they used Microsoft edge for that. However, their searches make a perfect timeline of their entire suspicious history on this windows machine.

   Here are the google searches that were conducted by the suspect along with the dates and times of searches:

MATCHING RESULTS (96 of 96)

Column view

URL	Last Visite...	Title	Visit...	Type...	Artif
https://www.google.com/search?q=tightvncserver&...	12/4/2022 3:19:58 PM	tightvncserver - Google Search	2	0	Chron
https://www.tightvnc.com/download.php	12/4/2022 3:20:02 PM	Download TightVNC	1	0	Chron
https://www.google.com/search?q=send+files+rem...	12/4/2022 4:34:36 PM	send files remotely from linux to windows - Google...	2	0	Chron
https://www.google.com/search?q=writing+stories...	12/4/2022 4:34:51 PM	writing stories for hollywood - Google Search	2	0	Chron
https://www.writersdigest.com/write-better-fiction/t...	12/4/2022 4:34:53 PM	Take Two: Ways to Submit Your Story to Hollywood -...	1	0	Chron
https://www.freelancewriting.com/screenwriting/ho...	12/4/2022 4:34:56 PM	How to Pitch Your Story Idea or Script to Hollywood...	1	0	Chron
https://www.theatlantic.com/magazine/archive/194...	12/4/2022 4:34:58 PM	Raymond Chandler on the Struggles of Hollywood...	2	0	Chron
https://screencraft.org/blog/how-to-write-a-novel-t...	12/4/2022 4:34:59 PM	How to Write a Novel That Hollywood Wants to Get...	1	0	Chron
https://www.studiobinder.com/blog/best-screenwrit...	12/4/2022 4:34:59 PM	15 Best Screenwriting Books to Help You Break Into...	1	0	Chron
https://www.google.com/search?q=learn+writing&r...	12/4/2022 4:35:04 PM	learn writing - Google Search	2	0	Chron
https://www.google.com/search?q=learn+writing+s...	12/4/2022 4:35:08 PM	learn writing stories - Google Search	2	0	Chron
https://www.grammarly.com/blog/how-to-write-a-s...	12/4/2022 4:35:15 PM	How to Write a Great Story in 5 Steps | Grammarly	1	0	Chron
https://www.masterclass.com/articles/complete-gui...	12/4/2022 4:35:17 PM	How to Write a Story In 6 Steps: A Complete Step-B...	2	0	Chron
https://www.liveabout.com/how-to-write-fiction-12...	12/4/2022 4:35:18 PM	Learn How to Write Fiction	1	0	Chron
https://thewritepractice.com/write-story/	12/4/2022 4:35:19 PM	How to Write a Story: The 10 Best Secrets	1	0	Chron
https://www.google.com/search?q=best+story+seri...	12/4/2022 4:35:34 PM	best story series podcasts - Google Search	2	0	Chron
https://www.google.com/search?q=best+story+seri...	12/4/2022 4:35:37 PM	best story series - Google Search	2	0	Chron
https://mydramalist.com/700551-the-best-story	12/4/2022 4:35:40 PM	The Best Story (2021) - MyDramaList	1	0	Chron
https://www.imdb.com/list/ls051291882/	12/4/2022 4:35:43 PM	Top 10 Tv Series with best storylines - IMDb	2	0	Chron
https://blwatcher.com/bl-series/the-best-story-dra...	12/4/2022 4:35:43 PM	The Best Story - BL Series Review | Plot, Cast, Ending...	1	0	Chron
https://www.themoviedb.org/tv/128924?language=...	12/4/2022 4:35:44 PM	The Best Story (TV Series 2021-2021) — The Movie...	1	0	Chron
https://www.imdb.com/title/tt21098268/	12/4/2022 4:35:46 PM	The Best Story (TV Mini Series 2021) - IMDb	1	0	Chron
https://www.quora.com/What-TV-series-have-great...	12/4/2022 4:35:48 PM	What TV series have great storylines? - Quora	2	0	Chron
https://www.google.com/search?q=download+putt...	12/4/2022 4:36:55 PM	download putty - Google Search	2	0	Chron
https://www.putty.org/	12/4/2022 4:36:56 PM	Download PuTTY - a free SSH and telnet client for...	1	0	Chron
https://www.digitalcitizen.life/hide-files-folders-win...	12/4/2022 5:21:16 PM	How to hide files and folders in Windows - Digital Ci...	2	0	Chron
https://winbuzzer.com/2021/06/24/how-to-hide-an...	12/4/2022 5:21:16 PM	How to Hide and Unhide Folders and Files on Wind...	1	0	Chron
http://www.filefriend.net/#FileFriend	12/4/2022 5:25:18 PM	FileFriend	2	0	Chron
https://www.google.com/search?q=pexel+images&...	12/4/2022 5:25:25 PM	pexel images - Google Search	2	0	Chron
https://www.pexels.com/	12/4/2022 5:25:27 PM	Free Stock Photos, Royalty Free Stock Images & Cop...	2	0	Chron
https://www.pexels.com/photo/lemon-fruit-on-top-...	12/4/2022 5:25:36 PM	Lemon Fruit on Top of a Melon · Free Stock Photo	2	0	Chron

MATCHING RESULTS (96 of 96)

Column view

URL	Last Visite...	Title	Visit...	Type...	Artif
https://www.google.com/search?q=pexel+images&...	12/4/2022 5:25:25 PM	pexel images - Google Search	2	0	Chron
https://www.pexels.com/	12/4/2022 5:25:27 PM	Free Stock Photos, Royalty Free Stock Images & Cop...	2	0	Chron
https://www.pexels.com/photo/lemon-fruit-on-top-...	12/4/2022 5:25:36 PM	Lemon Fruit on Top of a Melon · Free Stock Photo	2	0	Chron
https://www.pexels.com/photo/yellow-flowers-in-gl...	12/4/2022 5:25:46 PM	Yellow Flowers in Glass Vase · Free Stock Photo	2	0	Chron
https://www.pexels.com/photo/green-potted-plants...	12/4/2022 5:25:51 PM	Green Potted Plants on Table · Free Stock Photo	2	0	Chron
https://www.pexels.com/photo/a-plate-of-a-slice-of...	12/4/2022 5:26:01 PM	A Plate of a Slice of Cheesecake beside Tulips · Free...	2	0	Chron
https://www.pexels.com/photo/brown-and-white-fr...	12/4/2022 5:26:06 PM	Brown and White French Macaroons on Ceramic Pla...	2	0	Chron
https://www.pexels.com/photo/grayscale-photo-of-...	12/4/2022 5:26:18 PM	Grayscale Photo of Sea Waves · Free Stock Photo	2	0	Chron
https://www.pexels.com/photo/grayscale-photo-of-...	12/4/2022 5:26:21 PM	Grayscale Photo of Mountains under the Sky · Free S...	2	0	Chron
http://gmail.com/	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	0	Chron
https://gmail.com/	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	1	Chron
https://www.google.com/gmail/	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	0	Chron
https://accounts.google.com/ServiceLogin?service=...	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	0	Chron
https://mail.google.com/intl/en/mail/help/about.html	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	0	Chron
https://www.google.com/intl/en/mail/help/about.ht...	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	0	Chron
https://www.google.com/gmail/about/	12/4/2022 5:31:05 PM	Gmail: Private and secure email at no cost | Google...	1	0	Chron
https://accounts.google.com/AccountChooser/signi...	12/4/2022 5:31:44 PM	Gmail	1	0	Chron
https://accounts.google.com/AccountChooser?servi...	12/4/2022 5:31:44 PM	Gmail	1	0	Chron
https://accounts.google.com/ServiceLogin?continue...	12/4/2022 5:31:44 PM	Gmail	1	0	Chron
https://accounts.google.com/v3/signin/identifier?ds...	12/4/2022 5:31:44 PM	Gmail	2	0	Chron
https://accounts.google.com/v3/signin/challenge/p...	12/4/2022 5:32:02 PM	Gmail	1	0	Chron
https://accounts.google.com/speedbump/gaplustos...	12/4/2022 5:32:11 PM	Google Accounts	1	0	Chron
https://accounts.google.com/speedbump/changepa...	12/4/2022 5:32:14 PM	Change Password	1	0	Chron
https://accounts.google.com/speedbump/changepa...	12/4/2022 5:32:20 PM	Change Password	1	0	Chron
https://mail.google.com/mail/	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	2	0	Chron
https://mail.google.com/mail/u/0/	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	2	0	Chron
https://accounts.google.com/CheckCookie?continue...	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0	Chron
https://mail.google.com/accounts/SetOSID?authuse...	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0	Chron
https://accounts.youtube.com/accounts/SetSID?ssdc...	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0	Chron
https://www.google.com/search?q=facebook&rlz=1...	12/4/2022 5:33:01 PM	facebook - Google Search	2	0	Chron
https://www.facebook.com/?__req=a	12/4/2022 5:34:30 PM	Facebook	1	0	Chron

MATCHING RESULTS (96 of 96)

Column view

URL	Last Visite...	Title	Visit...	Type...	Artif
https://www.facebook.com/confirmemail.php?next=...	12/4/2022 5:34:30 PM	Facebook	1	0	Chron
https://mail.google.com/mail/u/0/#inbox/FMfcgzGr...	12/4/2022 5:34:41 PM	Security alert - scarter@eandt.one - EandT One Mail	1	0	Chron
https://www.facebook.com/friends	12/4/2022 5:36:04 PM	(1) Friends | Facebook	1	0	Chron
https://www.facebook.com/	12/4/2022 5:36:06 PM	(1) Facebook	5	0	Chron
https://www.facebook.com/search/top/?q=pbrooks...	12/4/2022 5:36:08 PM	(1) pbrooks@andt.one - Search Results | Facebook	1	0	Chron
https://www.facebook.com/search/top/?q=penelop...	12/4/2022 5:36:26 PM	penelope brooks - Search Results | Facebook	1	0	Chron
https://www.facebook.com/profile.php?id=1000678...	12/4/2022 5:36:39 PM	Penelope Brook | Facebook	2	0	Chron
https://www.facebook.com/profile.php?id=1000860...	12/4/2022 5:36:40 PM	(1) Penelope Brooks | Facebook	2	0	Chron
https://www.facebook.com/profile.php?id=1000881...	12/4/2022 5:37:13 PM	Sophie Carter | Facebook	1	0	Chron
https://www.chiark.greenend.org.uk/~sgtatham/put...	12/4/2022 5:38:55 PM	Download PuTTY: latest release (0.78)	1	0	Chron
https://www.google.com/search?q=how+to+hide+f...	12/4/2022 5:38:56 PM	how to hide files in windows 10 - Google Search	2	0	Chron
https://www.makeuseof.com/tag/hide-files-folders-...	12/4/2022 5:38:57 PM	How to Hide Files, Folders, and Drives in Windows 10	1	0	Chron
https://www.google.com/search?q=winscp&rlz=1C1...	12/4/2022 6:00:37 PM	winscp - Google Search	2	0	Chron
https://winscp.net/eng/index.php	12/4/2022 6:00:49 PM	WinSCP :: Official Site :: Free SFTP and FTP client for...	1	0	Chron
https://winscp.net/eng/download.php	12/4/2022 6:00:52 PM	WinSCP :: Official Site :: Download	1	0	Chron
https://winscp.net/download/WinSCP-5.21.6-Setup....	12/4/2022 6:00:56 PM	Downloading WinSCP-5.21.6-Setup.exe :: WinSCP	1	0	Chron
https://mail.google.com/mail/u/0/#inbox/FMfcgzGr...	12/4/2022 6:04:56 PM	FB-16467 is your Facebook confirmation code - scar...	1	0	Chron
https://mail.google.com/mail/u/0/#inbox/FMfcgzGr...	12/4/2022 6:05:11 PM	FB-16467 is your Facebook confirmation code - scar...	1	0	Chron
https://mail.google.com/mail/u/0/#inbox/FMfcgzGr...	12/4/2022 6:05:43 PM	FB-16467 is your Facebook confirmation code - scar...	2	0	Chron
https://mail.google.com/mail/u/0/#inbox/KtbxLxglq...	12/4/2022 6:23:44 PM	Glance on the Draft - scarter@eandt.one - EandT O...	1	0	Chron
https://mail.google.com/mail/u/0/#inbox?compose...	12/4/2022 6:25:51 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0	Chron
https://www.google.com/search?q=delete+file+per...	12/4/2022 6:28:04 PM	delete file perminantely - Google Search	2	0	Chron
https://mail.google.com/mail/u/0/#inbox?compose...	12/4/2022 6:32:07 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0	Chron
https://mail.google.com/mail/u/0/#inbox?compose...	12/4/2022 6:32:57 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	3	0	Chron
https://mail.google.com/mail/u/0/#inbox?compose...	12/4/2022 6:32:58 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0	Chron
https://mail.google.com/mail/u/0/#inbox	12/4/2022 6:33:56 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	7	0	Chron
https://www.google.com/search?q=amazon&rlz=1C...	12/4/2022 6:34:25 PM	amazon - Google Search	2	0	Chron
https://www.google.com/aclk?sa=l&ai=DChcSEwj87...	12/4/2022 6:34:27 PM	Amazon.com. Spend less. Smile more.	1	0	Chron
https://www.googleadservices.com/pagead/aclk?sa...	12/4/2022 6:34:27 PM	Amazon.com. Spend less. Smile more.	1	0	Chron
https://www.amazon.com/?tag=amazusnavi-20&hv...	12/4/2022 6:34:27 PM	Amazon.com. Spend less. Smile more.	1	0	Chron
https://www.amazon.com/s/ref=nb_sb_noss_1?url=s...	12/4/2022 6:34:35 PM	Amazon.com : super note	1	0	Chron

https://www.googleadservices.com/pagead/aclk?sa...	12/4/2022 6:34:27 PM	Amazon.com. Spend less. Smile more.	1	0	Chron
https://www.amazon.com/?tag=amazusnavi-20&hv...	12/4/2022 6:34:27 PM	Amazon.com. Spend less. Smile more.	1	0	Chron
https://www.amazon.com/s/ref=nb_sb_noss_1?url=s...	12/4/2022 6:34:35 PM	Amazon.com : super note	1	0	Chron
https://www.amazon.com/s?k=super+note&crid=3...	12/4/2022 6:34:36 PM	Amazon.com : super note	1	0	Chron
https://www.amazon.com/Samsung-Electronics-Unl...	12/4/2022 6:34:46 PM	Amazon.com: Samsung Electronics Galaxy Note 20 5...	2	0	Chron
https://www.avast.com/c-permanently-delete-files	12/4/2022 6:34:56 PM	How to Permanently Delete Files on Windows | Avast	1	0	Chron
https://www.makeuseof.com/tag/transfer-share-files...	12/4/2022 6:37:37 PM	How to Transfer and Share Files Between Windows a...	1	0	Chron
https://www.google.com/search?q=working+author...	12/4/2022 6:49:31 PM	working author tips - Google Search	2	0	Chron
https://www.thebookdesigner.com/13-tips-for-the-...	12/4/2022 6:49:33 PM	13 Tips for the Work-at-Home Author - The Book D...	1	0	Chron

Here is the history that Microsoft edge contains:

MATCHING RESULTS (126 of 126)

Column view

Entr...	URL	User	Accessed Dat...	Page Title	
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM		1
	https://login.live.com/oauth20_authorize.srf?client_i...	IEUser	12/4/2022 2:43:52 PM	Sign in to your Microsoft account	1
	https://www.msn.com/	IEUser	12/4/2022 2:44:09 PM		1
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM		1
	https://go.microsoft.com/fwlink/?LinkId=525773	IEUser	12/4/2022 2:44:10 PM		1
	https://go.microsoft.com/	IEUser	12/4/2022 2:44:10 PM		1
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM		1
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM	putty - Search	1
	https://www.bing.com/ck/a?!&&p=ffd93d158cef773...	IEUser	12/4/2022 4:34:03 PM		1
	https://putty.org/	IEUser	12/4/2022 4:34:04 PM		1
	https://putty.org꿀펙□v	IEUser	12/4/2022 4:34:04 PM		1
	file:///C:/Users/IEUser/Desktop/data	IEUser	12/4/2022 5:19:55 PM		1
	file:///C:/Users/IEUser/Desktop	IEUser	12/4/2022 5:19:55 PM		1
	file:///C:/Users/IEUser/Desktop/data/password.txt	IEUser	12/4/2022 5:20:10 PM		1
	file:///C:/Users/IEUser/Downloads/YellowHearts.jpg	IEUser	12/4/2022 6:27:00 PM		1
	file:///C:/Users/IEUser/Desktop/LastSceneMountains...	IEUser	12/4/2022 6:27:27 PM		1
	file:///C:/Users/IEUser/Downloads/pexels-yelena-odi...	IEUser	12/4/2022 5:27:39 PM		1
	file:///C:/Users/IEUser/Downloads/pexels-polina-kov...	IEUser	12/4/2022 5:27:49 PM		1
	file:///C:/Users/IEUser/Downloads/pexels-nati-96342...	IEUser	12/4/2022 5:28:41 PM		1
	file:///C:/Users/IEUser/Downloads/drafts	IEUser	12/4/2022 6:25:39 PM		1
	file:///C:/Users/IEUser/Downloads	IEUser	12/4/2022 6:25:39 PM		1
4	https://login.live.com/oauth20_authorize.srf?client_i...	IEUser	12/4/2022 2:43:52 PM	Sign in to your Microsoft account	1
14	file:///C:/Users/IEUser/Desktop/LastSceneMountains...	IEUser	12/4/2022 6:27:27 PM		1
5	file:///C:/Users/IEUser/Desktop/data	IEUser	12/4/2022 5:19:55 PM		1
9	file:///C:/Users/IEUser/Downloads/pexels-polina-kov...	IEUser	12/4/2022 5:27:49 PM		1
13	file:///C:/Users/IEUser/Downloads/YellowHearts.jpg	IEUser	12/4/2022 6:27:00 PM		1
10	file:///C:/Users/IEUser/Downloads/pexels-nati-96342...	IEUser	12/4/2022 5:28:41 PM		1
7	file:///C:/Users/IEUser/Desktop/data/password.txt	IEUser	12/4/2022 5:20:10 PM		1
12	file:///C:/Users/IEUser/Downloads	IEUser	12/4/2022 6:25:39 PM		1
6	file:///C:/Users/IEUser/Desktop	IEUser	12/4/2022 5:19:55 PM		1
8	file:///C:/Users/IEUser/Downloads/pexels-yelena-odi...	IEUser	12/4/2022 5:27:39 PM		1

23	https://putty.org/	IEUser	12/4/2022 4:34:04 PM		1
11	https://dl.google.com/tag/s/appguid%3D%7B8A69...	IEUser	12/4/2022 2:44:54 PM		1
13	https://dl.google.com/tag/s/appguid%3D%7B8A69...	IEUser	12/4/2022 2:44:59 PM		1
18	https://www.7-zip.org/	IEUser	12/4/2022 2:45:28 PM		1
5	https://www.microsoft.com/	IEUser	12/4/2022 2:44:11 PM		1
1	https://www.msn.com/	IEUser	12/4/2022 2:44:09 PM		1
10	https://www.google.com/	IEUser	12/4/2022 2:44:48 PM		1
2	https://go.microsoft.com/fwlink/?LinkId=525773	IEUser	12/4/2022 2:44:10 PM		1
3	https://go.microsoft.com/	IEUser	12/4/2022 2:44:10 PM		1
10	https://www.bing.com/ck/a?!&&p=da3814efa2f704...	IEUser	12/4/2022 2:45:27 PM		1
13	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM	putty - Search	1
3	https://www.bing.com/aclk?ld=e8OQqckSvv-jmTim...	IEUser	12/4/2022 2:44:47 PM		1
15	https://www.bing.com/ck/a?!&&p=ffd93d158cef773...	IEUser	12/4/2022 4:34:03 PM		1
16	https://putty.org/	IEUser	12/4/2022 4:34:04 PM	Download PuTTY - a free SSH and telnet client for...	1
5	https://dl.google.com/tag/s/appguid%3D%7B8A69...	IEUser	12/4/2022 2:44:54 PM		1
7	https://dl.google.com/tag/s/appguid%3D%7B8A69...	IEUser	12/4/2022 2:44:59 PM		1
11	https://www.7-zip.org/download.html	IEUser	12/4/2022 2:45:29 PM	Download	1
1	https://www.microsoft.com/en-us/edge?form=MA1...	IEUser	12/4/2022 2:44:12 PM	Microsoft Edge	1
6	https://www.google.com/chrome/thank-you.html?b...	IEUser	12/4/2022 2:44:55 PM	Google Chrome Web Browser	1
8	https://www.google.com/chrome/thank-you.html?in...	IEUser	12/4/2022 2:45:01 PM	Google Chrome Web Browser	1
4	https://www.google.com/chrome/bsem/download/e...	IEUser	12/4/2022 2:44:49 PM	Google Chrome Web Browser	1
	file:///C:/Windows/system32/oobe/FirstLogonAnim....	IEUser	3/19/2019 1:00:18 PM		1
	https://login.live.com/oauth20_authorize.srf?client_i...	IEUser	12/4/2022 2:43:52 PM	Sign in to your Microsoft account	1
	file:///C:/Users/IEUser/Desktop/data	IEUser	12/4/2022 5:19:55 PM		1
	file:///C:/Users/IEUser/Desktop	IEUser	12/4/2022 5:19:55 PM		1
	file:///C:/Users/IEUser/Desktop/data/password.txt	IEUser	12/4/2022 5:20:10 PM		1
	file:///C:/Users/IEUser/Downloads/pexels-yelena-odi...	IEUser	12/4/2022 5:27:39 PM		1
	file:///C:/Users/IEUser/Downloads/pexels-polina-kov...	IEUser	12/4/2022 5:27:49 PM		1

		file:///C:/Users/IEUser/Downloads/pexels-nati-96342...	IEUser	12/4/2022 5:28:41 PM		1
		file:///C:/Users/IEUser/Downloads	IEUser	12/4/2022 6:25:39 PM		1
		file:///C:/Users/IEUser/Downloads/YellowHearts.jpg	IEUser	12/4/2022 6:27:00 PM		1
		file:///C:/Users/IEUser/Desktop/LastSceneMountains...	IEUser	12/4/2022 6:27:27 PM		1
		https://www.microsoft.com/en-us/edge?form=MA1...	IEUser	12/4/2022 2:44:12 PM	Microsoft Edge	1
		https://www.google.com/chrome/bsem/download/e...	IEUser	12/4/2022 2:44:49 PM	Google Chrome Web Browser	1
		https://dl.google.com/tag/s/appguid%3D%7B8A69...	IEUser	12/4/2022 2:44:54 PM		1
		https://www.google.com/chrome/thank-you.html?b...	IEUser	12/4/2022 2:44:55 PM	Google Chrome Web Browser	1
		https://dl.google.com/tag/s/appguid%3D%7B8A69...	IEUser	12/4/2022 2:44:59 PM		1
		https://www.google.com/chrome/thank-you.html?in...	IEUser	12/4/2022 2:45:01 PM	Google Chrome Web Browser	1
		https://www.bing.com/ck/a?!&&p=da3814efa2f704...	IEUser	12/4/2022 2:45:27 PM		1
		https://www.7-zip.org/download.html	IEUser	12/4/2022 2:45:29 PM	Download	1
		https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM	putty - Search	1
		https://www.bing.com/ck/a?!&&p=ffd93d158cef773...	IEUser	12/4/2022 4:34:03 PM		1
		https://putty.org/	IEUser	12/4/2022 4:34:04 PM	Download PuTTY - a free SSH and telnet client for...	1
		https://www.msn.com/	IEUser	12/4/2022 2:44:09 PM		1
		https://go.microsoft.com/fwlink/?LinkId=525773	IEUser	12/4/2022 2:44:10 PM		1
		https://go.microsoft.com/	IEUser	12/4/2022 2:44:10 PM		1
		https://www.microsoft.com/en-us/edge?form=MA1...	IEUser	12/4/2022 2:44:11 PM		1
		https://www.microsoft.com/	IEUser	12/4/2022 2:44:11 PM		1
		https://www.bing.com/search?q=install+chrome&fo...	IEUser	12/4/2022 2:44:43 PM		1
		https://www.bing.com/	IEUser	12/4/2022 2:44:43 PM		1
		https://www.google.com/chrome/bsem/download/e...	IEUser	12/4/2022 2:44:48 PM		1
		https://www.google.com/	IEUser	12/4/2022 2:44:48 PM		1
		https://www.7-zip.org/download.html	IEUser	12/4/2022 2:45:28 PM		1
		https://www.7-zip.org/	IEUser	12/4/2022 2:45:28 PM		1
		https://putty.org/	IEUser	12/4/2022 4:34:04 PM		1
	11	file:///C:/Users/IEUser/Downloads/drafts	IEUser	12/4/2022 6:38:14 PM		2
	16	https://www.bing.com/ck/a?!&&p=da3814efa2f704...	IEUser	12/4/2022 2:45:27 PM		2
	8	https://www.bing.com/aclk?ld=e8OQqckSvv-jmTim...	IEUser	12/4/2022 2:44:47 PM		2
	22	https://www.bing.com/ck/a?!&&p=ffd93d158cef773...	IEUser	12/4/2022 4:34:03 PM		2

16	https://www.bing.com/ck/a?!&&p=da3814efa2f704...	IEUser	12/4/2022 2:45:27 PM		2
8	https://www.bing.com/aclk?ld=e8OQqckSvv-jmTim...	IEUser	12/4/2022 2:44:47 PM		2
22	https://www.bing.com/ck/a?!&&p=ffd93d158cef773...	IEUser	12/4/2022 4:34:03 PM		2
7	https://www.bing.com/	IEUser	12/4/2022 2:44:43 PM		2
21	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM		2
19	https://www.7-zip.org/a/7z2201-x64.exe	IEUser	12/4/2022 2:46:59 PM		2
17	https://www.7-zip.org/download.html	IEUser	12/4/2022 2:45:28 PM		2
4	https://www.microsoft.com/en-us/edge?form=MA1...	IEUser	12/4/2022 2:44:11 PM		2
12	https://www.google.com/chrome/thank-you.html?b...	IEUser	12/4/2022 2:44:55 PM		2
14	https://www.google.com/chrome/thank-you.html?in...	IEUser	12/4/2022 2:45:00 PM		2
9	https://www.google.com/chrome/bsem/download/e...	IEUser	12/4/2022 2:44:48 PM		2
14	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:34:03 PM	putty - Search	2
9	https://www.bing.com/search?q=nstall+7zip&form...	IEUser	12/4/2022 2:45:27 PM	nstall 7zip - Search	2
2	https://www.bing.com/search?q=install+chrome&fo...	IEUser	12/4/2022 2:44:47 PM	install chrome - Search	2
12	https://www.7-zip.org/a/7z2201-x64.exe	IEUser	12/4/2022 2:46:59 PM		2
	file:///C:/Users/IEUser/Downloads/drafts	IEUser	12/4/2022 6:38:14 PM		2
	https://www.bing.com/search?q=install+chrome&fo...	IEUser	12/4/2022 2:44:47 PM	install chrome - Search	2
	https://www.bing.com/search?q=nstall+7zip&form...	IEUser	12/4/2022 2:45:27 PM	nstall 7zip - Search	2
	https://www.7-zip.org/a/7z2201-x64.exe	IEUser	12/4/2022 2:46:59 PM		2
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:34:03 PM	putty - Search	2
	https://www.microsoft.com/en-us/edge?form=MA1...	IEUser	12/4/2022 2:44:11 PM		2
	https://www.google.com/chrome/bsem/download/e...	IEUser	12/4/2022 2:44:48 PM		2
	https://www.google.com/chrome/thank-you.html?b...	IEUser	12/4/2022 2:44:55 PM		2
	https://www.google.com/chrome/thank-you.html?in...	IEUser	12/4/2022 2:45:00 PM		2
	https://www.bing.com/	IEUser	12/4/2022 2:44:43 PM		2
	https://www.bing.com/ck/a?!&&p=da3814efa2f704...	IEUser	12/4/2022 2:45:27 PM		2
	https://www.7-zip.org/download.html	IEUser	12/4/2022 2:45:28 PM		2
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM		2
	https://www.bing.com/ck/a?!&&p=ffd93d158cef773...	IEUser	12/4/2022 4:34:03 PM		2
20	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM		3
6	https://www.bing.com/search?q=install+chrome&fo...	IEUser	12/4/2022 2:44:43 PM		3

	https://www.bing.com/search?q=install+chrome&fo...	IEUser	12/4/2022 2:44:43 PM	3
	https://www.bing.com/search?q=putty&filters=ufn...	IEUser	12/4/2022 4:33:59 PM	3
15	https://www.bing.com/search?q=nstall+7zip&form...	IEUser	12/4/2022 2:45:15 PM	4
	https://www.bing.com/search?q=nstall+7zip&form...	IEUser	12/4/2022 2:45:15 PM	4
3	https://login.live.com/oauth20_logout.srf?client_id=...	IEUser	12/4/2022 2:43:51 PM	9
2	https://login.live.com/oauth20_desktop.srf?lc=1033	IEUser	12/4/2022 2:43:51 PM	9
	https://login.live.com/oauth20_desktop.srf?lc=1033	IEUser	12/4/2022 2:43:51 PM	9
	https://login.live.com/oauth20_logout.srf?client_id=...	IEUser	12/4/2022 2:43:51 PM	9

Some of the important pieces of information that are seen when looking at these searches is that the suspect first looked up a download for TightVNC which is a remote desktop software server. Then they wanted to know how to send files remotely from Linux to windows. Next, they seemed to look up how to become a great writer. Then they went to look at how to hide files

on widows and downloaded PuTTY. Next, they downloaded some stock images. Then they went to their email to change a password (which is an important key to this case). Lastly, they browsed Facebook, downloaded WinSCP, and kept looking up how to hide files.

5. Can you find out if the suspect used this device to connect to another device?

   Yes, this is confirmed. Not only did the suspect download many applications that allow connecting to another device, but looking into Axiom's windows Event Logs - Script Events, it is seen that it logged the connecting and disconnecting of remote desktop services, which confirms it.

5860	3/19/2019 1:03:28 PM	153	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\LOCAL SERVICE	MSEDGEWIN10	3208
5861	3/19/2019 1:08:53 PM	163	WMI Registration of Permanent Event Consumer.			
5860	3/19/2019 1:09:01 PM	165	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\LOCAL SERVICE	MSEDGEWIN10	3656
5861	3/19/2019 1:14:03 PM	178	WMI Registration of Permanent Event Consumer.			
5860	3/19/2019 1:14:10 PM	181	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\LOCAL SERVICE	MSEDGEWIN10	7148
5861	3/19/2019 1:24:34 PM	193	WMI Registration of Permanent Event Consumer.			
5860	3/19/2019 1:24:44 PM	195	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\LOCAL SERVICE	MSEDGEWIN10	4024
5860	3/19/2019 1:24:44 PM	197	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\SYSTEM	MSEDGEWIN10	6884
5861	12/4/2022 4:17:50 PM	215	WMI Registration of Permanent Event Consumer.			
5861	12/4/2022 5:19:54 PM	222	WMI Registration of Permanent Event Consumer.			
5860	12/4/2022 5:20:05 PM	225	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\LOCAL SERVICE	MSEDGEWIN10	4728
5860	12/4/2022 2:42:06 PM	238	Remote Desktop Services: Session logoff succeeded.	NT AUTHORITY\SYSTEM	MSEDGEWIN10	3508

6. What is the used method for connection?

   It seems as if the suspect used the programs that they downloaded in order to run a PowerShell command that connected them to other machines. This information can be found in Axiom's Powershell history category.

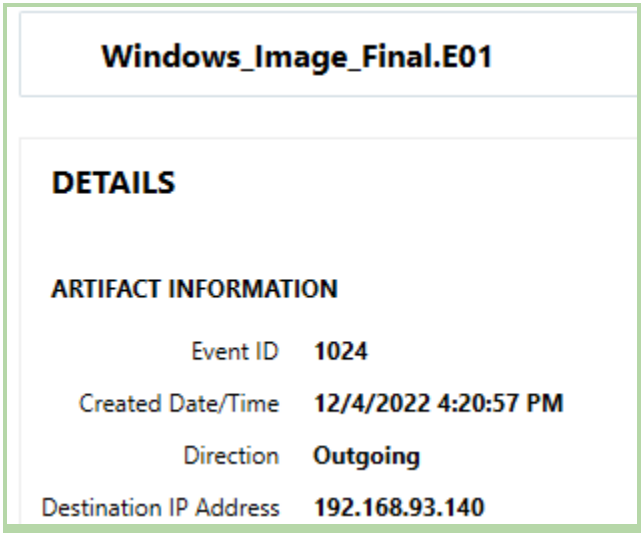
MATCHING RESULTS (4 of 4) Column view

User...	Command	Artifact type	Source	Reco...	Dele...	Loca...	E
IEUser	ssh user1@192.168.93.142	PowerShell History	Windows_Image_Final.E01 - Partition 1 (Microsoft N...	Parsing		Line: 1	W
IEUser	ssh user1@192.168.93.142:22	PowerShell History	Windows_Image_Final.E01 - Partition 1 (Microsoft N...	Parsing		Line: 2	W
IEUser	ssh user1@192.168.93.140:22	PowerShell History	Windows_Image_Final.E01 - Partition 1 (Microsoft N...	Parsing		Line: 3	W
IEUser	ssh user1@192.168.93.140	PowerShell History	Windows_Image_Final.E01 - Partition 1 (Microsoft N...	Parsing		Line: 4	W

As it is seen, the suspect used the ssh command to a different ip, which means he connected to a different machine.

7. What is the IP address of the other device? Provide as much information about the remote device as possible.

   By looking inside the connected devices, under Remote Desktop Protocol, I am able to see the outgoing direction of the connection. This is where it displays the ip address of 192.168.93.140.



It seems as if the suspect connected to that ip address of the other device. But then, it is seen that there was an incoming request, where the suspect

must have connected to this windows machine using the other VM.

MATCHING RESULTS (16 of 16) Column view

Even...	Created Date/...	Registry Key...	Dire...	Event Description Summary	Origin Service...	Origi...
		12/4/2022 3:13:19 PM	Outgoing			
		12/4/2022 3:13:07 PM	Outgoing			
1024	12/4/2022 3:11:27 PM		Outgoing			
1024	12/4/2022 3:12:50 PM		Outgoing			
1024	12/4/2022 3:13:17 PM		Outgoing			
1024	12/4/2022 3:14:15 PM		Outgoing			
1024	12/4/2022 3:15:44 PM		Outgoing			
1024	12/4/2022 3:21:19 PM		Outgoing			
1024	12/4/2022 4:02:35 PM		Outgoing			
1024	12/4/2022 4:02:59 PM		Outgoing			
1024	12/4/2022 4:08:14 PM		Outgoing			
1024	12/4/2022 4:20:57 PM		Outgoing			
1149	12/4/2022 4:16:08 PM		Incoming		IEUser	
1024	12/4/2022 4:24:50 PM		Outgoing			
25	12/4/2022 4:16:11 PM		Incoming		MSEDGEWIN10\IEUser	
24	12/4/2022 4:16:25 PM		Incoming	Remote Desktop Services: Session has been disconn...	MSEDGEWIN10\IEUser	

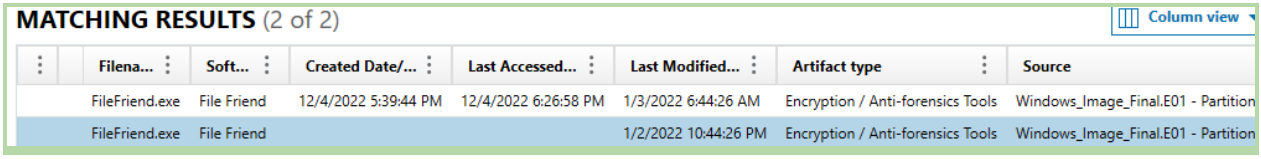
8. Based on the downloaded applications, is there any other way/ways the suspect might have used to connect to the other device?

Yes, there are multiple different applications that the suspect may have used to connect to another device. Looking at the applications that they downloaded, the ones that stand out to me that are not VMware would be Puppet, PuTTY, TightVNC, and WinSCP. All of these applications are related to the connection of different devices. What really strikes me as a possibility would be that the suspect used PuTTY and WinSCP to transfer files over to a linux machine that they did not want to be seen on this windows machine.

Application Na...	Comp...	Crea...	Key Last Upd...	Insta...	Version	Potential Location	Artifact
7-Zip 22.01 (x64)	Igor Pavlov		12/4/2022 2:46:09 PM	5601	22.01	C:\Program Files\7-Zip	Installed F
Google Chrome	Google LLC	12/4/2022	12/4/2022 2:45:46 PM		108.0.5359.95	C:\Program Files\Google\Chrome\Application	Installed F
Puppet (64-bit)	Puppet Labs	3/19/2019	3/19/2019 1:22:17 PM	58489	3.8.7		Installed F
PuTTY release 0.78 (64-bit)	Simon Tatham	12/4/2022	12/4/2022 4:37:19 PM	5664	0.78.0.0		Installed F
TightVNC	GlavSoft LLC.	12/4/2022	12/4/2022 3:20:27 PM	3084	2.8.63.0		Installed F
VMware Tools	VMware, Inc.	12/4/2022	12/4/2022 4:17:09 PM	100400	11.3.5.18557794		Installed F
WinSCP 5.21.6	Martin Prikryl	12/4/2022	12/4/2022 6:01:20 PM	100896	5.21.6	C:\Program Files (x86)\WinSCP	Installed F

9. Are there any anti-forensic tools installed on the machine?

   Yes, there is one major anti-forensics tool that is installed on this machine. Using Axiom, I was able to look at possible anti-forensics tools and find an executable known as FileFriend.exe.



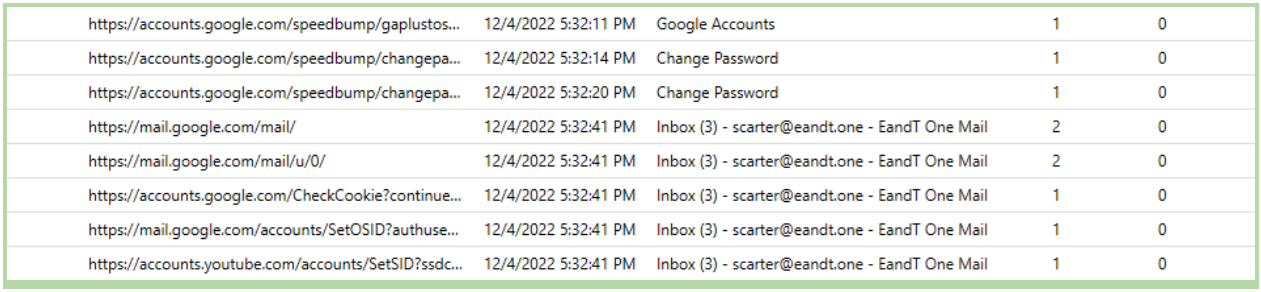
MATCHING RESULTS (2 of 2) — Column view

Filena...	Soft...	Created Date/...	Last Accessed...	Last Modified...	Artifact type	Source
FileFriend.exe	File Friend	12/4/2022 5:39:44 PM	12/4/2022 6:26:58 PM	1/3/2022 6:44:26 AM	Encryption / Anti-forensics Tools	Windows_Image_Final.E01 - Partition
FileFriend.exe	File Friend			1/2/2022 10:44:26 PM	Encryption / Anti-forensics Tools	Windows_Image_Final.E01 - Partition

   File Friend is an application that allows the user to password protect and encrypt any file.

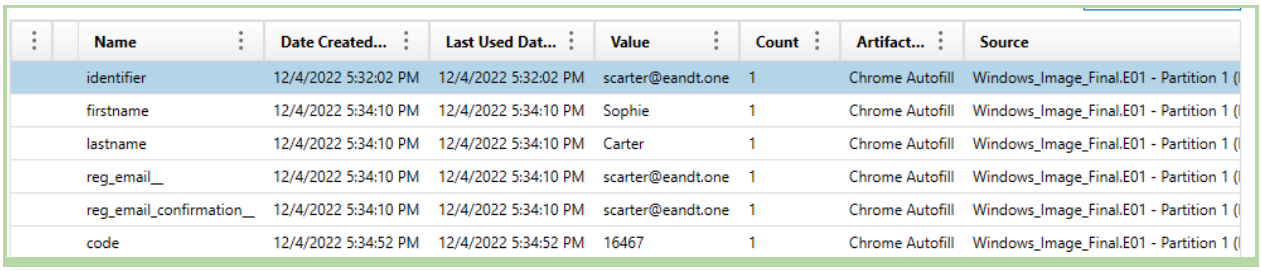
10. Are there any artifacts about the real suspect's name?

    Yes, the best artifact that is found regarding the suspect's real name is the name of the Gmail that they accessed within their chrome web history. Having a look at it, they seemed to use their email to change the password of an account.



https://accounts.google.com/speedbump/gaplustos...	12/4/2022 5:32:11 PM	Google Accounts	1	0
https://accounts.google.com/speedbump/changepa...	12/4/2022 5:32:14 PM	Change Password	1	0
https://accounts.google.com/speedbump/changepa...	12/4/2022 5:32:20 PM	Change Password	1	0
https://mail.google.com/mail/	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	2	0
https://mail.google.com/mail/u/0/	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	2	0
https://accounts.google.com/CheckCookie?continue...	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0
https://mail.google.com/accounts/SetOSID?authuse...	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0
https://accounts.youtube.com/accounts/SetSID?ssdc...	12/4/2022 5:32:41 PM	Inbox (3) - scarter@eandt.one - EandT One Mail	1	0

   It is also important to note that the only things that are found within google's autofill function for this user is the name "Sophie Carter"



Name	Date Created...	Last Used Dat...	Value	Count	Artifact...	Source
identifier	12/4/2022 5:32:02 PM	12/4/2022 5:32:02 PM	scarter@eandt.one	1	Chrome Autofill	Windows_Image_Final.E01 - Partition 1 (
firstname	12/4/2022 5:34:10 PM	12/4/2022 5:34:10 PM	Sophie	1	Chrome Autofill	Windows_Image_Final.E01 - Partition 1 (
lastname	12/4/2022 5:34:10 PM	12/4/2022 5:34:10 PM	Carter	1	Chrome Autofill	Windows_Image_Final.E01 - Partition 1 (
reg_email__	12/4/2022 5:34:10 PM	12/4/2022 5:34:10 PM	scarter@eandt.one	1	Chrome Autofill	Windows_Image_Final.E01 - Partition 1 (
reg_email_confirmation__	12/4/2022 5:34:10 PM	12/4/2022 5:34:10 PM	scarter@eandt.one	1	Chrome Autofill	Windows_Image_Final.E01 - Partition 1 (
code	12/4/2022 5:34:52 PM	12/4/2022 5:34:52 PM	16467	1	Chrome Autofill	Windows_Image_Final.E01 - Partition 1 (

11. Explain why you think this is the suspect's name.

I believe that this is the suspect’s name due to the fact that this is the only account that they have obvious access. They were able to access the email account (scarter@eandt.one) in order to change a password, which confirms that this is the suspect’s name. Added onto that, the only names in the google autofill are the names, Sophie Carter.

A conclusion is not necessary.

How to answer questions - When providing answers to questions, please also list the file and/or forensic artifacts where you got your answers along with information about those files such as dates & times, file size, location, etc. that will fully describe it. This context is very important!

You should also describe how you got your result. For example – A keyword search for the term 'marijuana' revealed 5 hits, one of which was the document – 'Your friendly neighborhood plumber.docx'. The document was located in the folder C:\users\john\Desktop and was 4235 KB in size. It is also a good idea to instead include a table if listing more than one piece of metadata like this:

Item	Description
Filename	Your friendly neighbourhood plumber.docx
Full path	C:\users\john\Desktop\Your friendly neighbourhood plumber.docx
Size	4235 KB
SHA1 Hash	6A204BD89F3C8348AFD5C77C717A097ABB0398A801
Created Date	11/01/2009 12:32:44
Modified Date	11/05/2010 05:32:09

If the item being described is an email, provide full email metadata like To, From, CC, Subject, Date and any other relevant details along with the message.