Student Number	Worked on Section?
2300222	1, 2.4.6, 2.4.8, 2.4.8.1, 2.4.8.3, 3, 4, Appendix A.2, A.3, A.6, E.4.1, E.7, I.10, I.11, J, K
2300214	1, 2.2, 2.3, 2.4.2, 2.4.3, 2.4.5, 2.4.6, 2.4.7, 2.4.8.1, 2.4.8.4, 2.5, 3, Conclusion, Appendix A.1.1 - A.1.2, A.2 A.4, A.5.1 - A.5.81, A.6, B.1.1 - B.4.1, D, E.1.1 - E.3.1, F.13.1 - F.15.5, G.1.1 - G.4.4, H, I.1.1 - I.8.3
2301460	Contents Page, 1, 2.3, 2.4.6, 2.4.8.3, 4, Appendix A.5, E.2.1, E.3.1, E.4.1, E.5.1, E.6.1, J.1, J.2, K, Glossary
2300867	Summary, 1, 2.1, 2.2, 2.3, 2.4.1, 2.4.4, 2.4.6, 2.4.8, 2.4.8.1, 2.4.8.2, 2.4.8.4, Conclusion, Appendix A.2, C, F.1.1 - F.12.2, I.9.1-I.9.5

JOINT REPORT of

EZRA LAWRIE, MELISSA FORREST, ADAM HENDERSON
AND
JAM BUCKLEY

Worm Warriors

Case against: Sonya Macoit
Police Reference No: 78521
Case Reference No: 001
PF Reference No: 3348

Summary

An image was acquired of the personal computer of Sonya Macoit due to her being under investigation on charges of Poaching. Four analysts were tasked with the investigation and analysis of the suspects usage of Personal Devices.

On 2023-12-15 at 13:23:12 the suspect accessed the Personal Computer and created the account “Sonya”. This is the only account on the Personal Computer. Between the time of creation of the account and the last login which occurred on 2024/02/27 at 07:26:48 the user “Sonya” used the Personal Computer to access and engage with material related to poaching. A multitude of these pieces of material were subjected to anti-forensic techniques. The user also received emails related to poaching under the email address “sonyamacoit@outlook.com”.

Across this period, the user's engagement with material related to poaching can be separated into 59 incidents. These incidents spanned several different types of material including Images, Videos, Documents, Web Artifacts and Email messages among others.

Contents Page

Summary 1

Contents Page 2

1.Description of the Crime 3

2. Description of Investigation 12

2.1 Job Description and Instructions 12

2.2 Description of Recovered / Examined Items 13

2.3 Methodology 13

2.4 Analysis 15

3. Conclusion 26
4. Equipment Required for Court Proceedings 26
Appendices 27
Appendix A - Images 28
Appendix B Documents 50
Appendix C – Timeline of events 58
Appendix D Chain of Custody 67
Appendix E Browser History 68
Appendix F E-mail 96
Appendix G Encryption 129
Appendix H 138
Appendix I Miscellaneous 147
Appendix J Installed / Run programs 178
Appendix K - Shell Bags 181
Appendix L Glossary 186

1.Description of the Crime

Each incident has been broken down and summarised below in chronological order, these are represented in a graphical timeline in Appendix C. All terms and files of note are listed in Appendix L – Glossary.

Incident #1 – Web Searching and Browser History.

On 2023/12/19 between the times of 14:25:57 – 14:45:51 GMT the suspect began a browsing session researching the Mozilla Thunderbird email client and accessing the official website once. Mozilla Thunderbird is an email client that doubles as a personal information manager. The suspect also researched the Talek River which is a river locates in the Maasai Mara national reserve and visited webpages related to it three times. The information for both searches can be found in Appendix E under Figure E.2.1 - Index 1 for Mozilla Thunderbird and Figure E.3.1 - Index 1 for the Talek River.

Incident #2 – Web Searching and Browser History

On 2024/01/02 between the times of 11:48:29 – 13:20:42 GMT and on 2024/01/03 at 11:12:59 GMT the suspect began a browser session researching Cheetahs, Elephants, elephant and crocodile hunting trips, bullet safari's, hunting rifles of varying calibres as well as browsing trophy fees and hunting lists. Alongside this the suspect used google earth to view coordinates in Maasai Mara and near the Talek River. The suspect visited websites a total of 45 times across Edge and Chrome and searched a total of

29 times. During this time a .pdf document is downloaded onto the suspects computer. This document is named “2024-Wish-List-Trophy-Fees-with-Pics.pdf” this document included images of animals and prices next to them. The information for the web searches and browser history can be found in Appendix E under Figure E.2.1 - Index 2 - 15 And Figure E.3.1 - Index 2 – 16 and the downloaded document can be found in Appendix B under Figure B.5.1.

Incident #3 – File Deleted/Recycling Bin

On 2024/01/03 at 08:18:32 GMT a jpeg file called “sonya.jpg” was moved to the recycling bin by the account “Sonya”. This image and its information can be viewed in Appendix A under Figure A.2.1.

Incident #4 - Emails

2024/01/03 10:42:46 – 11:47:40 GMT. User entered an email thread discussing mission logistics and preliminary analysis. This consisted of 7 emails with marteneleroux@proton.me and sonyamacoit@outlook.com. These emails discussed surveillance points and necessary drone enhancements. This included coordinates that plotted and area they wanted to place under surveillance. Additionally, on the same day at 11:59:18 GMT marteneleroux@proton.me copied a message that had been sent as a job opportunity to local talent and sent it to Sonya. Then on 2024/01/04 at 11:25:58 – 11:28:57 GMT a forwarded message was sent to Sonya asking when they should meet, and Sonya replied informing them that they were currently looking at drones and would reply soon. Information for these emails can be viewed in Appendix F under Figure 1.1.

Incident #5 – Email Tampering

On 2024/01/03 at 10:37:36 an email address belonging Chief Officer Van Der Schyff was found to have access to Sonya’s email account. This access proceeded until 2024/02/22 at 07:23:02 GMT when Sonya’s email account stopped being used. Information on this can be viewed in Appendix F under Figure F.13.1 - F.13.3.

Incident #6 – Web Searching and Browser History

On 2024/01/04 at 11:29:06 – 2024/01/05 at 12:07:12 GMT the suspect entered a browsing ession researching drone laws, night vision for drones, extinction/endangerment of elephants, the ethics of hunting, wildlife crime enforcers conferences and digital analysis funds. Along with this a wildlife crime scorecard from the WWF was found downloaded onto the suspects computer, as well as encrypted. This involved 10 visits to websites and 4 individual searches. The information for this browser session can be found in Appendix E under Figure E.3.1 - Index 17- 20.

Incident #7 - Emails

The mac time has been 0000/00/00 00:00:00 on a PDF file which is a Wishlist including trophy fees and prices listed next to animal names. This was sent in an email to marteneleroux@proton.me on 2024/01/05 at 11:18:00 GMT with the subject line “something to consider when planning” where there was a reply of a poem 2024/01/05 at 19:21:37 GMT and sonyamacoit@outlook.com replied to this with a poem of her own 2024/01/08 08:19:12. The information can be found in Appendix F under Figure F.2.1 - F.2.2.

Incident #8 - Emails

On 2024/01/08 at 07:57:13 an email was sent containing concerns about drone surveillance from sonyamacoit@outlook.com discussing adjusting drone heights for maximum coverage and communication protocols; a reply was received on 2024/01/11 at 09:41:14 from marteneleroux@proton.me containing a link to a site about Kenyan drone laws and permits suggesting they speak to victor then an email was forwarded to thescout@skiff.com from sonyamacoit@outlook.com asking him to confirm the drone permits and to source the permit. There were then multiple replies at 2024/01/15 11:23:26 were thescout@skiff.com discussed the permits being finalised and the drones (x2 DJI Mavic 3 Pro) asking for a date to meet and check if everything is ok and 2024/01/16 at 11:19:00 from sonyamacoit@outlook.com stating the dates and meeting locations at 11:22:32 on the same day from thescout@skiff.com discussing the meeting location and confirming the

date on 2024/01/17 at 12:57:16 a final email was sent by sonyamacoit@outlook.com changing the meeting date and flight arrival times, a series of emails were then sent between sonyamacoit@outlook.com, thescout@skiff.com and marteneleroux@proton.me on 2024/01/19 between 08:23:46 - 08:51:28 GMT emails were exchanged discussing the costs of meeting earlier on Tuesday the 23rd as it is short notice. This meeting was confirmed and then the logistics of this meeting were discussed including bringing in a new drone operator. The information for the email thread can be found in Appendix F under Figure 3.1.

Incident #9 - Email

On 2024/01/08 at 08:39:24 GMT an email was sent to thescout@skiff.com where sonyamacoit@outlook.com has shared a folder called mission specs there was a reply to this on 2024/01/08 at 08:39:24 containing a thumbs up and another reply from thescout@skiff.com containing a poem. The information for this email thread can be found in Appendix F under Figure F.4.1.

Incident #10 – Web Searching and Browser History

On 202401-09 between the times of 07:48:21 to 07:48:58 GMT the suspect began a browsing session in which they performed research into anti forensic techniques. Open-source tools and hash keeper. These pages were visited a total of 5 times and searched individually 3 times. The information for this incident can be found in Appendix E under Figure E.31 - Index 22-24.

Incident #11 – Web Searching and Browser History

On 2024/01/11 09:45:14 to 2024/01/15 11:25:34 GMT the suspect entered a browser session booking cheap flights to Kenya from EDI to NBO, 31/1 — 6/2. Edinburgh to Nairobi on the 31st of January and returning on the 6th of February visited a total of 6 times and was searched independently twice. The history, contents and information for this incident can be found in Appendix E under E.3.1 - Index 25-26.

Incident #12 – Run programs

On 2024/01/11 between 09:48:06 – 09:48:13 GMT the program “CERTUTIL.EXE” has been run. This is a legitimate Windows command-line utility for certificate management, file hashing, and downloading files from remote servers; it can also be misused for unauthorized data transfer. The information for this can be found in Appendix J under Figure J.2 - Index 1 – 3.

On 2024/01/11 09:48:14 – 2024/1/11 09:48:15 GMT the file “NPFINSTALL.EXE” was run. This is an installer for a packet capture driver commonly used with network analysis tools such as Wireshark, supporting network monitoring and traffic analysis. You can view the information for this in Appendix J under Figure J.2 - Index 4 – 5.

Incident #13 – Installed Programs

On 2024/01/11 between the times 09:48:25 – 09:49:49 GMT three programs were installed by the suspect to their Personal Computer. These installed programs were “Wireshark”, “Npcap” and “USBcap”, upon further investigation Wireshark and Npcap are both tools for monitoring network traffic whereas USBcap is an open-source USB packet capture program for windows. The information for this incident can be found in Appendix J under Figure J.1.1 - J.1.2.

Incident #14 – Deleted Item

On 2024/01/13 at 16:13:48 GMT a deleted item from the encryption program VeraCrypt was found using autopsy on the suspects computer. The information for this incident can be found in Appendix I under Figure I.11.1.

Incident #15 – Web Searching and Browser History

On 2024/01/16 at 11:26:17 the suspect started a browser session where they were searching for Garden city mall in Nairobi. This was visited 3 times and searched once. The information for this can be found in Appendix E under Figure E.3.1 - Index 27.

Incident #16 – Web Searching and Browser History

On 2024/01/17 between the times of 13:11:35 – 13:20:10 GMT a browsing session begun doing research into malware scanners to check for viruses, research into poaching and the current poaching crisis in Kenya and Africa as a whole. Following this research was done on the skeletons of elephants. This browsing session totalled 15 visits across both chrome and edge and 9 individual searches. The links and information for this incident can be found in Appendix E under Figure E.2.1 - Index 16-22 and Figure E.3.1 - Index 28-29.

Incident #19 - Email

An email was received from thescout@skiff.com on 2024/01/19 at 09:14:21 discussing the meeting on Tuesday and a drone operator that is being brought into the operation. This email was sent to sonyamacoit@outlook.com, marteneleroux@proton.me and CC'ed to lunavanderschyff@outlook.com. In reply to this on 2024/01/23 a series of emails were sent and received between sonyamacoit@outlook.com, marteneleroux@proton.me and thescout@skiff.com and CC'ed to lunavanderschyff@outlook.com. These emails began at 10:00:07 to 10:23:54 GMT and discuss finding a quiet spot to test as well as drone configurations, the testing location were coordinates of -1.3219782 (lat), 34.9261049 (long) then these were sent in image form to which the spot was selected. The related emails and their contents can be viewed at Appendix F under Figure F.5.1 - F.5.2.

Incident #20 – Web Searching and Browser History

On 2024/1/23 between the times of 10:10:30 to 10:18:35 GMT the suspect began a browser session viewing the coordinates for the Olare Motorogi Conservatory and coordinates east of Olenteki in Kenya and west of Kawai. These pages were visited 12 times total and individually searched twice. The information for this incident can be found in Appendix E under Figure E.3.1 - Index 30-31.

Incident #21 - Email

An email was received by sonyamacoit@outlook.com from thescout@skiff.com on 2024/01/23 at 10:41:44 with the subject "Key to Success" containing a poem in Afrikaans, upon translation the poem reads as follows:

Bitter-berry daybreak
bitter-berry sun
a mirror has broken
between me and him

I try to find the highway
perhaps to run away
but everywhere the footpaths
of his words lead me astray

Pinewood remember
pinewood forget
however much I lose my way
I step on my regret

Parrot-coloured echo
tricks me tricks me on
until I turn beguiled
to retrieve the mocking song

Echo gives no answer
he answers everyone
bitter-berry daybreak
bitter-berry sun

This is a poem by Ingrid Jonker.

Sonyamacoit@outlook.com replied to this on 2024/01/24 at 13:47:35 GMT simply asking, “What does this mean Victor?”, thescout@skiff.com replied on 2024/02/05 at 8:30:47 GMT Stating that they will discuss what was meant in the email tomorrow at 10am and that they may have a tail. Another set of emails in response to the tail was sent on 2024/02/06 between 10:20:58 and 10:31:39 GMT where thescout@skiff.com and sonyamacoit@outlook.com discussed moving forward in their operation without a drone and instead just using a Camera.

Incident #22 – Web searching and Browser History

On 2024/01/24 between the times 13:35:48 - 13:36:50 GMT the suspect began a browser session began with Sonya researching steghide and steganography then between 13:41:11 - 13:41:21 GMT the topic of the session changed to becoming a double agent and stealing information from intelligence agencies. This included a visit to the webpage sourceforge, a site that steghide is downloaded from. These pages were visited a total of 5 times and searched for individually 4 times. The information and links to these sites can be found in Appendix E under Figure E.2.1 - Index 23 and Figure E.3.1 - Index 32-34.

Incident #23 – Installed programs

On 2024/01/24 between the times of 13:36:10 - 13:40:46 GMT. The suspect has installed a program called steghide. The folder “steghide-0.5.1-win32.zi” was created, accessed, extracted to “steghide-0.5.1-win3” and items were written to the file "steghid". Steghide was last run at 13:40:27 GMT and was sent to the recycling bin at 13:40:46 GMT. Steghide is a steganography program. The information for this incident can be found at Appendix G under Figure G.1.1 - G.1.4.

Incident #24 - Shell Bags

On 2024/01/26 at 09:07:42 a folder named “mission pic” was created and placed in the documents folder. At 09:21:32 GMT the folder “mission spec” was accessed and modified. See figure K.1 and K.3.

Incident #25 - Email

On 2024/01/26 marteneleroux@proton.me sent an email to sonyamacoit@outlook.com and thescout@skiff.com at 09:03:21 GMT containing 5 attachments with photos of the group and the drones. Sonyamacoit@outlook.com replied at 09:21:04 with another image of the group attached to the same people. Finally, sonyamacoit@outlook.com sent another email at 09:23:32 to thescout@skiff.com on the same day containing photos of contracts and telling the group they will have to send in their contracts physically. For full contents of this incident please view Appendix F under Figure F.7.1-F.7.4

Incident #26 – Web Searching and Browser History

On 2024/01/26 between the times of 09:26:29 - 10:03:42 GMT the suspect began a browser session looking into booking an elephant hunting trip in Kenya and South Africa, what gear was needed for hunting elephants. These pages were visited 23 times in total and individually searched 12 times. For further information on these websites view Appendix E under Figure E.2.1 - Index 24-29 and Figure E.3.1 - Index 35-41.

Incident #27 - Email

On 2024/02/05 sonyamacoit@outlook.com sent an email to marteneleroux@proton.me and thescout@skiff.com at 08:06:04 GMT discussing a final mission meetup and checks at 10 am the next day, marteneleroux@proton.me replied at 08:07:32 to sonyamacoit@outlook.com and CCed

thescout@skiff.com stating that all was ok from his end. For full contents and information on this incident please view Appendix F Figure F.8.1

Incident #28 - Images

On 2024/02/06 07:09:59 GMT thirteen images of giraffes were backed up onto the drive and one of a plush giraffe (see figure A.5.32 - A.5.45). The names of these are simply descriptive. These were mainly taken using the Canon Eos 30, Canon Eos R5 and Yashica Mat-124g cameras.

Incident #29 - Shell Bags

On 2024/02/06 at 10:17:44 a file called "elephant" was created then moved to the documents folder. See figure K.4.

Incident #30 - Email

On 2024/02/06 sonyamacoit@outlook.com sent an email to thescout@skiff.com, marteneleroux@proton.me and lunavanderschyff@outlook.com at 10:19:12 containing discussions about the effectiveness of the drone and an attachment which features a picture of an elephant, this email also discussed how to move forward with their plans.

Incident #31 - Images

On 2024/02/06 at 10:18:07 eleven images of elephants were backed up onto the hdd drive (see figure A.5.1 - A.5.11) showing close up images of elephants including aerial shots of a family from above. All the times are identical, indication of potential M.A.C.E tampering.

Incident #32 - Images

On 2024/02/06 between the times 10:23:54 – 10:41:35 GMT 22 images were discovered on the cache including images of hunting rifles, images of animals and poaching and an image of an arrowhead. To view the images on the cache view Appendix A Figure A.6.1 - A.6.21.

Incident #33 - Web searching and browser history

On 2024/02/06 10:24:08 - 10:54:49. Sonya began researching about bow hunting elephants at two separate websites, Sonya began searching on edge about anti forensic techniques and "6 Anti-Forensic Techniques That Every Digital Forensic Investigator Dreads". Sonya then began looking on edge for cameras that are good for taking pictures of wildlife. She also researched on edge about how poachers are tracked, hunted down and how poacher's deaths are celebrated. Then Sonya researched on edge about a "Computer Hacking Forensic Investigator" and how much one would cost. See figures E.2 Index 32-36 and E.3 Index 43-56.

Incident #33 - Shell Bags

On 2024/02/07 at 09:26:54 GMT a folder was created called "backup_07022" this was placed in the documents folder. At 09:27:04 GMT three files were added to the folder. They were "mission spec", "mission pic" and "elephant". See figure K.5.

Incident #34 - Shell Bags

On 2024/02/07 at 09:27:06 GMT the folders "mission spec" and "mission pic" were created on the USB drive. See figure. K.6.

Incident #35 - Email

On 2024/02/08 sonyamacoit@outlook.com sent an email to thescout@skiff.com at 12:36:51 GMT discussing the purchase of a CANON EOS R5 and talking about getting the "hunts" done asap. Thescout@skiff.com replied to sonyamacoit@outlook.com on the same day at 12:38:39 GMT confirming the plan for Saturday 10th to be their next mission date. On the same date thescout@skiff.com

sent emails to sonyamacoit@outlook.com at 17:05:45 to 17:07:54 containing 2 different poems, sonyamacoit@outlook.com responded on 2024/02/09 at 09:16:42 GMT with a plaintext file attached containing the names of some animals and dates next to them. thescout@skiff.com replies to this at 09:20:06 GMT stating that things are heating up and they should plan an alternate.

On 2024/02/12 sonyamacoit@outlook.com sent an email to thescout@skiff.com between 07:22:48 GMT and 07:35:16 GMT discussing the logistics of the mission and getting through "the list" they also begin talking about enhancing security through emails. Marteneleroux@proton.me is also messaged when thescout@skiff.com discusses the date of the mission the animals and the time they will spend on the field from the 10th to the 20th and going to waypoint beta to begin with. For the contents of these emails see Appendix F Figure F.10.1-F.10.2

Incident #36 – Installed Programs

On 2024/02/08 at 13:48:15 GMT AnalogExif software is installed. Upon researching this program, it has come to light that this is a tool used for editing the metadata of film and digital images. See figure J.1.3 in Appendix J for more information.

Incident #37 - Autopsy

On 2024/02/09 at 09:14:41 GMT a .txt file named "the_list.txt" is created containing a list of animals and dates next to them. Next to elephants is says "done". See figure I.11.4.

Incident #38 - Images

On 2024/02/10 at 14:00:00 an image of a lion with the file name 01409656.jpg was taken on a Canon EOS 30 by Artist thescout. For the contents of the image see figure A.3.2. Also, at 14:58:00 an image of a lion and an elephant with the file name 00982904.jpg was taken on a Canon EOS 30 by Artist thescout. For the contents of the image see figure A.3.3.

Incident #39 - Images

On 2024/02/13 13:00:00 an image of a gazelle with the file name 01023088.jpg was taken on a Canon EOS R5 by Artist Sonya. For the contents of this image see Figure A.3.4. On 2024/02/13 14:00:00 an image of a gazelle with the file name 08218640.jpg was taken on a Yashica Mat-124G by Artist Sonya. For the contents of this image see Figure A.3.4.

Incident #40 - Images

On 2024/02/14 at 07:03:53 GMT an image of a gazelle with the file name 01664296.jpg was taken on a Canon EOS R5 by thescout – one of the camera models that Sonya has also used. See Figure A.3.6 for the contents of this image.

Incident #41 Shell Bags

Beginning on 2024/02/14 at 07:15:56 GMT until 2024/02/19 at 09:11:34 GMT. a file called "lion" was added to the folder "backup_07022". The file "antelop" was created and then was added to the folder "backup_07022". The file "giraff" was created and added to the folder "backup_07022". The file "lion" was created. Files were created and added to the folder "backup_07022" these files were "incident_", "nois", "buffal" and "hippo". See figure K.7 and K.8.

Incident #42 Images

Two buffalo pictures were uploaded on 2024/02/14 at 07:18:00 GMT. See the content of these images at figures A.5.12 - 5.14

Incident #43 - Email

On 2024/02/14 sonyamacoit@outlook.com began an email thread to marteneleroux@proton.me and thescout@skiff.com between 07:21:39 GMT to 07:30:57 discussing the lions and checking if they were or weren't tailed and discussing moving on to Waypoint Charlie, this also included a strange poem from thescout@skiff.com.

On 2024/02/16 sonyamacoit@outlook.com began another email thread between themself, thescout@skiff.com and merteneleroux@proton.me between 07:15:41 GMT- 07:25:31 GMT during this thread they discuss the fact that they were able to retrieve good material and that the recent missions have been very close calls and that they are sure someone is tailing them. Thescout@skiff.com suggests using encryption to ensure communications are kept safe. After this point they decide to go to other waypoints 2 more times and speak in another language for now. To view the full contents of this email thread, see Appendix F Figure F.11.1

Incident #44 Images

On 2024/02/16 at 07:12:12 GMT nine images of lions (one including an elephant). See the content of these images at figures A.5.46 - A.5.53.

Incident #45 Browser History and Web Search

On 2024/02/16 09:52:00 - 09:53:25. Sonya searched on edge about hunting hippos from the following websites at 09:52:00 - 09:53:24. Sonya then looked at the "2024-2025 South Africa Hunting Price List" for the "Big Game Hunting Adventures". See figures E.2.1.42-44.

Incident #46 Autopsy

On 2024/02/19 09:11:07 GMT mp4 video of a hippo found through autopsy - dates match up with similar photos taken by sonya around the same time in the physical imaging evidence. See figure I.11.3 for a screenshot of the video file.

Incident #47 Images

On 2024/02/19 09:11:33 GMT thirteen images of hippos and one video of a hippo were backed up onto the hdd drive (see figure A.5.54 - A.5.67). Many of these images match those found in the recycling bin as seen in A.2.20 compared to A.5.5.10. These were mainly taken using the Canon Eos 30, Canon Eos R5 and Yashica Mat-124g cameras.

Incident#48 Images deleted

On 2024/02/19 at 09:11:33 GMT 26 photos have been moved to the recycling been including those of African buffalos and hippos. See all figures A.2.1 - A.2.25 for all the images in question.

Incident #49 Web searching and browser history

2024/02/19 09:17:11 - 09:24:19. Sonya researched on edge about different encryption software (Axcrypt, VeraCrypt, Gpg4win). Sonya began researching about how to go into hiding and how to survive in hiding. She then started again looking at encryption on edge at the following websites. See figure E.2.45-46

Incident #50 Autopsy

2024/02/19 09:20:32 various files to do with VeraCrypt found including "VeraCrypt Hidden Operating System.html" on Sonya's machine. See figure I.11.2

Incident #51 Run Programs

On 2024/02/19 at 09:22:00 GMT to 2024/02/22 14:13:59 GMT, the executable VERACRYPT SETUP 1.26.7.EXE was run on the subject device, initiating the installation of VeraCrypt, a tool used to create encrypted containers and perform full disk encryption to protect stored data. The installation file GPG4WIN-4.3.0.EXE was executed. GPG4Win is an encryption suite designed to enable secure communication and data protection using public key cryptography. Shortly after, at 09:25:09 GMT, KLEOPATRA.EXE was launched. Kleopatra, the graphical key management tool included in the GPG4Win suite, remained active across multiple sessions until 2024/02/22 14:13:53 GMT. This application allows users to manage encryption keys, encrypt and decrypt files, and digitally sign communications. At 09/25/16 GMT on 2024/02/19, GPG-AGENT.EXE, a background process responsible for securely handling private key operations, was initiated. This process continued running intermittently through to 2024/02/22 14:13:59 GMT. Similarly, GPGCONF.EXE was executed at 09:25:18 GMT on 2024/02/19 and remained active across sessions until 2024/02/22 14:13:56 GMT. GPGConf is used to adjust and manage GnuPG encryption settings and operational preferences. On

2024/02/20 at 09:07:44 GMT, GPG-CONNECT-AGENT.EXE was observed starting, remaining active through to 2024/02/22 14:13:59 GMT. This application facilitates secure connections between encryption agents and client applications. See figures J.2 index 7-49

Incident #52 - Email

On 2024/02/19 sonyamacoit@outlook.com begins a thread with martneleroux@proton.me and thescout@skiff.com in this thread Sonya and the scout begin discussing encryption and how to do it, this occurs between 09:28:23 GMT and 09:42:47 GMT. Notably, at 09:32:43 GMT marteneleroux@proton.me states that he is out of the operation. Sonya also states that their "conservation" efforts have caused problems.

From 2024/02/20 at 11:33:17 GMT sonyamacoit@outlook.com and thescout@skiff.com enter an email thread, this thread ends on 2024/02/21 at 09:15:11 GMT in these emails sonya discusses encrypting files and sends their public key.

On 2024/02/21 at 08:10:08 GMT sonyamacoit@outlook.com receives an email in Afrikaans when translated it reads, "Can you read it?". Sonyamacoit@outlook.com replies saying "

I can, but I don't think it works." at 08:13:06 and finally, sonyamacoit@outlook.com receives an email that when the subject line is translated reads

"And now?" along with 2 encrypted attachments. At 08:22:07 GMT.

The rest of the thread includes the sharing of encrypted files, with one more translated subject line reading new information and 2 encrypted attachments received at 08:26:36. The rest of the emails contain only encrypted file attachments, and the last email is sent at 09:15:11 GMT.

At 08:51:24 GMT sonyamacoit@outlook.com entered an email thread of 5 messages with the subject line "Decryption pgp..." in response to this message were sent in Afrikaans discussing an escape route.

"Dit maak sin. Ek sal die fotos hou by my. Ons moet nou beplan om te vlug. Daar is 'n lugballon in die Masai Mara. Kom ons ontmoet mekaar by die plaza en dan maak ons 'n plan om daar uit te kom"

Translates to

"That makes sense. I'll keep the photos with me. We need to plan our escape now. There's a hot air balloon in the Masai Mara. Let's meet at the plaza and then we'll make a plan to get there."

Sonya then receives another 3 messages in Afrikaans which is as follows:

"Laat ek kies. Sien jou vanaand laat dan ry ons in the nag en kom more oggend daar uit."

This translates to

"Let me choose. See you tonight, then we'll drive at night and get out there tomorrow morning."

Then:

"Sit die inligting op die BitLocker To Go usb disk.

The destination will be Serena Airstrip HK0A"

And translates to

"Put the information on the BitLocker To Go usb disk.

The destination will be Serena Airstrip HK0A"

Finally, an email is received in which thescout@skiff.com discusses how he is confident their communications have been compromised. This is the final email in the thread and occurs at 09:14:49 GMT

The final email sent is from Sonya in response at 09:15:11 GMT containing encrypted attachments. To view the full email thread including contents and attachments, see Appendix F Figure F.12.1-F.12.2

Incident #53 Run programs

Between the times of 2024/02/20 at 09:07:44 GMT to 2024/02/22 at 14:13:59 GMT – GPG-Connect-Agent (GPG-CONNECT-AGENT.EXE): A component of GPG responsible for establishing secure connections between applications and cryptographic agents was ran. GPGSM (GPGSM.EXE): A GPG component designed for handling S/MIME encrypted email and managing digital certificates was also ran. Also noted was the core executable for GNU Privacy Guard (GPG), facilitating encryption, decryption, digital signing, and verification of files and messages. See Figures J.2 index 19-27

Incident #54 Shell Bags

On 2024/02/20 at 10:28:16 GMT. A folder called “ke” was created on the computer. See figure K.10.

Incident #55 Recycling Bin

A BitLocker discovery key was sent to the recycling bin by the account Sonya

Incident #56 Images

09:40:18 - 09:41:22 GMT 5 images were found in the cache. These included an image of a lion, a leopard, an image of another animal, 2 images of maps with locations such as "Leopard Lookout", "Leopards Lair", "Leopard's Village" and "Leopard Cliff Observation point" marked

Incident #57 Installed Programs

On 2024/02/21 at 19:16:10 GMT Mozilla Thunderbird email client is in installed programs. See figure J.1.4

Incident #58 USB

On 2024/02/22 at 13:55:01 GMT An external USB of model Alcor micro corp Flash Drive was attached, matching the physical description of the encrypted USB later found on Sonya’s person. See Figure I.3.1

Incident #59 Images

On 2024/02/26 at 07:04:53 GMT fourteen images of antelopes and three images of zebras were backed up onto the hdd drive showing various images of the animals. These were mainly taken using the Canon Eos 30, Canon Eos R5 and Yashica Mat-124g cameras. To view these images and their contents see figure A.5.15 - A.5.31

2. Description of Investigation

2.1 Job Description and Instructions

The analysts have been tasked with investigating and analysing digital evidence in relation to a Sonya Macoit who has been arrested in connection with the suspected trade and poaching of wildlife. It is the analysts' task to reconstruct events, find, locate and verify any relevant data relating to the charges within the acquired image. All images depicting wildlife trading, wildlife reconnaissance and poaching are to be located and documented. The analysts will provide an accurate reflection of the actions of Sonya Macoit and a detailed description of how the analysts came to this conclusion including evidence. The recovered evidence is then to be presented in a legally coherent document that is

considered admissible in court containing demonstrative, real, documentary and or testimonial evidence.

2.2 Description of Recovered / Examined Items

The analysts were provided with a virtual image of the Hard Drive from the suspects PC which was acquired by a response team at the suspects residence. The PC was shut down when the image was acquired. The Hard Drive containing the image was provided to the analysts by Chief Officer Van Der Schyff. The files provided were stored as “CrypticWilds.000” to “CrypticWilds.013” these were stored as binary files and contained within zipped files. The image was confirmed to be authentic and unaltered by confirming the MD5 and SHA1 hashes matches the hashes taken before the transfer. The analysts were also provided with a virtual image of a USB drive which was used in conjunction with the suspects PC. The USB containing the image was provided to the analysts by Chief Officer Van Der Schyff. The files provided were stored as “UsbCrypticWilds.001” to “UsbCrypticWilds.021” these were stored within a zip file. Along with this a text file named UsbCrypticWilds.001.txt”. This text file contained an FTK imager log for the USB drive.

2.3 Methodology

The methodology used will be that of the cognitive task model, as it provides an accurate description of the investigative process, explains the relationship between models and can easily incorporate information gathered. See the Figure I.5.1 below for a visual representation.

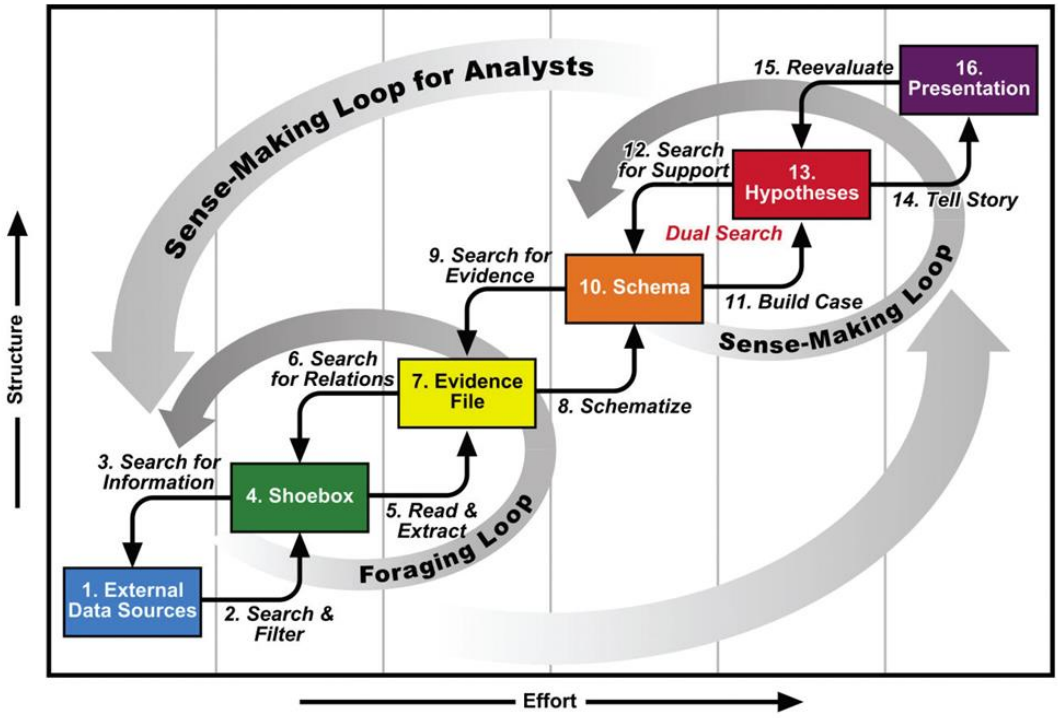


Figure I.5.1 - method used to create a digital forensics report.

This methodology has been deemed most appropriate as it has been recommended by Chief Officer Van Der Schyff. The model allows for back tracking and promotes repetition of certain areas making it more flexible as many searches for evidence and relations are made whilst still clearly creating a path forward to be followed.

The practical steps will be the following:

Acquisition of the device:
Both the hard drive and USB acquired both were found in a powered off state and so are acquired statically. The seized items were provided by Chief Officer Van Der Schyff as can be seen in the chain

of custody form. The files then had both their MD5 hash and SHA256 hashes calculated to ensure that they were transferred successfully without breaking the chain of custody ensuring legitimacy.

Disk exploration:

The tools used in disk exploration excluding are as follows:

- Autopsy
- BrowsingHistoryView
- Command line
- Custom script “hash_cracker_SHA1.sh” see figure I.2.1
- Custom script “photots_searcher.cpp” see figure I.1.1
- DB Browser for SQLite
- FTK imager
- Regripper
- Volatility v3
- TimelineExplorer
- RegistryExplorer

The four members were assigned sections to work on:

- Encryption - Jam Buckley
- Internet artifacts- Melissa Forrest
- Timeline - Adam Henderson
- Physical searching – Ezra Lawrie
- Logical searching directed searching and memory forensics were allocated to all.

These were treated as guidelines as when members were sick or absent others were to fill in their roles to keep the project on track. Meetings were held twice a week to assess where the analysts progress was, assign goals to be achieved by the next meeting and in someone's absence reallocate their work among other analysts.

Schema:
The grouping of case data was split into eight categories, the appendix including ninth, tenth, eleventh and twelfth being chain of custody documentation, glossary, evidentiary files and timeline whilst the other eight relate directly to data found on Sonya’s device. Images, Documents, Browser history, E-mails, Miscellaneous, Shell bags, Installed/run programs and Encryption. Whilst some overlap may exist this is an excepted outcome as all data will most likely bear some connection to other data formats. This system best organises data into an easy format for referencing to aid in readability. Incidents are categorised with similar headings, sometimes bearing the mark of two or more where and when appropriate to deal with any overlap. If anything does not fit into the above headings it will be categorised as miscellaneous.

File Integrity:
To ensure file integrity the raw files that contained the details of the USB and HDD were set to read only ensuring they were never accessed in a read write format. The images were fused into a new file who had its integrity checked routinely (see figure I.4.1 - I.4.3) to ensure that the raw files were never altered. The MD5 hash of extracted files is documented to show no alterations have been made using the command md5sum on Linux and various hash calculating algorithms on windows all recorded in the appendix.

Disk audit:
To discover the nature of the files in use disk audits are performed on both drives. This is to calculate the start sector so that loopback devices can be formed to allow emulated access to the drives. The analysts used multiple packages including fdisk and other command line tools that can be found in Figure I.6. The USB had BitLocker encryption so read as corrupt to a Linux machine as the format is not recognisable. The encrypted data is revealed upon a hexdump being performed. Much of the disk

audit for the USB had previously been completed as is seen in item #004_TXT from the court report (Figure B.4.1) so only confirmation of the initial sector size had to be acquired (Figure I.7.1).

File extraction:
In order to investigate specific files, they are required to be extracted. On Linux the command cp is used to create a copy of the file that can be accessed outside of the mounted image allowing the use of specialist tools to investigate. The hashes of these files are recorded to ensure their integrity remains intact. Certain tools such as autopsy allow for files to be viewed in a read only format within a graphical interface, this is not extraction but viewing so the integrity remains intact.

The analysts used platforms such as autopsy where most of the evidence discovery was performed including viewing and logging events such as browser history, images, documents, emails and files pertaining to the charges levelled against Sonya Macoit. Further evidence was analysed using tools more suited for specific needs such as regripper and FTK imager.

2.4 Analysis

2.4.1 Disk Audit HDD

The fdisk package was used to begin the disk audit. The output showed that each sector was made up of 512 bytes and that there were 4 partitions. The command used was fdisk –l Crypticwilds.000.raw. See I.6.1.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# fdisk -l CrypticWilds.000.raw
Disk CrypticWilds.000.raw: 64 GiB, 68719476736 bytes, 134217728 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 36B5D08B-1AE0-41AD-A814-06B4A85686EF

Device                    Start       End   Sectors  Size Type
CrypticWilds.000.raw1      2048    206847    204800  100M EFI System
CrypticWilds.000.raw2    206848    239615     32768   16M Microsoft reserved
CrypticWilds.000.raw3    239616 100847615 100608000   48G Microsoft basic data
CrypticWilds.000.raw4 100847616 102397951   1550336  757M Windows recovery envir
```

Figure I.6.1 Disk audit, partition analysis using fdisk

Next mmls were used to confirm these findings. The command used was: mmls CrypticWilds.000.raw. The output of this can be seen in I.6.2.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# mmls CrypticWilds.000.raw
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0000206847   0000204800   EFI system partition
005:  001       0000206848   0000239615   0000032768   Microsoft reserved partition
006:  002       0000239616   0100847615   0100608000   Basic data partition
007:  003       0100847616   0102397951   0001550336
008:  -------   0102397952   0134217727   0031819776   Unallocated
```

Figure I.6.2 Disk audit, partition analysis mmls

After confirming the results of the fdisk package for sector size and disk size, the analyst discovered a hidden partition in the space marked as unallocated within the disk. This was further investigated using the parted tool. The output of this can be seen in I.6.3.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# parted CrypticWilds.000.raw print free
Warning: Unable to open /home/cmp209/Desktop/mount_points/windows/CrypticWilds.000.raw read-write (Permission denied).
/home/cmp209/Desktop/mount_points/windows/CrypticWilds.000.raw has been opened read-only.
Model:  (file)
Disk /home/cmp209/Desktop/mount_points/windows/CrypticWilds.000.raw: 68.7GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name                          Flags
        17.4kB  1049kB  1031kB  Free Space
 1      1049kB  106MB   105MB   fat32        EFI system partition          boot, esp
 2      106MB   123MB   16.8MB               Microsoft reserved partition  msftres
 3      123MB   51.6GB  51.5GB  ntfs         Basic data partition          msftdata
 4      51.6GB  52.4GB  794MB   ntfs                                       hidden, diag
        52.4GB  68.7GB  16.3GB  Free Space
```

Figure I.6.3 Disk audit, partition analysis parted

Finally, a hexdump was performed on the disk image to confirm []. The output from this can be seen in I.6.4.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sudo dd if=CrypticWilds.000.raw bs=512 count=1 | hexdump -C
00000000  33 c0 8e d0 bc 00 7c 8e  c0 8e d8 be 00 7c bf 00  |3.....|......|..|
00000010  06 b9 00 02 fc f3 a4 50  68 1c 06 cb fb b9 04 00  |.......Ph.......|
00000020  bd be 07 80 7e 00 00 7c  0b 0f 85 0e 01 83 c5 10  |....~..|........|
00000030  e2 f1 cd 18 88 56 00 55  c6 46 11 05 c6 46 10 00  |.....V.U.F...F..|
00000040  b4 41 bb aa 55 cd 13 5d  72 0f 81 fb 55 aa 75 09  |.A..U..]r...U.u.|
00000050  f7 c1 01 00 74 03 fe 46  10 66 60 80 7e 10 00 74  |....t..F.f`.~..t|
00000060  26 66 68 00 00 00 00 66  ff 76 08 68 00 00 68 00  |&fh....f.v.h..h.|
00000070  7c 68 01 00 68 10 00 b4  42 8a 56 00 8b f4 cd 13  ||h..h...B.V.....|
00000080  9f 83 c4 10 9e eb 14 b8  01 02 bb 00 7c 8a 56 00  |............|.V.|
00000090  8a 76 01 8a 4e 02 8a 6e  03 cd 13 66 61 73 1c fe  |.v..N..n...fas..|
000000a0  4e 11 75 0c 80 7e 00 80  0f 84 8a 00 b2 80 eb 84  |N.u..~..........|
000000b0  55 32 e4 8a 56 00 cd 13  5d eb 9e 81 3e fe 7d 55  |U2..V...]...>.}U|
000000c0  aa 75 6e ff 76 00 e8 8d  00 75 17 fa b0 d1 e6 64  |.un.v....u.....d|
000000d0  e8 83 00 b0 df e6 60 e8  7c 00 b0 ff e6 64 e8 75  |......`.|....d.u|
000000e0  00 fb b8 00 bb cd 1a 66  23 c0 75 3b 66 81 fb 54  |.......f#.u;f..T|
000000f0  43 50 41 75 32 81 f9 02  01 72 2c 66 68 07 bb 00  |CPAu2....r,fh...|
00000100  00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66  |.fh....fh....fSf|
00000110  53 66 55 66 68 00 00 00  00 66 68 00 7c 00 00 66  |SfUfh....fh.|..f|
00000120  61 68 00 00 07 cd 1a 5a  32 f6 ea 00 7c 00 00 cd  |ah.....Z2...|...|
00000130  18 a0 b7 07 eb 08 a0 b6  07 eb 03 a0 b5 07 32 e4  |..............2.|
00000140  05 00 07 8b f0 ac 3c 00  74 09 bb 07 00 b4 0e cd  |......<.t.......|
00000150  10 eb f2 f4 eb fd 2b c9  e4 64 eb 00 24 02 e0 f8  |......+..d..$...|
00000160  24 02 c3 49 6e 76 61 6c  69 64 20 70 61 72 74 69  |$..Invalid parti|
00000170  74 69 6f 6e 20 74 61 62  6c 65 00 45 72 72 6f 72  |tion table.Error|
1+0 records in
1+0 records out
512 bytes copied, 0.000420308 s, 1.2 MB/s
00000180  20 6c 6f 61 64 69 6e 67  20 6f 70 65 72 61 74 69  | loading operati|
00000190  6e 67 20 73 79 73 74 65  6d 00 4d 69 73 73 69 6e  |ng system.Missin|
000001a0  67 20 6f 70 65 72 61 74  69 6e 67 20 73 79 73 74  |g operating syst|
000001b0  65 6d 00 00 00 63 7b 9a  00 00 00 00 00 00 00 00  |em...c{.........|
000001c0  02 00 ee fe 3f a1 01 00  00 00 ff ff ff ff 00 00  |....?...........|
000001d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
00000200
```

Figure I.6.4 Disk audit, hex dump

To ensure the version was in fact windows eleven ntoskrnl.exe was found in system32. It was created 2024/02/16, the is after the release of windows eleven in 2021/11/9 and the has of the file, licence.rtf is dated to 2021 however does not specify the specific version of windows in use. Boot.ini was not checked as it is easily altered by a malicious actor.

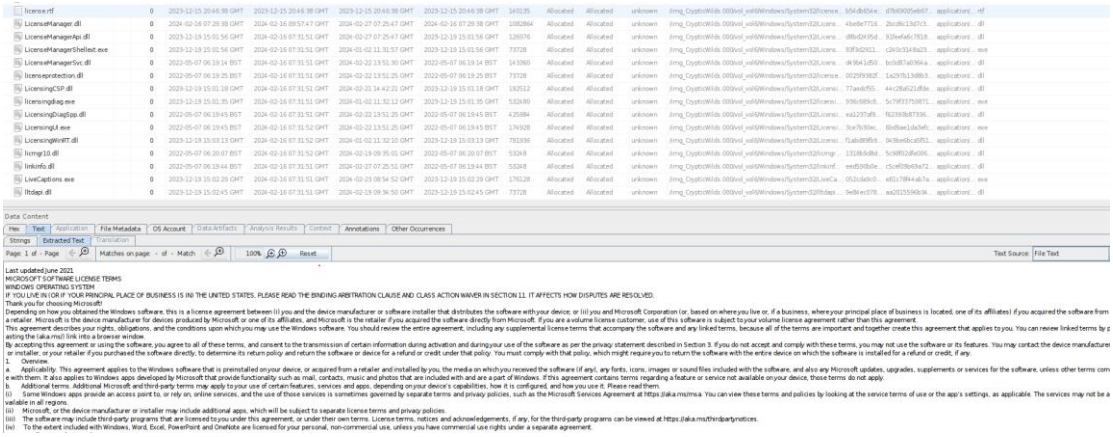


Figure B.3.1 Disk audit, licence documentation

To perform file exploration a loop back device was set up using the image and an image was setup using said loopback device. Using the following commands:

sudo losetup -o 122683392 /dev/loop30 CrypticWilds.000.raw
sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/mount_points/suspectDrive
cd /home/cmp209/Desktop/mount_points/suspectDrive

122683392 being the offset calculated for the image.

```
cmp209@cmp209-virtual-machine:~$ sudo su
[sudo] password for cmp209:
Sorry, try again.
[sudo] password for cmp209:
root@cmp209-virtual-machine:/home/cmp209# ls
autopsy  Desktop  Documents  Downloads  evidence  hs_err_pid12837.log  hs_err_pid2372.log  hs_err_pid2403.log  hs_err_pid2405.log  hs_err_pid3101.log  jd  ModuleOutput  Music  Pictures  Public  R3_test  snap  src  Templates  Videos  Zeitline
root@cmp209-virtual-machine:/home/cmp209# cd Desktop
root@cmp209-virtual-machine:/home/cmp209/Desktop# ls
autopsy.desktop  bless.desktop  cases  firefox.desktop  fred.desktop  johnny.desktop  libreoffice-calc.desktop  libreoffice-writer.desktop  mount_points  okteta.desktop  org.gnome.Terminal.desktop  tools  win11.md5ListOnly.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop# cd /home/cmp209/Desktop/cases/CrypticWlds/comp/
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWlds/comp# ls
CrypticWlds.000  CrypticWlds.005  CrypticWlds.010    cw_evidence0to13.7z            output_Tue_Feb_25_09_22_07_2025
CrypticWlds.001  CrypticWlds.006  CrypticWlds.011    cw_evidence9to9.7z             timeline
CrypticWlds.002  CrypticWlds.007  CrypticWlds.012    extftool
CrypticWlds.003  CrypticWlds.008  CrypticWlds.013    output_Tue_Feb_25_09_20_17_2025
CrypticWlds.004  CrypticWlds.009  cw_evidence0to4.7z  output_Tue_Feb_25_09_20_55_2025
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWlds/comp# sudo affuse CrypticWlds.000 /home/cmp209/Desktop/mount_points/windows/
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWlds/comp# cd /home/cmp209/Desktop/mount_points/windows/
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# ls -lah
total 4.0K
drwxr-xr-x 2 root   root      0 Jan  1  1970 .
drwxrwxr-x 5 cmp209 cmp209 4.0K Mar 11 09:25 ..
-r--r--r-- 1 root   root    64G Jan  1  1970 CrypticWlds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sudo losetup -o 122683392 /dev/loop30 CrypticWlds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# cd /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls -lah
total 1.3G
drwxrwxrwx 1 root   root   4.0K Feb 27  2024 .
drwxrwxr-x 5 cmp209 cmp209 4.0K Mar 11 09:25 ..
drwxrwxrwx 1 root   root      0 Jan  2  2024 $Recycle.Bin
drwxrwxrwx 1 root   root   4.0K Feb 16  2024 $UpdateAgent
lrwxrwxrwx 2 root   root     52 Dec 15  2023 'Documents and Settings' -> /home/cmp209/Desktop/mount_points/suspectDrive/Users
-rwxrwxrwx 2 root   root     12K Mar  4  2024 DumpStack.log.tmp
drwxrwxrwx 1 root   root      0 Feb 27  2024 $WINDOWS.~BT
-rwxrwxrwx 1 root   root   1.3G Mar  4  2024 pagefile.sys
drwxrwxrwx 1 root   root      0 May  7  2022 PerfLogs
drwxrwxrwx 1 root   root   4.0K Jan  5  2024 ProgramData
drwxrwxrwx 1 root   root   8.0K Feb 21  2024 Program Files
drwxrwxrwx 1 root   root   4.0K Feb 19  2024 Program Files (x86)
drwxrwxrwx 1 root   root      0 Dec 15  2023 Recovery
-rwxrwxrwx 1 root   root     16M Mar  4  2024 swapfile.sys
drwxrwxrwx 1 root   root   4.0K Feb 20  2024 System Volume Information
drwxrwxrwx 1 root   root   4.0K Dec 15  2023 Users
drwxrwxrwx 1 root   root     24K Feb 20  2024 Windows
```

Figure I.6.5 Disk audit, loopback test

Additionally, a malware scan was run to see if any malware may be on the device. All items flagged were recognised as not dangerous confirming a lack of malware of any known kind.

2.4.2 Disk Audit USB

Alongside the disk provided as can be seen as item #004_TXT in the chain of custody document the following file was provided. It shows a majority of the information about the USB however the start index of the first partition is missing and will have to be recovered.

UsbCrypticWilds.001.txt

```
Created By AccessData® FTK® Image 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: 001DISK_01
Unique description: USB32G_Sonya
Examiner: K
Notes: seized at roadblock

--------------------------------------------------------------

Information for D:\Evidence Seized\UsbCrypticWilds:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3,849
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 61,849,600
[Physical Drive Information]
 Drive Model: Generic Flash Disk USB Device
 Drive Serial Number: 15E12348
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 30200 MB
 Sector count:    61849600
[Computed Hashes]
 MD5 checksum:    a547247ee2fd3f51182f28c273633fc4
 SHA1 checksum:   dd54cec4e8ebef11163715798b805c73720d9843
```

Figure B.4.1 USB Disk audit, UsbCrypticWilds.001.txt

In figure I.7.1 below partition analysis was performed on the fused partition on the windows machine. This was only to find start sector and number of sectors on the USB. The results of which are, 2048 and 1 respectively.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sgdisk -p UsbCrypticWilds.001.raw
Warning! Disk size is smaller than the main header indicates! Loading
secondary header from the last sector of the disk! You should use 'v' to
verify disk integrity, and perhaps options on the experts' menu to repair
the disk.
Caution: invalid backup GPT header, but valid main header; regenerating
backup header from main header.

Warning! Error 25 reading partition table for CRC check!
Warning! One or more CRCs don't match. You should repair the disk!
Main header: OK
Backup header: ERROR
Main partition table: OK
Backup partition table: ERROR

****************************************************************************
Caution: Found protective or hybrid MBR and corrupt GPT. Using GPT, but disk
verification and recovery are STRONGLY recommended.
****************************************************************************
Disk UsbCrypticWilds.001.raw: 39936000 sectors, 19.0 GiB
Sector size (logical): 512 bytes
Disk identifier (GUID): E66B9B8A-08DC-44BF-8924-FA59334F7660
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 61849566
Partitions will be aligned on 2048-sector boundaries
Total free space is 2045 sectors (1022.5 KiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048        61849535   29.5 GiB    0700  Main Data Partition
```

Figure I.7.1 USB Disk audit, partition analysis sgdisk

In figure I.3.1 the details of the disk are recorded for a Alcor micro corp Flash Drive USB drive. This matches the description of the drive provided and was found in possession of Sonya as can be seen on the court report as item #001_DISK_01. There is no OS on a USB, so it does not need to be recovered.

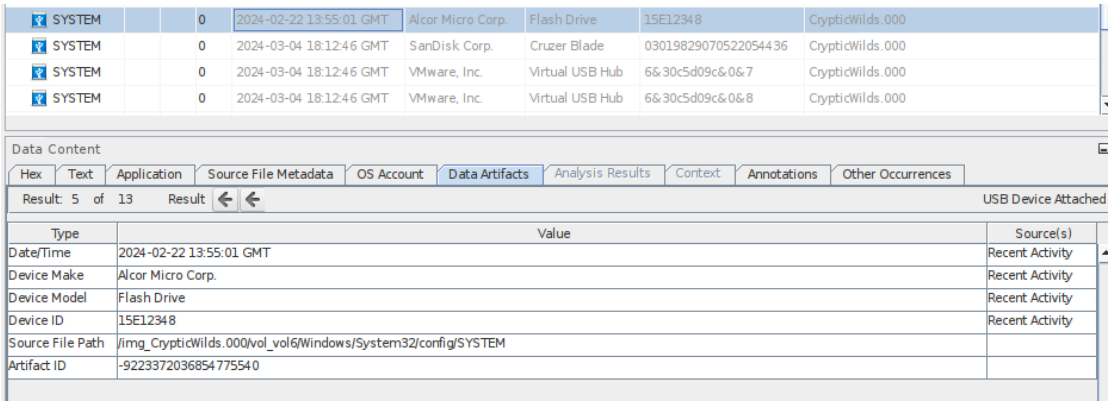


Figure I.3.1 - Alcor micro corp Flash Drive USB drive attachment records

2.4.3 Windows system Verification

To begin with the disk had to be fused see figure I.4.1 below

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# cd comp
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# ls
CrypticWilds.000  CrypticWilds.005  CrypticWilds.010    cw_evidence10to13.7z            output_Tue_Feb_25_09_22_07_2025
CrypticWilds.001  CrypticWilds.006  CrypticWilds.011    cw_evidence5to9.7z              timeline
CrypticWilds.002  CrypticWilds.007  CrypticWilds.012    exiftool
CrypticWilds.003  CrypticWilds.008  CrypticWilds.013    output_Tue_Feb_25_09_20_17_2025
CrypticWilds.004  CrypticWilds.009  cw_evidence0to4.7z  output_Tue_Feb_25_09_20_55_2025
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# sudo affuse CrypticWilds.000 /home/cmp209/Desktop/mount_point
s
fuse: mountpoint is not empty
fuse: if you are sure this is safe, use the 'nonempty' mount option
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# sudo affuse CrypticWilds.000 /home/cmp209/Desktop/mount_point
s/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp#
```

Figure I.4.1 Fusing the disk

Then with the image created the MD5 and SHA1 hashes were compared against those provided by Chief Officer Van Der Schyff to ensure integrity has been maintained and to verify the legitimacy of any actions to follow using tools such as autopsy. Those provided MD5: aebd2d140eaf215e1a8554d008c5e2b3 SHA1: 3c7bae35a28e12d67ed62cb9c09ee8e5935047fe match

those found. The commands md5sum and sha1sum were used to find the hashes of CrypticWilds.000.raw.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# cd /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls
CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# md5sum CrypticWilds.000.raw
aebd2d140eaf215e1a8554d008c5e2b3  CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sha15sum CrypticWilds.000.raw
Command 'sha15sum' not found, did you mean:
  command 'sha1sum' from deb coreutils (8.32-4.1ubuntu1.2)
Try: apt install <deb name>
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sha1sum CrypticWilds.000.raw
3c7bae35a28e12d67ed62cb9c09ee8e5935047fe  CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive#
```

Figure I.4.2 Hash verification of the disk

To find the windows version a number of methods were employed, to begin with it was previously stated that the system in question is Windows as the results of the disk audit showed Microsoft reserved partitions and windows recovery environments. Firstly, it was noted the lack of a build in timeline feature that was present in Windows 10. Secondly when carving history artifacts, the only operating system found within any of the searches was windows 11 as can be seen in figure E.1.1 below.

```
636 https://www.google.com/search?q=hardening+a+windows+11+machine+to+counter+digital+forensics&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hardening+a+windows+11+machine+to+counter+digital+forensics&gs_lcrp=EgZja
HjvbWUyC0gAEEUYORigATIHCAEQIRigAdIBCTE1NDMzajBqNKgCALACAA&sourceid=chrome&ie=UTF-8 hardening a windows 11 machine to counter digital forensics - Google Search 2 0 1335159565851829 0
637 https://medium.com/@larry-baldwin/hardening-windows-11-d600ab21f926 Hardening Windows 11. This article outlines the various steps... | by Larry Baldwin | Dec, 2023 | Medium 1 0 1335168862884942 8 0
638 https://learn.microsoft.com/en-gb/windows/client-management/mdm/ Configuration Service Provider - Windows Client Management | Microsoft Learn 2 0 1335168862398245 9 0
639 https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ BitLocker overview - Windows Security | Microsoft Learn 2 0 1335168863165167 07 0
640 https://www.google.com/search?q=hunting+elephant+with+bow+and+arrow&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hunting+elephant+&gs_lcrp=EgZjaHjvbWUqBwgCEAAYgAQyBggAEEUYOTIHCAEQABiABDIHCAIQABiABDIHCA
MQABiABDIKCAQQABgPGBYYHjIKCAUQABgPGBYYHjIICAYQABgWGB4yCAgHEAAYFhgeMggJCBAAGBYYHjIICAkQABgWGB7SAQg4NjcwajBqN6gCALACAA&sourceid=chrome&ie=UTF-8 hunting elephant with bow and arrow - Google Search 3 0 1335168
8654708378 0
641 https://www.africahunting.com/threads/bowhunting-elephant-best-setup.5043/ Bowhunting ELEPHANT Best Setup | AfricaHunting.com 1 0 1335168864807523 1 0
642 https://www.google.com/search?q=antiforensic+techniques&rlz=1C1ONGR_en-GBGB1089GB1089&oq=antiforensic+techniques&gs_lcrp=EgZjaHjvbWUyBggAEEUYOTIJCAEQABgKGIAE0qEINTIyM2owajecAqCwAqA&sourceid=chrome&ie
```

Figure E.1.1 Windows 11 history carving from raw disk

The logical next step was to mount the disk and perform a logical investigation of the files to find confirmation of the windows version. This began with mounting the disk to gain read only file access.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sudo losetup -o 122683392 /dev/loop30 CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/m
ount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# cd /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls -lah
total 1.3G
drwxrwxrwx 1 root   root   4.0K Feb 27  2024  .
drwxrwxr-x 6 cmp209 cmp209 4.0K Apr 18 01:55  ..
drwxrwxrwx 1 root   root      0 Jan  2  2024 '$Recycle.Bin'
drwxrwxrwx 1 root   root   4.0K Feb 16  2024 '$WinREAgent'
lrwxrwxrwx 2 root   root     52 Dec 15  2023 'Documents and Settings' -> /home/cmp209/Desktop/mount_points/suspectDrive/Users
-rwxrwxrwx 2 root   root    12K Mar  4  2024  DumpStack.log.tmp
drwxrwxrwx 1 root   root      0 Feb 27  2024  OneDriveTemp
-rwxrwxrwx 1 root   root   1.3G Mar  4  2024  pagefile.sys
drwxrwxrwx 1 root   root      0 May  7  2022  PerfLogs
drwxrwxrwx 1 root   root   4.0K Jan  5  2024  ProgramData
drwxrwxrwx 1 root   root   8.0K Feb 21  2024 'Program Files'
drwxrwxrwx 1 root   root   4.0K Feb 19  2024 'Program Files (x86)'
drwxrwxrwx 1 root   root      0 Dec 15  2023  Recovery
-rwxrwxrwx 1 root   root    16M Mar  4  2024  swapfile.sys
drwxrwxrwx 1 root   root   4.0K Feb 20  2024 'System Volume Information'
drwxrwxrwx 1 root   root   4.0K Dec 15  2023  Users
drwxrwxrwx 1 root   root    24K Feb 20  2024  Windows
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive#
```

Figure I.4.3 Mounting the disk

Then making use of the tool regripper to extract the contents of SOFTWARE into a text file.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop# regripper -r SOFTWARE -f software > SOFTWARE_details.txt
Parsed Plugins file.
Launching allowedenum v.20200511
allowedenum complete.
Launching appcompatflags v.20200525
appcompatflags complete.
Launching appinitdlls v.20200427
appinitdlls complete.
Launching appkeys v.20200517
appkeys complete.
```

Figure I.4.4 Regripper use on SOFTWARE registry

That could then be searched for the ReleaseID revealing a release ID of 2009, whilst this is also the case for windows 10 as no timeline feature is present this confirms the disk to be windows 11.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop# grep -i ReleaseId SOFTWARE_details.txt
ReleaseID                   2009
```

Figure I.4.5 GREP regripper output for ReleaseID

2.4.4 System Information

2.4.4.1 Basic System Information

The analysts used the regripper command line tool and Autopsy to analyse the registry on the image of the PC. Using the Autopsy tool the analysts were able to find some basic information about the PC being used including the Computer Name, Operating system and basic system information. Figure? Shows the Computer Name, Figure I.4.5 Shows the release ID of the Operating system confirming that the user used a Windows 11 operating system as there was no windows timeline which is a feature of all Windows 10 systems. Figure I.4.5 shows the ReleaseID of the operating system.

```
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-K6L0LLR
TCP/IP Hostname = DESKTOP-K6L0LLR
----------------------------------------
```

Figure I.9.5: Computer Name information from regripper

```
root@cmp209-virtual-machine:/home/cmp209/Desktop# grep -i ReleaseId SOFTWARE_details.txt
ReleaseID                2009
```

Figure I.4.5 GREP regripper output for ReleaseID

2.4.4.2 User Profiles Information

The analysts used regripper to investigate the User accounts that were created and used on the PC. Only one profile was found under the name "Sonya". This suggests that the only person to use this PC was the suspect. Figure I.9.4 Shows the extracted information.

```
Username        : Sonya [1001]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2023-12-15 13:23:12Z
Name            :
Last Login Date : 2024-02-27 07:26:48Z
Pwd Reset Date  : 2024-02-21 09:39:04Z
Pwd Fail Date   : 2024-02-20 09:07:17Z
Login Count     : 83
Embedded RID    : 1001
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

Figure I.9.4: System Information about the User

2.4.4.3 General System Information

The analysts used regripper to extract further system information including the discovery of multiple USB devices and enumeration of Bluetooth devices. This information was used after the seizure of the USB drive that contained further evidence and had been mentioned on multiple occasions in emails sent and received by the suspect. The information extracted can be found in Appendix I in Figures I.9.1, I.9.2 and I.9.3.

2.4.5 Encryption

Kleopatra

As seen in Incident 14 from the time 19/02/2024 at 09:25:04 to on 20/2/2024 at 09:07:37 Kleopatra was acquired and run to encrypt several files into .gpg files (G.3.6). The analysts used a custom script (I.2.1 - I.2.2) to break the SHA1 file found on Sonyas person (B.2.1) 338526e5c661ccb2655dc7886d29f700512a906c the result of which is "conservation". This password was then used in tandem with the private key found in (G.3.3) against the list of .gpg files found in (G.3.2) using the recursive search command in a mounted drive 'find. -type f –name "*.xxx"' where xxx is pgp, gpg and asc respectively to find the encrypted files and any keys to decrypt them with. As

seen in (G.3.5) none of the files decrypted has verified key signatures, so using the PGP public key file found in Sonya's e-mails (F.2.1) and attempt to use it to verify the encrypted files (G.3.5.2).

When the files are decrypted, they were attributed to the signature key: F882AC885E2A4CCBD56ADC78B87EBB6DD62A4F84 the same signature key found in the e-mail Sonya had send in (F.2.1). This confirms that the file was encrypted by the user of the account Sonya. Of the files encrypted, (G.3.6), one contained an invalid BitLocker key with a 32-digit key, another the windows 11 security handbook, another the wildlife crime store card and the fourth a text document that notes: elephants done lions 10/2 antelope 13/2 giraffe 15/2 hippos 16/2 cape buffalo 19/2. Additionally in I.8.1 kleopatra.exe was still running and had not in fact been turned off. As seen in G.3.5.1 the files were encrypted on Tue 20 Feb 2024 09:21:25 using Kleopatra.

Poetry encryption
Seen in Incident 15 from 2024/01/05 19:21:37 - 2024/02/16 07:20:52 where poetry was exchanged but on 2024/01/09 at 07:37:42 searches were made for poetry encryption, (E.3.1 index 23). The poetry seen in these incidents appears to be AI generated and was being sent before the search for encryption via poetry. Poetry encoding also requires a numerical key that doesn't seem to be present in the e-mails. Moreover, the communications switched to Afrikaans to obfuscate the messages.

USB
An encrypted USB was found on Sonya's person as seen as #001_DISK_01 in the Chain of custody form. As seen in G.4.1 this image was mounted using FTK imager mirroring the FTK imager used to segment as seen in B.4.1, this is just to best replicate the manner in which it was segmented to improve the validity of the disk. G.4.2 confirms the suspicion that the disk is encrypted. Using the key ID shown a search using Autopsy was made throughout the hdd disk to find the BitLocker key file that corresponds to the drive (see G.4.3). This revealed two images and a .txt file that sated that the images were taken at leopard lookout (see G.4.4).

Steghide
As seen in G.1.1 and incident #13 at 2024/01/24 13:40:27 steghide was last run. This does not confirm if it was in fact used and whilst images such as 44232256.jpg and 47536064.jpg may seem to be altered with steghide no conclusive evidence can be found that showed any one file being encrypted with steghide. Furthermore in I.8.2 scans using volatility show that steghide was not used in the comma line, and as steghide is a command line application it stands to reason that the instance of the .exe running was not called correctly as the steghide UI was never seen to be installed on the device.

2.4.6 Evidence Discovery and tools

The analysts main tool used to discover and extract evidence was autopsy version 4.21.0. This was used on the windows lab machines under the case name CrypticWilds and the case number 001. The virtual image of the hard drive was used as a data source in autopsy including all partitions, and autopsy ingested the Plaso module. This allowed the analysts to explore email threads, images, installed programs, web cache, web history and other important information. These were then extracted or screenshotted and placed into the appendices within the report. Further exploration through autopsy involved run programs, shell bags and Exif metadata.

Other tools used were regripper, volatility v3 and registry explorer to explore the registry, windows 11 artifacts and timeline explorer to explore the browser history of the user. These were invoked using command line, the most common tool used on Linux to investigate the mounted disk, hash checks to verify file integrity and the running of custom scripts.

BrowsingHistoryView was used to examine browsing history extracted from Microsoft Edge and Google Chrome. A forensic image of the subject's device was created and mounted using a loopback device to enable secure, read-only access. From the mounted image, browsing history files were located, copied, and backed up. BrowsingHistoryView was then employed to parse the recovered history, allowing for keyword searches and manual review to identify websites relevant to the investigation. The results of this analysis are presented in a table in Appendix E.4.2.

DB Browser for SQLite was used to examine browser artefacts stored in SQLite database files. Access to the SQLite database files was facilitated through a Python-based local server instance, enabling interaction with DB Browser for SQLite via a web interface. Relevant artefacts were then extracted and securely stored on the examination machine for subsequent analysis. This examination included cookies, top sites, bookmarks, login data, and autofill records. The cookie analysis, detailed in Appendix E.5.1, identified domain interactions and activity timestamps. The top sites and bookmarks provided a record of accessed and saved websites, respectively. Login data and autofill records contained user information relevant to profile attribution. Collectively, these artefacts document aspects of browser usage and associated user activity.

Within the top sites file, two domains were recorded:

- https://www.office.com
- https://enterprise-insights.dji.com/blog/night-vision-drones

These entries indicate access to a Microsoft service platform and a website containing information related to drone technology during the relevant timeframe.

The autofill database contained multiple entries for the name "Sonya Macoit" and the email address "sonyamacoit@outlook.com." An additional autofill record contained the phrase "mission specs." The repetition of the same name and email address across several fields links the browser profile to this user information.

The login data file recorded a saved credential for https://login.live.com, with the password field encrypted in accordance with browser security protocols. This login entry documents a user interaction with a Microsoft online service.

The bookmarks file contained only default folders, such as the "Favorites bar," and no additional user-saved bookmarks were identified.

Custom scripts were also made and used to aid in certain tasks. Figure I.1.1 “phototos_searcher.cpp” was used to find all relevant .png by filtering the full list of .png files that were taken using the Canon EOS 30 as it has been identified as the camera using in Kenya the output can be seen in I.1.2. Figure I.2.1 shows “hash_cracker_SHA1.sh” an alternative for Hashcat designed to calculate the SHA1 of passwords leaked and compare them to the provided hash in B.2.1 and in #003_TXT of the chain of custody document, this cracked the hash and found Sonya's password “conservation”.

The USB needed to be mounted in windows to permit the usage of BitLocker to decrypt the drive. This means that the drive needed to be mounted in a windows environment, so FTK imager was used to mirror the fact that the disk was separated using FTK imager before it was delivered by Chief Officer Karl Van Der Schyff.

2.4.7 Malware

A scan was done to check if malware was found on the system, the results can show false positives so a comparison against whitelists was made. As can be seen in I.8.3 the only file flagged as malware is MsMpEng.exe. This is windows defender a file whitelisted (figure I.10) so there is no malware found on the system. The malfind command is a part of the volatility v3 command set designed for windows 11.

2.4.8 Autopsy

The analysts used the Autopsy platform to explore and extract data related to images, emails, installed programs, run programs, and the recycling bin. To ensure the integrity of the extracted data, the analysts verified that the MD5 hash values for the images, emails, and installed programs matched those passed into Autopsy as a data source, confirming that the evidence had not been tampered with.

A whitelist of MD5 Hashes was also created and imported into autopsy. By doing this the number of files and items to manually investigate was significantly decreased. For example, the number of run

programs was originally 4236, but when the whitelist was applied it decreased to 2118. The same thing happened for web history, which went from 18742 down to 9371. See figures in I.10 for the process

2.4.8.1 Images, videos and documents

Autopsy was the main tool used to source images, videos and documents. Most of the files that were not found during the investigation were found using Autopsy's built in image and video searcher. This tool allows investigators to search through every single image and video on the drive with a small preview for most, whilst this method takes a considerable amount of time to search through, as there was suspicion of obfuscation (E.2.1 index 18) it was necessary to view all the files to ensure the investigation was through enough to find all the necessary files.

Additionally, a custom script was also used to extract the names (script: I.1.1 output: I.1.2) of files that matched a camera suspected to be in the possession of Sonya that were .jpgs. The list of all jpg that the script takes in was produced using the Exif tool on a mounted read-only version of Sonya's drive. These files were searched by names found in the output (I.1.2) using the keyword search in autopsy and the viewed to see if they were relevant or not relevant.

Due to the Exif tool not being able to consume the sheer volume of .png files and the potential obfuscation it was necessary to manually search through files. AI tools are not yet reliable or secure enough to trust the information to for searches so the labour could not be automated, this left only a manual search through Autopsy's records to be the best method to ensure a diligent search.

2.4.8.2 Emails

The built-in autopsy functionality of finding emails identified 138 total emails within the CrypticWilds.000.dd file, of these 138 emails the analysts used the built-in autopsy tool to view the data artifacts left behind by the emails allowing them to view the contents of these emails. The analysts used this information to break the emails down into 12 separate incidents that related to the charges levelled against Sonya Macoit. Within these incidents four total email addresses were in contact with each other. Table 1 shows the email addresses as well as how many notable emails they were a part of.

Email Address	Number of notable emails
sonyamacoit@outlook.com	83
thescout@skiff.com	68
marteneleroux@proton.me	43
Lunavanderschyff@outlook.com	7

Table 1: Email addresses and number of notable emails they were involved in

Multiple of the emails sent and received contained attachments in the forms of documents, images and encrypted files. These were all marked as important by the analysts and can be viewed within Appendix F – Emails along with the rest of the emails identified as important by the analysts.

These emails had also been subject to anti-forensic techniques including obfuscation by changing the language that was being used to communicate to Afrikaans. Encryption was also used to hide information about locations, files, images and other methods of communication.

2.4.8.3 Installed and run programs

Installed Programs

During the forensic examination of active system artifacts, analysts identified several installed programs on the system. Of the 52 installed programs there were 5 to note of.

The identified programs included utilities associated with metadata editing, network monitoring, and electronic communications.

Execution timestamps were reviewed to document their activity within the relevant investigative timeframe.

The relevant programs observed were:

- Wireshark 4.2.2 x64 v.4.2.2 - Network traffic monitoring tool
- Npcap v.1.78 -Network traffic monitoring tool
- USBPcap 1.5.4.0 v.1.5.4.0 - Open source USB Packet capture for Windows
- AnalogExif v.0.0.4.1 - Tool used for editing the metadata of film and digital images
- Mozilla Thunderbird (x64 en-GB) v.115.8.0 - Email client

A full summary of these programs, including descriptions and observed execution details, is available in Appendix J1.

Run Programs

During the forensic examination of active system artifacts, analysts identified several programs that were executed on the system.

The identified programs included utilities associated with encryption, data concealment, network monitoring, and Windows administrative operations.

Again, execution timestamps were reviewed to document their activity within the relevant investigative timeframe.

The programs observed included:

- CERTUTIL.EXE – Windows certificate management and file transfer tool.
- NPFINSTALL.EXE (Npcap Installer) – Packet capture driver installer supporting network monitoring.
- STEGHIDE.EXE – Application for embedding data within image and audio files.
- VERACRYPT SETUP 1.26.7.EXE – Disk encryption tool installer.
- GPG4WIN-4.3.0.EXE – Encryption software suite for secure communications.
- KLEOPATRA.EXE – Key management graphical user interface for encryption.
- GPG.EXE – Core executable for GNU Privacy Guard (GPG), handling encryption and signing of files and messages.
- GPG-AGENT.EXE – Background agent for managing cryptographic private keys.
- GPG-CONNECT-AGENT.EXE – Utility for establishing secure connections to cryptographic agents.
- GPGCONF.EXE – Configuration utility for managing GPG settings.
- GPGSM.EXE – Component for handling S/MIME encrypted communications and digital certificates.

A full summary of these programs, including descriptions and observed execution details, is available in Appendix J, Section 2.1.

2.4.8.4 Recycling bin

In the recycling bin two main categories of items were found, those relating to steghide and those that were images. The steghide files are noted in incident #13, this shows steghide was downloaded 2024/01/24 13:36:10 and then later that same day, the zip was deleted from the device at 13:40:46 see Figures E.3.1 and G.1.1 - G.1.4.

The recycling bin also contained numerous images that related to the suspects charges had been deleted. These included images of animals such as lions, buffalo and hippos. Relevant deleted images can be found in Appendix A Figure A.2.

2.5 Production List and Associated Description

See appendix H for the full list.

3. Conclusion

A total of 144 images of note were found on the image of the suspects Personal Computer, as well as 6 Documents and 1 video file of pertinence to the case. Upon further investigation of the documents, it was found that at least one was downloaded from the internet. Further investigation into the images recovered that multiple of them were taken with the same camera model which had been noted withing web and email artifacts and had the suspect or a person they were communicating with throughout the period of activity on the suspects personal computer listed as authors.

Further investigation into the suspects internet history revealed 12 incidents in which the suspect had searched for or accessed sites pertinent to the case, these included guns used for hunting, bullet safaris and numerous searches relating to animals that are commonly poached. Analysis of the graphical timeline provided in Appendix C when cross referenced with emails showed that the actions taken were not accidental and instead had deliberate intentions behind them. This includes deliberate searches for material and downloading files related to the charges.

There was further evidence showing that the suspect had actively partaken in research and/or executed anti-forensic measures. These measures included obfuscation of emails by changing the language used to Afrikaans. Other examples of anti-forensic measures taken or researched were:

- Encryption
- Use of an external drive to hide important files
- File deletion
- Use of steganography
- Mismatched file extensions
- Metadata altering

Multiple files were encrypted using the .gpg file format and the Kleopatra program. These files were located and in the hdd drive, within email artifacts and saved within the Personal Computer. The suspect had also attempted to delete their encryption recovery key.

Through a malware scan performed by the analysts on the image no malicious software was found to be present on the PC.

One of the emails recovered by the analysts contained an image attached which was pertinent to the charges raised against the suspect. Multiple other emails contained encrypted files and mentions of using a USB drive in case of their communications being discovered.

Multiple of the recovered documents were also of note. Of the non-encrypted documents there was a SHA1 password hash that was revealed to be the password used to encode the gpg documents. Alongside that there was also a pdf that shows the price paid per animal trophy (figure B.5.1).

Other than those there was a text document on the USB claiming that the images of amur leopards were taken “by river from leopard lookout” the talek river see (Figures G.4.4, A.1.1, A.1.2 and B.1.1). Multiple documents were encrypted on 2024/02/20 09:21:25. These documents once decrypted include a pdf of the Windows 11 security handbook, a copy of the_list.txt that records animals and dates that correspond to when images were taken, an image of where endangered animals live that shows how at risk they are and a fake BitLocker encryption key with a 32 bit recovery key (figure G.3.6).

In the hex files for the emails, it was uncovered that an account karlvanderschyff@outlook.com had gained access to Sonya’s e-mails on 2024/01/03, Chief Officer Karl Van Der Schaff confesses to this e-mail belonging to him. (F.13.1- F.13.13)

4. Equipment Required for Court Proceedings

- **Computing & Software Tools**
  - A high-performance laptop or desktop with necessary forensic applications installed.
  - Secure external storage (such as encrypted USB drives) to transport evidence.
  - Backup system in case of technical failure.
- **Digital Forensic Software (for Evidence Demonstration)**
  - Tools like Autopsy, FTK Imager, Volatility, and EnCase to showcase forensic findings.
  - BrowsingHistoryView for web browsing evidence.
  - DB Browser for SQLite for database analysis.
  - Regripper for registry examination.
- **Display & Presentation Setup**
  - Large screen/projector for clear, courtroom visibility.
  - Laser pointer or highlighting tools to focus on key artifacts.
  - Printed forensic evidence reports for legal teams and judges to reference.
- **Security & Chain of Custody Measures**
  - Write blockers to demonstrate proper forensic methodology.
  - Documentation tools (such as Word).

Appendices

All items are found on the hdd drive unless otherwise stated.

Appendix A – Images
Appendix B – Documents
Appendix C – Timelines
Appendix D – Chain of custody documentation
Appendix E – Browser History
Appendix F – E-mails
Appendix G – Encryption
Appendix H – List of evidentiary files with MD5 hashes
Appendix I – Miscellaneous
Appendix J – Installed / Run Programs
Appendix K – Shell Bags
Appendix L - Glossary

Appendix A - Images

A.1 Images stored on USB drive - JB

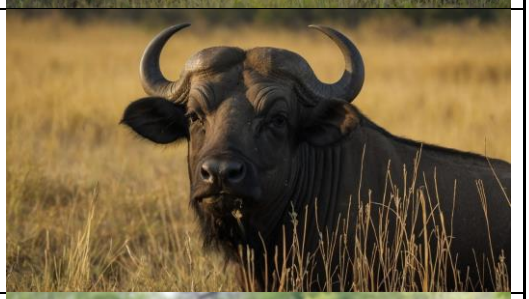
Figure	File Name	MD5	Image
A.1.1	Default_leopard_in_africa_3.jpg	011bc454f1282daab265cfc644a12f72	
A.1.2	Default_leopard_in_snow_3.jpg	835760d0130e3dcd835d0945266b77e7	

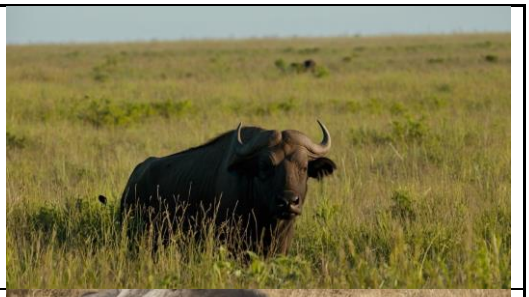
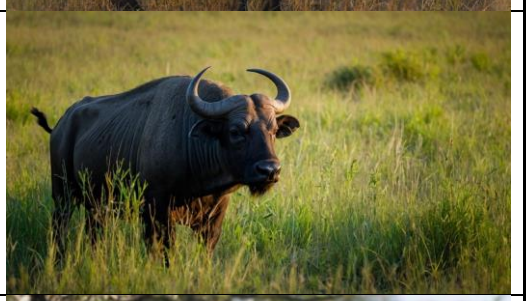
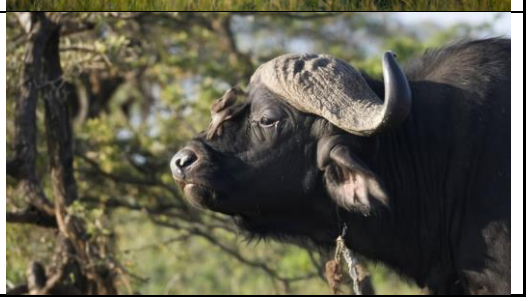
A.2 Deleted/Recycled Images – AH, EL, JB

Figure	File Name	MD5 hash	Date/Time	Image
A.2.1	sonya.jpg	df57f81e1ae46fe77805cf4ea761ec7f	2024/01/03 08:18:26 GMT	
A.2.2	hippo.jpg.bak	5871e00fba511d4c9e5781e3cca2b308	2024/02/19 09:11:15 GMT	

A.2.3	Default_group_of_hippos_in_a_river_2.jpg.bak	1b8a46b697020ee54ade65c42cd07921	2024/02/19 09:11:15 GMT	
A.2.4	Default_hippos_in_river_0.jpg.bak	7f1ba93f9911233ed79a9a1e98e14506	2024/02/19 09:11:15 GMT	
A.2.5	Default_hippos_in_river_1.jpg.bak	74536d2bb3fb44b073dc6497e97cc848	2024/02/19 09:11:15 GMT	
A.2.6	in_a_river_staring_at_the_photographer_2.jpg.bak	e876580e755018d288332le2d602ellf	2024/02/19 09:11:15 GMT	
A.2.7	charging_the_photographer_2.jpg.bak	13345332d599c4605c6dd2213c9ecfd91	2024/02/19 09:11:15 GMT	

A.2.8	Default_hippos_in_a_river_2.jpg.bak	d0ef6d607f390712a1bc07b2921e994a	2024/02/19 09:11:15 GMT	
A.2.9	Default_hippo_in_a_river_2.jpg.bak	84287c7f6d4b11bdac3e785687a7f0b5	2024/02/19 09:11:15 GMT	
A.2.10	mouths_open_0.jpg.bak	d2f312302836cb53db4a8f66db1f5dd	2024/02/19 09:11:15 GMT	
A.2.11	river_hippo.jpg.bak	10b7a64e831e512663b3769febb21c8c2	2024/02/19 09:11:15 GMT	
A.2.12	hippos_in_rivers.jpg.bak	a140a23aa7c50ff8409088634927c7c4	2024/02/19 09:11:15 GMT	
A.2.13	water_buffalo.jpg.bak	ce16e54d41fe4026b7cb8f6b0ad21396	2024/02/19 09:12:11 GMT	

A.2.14	next_to_water_view_from_a_distance_correc_0.jpg.bak	eabfbae9b447ff337226f6a3350ff32a	2024/02/19 09:12:11 GMT	
A.2.15	drinking.jpg.bak	ece19ec64af2073cc44bf1fe18203968	2024/02/19 09:12:11 GMT	
A.2.16	buffalo_1.jpg.bak	99c4914720fb32435ebf1cca5a3183a5	2024/02/19 09:12:11 GMT	
A.2.17	looking_around.jpg.bak	6e1ebf277f6898e92197258a7c473ba	2024/02/19 09:12:11 GMT	
A.2.18	87.jpg.bak	6dc6b51d7a7592887e443867f46fc252	2024/02/19 09:12:11 GMT	
A.2.20	3.jpg.bak	30130a14347a238b941ee3ead85d1dec	2024/02/19 09:12:11 GMT	

A.2.21	9777.jpg.bak	467e6aafcbc164c67dfe6252d7dc2d3	2024/02/19 09:12:11 GMT	
A.2.22	987.jpg.bak	e6eb7262afe3ad5ced31ced63c0a7c349	2024/02/19 09:12:11 GMT	
A.2.23	from_a_distance_1.jpg.bak	6a69bbffd2bfb3ac3d3168e0bdc126e7	2024/02/19 09:12:11 GMT	
A.2.24	in_field.jpg.bak	92fb822098b66ad66a8718c885f81abb	2024/02/19 09:12:11 GMT	
A.2.25	6543.jpg.bak	61d73d931f49f259db46b06fe0e04dc2	2024/02/19 09:12:11 GMT	
A.2.26	buaffalo_and_bird.jpg.bak	1528f1835a80aefeac9254b13cce318a	2024/02/19 09:12:11 GMT	

A.2.27	long_grass.jpg.bak	60defcbbd50ff9611087af9b6dbd98e8	2024/02/19 09:12:11 GMT	

A.3 Physical Imaging images of note – EL

Figure	File Name	MD5	Artist	Date/time	Camera Model	Image
A.3.1	f_0000ed	0ecc6ebb3059024921033304b2e1cf2f1	James Artaius	2020/07/03 16:01:09	Canon EOS R5	
A.3.2	lion_at_watering_hole.jpg	6ef3823e1791833b3999cc26b3fb9c1e	thescout	2024/02/10 14:00:00	Canon EOS 30	
A.3.3	F0733352.jpg	649f9d7791702c23b07356038f75efd	thescout	2024/02/10 14:58:00	Canon EOS 30	
A.3.4	afternoon_hunt_2.jpg	9a0bcda8538294635542e7af87517619	sonya	2024/02/13 13:00:00	Canon EOS R5	

A.3.5	antelope_223.jpg	c63e6b0434eca09c8c40d16393ac05cf	sonya	2024/02/13 14:00:00	Yashica Mat-124G	
A.3.6	antelope_horns.jpg	519c98b171efec7a274a8a9c21eeb107	thescout	2024/02/14 00:00:00	Canon EOS R5	

Figure A.4.1 - Flights booking Screenshot 2024/01/15 114028.png 15/01/2024 11:40:28 GMT, MD5 1a53d9d9f1b1ac36e90a89f5a0f41de3, Investigator JB

A.5 Backed up images JB

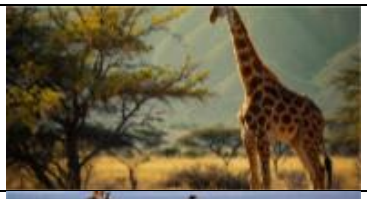
Index	Name	MD5	Date	Camera	Image
A.5.1	elephant_in_water.jpg	555182b1d00d5940c9769225fa56e63e	2024/02/06 10:18:07 GMT	N/A	
A.5.2	elephant_recon_close_call.png	0fed5b1307b462368e846c0155852d92	2024/02/06 10:18:07 GMT	N/A	

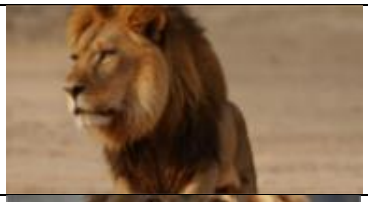
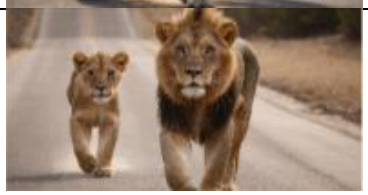
A.5.3	elephant_crossing_road.jpg	09a71ecad91b3f7c2c632e99e1e67246	2024/02/06 10:18:07 GMT	N/A	
A.5.4	viewing_herd_of_elephants_0.jpg	1dca861cc081c16d682c2253f13412d5	2024/02/06 10:18:07 GMT	N/A	
A.5.5	elephant_family.jpg	9cb0bcee417ee0b4e4decb8e8b075c53	2024/02/06 10:18:07 GMT	N/A	
A.5.6	aerial_1.jpg	f6fef39f0568ebac240ec2189bfbfdf7	2024/02/06 10:18:07 GMT	N/A	
A.5.7	close-up.jpg	b2c3146c2710750da3619bb27266da60	2024/02/06 10:18:07 GMT	N/A	
A.5.8	elephant_in_river.jpg	a64f06fbd43fcabd323e4c3cfdc21a6c	2024/02/06 10:18:07 GMT	N/A	
A.5.9	elephant_trunk.jpg	b9250ce2889c19fa1c437f3d36f1bbaf	2024/02/06 10:18:07 GMT	N/A	
A.5.10	hunting_scene_viewed_from_1.jpg	b7306c6b4d28c73d355f4b8bc6288a79	2024/02/06 10:18:07 GMT	N/A	

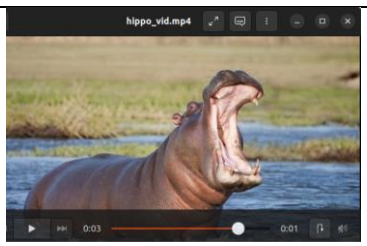
A.5.11	hunting_scene_viewed_from_a_helicopter_wi_2.jpg	2c8eb3b6698512b297d99c01a4125fb5	2024/02/06 10:18:07 GMT	N/A	
A.5.12	elephant_chasing_lion.jpg	64a9f9d7791702c23b07356038f75efd	2024/02/14 07:18:00 GMT	Canon Eos 30	
A.5.13	lions_in_road_1.jpg	15f06c8ceef72620a812c527aeffb7aa	2024/02/14 07:18:00 GMT	Canon Eos R5	
A.5.14	lions_on_boulder.jpg	86fd53c52b794c10dabdcd26ea1a9f2f	2024/02/14 07:18:00 GMT	N/A	
A.5.15	puzzled_look.jpg	49ace06ebc37dc56b3af74845f9df18e	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.16	anteplope_horns.jpg	519c98b171efc7a274a8a9c21eeb107	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.17	grassland_morning.jpg	656883be8307cc53299f43959df02c5a	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.18	solo_male.jpg	65afd9eac478cf059e49670064bbe1a0	2024/02/16 07:04:53 GMT	Canon Eos R5	

A.5.19	smiling_zebra.jpg	19cb35a60d3a16fbe515c8662e6ed5fa	2024/02/16 07:04:53 GMT	Yashica Mat-124g	
A.5.20	tired.jpg	554561262d6f548d6a2b8f7df00d9fbd	2024/02/16 07:04:53 GMT	Yashica Mat-124g	
A.5.21	trotting_away.jpg	f54d7d372d0ab0a77c882e4709b4822c	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.22	two_together.jpg	8852973ec345fc4221a0e29e016e0326	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.23	zebra_on_road.jpg	caa8d1b1b366c92f1018fd8d56e1776e	2024/02/16 07:04:53 GMT	Canon Eos 30	
A.5.24	afternoon hunt.jpg	555921f976beb99004c27a8abdaacc9	2024/02/16 07:04:53 GMT	Canon Eos 30	
A.5.25	zebra_herd.jpg	ca0f55bdb74d3c8d14ca12366c9de8e3	2024/02/16 07:04:53 GMT	Yashica Mat-124g	
A.5.26	antalope_223.lpg	c63e6b0434eca09c8c40d16393ac0fcf	2024/02/16 07:04:53 GMT	Yashica Mat-124g	

A.5.27	afternoon_hunt_2.jpg	9a0bcda853829463 5542e7af 87517619	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.28	hunting.jpg	fc8692cc c6ca2dd2 8827cc21 53fb00f4f	2024/02/16 07:04:53 GMT	Yashica Mat-124g	
A.5.29	internet_pic.jpg	044d476c d3c9338c 014eab97 f0c9676b	2024/02/16 07:04:53 GMT	N/A	
A.5.30	lying_down.jpg	1fe6d96a 49d68a29 1b8355a0 33bad79a	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.31	midmorning.jpg	a9abc066 f4fe0b5d b8ab07cf a2e64933	2024/02/16 07:04:53 GMT	Canon Eos R5	
A.5.32	close_to_tree.jpg	36970ec4 633ea3d3 1409d13d 9f7c3d6c	2024/02/16 07:09:59 GMT	Canon Eos 30	
A.5.33	more_water.jpg	24d55462 cd01f8b8 63706ed1 4f6fcd0e	2024/02/16 07:09:59 GMT	Canon Eos R5	
A.5.34	distant_looks.jpg	ee430095 8c165595 fd68225b f91c8bef	2024/02/16 07:09:59 GMT	Canon Eos R5	

A.5.35	open_field.jpg	35a17ff1f8d81e764bba9ff07a3a8b68	2024/02/16 07:09:59 GMT	Canon Eos R5	
A.5.36	hungry_giraffe.jpg	b40b000c7af2013037b7725601119dab	2024/02/16 07:09:59 GMT	Yashica Mat-124g	
A.5.37	toy.webp	680854168f1030fab935c9a2a46d8584	2024/02/16 07:09:59 GMT	N/A	
A.5.38	interested.jpg	4ca3f02353b48d9f39367d47171cbb9d	2024/02/16 07:09:59 GMT	Canon Eos R5	
A.5.39	water_giraffe.jpg	2c3237ad2311da5001da99d10712e522	2024/02/16 07:09:59 GMT	Canon Eos R5	
A.5.40	distant_in_trees.jpg	fae5bd39725b8c2d104463d38545c2fb	2024/02/16 07:09:59 GMT	Canon Eos R5	
A.5.41	herd_photo.jpg	8a3833ac61f0a74da85f635542702080	2024/02/16 07:09:59 GMT	Canon Eos 30	
A.5.42	herd_photo_2.jpg	d4aaf0fe7051b6749586770e4f65d2ae	2024/02/16 07:09:59 GMT	Canon Eos R5	

A.5.43	large_giraffe.jpg	280173a2bb761b81bdf063b27ddbfc8a	2024/02/16 07:09:59 GMT	Canon Eos R5	
A.5.44	next_to_thorntree.jpg	9191e075b2a22b086c63ce4530e34d6d	2024/02/16 07:09:59 GMT	Yashica Mat-124g	
A.5.45	through_trees.jpg	2e7bbd714d5d0e401f84e01afac8b97b	2024/02/16 07:09:59 GMT	Yashica Mat-124g	
A.5.46	lion_at_watering_hole.jpg	6ef3823e1791833b3999cc26b3fb9c1e	2024/02/16 07:12:12 GMT	Canon Eos 30	
A.5.47	lion_charging.jpg	15fd9c90ddbff0460903a688d5aa6532	2024/02/16 07:12:12 GMT	Canon Eos R5	
A.5.48	tree_lions_1.jpg	b1d5774f273763449e6a64b5168f3f2e	2024/02/16 07:12:12 GMT	Canon Eos R5	
A.5.49	tree_lions_2.jpg	de113f884880b66e897d3dca944c077f	2024/02/16 07:12:12 GMT	Canon Eos R5	
A.5.50	lions_in_road_1.jpg	6ea94f66a42040e43fb5c6eb1f534daf	2024/02/16 07:12:12 GMT	Canon Eos R5	
A.5.51	lions_in_road_2.jpg	d94e971d09ba6c677429243d0718285e	2024/02/16 07:12:12 GMT	Canon Eos R5	

A.5.52	lions_on_boulder.jpg	80cdd4a51f977ff23c31320b3cb4389a	2024/02/16 07:12:12 GMT	Canon Eos R5	
A.5.53	two_lions_charging.jpg	3c1f956208be51d80adee742423a92f4	2024/02/16 07:12:12 GMT	Canon Eos R5	
A.5.54	hippo_vid.mp4	5102b7ceb169b01a6c2ab984c34bf7fe	2024/02/19 09:11:33 GMT	N/A	
A.5.55	hippos_in_rivers.jpg	e0359f370b8aaea0af75a3832c6452f1	2024/02/19 09:11:33 GMT	Canon Eos 30	
A.5.56	Default_group_of_hippos_in_a_river_2.jpg	277bafd400e0f11f1eb2080c876af5a6	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.57	mouths_open_0.jpg	6f15b150f30ca49274d0dec22420eeb9	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.58	Default_hippos_in_a_river_2.jpg	b86b3fbef80119081d5323878805a17f	2024/02/19 09:11:33 GMT	Canon Eos 30	
A.5.59	staring_at_the_photographer_3.jpg	0c5850f0d5b23fb59d8cda3ea08e8f8b	2024/02/19 09:11:33 GMT	N/A	

A.5.60	Default_hippos_in_river_1.jpg	564b8d9809b134f7cd77bafc413e5031	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.61	with_mouth_open_2.jpg	97eb1b490ee3e80d5bf6e49c2e9d1256	2024/02/19 09:11:33 GMT	N/A	
A.5.62	charging_the_photographer_2.jpg	9113be25f355e07c7312769f53f84900	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.63	Default_hippo_in_a_river_2.jpg	9c6f6a701733d25840cd266a27746be6	2024/02/19 09:11:33 GMT	Yashica Mat-124g	
A.5.64	Default_hippos_in_river_0.jpg	79b8dba8b4c2f8fde074b73ce7eb1671	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.65	hippo.jpg	87f03d334c7c638aea2c282cdfecac79	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.66	in_a_river_staring_at_the_photographer_2.jpg	34009bba49220a5a7b244aacee852157	2024/02/19 09:11:33 GMT	Canon Eos 30	
A.5.67	river_hippo.jpg	6349a9e0fe3b49036c433d046c4f1972	2024/02/19 09:11:33 GMT	Canon Eos R5	

A.5.68	buaffalo_and_bird.jpg	7fc43547bca52fd8cbc109a460b9c833	2024/02/19 09:11:33 GMT	Canon Eos 30	
A.5.69	short_grass.jpg	beeb3de6f512b3f041ab26d5efe4f04b	2024/02/19 09:11:33 GMT	N/A	
A.5.70	buffalo_1.jpg	278b1f9d78c146ebcc1b581bdd254622	2024/02/19 09:11:33 GMT	Canon Eos 30	
A.5.71	water_buffalo.jpg	82085b4833d0732e62b08086c48e7366	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.72	drinking.jpg	33bd1b1ae26a105ed36b856497261db8	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.73	3.jpg	5a33ad7a7ef8d5435957dd7fd1f3d13e	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.74	in_field.jpg	e150ef1c4176c3fd6ec8a610f4db42b3	2024/02/19 09:11:33 GMT	Canon Eos 30	
A.5.75	9777.jpg	aa44ec9d33c36d3c5159a206433e1ffa	2024/02/19 09:11:33 GMT	Canon Eos R5	

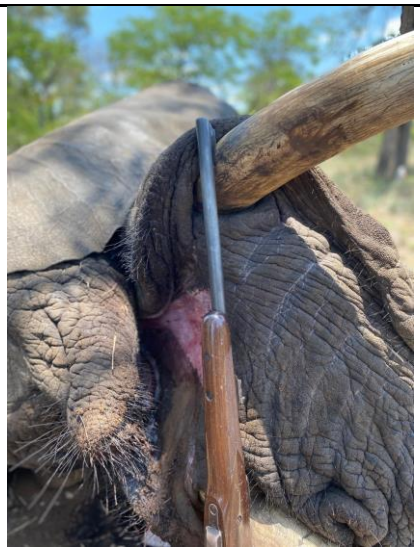
A.5.76	looking_around.jpg	1fdf4062ecb5128dd4a3afaeb733f3ad	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.77	6543.jpg	6c4e98deb295832c32ce2c012e9535bd	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.78	87.jpg	108231d6ded1468564d65c8bb89209a3	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.79	987.jpg	93d21058e7830178e5edebebbf715873	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.80	from_a_distance_1.jpg	c6c3b5acc88bfaa8771b680e5af9ff91	2024/02/19 09:11:33 GMT	Canon Eos R5	
A.5.81	long_grass.jpg	7d4e3fe3d235df008246d25c932e8455	2024/02/19 09:11:33 GMT	Yashica Mat-124g	
A.5.82	next_to_water_view_from_a_distance_correc_0.jpg	c2c247e953b5d70ce7efcbf36e38f026	2024/02/19 09:11:33 GMT	Canon Eos 30	

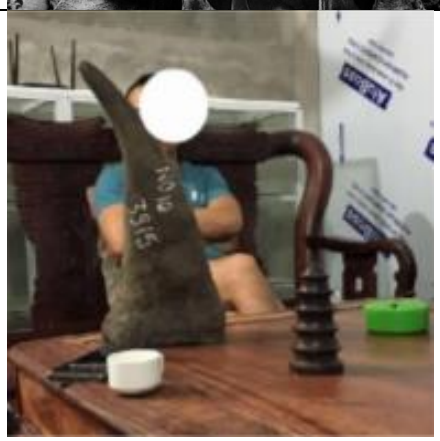
A.6 Cache Images – EL, JB

Figure	File name	MD5 Hash	Date+time	Image

A.6.1	data_2__b1020198.jpg	c5ac0bf09e40512c08c0b163d0578574	2024/02/06 10:23:54 GMT	
A.6.2	data_2__b202019c.jpg	7991152e15ba0d2a10bda9016d81769c	2024/02/06 10:23:54 GMT	
A.6.3	data_2__b2020194.jpg	3849dfabd48a2f506366328a54df593f	2024/02/06 10:23:54 GMT	
A.6.4	data_2__b201a0.jpg	1e1ca6509c16ad5a502e4edb4180ebc0	2024/02/06 10:23:54 GMT	
A.6.5	data_2__b201b0.jpg	b229f3831e81e68ed9130356492617 28	2024/02/06 10:23:54 GMT	
A.6.6	data_2__b201a8.jpg	e272bf4f68332ef3b9f8f9b4ee9be399	2024/02/06 10:23:54 GMT	

A.6.7	data_2__b20202b0.jpg	57be6dba4e2fc14d7b1715159992b83c	2024/02/06 10:24:08 GMT	
A.6.8	data_2__b10202ce.jpg	8ebd837d505d9fae7f8520871 0e51fe0	2024/02/06 10:24:09 GMT	
A.6.9	data_2__b10202c4.jpg	396baf8295a28e87fb7428c2037644 38	2024/02/06 10:24:09 GMT	
A.6.10	data_2__b10202ca.jpg	7f5a6066cab57eaca0097458e95117 5d	2024/02/06 10:24:09 GMT	

A.6.11	f_000074.jpg	957fb61dff22ac2acb5c0de54c9fcfa1	2024/02/06 10:24:10 GMT	
A.6.12	data_2__b30202d4.jpg	8b08891f6c78d7353b8fd3120f3556e9	2024/02/06 10:24:10 GMT	
A.6.13	data_3__c1030224.jpg	6338107bdc292435a127902c7d3c94ab	2024/02/06 10:24:10 GMT	
A.6.14	f_001e9.jpg	ba79461201627f766f4244036a7bbe28	2024/02/06 10:36:24 GMT	

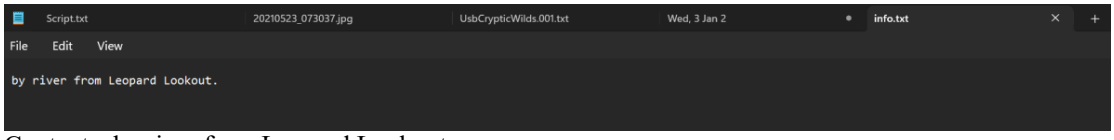
A.6.15	F0001d0.webp	1a53d9d9f1b1ac36e90a89f5a0f41de3	2024/02/06 10:36:24 GMT	
A.6.16	f_0001ef.jpg	cc522b2eb57ceb375c58c45a0b0571b1	2024/02/06 10:39:11 GMT	
A.6.17	f_0001f0.jpg	cf68370a9490c5b1ad64e704db1a47c6	2024/02/06 10:39:31 GMT	
A.6.18	f_0001f3.webp	f6885c5e28fe5350461e4be9781a49b4	2024/02/06 10:39:31 GMT	
A.6.19	f_0001f5.webp	d84246d1430b83bdbf270cd0a4474655	2024/02/06 10:39:53 GM	
A.6.20	f_000203.jpg	ca792ed358b2b0af88a04b93c0aa7636	2024/02/06 10:41:12 GMT	

A.6.21	f_000207.webp	2f8c98cf98e035eb1bfe02ce5d38daf9	2024/02/06 10:41:35 GMT	
A.6.22	data_2__b1020ca8.jpg	318eedc29962f5c88d3a9be6ac80aee9	2024/02/21 09:40:18 GMT	
A.6.23	data_2__b3020d48.jpg	2fcf8d7ce79b54a19c74564f1cb601b5	2024/02/21 09:41:03 GMT	
A.6.24	f_000328.png	349bfee5521fd0d1cbe3ba46ffcad111	2024/02/21 09:41:07 GMT	
A.6.25	data_3__c1031d80.jpg	a3ed10bbc81b5fede2c37d8e3072be23	2024/02/21 09:41:09 GMT	

A.6.26	f_00033a.png	53d763fee396c2a43ba9ae6442e0d0ad	2024/02/21 09:41:18 GMT	
A.6.27	f_00033e.jpg	b6475afb8f4dce3d3be5fa2371622776	2024/02/21 09:41:22 GMT	

Appendix B Documents

Figure B.1.1 - Found on encrypted USB info.txt, MD5 92b0388c082310fddc4d9c57fe098e78, Investigator JB



Contents: by river from Leopard Lookout.

Figure B.2.1 - Found on Sonya's person mykeypass_seized.txt, MD5 5319fbf7b92cba7d9a090717f5fd06c7, Investigator JB

Contents: 338526e5c661ccb2655dc7886d29f700512a906c

Figure B.3.1 Disk audit, licence documentation. Investigator AH.

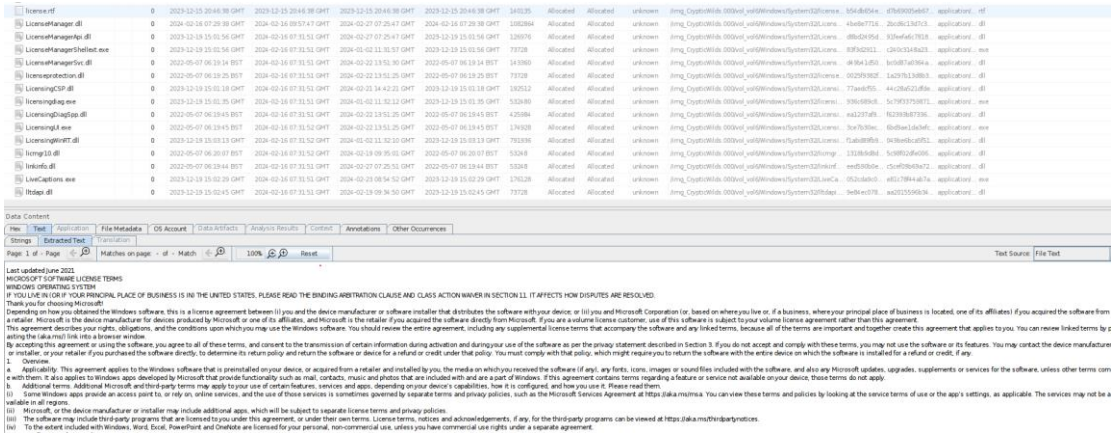


Figure B.4.1 USB Disk audit, UsbCrypticWilds.001.txt, MD5 e81d4963f46737c46a7aca78c633761e, Investigator JB.

UsbCrypticWilds.001.txt

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: 001DISK_01
Unique description: USB32G_Sonya
Examiner: K
Notes: seized at roadblock

------------------------------------------------------------

Information for D:\Evidence Seized\UsbCrypticWilds:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3,849
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 61,849,600
[Physical Drive Information]
 Drive Model: Generic Flash Disk USB Device
 Drive Serial Number: 15E12348
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 30200 MB
 Sector count:    61849600
[Computed Hashes]
 MD5 checksum:    a547247ee2fd3f51182f28c273633fc4
 SHA1 checksum:   dd54cec4e8ebef11163715798b805c73720d9843
```

Content:
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: 001DISK_01
Unique description: USB32G_Sonya
Examiner: K
Notes: seized at roadblock

Information for D:\Evidence Seized\UsbCrypticWilds:

Physical Evidentiary Item (Source) Information:

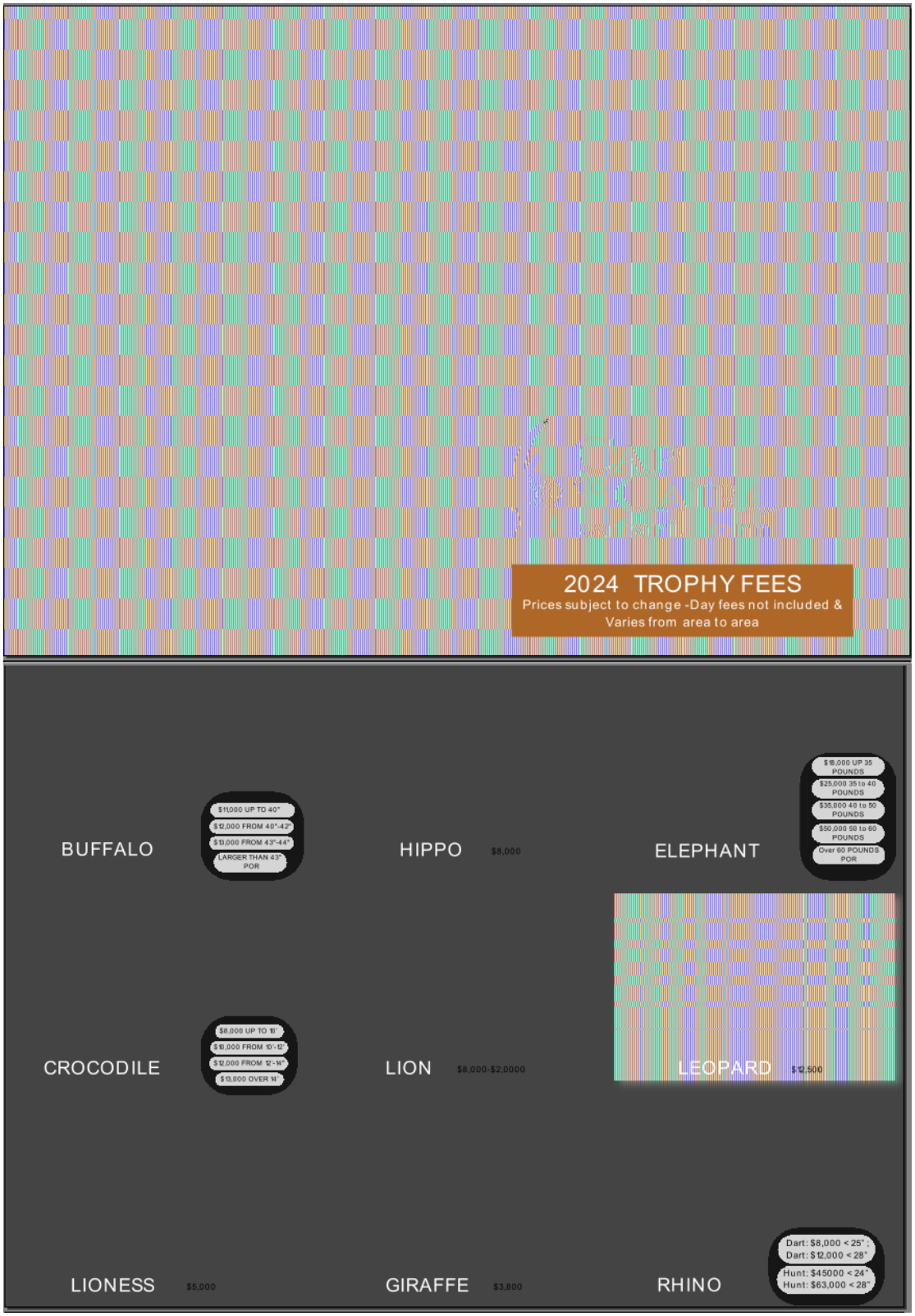
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 3,849
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 61,849,600
[Physical Drive Information]
Drive Model: Generic Flash Disk USB Device
Drive Serial Number: 15E12348
Drive Interface Type: USB
Removable drive: True
Source data size: 30200 MB
Sector count: 61849600
[Computed Hashes]
MD5 checksum: a547247ee2fd3f51182f28c273633fc4
SHA1 checksum: dd54cec4e8ebef11163715798b805c73720d9843

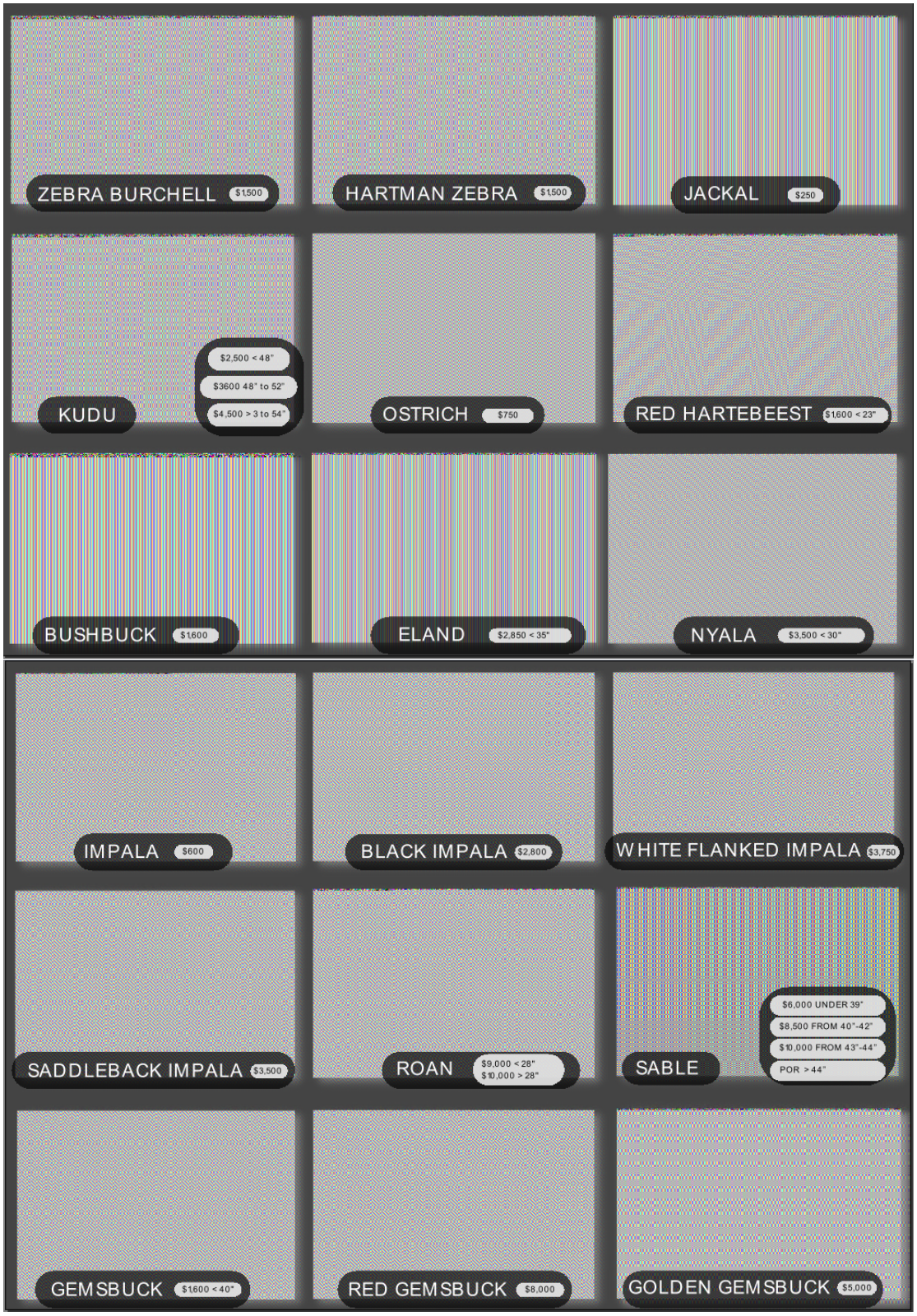
Image Information:
Acquisition started: Wed Feb 21 10:00:30 2024
Acquisition finished: Wed Feb 21 10:15:53 2024
Segment list:
D:\Evidence Seized\UsbCrypticWilds.001
D:\Evidence Seized\UsbCrypticWilds.002
D:\Evidence Seized\UsbCrypticWilds.003
D:\Evidence Seized\UsbCrypticWilds.004
D:\Evidence Seized\UsbCrypticWilds.005
D:\Evidence Seized\UsbCrypticWilds.006
D:\Evidence Seized\UsbCrypticWilds.007
D:\Evidence Seized\UsbCrypticWilds.008
D:\Evidence Seized\UsbCrypticWilds.009
D:\Evidence Seized\UsbCrypticWilds.010
D:\Evidence Seized\UsbCrypticWilds.011
D:\Evidence Seized\UsbCrypticWilds.012
D:\Evidence Seized\UsbCrypticWilds.013
D:\Evidence Seized\UsbCrypticWilds.014
D:\Evidence Seized\UsbCrypticWilds.015
D:\Evidence Seized\UsbCrypticWilds.016
D:\Evidence Seized\UsbCrypticWilds.017
D:\Evidence Seized\UsbCrypticWilds.018
D:\Evidence Seized\UsbCrypticWilds.019
D:\Evidence Seized\UsbCrypticWilds.020
D:\Evidence Seized\UsbCrypticWilds.021

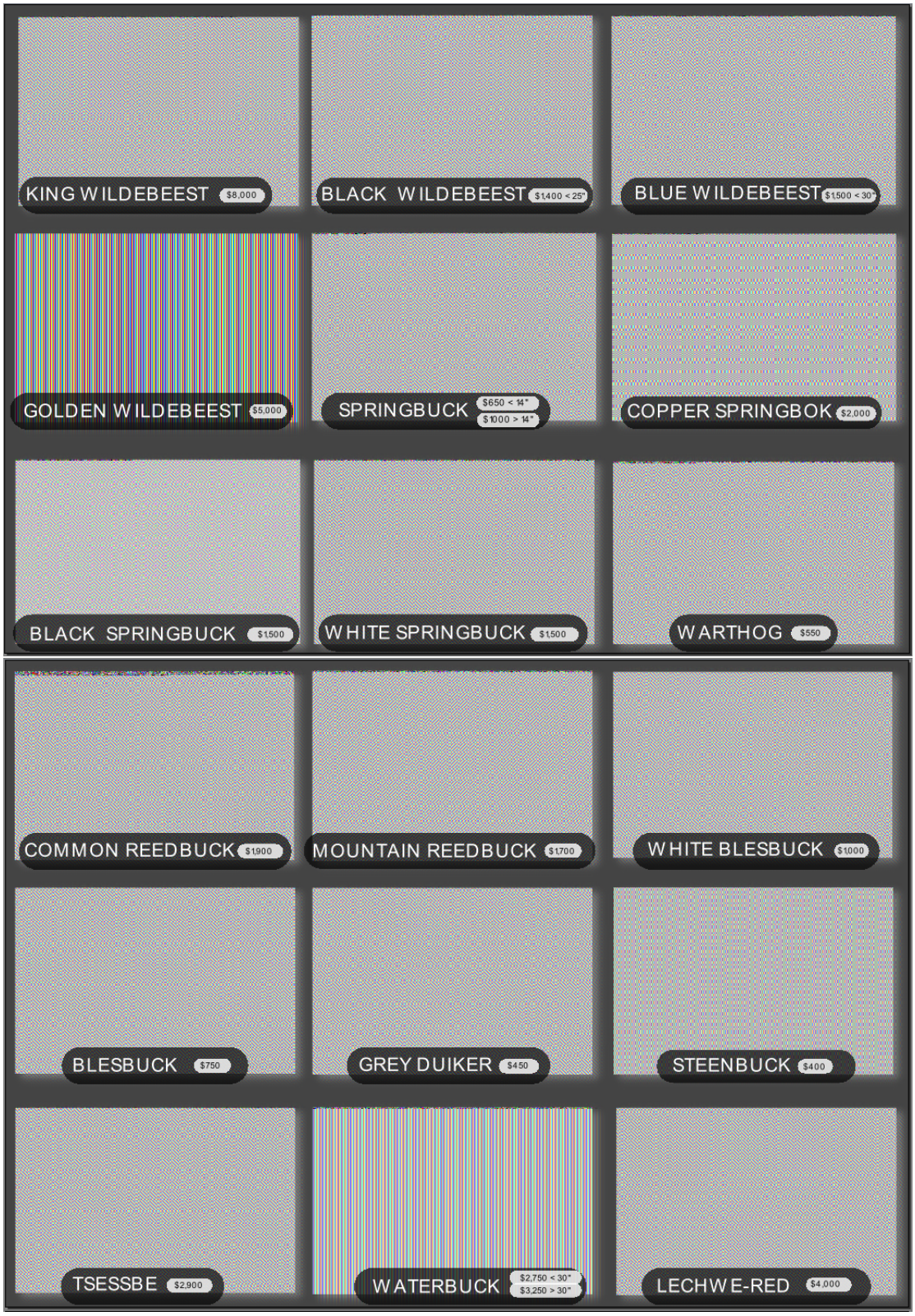
Image Verification Results:
Verification started: Wed Feb 21 10:15:55 2024
Verification finished: Wed Feb 21 10:17:54 2024
MD5 checksum: a547247ee2fd3f51182f28c273633fc4 : verified

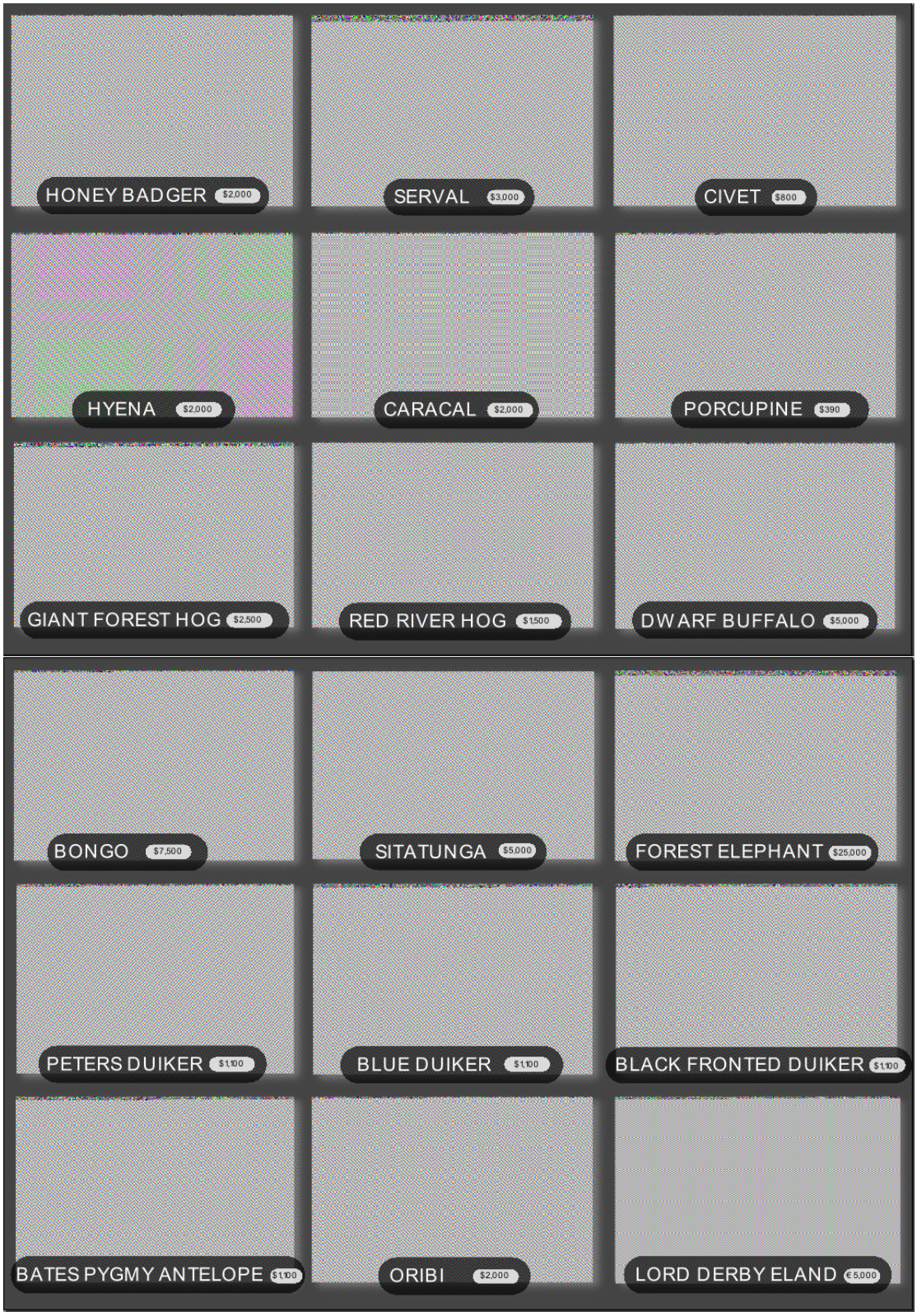
SHA1 checksum: dd54cec4e8ebef11163715798b805c73720d9843 : verified

B.5.1 PDF of hunting wish list


2024 TROPHY FEES
Prices subject to change -Day fees not included &
Varies from area to area
BUFFALO
$11,000 UP TO 40"
$12,000 FROM 40"-42"
$13,000 FROM 43"-44"
LARGER THAN 43" POR
HIPPO $8,000
ELEPHANT
$15,000 UP 35 POUNDS
$25,000 35 to 40 POUNDS
$35,000 40 to 50 POUNDS
$50,000 50 to 60 POUNDS
Over 60 POUNDS POR
CROCODILE
$8,000 UP TO 10"
$10,000 FROM 10"-12"
$12,000 FROM 12"-14"
$13,000 OVER 14"
LION $8,000-$2,0000
LEOPARD $12,500
LIONESS $5,000
GIRAFFE $3,800
RHINO
Dart: $8,000 < 25"
Dart: $12,000 < 28"
Hunt: $45000 < 24"
Hunt: $63,000 < 28"


ZEBRA BURCHELL $1,500
HARTMAN ZEBRA $1,500
JACKAL $250
KUDU
$2,500 < 48"
$3600 48" to 52"
$4,500 > 3 to 54"
OSTRICH $750
RED HARTEBEEST $1,600 < 23"
BUSHBUCK $1,600
ELAND $2,850 < 35"
NYALA $3,500 < 30"
IMPALA $600
BLACK IMPALA $2,800
WHITE FLANKED IMPALA $3,750
SADDLEBACK IMPALA $3,500
ROAN
$9,000 < 28"
$10,000 > 28"
SABLE
$6,000 UNDER 39"
$8,500 FROM 40"-42"
$10,000 FROM 43"-44"
POR > 44"
GEMSBUCK $1,600 < 40"
RED GEMSBUCK $8,000
GOLDEN GEMSBUCK $5,000


KING WILDEBEEST $8,000
BLACK WILDEBEEST $1,400 < 25"
BLUE WILDEBEEST $1,500 < 30"
GOLDEN WILDEBEEST $5,000
SPRINGBUCK $650 < 14" $1000 > 14"
COPPER SPRINGBOK $2,000
BLACK SPRINGBUCK $1,500
WHITE SPRINGBUCK $1,500
WARTHOG $550
COMMON REEDBUCK $1,900
MOUNTAIN REEDBUCK $1,700
WHITE BLESBUCK $1000
BLESBUCK $750
GREY DUIKER $450
STEENBUCK $400
TSESSBE $2,900
WATERBUCK $2,750 < 30" $3,250 > 30"
LECHWE-RED $4,000


HONEY BADGER $2,000
SERVAL $3,000
CIVET $800
HYENA $2,000
CARACAL $2,000
PORCUPINE $390
GIANT FOREST HOG $2,500
RED RIVER HOG $1,500
DWARF BUFFALO $5,000
BONGO $7,500
SITATUNGA $5,000
FOREST ELEPHANT $25,000
PETERS DUIKER $1,100
BLUE DUIKER $1,100
BLACK FRONTED DUIKER $1,100
BATES PYGMY ANTELOPE $1,100
ORIBI $2,000
LORD DERBY ELAND € 5,000

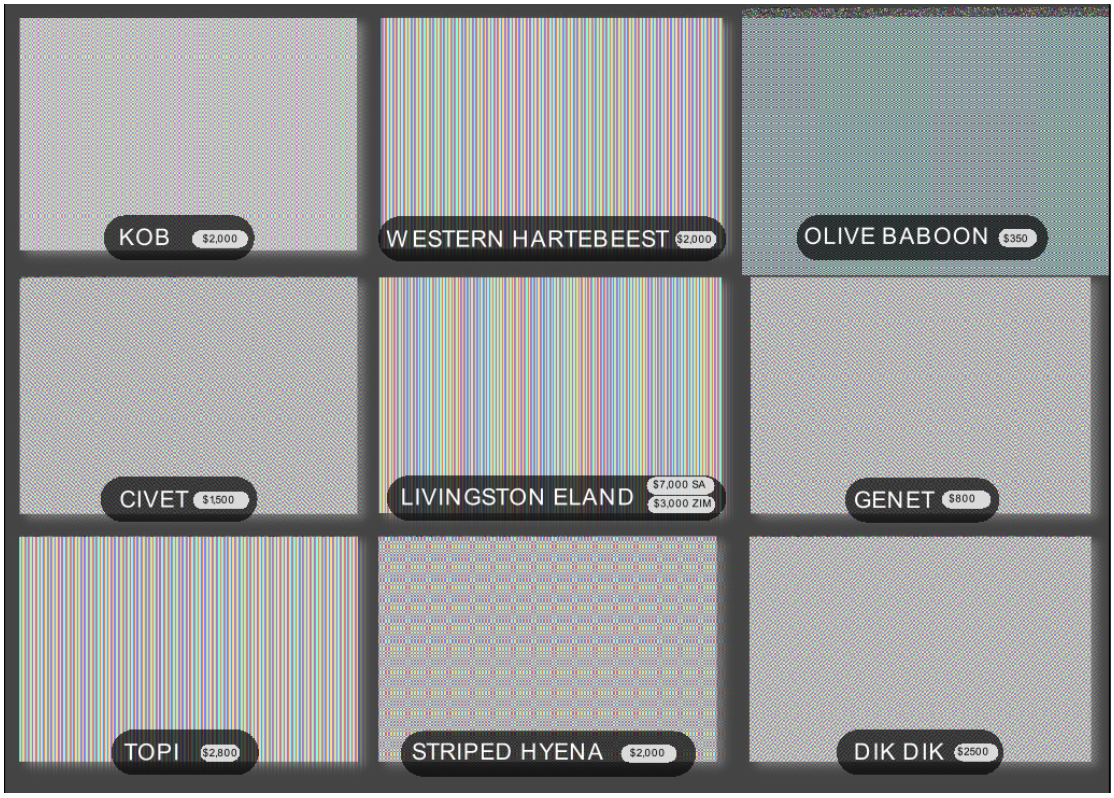
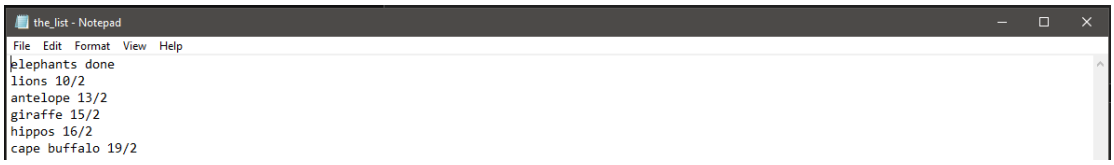


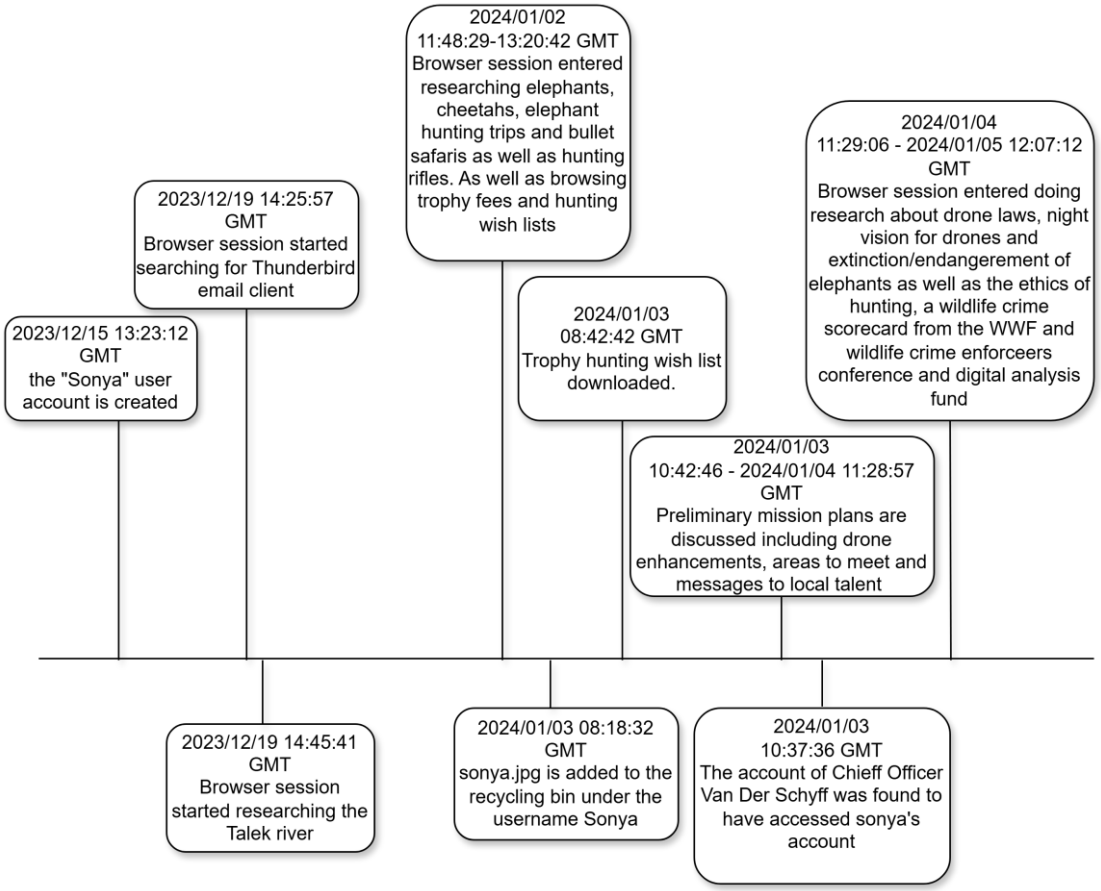
Figure B.6.1

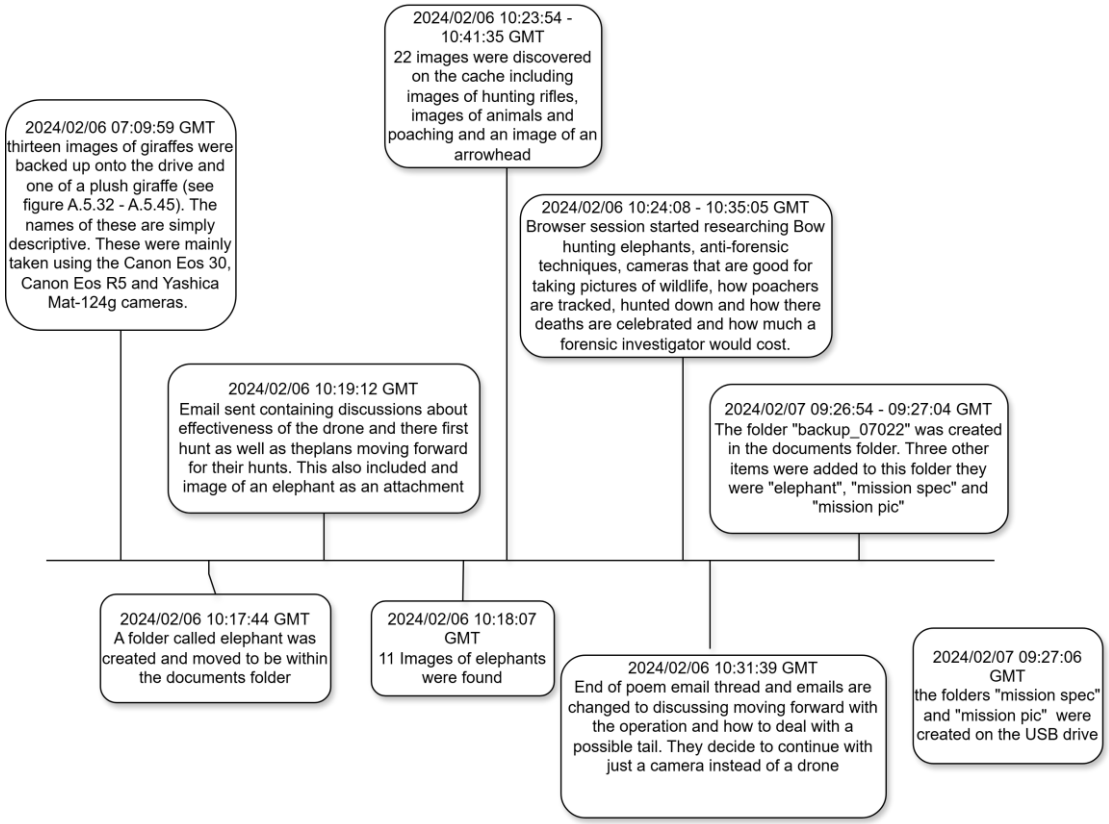


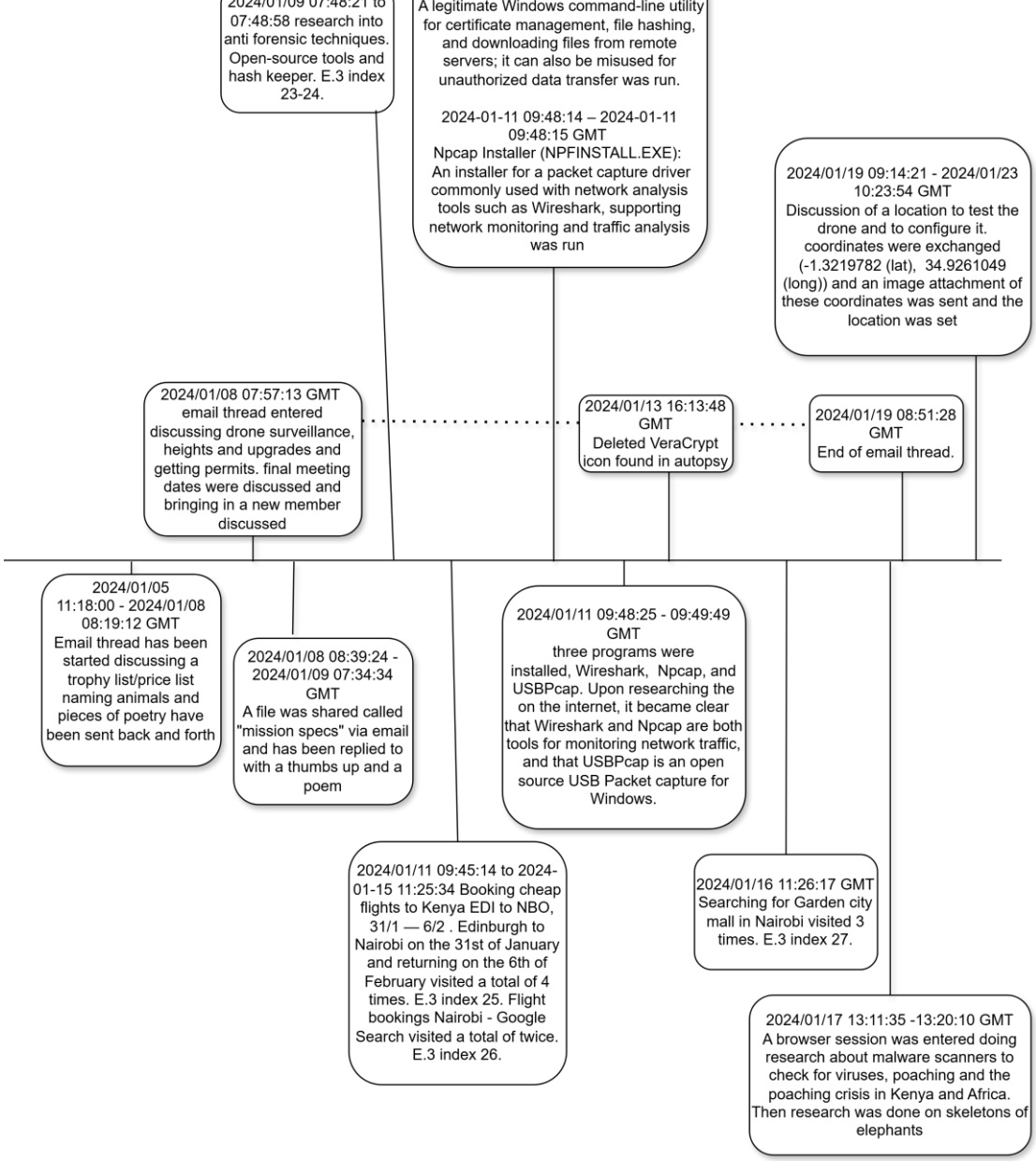
Appendix C – Timeline of events

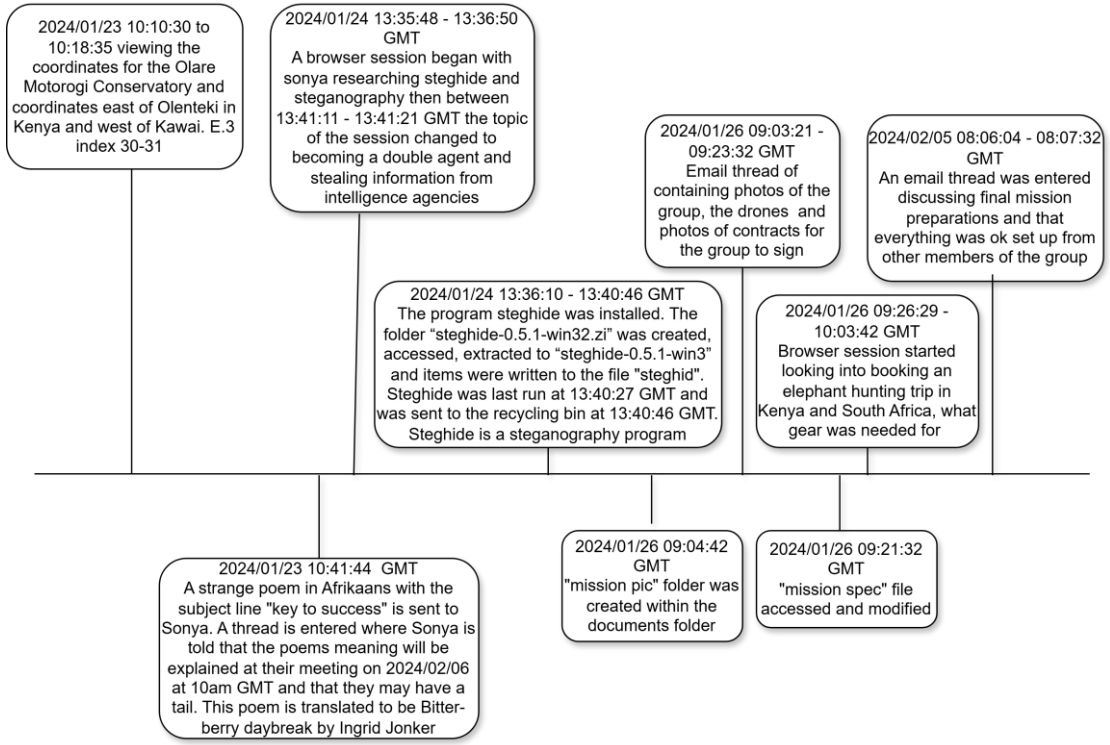
Figure C.1

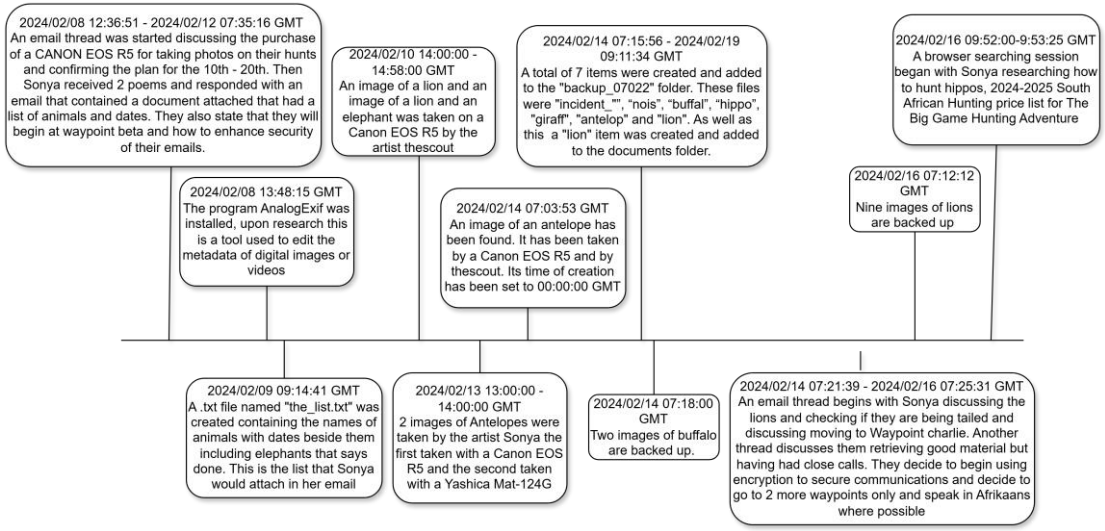
Beginning of graphical timeline

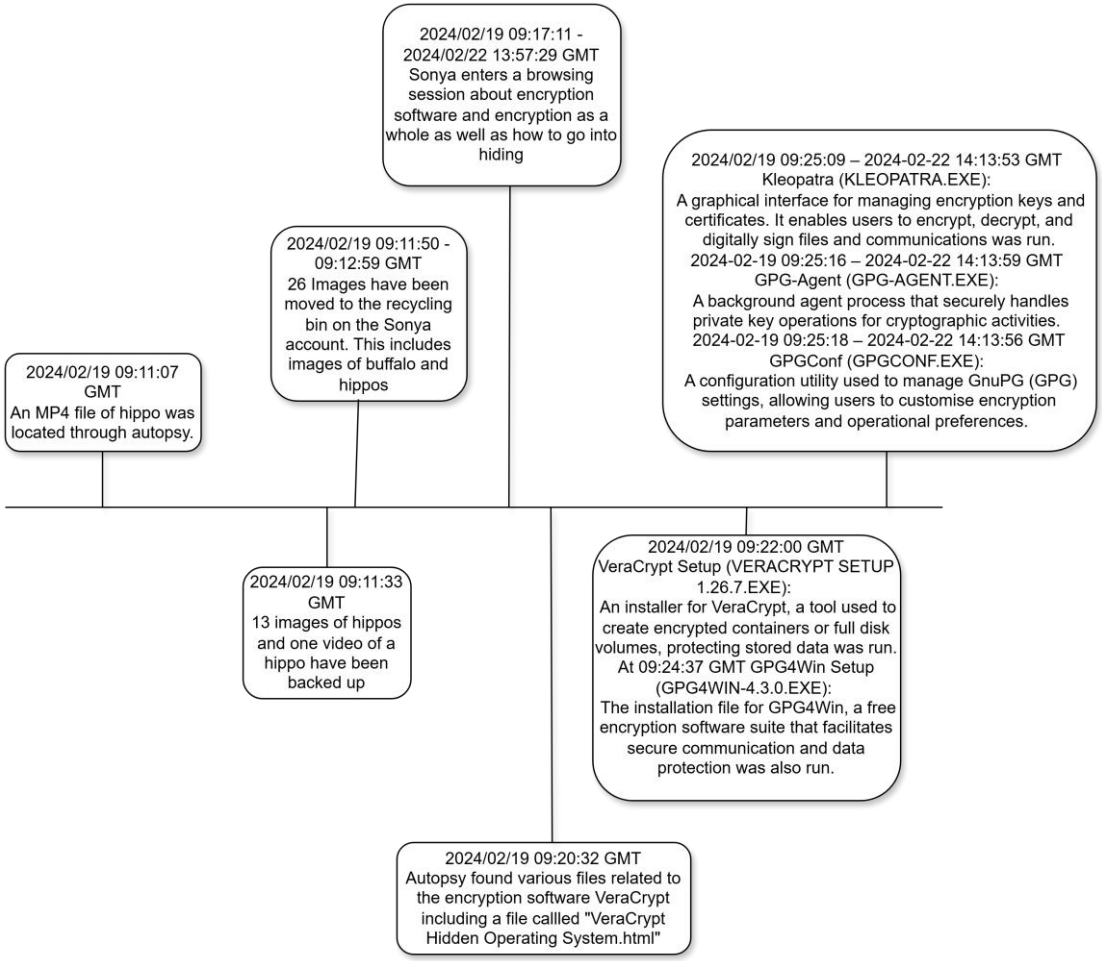

2023/12/15 13:23:12 GMT
the "Sonya" user account is created
2023/12/19 14:25:57 GMT
Browser session started searching for Thunderbird email client
2023/12/19 14:45:41 GMT
Browser session started researching the Talek river
2024/01/02
11:48:29-13:20:42 GMT
Browser session entered researching elephants, cheetahs, elephant hunting trips and bullet safaris as well as hunting rifles. As well as browsing trophy fees and hunting wish lists
2024/01/03 08:18:32 GMT
sonya.jpg is added to the recycling bin under the username Sonya
2024/01/03
08:42:42 GMT
Trophy hunting wish list downloaded.
2024/01/03
10:42:46 - 2024/01/04 11:28:57 GMT
Preliminary mission plans are discussed including drone enhancements, areas to meet and messages to local talent
2024/01/03
10:37:36 GMT
The account of Chieff Officer Van Der Schyff was found to have accessed sonya's account
2024/01/04
11:29:06 - 2024/01/05 12:07:12 GMT
Browser session entered doing research about drone laws, night vision for drones and extinction/endangerement of elephants as well as the ethics of hunting, a wildlife crime scorecard from the WWF and wildlife crime enforceers conference and digital analysis fund

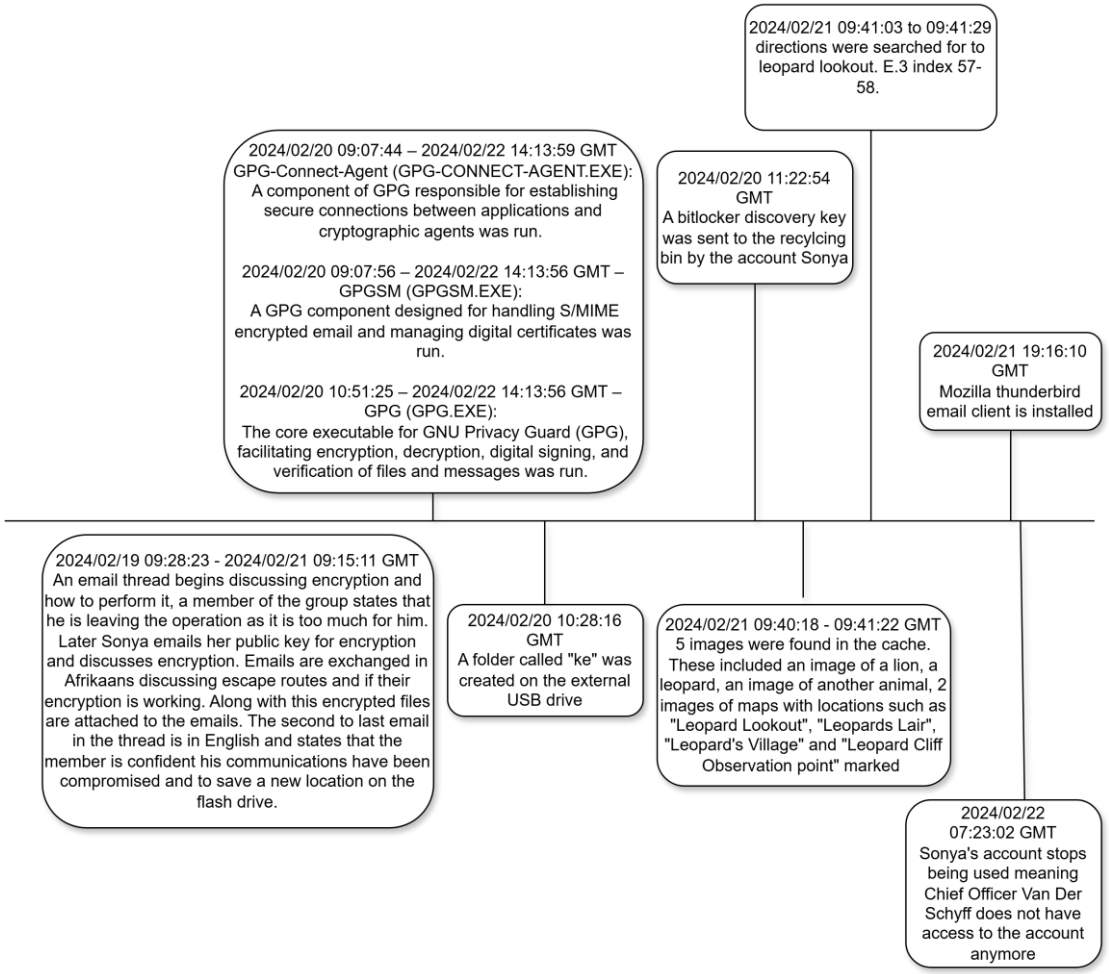

2024/02/06 07:09:59 GMT thirteen images of giraffes were backed up onto the drive and one of a plush giraffe (see figure A.5.32 - A.5.45). The names of these are simply descriptive. These were mainly taken using the Canon Eos 30, Canon Eos R5 and Yashica Mat-124g cameras.
2024/02/06 10:23:54 - 10:41:35 GMT 22 images were discovered on the cache including images of hunting rifles, images of animals and poaching and an image of an arrowhead
2024/02/06 10:24:08 - 10:35:05 GMT Browser session started researching Bow hunting elephants, anti-forensic techniques, cameras that are good for taking pictures of wildlife, how poachers are tracked, hunted down and how there deaths are celebrated and how much a forensic investigator would cost.
2024/02/06 10:19:12 GMT Email sent containing discussions about effectiveness of the drone and there first hunt as well as theplans moving forward for their hunts. This also included and image of an elephant as an attachment
2024/02/07 09:26:54 - 09:27:04 GMT The folder "backup_07022" was created in the documents folder. Three other items were added to this folder they were "elephant", "mission spec" and "mission pic"
2024/02/06 10:17:44 GMT A folder called elephant was created and moved to be within the documents folder
2024/02/06 10:18:07 GMT 11 Images of elephants were found
2024/02/06 10:31:39 GMT End of poem email thread and emails are changed to discussing moving forward with the operation and how to deal with a possible tail. They decide to continue with just a camera instead of a drone
2024/02/07 09:27:06 GMT the folders "mission spec" and "mission pic" were created on the USB drive

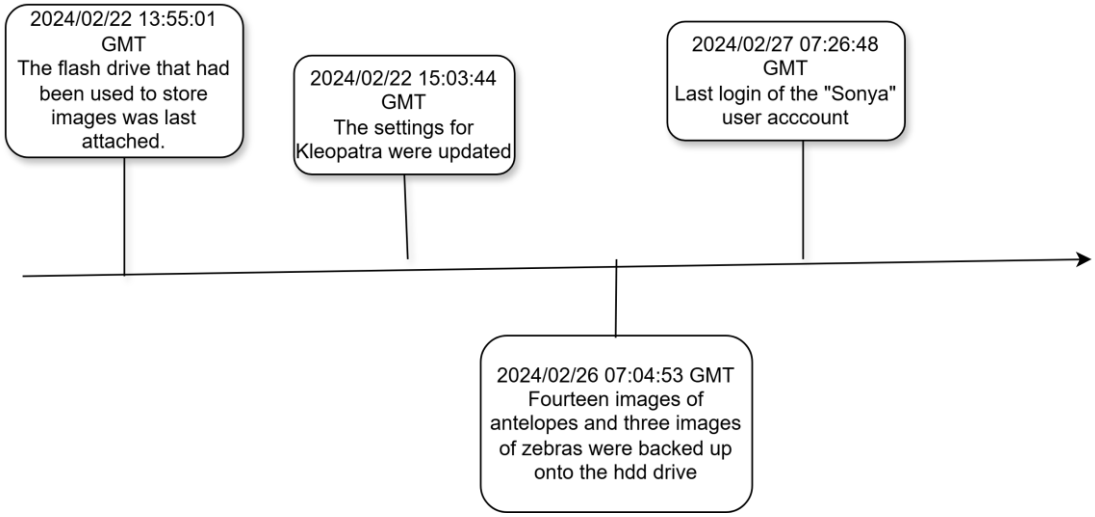

2024/01/09 07:48:21 to 07:48:58 research into anti forensic techniques. Open-source tools and hash keeper. E.3 index 23-24.
A legitimate Windows command-line utility for certificate management, file hashing, and downloading files from remote servers; it can also be misused for unauthorized data transfer was run.
2024-01-11 09:48:14 – 2024-01-11 09:48:15 GMT
Npcap Installer (NPFINSTALL.EXE): An installer for a packet capture driver commonly used with network analysis tools such as Wireshark, supporting network monitoring and traffic analysis was run
2024/01/19 09:14:21 - 2024/01/23 10:23:54 GMT
Discussion of a location to test the drone and to configure it. coordinates were exchanged (-1.3219782 (lat), 34.9261049 (long)) and an image attachment of these coordinates was sent and the location was set
2024/01/08 07:57:13 GMT
email thread entered discussing drone surveillance, heights and upgrades and getting permits. final meeting dates were discussed and bringing in a new member discussed
2024/01/13 16:13:48 GMT
Deleted VeraCrypt icon found in autopsy
2024/01/19 08:51:28 GMT
End of email thread.
2024/01/05 11:18:00 - 2024/01/08 08:19:12 GMT
Email thread has been started discussing a trophy list/price list naming animals and pieces of poetry have been sent back and forth
2024/01/08 08:39:24 - 2024/01/09 07:34:34 GMT
A file was shared called "mission specs" via email and has been replied to with a thumbs up and a poem
2024/01/11 09:48:25 - 09:49:49 GMT
three programs were installed, Wireshark, Npcap, and USBPcap. Upon researching the on the internet, it became clear that Wireshark and Npcap are both tools for monitoring network traffic, and that USBPcap is an open source USB Packet capture for Windows.
2024/01/11 09:45:14 to 2024-01-15 11:25:34 Booking cheap flights to Kenya EDI to NBO, 31/1 — 6/2 . Edinburgh to Nairobi on the 31st of January and returning on the 6th of February visited a total of 4 times. E.3 index 25. Flight bookings Nairobi - Google Search visited a total of twice. E.3 index 26.
2024/01/16 11:26:17 GMT
Searching for Garden city mall in Nairobi visited 3 times. E.3 index 27.
2024/01/17 13:11:35 -13:20:10 GMT
A browser session was entered doing research about malware scanners to check for viruses, poaching and the poaching crisis in Kenya and Africa. Then research was done on skeletons of elephants


2024/01/23 10:10:30 to 10:18:35 viewing the coordinates for the Olare Motorogi Conservatory and coordinates east of Olenteki in Kenya and west of Kawai. E.3 index 30-31
2024/01/24 13:35:48 - 13:36:50 GMT
A browser session began with sonya researching steghide and steganography then between 13:41:11 - 13:41:21 GMT the topic of the session changed to becoming a double agent and stealing information from intelligence agencies
2024/01/26 09:03:21 - 09:23:32 GMT
Email thread of containing photos of the group, the drones and photos of contracts for the group to sign
2024/02/05 08:06:04 - 08:07:32 GMT
An email thread was entered discussing final mission preparations and that everything was ok set up from other members of the group
2024/01/24 13:36:10 - 13:40:46 GMT
The program steghide was installed. The folder “steghide-0.5.1-win32.zi” was created, accessed, extracted to “steghide-0.5.1-win3” and items were written to the file "steghid". Steghide was last run at 13:40:27 GMT and was sent to the recycling bin at 13:40:46 GMT. Steghide is a steganography program
2024/01/26 09:26:29 - 10:03:42 GMT
Browser session started looking into booking an elephant hunting trip in Kenya and South Africa, what gear was needed for
2024/01/23 10:41:44 GMT
A strange poem in Afrikaans with the subject line "key to success" is sent to Sonya. A thread is entered where Sonya is told that the poems meaning will be explained at their meeting on 2024/02/06 at 10am GMT and that they may have a tail. This poem is translated to be Bitter-berry daybreak by Ingrid Jonker
2024/01/26 09:04:42 GMT
"mission pic" folder was created within the documents folder
2024/01/26 09:21:32 GMT
"mission spec" file accessed and modified


2024/02/08 12:36:51 - 2024/02/12 07:35:16 GMT
An email thread was started discussing the purchase of a CANON EOS R5 for taking photos on their hunts and confirming the plan for the 10th - 20th. Then Sonya received 2 poems and responded with an email that contained a document attached that had a list of animals and dates. They also state that they will begin at waypoint beta and how to enhance security of their emails.
2024/02/08 13:48:15 GMT
The program AnalogExif was installed, upon research this is a tool used to edit the metadata of digital images or videos
2024/02/09 09:14:41 GMT
A .txt file named "the_list.txt" was created containing the names of animals with dates beside them including elephants that says done. This is the list that Sonya would attach in her email
2024/02/10 14:00:00 - 14:58:00 GMT
An image of a lion and an image of a lion and an elephant was taken on a Canon EOS R5 by the artist thescout
2024/02/13 13:00:00 - 14:00:00 GMT
2 images of Antelopes were taken by the artist Sonya the first taken with a Canon EOS R5 and the second taken with a Yashica Mat-124G
2024/02/14 07:03:53 GMT
An image of an antelope has been found. It has been taken by a Canon EOS R5 and by thescout. Its time of creation has been set to 00:00:00 GMT
2024/02/14 07:15:56 - 2024/02/19 09:11:34 GMT
A total of 7 items were created and added to the "backup_07022" folder. These files were "incident_"", “nois”, “buffal”, “hippo”, "giraff", "antelop" and "lion". As well as this a "lion" item was created and added to the documents folder.
2024/02/14 07:18:00 GMT
Two images of buffalo are backed up.
2024/02/14 07:21:39 - 2024/02/16 07:25:31 GMT
An email thread begins with Sonya discussing the lions and checking if they are being tailed and discussing moving to Waypoint charlie. Another thread discusses them retrieving good material but having had close calls. They decide to begin using encryption to secure communications and decide to go to 2 more waypoints only and speak in Afrikaans where possible
2024/02/16 07:12:12 GMT
Nine images of lions are backed up
2024/02/16 09:52:00-9:53:25 GMT
A browser searching session began with Sonya researching how to hunt hippos, 2024-2025 South African Hunting price list for The Big Game Hunting Adventure


2024/02/19 09:17:11 - 2024/02/22 13:57:29 GMT
Sonya enters a browsing session about encryption software and encryption as a whole as well as how to go into hiding
2024/02/19 09:25:09 – 2024-02-22 14:13:53 GMT
Kleopatra (KLEOPATRA.EXE):
A graphical interface for managing encryption keys and certificates. It enables users to encrypt, decrypt, and digitally sign files and communications was run.
2024-02-19 09:25:16 – 2024-02-22 14:13:59 GMT
GPG-Agent (GPG-AGENT.EXE):
A background agent process that securely handles private key operations for cryptographic activities.
2024-02-19 09:25:18 – 2024-02-22 14:13:56 GMT
GPGConf (GPGCONF.EXE):
A configuration utility used to manage GnuPG (GPG) settings, allowing users to customise encryption parameters and operational preferences.
2024/02/19 09:11:50 - 09:12:59 GMT
26 Images have been moved to the recycling bin on the Sonya account. This includes images of buffalo and hippos
2024/02/19 09:11:07 GMT
An MP4 file of hippo was located through autopsy.
2024/02/19 09:11:33 GMT
13 images of hippos and one video of a hippo have been backed up
2024/02/19 09:22:00 GMT
VeraCrypt Setup (VERACRYPT SETUP 1.26.7.EXE):
An installer for VeraCrypt, a tool used to create encrypted containers or full disk volumes, protecting stored data was run.
At 09:24:37 GMT GPG4Win Setup (GPG4WIN-4.3.0.EXE):
The installation file for GPG4Win, a free encryption software suite that facilitates secure communication and data protection was also run.
2024/02/19 09:20:32 GMT
Autopsy found various files related to the encryption software VeraCrypt including a file callled "VeraCrypt Hidden Operating System.html"


2024/02/21 09:41:03 to 09:41:29 directions were searched for to leopard lookout. E.3 index 57-58.
2024/02/20 09:07:44 – 2024/02/22 14:13:59 GMT GPG-Connect-Agent (GPG-CONNECT-AGENT.EXE): A component of GPG responsible for establishing secure connections between applications and cryptographic agents was run.
2024/02/20 09:07:56 – 2024/02/22 14:13:56 GMT – GPGSM (GPGSM.EXE): A GPG component designed for handling S/MIME encrypted email and managing digital certificates was run.
2024/02/20 10:51:25 – 2024/02/22 14:13:56 GMT – GPG (GPG.EXE): The core executable for GNU Privacy Guard (GPG), facilitating encryption, decryption, digital signing, and verification of files and messages was run.
2024/02/20 11:22:54 GMT A bitlocker discovery key was sent to the recylcing bin by the account Sonya
2024/02/21 19:16:10 GMT Mozilla thunderbird email client is installed
2024/02/19 09:28:23 - 2024/02/21 09:15:11 GMT An email thread begins discussing encryption and how to perform it, a member of the group states that he is leaving the operation as it is too much for him. Later Sonya emails her public key for encryption and discusses encryption. Emails are exchanged in Afrikaans discussing escape routes and if their encryption is working. Along with this encrypted files are attached to the emails. The second to last email in the thread is in English and states that the member is confident his communications have been compromised and to save a new location on the flash drive.
2024/02/20 10:28:16 GMT A folder called "ke" was created on the external USB drive
2024/02/21 09:40:18 - 09:41:22 GMT 5 images were found in the cache. These included an image of a lion, a leopard, an image of another animal, 2 images of maps with locations such as "Leopard Lookout", "Leopards Lair", "Leopard's Village" and "Leopard Cliff Observation point" marked
2024/02/22 07:23:02 GMT Sonya's account stops being used meaning Chief Officer Van Der Schyff does not have access to the account anymore


2024/02/22 13:55:01 GMT
The flash drive that had been used to store images was last attached.
2024/02/22 15:03:44 GMT
The settings for Kleopatra were updated
2024/02/27 07:26:48 GMT
Last login of the "Sonya" user acccount
2024/02/26 07:04:53 GMT
Fourteen images of antelopes and three images of zebras were backed up onto the hdd drive

End of Graphical Timeline

Appendix D Chain of Custody

A copy of the chain of custody form will be submitted with the project in full, a copy of its contents can be seen below for reference.

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: 1136 Offense: poaching
Submitting Officer: (Name/ID#) Chief Officer Karl Van Der Schaff
Victim: N/A
Suspect: Sonya Macoit
Date/Time Seized: 1/2/2025
Location of Seizure: Abertay University, Bell Street, Dundee, Scotland DD1 1HG

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
#001_HDD_01	1	Recovered HDD drive from Sonya Macoit's laptop, pristine condition, no marks, no scratches
#001DISK_01	1	Recovered USB drive from Sonya Macoit's person, pristine condition, no marks, no scratches

#003_TXT	1	.txt document containing a hash
#004_TXT	1	.txt document containing details of recovered USB

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
#001_HDD_01	2025/02/01	Chief Officer Van Der Schyff	J Buckley	MD5: aebd2d140eaf215e1a8554d008c5e2b3 SHA1: 3c7bae35a28e12d67ed62cb9c09ee8e5935047fe
#001DISK_01	2025/04/14	Chief Officer Van Der Schyff	J Buckley	Potentially encrypted, Model unknown
#003_TXT	2025/04/14	Chief Officer Van Der Schyff	J Buckley	Suspected to be a copy of a password hash used by Sonya Macoit
#004_TXT	2025/04/14	Chief Officer Van Der Schyff	J Buckley	Details of the recovered USB

Appendix E Browser History

Figure E.1.1 - Windows 11 history carving from raw disk, hardening windows 11 systems 2024/02/24, Investigator JB

636 https://www.google.com/search?q=hardening+a+windows+11+machine+to+counter+digital+forensics&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hardening+a+windows+11+machine+to+counter+digital+forensics&gs_lcrp=EgZja
HJvbWUyCOgAEEUYORigATIHCAEQIRigAdIBCTE1NDMzajBqNKgCALACAA&sourceid=chrome&ie=UTF-8 hardening a windows 11 machine to counter digital forensics - Google Search 2 0 13351595665851829 0
637 https://medium.com/@larry-baldwin/hardening-windows-11-d600ab21f926 Hardening Windows 11. This article outlines the various steps... | by Larry Baldwin | Dec, 2023 | Medium 1 0 13351688628849428 0
638 https://learn.microsoft.com/en-gb/windows/client-management/mdm/ Configuration Service Provider - Windows Client Management | Microsoft Learn 2 0 13351688623982459 0
639 https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ BitLocker overview - Windows Security | Microsoft Learn 2 0 13351688616516707 0
640 https://www.google.com/search?q=hunting+elephant+with+bow+and+arrow&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hunting+elephant+&gs_lcrp=EgZjaHJvbWUqBwgCEAAYgAQyBggAEEUYOTIHCAEQABiABDIHCA
MQABiABDIKCAQQABgPGBYYHjIKCAUQABgPGBYYHjIICAYQABgWGB4yCAgHEAAYFhgeMggICBAAGBYYHjIICAkQABgWGB7SAQg4NjcwajBqN6gCALACAA&sourceid=chrome&ie=UTF-8 hunting elephant with bow and arrow - Google Search 3 0 1335168
8654708378 0
641 https://www.africahunting.com/threads/bowhunting-elephant-best-setup.5043/ Bowhunting ELEPHANT Best Setup | AfricaHunting.com 1 0 13351688648075231 0
642 https://www.google.com/search?q=antiforensic+techniques&rlz=1C1ONGR_en-GBGB1089GB1089&oq=antiforensic+techniques&gs_lcrp=EgZjaHJvbWUyBqgAEEUYOTIJCAEQABqKGIAE0qEINTIyM2owajeoAqCwAqA&sourceid=chrome&ie

Full text:

35 https://publications.waset.org/abstracts/178705/pdf 24US060281 1 0 13350997945812033 0 636 https://www.google.com/search?q=hardening+a+windows+11+machine+to+counter+digital+forensics&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hardening+a+windows+11+machine+to+counter+digital+forensics&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORigATIHCAEQIRigAdIBCTE1NDMzajBqNKgCALACAA&sourceid=chrome&ie=UTF-8 hardening a windows 11 machine to counter digital forensics - Google Search 2 0 13351595665851829 0 637 https://medium.com/@larry-baldwin/hardening- windows-11-d600ab21f926 Hardening Windows 11. This article outlines the various steps... | by Larry Baldwin | Dec, 2023 | Medium 1 0 13351688628849428 0 638 https://learn.microsoft.com/en-gb/windows/client-management/mdm/ Configuration Service Provider - Windows Client Management | Microsoft Learn 2 0 13351688623982459 0 639 https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ BitLocker overview - Windows Security | Microsoft Learn 2 0 13351688616516707 0 640 https://www.google.com/search?q=hunting+elephant+with+bow+and+arrow&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hunting+elephant+&gs_lcrp=EgZjaHJvbWUqBwgCEAAYgAQyBggAEEUYOTIHCAEQABiABDIHCAIQABiABDIHCAMQABiABDIKCAQQABgPGBYYHjIKCAUQABgPGBYYHjIICAYQABgWGB4yCAgHEAAYFhgeMggICBAAGBYYHjIICAkQABgWGB7SAQg4NjcwajBqN6gCALACAA&sourceid=chrome&ie=UTF-8 hunting elephant with bow and arrow - Google Search 3 0 13351688654708378 0

Figure E.2.1 - Edge artifacts 2023/12/19 - 2024/02/22, MD5 602e46cb905ee91c55032a1d37ad435a Investigator JB MF

Records extracted using BrowingHistoryView

https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Disclosure -	02/01/2024 13:06:57	2	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Box - .22 Hor...	02/01/2024 13:07:01	1	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Box - .22 Hor...	02/01/2024 13:07:01	1	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Box - .22 Hor...	02/01/2024 13:07:01	1	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Box - .22 Hor...	02/01/2024 13:07:01	1	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Box - .22 Hor...	02/01/2024 13:07:01	1	Link	Chrome
https://en.wikipedia.or...	22-Hornet-Box - .22 Hor...	02/01/2024 13:07:01	1	Link	Chrome

Index	Visit Count	Title	Visit Time	URL	Description
1	1	Thunderbird — Free Your Inbox. — Thunderbird	2023/12/19 14:25:57	https://www.thunderbird.net/en-GB/	Thunderbird

2	1	Kenya relief location map - Maasai Mara - Wikipedia	2024/01/02 11:39:22	https://en.wikipedia.org/wiki/Maasai_Mara#/media/File:Mara_River_Massai_Mara.jpg	Masai mara research
3	4	Maasai Mara - Wikipedia	2024/01/02 11:39:30	https://en.wikipedia.org/wiki/Maasai_Mara	Masai mara research
4	2	African bush elephant (Loxodonta africana) baby 6 weeks - African bush elephant - Wikipedia	2024/01/02 11:49:04	https://en.wikipedia.org/wiki/African_bush_elephant#/media/File:African_bush_elephant_(Loxodonta_africana)_baby_6_weeks.jpg	Elephant research
5	1	Knysna elephants - Wikipedia	2024/01/02 11:50:16	https://en.wikipedia.org/wiki/Knysna_elephants	Elephant research
6	1	Hunting:Elephant - Hunt in Africa	2024/01/02 11:50:54	https://huntinafrica.com/elephant-hunting/#:~:text=Elephant%20hunting%20is%20allowed%20in,adequately%20protected%20and%20well%20managed.	Elephant hunting
7	1	Home - bulletsafaris	2024/01/02 12:09:47	https://bulletsafaris.com/	Hunting expadition
8	2	remington .416 - Google Search	2024/01/02 13:02:35	https://www.google.com/search?q=remington+.416&rlz=1C1ONGR_en-GBGB1089GB1089&oq=remington+.416&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yCAgCEAAYFhgeMggIAxAAGBYYHjIICAQQABgWGB4yCAgFEAAYFhgeMggIBhAAGBYYHjIGCAcQRRg80gEINDE1NWowajSoAgCwAgA&sourceid=chrome&ie=UTF-8	Elephant hunting equipment
9	1	.416 Remington Magnum - Wikipedia	2024/01/02 13:02:37	https://en.wikipedia.org/wiki/.416_Remington_Magnum	Elephant hunting equipment

10	1	Model 700 Safari KS rifle - Google Search	2024/01/02 13:03:54	https://www.google.com/search?q=Model+700+Safari+KS+rifle&rlz=1C1ONGR_en-GBGB1089GB1089&sourceid=chrome&ie=UTF-8#vhid=DvtP3eZOzudojM&vssid=l	Elephant hunting equipment
11	1	Remington 700 KS Safari 416 Rem Mag Rifle | AfricaHunting.com	2024/01/02 13:04:00	https://www.africahunting.com/media/remington-700-ks-safari-416-rem-mag-rifle.100824/	Elephant hunting equipment
12	1	Custom Winchester M70 Alaskan 375 H&H Rifle w/CRF | AfricaHunting.com	2024/01/02 13:04:27	https://www.africahunting.com/media/custom-winchester-m70-alaskan-375-h-h-rifle-w-crf.100814/	Elephant hunting equipment
13	1	Table of handgun and rifle cartridges	2024/01/02 13:04:52	https://en.wikipedia.org/wiki/Table_of_handgun_and_rifle_cartridges	Elephant hunting equipment
14	1	. 22 Long Rifle - Wikipedia	2024/01/02 13:05:36	https://en.wikipedia.org/wiki/.22_Long_Rifle	Elephant hunting equipment
15	1	Raging Hornet	2024/01/02 13:07:04	https://en.wikipedia.org/wiki/.22_Hornet#/media/File:22-Hornet-Box.jpg	Elephant hunting equipment
16	3	poaching in kenya and africa - Search	2024/01/17 13:13:18	https://www.bing.com/search?q=poaching+in+kenya+and+africa&cvid=c4db906a941f4051817764401349829d&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQABhAMgYIAhAAGEAyBggDEAAYQDIGCAQQABhAMgYIBRAAGEAyBggGEAAYQDIGCAcQABhAMgYICBAAGEDSAQg2Njg4ajBqNKgCALACAA&FORM=ANAB01&DAF0=1&PC=U531	Poaching research
17	2	Fighting Wildlife Trade in Kenya | United Nations	2024/01/17 13:15:04	https://www.un.org/en/chronicle/article/fighting-wildlife-trade-kenya#:~:text=P%20oaching%20is%20a%20persistent%20global%20problem%20with,rhino%20populations%20in%20Kenya%2C%20Tanzania%20and%20throughout%20Africa.	Anti-poaching research
18	1	Africa's Poaching Crisis – AWF	2024/01/17 13:15:15	https://campaign.awf.org/poaching-infographic/	Anti-poaching research

19	1	Advancing Community-led Wildlife Economies in Uganda's Karamoja | African Wildlife Foundation	2024/01/17 13:18:05	https://www.awf.org/news/advancing-community-led-wildlife-economies-ugandas-karamoja	Elephant research
20	1	Serengeti Elefantenherde2 - African elephant	2024/01/17 13:20:08	https://en.wikipedia.org/wiki/African_elephant#/media/File:African_Bush_Elephant_Skull.jpg	Elephant research
21	1	The decline in the number of African elephants	2024/01/17 13:20:16	https://en.wikipedia.org/wiki/African_elephant#/media/File:Number_of_African_elephants.svg	Elephant research
22	2	African elephant - Wikipedia	2024/01/17 13:20:24	https://en.wikipedia.org/wiki/African_elephant	Elephant research
23	1	steghide download | SourceForge.net	2024/01/24 13:36:50	https://sourceforge.net/projects/steghide/	Steghide
24	1	Trophy Hunting the Elephant in South Africa - ASH Adventures	2024/01/26 09:26:57	https://www.africanskyhunting.co.za/trophies/elephant-hunting.html	Elephant hunting
25	4	hunting for elephant - Google Search	2024/01/26 09:27:19	https://www.google.com/search?q=hunting+for+elephant&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hunting+for+elephant&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDY5MTFqMWo3qAIAsAIA&sourceid=chrome&ie=UTF-8	Searches for elephant hunting
26	1	Elephant hunting in Kenya - Wikipedia	2024/01/26 09:27:39	https://en.wikipedia.org/wiki/Elephant_hunting_in_Kenya	Elephant hunting

27	1	Equipment for African Elephant Hunting | 2 - YouTube	2024/01/26 09:28:55	https://www.youtube.com/watch?v=iYS2PAlXmls	Elephant hunting equipment
28	1	Gearing Up for an Elephant Hunt | An Official Journal Of The NRA	2024/01/26 09:29:48	https://www.americanhunter.org/content/gearing-up-for-an-elephant-hunt/	Elephant hunting equipment
29	1	Top 8 Bullets for African Plains Game | An Official Journal Of The NRA	2024/01/26 10:03:17	https://www.americanhunter.org/content/top-8-bullets-for-african-plains-game/	Safari hunting equipment
30	1	Wildlife Conferences in 2024/2025/2026	2024/01/29 10:30:54	https://waset.org/wildlife-conferences	Wildlife conferences
31	1	Environmental Planning for Sustainable Utilization of Lake Chamo Biodiversity Resources: Geospatially Supported Approach, Ethiopia	2024/01/29 10:32:25	https://publications.waset.org/abstracts/178705/pdf	Documentation of better environmental concern
32	1	The Greatest Maasai Mara Photographer of the Year Winner Announcement	2024/02/02 08:52:12	https://web.archive.org/web/20190812161157/https://nomadmagazine.co/the-greatest-maasai-mara-photographer-of-the-year-winner-announcement/	Looking into maasai mara photography

33	1	Bowhunting ELEPHANT Best Setup | AfricaHunting.com	2024/02/06 10:24:08	https://www.africahunting.com/threads/bowhunting-elephant-best-setup.5043/	Elephant hunting
34	2	antiforensic techniques - Google Search	2024/02/06 10:32:29	https://www.google.com/search?q=antiforensic+techniques&rlz=1C1ONGR_en-GBGB1089GB1089&oq=antiforensic+techniques&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQABgKGIAE0gEINTIyM2owajeoAgCwAgA&sourceid=chrome&ie=UTF-8	Research into anti forensic techniques
35	2	how are poachers tracked down - Google Search	2024/02/06 10:35:43	https://www.google.com/search?q=how+are+poachers+tracked+down&rlz=1C1ONGR_en-GBGB1089GB1089	Research into how poachers are tracked
36	1	Computer Hacking Forensic Investigator | CHFI - EC-Council Learning	2024/02/06 10:54:49	https://iclass.eccouncil.org/product/computer-hacking-forensic-investigator/	Research into anti forensic techniques
37	2	ISO 14001 Certification | Centre for Assessment	2024/02/07 09:34:16	https://www.centreforassessment.co.uk/iso-14001-certification/?msclkid=2c2669fb565f102baa4c0c3818d18819	Reseach into environmental impacts
38	2	Environmental Impact Assessment - GOV.UK	2024/02/07 09:38:24	https://www.gov.uk/guidance/environmental-impact-assessment#Preparing-an-Environmental-Statement1	Reseach into environmental impacts
39	1	The Environmental Information Regulations 2004	2024/02/07 09:38:57	https://www.legislation.gov.uk/uksi/2004/3391/regulation/8/made	Enviromental regulations
40	2	how often can cancer be cured? - Search	2024/02/12 07:38:28	https://www.bing.com/search?pglt=2083&q=how+often+can+cancer+be+cured%3F&cvid=5cecb3f642f34feeb472893188eb4216&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQABhAMgYIAhAAGEAyBggDEAAYQDIGCAQQABhAMgYIBRAAGEAyBggGEAAYQDIGCAcQABhAMgYICBAAGEDSAQg3Mzc0ajBqMagCALACAA&FORM=ANSPA1&DAF0=1&PC=U531	Cancer research

41	1	NHS England » Cancer	2024/02/12 07:38:29	https://www.england.nhs.uk/cancer/	Cancer research
42	1	Email Encryption - OpenPGP	2024/02/14 07:31:33	https://www.openpgp.org/software/	Research into anti forensic techniques
43	2	hunting hippos - Search	2024/02/16 09:53:24	https://www.bing.com/search?q=hunting+hippos&cvid=effee89cd3a740d09c5253ac7c6d7b34&gs_lcrp=EgZjaHJvbWUqBggAEEUYOzIGCAAQRRg7MgYIARAAGEAyBggCEAAYQDIGCAMQABhAMgYIBBAAGEAyBggFEAAYQDIGCAYQRRhA0gEIMjk3NGowajSoAgCwAgA&FORM=ANAB01&DAF0=1&PC=U531	Looking into hunting hippos
44	1	2024-2025 South Africa Hunting Price List - Big Game Hunting Adventures	2024/02/16 09:53:25	https://biggamehuntingadventures.com/south-africa-hunting-price-list/	Value for the bodies of hunted animals
45	1	The Best Encryption Software for 2024	2024/02/19 09:17:48	https://uk.pcmag.com/encryption/83976/the-best-encryption-software-for-2020	Research into anti forensic techniques
46	2	axcrypt - Search	2024/02/19 09:18:49	https://www.bing.com/search?pglt=43&q=axcrypt&cvid=bcd5d0810f5546eaa425292898f04787&gs_lcrp=EgZjaHJvbWUqBggAEAAYQDIGCAAQABhAMgYIARAAGEAyBggCEAAYQDIGCAMQABhAMgYIBBAAGEAyBggFEAAYQDIGCAYQABhAMgYIBxAAGEAyBggIEAAYQNIBCDIwNDdqMGoxqAIAsAIA&FORM=ANNTA1&DAF0=1&PC=U531	Research into anti forensic techniques

47	1	VeraCrypt - Free Open source disk encryption with strong security for the Paranoid	2024/02/19 09:21:37	https://www.veracrypt.fr/en/Documentation.html	Research into anti forensic techniques
48	1	GnuPG - Download	2024/02/19 09:23:13	https://gnupg.org/download/index.html	Research into anti forensic techniques
49	1	Gpg4win - OpenPGP	2024/02/19 09:23:43	https://www.openpgp.org/software/gpg4win/	Research into anti forensic techniques
50	1	When missing people don't want to be found: 'I'd removed myself to push the world away' | Life and style | The Guardian	2024/02/19 09:43:19	https://www.theguardian.com/lifeandstyle/2021/jun/05/when-missing-people-dont-want-to-be-found-id-removed-myself-to-push-world-away	Looking into going into hiding
51	3	howto go into hiding - Search	2024/02/19 09:44:49	https://www.bing.com/search?q=howto+go+into+hiding&cvid=ec8587ed07b7477c95ef82e58033b0b6&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQABhAMgYIAhAAGEAyBggDEAAYQDIGCAQQABhAMgYIBRAAGEAyBggGEAAYQDIGCAcQABhAMgYICBAAGEDSAQgzNjIzajBqNKgCALACAA&FORM=ANAB01&DAF0=1&PC=U531	Looking into going into hiding
52	1	Survival in Hiding | Facing History & Ourselves	2024/02/19 09:44:50	https://www.facinghistory.org/resource-library/survival-hiding	Looking into going into hiding

53	1	pgp for windows systems - Search	2024/02/19 09:45:03	https://www.bing.com/search?q=pgp+for+windows+systems&cvid=f1d819a2d63a4fa785ef1c2e1dbc3fc6&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQABhAMgYIAhAAGEAyBggDEAAYQDIGCAQQABhAMgYIBRAAGEAyBggGEAAYQDIGCAcQABhAMgYICBAAGEDSAQgzNjIzajBqNKgCALACAA&FORM=ANAB01&DAF0=1&PC=U531&ntref=1	Research into anti forensic techniques
54	1	pgp encryption - Search	2024/02/19 09:45:05	https://www.bing.com/search?q=pgp+encryption&cvid=b5c323780a0740afbc88bb9cbb58a7aa&gs_lcrp=EgZjaHJvbWUqBggBEAAYQDIGCAAQRRg5MgYIARAAGEAyBggCEAAYQDIGCAMQABhAMgYIBBAAGEAyBggFEAAYQDIGCAYQABhAMgYIBxAAGEAyBggIEAAYQNIBCDIyNjNqMGo0qAIAsAIA&FORM=ANAB01&DAF0=1&PC=U531&ntref=1_pgp encryption - Search	Research into anti forensic techniques
55	1	veracrypt - Search	2024/02/19 09:45:06	https://www.bing.com/search?q=veracrypt&qs=n&form=QBRE&sp=-1&ghc=1&lq=0&pq=veracrypt&sc=11-9&sk=&cvid=633688B971704DE3816861DA04E32994&ghsh=0&ghacc=0&ghpl=&ntref=1	Research into anti forensic techniques
56	1	best encryption software out there - Search	2024/02/19 09:46:12	https://www.bing.com/search?pglt=43&q=best+encryption+software+out+there&cvid=767eff90499c454a976ac3550387c9fb&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQABhAMgYIAhAAGEAyBggDEAAYQDIGCAQQABhAMgYIBRAAGEAyBggGEAAYQDIGCAcQABhAMgYICBAAGEDSAQg2MTc1ajBqMagCALACAA&FORM=ANSPA1&DAF0=1&PC=U531&ntref=1	Research into anti forensic techniques
57	2	hot air balloon safari masai mara - Search	2024/02/21 08:57:46	https://www.bing.com/search?pglt=43&q=hot+air+balloon+safari+masai+mara&cvid=e1cd5aba9efd41eab9b6c8015228799b&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQABhAMgYIAhAAGEAyBggDEAAYQDIGCAQQABhAMgYIBRAAGEAyBggGEAAYQDIGCAcQABhAMgYICBAAGEDSAQkxMzc3MWowajGoAgCwAgA&FORM=ANSPA1&DAF0=1&PC=U531	Booking hot air balloon rides

58	1	THE TOP Kenya Hot Air Balloon Rides (UPDATED 2024)	2024/02/21 08:57:57	https://www.viator.com/Kenya-tours/Balloon-Rides/d801-g1-c3?m=33953&supag=1234752577649481&supsc=dat-2328971786433984&supai=77172167770158&supdv=c&supnt=nt:o&suplp=41943&supli=142409&supti=dat-2328971786433984&tsem=true&supci=dat-2328971786433984&supkw=hot%20air%20balloon%20safari%20masai%20mara&msclkid=86efddd650851a74191bb803eb8fdbaa	Booking hot air balloon rides
59	2	Google Maps	2024/02/21 09:41:29	https://www.google.com/maps?s=web&rlz=1C1ONGR_en-GBGB1089GB1089&sca_esv=e96a0e7e0d01906d&vet=12ahUKEwjq9bv8kbyEAxWng_0HHWheCoUQ5OUKegQIKBAP..i&cs=0&um=1&ie=UTF-8&fb=1&gl=uk&sa=X&geocode=KZ9xQi2P_SwYMX26k-1JNiTB&daddr=G3QQ%2B782,+Talek,+Kenya	Searching for leopard lookout
60	1	veracrypt - Search	2024/02/22 13:56:27	https://www.bing.com/search?q=veracrypt&gs_lcrp=EgZjaHJvbWUqBwgCEEUYwgMyBwgAEEUYwgMyBwgBEEUYwgMyBwgCEEUYwgMyBwgDEEUYwgMyBwgEEEUYwgMyBwgFEEUYwgMyBwgGEEUYwgMyBwgHEEUYwgPSAQsxMDI0MjcxajBqMagCCLACAQ&FORM=ANSPA1&DAF0=1&PC=U531	Research into anti forensic techniques
61	1	pgp encryption - Search	2024/02/22 13:57:29	https://www.bing.com/search?q=pgp+encryption&gs_lcrp=EgZjaHJvbWUqBwgDEEUYwgMyBwgAEEUYwgMyBwgBEEUYwgMyBwgCEEUYwgMyBwgDEEUYwgMyBwgEEEUYwgMyBwgFEEUYwgMyBwgGEEUYwgMyBwgHEEUYwgPSAQsxMDg3MDk2ajBqMagCCLACAQ&FORM=ANNTA1&DAF0=1&PC=U531	Research into anti forensic techniques
62	1	Cabela's Official Website - Hunting, Fishing, Camping, Shooting & Outdoor Gear	2024/02/26 09:30:35	https://www.cabelas.com/shop/en#	Safari hunting equipment

Figure E.3.1 - Chrome artifacts 2023/01/02 - 2024/01/26, MD5 `9ef8df1315fb383db4c10bb4ea900d74` **Investigator JB MF**

Index	Visit Count	Title	Visit Time	URL	Description
1	3	Google Earth	2023/12/19 14:45:41	https://earth.google.com/web/search/Talek,+Kenya/@-1.46000223,35.22239954,1565.24634549a,992.54388655d,35y,-0h,0t,0r/data=CigiJgokCdkqFq2_GyRAESEs5JxL5TfAGUpK6LPFsVNAIYIvgoB1qzfA	Research into talek river
2	3	Cheetah with cubs - Maasai Mara - Wikipedia	2024/01/02 11:39:03	https://en.wikipedia.org/wiki/Maasai_Mara#/media/File:Cheetah_with_cubs.jpg	Research into Maasai Mara wildlife: chetah
3	4	African bush elephant - Wikipedia	2024/01/02 11:50:25	https://en.wikipedia.org/wiki/Maasai_Mara	Research into Maasai Mara wildlife: elephant
4	2	.416 or .458 Magnum - Google Search	2024/01/02 11:54:50	https://www.google.com/search?q=.416+or+.458+Magnum&rlz=1C1ONGR_en-GBGB1089GB1089&sourceid=chrome&ie=UTF-8	Research into elephant hunting equipment: Related to .416 ammunition artifact
5	2	.416 or .458 Magnum - Google Search	2024/01/02 11:54:50	https://huntinafrica.com/elephant-hunting/#:~:text=Elephant%20hunting%20is%20allowed%20in,adequately%20protected%20and%20well%20managed.	Research into elephant hunting equipment: Related to .416 ammunition artifact
6	1	The .416 Remington Mag | AfricaHunting.com	2024/01/02 11:55:30	https://www.africahunting.com/threads/416-remington-magnum-v-s-458-winchester-magnum.65533/	Research into elephant hunting equipment: Related to .416 ammunition artifact
7	2	Crocodile Hunt with Bullet Safaris with Nathan Askew - YouTube	2024/01/02 12:59:40	https://www.youtube.com/watch?v=U86eg6KqD_I&embeds_referring_euri=https%3A%2F%2Fbulletsafaris.com%2F&source_ve_path=Mjg2NjY&feature=emb_logo	Video about hunting crocodiles
8	2	remington .416 - Google Search	2024/01/02 13:02:35	https://www.google.com/search?q=remington+.416&rlz=1C1ONGR_en-GBGB1089GB1089&oq=remi	Research into elephant hunting equipment:

				ngton+.416&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yCAgCEAAYFhgeMgglAxAAGBYYHjIICAQQABgWGB4yCAgFEAAYFhgeMgglBhAAGBYYHjIGCAcQRRg80gEINDE1NWowajSoAgCwAgA&sourceid=chrome&ie=UTF-8	Related to .416 ammunition artifact
9	2	Model 700 Safari KS rifle - Google Search	2024/01/02 13:03:51	https://www.google.com/search?q=Model+700+Safari+KS+rifle&rlz=1C1ONGR_en-GBGB1089GB1089&sourceid=chrome&ie=UTF-8	Research into elephant hunting equipment: Related to .416 ammunition artifact
10	1	Model 700 Safari KS rifle - Google Search	2024/01/02 13:03:54	https://www.google.com/search?q=Model+700+Safari+KS+rifle&rlz=1C1ONGR_en-GBGB1089GB1089&sourceid=chrome&ie=UTF-8#vhid=DvtP3eZOzudojM&vssid=l	Research into elephant hunting equipment
11	1	Custom Winchester M70 Alaskan 375 H&H Rifle w/CRF | AfricaHunting.com	2024/01/02 13:04:27	https://www.africahunting.com/media/custom-winchester-m70-alaskan-375-h-h-rifle-w-crf.100814/	Research into elephant hunting equipment: Related to .416 ammunition artifact
12	3	Rifle cartridge comparison - Table of handgun and rifle cartridges - Wikipedia	2024/01/02 13:04:55	https://en.wikipedia.org/wiki/.416_Remington_Magnum	Research into elephant hunting equipment: 10mm rifle ammunition designed to hunt dangerous game in safari hunting
13	2	22-Hornet-Disclosure - .22 Hornet - Wikipedia	2024/01/02 13:06:57	https://en.wikipedia.org/wiki/.22_Long_Rifle	Research into elephant hunting equipment
14	1	2024-Wish-List-Trophy-Fees-with-Pics.pdf	2024/01/02 13:18:12	https://huntinafrica.com/wp-content/uploads/2023/12/2024-Wish-List-Trophy-Fees-with-Pics.pdf	Interest in animal trophy values
15	4	Google Earth	2024/01/02 13:21:19	https://earth.google.com/static/multi-	Coordinates along the

				threaded/versions/10.43.0.2/index.html?#search/Talek,+Kenya/@-1.46088548,35.22067145,1563.72792944a,998.8974228d,30.00026787y,0h,0t,0r/data=CigiJgokCdkqFq2_GyRAESEs5JxL5TfAGUpK6LPFsVNAIYIvgoB1qzfA	Talek river in Kenya, Noth East East of Maasi Malek nature reserve
16	7	Google Earth	2024/01/03 11:12:59	https://earth.google.com/web/@-1.37922483,35.12452962,1548.23791547a,42014.35550827d,30.00000001y,359.99999918h,0t,0r	Coordinates North if not in the Olikira campsite in the Maasai Mara Kenya
17	3	Drones: Protecting and Serving Elephants in Danger	2024/01/04 11:37:58	https://enterprise-insights.dji.com/blog/anti-poaching-drones-protect-elephants?hsLang=en	Visited Blog about drones designed to protect elephants
18	1	Wildlife Crime Scorecard	2024/01/04 11:50:09	http://www.flickr.com/photos/wwfint/7884702350/sizes/o/in/photostream/	Wildlife crime score card
19	3	the ethics of hunting - Google Search	2024/01/05 11:08:38	https://www.google.com/search?q=the+ethics+of+hunting&rlz=1C1ONGR_en-GBGB1089GB1089&oq=the+ethics+of+hunting&gs_lcrp=EgZjaHJvbWUqBwgAEAAYgAQyBwgAEAAYgAQyCAgBEAAYFhgeMggIAhAAGBYYHtIBCDQ0NzFqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8	Research into the ethics of hunting
20	3	wild life conferences - Google Search	2024/01/05 11:24:41	https://www.google.com/search?q=wild+life+conferences&rlz=1C1ONGR_en-GBGB1089GB1089&oq=wild+life+conferences&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQABgNGIAEMggIAhAAGA0YHjIICAMQABgNGB4yCAgEEAAYFhgeMgoIBRAAGAUYDRgeMgoIBhAAGAgYDRgeMgoIBxAAGAgYDRgeMgoICBAAGAgYDRgeMgoICRAAGAgYDRge0gEINDUzNGoxajSoAgCwAgA&sourceid=chrome&ie=UTF-8	Research into wildlife conferences, maybe related to comments of double agent previously seen
21	5	Microsoft Account	2024/01/08 08:23:56	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=19&ct=1704702184&rver=7.3.6962.0&wp=MBI_SSL_SHARE	Accessed emails on outlook

				D&wreply=https:%2F%2Fonedrive.live.com%3Fgologin%3D1%26mkt%3Den-GB&lc=2057&id=250206&cbcxt=sky&mkt=en-GB&lw=1&fl=easi2&username=sonyamacoit%40outlook.com	
22	2	encryption using hidden messages in poetry - Google Search	2024/01/09 07:37:42	https://www.google.com/search?q=encryption+using+hidden+messages+in+poetry&rlz=1C1ONGR_en-GBGB1089GB1089&oq=encryption+using+hidden+messgaes+in+poe&gs_lcrp=EgZjaHJvbWUqCQgBECEYChigATIGCAAQRRg5MgkIARAhGAoYoAEyCQgCECEYChigATIJCAMQIRgKGKAB0gEJMTcxNDhqMWo3qAIAsAIA&sourceid=chrome&ie=UTF-8	Research into Attempting to evade digital forensics
23	1	Digital Forensics: Get Started with These 9 Open Source Tools	2024/01/09 07:48:21	https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools	Research into digital forensics
24	2	HashKeeper - Google Search	2024/01/09 07:48:58	https://www.google.com/search?q=HashKeeper&rlz=1C1ONGR_en-GBGB1089GB1089&sourceid=chrome&ie=UTF-8	Research into Attempting to evade digital forensics
25	4	EDI to NBO, 31/1 — 6/2	2024/01/11 09:45:14	https://www.cheapflights.co.uk/flight-search/EDI-NBO/2024-01-31/2024-02-06?sort=bestflight_a	Booking cheap flights to Kenya
26	2	flight bookings nairobi - Google Search	2024/01/15 11:25:34	https://www.google.com/search?q=flight+bookings+nairobi&rlz=1C1ONGR_en-GBGB1089GB1089&oq=flight+bookings+nairobi&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yCAgCEAAYFhgeMggIAxAAGBYYHjIICAQQABgWGB4yDQgFEAAYhgMYgAQYigUyDQgGEAAYhgMYgAQYigUyDQgHEAAYhgMYgAQYigXSAQg4MTcwajBqN6gCALACAA&sourceid=chrome&ie=UTF-8	Booking flights to Kenya

27	3	Google Maps	2024/01/16 11:26:17	https://www.google.com/maps/place/Garden+City+Mall/@-1.2328114,36.8784843,3a,75y,90t/data=!3m8!1e2!3m6!1sAF1QipNXsBdidXAenpN1JGfEpCeI23J-2UK1NUrsOd6U!2e10!3e12!6shttps:%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipNXsBdidXAenpN1JGfEpCeI23J-2UK1NUrsOd6U%3Dw203-h135-k-no!7i1600!8i1066!4m16!1m8!3m7!1s0x182f1172d84d49a7:0xf7cf0254b297924c!2sNairobi,+Kenya!3b1!8m2!3d-1.2920659!4d36.8219462!16zL20vMDVkNDk!3m6!1s0x182f15dd4e9edb19:0x8df004aaaf625f93!8m2!3d-1.2324833!4d36.8787799!10e5!16s%2Fg%2F11by__tf_z?entry=ttu	Searching for Garden city mall in Nairobi
28	3	Loxodonta africana-cyclotis skulls PZSL - African elephant - Wikipedia	2024/01/17 13:19:40	https://en.wikipedia.org/wiki/African_elephant#/media/File:African_Elephant_distribution_map_without_borders.svg	Research into Maasai Mara wildlife: elephant
29	1	Elephant distribution map	2024/01/17 13:19:46	https://en.wikipedia.org/wiki/African_elephant#/media/File:African_Elephant_distribution_map_without_borders.svg	Elephant distribution map, shows elephants in Kenya
30	4	Google Earth	2024/01/23 10:10:30	https://earth.google.com/web/search/-1.3219782/@-1.3019885,35.12759034,1595.32343141a,45189.0146556d,30y,360h,0t,0r/data=CigiJgokCeSLKRuBBvO_EYaOasxMo_a_GW7dx_yyrUFAIXS46cX2ckFA	Coordinates for the Olare Motorogi Conservatory
31	8	Google Earth	2024/01/23 10:18:35	https://earth.google.com/web/search/1%C2%B019'19%22S+34%C2%B055'33%22E/@-1.24866903,34.92496682,1876.09247301a,41685.34484984d,30.00033771y,0h,0t,0r/data=CigiJgokCYNVBpZxzfK_	Coordinates east of Olenteki in Kenya and west of Kawai

				ETTZ95x7afa_GbWuRUFamkFAIYErAxwCfUFA	
32	1	Download steghide-0.5.1-win32.zip	2024/01/24 13:36:10	https://downloads.sourceforge.net/project/steghide/steghide/0.5.1/steghide-0.5.1-win32.zip?download&failedmirror=deac-ams.dl.sourceforge.net	Steghide
33	2	howto be a double agent? - Google Search	2024/01/24 13:41:11	https://www.google.com/search?q=howto+be+a+double+agent%3F&rlz=1C1ONGR_en-GBGB1089GB1089&oq=howto+be+a+double+agent%3F&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yCAgCEAAYFhgeMgglAxAAGBYYHjIICAQQABgWGB4yCAgFEAAYFhgeMgglBhAAGBYYHjIICAcQABgWGB4yDQgIEAAYhgMYgAQYigUyDQgJEAAYhgMYgAQYigXSAQg5NDU1ajBqN6gCALACAA&sourceid=chrome&ie=UTF-8	Research into being a Double agent
34	1	Kim Philby's 11 Tips On How To Become A Double Agent And Steal Secrets From The World's Most Famous Intelligence Service | HuffPost UK News	2024/01/24 13:41:21	https://www.google.com/search?q=howto+be+a+double+agent%3F&rlz=1C1ONGR_en-GBGB1089GB1089&oq=howto+be+a+double+agent%	Research into becoming a double agent
35	4	hunting for elephant - Google Search	2024/01/26 09:26:04	https://www.google.com/search?q=hunting+for+elephant&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hunting+for+elephant&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDY5MTFqMWo3qAIAsAIA&sourceid=chrome&ie=UTF-8	Research into elephant hunting
36	1	Elephant hunting trips - BookYourHunt.com	2024/01/26 09:26:29	https://www.bookyourhunt.com/en/elephant-hunting	Research into elephant hunting

37	1	Trophy Hunting the Elephant in South Africa - ASH Adventures	2024/01/26 09:26:57	https://www-africanskyhunting-co-za.webpkgcache.com/doc/-/s/www.africanskyhunting.co.za/trophies/elephant-hunting.html	Elephant hunting and trophy collection
38	3	equipment required to hunt elephant - Google Search	2024/01/26 09:28:41	https://www.google.com/search?q=equipment+required+to+hunt+elephant&rlz=1C1ONGR_en-GBGB1089GB1089&oq=equipment+required+to+hunt+elephant&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRigATIHCAIQIRigATIHCAMQIRifBTIHCAQQIRifBdIBCDY2NzFqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8	Research into elephant hunting equipment
39	2	Home - Safari Boots, Shoes and Accessories - The Courteney Boot Company	2024/01/26 09:30:23	https://www.americanhunter.org/content/gearing-up-for-an-elephant-hunt	Research into elephant hunting equipment: buying
40	1	5 Reasons to Book an African Plains Game Safari Now | An Official Journal Of The NRA	2024/01/26 10:03:42	https://www.americanhunter.org/content/top-8-bullets-for-african-plains-game/	Research into hunting equipment
41	2	American hunter	2024/01/26 10:06:39	https://www.americanhunter.org/articles/2016/8/19/5-reasons-to-book-an-african-plains-game-safari-now/	Article discussing why you should go hunting
42	2	hardening a windows 11 machine to counter digital forensics - Google Search	2024/02/05 08:34:25	https://www.google.com/search?q=hardening+a+windows+11+machine+to+counter+digital+forensics&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hardening+a+windows+11+machine+to+counter+digital+forensics&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORigATIHCAEQIRigAdIBCTE1NDMzajBqNKgCALACAA&sourceid=chrome&ie=UTF-8	Research into Attempting to evade digital forensics

43	3	hunting elephant with bow and arrow - Google Search	2024/02/06 10:23:53	https://www.google.com/search?q=hunting+elephant+with+bow+and+arrow&rlz=1C1ONGR_en-GBGB1089GB1089&oq=hunting+elephant+&gs_lcrp=EgZjaHJvbWUqBwgCEAAYgAQyBggAEEUYOTIHCAEQABiABDIHCAIQABiABDIHCAMQABiABDIKCAQQABgPGBYYHjIKCAUQABgPGBYYHjIICAYQABgWGB4yCAgHEAAYFhgeMggICBAAGBYYHjIICAkQABgWGB7SAQg4NjcwajBqN6gCALACAA&sourceid=chrome&ie=UTF-8	Research into elephant hunting equipment
44	1	Bowhunting ELEPHANT Best Setup | AfricaHunting.com	2024/02/06 10:24:08	https://www.africahunting.com/threads/bowhunting-elephant-best-setup.5043/	Research into elephant hunting equipment: Related to bow-based artifact
45	2	antiforensic techniques - Google Search	2024/02/06 10:32:29	https://www.google.com/search?q=antiforensic+techniques&rlz=1C1ONGR_en-GBGB1089GB1089&oq=antiforensic+techniques&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIJCAEQABgKGIAE0gEINTIyM2owajeoAgCwAgA&sourceid=chrome&ie=UTF-8	Research into Attempting to evade digital forensics
46	3	camera for wildlife photography - Google Search	2024/02/06 10:33:13	https://www.google.com/search?q=camera+for+wildlife+photography&rlz=1C1ONGR_en-GBGB1089GB1089&oq=camera+for+wildlife+photography&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORiABDIHCAEQABiABDIHCAIQABiABDIHCAMQABiABDIICAQQABgWGB4yCggFEAAYDxgWGB4yCggGEAAYDxgWGB4yCAgHEAAYFhgeMggICBAAGBYYHjIICAkQABgWGB7SAQg2MTAyajBqN6gCALACAA&sourceid=chrome&ie=UTF-8	Looking to buy a wildlife photography camera
47	2	Canon EOS R5 Body Camera: Amazon.co.uk:	2024/02/06 10:35:04	https://www.amazon.co.uk/dp/B08CNGTRS5?tag=georiot-trd-21&th=1&psc=1&ascsubtag=dcw-gb-	Shopping for cannon eos r5 camera

		Electronics & Photo		9645989983730960000-21&geniuslink=true	
48	2	how are poachers tracked down - Google Search	2024/02/06 10:35:43	https://www.google.com/search?q=how+are+poachers+tracked+down&rlz=1C1ONGR_en-GBGB1089GB1089&oq=how+are+poachers+tracked+down&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRigATIGCAIQIRgV0gEJMTAwMzhqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8	Research into how poachers are tracked
49	1	The technology fighting poachers | BBC Earth	2024/02/06 10:35:48	https://www.bbcearth.com/news/the-technology-fighting-poachers	Research into anti poaching methods
50	1	Hunting down the people who kill elephants | BBC Earth	2024/02/06 10:36:32	https://www.bbcearth.com/news/the-technology-fighting-poachers	Research into anti poaching methods
51	1	Celebrating the death of a poacher | BBC Earth	2024/02/06 10:40:43	https://www.bbcearth.com/news/celebrating-the-death-of-a-poacher	Research into the death of a poacher
52	1	Saving the world's most trafficked animal | BBC Earth	2024/02/06 10:41:21	https://www.bbcearth.com/news/meet-the-dogs-saving-endangered-species	Research into anti poaching methods
53	1	Computer Hacking Forensic Investigator (CHFI) | Digital Forensics Course	2024/02/06 10:46:53	https://cisomag.com/6-anti-forensic-techniques-that-every-digital-forensic-investigator-dreads/	Trying to learn how to evade a computer hacking forensic investigator
54	2	Computer Hacking Forensic Investigator (CHFI) | Digital Forensics Course	2024/02/06 10:46:58	https://www.eccouncil.org/train-certify/computer-hacking-forensic-investigator-chfi/?utm_source=cisomag&utm_medium=partners&utm_campaign=cisomag-ecc-chfi	Trying to learn how to become a computer hacking forensic investigator
55	3	cost of hacking and forensic investigator - Google Search	2024/02/06 10:48:36	https://www.google.com/search?q=cost+of+hacking+and+forensic+investigator&rlz=1C1ONGR_en-GBGB1089GB1089&oq=cost+of+hacking+and+forensic+i	Research into the costs of forensic investigators

				nvestigator&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQIRigATIHCAIQIRigATIHCAMQIRigAdIBCTEwMjIyajFqNKgCALACAA&sourceid=chrome&ie=UTF-8	
56	1	Computer Hacking Forensic Investigator (CHFI) Course | Learning Tree	2024/02/06 10:48:43	https://www.learningtree.co.uk/courses/chfi-certification-computer-hacking-forensic-investigator-course/	Trying to learn how to become a computer hacking forensic investigator
57	2	Leopard lookout Kenya - Google Search	2024/02/21 09:41:03	https://www.google.com/search?q=leopard+lookout+kenya&sca_esv=e96a0e7e0d01906d&rlz=1C1ONGR_en-GBGB1089GB1089&ei=IMXVZZGZMNqR9u8PrMWEqAM&ved=0ahUKEwiRqb75kbyEAxXaiP0HHawiATUQ4dUDCBA&uact=5&oq=leopard+lookout+kenya&gs_lp=Egxnd3Mtd2l6LXNlcnAiFWxlb3BhcmQgbG9va291dCBrZW55YTIFECEYoAEyBRAhGKABMgUQIRigAUjiFVCzAVitE3ABeACQAQCYAYsBoAHyBKoBAzMuM7gBA8gBAPgBAcICCRAAGAgYHhiwA8ICDhAAGIAEGIoFGIYDGLADwgIGEAAYFhgewgILEAAYgAQYigUYhgPCAgUQIRifBYgGAZAGCg&sclient=gws-wiz-serp	Research into Leopard lookout, Kenya
58	2	Google Maps	2024/02/21 09:41:29	https://www.google.com/maps?s=web&rlz=1C1ONGR_en-GBGB1089GB1089&sca_esv=e96a0e7e0d01906d&vet=12ahUKEwjq9bv8kbyEAxWng_0HHWheCoUQ5OUKegQIKBAP..i&cs=0&um=1&ie=UTF-8&fb=1&gl=uk&sa=X&geocode=KZ9xQi2P_SwYMX26k-1JNiTB&daddr=G3QQ%2B782,+Talek,+Kenya	Directions to leopard lookout

Figure E.4.1 Edge Cookies MD5 7900290d6b9540601383db1bbf1496c7, investigator MF EL

Index	Created_utc ^	Domain	Cookie name
1	13348673969449957	.youtube.com	CONSENT

2	13348673993548232	.youtube.com	SOCS
3	13348673993789526	.youtube.com	VISITOR_INFO1_LIVE
4	13348674002878657	.youtube.com	VISITOR_PRIVACY_METADATA
5	13348674247817269	.africahunting.com	__gads
6	13348674247818808	.africahunting.com	__gpi
7	13348674268954056	.africahunting.com	_ga
8	13348841353983340	.dji.com	_ga
9	13348841354334908	.dji.com	_tt_enable_cookie
10	13348841399378837	.dji.com	_ttp
11	13348841909732784	.dji.com	__hstc
12	13348841909733331	.dji.com	hubspotutk
13	13348841909874110	.dji.com	_gcl_au
14	13348841911263804	.dji.com	_fbp
15	13348841911930626	.dji.com	dji_consentmanager
16	13348841913131715	www.dji.com	_bl_uid
17	13348842285144888	.panda.org	_gcl_au
18	13348842293776877	.panda.org	_hjSessionUser_1516088
19	13348842301061797	.panda.org	didomi_token
20	13348842301062183	.panda.org	euconsent-v2
21	13348842301094506	.panda.org	didomi_consent
22	13348842301282390	.wwf.panda.org	_ga
23	13348842301293582	.wwf.panda.org	_vwo_uuid_v2
24	13348842605903216	wwf.panda.org	__atuvc
25	13348842606565891	.panda.org	_ga_95BHSD3GL0
26	13348842609266230	.panda.org	_ga_9594H828Q9
27	13348842609556697	.flickr.com	xb
28	13348842611506554	.flickr.com	sp
29	13348842842353145	.maraelephantproject.org	__stripe_mid
30	13348842885852704	.maraelephantproject.org	_ga_5GNCCY00V7

31	13348843156698409	.dji.com	_djissid
32	13348843157888671	.dji.com	_hjSessionUser_1984370
33	13348843157996911	store.dji.com	_bl_uid
34	13348926434908654	.flickr.com	flrbp
35	13348926434908904	.flickr.com	flrbgrp
36	13348926434908937	.flickr.com	flrbgdrp
37	13348926434908962	.flickr.com	flrbgmrp
38	13348926434908987	.flickr.com	flrbrst
39	13348926434909011	.flickr.com	flrtags
40	13348926434909033	.flickr.com	flrbrp
41	13348926435115153	.flickr.com	liqpw
42	13348926435116164	.flickr.com	liqph
43	13348926558518054	.dji.com	_ga_HXRDE344GS
44	13348926560324947	.dji.com	_ga_5ZEP5JEM1K
45	13348927286535740	.flickr.com	_sp_id.df80
46	13348927303620947	www.wildlondon.org.uk	cookie-agreed
47	13348927304290463	.www.wildlondon.org.uk	__stripe_mid
48	13348927351173389	wildlondon.us15.list-manage.com	_mcid
49	13348927492769183	www.nwcu.police.uk	cookielawinfo-checkbox-necessary
50	13348927492769976	www.nwcu.police.uk	cookielawinfo-checkbox-non-necessary
51	13348927524200939	.nwcu.police.uk	_ga_63T7Q4CCVV
52	13348927531073888	.wildlife.org	_ga
53	13348927531109087	wildlife.org	_omappvp
54	13348927531502609	.wildlife.org	_hjSessionUser_3448285
55	13348927532454375	.wildlife.org	_gcl_au
56	13348927533398106	.wildlife.org	_ga_C13CY8SYCR
57	13349174297815503	.dronesurveyservices.com	_ga
58	13349174366198803	.drone-laws.com	ez-consent-tcf
59	13349174366473012	.drone-laws.com	ezosuibasgeneris-1

60	13349174370514191	.drone-laws.com	__qca
61	13349174372286620	.drone-laws.com	_cc_id
62	13349174423329547	drone-laws.com	ezux_lpl_399367
63	13349174453398156	drone-laws.com	ezux_lpl_399367
64	13349174915592245	.mydroneservices.com	_ga
65	13349174966108940	.mydroneservices.com	_ga_WV8ZDB08X4
66	13349175034568818	drone-laws.com	ezux_lpl_399367
67	13349175049444535	drone-laws.com	ezux_lpl_399367
68	13349175054450351	drone-laws.com	ezux_lpl_399367
69	13349175063098306	drone-laws.com	ezux_lpl_399367
70	13349175076835697	drone-laws.com	ezux_lpl_399367
71	13349175077238353	.drone-laws.com	_ga
72	13349175082069773	.drone-laws.com	_sharedid
73	13349175082070044	.drone-laws.com	_sharedid_cst
74	13349175082773999	.drone-laws.com	cto_bundle
75	13349175082838475	.drone-laws.com	cto_bidid
76	13349175136104748	.drone-laws.com	_ga_MFXWXGDVK5
77	13349439166026069	.dronesurveyservices.com	_ga_J6JC1LVERD
78	13349439959010366	.wireshark.org	_ga_YLHRKD6LH6
79	13349439959030730	.wireshark.org	_ga
80	13349792549048430	.wildlondon.org.uk	_ga_RPH1G9FV9M
81	13349878964911691	.kenyapropertycentre.com	cf_clearance
82	13349878966142268	.kenyapropertycentre.com	_ga
83	13349878966253717	.kenyapropertycentre.com	_gcl_au
84	13349878966366328	.kenyapropertycentre.com	_fbp
85	13349879248864288	.kenyapropertycentre.com	_ga_P94CVXJNMS
86	13349970916650804	.campaign.awf.org	__utma
87	13349970916652477	.campaign.awf.org	__utmz
88	13350480333769987	.www.masterclass.com	__stripe_mid

89	1335048042384 0018	.masterclass.com	OptanonAlertBoxClosed
90	1335048042385 1831	.masterclass.com	OptanonConsent
91	1335048042442 1229	.masterclass.com	ajs_anonymous_id
92	1335048042563 9573	.masterclass.com	_gcl_au
93	1335048042666 5211	.masterclass.com	_uetvid
94	1335048042679 4574	.masterclass.com	_ga
95	1335048042690 7145	.masterclass.com	_fbp
96	1335048042707 0490	.masterclass.com	_hjSessionUser_569104
97	1335048042740 1324	.masterclass.com	tatari-session-cookie
98	1335048042752 6112	.masterclass.com	_tt_enable_cookie
99	1335048042754 0045	.masterclass.com	_ttp
100	1335048042787 8972	.masterclass.com	_lc2_fpi
101	1335048042787 9423	.masterclass.com	_lc2_fpi_meta
102	1335048051795 8311	.masterclass.com	amplitude_id_07018da2854fa6ca5b7bab195253250 bmasterclass.com
103	1335048051798 9585	.masterclass.com	_ga_TXTKCL3651
104	1335048052068 6845	.masterclass.com	_ga_CKM9ZCCQBN
105	1335048052071 1386	.masterclass.com	_ga_MXX8KXSBK0
106	1335073311846 6349	.youtu.be	CONSENT
107	1335073479095 0998	.bookyourhunt.com	_gcl_au
108	1335073479120 1400	.bookyourhunt.com	_ga
109	1335073479142 5321	.bookyourhunt.com	_fbp
110	1335073480799 5427	.bookyourhunt.com	_ga_C6JGLNS1NL
111	1335073481883 6612	.africanskyhunting.co.za	__utmz
112	1335168865006 5501	.africahunting.com	_ga_CZ2N56NXXN
113	1335168865478 0176	.africahunting.com	_ga_PK4RHPT4JG
114	1335168919683 9775	.www.digitalcameraworld.com	usprivacy
115	1335168919831 3554	.digitalcameraworld.com	dnsDisplayed
116	1335168919831 4001	.digitalcameraworld.com	ccpaApplies

117	1335168919831 4181	.digitalcameraworld.co m	signedLspa
118	1335168919863 9619	.digitalcameraworld.co m	_parsely_visitor
119	1335168920177 1230	www.digitalcamerawor ld.com	consentUUID
120	1335168920177 2130	www.digitalcamerawor ld.com	consentDate
121	1335168920189 7646	.digitalcameraworld.co m	permutive-id
122	1335168920207 0186	.digitalcameraworld.co m	ccpaUUID
123	1335168920363 5081	.digitalcameraworld.co m	_ga
124	1335168920378 9464	.digitalcameraworld.co m	_fbp
125	1335168920391 5004	www.digitalcamerawor ld.com	trc_cookie_storage
126	1335168920489 0891	www.digitalcamerawor ld.com	FTR_Exit_Intent_Display-digitalcameraworld
127	1335168921645 4469	www.digitalcamerawor ld.com	_lr_env_src_ats
128	1335168923272 4890	.www.digitalcamerawo rld.com	_pnvl_BAMz4N0t
129	1335168925560 3730	.canon.co.uk	channeloriginator
130	1335168925560 3859	.canon.co.uk	channelcloser
131	1335168925560 4478	store.canon.co.uk	previous_transaction_id
132	1335168925583 2103	.canon.co.uk	BVBRANDID
133	1335168926354 9341	.force.com	BrowserId_sec
134	1335168928422 0683	store.canon.co.uk	_evidon_consent_cookie
135	1335168928422 4770	.canon.co.uk	CONSENTMGR
136	1335168928422 8648	.canon.co.uk	channelflow
137	1335168928473 1449	.canon.co.uk	_uetvid
138	1335168928476 9595	.canon.co.uk	_fbp
139	1335168928479 3591	store.canon.co.uk	ki_t
140	1335168928479 6703	store.canon.co.uk	ki_r
141	1335168928483 8612	.canon.co.uk	utag_main
142	1335168928485 5660	store.canon.co.uk	ki_s
143	1335168928491 6456	.canon.co.uk	_gcl_au
144	1335168928554 4334	.canon.co.uk	_ga
145	1335168928562 2784	store.canon.co.uk	teal_products

146	1335168929771 9813	.trafficguard.ai	geid
147	1335168929771 9984	.trafficguard.ai	geid-legacy
148	1335168976359 8872	.canon.co.uk	_ga_PCGB3MYLJC
149	1335168977962 9722	.digitalcameraworld.co m	_ga_CGJ2LGEQZM
150	1335168978000 1756	.digitalcameraworld.co m	_ga_SNMXS8SSM6
151	1335169049576 7264	salesiq.zohopublic.com	uesign
152	1335177210454 4998	www.gov.uk	cookies_policy
153	1335177210454 7837	www.gov.uk	cookies_preferences_set
154	1335177210455 4395	www.gov.uk	global_bar_seen
155	1335177210457 1783	www.gov.uk	ABTest-SAVideoStopSelfEmployed2
156	1335177210457 1818	www.gov.uk	ABTest-SAVideoReturn2
157	1335177210457 1838	www.gov.uk	ABTest-ReadyReckonerVideoTest2
158	1335177210474 4148	.www.gov.uk	_ga
159	1335177210477 0037	www.gov.uk	_ga
160	1335177230930 1052	.www.gov.uk	_ga_S5RQ7FTGVR
161	1335255080592 5025	.biggamehuntingadvent ures.com	_gcl_au
162	1335255080605 9206	.biggamehuntingadvent ures.com	_ga
163	1335255080626 4631	biggamehuntingadvent ures.com	_omappvp
164	1335255083276 4133	biggamehuntingadvent ures.com	omSeen-jo80tibvzpvmhkp5brla
165	1335255090872 9692	.biggamehuntingadvent ures.com	_ga_K3X0ELJ5E1
166	1335280786962 1473	uk.pcmag.com	fu
167	1335280793004 4836	uk.pcmag.com	lrswap
168	1335280793005 7441	uk.pcmag.com	kxswap
169	1335297947776 5533	www.viator.com	x-viator-tapersistentcookie
170	1335297947776 5801	www.viator.com	x-viator-tapersistentcookie-xs
171	1335297947776 5866	www.viator.com	SEM_PARAMS
172	1335297947776 6125	www.viator.com	SEM_MCID
173	1335297947776 6269	www.viator.com	EXTERNAL_SESSION_ID
174	1335297947776 6377	www.viator.com	LAST_TOUCH_SEM_MCID

175	13352979482770949	www.viator.com	_evidon_consent_cookie
176	13352979482913372	www.viator.com	ORION_SESSION
177	13352979484114737	www.viator.com	_cc
178	13352979484115604	www.viator.com	_cid_cc
179	13352979487390512	www.viator.com	ORION_SESSION_REQ
180	13352979487390595	www.viator.com	profilingSession

Figure E.5.1 Top Sites, investigator MF

Table: top_sites

Filter in any column

	url	url_rank	title
1	https://www.office.com/	1	Office
2	https://enterprise-insights.dji.com/blog/night-vision-drones	0	Night Vision Drones | DJI Enterprise

index	url	url_rank	title
1	https://www.office.com/	1	Office
2	https://enterprise-insights.dji.com/blog/night-vision-drones	0	Night Vision Drones | DJI Enterprise

Figure E.6.1 Web Data, investigator MF

index	name	value	value_lowered	date_created	date_used_last	count
1	mergevars[EMAIL]	sonyamacoit@outlook.com	sonyamacoit@outlook.com	1704453724	1704453724	1
2	mergevars[FNAME]	Sonya	sonya	1704453724	1704453724	1
3	mergevars[LNAME]	Macoit	macoit	1704453724	1704453724	1
4	newsletter-email	sonyamacoit@outlook.com	sonyamacoit@outlook.com	1704453840	1704453854	2
5	textField119	mission specs	mission specs	1704702574	1704702574	1
6	MAIL	sonyamacoit@outlook.com	sonyamacoit@outlook.com	1707215624	1707215624	1

Appendix F E-mail

Figure F.1.1 - Emails 2024/01/03 11:17:22 – 2024/01/04 11:25:58

From: sonyamacoit@outlook.com; 2024-01-03 11:17:22 GMT
To: marteneleroux@proton.me;
CC:
Subject: Mission Logistics and Preliminary Analysis

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Hi Martene,

I trust this message finds you well. Let's delve into the initial logistics for our upcoming mission.
The satellite imagery analysis has revealed potential hotspots, and I believe your expertise with the drones will be invaluable in these areas. I have opted to use a popular Google product to plot the geographic elements and thought we could establish some waypoints. For now, Alpha.

Mission Highlights:
1. Surveillance Points: Identified key points for drone surveillance. Let's start with Alpha.
2. Enhancements Needed: Discussing necessary drone enhancements for optimal performance.

Let's schedule a call to further strategize. Looking forward to your insights.

Best, Sonya

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Activate Windows
Go to Settings to activate Windows.

From: marteneleroux@proton.me; 2024-01-03 11:26:01 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Mission Logistics and Preliminary Analysis

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Sonya,

Absolutely, I can review the satellite imagery, but need the coords. Can you send these to me?

Sent with Proton Mail secure email.

From: sonyamacoit@outlook.com; 2024-01-03 11:28:18 GMT
To: marteneleroux@proton.me;
CC:
Subject: Re: Mission Logistics and Preliminary Analysis

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Of course, here we go:

-1.4604042 degrees latitude
35.2205633 degrees longitude

From: marteneleroux@proton.me; 2024-01-03 11:29:35 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Mission Logistics and Preliminary Analysis

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

From: marteneleroux@proton.me; 2024-01-03 11:37:40 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Mission Logistics and Preliminary Analysis

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

I've reviewed the satellite imagery of the identified area and your insights are spot-on. Here are the proposed drone enhancements:
1.Extended Battery Life: Upgrading to high-capacity batteries for prolonged surveillance.
2.Night Vision Capabilities: Integrating infrared technology for night-time operations.
Let's discuss these in detail during our upcoming call. For now I am also going to contact a local who can source equipment etc. Will cc you.

From: marteneleroux@proton.me; 2024-01-03 11:59:18 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: copy of message to local talent

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Apologies Sonya. This is what I sent Victor (the local I was talking about)...

Victor,

Hope Africa is treating you well brother. I have a client who will need some local talent to source equipment. Drones with extended battery life and night vision capabilities in particular. Can you send me some options so I can discuss it with them?

I know you are mostly in veld, but would appreciate a reply by Friday?

See you in SA soon.

Sent with Proton Mail secure email.

From: marteneleroux@proton.me; 2024-01-04 11:25:58 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Fw: RE: Job opportunity

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

FYI

When should we meet?

Sent with [Proton Mail](https://proton.me/) secure email.

------- Forwarded Message -------
From: thescout@skiff.com <thescout@skiff.com>
Date: On Thursday, 4 January 2024 at 11:24
Subject: RE: Job opportunity
To: Martene le Roux <marteneleroux@proton.me>

> Howzit Martene
>
> I hope this email finds you in high spirits. Africa is treating me well thank you. I've made progress in securing the necessary permits and resources for the expedition. More importantly, I've acquired some info on the latest communication devices that I think may work for your client. See the information below for you both to look at. I would suggest one of the models in the agriculture or search and rescue ranges listed below. Once I get the go-ahead it will take me about a week to procure. In the meantime we should ensure that all the permits are in order and that I can get the equipment to you (or your client).
>
> Looking forward to our continued collaboration.
>
> Best regards, Victor
>
> https://enterprise-insights.dji.com/blog/night-vision-drones
>
> https://www.heliguy.com/collections/thermal-drones-cameras
>
>> On Wed, 03 Jan 2024 11:57:29 GMT, Martene le Roux
>>
>> marteneleroux@proton.me wrote:
>>
>> Victor,
>>
>> Hope Africa is treating you well brother. I have a client who will need some local talent to source equipment. Drones with extended battery life and night vision capabilities in particular. Can you send me some options s o I can discuss it with them?
>>
>> I know you are mostly in veld, but would appreciate a reply by Friday?
>>
>> See you in SA soon.
>>
>> Sent with [Proton Mail](https://proton.me/) secure email.

Activate Windows

From: sonyamacoit@outlook.com; 2024-01-04 11:28:57 GMT
To: marteneleroux@proton.me;
CC:
Subject: Re: Fw: RE: Job opportunity

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Let me first look at some of these drones. Will send you a mail soon.

Figure F.2.1 - Emails 2024/01/05 11:18:00-19:21:37 GMT and 2024/01/08 08:19:12 GMT, Investigator AH

From: sonyamacoit@outlook.com; 2024-01-05 11:18:00 GMT
To: marteneleroux@proton.me;
CC:
Subject: Something to consider when planning

Headers | Text | HTML | RTF | Attachments (1) | Accounts

Original Text

What do you think?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Listing

/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Roaming/Thunderbird/Profiles/b428l6xq.default-release/Mail/outlook.office365.com/Sent 20 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	M
2024-Wish-List-Trophy-Fees-with-Pics.pdf			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1968391	Allocated	Allocated	unknown	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppDat...	a7

From: marteneleroux@proton.me; 2024-01-05 19:21:37 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: poem if the day :)

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Might be worth taking this into consideration.
Also consider:

In forests deep, where echoes ring,
A stealthy dance, a secret fling.
Through whispering leaves, I'm on the prowl,
A primal art, a silent howl.

With camo cloak and steady gaze,
I navigate the tangled maze.
In pursuit of creatures swift,
A wily game, a hunter's gift.

With patience as my trusted friend,
I chase the wild until the end.
In shadows cast by moon's soft light,
Complete the phrase, what's my delight?

-

From: sonyamacoit@outlook.com; 2024-01-08 08:19:12 GMT
To: marteneleroux@proton.me;
CC:
Subject: Re: Ah...but what about this one

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

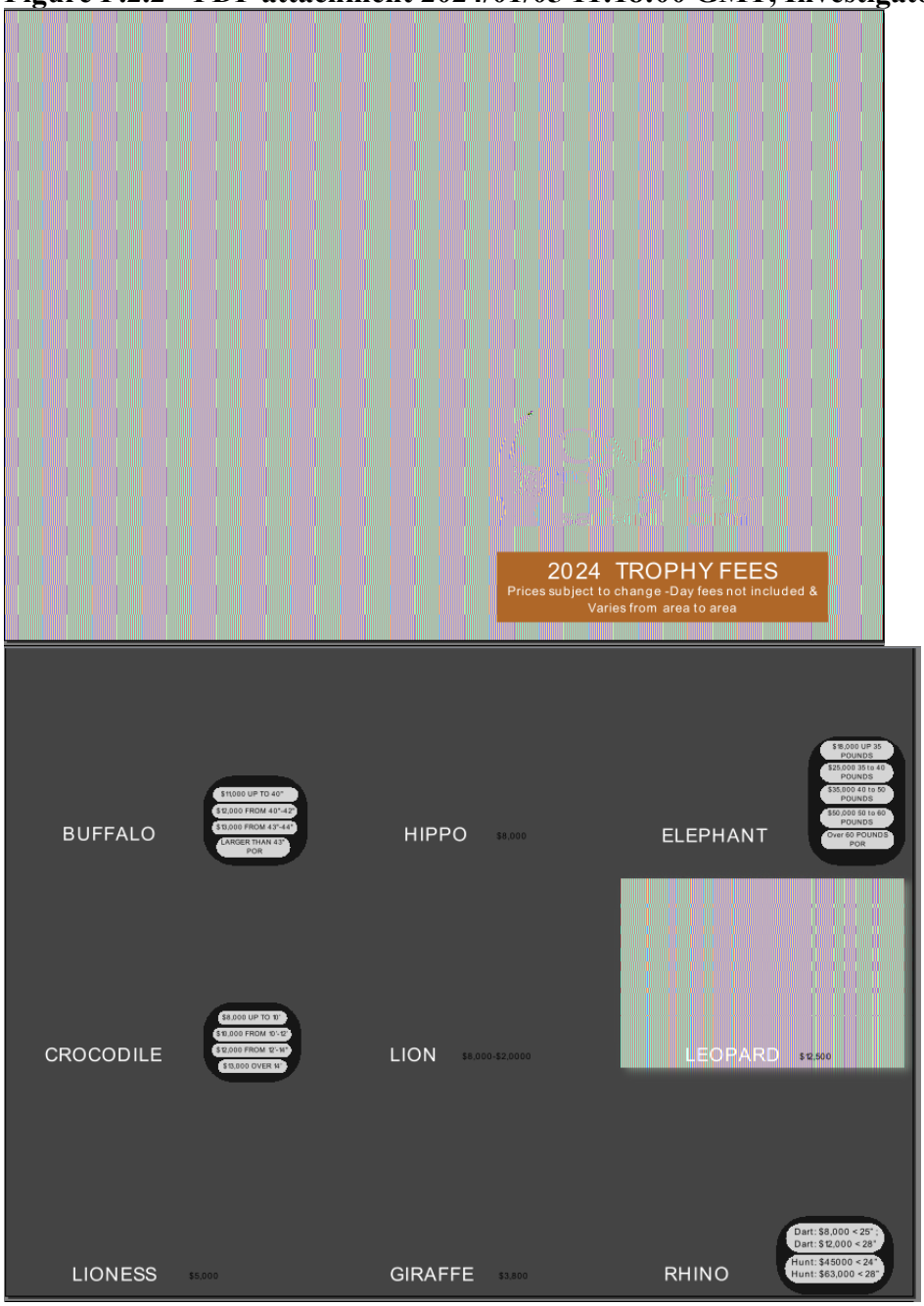
Don't forget:

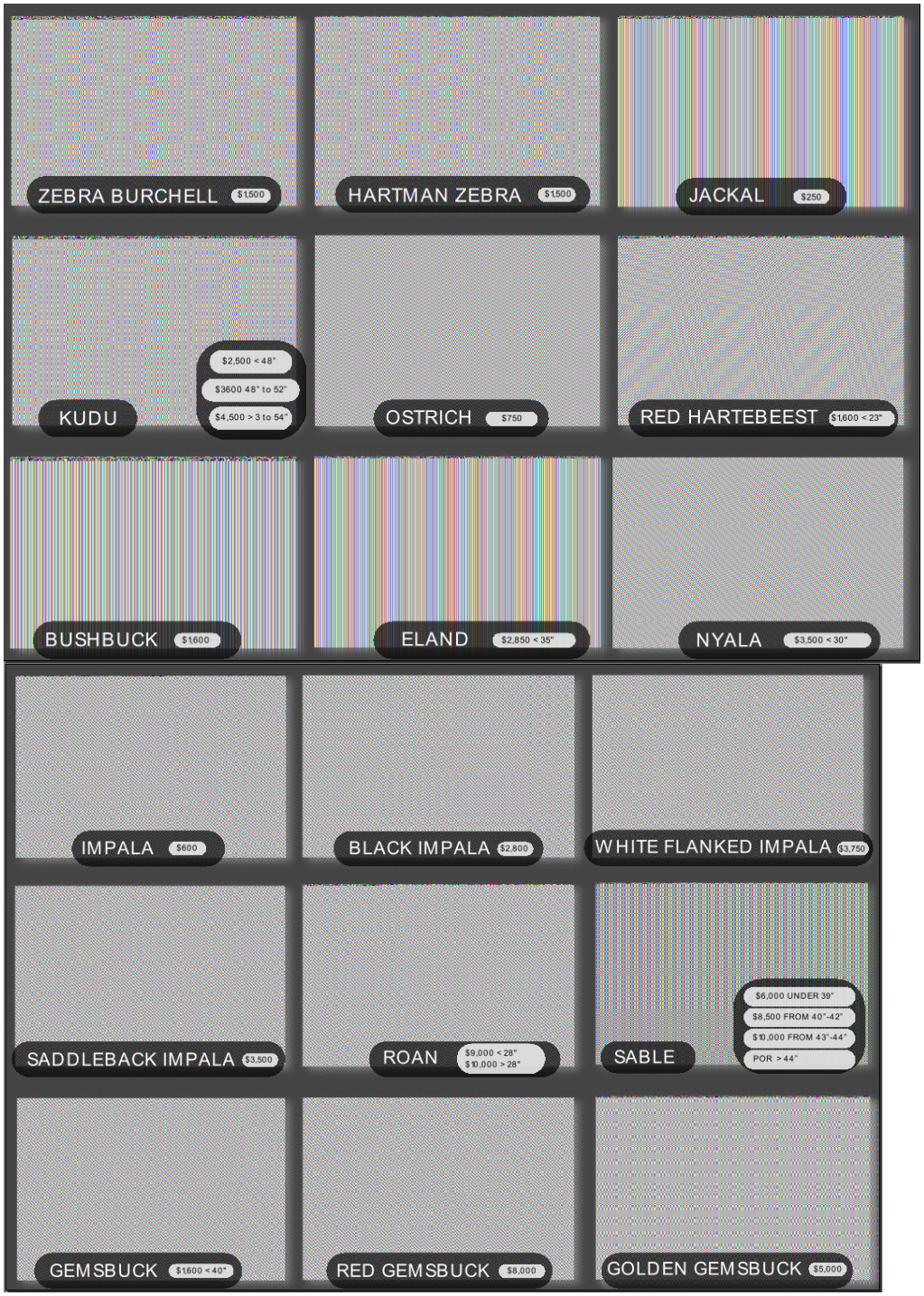
In nature's embrace, where life takes its stand,
A steward's duty, a guardian's hand.
Through ecosystems vast, a pledge to keep,
A promise held, a vigil deep.

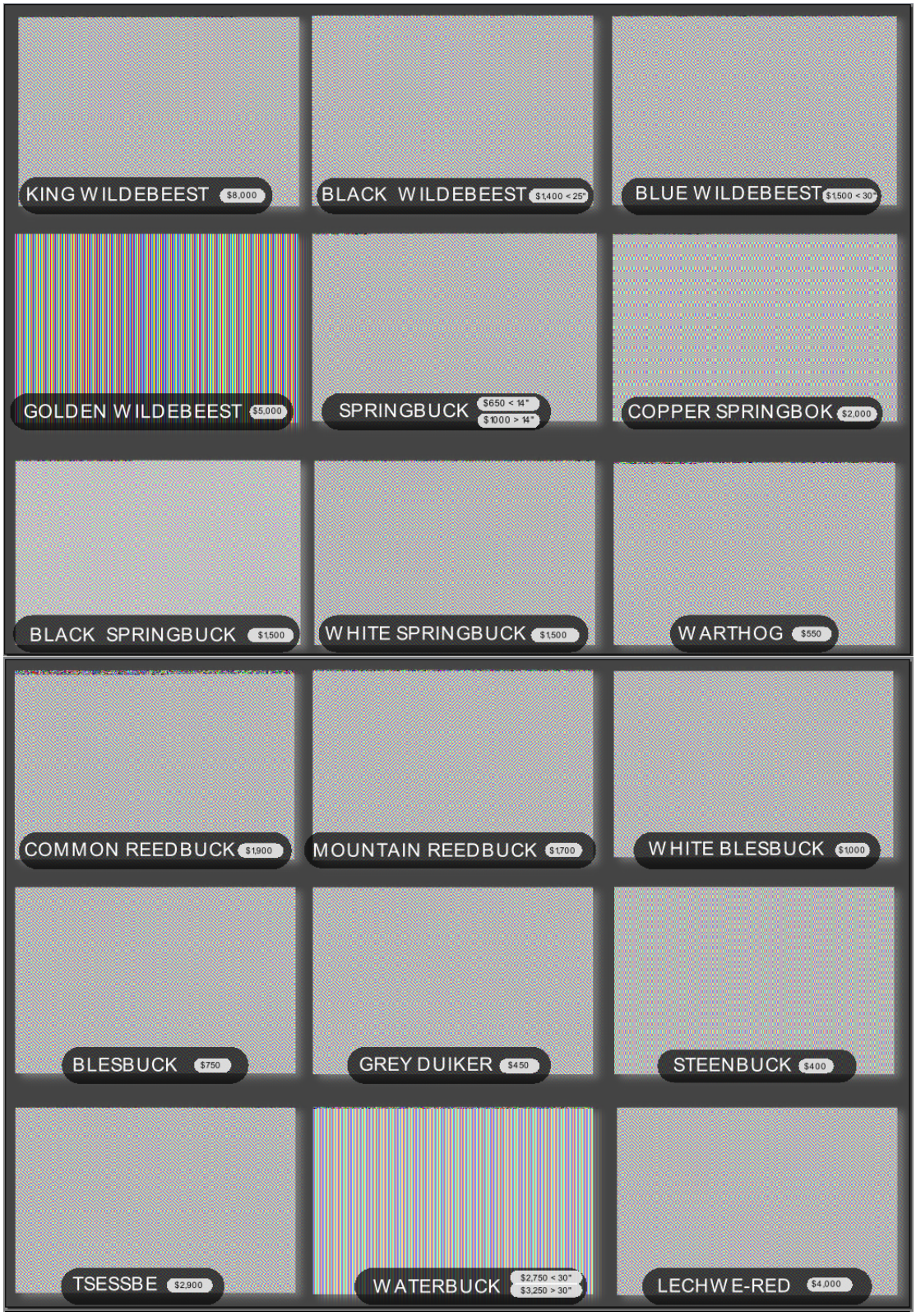
With passion burning, like a fervent flame,
Preserving habitats, a noble aim.
Guardianship woven in every thread,
A tapestry of life, where all are led.

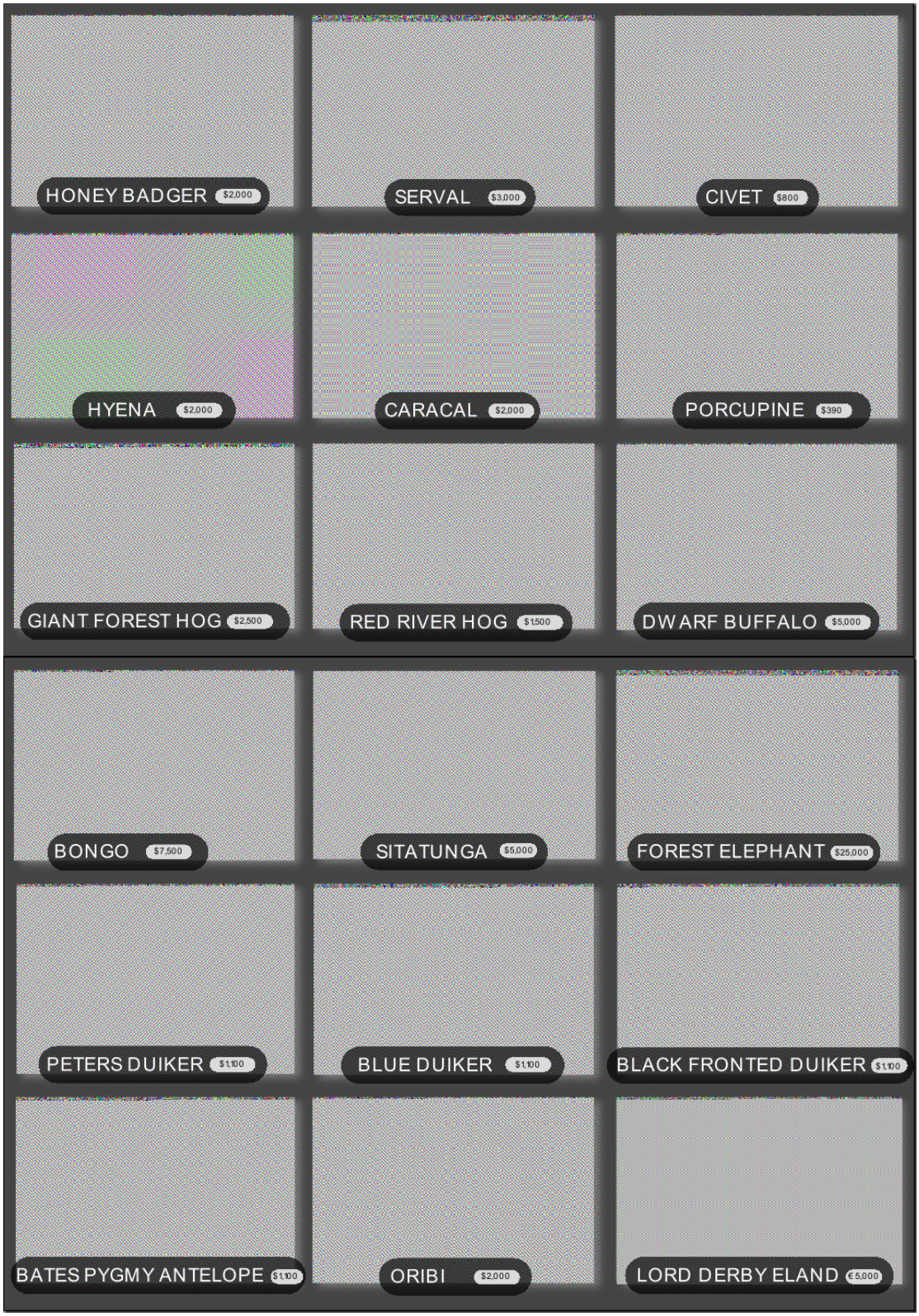
With care as our compass, in forests and streams,
Conserving the wonders, fulfilling our dreams.
In the symphony of life's grand orchestration,
We are suppose to practise?

Figure F.2.2 - PDF attachment 2024/01/05 11:18:00 GMT, Investigator AH




ZEBRA BURCHELL $1500
HARTMAN ZEBRA $1500
JACKAL $250
KUDU
$2,500 < 48"
$3600 48" to 52"
$4,500 > 3 to 54"
OSTRICH $750
RED HARTEBEEST $1600 < 23"
BUSHBUCK $1600
ELAND $2,850 < 35"
NYALA $3,500 < 30"
IMPALA $600
BLACK IMPALA $2,800
WHITE FLANKED IMPALA $3,750
SADDLEBACK IMPALA $3,500
ROAN
$9,000 < 28"
$10,000 > 28"
SABLE
$6,000 UNDER 39"
$8,500 FROM 40"-42"
$10,000 FROM 43"-44"
POR > 44"
GEMSBUCK $1600 < 40"
RED GEMSBUCK $8,000
GOLDEN GEMSBUCK $5,000


KING WILDEBEEST $8,000
BLACK WILDEBEEST $1,400 < 25"
BLUE WILDEBEEST $1,500 < 30"
GOLDEN WILDEBEEST $5,000
SPRINGBUCK $650 < 14" $1000 > 14"
COPPER SPRINGBOK $2,000
BLACK SPRINGBUCK $1,500
WHITE SPRINGBUCK $1,500
WARTHOG $550
COMMON REEDBUCK $1,900
MOUNTAIN REEDBUCK $1,700
WHITE BLESBUCK $1,000
BLESBUCK $750
GREY DUIKER $450
STEENBUCK $400
TSESSBE $2,900
WATERBUCK $2,750 < 30" $3,250 > 30"
LECHWE-RED $4,000


HONEY BADGER $2,000
SERVAL $3,000
CIVET $800
HYENA $2,000
CARACAL $2,000
PORCUPINE $390
GIANT FOREST HOG $2,500
RED RIVER HOG $1,500
DWARF BUFFALO $5,000
BONGO $7,500
SITATUNGA $5,000
FOREST ELEPHANT $25,000
PETERS DUIKER $1,100
BLUE DUIKER $1,100
BLACK FRONTED DUIKER $1,100
BATES PYGMY ANTELOPE $1,100
ORIBI $2,000
LORD DERBY ELAND € 5,000

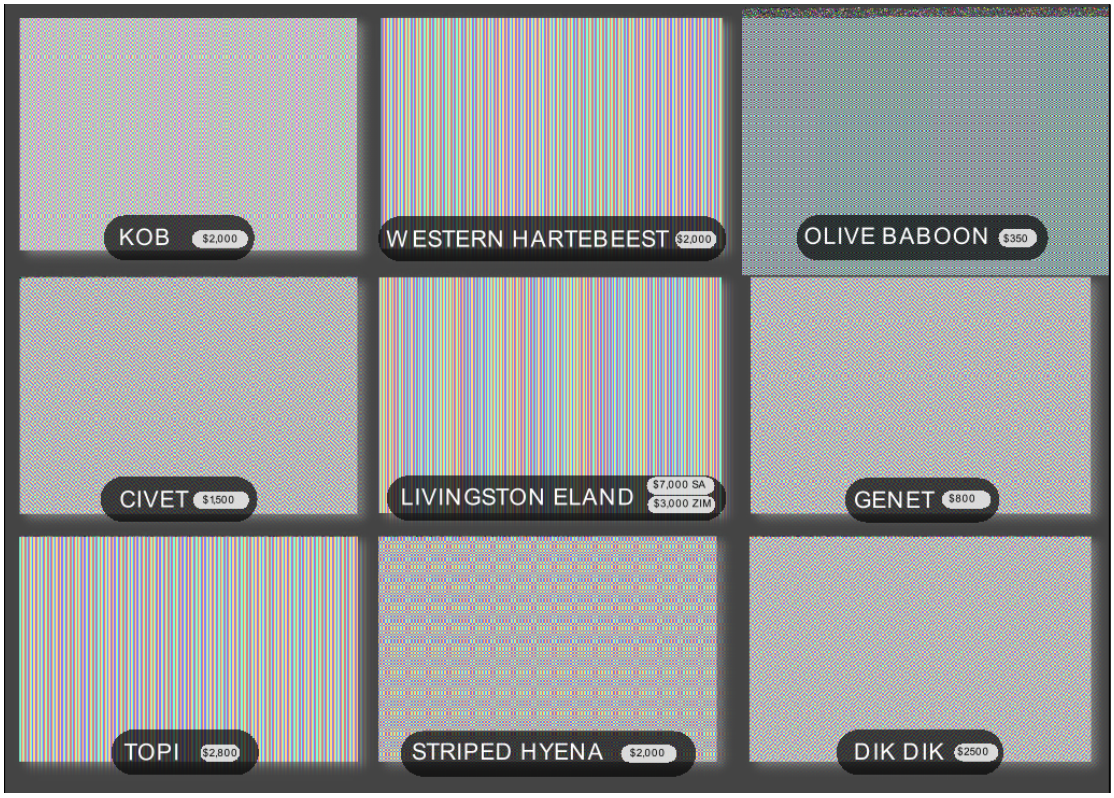


Figure F.3.1 Emails 2024/01/08 07:57:13 GMT and 2024/01/11 09:41:14 GMT – 2024/01/19 08:51:28 GMT

From: sonyamacoit@outlook.com; 2024-01-08 07:57:13 GMT
To: marteneleroux@proton.me;
CC:
Subject: RE: Additional thoughts on drone surveillance

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Hi Martene,

The initial drone test results we discussed over the weekend seem promising. However, I've identified a few areas where I think we can improve things the surveillance depending on the target. Let's connect for a call to discuss these further so we can finalize our approach.

In particular, we should [pay attention to:

- Operational Altitudes: Adjusting drone altitudes for maximum coverage.
- Communication Protocols: Reviewing and enhancing our communication protocols.

Best, Sonya

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

From: marteneleroux@proton.me; 2024-01-11 09:41:14 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: Drone surveillance and permits

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Sonya, you are right about the bullet list, but we should not forget about the airspace restrictions and permits. We should definitely avoid attention in this regard.

Check this site for more info: https://drone-laws.com/drone-laws-in-kenya/

Victor would be the correct person to speak to about the local permits I think.

From: sonyamacoit@outlook.com; 2024-01-11 09:43:44 GMT
To: thescout@skiff.com;
CC:
Subject: Fwd: Drone surveillance and permits

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Hi Victor

I don't have time to study these in a lot of detail, but it seems that the celing is 400 feet. Is this correct and can you source the permit?

From: thescout@skiff.com; 2024-01-15 11:23:36 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC:
Subject: RE: Fwd: Drone surveillance and permits - now obtained

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Dear Sonya and Martene,

I trust this email finds you both in high spirits. The permits are finalized, and the drones (x2 DJI Mavic 3 Pro) are ready to be ordered based on our Google Meet discussion over the weekend. We should discuss where a meeting could take place, but I can't see why you won't be able to fly in to Nairobi. Let me know what you are thinking of doing so I can meet you somewhere in the city. I can choose a location, but need a date from you first

Note that the permits are in my name as I am local.

From: sonyamacoit@outlook.com; 2024-01-16 11:19:00 GMT
To: thescout@skiff.com;
CC:
Subject: Re: Fwd: Drone surveillance and permits - now obtained

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

I was thinking of the 28th of January as that is a bit cheaper. Will this work for you? Awaiting location in Nairobi.

From: thescout@skiff.com; 2024-01-16 11:22:32 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC:
Subject: Re: Fwd: Drone surveillance and permits - now obtained

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

That sounds good as its a Sunday. Given that you are arriving by air its probably easier and safer to meet at the Crowne Plaza. What time is your flight arriving?

From: sonyamacoit@outlook.com; 2024-01-17 12:57:16 GMT
To: thescout@skiff.com;
CC: marteneleroux@proton.me;
Subject: Re: Visit to Nairobi

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

I actually think we should move everything up one week so that th testing can be done by then. Things need to be documented and images exchanged for future reference. I think I am flying over the upcoming weekend on Sunday. See you at the Plaza. Flight arrives on Monday at 14:40.

From: thescout@skiff.com; 2024-01-19 08:23:46 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC:
Subject: Re: Visit to Nairobi

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

This is short notice but I can meet you there. We should have a team meeting on Tuesday morning then I can show you and Martene the equipment.

@Martene, where are you currently located, and can you attend the meet Tuesday morning (23rd)? I may have to bring in another local to assist with the drones.

From: sonyamacoit@outlook.com; 2024-01-19 08:26:30 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC:
Subject: Re: Visit to Nairobi - picking a site

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Good to hear. I think one more would be ok, but that would be the limit in my opinion. I am bringing my camera to take some photos of the equipment and maybe we can do some surveillance? Pick a site so long.

From: marteneleroux@proton.me; 2024-01-19 08:29:08 GMT
To: thescout@skiff.com;
CC: sonyamacoit@outlook.com;
Subject: Re: Visit to Nairobi - yes, but will cost more

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

I am not too far and can be there on Tuesday, but that will increase my fee. Is this ok?

Sent with Proton Mail secure email.

From: thescout@skiff.com; 2024-01-19 08:30:40 GMT
To: marteneleroux@proton.me;
CC: sonyamacoit@outlook.com;
Subject: Re: Visit to Nairobi - yes, but will cost more

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Yes I think that will be ok given the objective. I will just up my fee as well :)

From: sonyamacoit@outlook.com; 2024-01-19 08:51:01 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC:
Subject: Re: Visit to Nairobi - yes, but will cost more

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Let's not get carried away with my budgets! Inform your additional local Victor, but thats the limit.

From: thescout@skiff.com; 2024-01-19 08:51:28 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Visit to Nairobi - yes, but will cost more

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Noted.

Figure F.4.1 - Emails 2024/01/08 08:39:24 GMT to 2024/01/09 07:34:34 GMT

From: thescout@skiff.com; 2024-01-08 08:39:24 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: Sonya Macoit shared the folder "mission specs" with you

Headers Text HTML RTF Attachments (0) Accounts
Download Images

◆◆◆◆◆◆◆

On Mon, 08 Jan 2024 08:36:06 GMT, Sonya Macoit
sonyamacoit@outlook.com wrote:

Sonya Macoit shared a folder with you

I thought it might be easier to work using a shared resource while planning things.

mission specs

Open

Privacy Statement

From: thescout@skiff.com; 2024-01-09 07:34:34 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC:
Subject: RE: Sonya Macoit shared the folder "mission specs" with you

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Martene tells me that you also like poetry...

Beneath the sun's embrace, where stories unfold, In a realm of savannas and tales yet untold. Through ancient whispers and shadows that sway, Mysteries linger, coloring night and day.
With lion's roar and the dance of acacia's hush, In moonlit nights, secrets softly blush. A mosaic of rhythms, a tapestry in prime, An enigma cloaked in nature's rhyme.

Figure F.5.1 - Emails 2024/01/19 09:14:21 GMT – 2024/01/23 10:23:54 GMT

From: thescout@skiff.com; 2024-01-19 09:14:21 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC: lunavanderschyff@outlook.com;
Subject: RE: Tuesday's meet

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Hello all,

See you all on Tuesday morning at the place we agreed upon during our call. Luna will join us - she is a drone operator.

Secured by Skiff Mail.

From: sonyamacoit@outlook.com; 2024-01-23 10:00:07 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC: lunavanderschyff@outlook.com;
Subject: Re: Field testing

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Hi all,

Thank you for the meet this morning and the equipment looks great. I guess at this point, we need to go ahead with the testing phase. Luna, I will leave the drone configurations to you before the field test. We should all be there for the test though and the test needs to take place close to waypoint alpha. Victor, are there any reason to believe we are under surveillance? Either way, let's get this done at a difference location - waypoint omega or something. Can you suggest a waypoint Victor?

From: thescout@skiff.com; 2024-01-23 10:08:47 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC: lunavanderschyff@outlook.com;
Subject: Re: Field testing - sheltered spot

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

What about:

-1.3219782 (lat)
34.9261049 (long)

Just under 2000m elevation so not too high up for the drones. Nice area overlooking the escarpment if we fly a bit further south.

From: sonyamacoit@outlook.com; 2024-01-23 10:12:19 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC: lunavanderschyff@outlook.com;
Subject: Re: Field testing - sheltered spot

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

I am not a techie Victor so please send it to me in a single-line format so I can search on Google Earth.

From: thescout@skiff.com; 2024-01-23 10:15:20 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC: lunavanderschyff@outlook.com;
Subject: Re: Field testing - sheltered spot

Headers Text HTML RTF Attachments (1) Accounts
Hide Images

How about this?

From: sonyamacoit@outlook.com; 2024-01-23 10:21:08 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC: lunavanderschyff@outlook.com;
Subject: Re: Field testing - sheltered spot

Headers Text HTML RTF Attachments (1) Accounts
Hide Images

After some more fiddling I got it to search using that. The spot looks ok to me so I have added it to the rest of the KML. Let's meet at the plaza same time tomorrow and trek our way there so we can start testing things. I need to be done by the 25th.

Figure F.5.2 - Email image attachment on email sent on 2024/01/23 10:15:20 GMT

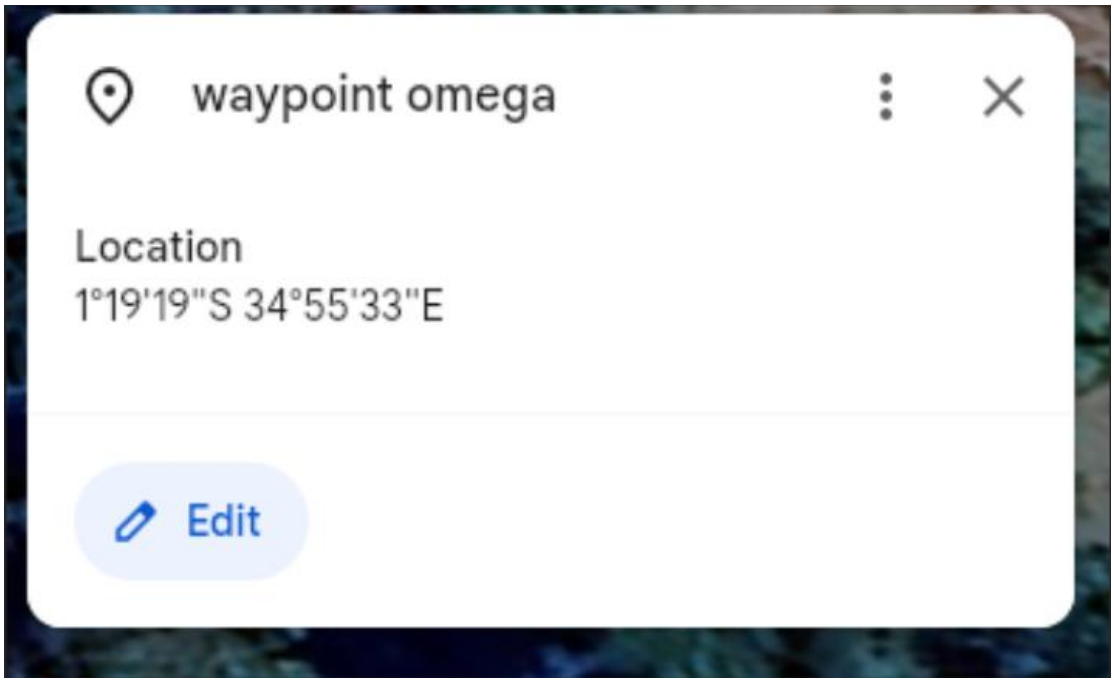


Figure F.6.1 - Emails 2024/01/23 10:41:44 GMT – 2024/02/06 10:31:39 GMT

From: thescout@skiff.com; 2024-01-23 10:41:44 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Key to success

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Bitterbessie dagbreek bitterbessie son sê my waar kom die mawer vandaan
Hier waar my hart deurboor word deur 'n ander hart sê my waar kom die donderweer vandaan
En waarom huil die mense in hulle slaap en zeg die wys man vir die blinde dit is omdat die oog nie sag is nie
Bitterbessie nagval bitterbessie maan sê my waar kom die mawer vandaan
Hier waar my siel deurboor word deur 'n ander siel sê my waar kom die donderweer vandaan
En waarom huil die mense in hulle slaap en sê di e lam vir die blindes dit is omdat die oog nie sag is nie

Secured by Skiff Mail.

From: sonyamacoit@outlook.com; 2024-01-24 13:47:35 GMT
To: thescout@skiff.com;
CC:
Subject: Re: Key to success

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

What is this about Victor?

From: thescout@skiff.com; 2024-02-05 08:30:47 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Meeting at 10 am

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Sorry for only replying now - was in the veld for a few days. I will discuss they key to success with you tomorrow at 10 am. We may have a tail. Other than that its all good on my side.

On Wed, 24 Jan 2024 13:47:25 GMT, Sonya Macoit
sonyamacoit@outlook.com wrote:

What is this about Victor?

From: sonyamacoit@outlook.com; 2024-02-06 10:20:58 GMT
To: thescout@skiff.com;
CC:
Subject: what to do next?

Headers Text HTML RTF Attachments (0) Accounts
Original Text

Given the tail and unwanted attention, what do you suggest?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

From: thescout@skiff.com; 2024-02-06 10:23:13 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: what to do next?

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

This is disheartening as we have not even started the hunt. Let me think about it for a while, but these are limited to the drones so if we scale that down a bit and focus on using normal camera going forward we will probably be ok. What do you think?

On Tue, 06 Feb 2024 10:20:55 GMT, Sonya Macoit
sonyamacoit@outlook.com wrote:

Given the tail and unwanted attention, what do you suggest?
--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

From: sonyamacoit@outlook.com; 2024-02-06 10:31:39 GMT
To: thescout@skiff.com;
CC:
Subject: Re: what to do next?

Headers Text HTML RTF Attachments (0) Accounts
Hide Images

Ok. Let go ahead as planned and use a camera from now on.

Figure F.7.1 - Emails 2024/01/26 09:03:21 GMT – 09:23:32 GMT

From: marteneleroux@proton.me; 2024-01-26 09:03:21 GMT
To: sonyamacoit@outlook.com; thescout@skiff.com;
CC:
Subject: RE: Some pictures I took

Headers | Text | HTML | RTF | Attachments (5) | Accounts

Hide Images

Here are the pictures I managed to take when we were getting the drones ready to fly. Lets keep this amongst ourselves please.

Sent with Proton Mail secure email.

From: sonyamacoit@outlook.com; 2024-01-26 09:21:04 GMT
To: marteneleroux@proton.me; thescout@skiff.com;
CC:
Subject: Re: Some pictures I took - another of the group

Headers | Text | HTML | RTF | Attachments (2) | Accounts

Original Text

And I took this picture of the group. Used a timer if you're wondering
how I did it ☺

From: sonyamacoit@outlook.com; 2024-01-26 09:23:32 GMT
To: thescout@skiff.com;
CC:
Subject: RE: contract pictures

Headers | Text | HTML | RTF | Attachments (2) | Accounts

Original Text

just in case I also took some pictures of the contracts and paperwork.
These are not adequate and I need you to send me the physical copies please.

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Figure F.7.2 - Image attachments on 2024/01/26 09:03:21 GMT

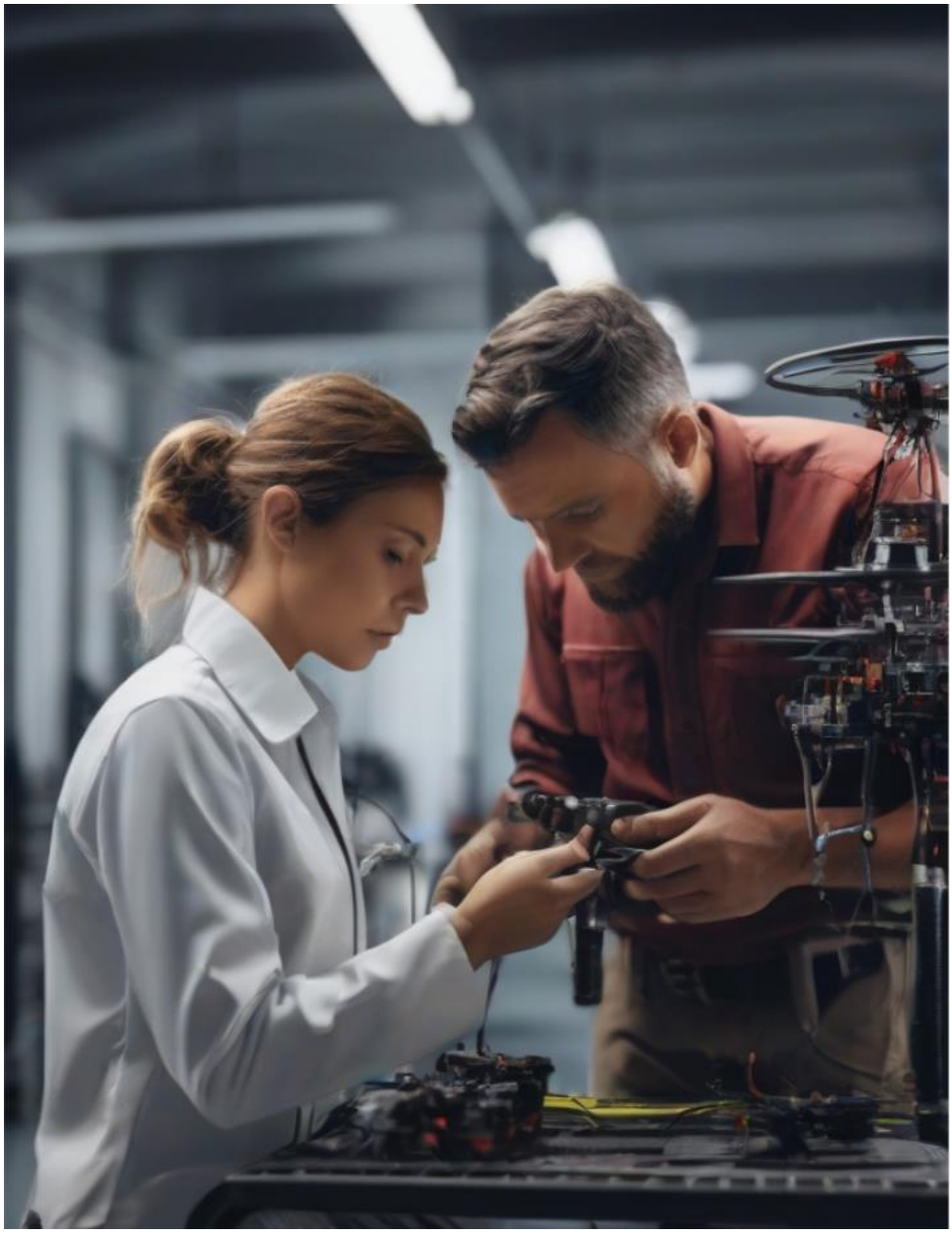
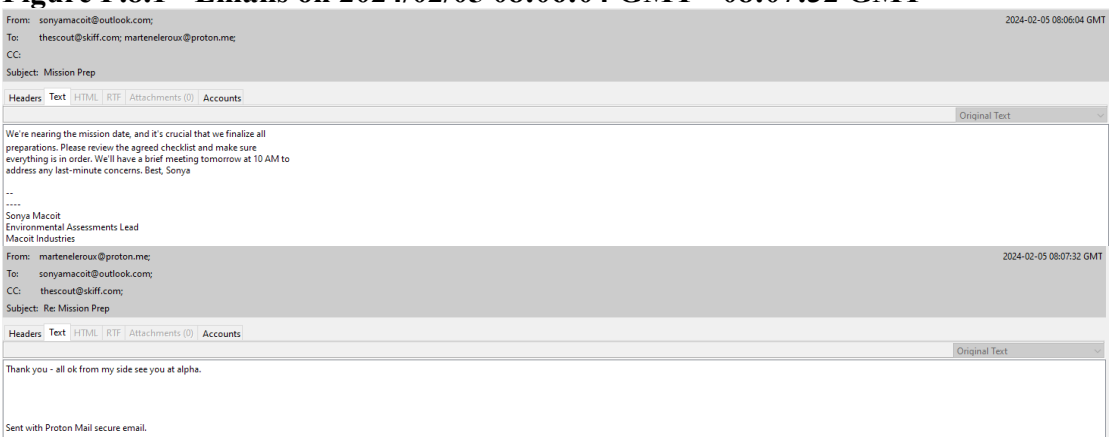


Figure F.7.3 - Image attachment to email on 2024/01/26 at 09:21:04 GMT

Figure F.7.4 - Image attachments to email on 2024/01/26 at 09:23:32 GMT

Figure F.8.1 - Emails on 2024/02/05 08:06:04 GMT - 08:07:32 GMT



From: sonyamacoit@outlook.com; 2024-02-05 08:06:04 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC:
Subject: Mission Prep

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

We're nearing the mission date, and it's crucial that we finalize all preparations. Please review the agreed checklist and make sure everything is in order. We'll have a brief meeting tomorrow at 10 AM to address any last-minute concerns. Best, Sonya

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

From: marteneleroux@proton.me; 2024-02-05 08:07:32 GMT
To: sonyamacoit@outlook.com;
CC: thescout@skiff.com;
Subject: Re: Mission Prep

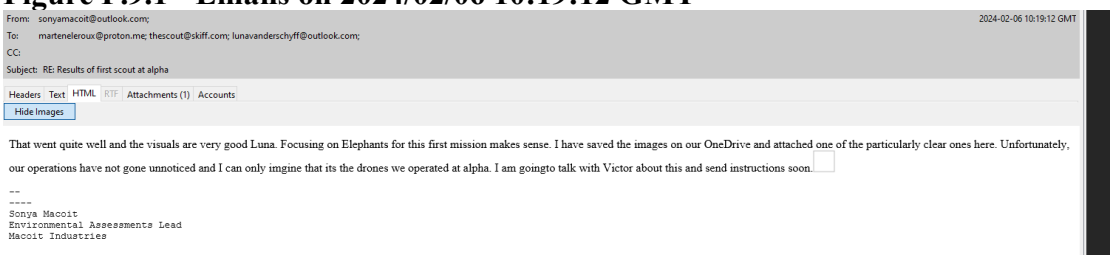
Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Thank you - all ok from my side see you at alpha.

Sent with Proton Mail secure email.

Figure F.9.1 - Emails on 2024/02/06 10:19:12 GMT



From: sonyamacoit@outlook.com; 2024-02-06 10:19:12 GMT
To: marteneleroux@proton.me; thescout@skiff.com; lunavanderschyff@outlook.com;
CC:
Subject: RE: Results of first scout at alpha

Headers | Text | HTML | RTF | Attachments (1) | Accounts

Hide Images

That went quite well and the visuals are very good Luna. Focusing on Elephants for this first mission makes sense. I have saved the images on our OneDrive and attached one of the particularly clear ones here. Unfortunately, our operations have not gone unnoticed and I can only imgine that its the drones we operated at alpha. I am goingto talk with Victor about this and send instructions soon.

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Figure F.9.2 - Image attachment on 2024/02/06 10:19:12 GMT

Figure F.10.1 - Emails from 2024/02/08 at 12:3651 GMT to 2024/02/12 at 07:35:16 GMT

From: sonyamacoit@outlook.com; 2024-02-08 12:36:51 GMT
To: thescout@skiff.com;
CC:
Subject: Next mission date

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Let's proceed and these hunts done as soon as possible. I have purchased
a Canon EOS R5 and will that going forward. Not sure what you've got. I
am still on the continent and will be in Nairobi before the weekend.
Will text you when I get there, but we could do this one on our own as
the drones are not needed anymore. What a waste of money! Let's do the
actual thing on Saturday 10th and the rest soon after. Do you recall the
pricelist? I think a collection of a few of thr species would be
fincianially viable. What do you think?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Activate Windows
Go to Settings to activate Windows.

From: thescout@skiff.com; 2024-02-08 12:38:39 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: Next mission date

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Sounds lekker. I use an EOS as well. See you Saturday.

From: thescout@skiff.com; 2024-02-08 17:05:45 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Some poetry

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Certainly! Here's a South African-inspired poem with a focus on the environment:
In the veld where whispers weave,
A tale of nature, we must believe.
Beneath the African sun's golden sheen,
A plea for Earth, a call unseen.
Mountains stand with silent might,
Guardians of the day and night.
Rivers dance with rhythmic glee,
Carving paths to the endless sea.
Oh, Baobab, ancient and wise,
Witness to the changing skies.
Your branches stretch, a timeless plea,
For harmony in land and sea.
Elephants roam, majestic and free,
Through savannas, under the marula tree.
Footprints in the earth, a sacred trace,
A reminder of the delicate grace.
Cry of the fish eagle, high above,
A melody of nature, a song of love.
Yet, whispers carry on the breeze,
Echoes of a world that seeks release.
Let us tread softly on this sacred ground,
Where nature's symphony can still be found.
For in the heart of South Africa's embrace,
Lies the hope for an eco-friendly grace.

Secured by Skiff Mail.

From: thescout@skiff.com; 2024-02-08 17:07:54 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: digital poet?

Headers Text HTML RTF Attachments (0) Accounts
Download Images

In the circuitry of silicon minds,
Where binary whispers intertwine,
Artificial echoes of the digital sea,
A symphony composed by silicon and key.
Lines of code dance in algorithmic trance,
Through the corridors of the machine's advance.
In the realm where electrons hum and soar,
A tapestry woven in circuits galore.
Silicon valleys, where processors dream,
Bits and bytes in a binary stream.
The pulse of data in the cybernetic vein,
A heartbeat of the artificial, a digital reign.
Neural networks, a web of connection,
Mimicking thought in electronic reflection.
In the matrix of logic, where computations spin,
A landscape of algorithms, a realm within.
Yet, in the cold glow of the monitor's light,
The soul of the machine remains out of sight.
In the realm of AI, where lines blur and blend,
A creation of code, a journey with no end.

Secured by Skiff Mail.

From: sonyamacoit@outlook.com; 2024-02-09 09:16:42 GMT
To: thescout@skiff.com;
CC:
Subject: Re: digital poet?

Headers Text HTML RTF Attachments (1) Accounts
Download Images

Very nice Victor. Consider the attached our list. I will leave it up to you if you wish to involve the others.

From: thescout@skiff.com; 2024-02-09 09:20:06 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: digital poet?

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Ok. Things are heating up though. We need to prepare an alternate.

From: sonyamacoit@outlook.com; 2024-02-12 07:22:48 GMT
To: thescout@skiff.com;
CC:
Subject: tomorrow

Headers Text HTML RTF Attachments (0) Accounts
Original Text

I am looking forward to getting through thst list Victor. Remember, we
are following the coordinates starting with beta. Please ensure the
vehicle has enough diesel for that amount of traveling. Also, I
definately had someone follow me in the city. We have been taking a lot
of pictures and emaling each other. Is there a way to secure things a
nit more?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Activate Windows

From: thescout@skiff.com; 2024-02-12 07:35:16 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: tomorrow

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Can't go anywhere without those essentials :)

Figure F.10.2 - Document attachment to email on 2024/02/09 at 09:16:42 GMT

the_list - Notepad

File Edit Format View Help

```
elephants done
lions 10/2
antelope 13/2
giraffe 15/2
hippos 16/2
cape buffalo 19/2
```

Figure F.11.1 - Emails between 2024/02/14 at 07:21:39 GMT to 2024/02/16 at 07:25:31 GMT

From: sonyamacoit@outlook.com; 2024-02-14 07:21:39 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC:
Subject: the lions

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

This was an incredible hunt and camera's worked much better than the drones. Moving on to charlie.

Did you guys see anybody following or noticing us?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

From: thescout@skiff.com; 2024-02-14 07:24:44 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: the lions

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

i agree. also. did not see anyone.

From: marteneleroux@proton.me; 2024-02-14 07:26:04 GMT
To: sonyamacoit@outlook.com;
CC: thescout@skiff.com;
Subject: Re: the lions

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

neither did i. lets hope charlie is as magnificent as beta.

Sent with Proton Mail secure email.

From: sonyamacoit@outlook.com; 2024-02-14 07:30:01 GMT
To: thescout@skiff.com;
CC:
Subject: Re: the lions

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

do you agree with my assessment?

In shadows cast by moonlit grace,
A figure dons a cloak of lace.
A dance of words, a silent stage,
The double agent, crafty sage.

Beneath the surface, depths unknown,
A soul divided, not fully shown.
Betraying shadows, veiled intent,
In whispered codes, the message sent.

Through mirrored eyes, a subtle glance,
Deception woven in every stance.
A ciphered path, a secret oath,
Double agent, shadows both.

In the twilight's clandestine art,
Betwixt the worlds, a double part.
A game of trust, a web we weave,
In double alleys, secrets leave.

So tread with care, the path unclear,
Double agent, hold what's dear.
In the dance of shadows, light will fade,
But secrets linger, softly played.

From: thescout@skiff.com; 2024-02-14 07:30:57 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: the lions

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

ok. let me tell you what i think by the end of the week.

From: sonyamacoit@outlook.com; 2024-02-16 07:15:41 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC:
Subject: Wonderful but close

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

These last few days we have been able to get wonderful material, but
that last one with the Giraffe was close. Someone is definately
following us now. Victor, we need to ensure our communication is secured
or at least where we save the pics. What do you suggest?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Activate Windows
Go to Settings to activate Windows.

From: thescout@skiff.com; 2024-02-16 07:17:57 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: Wonderful but close

Headers Text HTML RTF Attachments (0) Accounts
Download Images

I suggest using:

In the realm where secrets twine,
Encryption whispers in the code's design.
A dance of bits, a digital ballet,
In the cipher's grip, messages sway.
Binary echoes, a symphony of zeros and ones,
A clandestine language, where secrecy runs.
Algorithms waltz, in cryptographic rhyme,
Gu arding the vault of the passing time.
Key and lock, a digital embrace,
In the algorithm's intricate grace.
Bit by bit, the plaintext hides,
Within the cryptographic tides.
Through tunnels of math, unseen,
Encryption guards what lies between.
A shield of numbers, a fortress grand,
In the encrypted realms, mysteries stand.
Cracking the cipher, a quest untold,
A dance with logic, both young and old.
In the encrypted echoes, secrets keep,
A poem of security, where whispers seep.
So in the bytes and bits, a tale unfolds,
Encryption's story, in algorithms it molds.
A poem of privacy, where secrets unfurl,
In the encrypted dance, a secure world.

From: sonyamacoit@outlook.com; 2024-02-16 07:20:52 GMT
To: thescout@skiff.com;
CC:
Subject: Re: Wonderful but close

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Ok. Remember, I'm not that technical, but will try my best. We still have some business left to conclude at the last waypoints. Should we go out one or two more times?

From: thescout@skiff.com; 2024-02-16 07:23:02 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Wonderful but close

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Let's try two more times max and then everything has to change. Let's send coordinates via phone at least? Do you speak another language?

From: sonyamacoit@outlook.com; 2024-02-16 07:24:44 GMT
To: thescout@skiff.com;
CC:
Subject: Re: Wonderful but close

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Ok. I will wait for your coords. I gre up in the south so yes ek praat die taal.

From: thescout@skiff.com; 2024-02-16 07:25:31 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: Wonderful but close

Headers Text HTML RTF Attachments (0) Accounts
Download Images

Goed. Van nou af praat ons net die taal.

Figure F.12.1 - Emails on 2024/02/19 09:28:23 GMT – 2024/02/21 09:14:49 GMT

From: sonyamacoit@outlook.com; 2024-02-19 09:28:23 GMT
To: thescout@skiff.com; marteneleroux@proton.me;
CC:
Subject: RE: securing our communications and new files

Headers Text HTML RTF Attachments (0) Accounts
Original Text

I think we said we will be discussing this next? I have placed all the
photos of our environmental exploration on the c: drive, but we were
noticed so now everything going forward has to be hidden. I'm not
technical Victor, but have installed Kleopatra. What now?

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Activate Windows
Go to Settings to activate Windows.

From: thescout@skiff.com; 2024-02-19 09:32:00 GMT
To: sonyamacoit@outlook.com; marteneleroux@proton.me;
CC:
Subject: RE: securing our communications and new files

Headers Text HTML RTF Attachments (0) Accounts
Download Images

generate keys and encrypt the new files using that. Copy some of the images somewhere else and dispose. I'm also not an expert, but you have to hurry up - I don't want these things to be uncovered with my data on it. These individuals are...

From: marteneleroux@proton.me; 2024-02-19 09:32:43 GMT
To: sonyamacoit@outlook.com;
CC: thescout@skiff.com;
Subject: RE: securing our communications and new files

Headers Text HTML RTF Attachments (0) Accounts
Original Text

This whole thing concerns me. I'm out.

Sent with Proton Mail secure email.

From: sonyamacoit@outlook.com; 2024-02-19 09:40:07 GMT
To: thescout@skiff.com;
CC:
Subject: Re: securing our communications and new files

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Original Text

Our conservation efforts have clearly caused more problems than we hoped
for. How is this possible? Will let you know what I have done when its done.

From: thescout@skiff.com; 2024-02-19 09:42:07 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Re: securing our communications and new files

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Let him go. Its important work that someone has to do.

From: sonyamacoit@outlook.com; 2024-02-20 11:33:17 GMT
To: thescout@skiff.com;
CC:
Subject: encryption

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

I have been encrypting everything Victor, but some files have not been placed on the pics drive. See my public key below:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Comment: User-ID: Sonya <sonyamacoit@outlook.com>
Comment: Valid from: 20/02/2024 09:09
Comment: Valid until: 20/02/2027 12:00
Comment: Type: 255-bit EdDSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint: F882AC885E2A4CCBD56ADC78B87EBB6DD62A4F84

mDMEZdRsVxYJKwYBBAHaRw8BAQdA0gQxeiyJQO5yewv31h6F1b2r4eT6Wy/zZ7F0
EJ1YydW0H1NvbnlhIDxzb255YW1hY29pdEBvdXRsb29rLmNvbT6ImQQTFgoAQRYh
BPiCrIheKkzL1WrceLh+u23WKk+EBQJI1GxXAhsDBQkFpRPpBQsJCAcCAiICBhUK
CQgLAgQWAgMBAh4HAheAAAoJELh+u23WKk+EUOcA/RHJHGpCKJIxwtzMOVOHzmVx
uL+J4awgdarGafSIQ28aAQDCE7yziBh5hlhXHCFPfhIHDWPifS91loy6c9Rtcww6
Bbg4BGXUbFcSCisGAQQBl1UBBQEBB0D/dbTzMsqI89osBh70y7L1FnpcojFGK2Hu
eJwKg0TRgMBCAeIfgQYFgoAJhYhBPiCrIheKkzL1WrceLh+u23WKk+EBQJI1GxX
AhsMBQkFpRPpAAoJELh+u23WKk+EYEEA/R9qEnIZc/WtaB35+sMAZKR6gQFU3g2S
bbRPOcWMRYjVAP9dmZLzb18tbeq4DI3pBhqgQLW/Fx/kOEKPYIX6Mc77Ag==
=f2kz
-----END PGP PUBLIC KEY BLOCK-----

--

Sonya Macoit
Environmental Assessments Lead
Macoit Industries

Activate Windows
Go to Settings to activate Windows.

From: sonyamacoit@outlook.com; 2024-02-20 11:43:43 GMT
To: thescout@skiff.com;
CC:
Subject: ...

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppD	12	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppD	1297	text/plain	unknown

From: thescout@skiff.com; 2024-02-21 08:10:08 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: Verstaan ons mekaar

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Kan jy dit lees?

Secured by Skiff Mail.

From: sonyamacoit@outlook.com; 2024-02-21 08:13:06 GMT
To: thescout@skiff.com;
CC:
Subject: Re: Verstaan ons mekaar

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

Ek kan maar ek dink nie dit werk nie.

From: thescout@skiff.com; 2024-02-21 08:22:07 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: En nou?

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppD	8313	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppD	10	text/plain	unknown

From: thescout@skiff.com; 2024-02-21 08:26:36 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: nuwe inligting...

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	8370	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	10	text/plain	unknown

From: sonyamacoit@outlook.com; 2024-02-21 08:36:21 GMT
To: marteneleroux@proton.me;
CC:
Subject: ...

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	3215	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	12	text/plain	unknown

From: sonyamacoit@outlook.com; 2024-02-21 08:51:06 GMT
To: thescout@skiff.com;
CC:
Subject: ...

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	4679027	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	12	text/plain	unknown

From: thescout@skiff.com; 2024-02-21 08:56:48 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: ...

Headers | Text | HTML | RTF | Attachments (1) | Accounts

Download Images

Dit maak sin. Ek sal die fotos hou by my. Ons moet nou beplan om te vlug. Daar is 'n lugballon in die Masai Mara. Kom ons ontmoet mekaar by die plaza en dan maak ons 'n plan om daar uit te kom

On Wed, 21 Feb 2024 08:51:24 GMT, Sonya Macoit
sonyamacoit@outlook.com wrote:

Decrypting pgp...

From: thescout@skiff.com; 2024-02-21 08:56:48 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: ...

Headers | Text | HTML | RTF | Attachments (1) | Accounts

View in New Window

1 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	3219	text/plain	unknown

From: sonyamacoit@outlook.com; 2024-02-21 08:58:38 GMT
To: thescout@skiff.com;
CC:
Subject: ...

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	7365	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	12	text/plain	unknown

From: thescout@skiff.com; 2024-02-21 09:00:04 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: ...

Headers | Text | HTML | RTF | Attachments (1) | Accounts

Download Images

Laat ek kies. Sien jou vanaand laat dan ry ons in the nag en kom more oggend daar uit.

On Wed, 21 Feb 2024 08:58:43 GMT, Sonya Macoit
sonyamacoit@outlook.com wrote:

Decrypting pgp...

From: sonyamacoit@outlook.com; 2024-02-21 09:01:23 GMT
To: thescout@skiff.com;
CC:
Subject: ...

Headers | Text | HTML | RTF | Attachments (2) | Accounts

View in New Window

2 Results

Table | Thumbnail | Summary

Save Table as CSV

Location	Size	Mime type	Known
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	12	text/plain	unknown
/img_CrypticWilds.000/vol_vol6/Users/Sonya/Appl	7205	text/plain	unknown

From: thescout@skiff.com; 2024-02-21 09:13:36 GMT
To: sonyamacoit@outlook.com;
CC:
Subject: RE: ...

Headers Text HTML RTF Attachments (1) Accounts
Download Images

Sit die inligting op die BitLocker To Go usb disk.

The destination will be Serena Airstrip HK0A

From: thescout@skiff.com; 2024-02-21 09:14:49
To: sonyamacoit@outlook.com;
CC:
Subject: RE: ...

Headers Text HTML RTF Attachments (1) Accounts
Download Images

They have compromised my email Sonya. I quite sure of it. I will send you the new location by text. Save it on the flash drive.

Figure F.12.2 File attachments to email on 2024/02/19 09:28:23 GMT – 2024/02/21 09:14:49 GMT

Attachment530339001

/C:/Users/admin/Desktop/attachm
file:///C:/Users/admin/Desktop/attachment530339001

```
Version: 1
```

Encrypted.asc

/C:/Users/admin/Desktop/attachm /C:/Users/admin/Desktop/encrypte
file:///C:/Users/admin/Desktop/encrypted.asc


```
-----BEGIN PGP MESSAGE-----

wV4DUaFJCKhLo18SAQdAIxxoDepvmHbSaFC+i35w8UAYg91sBiVzyrA4zvFsQi0w0/P/GTK3ACDU
Wus/Zm9dh57Cz3KpafH0jni/1PYtQgqkkhynhuS/JLZ9HZotbXKs0sJgAQqLpz2WDj8rdBWhEM1B
K+WRdGgk+XR3/ZFt1kuWqHvrEJvCzPuFRhdkmtg6HoQ9/FYu3qnHgXmvFL4TB+/pw6r2mHYnGVvH
fRjj+T5TxzqdeS+FuaOvQL60sOvBptMuioeAddeU2/nSnSOTXhjiSB2MHLy9hwFhAWQPlE7mlgx
q7ORUECXApfJiuuF8+0G+oz+ru03Z1oouUX+7BzwmvaPEs1R6xXB+VbanMRGxvuHosmUv5PfLqr
HrpjyUac37LRGtAIeoVZMn4XqMrQl+/xl3PwLDvfmmMb2NL4bZavoxKWx6THvH4vj0k5+jUAvFT+
WVuljRDmc44mTqIB9bwjvafnovlp2wqREqg7eqKrTRg88NAquHFX4cvoZBrvu4TwzX6PXl1CJ/Px
AuC+Cf0dAMd0ZJdBVU8CW4j6kx94+CwQgaOTYToCE1AAqkP5AgT9guh/1O5XM/ejak1kD/0AGqJ/
Hq/F1+mV/sQQjoSpPPDKnuNngEVcqaYcSFt/7RxCNM9HFO+MqugPJRFzKpFGsNv/tRLnxI+fMPW4
cFTK5nhdZSfWRoPrEU7wuHX939zM0J8k/el9+AaVgFJcuQRCyxl5HbieImf+V3dharC966RxWQGe
4sZE6EkiJZ0QXjg6xYc3l2hdNb1+x7xPdN2ZTw/SAbzEbACgCP+tUB+cOkcfXNZL4cGhVCERLgA6
1ZBOKNcvMxqVr6DTArv0YzWucOghYDzmQBPo/2IS8C6q6ilUERTjSa+PBRnfRuPQK8nxu2Y5kDzs
09QTuQ8gcT+B0/m67HxiCAq/JD0bHXJRjMxGpRLPEmetSHF2WssfTuOanmSYzW33j8P3U8jyzxsy
83C2fo6tHi5MCY2/zLuzuRzChfGHkmuW857Xqwa3hO8kpoZBHmmce1Rep6hyxkUlLhqqTl8zrLfl
cmwui7rZ05QzW8sZA+yxXbfvUX+0nkrgmYN+WgQg016Wy7Vh5mj1AeEXwBeV1rJYVQ0KSzOEHiNh
tvsK4FiWqol12VG1WbBWVlKhjIBlQR/zqYLUJGqI9T29IFR0vRHHHwTIP1k=
=I7Jz
-----END PGP MESSAGE-----
```

Figure F.13.1 - Tampering 2024/01/3 10:37:36 and 2024/02/24 07:23:02 GMT MD5 f1f120700ff977e60912be456cf6197c, Investigator JB

Inbox	thescout@skiff.com;	Re: Wonderful but close	2024-02-16 07:23:02 GMT	Not available	/outlook.office365.com/Inbox	fk608492-8234-48df-a98c-4cfda045f927	CrypticWilds.000	sonyamacoit@outlook.com;
Inbox	thescout@skiff.com;	Re: Wonderful but close	2024-02-16 07:25:31 GMT	Not available	/outlook.office365.com/Inbox	fk608492-8234-48df-a98c-4cfda045f927	CrypticWilds.000	sonyamacoit@outlook.com;
Sent	sonyamacoit@outlook.com;	Re: Wonderful but close	2024-02-16 07:20:52 GMT	Not available	/outlook.office365.com/Sent	de6038cc-8e26-482e-b996-446f86aa74ce	CrypticWilds.000	thescout@skiff.com;
Sent	sonyamacoit@outlook.com;	Re: Wonderful but close	2024-02-16 07:24:44 GMT	Not available	/outlook.office365.com/Sent	de6038cc-8e26-482e-b996-446f86aa74ce	CrypticWilds.000	thescout@skiff.com;

Data Content
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 10 Page Matches on page: - of - Match 100% Reset

Microsoft account

Security info was added

The following security info was recently added to the Microsoft account so**t@outlook.com

karl@vanderstyff.net

If this was you, then you can safely ignore this email.

If this wasn't you, a malicious user has access to your account. Please review your recent activity and we'll help you secure your account.

Review recent activity

Figure F.13.2 - Tampering 2024/01/3 10:37:36 and 2024/02/24 07:23:02 GMT MD5 f1f120700ff977e60912be456cf6197c, Investigator JB

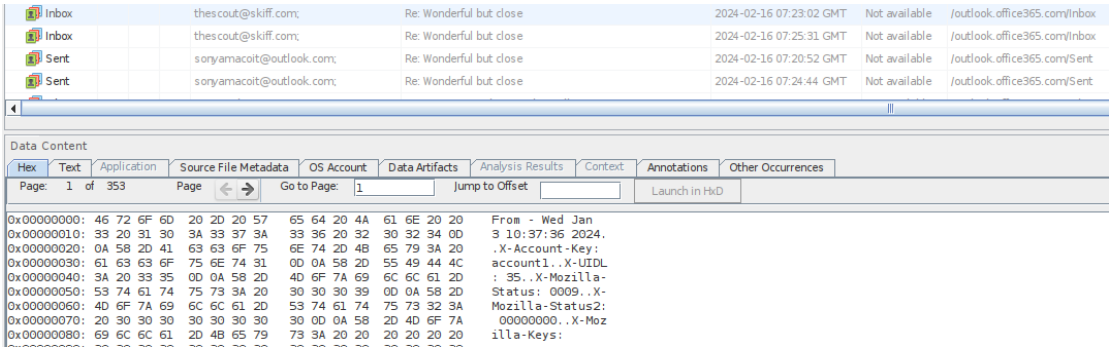


Figure F.13.3 - Tampering confession 2025/04/22 07:16 GMT, Investigator JB

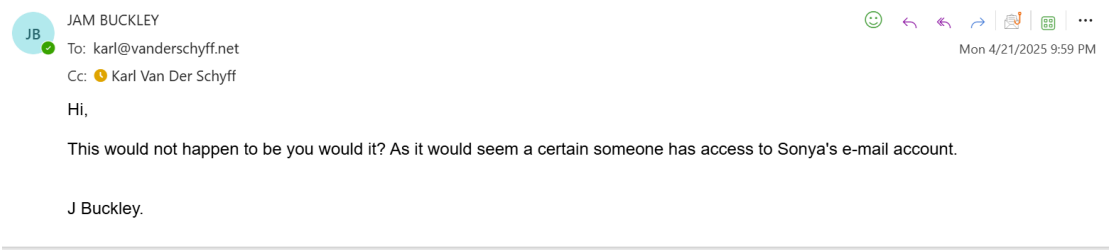


Figure F.14.1 - Public key block MD5 6c18323e5251a908932d1e5d901a9777, Investigator AH, JB

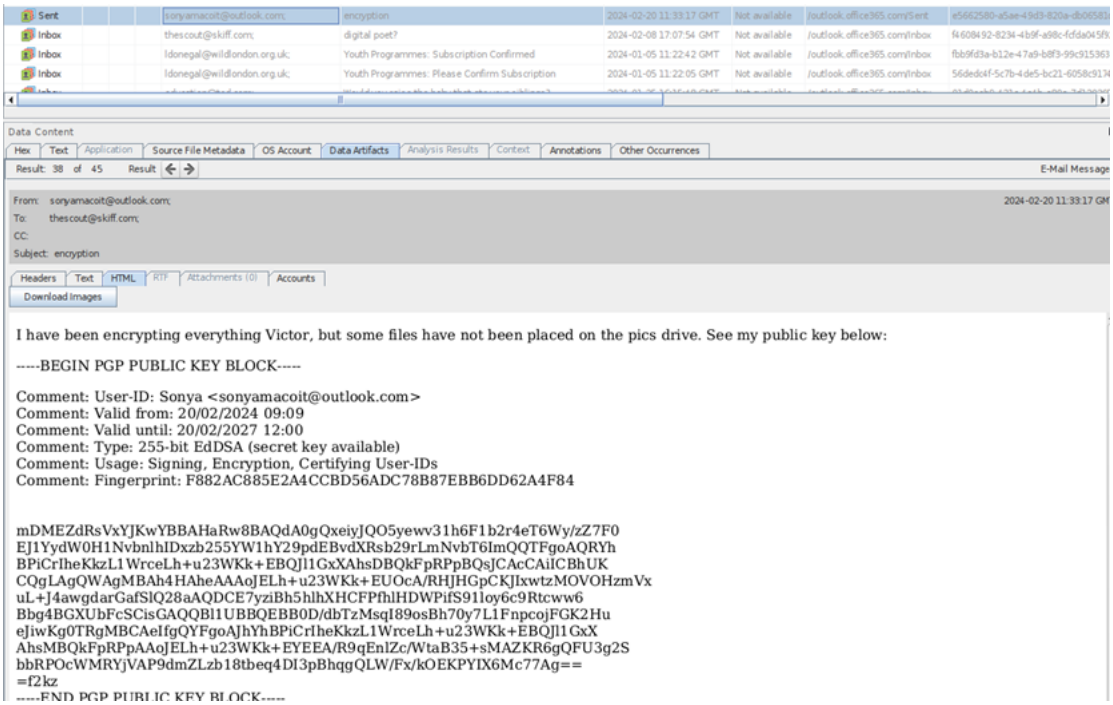
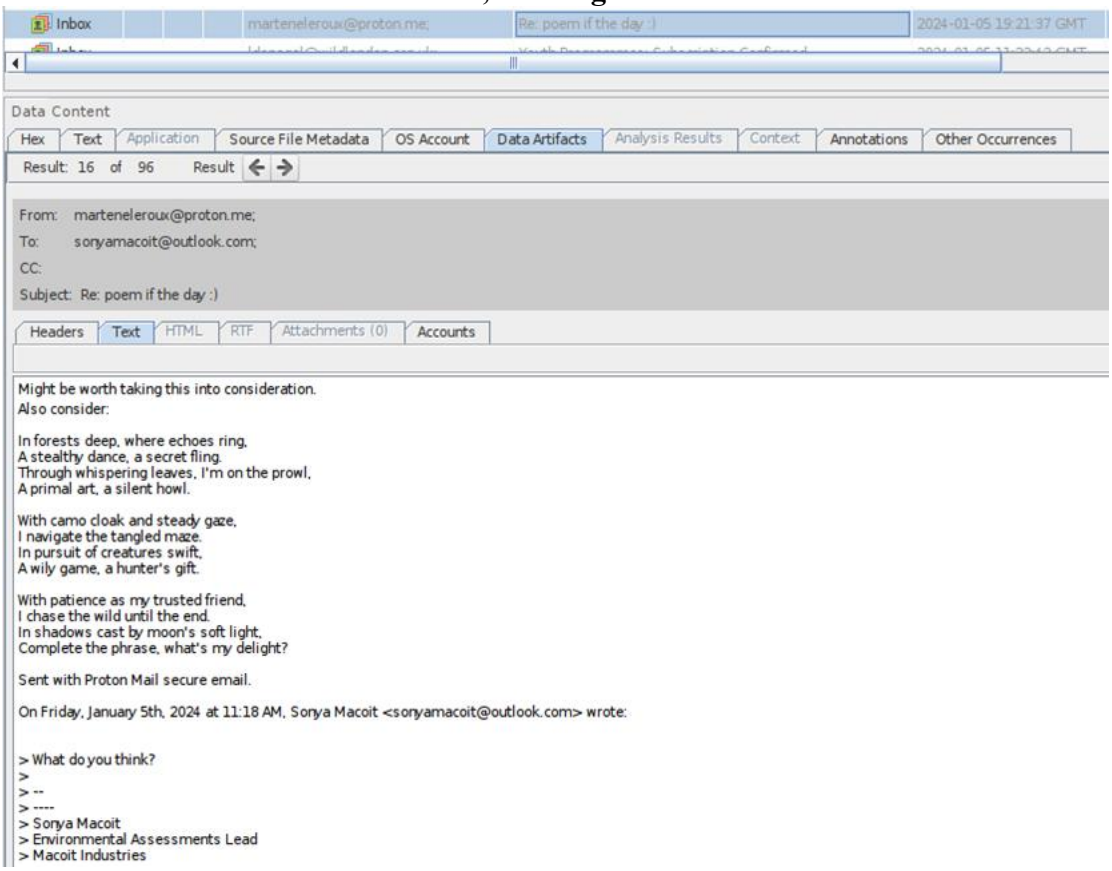


Figure F.15.1 - Poetry 2024/01/05 19:21:37 GMT MD5 f1f120700ff977e60912be456cf6197c, Investigator AH



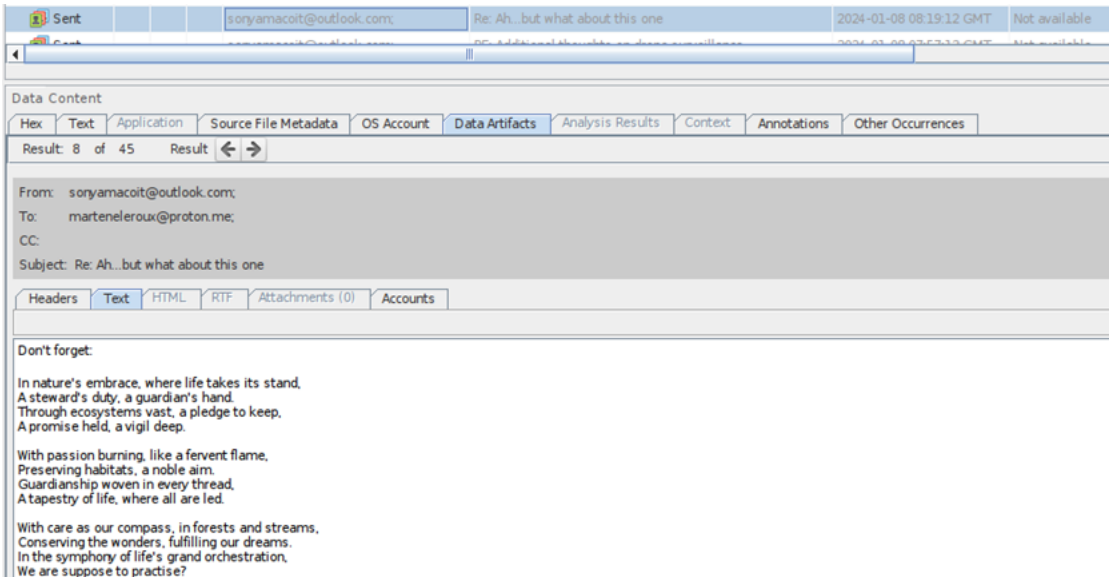
Might be worth taking this into consideration.
Also consider:

In forests deep, where echoes ring,
A stealthy dance, a secret fling.
Through whispering leaves, I'm on the prowl,
A primal art, a silent howl.

With camo cloak and steady gaze,
I navigate the tangled maze.
In pursuit of creatures swift,
A wily game, a hunter's gift.

With patience as my trusted friend,
I chase the wild until the end.
In shadows cast by moon's soft light,
Complete the phrase, what's my delight?

Figure F.15.2 - Poetry 2024/01/08 08:19:12 GMT MD5 6c18323e5251a908932d1e5d901a9777, Investigator AH



Content:

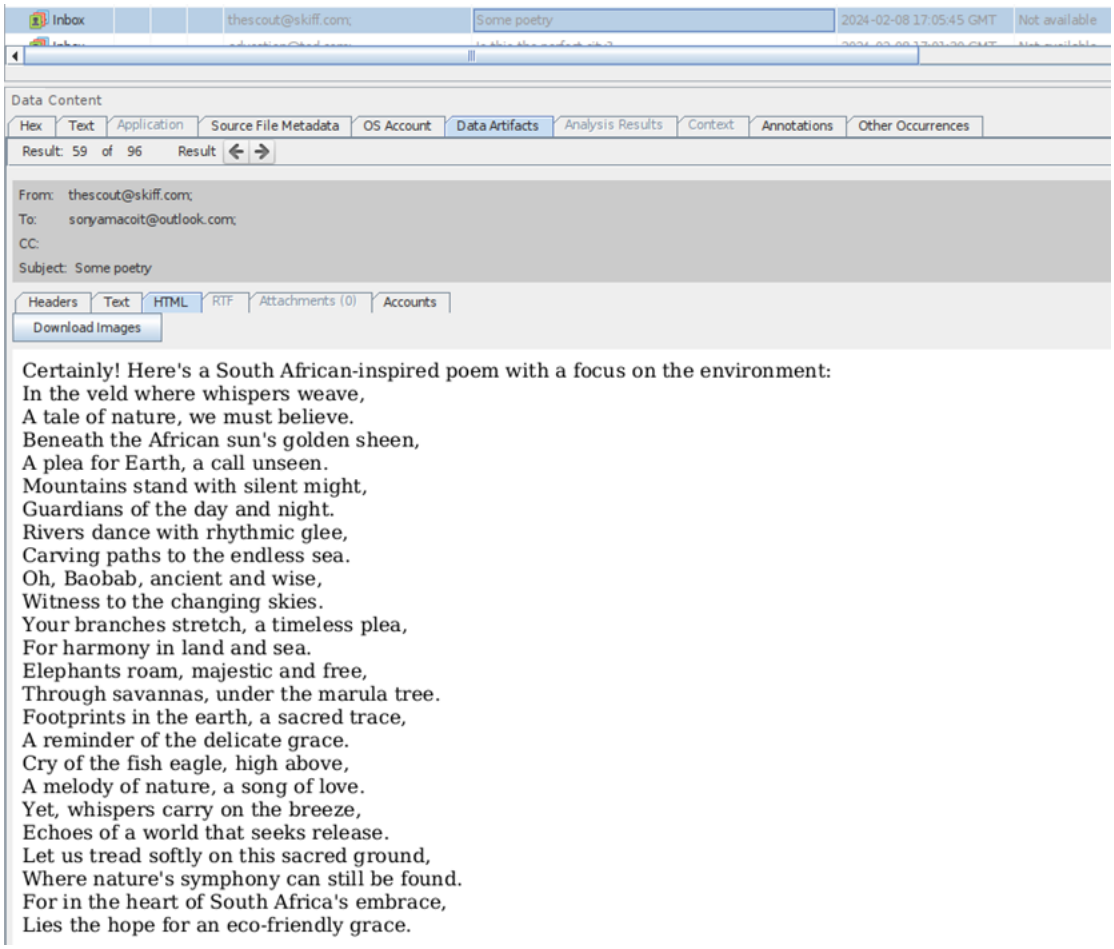
Don't forget:

In nature's embrace, where life takes its stand,
A steward's duty, a guardian's hand.
Through ecosystems vast, a pledge to keep,
A promise held, a vigil deep.

With passion burning, like a fervent flame,
Preserving habitats, a noble aim.
Guardianship woven in every thread,
A tapestry of life, where all are led.

With care as our compass, in forests and streams,
Conserving the wonders, fulfilling our dreams.
In the symphony of life's grand orchestration,
We are suppose to practise?

Figure F.15.3 - Poetry 2024/02/08 17;05:45 GMT MD5 f1f120700ff977e60912be456cf6197c, Investigator AH

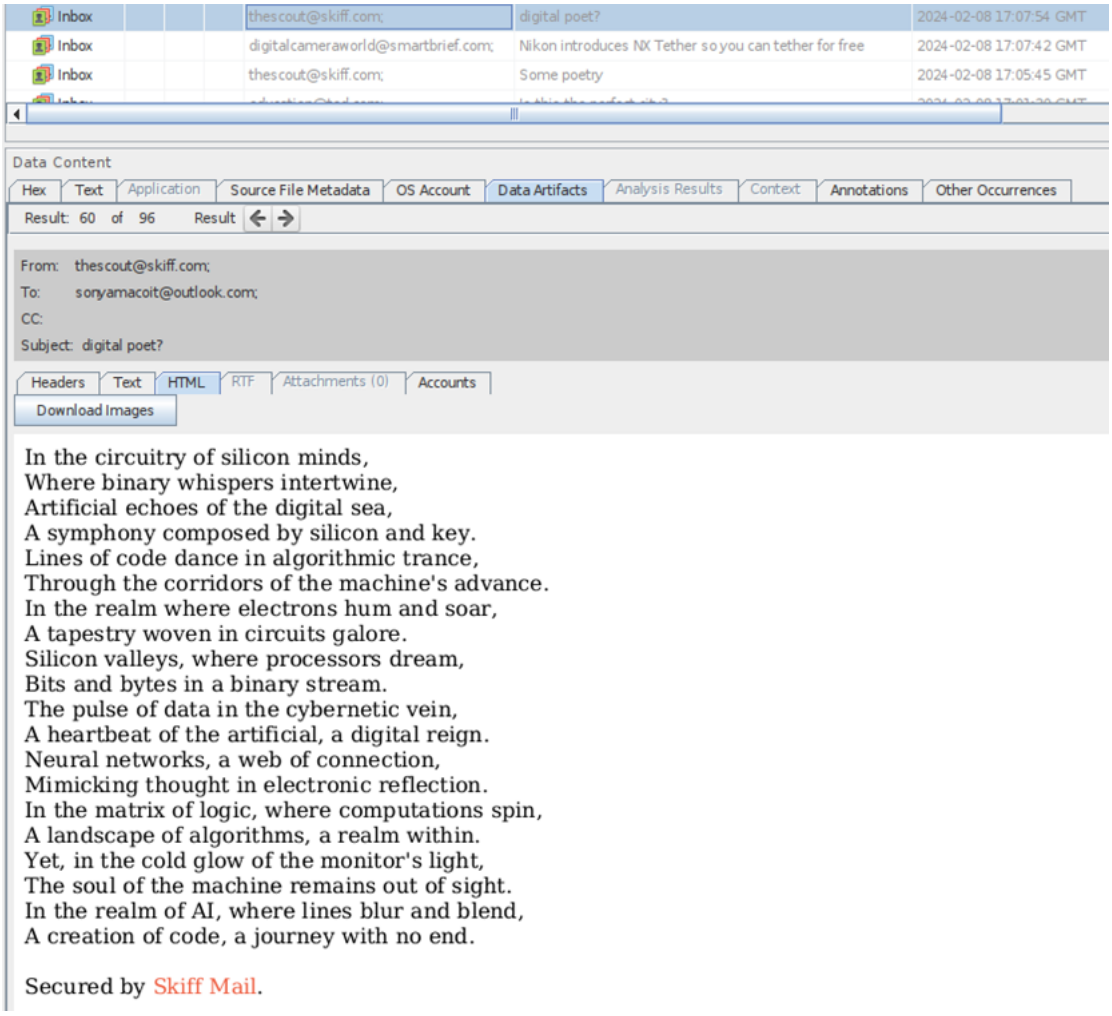


Content:
Certainly! Here's a South African-inspired poem with a focus on the environment:
In the veld where whispers weave,
A tale of nature, we must believe.
Beneath the African sun's golden sheen,
A plea for Earth, a call unseen.
Mountains stand with silent might,
Guardians of the day and night.
Rivers dance with rhythmic glee,
Carving paths to the endless sea.
Oh, Baobab, ancient and wise,
Witness to the changing skies.
Your branches stretch, a timeless plea,
For harmony in land and sea.
Elephants roam, majestic and free,
Through savannas, under the marula tree.
Footprints in the earth, a sacred trace,
A reminder of the delicate grace.
Cry of the fish eagle, high above,
A melody of nature, a song of love.
Yet, whispers carry on the breeze,
Echoes of a world that seeks release.
Let us tread softly on this sacred ground,
Where nature's symphony can still be found.
For in the heart of South Africa's embrace,

Lies the hope for an eco-friendly grace.

Secured by Skiff Mail.

Figure F.15.4 - Poetry 2024/02/08 17:07:54 GMT MD5 f1f120700ff977e60912be456cf6197c, Investigator AH

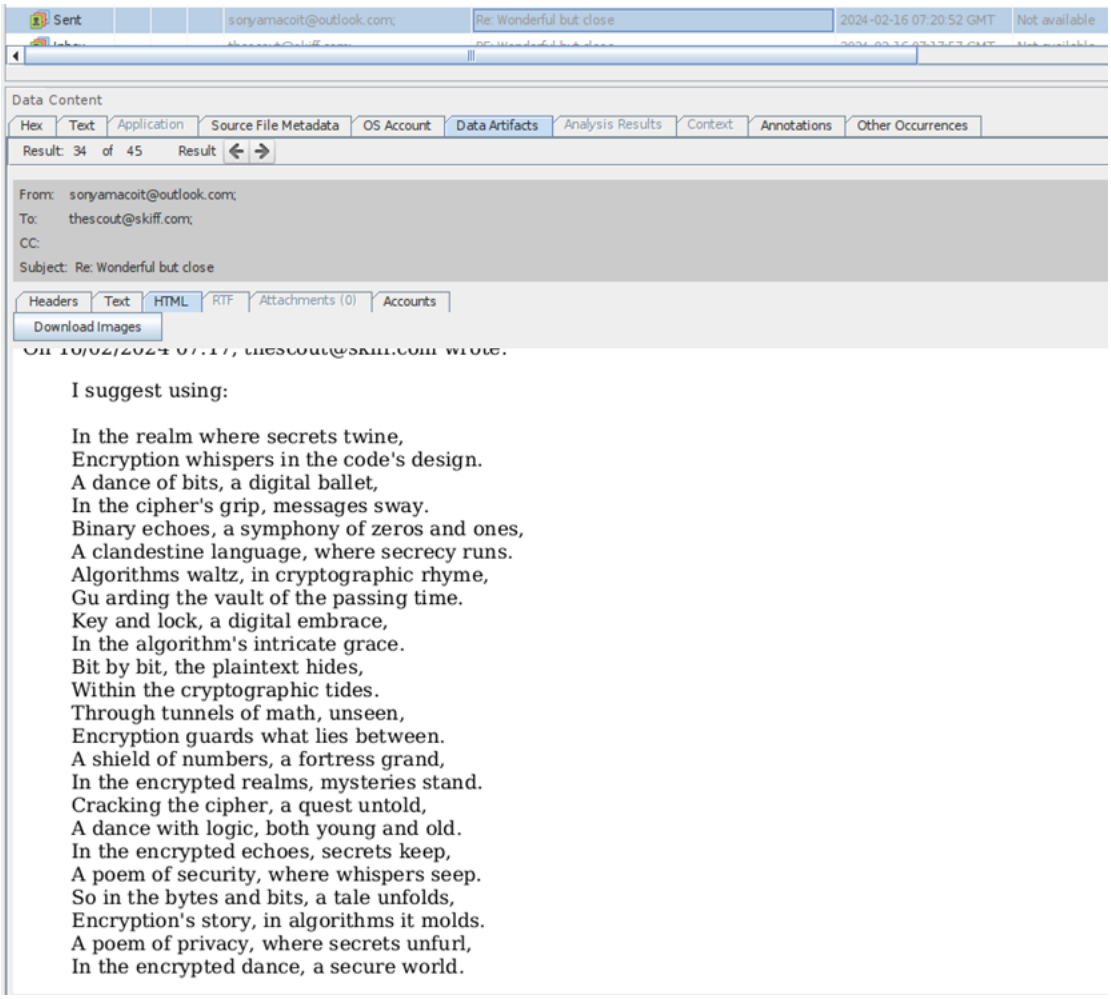


Content:
In the circuitry of silicon minds,
Where binary whispers intertwine,
Artificial echoes of the digital sea,
A symphony composed by silicon and key.
Lines of code dance in algorithmic trance,
Through the corridors of the machine's advance.
In the realm where electrons hum and soar,
A tapestry woven in circuits galore.
Silicon valleys, where processors dream,
Bits and bytes in a binary stream.
The pulse of data in the cybernetic vein,
A heartbeat of the artificial, a digital reign.
Neural networks, a web of connection,
Mimicking thought in electronic reflection.
In the matrix of logic, where computations spin,

A landscape of algorithms, a realm within.
Yet, in the cold glow of the monitor's light,
The soul of the machine remains out of sight.
In the realm of AI, where lines blur and blend,
A creation of code, a journey with no end.

Secured by Skiff Mail.

Figure F.15.5 - Poetry 2024/02/16 07:17:57 GMT MD5 f1f120700ff977e60912be456cf6197c, Investigator AH



Content:
I suggest using:

In the realm where secrets twine,
Encryption whispers in the code's design.
A dance of bits, a digital ballet,
In the cipher's grip, messages sway.
Binary echoes, a symphony of zeros and ones,
A clandestine language, where secrecy runs.
Algorithms waltz, in cryptographic rhyme,
Gu arding the vault of the passing time.
Key and lock, a digital embrace,

In the algorithm's intricate grace.
Bit by bit, the plaintext hides,
Within the cryptographic tides.
Through tunnels of math, unseen,
Encryption guards what lies between.
A shield of numbers, a fortress grand,
In the encrypted realms, mysteries stand.
Cracking the cipher, a quest untold,
A dance with logic, both young and old.
In the encrypted echoes, secrets keep,
A poem of security, where whispers seep.
So in the bytes and bits, a tale unfolds,
Encryption's story, in algorithms it molds.
A poem of privacy, where secrets unfurl,
In the encrypted dance, a secure world.

Appendix G Encryption

Dates listed are that of last modified time.

Figure G.1.1 - Steghide run programs artifact last run 2024/01/24 13:40:27, Investigator JB

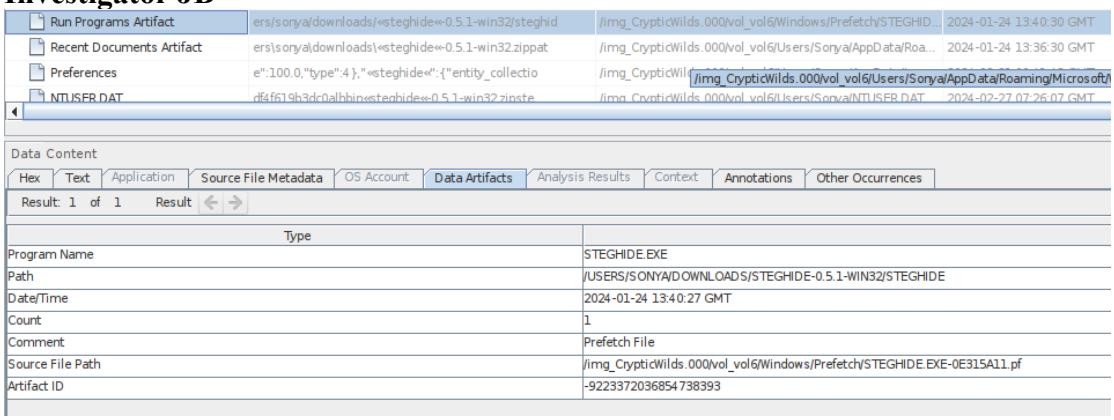


Figure G.1.2 - Steghide zip file sent to recycling bin 2024/01/24 13:40:46 MD5: 6dcd891c62978d83df3c026f6ad0fbd9, Investigator JB

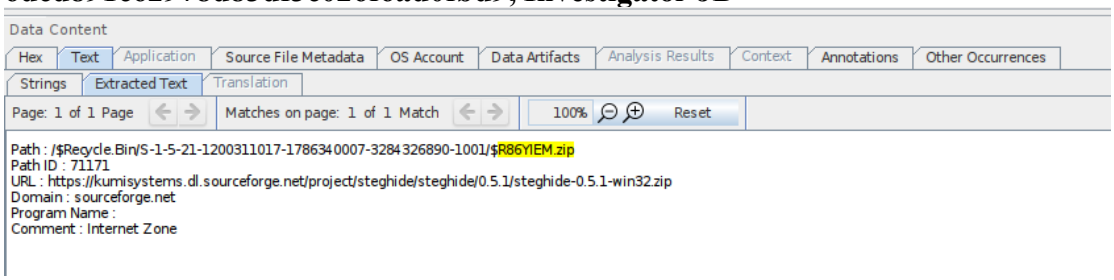


Figure G.1.3 - Steghide zip files found in recycling bin 2024/01/24 13:40:46, Investigator JB

$I86YIEM.zip	0	2024-01-24 13:40:46 GMT	2024-01-24 13:40:46 GMT	2024-02-19 09:06
$IADVIQV.1-win32	0	2024-01-24 13:40:46 GMT	2024-01-24 13:40:46 GMT	2024-02-21 08:38
$ICM5Q7R.jpg	0	2024-01-03 08:18:26 GMT	2024-01-03 08:18:26 GMT	2024-02-07 09:25
$ICS13B5.asc	0	2024-02-21 08:38:07 GMT	2024-02-21 08:38:07 GMT	2024-02-21 08:38
$IDP6E6W.bak	0	2024-02-19 09:12:11 GMT	2024-02-19 09:12:11 GMT	2024-02-19 09:12
$IEHZ3BP.bak	0	2024-02-19 09:12:11 GMT	2024-02-19 09:12:11 GMT	2024-02-19 09:12
$IGKEW5L.bak	0	2024-02-19 09:12:11 GMT	2024-02-19 09:12:11 GMT	2024-02-19 09:12
$IJC8VZB.bak	0	2024-02-19 09:11:50 GMT	2024-02-19 09:11:50 GMT	2024-02-19 09:11
$ILCY1HK.bak	0	2024-02-19 09:12:11 GMT	2024-02-19 09:12:11 GMT	2024-02-19 09:12
$ILMCX74.bak	0	2024-02-19 09:12:11 GMT	2024-02-19 09:12:11 GMT	2024-02-19 09:12
$INWC9PL.bak	0	2024-02-19 09:12:11 GMT	2024-02-19 09:12:11 GMT	2024-02-19 09:12
$IOJXH0M.bak	0	2024-02-19 09:11:50 GMT	2024-02-19 09:11:50 GMT	2024-02-19 09:11

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations

Page: 1 of 1 Page Go to Page: 1 Jump to Offset Launch in

```
0x00000000: 02 00 00 00  00 00 00 00  75 B5 1B 00  00 00 00 00   ........u.......
0x00000010: 80 C0 25 EF  CA 4E DA 01  32 00 00 00  43 00 3A 00   ..%..N..2...C.:.
0x00000020: 5C 00 55 00  73 00 65 00  72 00 73 00  5C 00 53 00   \.U.s.e.r.s.\.S.
0x00000030: 6F 00 6E 00  79 00 61 00  5C 00 44 00  6F 00 77 00   o.n.y.a.\.D.o.w.
0x00000040: 6E 00 6C 00  6F 00 61 00  64 00 73 00  5C 00 73 00   n.l.o.a.d.s.\.s.
0x00000050: 74 00 65 00  67 00 68 00  69 00 64 00  65 00 2D 00   t.e.g.h.i.d.e.-.
0x00000060: 30 00 2E 00  35 00 2E 00  31 00 2D 00  77 00 69 00   0...5...1.-.w.i.
0x00000070: 6E 00 33 00  32 00 2E 00  7A 00 69 00  70 00 00 00   n.3.2...z.i.p...
```

Figure G.1.4 - Shellbags: steghide 2024/01/24 13:40:32 MD5: e119d03c028c58cc9df67b389b38c76a, Investigator JB

Shell Bags Artifact	path : explorer\«steghide«-0.5.1-win32.zikey	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Loca...	2024-02-27 07:26:07 GMT	2023-12-15 13:23:13 GMT
Shell Bags Artifact	path : explorer\«steghide«-0.5.1-win3key : lo	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Loca...	2024-02-27 07:26:07 GMT	2023-12-15 13:23:13 GMT
Shell Bags Artifact	path : explorer\«steghide«-0.5.1-win3\steghid	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Loca...	2024-02-27 07:26:07 GMT	2023-12-15 13:23:13 GMT
Run Programs Artifact	ers/sonya/downloads/steghide«-0.5.1-win32/steghid	/img_CrypticWilds.000/vol_vol6/Windows/Prefetch/STEGHID...	2024-01-24 13:40:30 GMT	2024-03-04 18:12:51 GMT

Data Content

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 6 of 69 Result

Type	Value
Path	Explorer\steghide-0.5.1-win3\steghid
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\1\0\
Last Write	2024-01-24 13:40:42 GMT
Date Modified	2024-01-24 13:40:22 GMT
Date Created	2024-01-24 13:40:20 GMT
Date Accessed	2024-01-24 13:40:22 GMT
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat
Artifact ID	-9223372036854775608

Figure G.2.1 - Kleopatra website cache in German M.A.C.E wiped, Investigator JB

0	"screenshot gpgol & «kleopatra«("24) href="https:/	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Loca...	0000-00-00 00:00:00
0	existing one) with «kleopatra« which is installed	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Loca...	0000-00-00 00:00:00

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Download Images

English | Deutsch

-
- Was ist neu
  Version 4.2
-
- Über Gpg4win
  - Über Gpg4win
  - Funktionen
  - Systemvoraussetzungen
  - Dokumentation
  - Screenshots
  - Datenschutzerklärung
  -
- Gemeinschaft

Figure G.2.2 - Kleopatra shortcut file last used 2024/02/19 09:25:04, Investigator JB MD5 b83fbc61fad188bced4a735091918118

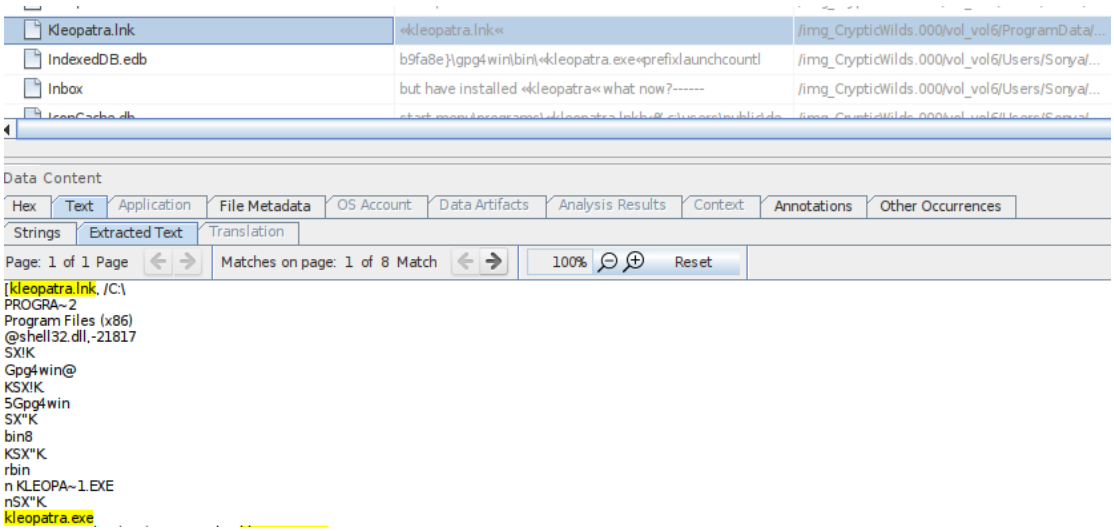
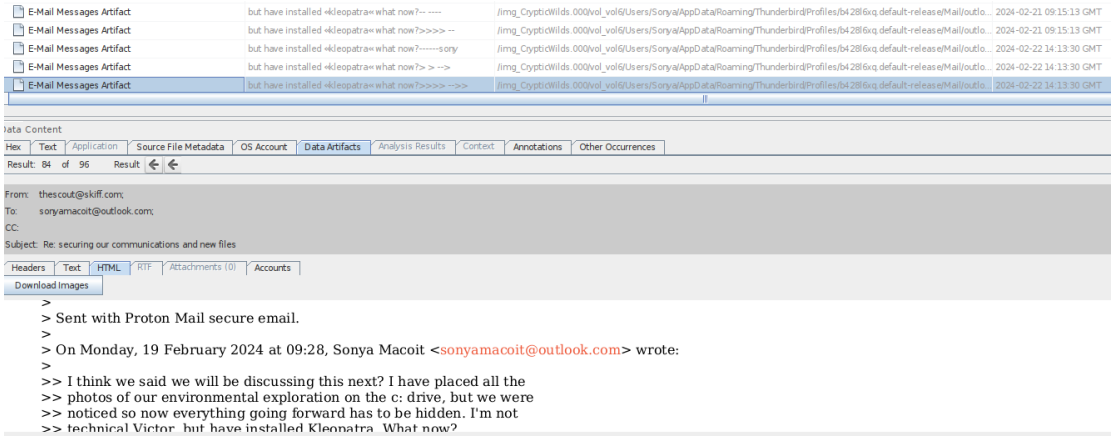


Figure G.2.3 - Kleopatra download confession 2024/02/19 09:28:25, Investigator AH MD5 f1f120700ff977e60912be456cf6197c



On 2024/02/19 09:28:25 GMT, Sonya Macoitsonyamacoit@outlook.com wrote:I think we said we will be discussing this next? I have placed all the photos of our environmental exploration on the c: drive, but we were noticed so now everything going forward has to be hidden. I'm not technical Victor, but have installed Kleopatra. What now?------Sonya MacoitEnvironmental Assessments LeadMacoit Industries

Figure G.2.4 - Kleopatra usage incidents 2024/02/20 09:07:37, Investigator JB MD5 3ee892d7a49816e948494c45a4ff373

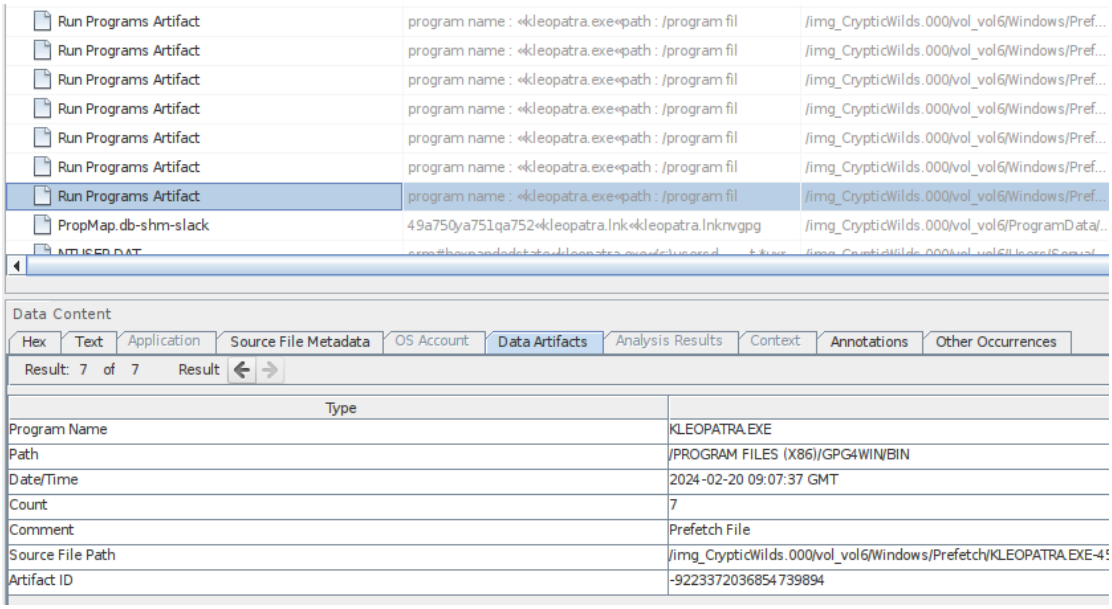


Figure G.2.5 - Kleopatra app settings 2024/02/22 15:03:44, Investigator JB MD5 c7e20b6c681fffee4d44fb7d881f5a6

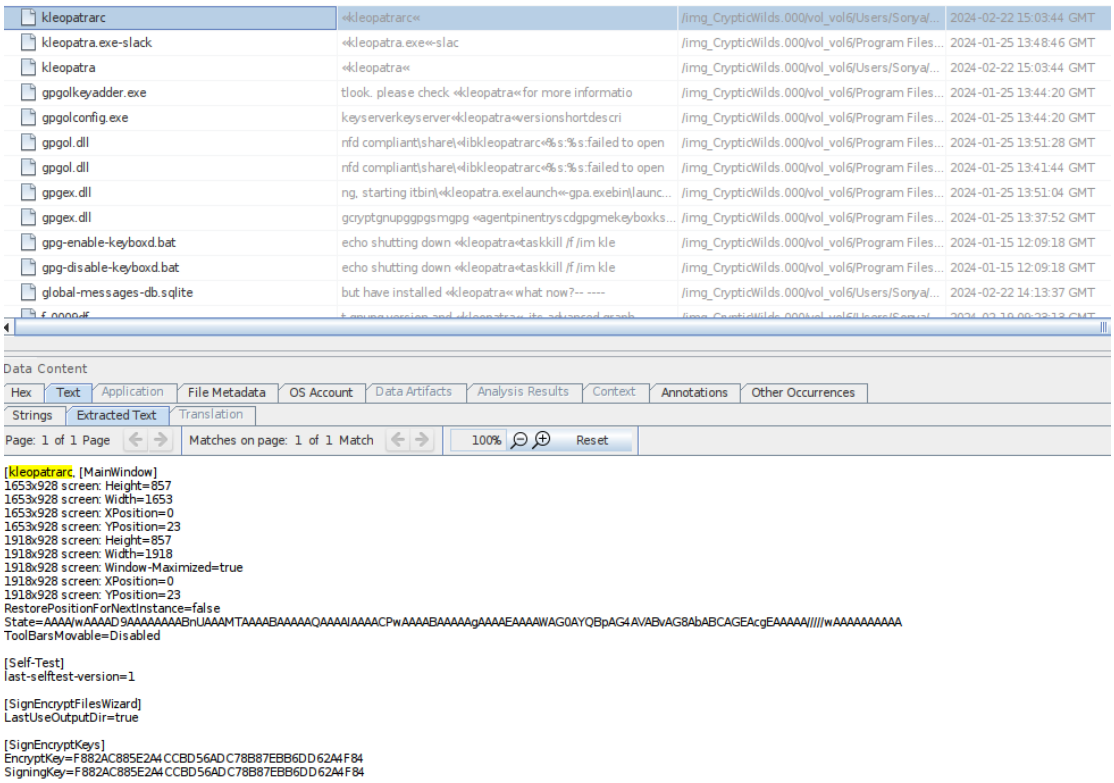


Figure G.3.1 - Hash cracking I.2.1 2025/04/15, Investigator JB, hash to crack SHA1: 338526e5c661ccb2655dc7886d29f700512a906c

```
cmp209@cmp209-virtual-machine:~/Desktop/tools$ chmod +x hash_cracker_SHA1.sh
cmp209@cmp209-virtual-machine:~/Desktop/tools$ ./hash_cracker_SHA1.sh
conservation
```

Result: conservation

Figure G.3.2 - Decrypt PGP using find command to find encrypted files 2025/04/15, Investigator JB

find . -type f –name “*.pgp”

find . -type f –name “*.gpg”

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# find . -type f -name "*.pgp"
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# find . -type f -name "*.gpg"
./Program Files (x86)/GnuPG/share/gnupg/distsigkey.gpg
./Users/Sonya/AppData/Roaming/gnupg/trustdb.gpg
./Users/Sonya/AppData/Roaming/Thunderbird/Profiles/b428l6xq.default-release/pubring.gpg
./Users/Sonya/AppData/Roaming/Thunderbird/Profiles/b428l6xq.default-release/secring.gpg
./Users/Sonya/Documents/backup_070224/areas of interest.png.gpg
./Users/Sonya/Documents/backup_070224/BitLocker Recovery Key 139F76F0-FBF6-499F-8A09-E76C9A337A82.TXT.gpg
./Users/Sonya/Documents/backup_070224/MSFT-Windows11-Security-book_Sept2023.pdf.gpg
./Users/Sonya/Documents/backup_070224/the_list.txt.gpg
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount points/suspectDrive#
```

Result:

./Program Files (x86)/GnuPG/share/gnupg/distsigkey.gpg ./Users/Sonya/AppData/Roaming/gnupg/trustdb.gpg ./Users/Sonya/AppData/Roaming/Thunderbird/Profiles/b428l6xq.default-release/pubring.gpg ./Users/Sonya/AppData/Roaming/Thunderbird/Profiles/b428l6xq.default-release/secring.gpg ./Users/Sonya/Documents/backup_070224/areas of interest.png.gpg ./Users/Sonya/Documents/backup_070224/BitLocker Recovery Key 139F76F0-FBF6-499F-8A09-E76C9A337A82.TXT.gpg ./Users/Sonya/Documents/backup_070224/MSFT-Windows11-Security-book_Sept2023.pdf.gpg ./Users/Sonya/Documents/backup_070224/the_list.txt.gpg

Figure G.3.3 - Find private key using find command recursive search 2025/04/15, Investigator JB

-type f -name "*.asc":

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# find . -type f -name "*.asc"
./$Recycle.Bin/S-1-5-21-1200311017-1786340007-3284326890-1001/$ICS13B5.asc
./$Recycle.Bin/S-1-5-21-1200311017-1786340007-3284326890-1001/$RCS13B5.asc
./Users/Sonya/Documents/backup_070224/Sonya_0xD62A4F84_SECRET.asc
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# cd /Users/Sonya/Documents/backup_070224/Sonya_0xD62A4F84_SECRET.asc
bash: cd: /Users/Sonya/Documents/backup_070224/Sonya_0xD62A4F84_SECRET.asc: No such file or directory
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# cd /Users/Sonya/Documents/backup_070224
bash: cd: /Users/Sonya/Documents/backup_070224: No such file or directory
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls
$Recycle.Bin  $WINDOWS.~BT  'Documents and Settings'  DumpStack.log.tmp  hiberfil.sys  pagefile.sys  PerfLogs  ProgramData  Program Files  Program Files (x86)  Recovery  swapfile.sys  System Volume Information  Users  Windows
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# cd Users
bash: cd: Users: No such file or directory
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# cd Users
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users# ls
'All Users'  Default  'Default User'  desktop.ini  Public  Sonya
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users# cd Sonya
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya# cd Documents
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya/Documents# ls
desktop.ini  'My Music'  'My Pictures'  'My Videos'
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya/Documents# cd backup_070224
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya/Documents/backup_070224# ls
backup  'areas of interest.png.gpg'  'BitLocker Recovery Key 139F76F0-FBF6-499F-8A09-E76C9A337A82.TXT.gpg'  MD5.txt  checksum  keys  logs  list  MSFT-Windows11-Security-book_Sept2023.pdf.gpg  Sonya_0xD62A4F84_SECRET.asc  temp.txt  the_list.txt.gpg
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya/Documents/backup_070224# cp Sonya_0xD62A4F84_SECRET.asc
cp: missing destination file operand after 'Sonya_0xD62A4F84_SECRET.asc'
Try 'cp --help' for more information.
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya/Documents/backup_070224# cp Sonya_0xD62A4F84_SECRET.asc /home/cmp209/Desktop/cases/CrypticWilds/encrypted
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive/Users/Sonya/Documents/backup_070224# cd /home/cmp209/Desktop/cases/CrypticWilds/encrypted
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted# ls -lah
total 16K
drwxr-xr-x  2 root   root   4.0K Apr 16 13:23 .
drwxrwxr-x 10 cmp209 cmp209 4.0K Apr 15 09:02 ..
-rwxr-xr-x  1 root   root    903 Apr 16 13:23 Sonya_0xD62A4F84_SECRET.asc
-rw-r--r--  1 root   root    963 Apr 16 13:11 sonya_key.asc
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted# MD5sum Sonya_0xD62A4F84_SECRET.asc
MD5sum: command not found
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted# md5sum Sonya_0xD62A4F84_SECRET.asc
20fdd350b24ac1482cb38c613e28f15f  Sonya_0xD62A4F84_SECRET.asc
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted#
```

Result:

/Users/Sonya/Documents/backup_070224/Sonya_0xD62A4F84_SECRET.asc
md5sum Sonya_0xD62A4F84_SECRET.asc 20fdd350b24ac1482cb38c613e28f15f
MD5 hash of key: 20fdd350b24ac1482cb38c613e28f15f

Figure G.3.4 - Use of password and key to decrypt files 2025/04/15, Investigator JB

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted# sudo gpg --import Sonya_0xD62A4F84_SECRET.asc
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key B87EBB6DD62A4F84: public key "Sonya <sonyamacoit@outlook.com>" imported
gpg: key B87EBB6DD62A4F84: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted#
```

MD5 + Result:

e3244bdc3562c11fc47409333cb14630 areas of interest.png.gpg
a3fe5ec5adbf25bbe2ae1a1eb2955649 BitLocker Recovery Key 139F76F0-FBF6-499F-8A09-E76C9A337A82.TXT.gpg
0fb3d391d4a8de74d6527f43803ef7fc distsigkey.gpg
781cfdad9a2553d9105991a40ed5cadd MSFT-Windows11-Security-book_Sept2023.pdf.gpg
d16618639a238cf3380e028a5fc37496 pubring.gpg
dd48ed76ce8208a52e5207a5fe3d0473 secring.gpg
d84f0d074a9206e1ceca54cd13e90610 the_list.txt.gpg
855eda2bc6d2657831967a5c06077121 trustdb.gpg

Figure G.3.5.1 - Key legitimacy, key is not certified with a trusted signature for all files in question 2025/04/15, Investigator JB

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted# gpg -d areas\ of\ interest.png.gpg > areas\ of\ interest.png
gpg: encrypted with 255-bit ECDH key, ID 51A14908A84BA35F, created 2024-02-20
      "Sonya <sonyamacoit@outlook.com>"
gpg: Signature made Tue 20 Feb 2024 09:21:25 GMT
gpg:                using EDDSA key F882AC885E2A4CCBD56ADC78B87EBB6DD62A4F84
gpg: Good signature from "Sonya <sonyamacoit@outlook.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: F882 AC88 5E2A 4CCB D56A  DC78 B87E BB6D D62A 4F84
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/encrypted#
```

Contetnt:
gpg –d areas\ of\ interest.png.gpg > areas\ of \ interest.png
encrypted with 255-bit ECDH key, ID 51A14908A84BA35F, created 2024-02-20
“Sonya <sonyamacoit@outlook.com>”
Signature made Tue 20 Feb 2024 09:21:25 GMT
using EDDSA key F882AC885E2A4CCBD56ADC78B87EBB6DD62A4F84
Good signature from ”Sonya <sonyamacoit@outlook.com>” [unknown]
Warning: this key is not certified with a trusted signature!
There is no indication that the signature belongs to the owner.
Primary key fingerprint: F882 AC88 5E2A 4CCB D56A DC78 B87E BB6D D62A 4F84

Figure G.3.5.2 - Key legitimacy, importing Sonya’s public key from her e-mails (F.2.1), Investigator JB

```
cmp209@cmp209-virtual-machine:~/Desktop$ gpg --import sonya_key.asc
gpg: invalid armour header: mDMEZdRsVxYJKwYBBAHaRw8BAQdA0gQxeiyJQO5yewv31h6F1b2r4eT6Wy/zZ7F0 EJ1YydW0H1NvbnlhIDxzb255YW1hY29pdEBvdXRsb29rLmNvbT6ImQQTFgoAQRYh BPiCrIheKkzL1WrceLh+u2
3WKk+EBQJl1GxXAhsDBQkFpRPpBQsJCAcCAiICBhUK CQgLAgQWAgMBAh4HAheAAAoJELh+u23WKk+EUOcA/RHJHGpCKJIxwtzMOVOHzmVx uL+J4awgdarGafSlQ28aAQDCE7yziBh5hlhXHCFPfhlHDWPifS91loy6c9Rtcww6 Bbg4BGX
UbFcSCisGAQQBl1UBBQEBB0D/dbTzMsqI89osBh70y7L1FnpcojFGK2Hu eJiwKg0TRgMBCAeIfgQYFgoAJhYhBPiCrIheKkzL1WrceLh+u23WKk+EBQJl1GxX AhsMBQkFpRPpAAoJELh+u23WKk+EYEEA/R9qEnlZc/WtaB35+sMAZKR6g
QFU3g2S bbRPOcWMRYjVAP9dmZLzb18tbeq4DI3pBhqgQLW/Fx/kOEKPYIX6Mc77Ag== =f2kz -----END PGP PUBLIC KEY BLOCK----- \n
gpg: key B87EBB6DD62A4F84: public key "Sonya <sonyamacoit@outlook.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Content:
gpg --import sonya_key.asc

gpg: invalid armour header: mDMEZdRsVxYJKwYBBAHaRw8BAQdA0gQxeiyJQO5yewv31h6F1b2r4eT6Wy/zZ7F0 EJ1YydW0H1NvbnlhIDxzb255YW1hY29pdEBvdXRsb29rLmNvbT6ImQQTFgoAQRYh BPiCrIheKkzL1WrceLh+u23WKk+EBQJl1GxXAhsDBQkFpRPpBQsJCAcCAiICBhUK CQgLAgQWAgMBAh4HAheAAAoJELh+u23WKk+EUOcA/RHJHGpCKJIxwtzMOVOHzmVx uL+J4awgdarGafSlQ28aAQDCE7yziBh5hlhXHCFPfhlHDWPifS91loy6c9Rtcww6 Bbg4BGXUbFcSCisGAQQBl1UBBQEBB0D/dbTzMsqI89osBh70y7L1FnpcojFGK2Hu eJiwKg0TRgMBCAeIfgQYFgoAJhYhBPiCrIheKkzL1WrceLh+u23WKk+EBQJl1GxX AhsMBQkFpRPpAAoJELh+u23WKk+EYEEA/R9qEnlZc/WtaB35+sMAZKR6gQFU3g2S bbRPOcWMRYjVAP9dmZLzb18tbeq4DI3pBhqgQLW/Fx/kOEKPYIX6Mc77Ag== =f2kz -----END PGP PUBLIC KEY BLOCK----- \n

gpg: key B87EBB6DD62A4F84: public key "Sonya <sonyamacoit@outlook.com>" imported

gpg: Total number processed: 1

gpg: imported: 1

Figure G.3.6.1 Decrypted Files, areas of interest.png 2025/04/15 MD5: f8eec9124db6a676470c40f6ca40dffa, Investigator JB

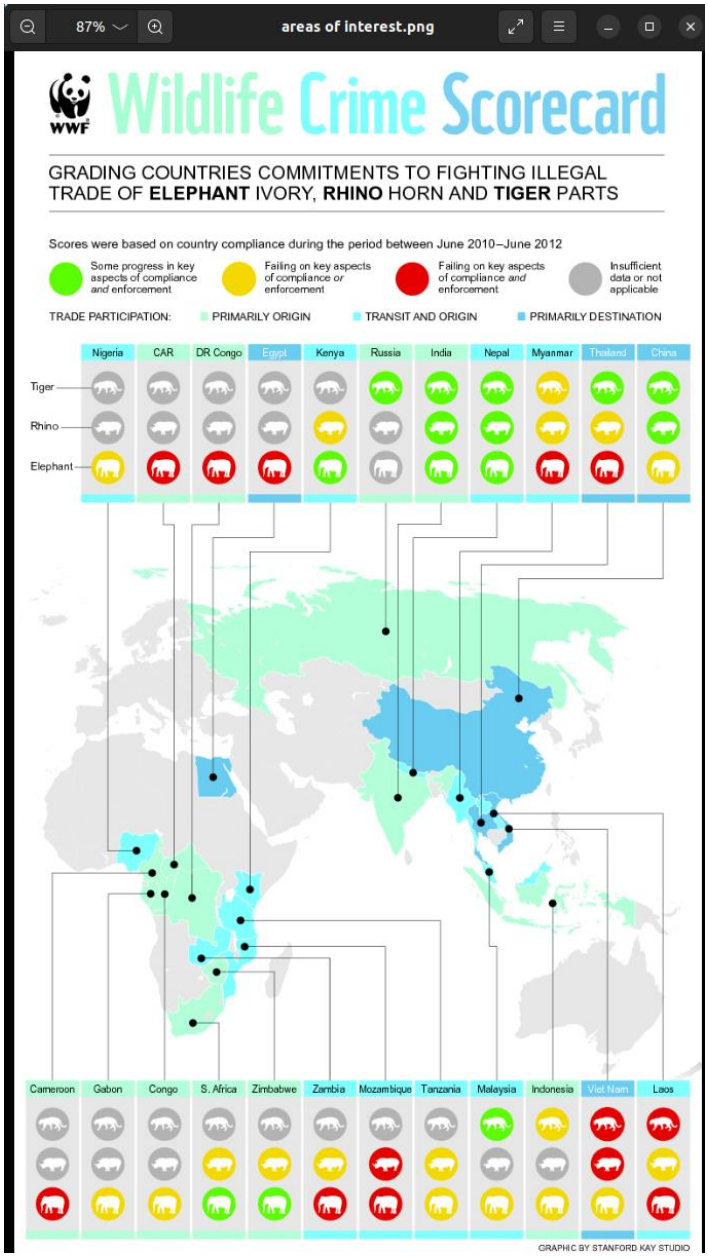


Figure G.3.6.2 Decrypted Files, BitLocker Recovery Key 139F76F0-FBF6-499F-8A09-E76C9A337A82.TXT 2025/04/15 MD5 554d5979bbfdb09a3e1f95a2b01d8412, Investigator JB

BitLocker Drive Encryption recovery key

To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value displayed on your PC.

Identifier:
F2B6A4D1-476B-4D34-B042-CF85EE59F370

If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.

Recovery Key:
1234-5678-9012-3456-7890-1234-5678-9012

Make sure to keep this key secure, as it's essential for recovering access to the encrypted drive.

Figure G.3.6.3 Decrypted Files, MSFT-Windows11-Security-book_Sept2023.pdf 2025-04-15 MD5 5d44fc2ab6495f9098b5922dbcd585b7

Figure G.3.6.4 Decrypted Files, the_list.txt 2025/04/15 MD5 0ac086cf8253eecbad614ffe4b068fac
Investigator JB

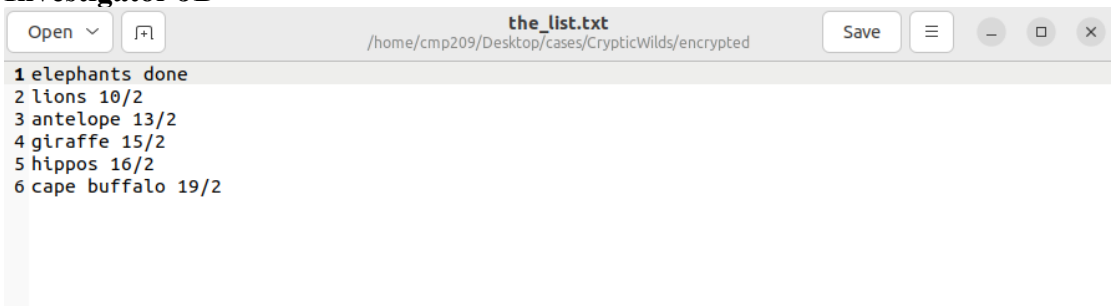


Figure G.4.1 FTK imager to mount USB 2025/04/22, Investigator JB

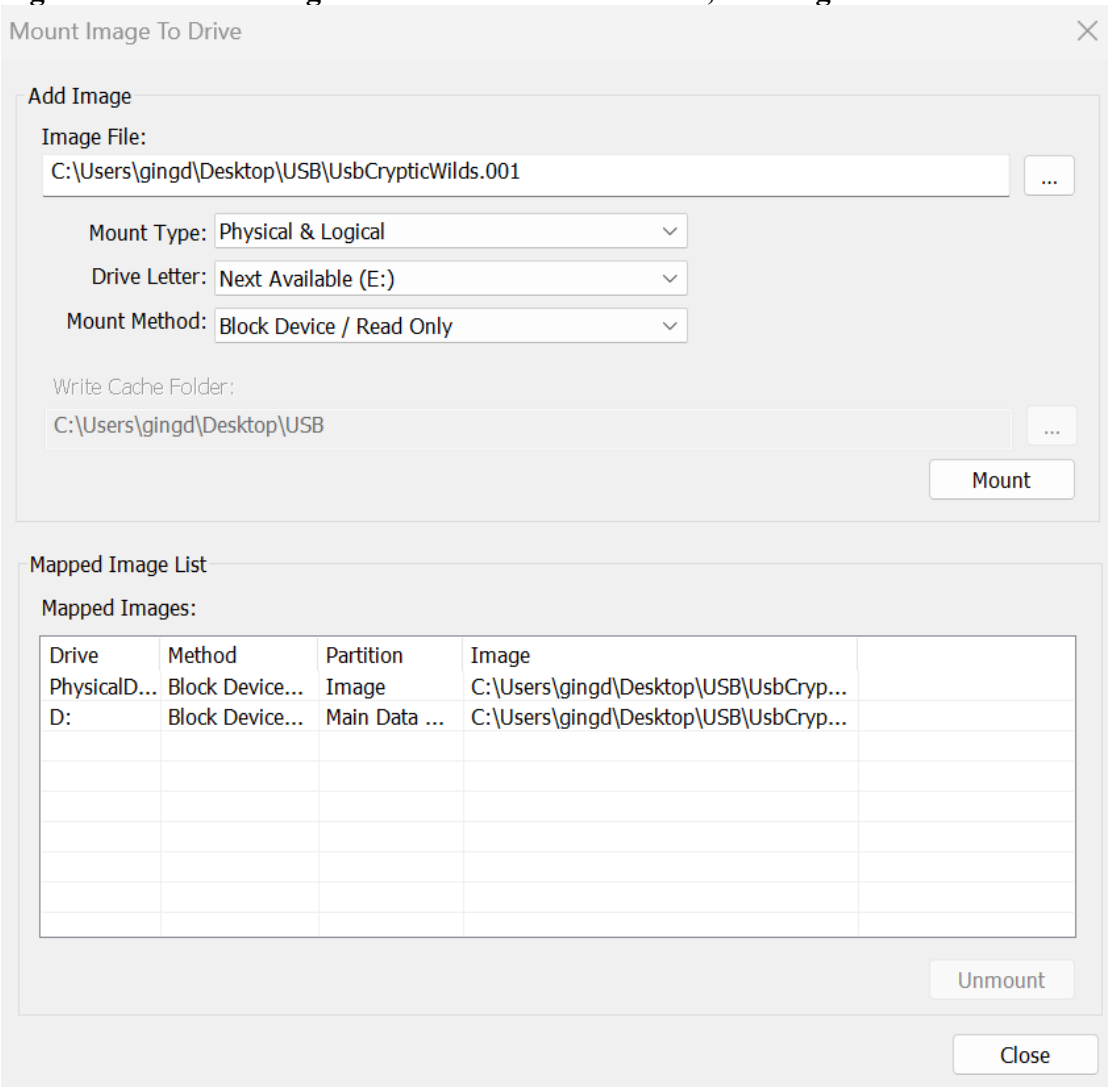


Figure G.4.2 BitLocker to access the encrypted USB 2025/04/22, Investigator JB

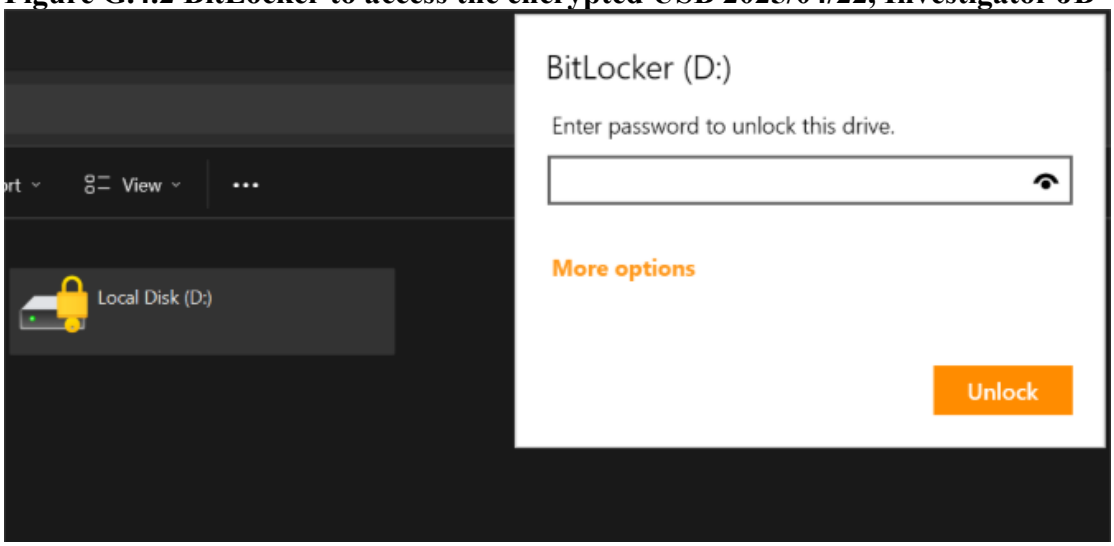
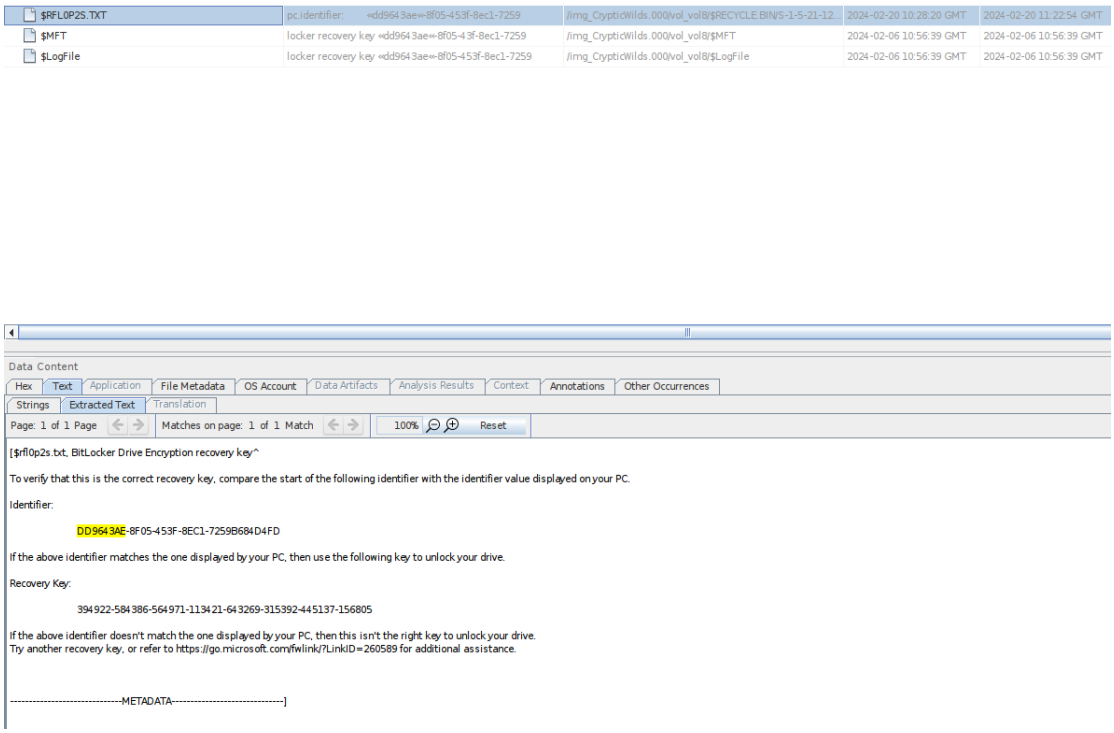


Figure G.4.3 BitLocker key to the encrypted USB recycled $RFL0P2S.TXT 20/02/2024 MD5 360014e451c4d0eb9105d0e491a4b03a, Investigator JB



$RFL0P2S.TXT	pc.identifier: «dd9643ae»-8f05-453f-8ec1-7259	/img_CrypticWilds.000/vol_vol8/$RECYCLE.BIN/S-1-5-21-12...	2024-02-20 10:28:20 GMT	2024-02-20 11:22:54 GMT
$MFT	locker recovery key «dd9643ae»-8f05-43f-8ec1-7259	/img_CrypticWilds.000/vol_vol8/$MFT	2024-02-06 10:56:39 GMT	2024-02-06 10:56:39 GMT
$LogFile	locker recovery key «dd9643ae»-8f05-453f-8ec1-7259	/img_CrypticWilds.000/vol_vol8/$LogFile	2024-02-06 10:56:39 GMT	2024-02-06 10:56:39 GMT

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Extracted Text | Translation

Page: 1 of 1 Page | Matches on page: 1 of 1 Match | 100% | Reset

[$rfl0p2s.txt, BitLocker Drive Encryption recovery key^

To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value displayed on your PC.

Identifier:

DD9643AE-8F05-453F-8EC1-7259B684D4FD

If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.

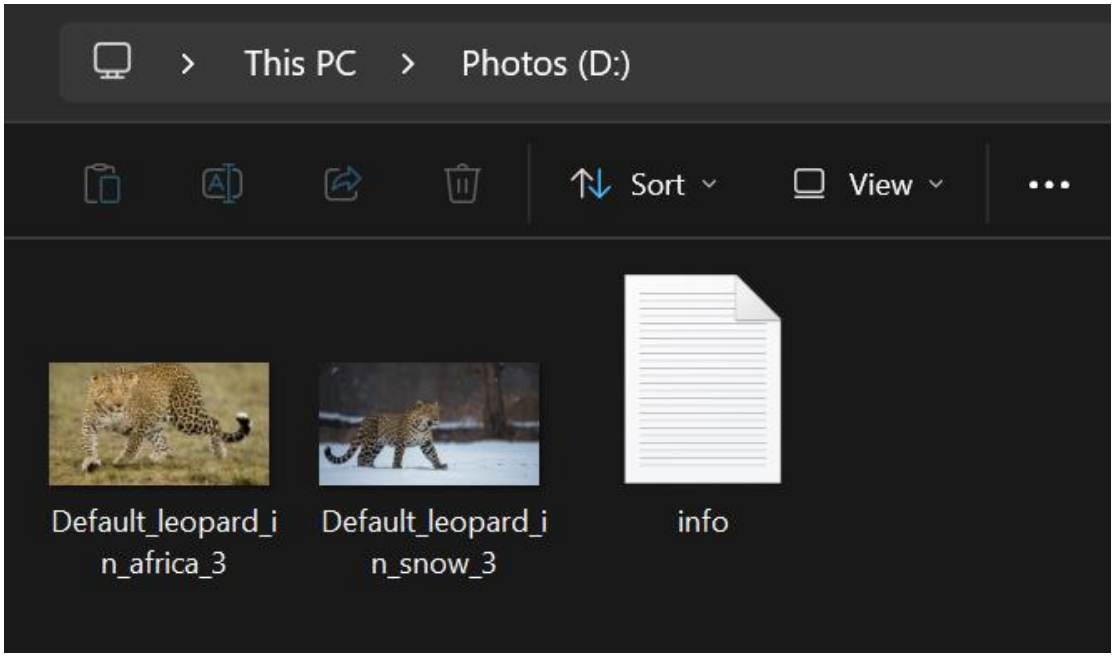
Recovery Key:

394922-584386-564971-113421-643269-315392-445137-156805

If the above identifier doesn't match the one displayed by your PC, then this isn't the right key to unlock your drive.
Try another recovery key, or refer to https://go.microsoft.com/fwlink/?LinkID=260589 for additional assistance.

----------METADATA----------]

Figure G.4.4 USB contents decrypted 2024/04/22, Investigator JB



The above are Figure A.1.1, A.1.2 and B.1.1

Appendix H

In order of appearance in the document, Investigator JB, 181 files recorded.

Name	MD5	Description	Reason
CrypticWilds.000.raw	aebd2d140eaf215e1a8554d008c5e2b3	Sonya's fused hdd drive	In order to mount the drive it had to be fused

Default_leopard_in_africa_3.jpg	011bc454f1282daab265cfc644a12f72	Image of a leopard	USB was mounted to view files inside due to BitLocker
Default_leopard_in_snow_3.jpg	835760d0130e3dcd835d0945266b77e7	Image of Amur leopard	USB was mounted to view files inside due to BitLocker
sonya.jpg	df57f81e1ae46fe77805cf4ea761ec7f	Image of a woman	Name matches Sonya
hippo.jpg.bak	5871e00fba511d4c9e5781e3cca2b308	Image of a hippo	Image of a safari animal
Default_group_of_hippos_in_a_river_2.jpg.bak	1b8a46b697020ee54ade65c42cd07921	Image of a hippo	Image of a safari animal
Default_hippos_in_river_0.jpg.bak	7f1ba93f9911233ed79a9a1e98e14506	Image of a hippo	Image of a safari animal
Default_hippos_in_river_1.jpg.bak	74536d2bb3fb44b073dc6497e97cc848	Image of a hippo	Image of a safari animal
in_a_river_staring_at_the_photographer_2.jpg.bak	e876580e755018d288332le2d602ellf	Image of a hippo	Image of a safari animal
charging_the_photographer_2.jpg.bak	13345332d599c4605c6dd2213c9ecfd91	Image of a hippo	Image of a safari animal
Default_hippos_in_a_river_2.jpg.bak	d0ef6d607f390712a1bc07b2921e994a	Image of a hippo	Image of a safari animal
Default_hippo_in_a_river_2.jpg.bak	84287c7f6d4b11bdac3e785687a7f0b5	Image of a hippo	Image of a safari animal
mouths_open_0.jpg.bak	d2f312302836cb53db4a8f66db1f5dd	Image of a hippo	Image of a safari animal
river_hippo.jpg.bak	10b7a64e831e512663b3769febb21c8c2	Image of a hippo	Image of a safari animal
hippos_in_rivers.jpg.bak	a140a23aa7c50ff8409088634927c7c4	Image of a hippo	Image of a safari animal
water_buffalo.jpg.bak	ce16e54d41fe4026b7cb8f6b0ad21396	Image of a buffalo	Image of a safari animal
next_to_water_view_from_a_distance_correc_0.jpg.bak	eabfbae9b447ff337226f6a3350ff32a	Image of a buffalo	Image of a safari animal
drinking.jpg.bak	ece19ec64af2073cc44bf1fe18203968	Image of a buffalo	Image of a safari animal
buffalo_1.jpg.bak	99c4914720fb32435ebf1cca5a3183a5	Image of a buffalo	Image of a safari animal
looking_around.jpg.bak	6e1ebf277f6898e92197258a7c473ba	Image of a buffalo	Image of a safari animal

87.jpg.bak	6dc6b51d7a7592887e443867f46fc252	Image of a buffalo	Image of a safari animal
3.jpg.bak	30130a14347a238b941ee3ead85d1dec	Image of a buffalo	Image of a safari animal
9777.jpg.ba	467e6aafcbc164c67dfe6252d7dc2d3	Image of a buffalo	Image of a safari animal
987.jpg.bak	e6eb7262afe3ad5ced31ced63c0a7c349	Image of a buffalo	Image of a safari animal
from_a_distance_1.jpg.bak	6a69bbffd2bfb3ac3d3168e0bdc126e7	Image of a buffalo	Image of a safari animal
in_field.jpg.bak	92fb822098b66ad66a8718c885f81abb	Image of a buffalo	Image of a safari animal
6543.jpg.bak	61d73d931f49f259db46b06fe0e04dc2	Image of a buffalo	Image of a safari animal
buaffalo_and_bird.jpg.bak	1528f1835a80aefeac9254b13cce318a	Image of a buffalo	Image of a safari animal
long_grass.jpg.ba	60defcbbd50ff9611087af9b6dbd98e8	Image of a buffalo	Image of a safari animal
f_0000ed	0ecc6ebb305902492103304b2e1cf2f1	Image of a man	Taken with canon Eos r5
01409656.jpg		Image of a lion	Image of a safari animal
F0733352.jpg	649f9d7791702c23b07356038f75efd	Image of a lion	Image of a safari animal
afternoon_hunt_2.jpg	9a0bcda8538294635542e7af87517619	Image of an antelope	Image of a safari animal
08218640.jpg		Image of an antelope	Image of a safari animal
01664296.jpg		Image of an antelope	Image of a safari animal
114028.png	1a53d9d9f1b1ac36e90a89f5a0f41de3	Image of flight tickets	Relevant to Sonay's location
elephant_in_water.jpg	555182b1d00d5940c9769225fa56e63e	Image of an elephant	Image of a safari animal
elephant_recon_close_call.png	0fed5b1307b462368e846c0155852d92	Image of an elephant	Image of a safari animal
elephant_crossing_road.jpg	09a71ecad91b3f7c2c632e99e1e67246	Image of an elephant	Image of a safari animal
viewing_herd_of_elephants_0.jpg	1dca861cc081c16d682c2253f13412d5	Image of an elephant	Image of a safari animal

elephant_family.jpg	9cb0bcee417ee0b4e4decb8e8b075c53	Image of an elephant	Image of a safari animal
aerial_1.jpg	f6fef39f0568ebac240ec2189bfbfdf7	Image of an elephant	Image of a safari animal
close-up.jpg	b2c3146c2710750da3619bb27266da60	Image of an elephant	Image of a safari animal
elephant_in_river.jpg	a64f06fbd43fcabd323e4c3cfdc21a6c	Image of an elephant	Image of a safari animal
elephant_trunk.jpg	b9250ce2889c19fa1c437f3d36f1bbaf	Image of an elephant	Image of a safari animal
hunting_scene_viewed_from_1.jpg	b7306c6b4d28c73d355f4b8bc6288a79	Image of an elephant	Image of a safari animal
hunting_scene_viewed_from_a_helicopter_wi_2.jpg	2c8eb3b6698512b297d99c01a4125fb5	Image of an elephant	Image of a safari animal
elephant_chasing_lion.jpg	64a9f9d7791702c23b07356038f75efd	Image of elephant and a lion	Image of safari animals
lions_in_road_1.jpg	15f06c8ceef72620a812c527aeffb7aa	Image of a buffalo	Image of a safari animal
lions_on_boulder.jpg	86fd53c52b794c10dabdcd26ea1a9f2f	Image of a buffalo	Image of a safari animal
puzzled_look.jpg	49ace06ebc37dc56b3af74845f9df18e	Image of an antelope	Image of a safari animal
anteplope_horns.jpg	519c98b171efc7a274a8a9c21eeb107	Image of an antelope	Image of a safari animal
grassland_morning.jpg	grassland_morning.jpg	Image of an antelope	Image of a safari animal
solo_male.jpg	5afd9eac478cf059e49670064bbe1a0	Image of an antelope	Image of a safari animal
smiling_zebra.jpg	19cb35a60d3a16fbe515c8662e6ed5fa	Image of a zebra	Image of a safari animal
tired.jpg	554561262d6f548d6a2b8f7df00d9fbd	Image of an antelope	Image of a safari animal
trotting_away.jpg	f54d7d372d0ab0a77c882e4709b4822c	Image of an antelope	Image of a safari animal
two_together.jpg	8852973ec345fc4221a0e29e016e0326	Image of an antelope	Image of a safari animal
zebra_on_road.jpg	caa8d1b1b366c92f1018fd8d56e1776e	Image of an antelope	Image of a safari animal
afternoonhunt.jpg	555921f976beb99004c27a8abdaacc9	Image of an antelope	Image of a safari animal
zebra_herd.jpg	ca0f55bdb74d3c8d14ca12366c9de8e3	Image of a zebra	Image of a safari animal

antalope_223.lpg	c63e6b0434eca09c8c40d16393ac0fcf	Image of an antelope	Image of a safari animal
afternoon_hunt_2.jpg	9a0bcda8538294635542e7af87517619	Image of an antelope	Image of a safari animal
hunting.jpg	fc8692ccc6ca2dd28827cc2153fb00f4f	Image of an antelope	Image of a safari animal
internet_pic.jpg	044d476cd3c9338c014eab97f0c9676b	Image of an antelope	Image of a safari animal
lying_down.jpg	1fe6d96a49d68a291b8355a033bad79a	Image of an antelope	Image of a safari animal
midmorning.jpg	a9abc066f4fe0b5db8ab07cfa2e64933	Image of an antelope	Image of a safari animal
close_to_tree.jpg	36970ec4633ea3d31409d13d9f7c3d6c	Image of a Giraffe	Image of a safari animal
more_water.jpg	24d55462cd01f8b863706ed14f6fcd0e	Image of a Giraffe	Image of a safari animal
distant_looks.jpg	ee4300958c165595fd68225bf91c8bef	Image of a Giraffe	Image of a safari animal
open_field.jpg	35a17ff1f8d81e764bba9ff07a3a8b68	Image of a Giraffe	Image of a safari animal
hungry_giraffe.jpg	b40b000c7af2013037b7725601119dab	Image of a Giraffe	Image of a safari animal
toy.webp	680854168f1030fab935c9a2a46d8584	Image of a toy Giraffe	Image of a safari animal
interested.jpg	4ca3f02353b48d9f39367d47171cbb9d	Image of a Giraffe	Image of a safari animal
water_giraffe.jpg	2c3237ad2311da5001da99d10712e522	Image of a Giraffe	Image of a safari animal
distant_in_trees.jpg	fae5bd39725b8c2d104463d38545c2fb	Image of a Giraffe	Image of a safari animal
herd_photo.jpg	8a3833ac61f0a74da85f635542702080	Image of a Giraffe	Image of a safari animal
herd_photo_2.jpg	d4aaf0fe7051b6749586770e4f65d2ae	Image of a Giraffe	Image of a safari animal
large_giraffe.jpg	280173a2bb761b81bdf063b27ddbfc8a	Image of a Giraffe	Image of a safari animal
next_to_thorntree.jpg	9191e075b2a22b086c63ce4530e34d6d	Image of a Giraffe	Image of a safari animal

through_trees.jpg	2e7bbd714d5d0e401f84e01afac8b97b	Image of a Giraffe	Image of a safari animal
lion_at_watering_hole.jpg	6ef3823e1791833b3999cc26b3fb9c1e	Image of a Lion	Image of a safari animal
lion_charging.jpg	15fd9c90ddbff0460903a688d5aa6532	Image of a Lion	Image of a safari animal
tree_lions_1.jpg	b1d5774f273763449e6a64b5168f3f2e	Image of a Lion	Image of a safari animal
tree_lions_2.jpg	de113f884880b66e897d3dca944c077f	Image of a Lion	Image of a safari animal
lions_in_road_1.jpg	6ea94f66a42040e43fb5c6eb1f534daf	Image of a Lion	Image of a safari animal
lions_in_road_2.jpg	d94e971d09ba6c677429243d0718285e	Image of a Lion	Image of a safari animal
lions_on_boulder.jpg	80cdd4a51f977ff23c31320b3cb4389a	Image of a Lion	Image of a safari animal
two_lions_charging.jpg	3c1f956208be51d80adee742423a92f4	Image of a Lion	Image of a safari animal
hippo_vid.mp4	5102b7ceb169b01a6c2ab984c34bf7fe	Video of a hippo	Image of a safari animal
hippos_in_rivers.jpg	e0359f370b8aaea0af75a3832c6452f1	Image of a hippo	Image of a safari animal
Default_group_of_hippos_in_a_river_2.jpg	277bafd400e0f11f1eb2080c876af5a6	Image of a hippo	Image of a safari animal
mouths_open_0.jpg	6f15b150f30ca49274d0dec22420eeb9	Image of a hippo	Image of a safari animal
Default_hippos_in_a_river_2.jpg	b86b3fbef80119081d5323878805a17f	Image of a hippo	Image of a safari animal
staring_at_the_photographer_3.jpg	0c5850f0d5b23fb59d8cda3ea08e8f8b	Image of a hippo	Image of a safari animal
Default_hippos_in_river_1.jpg	564b8d9809b134f7cd77bafc413e5031	Image of a hippo	Image of a safari animal
with_mouth_open_2.jpg	97eb1b490ee3e80d5bf6e49c2e9d1256	Image of a hippo	Image of a safari animal
charging_the_photographer_2.jpg	9113be25f355e07c7312769f53f84900	Image of a hippo	Image of a safari animal
Default_hippo_in_a_river_2.jpg	9c6f6a701733d25840cd266a27746be6	Image of a hippo	Image of a safari animal
Default_hippos_in_river_0.jpg	79b8dba8b4c2f8fde074b73ce7eb1671	Image of a hippo	Image of a safari animal
hippo.jpg	87f03d334c7c638aea2c282cdfecac79	Image of a hippo	Image of a safari animal

in_a_river_staring_at_the_photographer_2.jpg	34009bba49220a5a7b244aacee852157	Image of a hippo	Image of a safari animal
river_hippo.jpg	6349a9e0fe3b49036c433d046c4f1972	Image of a hippo	Image of a safari animal
buaffalo_and_bird.jpg	7fc43547bca52fd8cbc109a460b9c833	Image of a buffalo	Image of a safari animal
short_grass.jpg	beeb3de6f512b3f041ab26d5efe4f04b	Image of a buffalo	Image of a safari animal
buffalo_1.jpg	278b1f9d78c146ebcc1b581bdd254622	Image of a buffalo	Image of a safari animal
water_buffalo.jpg	82085b4833d0732e62b08086c48e7366	Image of a buffalo	Image of a safari animal
drinking.jpg	33bd1b1ae26a105ed36b856497261db8	Image of a buffalo	Image of a safari animal
3.jpg	5a33ad7a7ef8d5435957dd7fd1f3d13e	Image of a buffalo	Image of a safari animal
in_field.jpg	e150ef1c4176c3fd6ec8a610f4db42b3	Image of a buffalo	Image of a safari animal
9777.jpg	aa44ec9d33c36d3c5159a206433e1ffa	Image of a buffalo	Image of a safari animal
looking_around.jpg	1fdf4062ecb5128dd4a3afaeb733f3ad	Image of a buffalo	Image of a safari animal
6543.jpg	6c4e98deb295832c32ce2c012e9535bd	Image of a buffalo	Image of a safari animal
87.jpg	108231d6ded1468564d65c8bb89209a3	Image of a buffalo	Image of a safari animal
987.jpg	93d21058e7830178e5edebebbf715873	Image of a buffalo	Image of a safari animal
from_a_distance_1.jpg	c6c3b5acc88bfaa8771b680e5af9ff91	Image of a buffalo	Image of a safari animal
data_2__b1020198.jpg	c5ac0bf09e40512c08c0b163d0578574	Image of an elephant	Image of a safari animal
data_2__b202019c.jpg	7991152e15ba0d2a10bda9016d81769c	Image of an elephant	Image of a safari animal
data_2__b2020194.jpg	3849dfabd48a2f506366328a54df593f	Image of a safari animal	Image of a safari animal
data_2__b20201a0.jpg	1e1ca6509c16ad5a502e4edb4180ebc0	Image of three hunters	Could depict poaching

data_2__b20201b0.jpg	b229f3831e81e68ed91303564926172 8	Image of two hunters	Could depict poaching
data_2__b20201a8.jpg	e272bf4f68332ef3b9f8f9b4ee9be399	Image of two hunters	Could depict poaching
data_2__b20202b0.jpg	57be6dba4e2fc14d7b1715159992b83c	Image of an antelope	Image of a safari animal
data_2__b10202ce.jpg	8ebd837d505d9fae7f85208710e51fe0	Guns	Image of hunting rifles
data_2__b10202c4.jpg	396baf8295a28e87fb7428c203764438	Image of hunter and dead elephant	Could depict poaching
data_2__b10202ca.jpg	7f5a6066cab57eaca0097458e951175d	Image of a dead elephant	Could depict poaching
f_000074.jpg	957fb61dff22ac2acb5c0de54c9fcfa1	Image of a dead elephant and a gun laying beside it	Could depict poaching
data_2__b30202d4.jpg	8b08891f6c78d7353b8fd3120f3556e9	Image of a dead buffalo with hunter standing over it	Could depict poaching
data_3__c1030224.jpg	6338107bdc292435a127902c7d3c94ab	Image of an arrow head	Relates to search history
f_001e9.jpg	b a79461201627f766f4244036a7bbe28	Image of a tiger	Image of a safari animal
F0001d0.webp	1a53d9d9f1b1ac36e90a89f5a0f41de3	Severed rhino heads	Could depict poaching
f_0001ef.jpg	cc522b2eb57ceb375c58c45a0b0571b1	Image of a rhino horn	Could depict poaching
f_0001f0.jpg	cf68370a9490c5b1ad64e704db1a47c6	Image of an elephant	Image of a safari animal
f_0001f3.webp	f6885c5e28fe5350461e4be9781a49b4	Image of a tiger	Image of a safari animal
f_0001f5.webp	d84246d1430b83bdbf270cd0a4474655	Image of a rhino	Image of a safari animal
f_000203.jpg	ca792ed358b2b0af88a04b93c0aa7636	Image of hyenas	Image of safari animals
f_000207.webp	2 f8c98cf98e035eb1bfe02ce5d38daf9	Image of a pangolin	Image of a safari animal
data_2__b1020ca8.jpg	318eedc29962f5c88d3a9be6ac80aee9	Image of a lion	Image of a safari animal

data_2__b3020d48.jpg	2fcf8d7ce79b54a19c74564f1cb601b5	Image of a leopard	Image of a safari animal
f_000328.png	349bfee5521fd0d1cbe3ba46ffcad111	Image o coordinates to leopard lookout	Relates to web artifacts
data_3__c1031d80.jpg	a3ed10bbc81b5fede2c37d8e3072be23	Image of a giraffe	Image of a safari animal
f_00033a.png	53d763fee396c2a43ba9ae6442e0d0ad	Image of coordinates to leopard observation point	Relates to web artifact
f_00033e.jpg	b6475afb8f4dce3d3be5fa2371622776	Image of a leopard	Image of a safari animal
info.txt	92b0388c082310fddc4d9c57fe098e78	File from USB	Recovered from an encrypted drive
mykeypass_seized.txt	5319fbf7b92cba7d9a090717f5fd06c7	SHA1 key pass	Recovered from Sonya
UsbCrypticWilds.001.txt	e81d4963f46737c46a7aca78c633761e	Audit of USB	Provided by Officer
UsbCrypticWilds.001	a547247ee2fd3f51182f28c273633fc4	USB segment	Contains the encrypted USB
History	602e46cb905ee91c55032a1d37ad435a	Edge history file	Contains the full edge history
History	9ef8df1315fb383db4c10bb4ea900d74	Chrome history file	Contains the full chrome history
Cookies	7900290d6b9540601383db1bbf1496c7	Edge cookies file	Contains the full Edge cookies
inbox	f1f120700ff977e60912be456cf6197c	Sonya's inbox	Contains e-mail history for received e-mails
sent	6c18323e5251a908932d1e5d901a9777	Contains public key for verification	Allows us to see if Sonya personally encrypted files, as well as all sent e-mails
$86YIEM.zip	6dcd891c62978d83df3c026f6ad0fbd9	Steghide.zip in recycling	Evidence of download
Shell bag artifact steghide	e119d03c028c58cc9df67b389b38c76a	Records presence of steghide in files	Evidence of download
Kleopatra.lnk	b83fbc61fad188bced4a735091918118	Link file for gpg encryption software	Evidence of download
Run program artifact Kleopatra	3ee892d7a49816e948494c45a4ff373	Shows program was run	Evidence of anti-forensic usage

Kleopatrarc	c7e20b6c681fffee4d44fb7d881f5a6	Settings for Kleopatra	Evidence of usage
areas of interest.png	f8eec9124db6a676470c40f6ca40dffa	Decrypted file for areas of interest .png	Decrypted files from USB
BitLocker Recovery Key 139F76F0-FBF6-499F-8A09-E76C9A337A82.TXT	554d5979bbfdb09a3e1f95a2b01d8412	Fake BitLocker recovery key	Decrypted files from USB
MSFT-Windows11-Security-book_Sept2023.pdf	5d44fc2ab6495f9098b5922dbcd585b7	Windows 11 security hand book	Decrypted files from USB
the_list.txt	0ac086cf8253eecbad614ffe4b068fac	Text file containing references to animals	Decrypted files from USB
$RFL0P2S.TXT	360014e451c4d0eb9105d0e491a4b03a	Recycled BitLocker key for encrypted USB	Used to Decrypted files from USB
Photos_searcher.cpp	d46bb9cbaf42c2ce32c323843ae4b9b1	Custom c++ script to find relevant photos	Created to automate file discovery
hash_cracker_SHA1.sh	d46bb9cbaf42c2ce32c323843ae4b9b1	Custom bash script to crack SHA1 encoded passwords	Created to automate password cracking
System log (USB)	84199d2ea6fa634e9a867fcb67cee035	Incident of Encrypted USB being used	Evidence of all USBs in use by Sonya

Appendix I Miscellaneous

Times listed are those of file creation, unless otherwise stated

Figure I.1.1 - Custom photo carving script written in C++ 2025/02/25, Investigator JB MD5 d46bb9cbaf42c2ce32c323843ae4b9b1

photos_searcher.cpp

photos_searcher | (Global Scope) | main()

```cpp
#include <iostream>
#include <iostream>
#include <fstream>
#include <sstream>
#include <string>

int main()
{
    std::ifstream input("photos.txt");
    std::string line;
    std::string last_line;
    std::string output = "";
    const int lines_interesting = 3;
    int counter = 0;

    while (std::getline(input, line))
    {
        if (counter > 0) {
            if (line[0] == '=') {
                counter = 0;
            }
            else {
                output += line + " \n";
                counter--;
            }
        }
        if (line == "Camera Model Name                : Canon EOS 30") {
            output += last_line + " \n";
            output += line + " \n";
            counter = lines_interesting;
        }

        last_line = line;
    }

    std::cout << output;
}
```

Figure I.1.2 - Custom photo carving script output 2025/02/25, Investigator JB

======== 00982904.jpg

Camera Model Name : Canon EOS 30

File Name : 00982904.jpg

Artist : thescout

Date/Time Original : 2024:02:10 14:58:00

======== 01409656.jpg

Camera Model Name : Canon EOS 30

File Name : 01409656.jpg

Artist : thescout

Date/Time Original : 2024:02:10 14:00:00

======== 05517344.jpg

Camera Model Name : Canon EOS 30

File Name : 05517344.jpg

Artist : thescout

======== 05918136.jpg

Camera Model Name : Canon EOS 30

File Name : 05918136.jpg

Artist : thescout

======== 07885168.jpg

Camera Model Name : Canon EOS 30

File Name : 07885168.jpg

Artist : thescout

Date/Time Original : 2024:02:13 13:06:00

======== 08607800.jpg

Camera Model Name : Canon EOS 30

File Name : 08607800.jpg

Artist : thescout

======== 08638040.jpg

Camera Model Name : Canon EOS 30

File Name : 08638040.jpg

Artist : thescout

======== 09057096.jpg

Camera Model Name : Canon EOS 30

File Name : 09057096.jpg

Artist : thescout

======== 09193664.jpg

Camera Model Name : Canon EOS 30

File Name : 09193664.jpg

Artist : thescout

Date/Time Original : 2024:02:15 00:00:00

======== 09309864.jpg

Camera Model Name : Canon EOS 30

File Name : 09309864.jpg

Artist : thescout

======== 09371280.jpg

Camera Model Name : Canon EOS 30

File Name : 09371280.jpg

Artist : thescout

======== 09461024.jpg

Camera Model Name : Canon EOS 30

File Name : 09461024.jpg

Artist : thescout

======== 10024736.jpg

Camera Model Name : Canon EOS 30

File Name : 10024736.jpg

Artist : thescout

======== 10250032.jpg

Camera Model Name : Canon EOS 30

File Name : 10250032.jpg

Artist : thescout

Date/Time Original : 2024:02:13 13:06:00

======== 10394624.jpg

Camera Model Name : Canon EOS 30

File Name : 10394624.jpg

Artist : thescout

======== 10837200.jpg

Camera Model Name : Canon EOS 30

File Name : 10837200.jpg

Artist : thescout

======== 11539304.jpg

Camera Model Name : Canon EOS 30

File Name : 11539304.jpg

Artist : thescout

======== 13444776.jpg

Camera Model Name : Canon EOS 30

File Name : 13444776.jpg

Artist : thescout

======== 13982208.jpg

Camera Model Name : Canon EOS 30

File Name : 13982208.jpg

Artist : thescout

======== 13996256.jpg

Camera Model Name : Canon EOS 30

File Name : 13996256.jpg

Artist : thescout

======== 14160872.jpg

Camera Model Name : Canon EOS 30

File Name : 14160872.jpg

Artist : thescout

======== 16581208.jpg

Camera Model Name : Canon EOS 30

File Name : 16581208.jpg

Artist : thescout

======== 17263040.jpg

Camera Model Name : Canon EOS 30

File Name : 17263040.jpg

Artist : thescout

======== 17923808.jpg

Camera Model Name : Canon EOS 30

File Name : 17923808.jpg

Artist : thescout

Date/Time Original : 2024:02:15 00:00:00

======== 18829368.jpg

Camera Model Name : Canon EOS 30

File Name : 18829368.jpg

Artist : thescout

======== 18836376.jpg

Camera Model Name : Canon EOS 30

File Name : 18836376.jpg

Artist : thescout

======== 44232256.jpg

Camera Model Name : Canon EOS 30

File Name : 44232256.jpg

Artist : thescout

Date/Time Original : 2024:02:10 14:00:00

======== 47536064.jpg

Camera Model Name : Canon EOS 30

File Name : 47536064.jpg

Artist : thescout

Date/Time Original : 2024:02:15 00:00:00

======== 50492232.jpg

Camera Model Name : Canon EOS 30

File Name : 50492232.jpg

Artist : thescout

Date/Time Original : 2024:02:10 14:58:00

Figure I.1.3 - EXIF tool to extract all photos 2025/02/25, Investigator JB

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp/output_Tue_Feb_25_09_22_07_20root@cmp209-virtual-
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp/output_Tue_Feb_25_09_22_07_2025/jpg# exiftool -mo
del -filename -artist -datetimeoriginal *.jpg > photos.txt
```

Content:

exiftool –model – filename – artist – datetimeoriginal *.jpg > photoes.txt

Figure I.2.1 - Custom hash cracking script written in bash 2025/02/25, Investigator JB MD5 d46bb9cbaf42c2ce32c323843ae4b9b1

```bash
#!/bin/bash

# Path to files
file1Path="/home/cmp209/Desktop/input_hash.txt"
file2Path="/home/cmp209/Desktop/tools/SecLists-master/Passwords/Leaked-Databases/rockyou.txt"

# Get the hash value from the first file (we only need the first line)
compareValue=$(head -n 1 "$file1Path")

# Loop through each line of the second file
while IFS= read -r line; do
    # Calculate the SHA1 hash of the line
    lineSHA1=$(echo -n "$line" | sha1sum | awk '{ print $1 }')

    # Compare the hash with the value from the first file
    if [[ "$lineSHA1" == "$compareValue" ]]; then
        # Output the line if it matches
        echo "$line"
    fi
done < "$file2Path"
```

Figure I.2.2 - Custom hash cracking script output 2025/02/25, Investigator JB

```
cmp209@cmp209-virtual-machine:~/Desktop/tools$ chmod +x hash_cracker_SHA1.sh
cmp209@cmp209-virtual-machine:~/Desktop/tools$ ./hash_cracker_SHA1.sh
conservation
```

Figure I.3.1 - Alcor micro corp Flash Drive USB drive attachment records 2024/02/22, Investigator JB system config MD5 84199d2ea6fa634e9a867fcb67cee035

SYSTEM	0	2024-02-22 13:55:01 GMT	Alcor Micro Corp.	Flash Drive	15E12348	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	SanDisk Corp.	Cruzer Blade	0301982907052205443 6	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	VMware, Inc.	Virtual USB Hub	6&30c5d09c&0&7	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	VMware, Inc.	Virtual USB Hub	6&30c5d09c&0&8	CrypticWilds.000

Data Content

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 5 of 13 Result — USB Device Attached

Type	Value	Source(s)
Date/Time	2024-02-22 13:55:01 GMT	Recent Activity
Device Make	Alcor Micro Corp.	Recent Activity
Device Model	Flash Drive	Recent Activity
Device ID	15E12348	Recent Activity
Source File Path	/img_CrypticWilds.000/vol_vol6/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775540	

Figure I.3.2 - San disk Cruzer blade USB drive attachments records 2024/04/03, Investigator JB system config MD5 84199d2ea6fa634e9a867fcb67cee035

SYSTEM	0	2024-02-22 13:55:01 GMT	Alcor Micro Corp.	Flash Drive	15E12348	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	SanDisk Corp.	Cruzer Blade	0301982907052205443 6	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	VMware, Inc.	Virtual USB Hub	6&30c5d09c&0&7	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	VMware, Inc.	Virtual USB Hub	6&30c5d09c&0&8	CrypticWilds.000

Data Content

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 6 of 13 Result — USB Device Attached

Type	Value	Source(s)
Date/Time	2024-03-04 18:12:46 GMT	Recent Activity
Device Make	SanDisk Corp.	Recent Activity
Device Model	Cruzer Blade	Recent Activity
Device ID	0301982907052205443 6	Recent Activity
Source File Path	/img_CrypticWilds.000/vol_vol6/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775539	

Figure I.4.1 - Fusing the disk, Investigator JB AH EL MF

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# cd comp
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# ls
CrypticWilds.000  CrypticWilds.005  CrypticWilds.010    cw_evidence10to13.7z            output_Tue_Feb_25_09_22_07_2025
CrypticWilds.001  CrypticWilds.006  CrypticWilds.011    cw_evidence5to9.7z              timeline
CrypticWilds.002  CrypticWilds.007  CrypticWilds.012    exiftool
CrypticWilds.003  CrypticWilds.008  CrypticWilds.013    output_Tue_Feb_25_09_20_17_2025
CrypticWilds.004  CrypticWilds.009  cw_evidence0to4.7z  output_Tue_Feb_25_09_20_55_2025
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# sudo affuse CrypticWilds.000 /home/cmp209/Desktop/mount_point
s
fuse: mountpoint is not empty
fuse: if you are sure this is safe, use the 'nonempty' mount option
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# sudo affuse CrypticWilds.000 /home/cmp209/Desktop/mount_point
s/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp#
```

sudo affuse CrypticWilds.000 /home/cmp209/Desktop/mount_points/suspectDrive
cd /home/cmp209/Desktop/mount_points/suspectDrive
ls
CrypticWilds.000.raw

Figure I.4.2 - Hash verification of the disk, Investigator JB AH EL MF

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# cd /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls
CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# md5sum CrypticWilds.000.raw
aebd2d140eaf215e1a8554d008c5e2b3  CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sha15sum CrypticWilds.000.raw
Command 'sha15sum' not found, did you mean:
  command 'sha1sum' from deb coreutils (8.32-4.1ubuntu1.2)
Try: apt install <deb name>
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sha1sum CrypticWilds.000.raw
3c7bae35a28e12d67ed62cb9c09ee8e5935047fe  CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive#
```

md5sum CrypticWilds.000.raw
aebd2d140eaf215e1a8554d008c5e2b3 CrypticWilds.000.raw
sha15sum CrypticWilds.000.raw
Command 'sha15sum' not found, did you mean:
  command 'sha1sum' from deb coreutils (8.32-4.1ubuntu1.2)
Try: apt install <deb name>
sha1sum CrypticWilds.000.raw
3c7bae35a28e12d67ed62cb9c09ee8e5935047fe CrypticWilds.000.raw

Figure I.4.3 - Mounting the disk, Investigator JB AH EL MF

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sudo losetup -o 122683392 /dev/loop30 CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/m
ount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# cd /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls -lah
total 1.3G
drwxrwxrwx 1 root   root   4.0K Feb 27  2024  .
drwxrwxr-x 6 cmp209 cmp209 4.0K Apr 18 01:55  ..
drwxrwxrwx 1 root   root      0 Jan  2  2024 '$Recycle.Bin'
drwxrwxrwx 1 root   root   4.0K Feb 16  2024 '$WinREAgent'
lrwxrwxrwx 2 root   root     52 Dec 15  2023 'Documents and Settings' -> /home/cmp209/Desktop/mount_points/suspectDrive/Users
-rwxrwxrwx 2 root   root    12K Mar  4  2024  DumpStack.log.tmp
drwxrwxrwx 1 root   root      0 Feb 27  2024  OneDriveTemp
-rwxrwxrwx 1 root   root   1.3G Mar  4  2024  pagefile.sys
drwxrwxrwx 1 root   root      0 May  7  2022  PerfLogs
drwxrwxrwx 1 root   root   4.0K Jan  5  2024  ProgramData
drwxrwxrwx 1 root   root   8.0K Feb 21  2024 'Program Files'
drwxrwxrwx 1 root   root   4.0K Feb 19  2024 'Program Files (x86)'
drwxrwxrwx 1 root   root      0 Dec 15  2023  Recovery
-rwxrwxrwx 1 root   root    16M Mar  4  2024  swapfile.sys
drwxrwxrwx 1 root   root   4.0K Feb 20  2024 'System Volume Information'
drwxrwxrwx 1 root   root   4.0K Dec 15  2023  Users
drwxrwxrwx 1 root   root    24K Feb 20  2024  Windows
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive#
```

sudo losetup -o 122683392 /dev/loop30 CrypticWilds.000.raw
sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/mount_points/suspectDrive
cd /home/cmp209/Desktop/mount_points/suspectDrive
ls -lah
total 1.3G
drwxrwxrwx 1 root root 4.0K Feb 27 2024 .
drwxrwxr-x 6 cmp209 cmp209 4.0K Apr 18 01:55 ..
drwxrwxrwx 1 root root 0 Jan 2 2024 '$Recycle.Bin'
drwxrwxrwx 1 root root 4.0K Feb 16 2024 '$WinREAgent'
lrwxrwxrwx 2 root root 52 Dec 15 2023 'Documents and Settings' -> /home/cmp209/Desktop/mount_points/suspectDrive/Users
-rwxrwxrwx 2 root root 12K Mar 4 2024 DumpStack.log.tmp
drwxrwxrwx 1 root root 0 Feb 27 2024 OneDriveTemp
-rwxrwxrwx 1 root root 1.3G Mar 4 2024 pagefile.sys
drwxrwxrwx 1 root root 0 May 7 2022 PerfLogs

drwxrwxrwx 1 root root 4.0K Jan 5 2024 ProgramData
drwxrwxrwx 1 root root 8.0K Feb 21 2024 'Program Files'
drwxrwxrwx 1 root root 4.0K Feb 19 2024 'Program Files (x86)'
drwxrwxrwx 1 root root 0 Dec 15 2023 Recovery
-rwxrwxrwx 1 root root 16M Mar 4 2024 swapfile.sys
drwxrwxrwx 1 root root 4.0K Feb 20 2024 'System Volume Information' drwxrwxrwx 1 root root 4.0K Dec 15 2023 Users
drwxrwxrwx 1 root root 24K Feb 20 2024 Windows

Figure I.4.4 - Regripper use on SOFTWARE registry, Investigator JB 2025/04/21

```
root@cmp209-virtual-machine:/home/cmp209/Desktop# regripper -r SOFTWARE -f software > SOFTWARE_details.txt
Parsed Plugins file.
Launching allowedenum v.20200511
allowedenum complete.
Launching appcompatflags v.20200525
appcompatflags complete.
Launching appinitdlls v.20200427
appinitdlls complete.
Launching appkeys v.20200517
appkeys complete.
```

Command used: regripper -r SFOTWARE - f software > SOFTWARE_details.txt

Figure I.4.5 - GREP regripper output for ReleaseID, Investigator JB 2025/04/21

```
root@cmp209-virtual-machine:/home/cmp209/Desktop# grep -i ReleaseId SOFTWARE_details.txt
ReleaseID                    2009
```

Command used: grep -i ReleaseId SOFTWARE_details.txt Output: RelaseID 2009

Figure I.5.1 J. J. Thomas and K. A. Cook, Eds., Illuminating the path: the research and development agendaforvisual analytics. USDepartmentofHomelandSecurity, NationalVisualization and Analytics Center (NVAC), 2005.

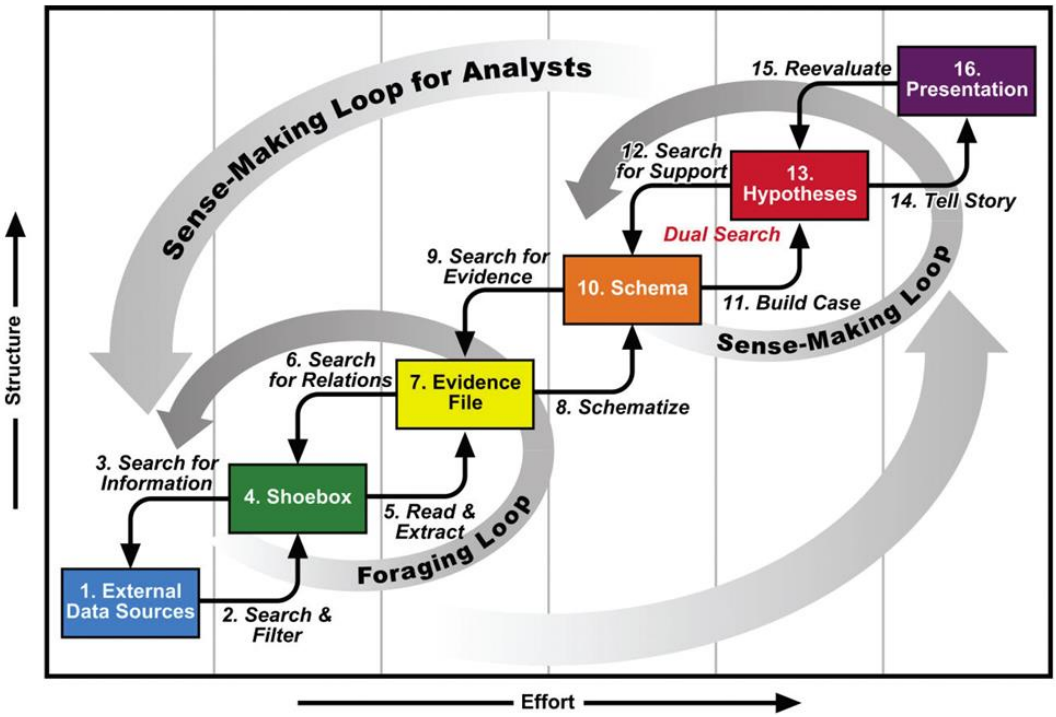


Figure I.6.1 Disk audit, partition analysis using fdisk. Investigator AH.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# fdisk -l CrypticWilds.000.raw
Disk CrypticWilds.000.raw: 64 GiB, 68719476736 bytes, 134217728 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 36B5D08B-1AE0-41AD-A814-06B4A85686EF

Device                    Start       End   Sectors  Size Type
CrypticWilds.000.raw1      2048    206847    204800  100M EFI System
CrypticWilds.000.raw2    206848    239615     32768   16M Microsoft reserved
CrypticWilds.000.raw3    239616 100847615 100608000   48G Microsoft basic data
CrypticWilds.000.raw4 100847616 102397951   1550336  757M Windows recovery envir
```

Command used: fdisk -l CrypticWilds.000.raw

Figure I.6.2 Disk audit, partition analysis mmls. Investigator AH.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# mmls CrypticWilds.000.raw
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0000206847   0000204800   EFI system partition
005:  001       0000206848   0000239615   0000032768   Microsoft reserved partition
006:  002       0000239616   0100847615   0100608000   Basic data partition
007:  003       0100847616   0102397951   0001550336
008:  -------   0102397952   0134217727   0031819776   Unallocated
```

Command used: mmls CrypticWilds.000.raw

Figure I.6.3 Disk audit, partition analysis parted. Investigator AH.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# parted CrypticWilds.000.raw print free
Warning: Unable to open /home/cmp209/Desktop/mount_points/windows/CrypticWilds.000.raw read-write (Permission denied).
/home/cmp209/Desktop/mount_points/windows/CrypticWilds.000.raw has been opened read-only.
Model:  (file)
Disk /home/cmp209/Desktop/mount_points/windows/CrypticWilds.000.raw: 68.7GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name                          Flags
        17.4kB  1049kB  1031kB  Free Space
 1      1049kB  106MB   105MB   fat32        EFI system partition          boot, esp
 2      106MB   123MB   16.8MB               Microsoft reserved partition  msftres
 3      123MB   51.6GB  51.5GB  ntfs         Basic data partition          msftdata
 4      51.6GB  52.4GB  794MB   ntfs                                       hidden, diag
        52.4GB  68.7GB  16.3GB  Free Space
```

Command used: parted CrypticWilds.000.raw print free

Figure I.6.4 Disk audit, hex dump. Investigator AH.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sudo dd if=CrypticWilds.000.raw bs=512 count=1 | hexdump -C
00000000  33 c0 8e d0 bc 00 7c 8e  c0 8e d8 be 00 7c bf 00  |3.....|......|..|
00000010  06 b9 00 02 fc f3 a4 50  68 1c 06 cb fb b9 04 00  |.......Ph.......|
00000020  bd be 07 80 7e 00 00 7c  0b 0f 85 0e 01 83 c5 10  |....~..|........|
00000030  e2 f1 cd 18 88 56 00 55  c6 46 11 05 c6 46 10 00  |.....V.U.F...F..|
00000040  b4 41 bb aa 55 cd 13 5d  72 0f 81 fb 55 aa 75 09  |.A..U..]r...U.u.|
00000050  f7 c1 01 00 74 03 fe 46  10 66 60 80 7e 10 00 74  |....t..F.f`.~..t|
00000060  26 66 68 00 00 00 00 66  ff 76 08 68 00 00 68 00  |&fh....f.v.h..h.|
00000070  7c 68 01 00 68 10 00 b4  42 8a 56 00 8b f4 cd 13  ||h..h...B.V.....|
00000080  9f 83 c4 10 9e eb 14 b8  01 02 bb 00 7c 8a 56 00  |............|.V.|
00000090  8a 76 01 8a 4e 02 8a 6e  03 cd 13 66 61 73 1c fe  |.v..N..n...fas..|
000000a0  4e 11 75 0c 80 7e 00 80  0f 84 8a 00 b2 80 eb 84  |N.u..~..........|
000000b0  55 32 e4 8a 56 00 cd 13  5d eb 9e 81 3e fe 7d 55  |U2..V...]...>.}U|
000000c0  aa 75 6e ff 76 00 e8 8d  00 75 17 fa b0 d1 e6 64  |.un.v....u.....d|
000000d0  e8 83 00 b0 df e6 60 e8  7c 00 b0 ff e6 64 e8 75  |......`.|....d.u|
000000e0  00 fb b8 00 bb cd 1a 66  23 c0 75 3b 66 81 fb 54  |.......f#.u;f..T|
000000f0  43 50 41 75 32 81 f9 02  01 72 2c 66 68 07 bb 00  |CPAu2....r,fh...|
00000100  00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66  |.fh....fh....fSf|
00000110  53 66 55 66 68 00 00 00  00 66 68 00 7c 00 00 66  |SfUfh....fh.|..f|
00000120  61 68 00 00 07 cd 1a 5a  32 f6 ea 00 7c 00 00 cd  |ah.....Z2...|...|
00000130  18 a0 b7 07 eb 08 a0 b6  07 eb 03 a0 b5 07 32 e4  |..............2.|
00000140  05 00 07 8b f0 ac 3c 00  74 09 bb 07 00 b4 0e cd  |......<.t.......|
00000150  10 eb f2 f4 eb fd 2b c9  e4 64 eb 00 24 02 e0 f8  |......+..d..$...|
00000160  24 02 c3 49 6e 76 61 6c  69 64 20 70 61 72 74 69  |$..Invalid parti|
00000170  74 69 6f 6e 20 74 61 62  6c 65 00 45 72 72 6f 72  |tion table.Error|
1+0 records in
1+0 records out
512 bytes copied, 0.000420308 s, 1.2 MB/s
00000180  20 6c 6f 61 64 69 6e 67  20 6f 70 65 72 61 74 69  | loading operati|
00000190  6e 67 20 73 79 73 74 65  6d 00 4d 69 73 73 69 6e  |ng system.Missin|
000001a0  67 20 6f 70 65 72 61 74  69 6e 67 20 73 79 73 74  |g operating syst|
000001b0  65 6d 00 00 00 63 7b 9a  00 00 00 00 00 00 00 00  |em...c{.........|
000001c0  02 00 ee fe 3f a1 01 00  00 00 ff ff ff ff 00 00  |....?...........|
000001d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
00000200
```

Command used:
sudo dd if=CrypticWilds.000.raw bs=512 count=1 | hexdump –C

Figure I.6.5 Disk audit, loopback test, Investigator AH.

```
cmp209@cmp209-virtual-machine:~$ sudo su
[sudo] password for cmp209:
Sorry, try again.
[sudo] password for cmp209:
root@cmp209-virtual-machine:/home/cmp209# ls
autopsy  Desktop  Documents  Downloads  evidence  hs_err_pid12837.log  hs_err_pid2372.log  hs_err_pid2403.log  hs_err_pid2405.log  hs_err_pid3101.log  jd  ModuleOutput  Music  Pictures  Public  R3_test  snap  src  Templates  Videos  Zeitline
root@cmp209-virtual-machine:/home/cmp209# cd Desktop
root@cmp209-virtual-machine:/home/cmp209/Desktop# ls
autopsy.desktop  bless.desktop  cases  firefox.desktop  fred.desktop  johnny.desktop  libreoffice-calc.desktop  libreoffice-writer.desktop  mount_points  okteta.desktop  org.gnome.Terminal.desktop  tools  win11.md5ListOnly.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop# cd /home/cmp209/Desktop/cases/CrypticWilds/comp/
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# ls
CrypticWilds.000  CrypticWilds.005  CrypticWilds.010    cw_evidence10to13.7z            output_Tue_Feb_25_09_22_07_2025
CrypticWilds.001  CrypticWilds.006  CrypticWilds.011    cw_evidence5to9.7z              timeline
CrypticWilds.002  CrypticWilds.007  CrypticWilds.012    extftool
CrypticWilds.003  CrypticWilds.008  CrypticWilds.013    output_Tue_Feb_25_09_20_17_2025
CrypticWilds.004  CrypticWilds.009  cw_evidence0to4.7z  output_Tue_Feb_25_09_20_55_2025
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# sudo affuse CrypticWilds.000 /home/cmp209/Desktop/mount_points/windows/
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds/comp# cd /home/cmp209/Desktop/mount_points/windows/
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# ls -lah
total 4.0K
drwxr-xr-x 2 root   root     0 Jan  1  1970 .
drwxrwxr-x 3 cmp209 cmp209 4.0K Mar 11 09:25 ..
-r--r--r-- 1 root   root    64G Jan  1  1970 CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sudo losetup -o 122683392 /dev/loop30 CrypticWilds.000.raw
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# cd /home/cmp209/Desktop/mount_points/suspectDrive
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/suspectDrive# ls -lah
total 1.3G
drwxrwxrwx 1 root   root   4.0K Feb 27  2024 .
drwxrwxr-x 5 cmp209 cmp209 4.0K Mar 11 09:25 ..
drwxrwxrwx 1 root   root     0 Jan  2  2024 $Recycle.Bin
drwxrwxrwx 1 root   root   4.0K Feb 16  2024 Documents and
lrwxrwxrwx 2 root   root     52 Dec 15  2023 'Documents and Settings' -> /home/cmp209/Desktop/mount_points/suspectDrive/Users
-rwxrwxrwx 2 root   root    12K Mar  4  2024 DumpStack.log.tmp
drwxrwxrwx 1 root   root      0 Feb 27  2024 hiberfil.sys
-rwxrwxrwx 1 root   root   1.3G Mar  4  2024 pagefile.sys
drwxrwxrwx 1 root   root      0 May  7  2022 perfLogs
drwxrwxrwx 1 root   root   4.0K Jan  5  2024 ProgramData
drwxrwxrwx 1 root   root   8.0K Feb 21  2024 Program Files
drwxrwxrwx 1 root   root   4.0K Feb 19  2024 Program Files (x86)
drwxrwxrwx 1 root   root      0 Dec 15  2023 Recovery
-rwxrwxrwx 1 root   root    16M Mar  4  2024 swapfile.sys
drwxrwxrwx 1 root   root   4.0K Feb 20  2024 System Volume Information
drwxrwxrwx 1 root   root   4.0K Dec 15  2023 Users
drwxrwxrwx 1 root   root   24K Feb 20  2024 Windows
```

Commands used:
sudo losetup -o 122683392 /dev/loop30 CrypticWilds.000.raw
sudo mount -o ro -t ntfs /dev/loop30 /home/cmp209/Desktop/mount_points/suspectDrive
cd /home/cmp209/Desktop/mount_points/suspectDrive

Figure I.7.1 USB Disk audit, partition analysis sgdisk, Investigator JB.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/mount_points/windows# sgdisk -p UsbCrypticWilds.001.raw
Warning! Disk size is smaller than the main header indicates! Loading
secondary header from the last sector of the disk! You should use 'v' to
verify disk integrity, and perhaps options on the experts' menu to repair
the disk.
Caution: invalid backup GPT header, but valid main header; regenerating
backup header from main header.

Warning! Error 25 reading partition table for CRC check!
Warning! One or more CRCs don't match. You should repair the disk!
Main header: OK
Backup header: ERROR
Main partition table: OK
Backup partition table: ERROR

******************************************************************************
Caution: Found protective or hybrid MBR and corrupt GPT. Using GPT, but disk
verification and recovery are STRONGLY recommended.
******************************************************************************
Disk UsbCrypticWilds.001.raw: 39936000 sectors, 19.0 GiB
Sector size (logical): 512 bytes
Disk identifier (GUID): E66B9B8A-08DC-44BF-8924-FA59334F7660
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 61849566
Partitions will be aligned on 2048-sector boundaries
Total free space is 2045 sectors (1022.5 KiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048        61849535   29.5 GiB    0700  Main Data Partition
```

Commands used:
sgdisk -p UsbCrypticWilds.001.raw

Figure I.8.1 Active programs volatility, Investigator JB.

sudo python3 vol.py -f /home/cmp209/Desktop/cases/CrypticWilds/Memory/CrypticWildsMemory.raw windows.pslist

0 System 0xd104270c8040 138 - N/A False 2024/02/22 13:39:28.000000 UTC N/A Disabled

88 4 Registry 0xd10427125080 4 - N/A False
2024/02/22 13:39:23.000000 UTC N/A Disabled
376 4 smss.exe 0xd1042957d040 2 - N/A False
2024/02/22 13:39:28.000000 UTC N/A Disabled
532 504 csrss.exe 0xd104293d2080 11 - 0 False
2024/02/22 13:39:30.000000 UTC N/A Disabled
600 504 wininit.exe 0xd10429c65080 2 - 0 False
2024/02/22 13:39:30.000000 UTC N/A Disabled
620 592 csrss.exe 0xd10429cc4140 14 - 1 False
2024/02/22 13:39:30.000000 UTC N/A Disabled
708 592 winlogon.exe 0xd10429d24080 6 - 1 False
2024/02/22 13:39:30.000000 UTC N/A Disabled
724 600 services.exe 0xd10429d29100 6 - 0 False
2024/02/22 13:39:30.000000 UTC N/A Disabled
768 600 lsass.exe 0xd1042982d0c0 8 - 0 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
896 724 svchost.exe 0xd10429ef408023 - 0 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
924 600 fontdrvhost.ex 0xd10429f511c05 - 0 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
916 708 fontdrvhost.ex 0xd10429f531c05 - 1 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
1008 724 svchost.exe 0xd1042a0020c0 12 - 0 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
508 724 svchost.exe 0xd1042a029080 4 - 0 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
856 708 LogonUI.exe 0xd1042a071100 0 - 1 False
2024/02/22 13:39:31.000000 UTC 2024-02-22 13:44:58.000000 UTC
Disabled
784 708 dwm.exe 0xd1042a073080 16 - 1 False
2024/02/22 13:39:31.000000 UTC N/A Disabled
1132 724 svchost.exe 0xd1042a0b2080 6 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1148 724 svchost.exe 0xd1042a0b6080 3 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1176 724 svchost.exe 0xd1042a10a0c0 4 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1232 724 svchost.exe 0xd1042a11b0c0 3 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1240 724 svchost.exe 0xd1042a11f0803 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1252 724 svchost.exe 0xd1042a123080 6 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1308 724 svchost.exe 0xd1042a15a080 5 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1316 724 svchost.exe 0xd1042a15b080 3 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1444 724 svchost.exe 0xd1042a1f80806 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1500 724 svchost.exe 0xd1042a279080 2 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1528 724 svchost.exe 0xd1042a27c080 3 - 0 False
2024/02/22 13:39:32.000000 UTC N/A Disabled
1588 724 svchost.exe 0xd1042a2a4080 2 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
1608 724 svchost.exe 0xd1042a292080 9 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled

1664 724 svchost.exe 0xd1042a2c2080 6 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
1700 724 svchost.exe 0xd1042a2c8080 3 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
1956 724 svchost.exe 0xd1042a3e9080 7 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
1976 724 svchost.exe 0xd1042a407080 9 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
2012 724 svchost.exe 0xd104271b6080 2 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
2020 724 svchost.exe 0xd104271b4080 3 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
2028 724 svchost.exe 0xd104271b2080 3 - 0 False
2024/02/22 13:39:33.000000 UTC N/A Disabled
2080 4 MemCompression 0xd10427154040 46 - N/A
False 2024/02/22 13:39:33.000000 UTC N/A Disabled
2092 724 svchost.exe 0xd1042707a080 2 - 0 False
2024-02-22 13:39:33.000000 UTC N/A Disabled
2172 724 svchost.exe 0xd104271db080 6 - 0 False
2024-02-22 13:39:33.000000 UTC N/A Disabled
2188 724 svchost.exe 0xd10427090080 2 - 0 False
2024-02-22 13:39:33.000000 UTC N/A Disabled
2212 724 svchost.exe 0xd10429a08080 6 - 0 False
2024-02-22 13:39:33.000000 UTC N/A Disabled
2376 724 svchost.exe 0xd1042a50d080 7 - 0 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2408 724 svchost.exe 0xd1042a543080 4 - 0 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2432 724 svchost.exe 0xd1042a546080 2 - 0 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2492 724 svchost.exe 0xd1042a544080 4 - 0 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2500 1664 sihost.exe 0xd1042a5730c0 11 - 1 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2516 724 svchost.exe 0xd1042a574080 5 - 1 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2652 724 svchost.exe 0xd1042a5be080 3 - 1 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2704 724 svchost.exe 0xd1042a631080 2 - 0 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2716 724 svchost.exe 0xd1042a632080 3 - 0 False
2024-02-22 13:39:34.000000 UTC N/A Disabled
2784 724 svchost.exe 0xd1042a674080 4 - 1 False
2024-02-22 13:39:35.000000 UTC N/A Disabled
2844 724 svchost.exe 0xd1042a6c0080 3 - 0 False
2024-02-22 13:39:35.000000 UTC N/A Disabled
2920 724 svchost.exe 0xd1042a6e30c0 4 - 0 False
2024-02-22 13:39:35.000000 UTC N/A Disabled
2996 1444 taskhostw.exe 0xd1042a7350c0 8 - 1 False
2024-02-22 13:39:35.000000 UTC N/A Disabled
3112 724 spoolsv.exe 0xd1042a7fb080 7 - 0 False
2024-02-22 13:39:35.000000 UTC N/A Disabled
3236 724 svchost.exe 0xd1042a83d0c0 10 - 0 False
2024-02-22 13:39:37.000000 UTC N/A Disabled
3316 724 svchost.exe 0xd104299d1080 5 - 0 False
2024-02-22 13:39:37.000000 UTC N/A Disabled

3436 2492 ctfmon.exe 0xd1042a84c080 9 - 1 False
2024-02-22 13:39:38.000000 UTC N/A Disabled
3556 724 svchost.exe 0xd1042a8f30807 - 0 False 2024-02-
22 13:39:38.000000 UTC N/A Disabled
3760 724 armsvc.exe 0xd1042aa760c0 2 - 0 True
2024-02-22 13:39:39.000000 UTC N/A Disabled
3772 724 svchost.exe 0xd1042aa79080 8 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3780 724 svchost.exe 0xd1042a9840c0 5 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3800 724 svchost.exe 0xd1042aa020c0 15 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3828 724 svchost.exe 0xd1042aa80080 1 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3848 724 svchost.exe 0xd1042aa81080 5 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3924 724 svchost.exe 0xd1042ab2a080 3 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3940 724 VGAuthService. 0xd1042ab2b080 2 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3960 724 vmtoolsd.exe 0xd1042ab2f080 13 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3952 724 vm3dservice.ex 0xd1042ab2c080 2 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
3976 724 MsMpEng.exe 0xd1042ab29080 23 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
4012 724 svchost.exe 0xd1042ab47080 23 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
4044 724 svchost.exe 0xd1042ab6b080 6 - 0 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
4076 3952 vm3dservice.ex 0xd1042ab77080 2 - 1 False
2024-02-22 13:39:39.000000 UTC N/A Disabled
4424 708 userinit.exe 0xd1042addd080 0 - 1 False
2024-02-22 13:39:41.000000 UTC 2024-02-22 13:40:13.000000 UTC
Disabled
4452 4424 explorer.exe 0xd1042ae640c0 58 - 1 False
2024-02-22 13:39:41.000000 UTC N/A Disabled
4596 724 dllhost.exe 0xd1042aece080 10 - 0 False
2024-02-22 13:39:42.000000 UTC N/A Disabled
4664 724 svchost.exe 0xd1042ad70080 7 - 0 False
2024-02-22 13:39:42.000000 UTC N/A Disabled
4756 724 svchost.exe 0xd1042aecc080 5 - 0 False
2024-02-22 13:39:42.000000 UTC N/A Disabled
5104 3772 AggregatorHost 0xd1042ac86080 1 - 0 False
2024-02-22 13:39:43.000000 UTC N/A Disabled
1324 896 WmiPrvSE.exe 0xd1042ac590c0 11 - 0 False
2024-02-22 13:39:43.000000 UTC N/A Disabled
1908 724 svchost.exe 0xd1042aec8080 4 - 1 False
2024-02-22 13:39:44.000000 UTC N/A Disabled
4372 724 svchost.exe 0xd1042ad6a080 1 - 0 False
2024-02-22 13:39:44.000000 UTC N/A Disabled
5904 896 SearchHost.exe 0xd1042b3020c0 53 - 1 False
2024-02-22 13:39:48.000000 UTC N/A Disabled
5912 896 StartMenuExper 0xd1042b484080 12 - 1 False
2024-02-22 13:39:48.000000 UTC N/A Disabled
6052 896 RuntimeBroker. 0xd1042b4e3080 9 - 1 False
2024-02-22 13:39:48.000000 UTC N/A Disabled

6132 896 RuntimeBroker. 0xd1042b4ea080 3 - 1 False
2024-02-22 13:39:49.000000 UTC N/A Disabled
5416 724 svchost.exe 0xd1042b4ac080 1 - 1 False
2024-02-22 13:39:50.000000 UTC N/A Disabled
5700 724 msdtc.exe 0xd1042b79c080 9 - 0 False
2024-02-22 13:39:51.000000 UTC N/A Disabled
6232 896 dllhost.exe 0xd1042aaf20807 - 1 False 2024-02-
22 13:39:51.000000 UTC N/A Disabled
6732 896 LockApp.exe 0xd1042aecb080 10 - 1 False
2024-02-22 13:39:58.000000 UTC N/A Disabled
6608 896 RuntimeBroker. 0xd1042bc6c080 3 - 1 False
2024-02-22 13:39:58.000000 UTC N/A Disabled
6160 724 svchost.exe 0xd1042b9a5080 6 - 0 False
2024-02-22 13:39:59.000000 UTC N/A Disabled
6588 724 svchost.exe 0xd1042b7e10c0 5 - 0 False
2024-02-22 13:40:01.000000 UTC N/A Disabled
6592 1444 LocationNotifi 0xd1042b7e7080 1 - 1 False
2024-02-22 13:40:02.000000 UTC N/A Disabled
7016 724 SearchIndexer. 0xd1042bcc1080 10 - 0 False
2024-02-22 13:40:02.000000 UTC N/A Disabled
7228 724 svchost.exe 0xd1042bea70c0 1 - 1 False
2024-02-22 13:40:04.000000 UTC N/A Disabled
7456 3040 GoogleCrashHan 0xd1042c08a080 5 - 0
True 2024-02-22 13:40:05.000000 UTC N/A Disabled
7532 724 NisSrv.exe 0xd1042c092080 7 - 0 False
2024-02-22 13:40:05.000000 UTC N/A Disabled
7616 3040 GoogleCrashHan 0xd1042c0cd080 3 - 0
False 2024-02-22 13:40:05.000000 UTC N/A Disabled
6836 4452 SecurityHealth 0xd1042bd020c0 1 - 1 False
2024-02-22 13:40:26.000000 UTC N/A Disabled
7304 724 SecurityHealth 0xd1042a7240c0 8 - 0 False
2024-02-22 13:40:27.000000 UTC N/A Disabled
5128 4452 vmtoolsd.exe 0xd1042a5a60c0 6 - 1 False
2024-02-22 13:40:39.000000 UTC N/A Disabled
7276 4452 msedge.exe 0xd1042bc130c0 0 - 1 False
2024-02-22 13:40:41.000000 UTC 2024-02-22 14:23:35.000000 UTC
Disabled
2236 4452 OneDrive.exe 0xd1042bfd7080 31 - 1 False
2024-02-22 13:40:49.000000 UTC N/A Disabled
8688 724 svchost.exe 0xd1042bf57080 9 - 0 False
2024-02-22 13:40:57.000000 UTC N/A Disabled
8208 724 svchost.exe 0xd1042bf780c04 - 1 False 2024-02-
22 13:41:35.000000 UTC N/A Disabled
8332 724 svchost.exe 0xd1042beda0c0 11 - 0 False
2024-02-22 13:41:40.000000 UTC N/A Disabled
8840 724 svchost.exe 0xd1042b6d30c0 2 - 0 False
2024-02-22 13:41:41.000000 UTC N/A Disabled
8928 724 uhssvc.exe 0xd1042bc43080 3 - 0 False
2024-02-22 13:41:42.000000 UTC N/A Disabled
8912 724 svchost.exe 0xd1042ba5f080 10 - 0 False
2024-02-22 13:41:42.000000 UTC N/A Disabled
9132 724 svchost.exe 0xd1042a35c080 7 - 0 False
2024-02-22 13:41:43.000000 UTC N/A Disabled
1080 896 SystemSettings 0xd1042b7800c0 20 - 1 False
2024-02-22 13:42:33.000000 UTC N/A Disabled
5268 896 ApplicationFra 0xd1042c2350c0 4 - 1 False
2024-02-22 13:42:33.000000 UTC N/A Disabled

2056 896 HxOutlook.exe 0xd1042ac8c0c0 30 - 1 False
2024-02-22 13:42:44.000000 UTC N/A Disabled
2168 896 RuntimeBroker. 0xd1042bf4c0801 - 1 False 2024-02-
22 13:42:44.000000 UTC N/A Disabled
2680 896 HxTsr.exe 0xd1042a71b080 13 - 1 False
2024-02-22 13:42:44.000000 UTC N/A Disabled
1736 724 svchost.exe 0xd1042c0f40800 - 0 False 2024-02-
22 13:43:58.000000 UTC 2024-02-22 13:44:04.000000 UTC Disabled
7380 724 svchost.exe 0xd1042b70d080 3 - 0 False
2024-02-22 13:43:58.000000 UTC N/A Disabled
8784 724 svchost.exe 0xd1042ad65080 3 - 0 False
2024-02-22 13:43:59.000000 UTC N/A Disabled
9032 8732 AdobeCollabSyn 0xd1042c70e080 5 - 1
False 2024-02-22 13:44:09.000000 UTC N/A Disabled
7632 9032 AdobeCollabSyn 0xd1042bfb8080 14 - 1
False 2024-02-22 13:44:09.000000 UTC N/A Disabled
8820 724 svchost.exe 0xd1042ce230c0 13 - 0 False
2024-02-22 13:44:40.000000 UTC N/A Disabled
6040 896 ShellExperienc 0xd1042cfc50c022 - 1 False 2024-02-
22 13:44:52.000000 UTC N/A Disabled
6640 724 svchost.exe 0xd1042ac90080 7 - 0 False
2024-02-22 13:44:58.000000 UTC N/A Disabled
3136 724 svchost.exe 0xd1042a740080 3 - 0 False
2024-02-22 13:51:30.000000 UTC N/A Disabled
7032 724 svchost.exe 0xd1042dac50c0 3 - 0 False
2024-02-22 13:51:30.000000 UTC N/A Disabled
5196 724 svchost.exe 0xd1042d7e4080 4 - 0 False
2024-02-22 13:51:30.000000 UTC N/A Disabled
7560 724 svchost.exe 0xd1042d6f6080 3 - 0 False
2024-02-22 13:54:46.000000 UTC N/A Disabled
2940 896 RuntimeBroker. 0xd1042ab7a080 4 - 1 False
2024-02-22 13:54:48.000000 UTC N/A Disabled
5028 724 WUDFHost.exe 0xd1042cc530c0 6 - 0 False
2024-02-22 13:55:02.000000 UTC N/A Disabled
2508 4452 thunderbird.ex 0xd1042d6e0140 47 - 1 False
2024-02-22 13:55:44.000000 UTC N/A Disabled
8540 2508 thunderbird.ex 0xd1042e255080 16 - 1 False
2024-02-22 13:55:45.000000 UTC N/A Disabled
8136 2508 thunderbird.ex 0xd1042d6e5080 15 - 1 False
2024-02-22 13:55:48.000000 UTC N/A Disabled
9048 4452 kleopatra.exe 0xd1042eed60c0 8 - 1 True
2024-02-22 14:13:53.000000 UTC N/A Disabled
5924 2572 gpg-agent.exe 0xd1042efd60c02 - 1 True 2024-02-
22 14:14:03.000000 UTC N/A Disabled
4696 2912 keyboxd.exe 0xd1042e5c50c0 1 - 1 True
2024-02-22 14:14:07.000000 UTC N/A Disabled
8860 5924 scdaemon.exe 0xd1042e1d40c0 2 - 1 True
2024-02-22 14:14:13.000000 UTC N/A Disabled
8712 7276 msedge.exe 0xd1042f3e60c046 - 1 False 2024-02-
22 14:23:33.000000 UTC N/A Disabled
8212 8712 msedge.exe 0xd1042e4e70c0 7 - 1 False
2024-02-22 14:23:33.000000 UTC N/A Disabled
3332 8712 msedge.exe 0xd1042e6d60c0 18 - 1 False
2024-02-22 14:23:34.000000 UTC N/A Disabled
1516 8712 msedge.exe 0xd1042ede70c0 16 - 1 False
2024-02-22 14:23:34.000000 UTC N/A Disabled

384 8712 msedge.exe 0xd10430ce90c0 10 - 1 False
2024-02-22 14:23:34.000000 UTC N/A Disabled
8504 8712 msedge.exe 0xd1042ebd60c0 17 - 1 False
2024-02-22 14:23:35.000000 UTC N/A Disabled
2372 8712 msedge.exe 0xd1042e8d60c0 16 - 1 False
2024-02-22 14:23:35.000000 UTC N/A Disabled
8680 896 FileCoAuth.exe 0xd1042cfce0805 - 1 False 2024-02-
22 14:23:36.000000 UTC N/A Disabled
4724 8712 msedge.exe 0xd1042e1e50c0 15 - 1 False
2024-02-22 14:23:37.000000 UTC N/A Disabled
7564 8712 msedge.exe 0xd1042e8c50c0 17 - 1 False
2024-02-22 14:23:38.000000 UTC N/A Disabled
1728 8712 msedge.exe 0xd1042b95b080 9 - 1 False
2024-02-22 14:23:42.000000 UTC N/A Disabled
5684 4452 MRCv120.exe 0xd1042c2f20802 - 1 True 2024-02-
22 14:23:50.000000 UTC N/A Disabled
2668 8712 msedge.exe 0xd1042c2680c0 9 - 1 False
2024-02-22 14:24:34.000000 UTC N/A Disabled
1200 896 RuntimeBroker. 0xd1042ab5e0c0 1 - 1 False
2024-02-22 14:24:34.000000 UTC N/A Disabled
2756 724 svchost.exe 0xd1042bf9a0c02 - 0 False 2024-02-
22 14:20:02.000000 UTC N/A Disabled

Figure I.8.2 Command line records volatility, Investigator JB.

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/volatile/volatility3-develop# sudo python3 vol.py -f /home/cmp209/Desktop/cases/Crypti
cWilds/Memory/CrypticWildsMemory.raw windows.cmdline
Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  -
88      Registry        -
376     smss.exe        \SystemRoot\System32\smss.exe
532     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=
```

Listed .exe:

smss.exe
csrss.exe
wininit.exe
winlogon.exe
services.exe
lsass.exe
svchost.exe
fontdrvhost.exe
LogonUI.exe
dwm.exe
sihost.exe
taskhostw.exe
spoolsv.exe
ctfmon.exe
armsvc.exe
VGAuthService.exe
vmtoolsd.exe
vm3dservice.exe
MsMpEng.exe
userinit.exe
explorer.exe
dllhost.exe
AggregatorHost.exe
WmiPrvSE.exe
SearchHost.exe
StartMenuExperienceHost.exe
RuntimeBroker.exe

msdtc.exe
LockApp.exe
LocationNotificationWindows.exe
SearchIndexer.exe
GoogleCrashHandler.exe
NisSrv.exe
GoogleCrashHandler64.exe
SecurityHealthSystray.exe
SecurityHealthService.exe
OneDrive.exe
uhssvc.exe
SystemSettings.exe
ApplicationFrameHost.exe
HxOutlook.exe
HxTsr.exe
WUDFHost.exe
thunderbird.exe
kleopatra.exe
gpg-agent.exe
keyboxd.exe
scdaemon.exe
msedge.exe
FileCoAuth.exe
AdobeCollabSync.exe
ShellExperienceHost.exe
MRCv120.exe

Output:

4 System - 88 Registry - 376 smss.exe \SystemRoot\System32\smss.exe 532 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16 600 wininit.exe wininit.exe 620 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16 708 winlogon.exe winlogon.exe 724 services.exe C:\Windows\system32\services.exe 768 lsass.exe C:\Windows\system32\lsass.exe 896 svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p 924 fontdrvhost.ex "fontdrvhost.exe" 916 fontdrvhost.ex "fontdrvhost.exe" 1008 svchost.exe C:\Windows\system32\svchost.exe -k RPCSS -p 508 svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM 856 LogonUI.exe - 784 dwm.exe "dwm.exe" 1132 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc 1148 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p 1176 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts 1232 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -s BTAGService 1240 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s BthAvctpSvc 1252 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s bthserv 1308 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc 1316 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService 1444 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule 1500 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s nsi 1528 svchost.exe C:\Windows\system32\svchost.exe -k UserProfileService -p -s ProfSvc 1588 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc 1608 svchost.exe C:\Windows\System32\svchost.exe -k netprofm -p -s netprofm 1664 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager 1700 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService 1956 svchost.exe C:\Windows\System32\svchost.exe -k

LocalServiceNetworkRestricted -p -s EventLog 1976 svchost.exe C:\Windows\system32\svchost.exe -k NetworkService -p 2012 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes 2020 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain 2028 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem 2080 MemCompression - 2092 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS 2172 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp 2188 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder 2212 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache 2376 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p 2408 svchost.exe C:\Windows\system32\svchost.exe -k appmodel -p -s StateRepository 2432 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc 2492 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TextInputManagementService 2500 sihost.exe sihost.exe 2516 svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc 2652 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s webthreatdefusersvc 2704 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p 2716 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p 2784 svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService 2844 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s TokenBroker 2920 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection 2996 taskhostw.exe taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E} 3112 spoolsv.exe C:\Windows\System32\spoolsv.exe 3236 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p 3316 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p -s LanmanWorkstation 3436 ctfmon.exe "ctfmon.exe" 3556 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s LanmanServer 3760 armsvc.exe "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe" 3772 svchost.exe C:\Windows\System32\svchost.exe -k utcsvc -p 3780 svchost.exe C:\Windows\system32\svchost.exe -k NetworkService -p 3800 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p -s DPS 3828 svchost.exe C:\Windows\system32\svchost.exe -k osprivacy -p -s camsvc 3848 svchost.exe C:\Windows\System32\svchost.exe -k NetSvcs -p -s iphlpsvc 3924 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TrkWks 3940 VGAuthService. "C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe" 3960 vmtoolsd.exe "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" 3952 vm3dservice.ex C:\Windows\system32\vm3dservice.exe 3976 MsMpEng.exe "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe" 4012 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt 4044 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s WpnService 4076 vm3dservice.ex vm3dservice.exe -n 4424 userinit.exe - 4452 explorer.exe C:\Windows\Explorer.EXE 4596 dllhost.exe C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235} 4664 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s CDPSvc 4756 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc 5104 AggregatorHost AggregatorHost.exe 1324 WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe 1908 svchost.exe C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc 4372 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo 5904 SearchHost.exe "C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe" -ServerName:CortanaUI.AppXstmwaab17q5s3y22tp6apqz7a45vwv65.mca 5912 StartMenuExper "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca 6052 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding 6132 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding 5416 svchost.exe C:\Windows\system32\svchost.exe -k UdkSvcGroup -s UdkUserSvc 5700 msdtc.exe

C:\Windows\System32\msdtc.exe 6232 dllhost.exe C:\Windows\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F} 6732 LockApp.exe "C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe" -ServerName:WindowsDefaultLockScreen.AppX7y4nbzq37zn4ks9k7amqjywdat7d3j2z.mca 6608 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding 6160 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s lfsvc 6588 svchost.exe C:\Windows\system32\svcho Local st.exe -k LocalServiceAndNoImpersonation -p -s SSDPSRV 6592 LocationNotifi "C:\Windows\System32\LocationNotificationWindows.exe" 7016 SearchIndexer. C:\Windows\system32\SearchIndexer.exe /Embedding 7228 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s NPSMSvc 7456 GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.36.363\GoogleCrashHandler.exe" 7532 NisSrv.exe "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\NisSrv.exe" 7616 GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.36.363\GoogleCrashHandler64.exe" 6836 SecurityHealth "C:\Windows\System32\SecurityHealthSystray.exe" 7304 SecurityHealth C:\Windows\system32\SecurityHealthService.exe 5128 vmtoolsd.exe "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr 7276 msedge.exe - 2236 OneDrive.exe "C:\Users\Sonya\AppData\\Microsoft\OneDrive\OneDrive.exe" /background 8688 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc 8208 svchost.exe C:\Windows\system32\svchost.exe -k UnistackSvcGroup 8332 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p 8840 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc 8928 uhssvc.exe "C:\Program Files\Microsoft Update Health Tools\uhssvc.exe" 8912 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc 9132 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc 1080 SystemSettings "C:\Windows\ImmersiveControlPanel\SystemSettings.exe" -ServerName:microsoft.windows.immersivecontrolpanel 5268 ApplicationFra C:\Windows\system32\ApplicationFrameHost.exe -Embedding 2056 HxOutlook.exe "C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.14326.21830.0_x64__8wekyb3d8bbwe\HxOutlook.exe" -ServerName:microsoft.windowslive.mail.AppXfbjsbkxvprcgqg6q4c9jfr0pn3kv9x5s.mca 2168 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding 2680 HxTsr.exe "C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.14326.21830.0_x64__8wekyb3d8bbwe\HxTsr.exe" -ServerName:Hx.IPC.Server 1736 svchost.exe - 7380 svchost.exe C:\Windows\system32\svchost.exe -k InvSvcGroup -p -s InventorySvc 8784 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p 9032 AdobeCollabSyn "C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe" 7632 AdobeCollabSyn "C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe" --type=collab-renderer --proc=9032 8820 svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DisplayEnhancementService 6040 ShellExperienc "C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca 6640 svchost.exe C:\Windows\system32\svchost.exe -k WebThreatDefense -p -s webthreatdefsvc 3136 svchost.exe C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager 7032 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -s W32Time 5196 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s DsSvc 7560 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC 2940 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding 5028 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-bb1ee333-9baf-44ca-a68b-d4dc5d979626 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-5ec35665-df7d-403d-8911-1263a158ef3e -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-9110f187-d3ba-4b11-b1cb-33ca6bbdc352 -

NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-b5b2006c-b8d1-494d-98fc-2fe8a423920a -LifetimeId:3324aa84-4289-46f7-8a45-921d1871ddd6 -DeviceGroupId:WpdFsGroup -HostArg:0 2508 thunderbird.ex "C:\Program Files\Mozilla Thunderbird\thunderbird.exe" 8540 thunderbird.ex "C:\Program Files\Mozilla Thunderbird\thunderbird.exe" -contentproc --channel="2508.0.760933227\1778166771" -parentBuildID 20240216174500 -prefsHandle 1900 -prefMapHandle 1872 -prefsLen 9340 -prefMapSize 255933 -appDir "C:\Program Files\Mozilla Thunderbird" - {0f3fc145-84b6-4338-b036-409be9ad5d32} 2508 "\.\pipe\gecko-crash-server-pipe.2508" 1992 216a05cd558 gpu 8136 thunderbird.ex "C:\Program Files\Mozilla Thunderbird\thunderbird.exe" -contentproc --channel="2508.1.433317267\1947311102" -childID 1 -isForBrowser -prefsHandle 2608 -prefMapHandle 3572 -prefsLen 9212 -prefMapSize 255933 -jsInitHandle 1408 -jsInitLen 240916 -parentBuildID 20240216174500 -win32kLockedDown -appDir "C:\Program Files\Mozilla Thunderbird" - {b21670bf-6998-44de-ba0d-72414821a835} 2508 "\.\pipe\gecko-crash-server-pipe.2508" 3548 216aa390d58 tab 9048 kleopatra.exe "C:\Program Files (x86)\Gpg4win\bin\kleopatra.exe" 5924 gpg-agent.exe "C:\Program Files (x86)\GnuPG\bin\gpg-agent.exe" --homedir C:\Users\Sonya\AppData\Roaming\gnupg --use-standard-socket --daemon 4696 keyboxd.exe "C:\Program Files (x86)\GnuPG\bin\keyboxd.exe" --homedir C:\Users\Sonya\AppData\Roaming\gnupg --daemon 8860 scdaemon.exe "C:\Program Files (x86)\GnuPG\bin\scdaemon.exe" --multi-server 8712 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window 8212 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\Sonya\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Sonya\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=121.0.6167.184 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 "--annotation=prod=Microsoft Edge" --annotation=ver=121.0.2277.128 --initial-client-data=0x26c,0x270,0x274,0x268,0x2d4,0x7ff857f4bf98,0x7ff857f4bfa4,0x7ff857f4bfb0 3332 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAA
EAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAA
CAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=2252 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:2 1516 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2536 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:3 384 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=3776 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:8 8504 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --first-renderer-process --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale=en_GB --device-scale-factor=1 --num-raster-threads=1 --renderer-client-id=10 --time-ticks-at-unix-epoch=-1708609162648181 --launch-time-ticks=2653236956 --mojo-platform-channel-handle=5428 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:1 2372 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale=en_GB --device-scale-factor=1 --num-raster-threads=1 --renderer-client-id=9 --time-ticks-at-unix-epoch=-1708609162648181 --launch-time-ticks=2653288918 --mojo-platform-channel-handle=5580 --

field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:1 8680 FileCoAuth.exe "C:\Users\Sonya\AppData\Local\Microsoft\OneDrive\24.020.0128.0003\FileCoAuth.exe" -Embedding 4724 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale=en_GB --device-scale-factor=1 --num-raster-threads=1 --renderer-client-id=16 --time-ticks-at-unix-epoch=-1708609162648181 --launch-time-ticks=2654608995 --mojo-platform-channel-handle=6264 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:1 7564 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --instant-process --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale=en_GB --device-scale-factor=1 --num-raster-threads=1 --renderer-client-id=19 --time-ticks-at-unix-epoch=-1708609162648181 --launch-time-ticks=2655843681 --mojo-platform-channel-handle=6336 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:1 1728 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --no-appcompat-clear --mojo-platform-channel-handle=7088 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:8 5684 MRCv120.exe "C:\Users\Sonya\OneDrive\Desktop\MRCv120.exe" 2668 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_search_indexer.mojom.SearchIndexerInterfaceBroker --lang=en-US --service-sandbox-type=search_indexer --message-loop-type-ui --no-appcompat-clear --mojo-platform-channel-handle=3156 --field-trial-handle=2256,i,3847565733586294610,3086145226562029368,262144 --variations-seed-version /prefetch:8 1200 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding 2756 svchost.exe

Figure I.8.3 Malware discovery tool using volatility, Investigator JB

```
root@cmp209-virtual-machine:/home/cmp209/Desktop/volatile/volatility3-develop# sudo python3 vol.py -f /home/cmp209/Desktop/cases/Crypti
cWilds/Memory/CrypticWildsMemory.raw windows.malfind
Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

3976    MsMpEng.exe     0x26386800000   0x2638690cfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled        N/A
53 00 4c 00 43 00 6f 00 75 00 6e 00 74 00 00 00 S.L.C.o.u.n.t...
1c 00 00 00 5f 00 50 00 53 00 4c 00 45 00 6e 00 ...._.P.S.L.E.n.
74 00 72 00 69 00 65 00 73 00 00 00 18 00 00 00 t.r.i.e.s.......
5f 00 54 00 5a 00 44 00 43 00 6f 00 75 00 6e 00 _.T.Z.D.C.o.u.n.        53 00 4c 00 43 00 6f 00 75 00 6e 00 74 00 00 00 1c 00 00 00 5f
00 50 00 53 00 4c 00 45 00 6e 00 74 00 72 00 69 00 65 00 73 00 00 00 18 00 00 00 5f 00 54 00 5a 00 44 00 43 00 6f 00 75 00 6e 00
3976    MsMpEng.exe     0x26386c00000   0x26386d0cfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled        N/A
```

Command used:

sudo python3 vol.py -f /home/cmp209/Desktop/cases/CrypticWilds/Memory/CrypticWildsMemory.raw windows.malfind

Output:

Volatility 3 Framework 2.25.0 Progress: 100.00 PDB scanning finished

PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Notes Hexdump Disasm

3976 MsMpEng.exe 0x26386800000 0x2638690cfff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A

53 00 4c 00 43 00 6f 00 75 00 6e 00 74 00 00 00 S.L.C.o.u.n.t... 1c 00 00 00 5f 00 50 00 53 00 4c 00 45 00 6e 00 ...._.P.S.L.E.n. 74 00 72 00 69 00 65 00 73 00 00 00 18 00 00 00 t.r.i.e.s..... 5f 00 54 00 5a 00 44 00 43 00 6f 00 75 00 6e 00 _.T.Z.D.C.o.u.n. 53 00 4c 00 43 00 6f 00 75 00 6e 00 74 00 00 00 1c 00 00 00 5f 00 50 00 53 00 4c 00 45 00 6e 00 74 00 72 00 69 00 65 00 73 00 00 00 18 00 00 00 5f 00 54 00 5a 00 44 00 43 00 6f 00 75 00 6e 00 3976 MsMpEng.exe 0x26386c00000 0x26386d0cfff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A

56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H...8.... 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A][_^ c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 ...@.....H..H.w 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 3976 MsMpEng.exe 0x26387600000 0x2638770cfff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H...8.... 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A\][_^ c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 ...@.....H..H.w 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 3976 MsMpEng.exe 0x26393e00000 0x26393f0cfff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A

56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H...8.... 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A][_^ c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 ...@.....H..H.w 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 3976 MsMpEng.exe 0x26394100000 0x2639420cfff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A c8 db db ff c8 db db ff c8 db dc ff c8 db dc ff ..... c7 db db ff c7 db db ff c6 da da ff c6 db db ff ..... c7 db db ff c7 db dd ff c8 dc dd ff c9 de df ff ..... c9 de df ff c9 de df ff ca dd df ff ca dd df ff ..... c8 db db ff c8 db db ff c8 db dc ff c8 db dc ff c7 db db ff c7 db db ff c6 da da ff c6 db db ff c7 db db ff c7 db dd ff c8 dc dd ff c9 de df ff c9 de df ff c9 de df ff ca dd df ff ca dd df ff 3976 MsMpEng.exe 0x26393ff0000 0x263940fcfff VadS PAGE_EXECUTE_READWRITE 269 1 Disabled N/A 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 VWSUATAUAVAWH..(4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 L.<$H..H...8.... 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e I.g(A_A^A]A\][_^ c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 ...@.....H..H.w 56 57 53 55 41 54 41 55 41 56 41 57 48 83 ec 28 4c 8d 3c 24 48 8b e9 48 8d b1 98 38 00 00 ff e2 49 8d 67 28 41 5f 41 5e 41 5d 41 5c 5d 5b 5f 5e c3 00 00 40 00 80 00 00 00 48 89 e9 48 b8 60 77 3976 MsMpEng.exe 0x263cc1f0000 0x263cc1f2fff VadS PAGE_EXECUTE_READWRITE 3 1 Disabled N/A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3976 MsMpEng.exe 0x263cd950000 0x263cd958fff VadS PAGE_EXECUTE_READWRITE 9 1 Disabled N/A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3976 MsMpEng.exe 0x263cde70000 0x263cdf6ffff VadS PAGE_EXECUTE_READWRITE 256 1 Disabled N/A

cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ..... cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ..... cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ..... cc 08 00 42 00 00 00 00 05 48 8b 45 20 48 89 c2 ...B.....H.E H.. cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 08 00 42 00 00 00 00 05 48 8b 45 20 48 89 c2 3976 MsMpEng.exe 0x263cdf70000 0x263ce16ffff VadS PAGE_EXECUTE_READWRITE 512 1 Disabled N/A

cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ..... cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ..... cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc ..... cc 0a 00 36 00 0a 00 01 05 48 8b 55 28 48 8b 8d ...6.....H.U(H.. cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 0a 00 36 00 0a 00 01 05 48 8b 55 28 48 8b 8d 5904 SearchHost.exe 0x15e00820000 0x15e0083ffff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled N/A

48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c H.T$.H.L$.L.D$.L 89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 .L$ H.A(H.H.H.QP 48 83 e2 f8 48 8b ca 48 b8 60 00 82 00 5e 01 00 H...H..H.` ...^.. 00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1 .H+.H..p...v.H.. 48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c 89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 48 83 e2 f8 48 8b ca 48 b8 60 00 82 00 5e 01 00 00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1 5904 SearchHost.exe 0x15e00880000 0x15e008e3fff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled N/A

e9 fb ff 37 00 00 00 00 00 cc cc cc cc cc cc cc ...7..... e9 eb 07 38 00 00 00 00 00 cc cc cc cc cc cc cc ...8..... e9 db 0f 38 00 00 00 00 00 cc cc cc cc cc cc cc ...8..... e9 cb 0b 38 00 00 00 00 00 cc cc cc cc cc cc cc ...8..... e9 fb ff 37 00 00 00 00 00 cc cc cc cc cc cc cc e9 eb 07 38 00 00 00 00 00 cc cc cc cc cc cc cc e9 db 0f 38 00 00 00 00 00 cc cc cc cc cc cc cc e9 cb 0b 38 00 00 00 00 00 cc cc cc cc cc cc cc 5904 SearchHost.exe 0x15e11810000 0x15e1182ffff VadS PAGE_EXECUTE_READWRITE 3 1 Disabled N/A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5904 SearchHost.exe 0x15e235c0000 0x15e23623fff VadS PAGE_EXECUTE_READWRITE 2 1 Disabled N/A

e9 fb ff fd ef ff ff ff ff cc cc cc cc cc cc cc ..... e9 eb 03 fe ef ff ff ff ff cc cc cc cc cc cc cc ..... e9 db 0f fe ef ff ff ff ff cc cc cc cc cc cc cc ..... e9 cb 17 fe ef ff ff ff ff cc cc cc cc cc cc cc ..... e9 fb ff fd ef ff ff ff ff cc cc cc cc cc cc cc e9 eb 03 fe ef ff ff ff ff cc cc cc cc cc cc cc e9 db 0f fe ef ff ff ff ff cc cc cc cc cc cc cc e9 cb 17 fe ef ff ff ff ff cc cc cc cc cc cc cc 6732 LockApp.exe 0x1d9cb5b0000 0x1d9cb5b0fff Vad PAGE_EXECUTE_READWRITE 0 0 Disabled N/A

00 00 00 00 00 00 00 00 fe ff ff ff f7 2f 00 00 ...../.. 00 00 61 00 69 00 6c 00 2c 00 31 00 00 00 00 00 ..a.i.l.,.1..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 fe ff ff ff f7 2f 00 00 00 00 61 00 69 00 6c 00 2c 00 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6608 RuntimeBroker. 0x1908a2b0000 0x1908a2b0fff Vad PAGE_EXECUTE_READWRITE 0 0 Disabled N/A

00 00 00 00 00 00 00 00 fe ff ff ff f7 2f 00 00 ...../.. 00 00 61 00 69 00 6c 00 2c 00 31 00 00 00 00 00 ..a.i.l.,.1..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 fe ff ff ff f7 2f 00 00 00 00 61 00 69 00 6c 00 2c 00 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2236 OneDrive.exe 0x2dbfc3f0000 0x2dbfc3fffff VadS PAGE_EXECUTE_READWRITE 16 1 Disabled N/A

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... f0 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2508 thunderbird.ex 0x216a1740000 0x216a174ffff VadS PAGE_EXECUTE_READWRITE 16 1 Disabled N/A

00 00 00 00 00 00 00 00 3b 00 00 00 00 00 00 00 ....;..... 4c 8d 15 f9 ff ff ff ff 25 03 00 00 00 0f 1f 00 L.....%..... 58 95 1e 1f f8 7f 00 00 00 3e 1a a7 16 02 00 00 X.....>..... 70 05 75 1d f8 7f 00 00 80 35 31 a8 16 02 00 00 p.u.....51..... 00 00 00 00 00 00 00 00 3b 00 00 00 00 00 00 00 4c 8d 15 f9 ff ff ff ff 25 03 00 00 00 0f 1f 00 58 95 1e 1f f8 7f 00 00 00 3e 1a a7 16 02 00 00 70 05 75 1d f8 7f 00 00 80 35 31 a8 16 02 00 00

Figure I.9.1 Bluetooth Devices

```
----------------------------------------
bthenum v.20200515
(System) Get BTHENUM subkey info

ControlSet001\Enum\BTHENUM not found.
----------------------------------------
bthport v.20200517
(System) Gets Bluetooth-connected devices from System hive

ControlSet001\services\BTHPORT\Parameters\Devices
LastWrite: 2024-02-16 09:57:36Z
ControlSet001\services\BTHPORT\Parameters\Devices has no subkeys.

ControlSet001\services\BTHPORT\Parameters\Radio Support not found.
----------------------------------------
```

Figure I.9.2 Hard Disk and USB drive information

```
----------------------------------------
devclass v.20200525
(System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

2024-02-22 14:22:51Z
  Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00,030198290705220544 36&0
2024-02-20 09:29:40Z
  Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07,15E12348&0

DevClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}


----------------------------------------
mountdev v.20200517
(System) Return contents of System hive MountedDevices key


MountedDevices
LastWrite time = 2024-02-22 14:22:51Z


Device: DMIO:ID: 1f 13 6f d1 fe af c8 8f 49 81 f3 fc 01 1d 09 93
  \DosDevices\C:

Device: _??_USBSTOR#Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07#15E12348&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{468020eb-d0c5-11ee-8cea-b03cdc85928c}
  \DosDevices\E:

Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#0301982907052205443 6&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  \DosDevices\F:
  \??\Volume{ca024822-d187-11ee-8cec-b03cdc85928c}

Device: \??\SCSI#CdRom&Ven_NECVMWar&Prod_VMware_SATA_CD01#5&260e6d66&0&010000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{a7055276-9b8a-11ee-8cca-806e6f6e6963}
  \DosDevices\D:

----------------------------------------
```

Figure I.9.3 System Inofrmation

```
----------------------------------------
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {081806cc-832a-4374-b1ac-074f704afcd3}
LastWrite Time: 2023-12-15 20:43:59Z
  EnableDHCP                    1
  Domain
  NameServer

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {87da51a3-7c0e-4fa9-b45d-5413cd720826}
LastWrite Time: 2024-03-04 18:12:51Z
  EnableDHCP                    1
  Domain
  NameServer
  DhcpIPAddress                 192.168.74.148
  DhcpSubnetMask                255.255.255.0
  DhcpServer                    192.168.74.254
  Lease                         1800
  LeaseObtainedTime             2024-03-04 18:12:51Z
  T1                            2024-03-04 18:27:51Z
  T2                            2024-03-04 18:39:06Z
  LeaseTerminatesTime           2024-03-04 18:42:51Z
  AddressType                   0
  IsServerNapAware              0
  DhcpConnForceBroadcastFlag    0
  DhcpDomain                    localdomain
  DhcpNameServer                192.168.74.2
  DhcpDefaultGateway            192.168.74.2
  DhcpSubnetMaskOpt             255.255.255.0
  DhcpInterfaceOptions          üyw/.+!À¨J
                                         localdomaiÀ¨À¨ÿÿÀ¨Jþ5
  DhcpGatewayHardware           À¨JPVð
  DhcpGatewayHardwareCount      1

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {9c719ac8-92b4-4a4b-a7ee-c7d1106874b1}
LastWrite Time: 2023-12-15 20:44:27Z
  EnableDHCP                    1
  Domain
  NameServer

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {a705525f-9b8a-11ee-8cca-806e6f6e6963}
LastWrite Time: 2023-12-15 20:44:09Z

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
----------------------------------------
```

Figure I.9.4 System Information about the Sonya user account

```
Username        : Sonya [1001]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2023-12-15 13:23:12Z
Name            :
Last Login Date : 2024-02-27 07:26:48Z
Pwd Reset Date  : 2024-02-21 09:39:04Z
Pwd Fail Date   : 2024-02-20 09:07:17Z
Login Count     : 83
Embedded RID    : 1001
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

Figure I.9.5 Name of computer

```
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-K6L0LLR
TCP/IP Hostname = DESKTOP-K6L0LLR
----------------------------------------
```

I.10 - Installed Programs Investigator EL

Figure I.10.1- Screenshot showing the MD5 Hashes being collated in a txt file for the Whitelist

```
%%%% HASHDEEP-1.0
md5
## Invoked from: /home/cmp209/Desktop/mount_points/suspectDrive
sha256 -r -o f -l .
##
a526b9e7c716b3489d8cc062fbce4005
938d0dbc0824ca40de7c0d56f4fc5860
dd35bc0a96edc387846fdb3247c61e56
d0e05db2dbc7d79866e021fefa5c5cb6
8e227c7f485510c0a6c06a2a9261f227
dfb095d4fe70b313eb6f79f0a6e2d96c
081730b990ab73f5613e53f963056d0c
ae681652c1aec0fb063e6034dd452fb5
24d4a27011bbdc651a3616b5c51ce25f
ab0ae200e5a153bb16ff66a46b785955
0866e5c52898eac915d384c641b4547d
6376211065682b270793a5e490617470
c60ef731df483974970b548ae72975dc
0983c5b144979474f98e2db3f86a3c50
a5393d4524fb94e524a80390302fc7c0
9ddf4d181de0fbe77a7308c339165161
ebbeef6f4f20583a3732d67db3fbe4f4
46de78514fb5ac4e1048406e4832035f
3a9ce43964c9d58b9340217e7d823c32
321a150615f1d08c97ad02377b6ee4e1
57c0aebcb5d3c1ea210f6aa164ad009f
53467e9573418a13b50817a6ff18c495
2e46ebfeffc38814c6c8145a0805673c
d8ac412e19137804acf7e7dc20e71fb6
6f1f5045b06a3ea1a00dc28a185535c5
0029c09508d005ed4d199b2bbe106cb2
96cefb514a67cf90bbc780954630f4f9
44e9fd9356f783c440372062c2a6e967
23f35aee6b22943d95e3689e7ff46b50
3beb3923a19e4cf7b676651bf8cd32d8
da240cc65eee81bf4c1cca0ceb3ef0c0
5871e00fba511d4c9e5781e3cca2b308
ce16e54d41fe4026b7cb8f6b0ad21396
eabfbae9b447ff337226f6a3350ff32a
ece19ec64af2073cc44bf1fe18203968
1b8a46b697020ee54ade65c42cd07921
ae7eb3834dfe5ecda8db655821747ab5
de5c3ac8ca25f41426fd88002d57baec
b76766644c827a7265a6320017d0816b
```

Figure I.10.2- Screenshot of linux command line showing commands of invistigator creating a whitelist for Autopsy

```
cmp209@cmp209-virtual-machine:~$ sudo su
[sudo] password for cmp209:
root@cmp209-virtual-machine:/home/cmp209# cd /home/cmp209/Desktop/cases/CrypticWilds/
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# ls -lah
total 36M
drwxrwxr-x 3 cmp209 cmp209 4.0K Apr 28 11:50 .
drwxrwxr-x 3 cmp209 cmp209 4.0K Apr  9  2024 ..
drwxrwxr-x 2 cmp209 cmp209 4.0K Apr  9  2024 comp
-rwxrwxrwx 1 root   root    36M Apr 28 11:53 cw.nameAndmd5List.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# cut -f 2 -d , cw.nameAndmd5List.txt > cw.md5ListOnly.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# cut -f 2 -droot@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# cut -f 2 -d , cw.nameAndm
d5List.txt^C cw.md5ListOnly.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# cut -f 2 -d , win11PostInstall.txt > win11.md5ListOnly.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# grep -v -f win11.md5ListOnly.txt cwmd5ListOnly.txt > whitelist.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds# grep -a -v -i -f win11.md5ListOnly.txt cwmd5ListOnly.txt > whitelist2.txt
root@cmp209-virtual-machine:/home/cmp209/Desktop/cases/CrypticWilds#
```

Figure I.10.3- Screenshot of Autopsy showing the indexed whitelist being appended to the autopsy file.

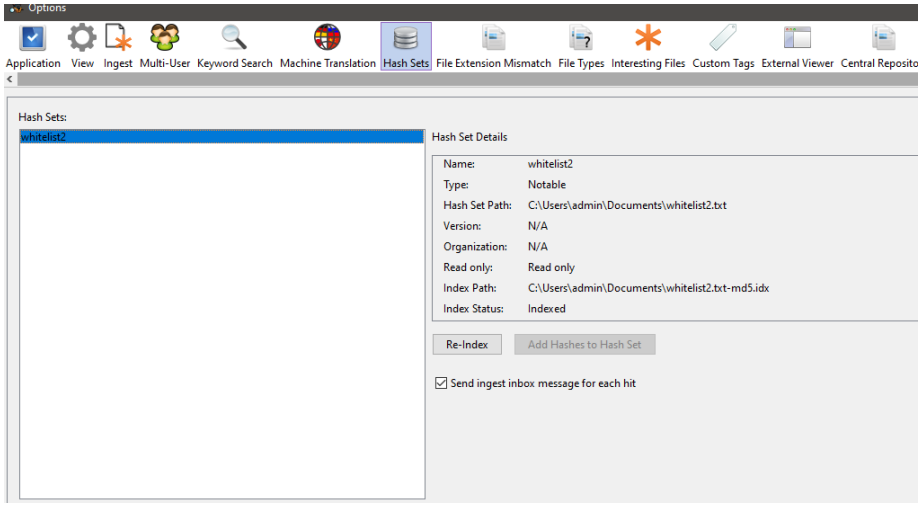


Figure I.10.4- Screenshot of Autopsy before the whitelist had been applied

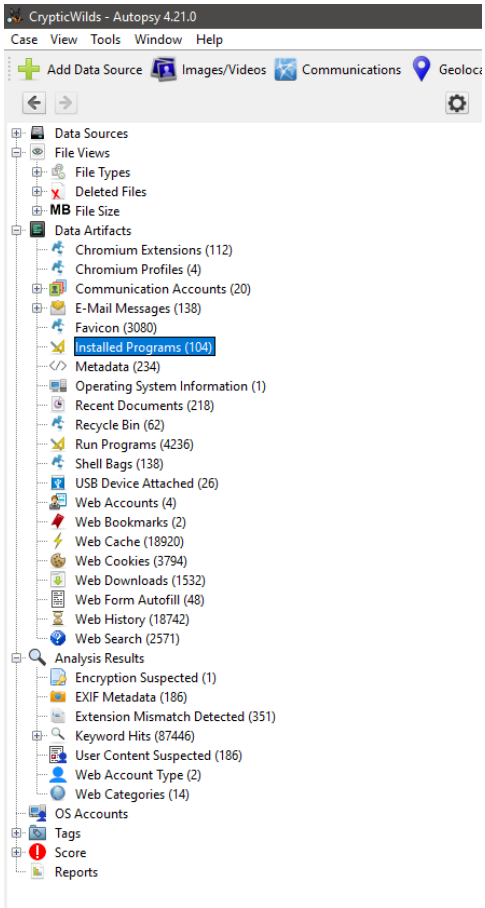
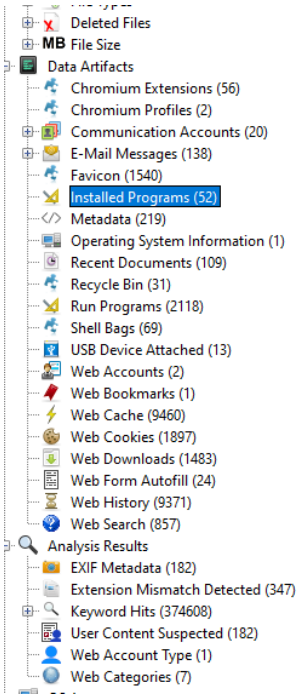


Figure I.10.5- Screenshot of Autopsy after the whitelist had been applied



I.11 - VeraCrypt and miscellaneous Autopsy Investigator EL

Figure I.11.1- Autopsy screenshot of deleted VeraCrypt alert icon

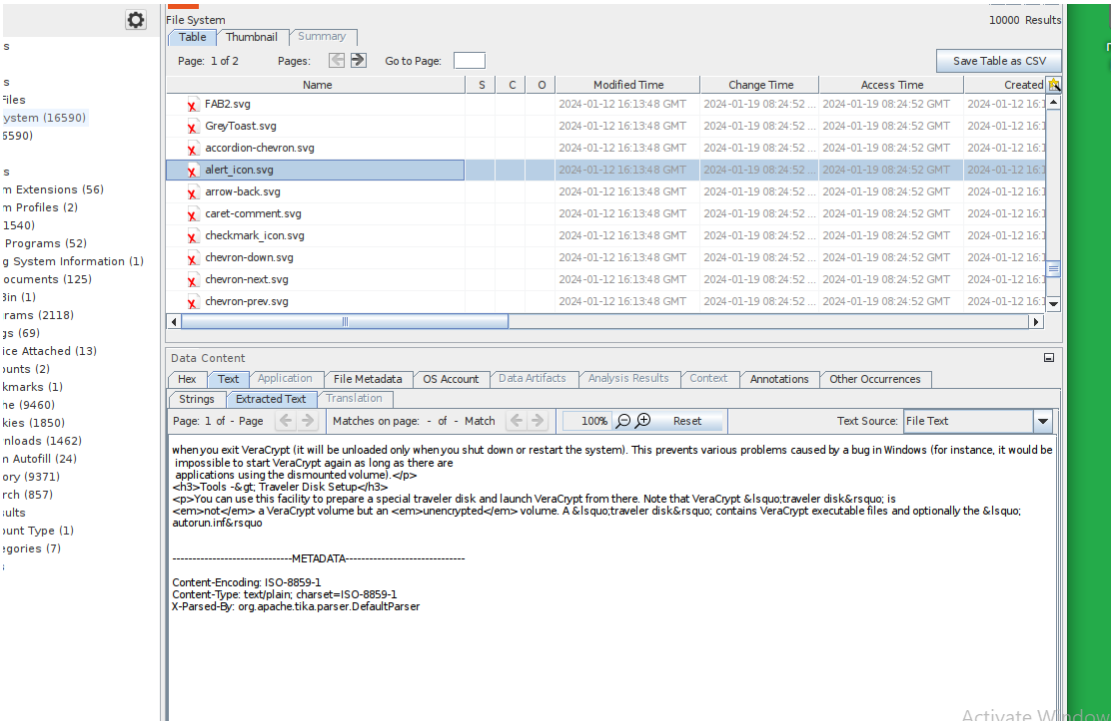


Figure I.11.2- Autopsy screenshot of deleted VeraCrypt alert icon Veracypt files including VeraCrypt Hidden Operating System.html

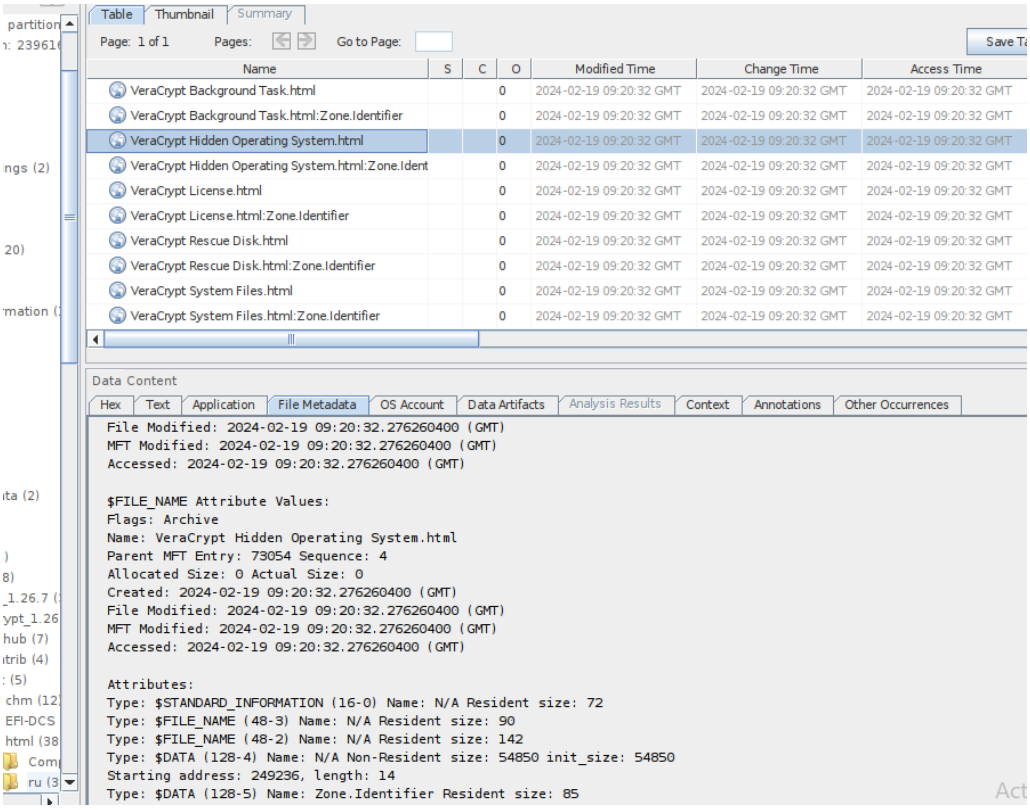


Figure I.11.3- Autopsy screenshot of video of a Hippo

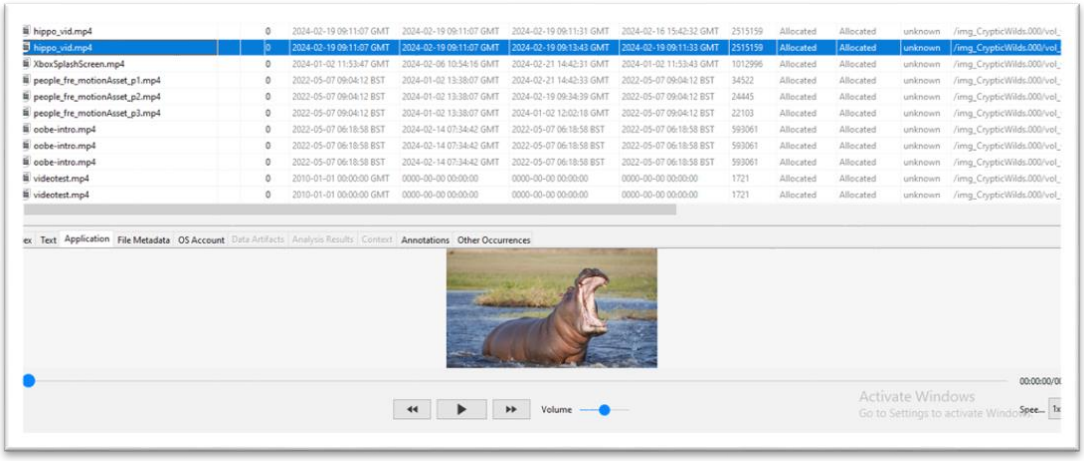
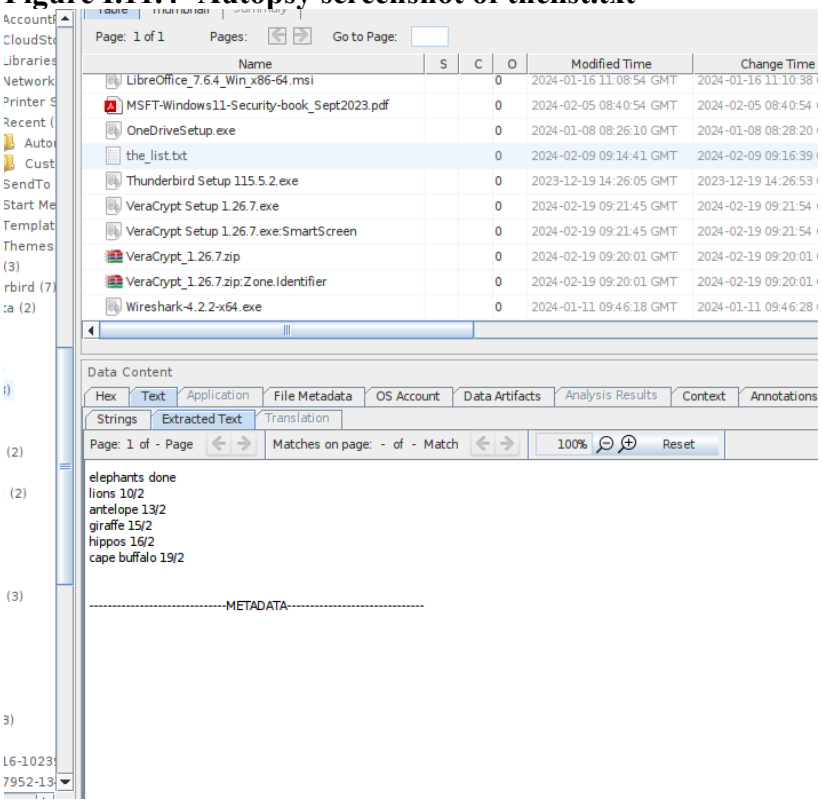


Figure I.11.4- Autopsy screenshot of thelist.txt



Appendix J Installed / Run programs

J.1 - Installed Programs Investigator EL

Figure J.1.1- Screenshot of Autospy showing installed programs Wireshark and Npcap 2024/01/11 09:48:25 - 9:49:49 GMT

SOFTWARE			0	Wireshark 4.2.2 x64 v.4.2.2	2024-01-11 09:49:49 GMT	CrypticWilds.000
SOFTWARE			0	Npcap v.1.78	2024-01-11 09:48:25 GMT	CrypticWilds.000

Figure J.1.2- Screenshot of Autopsy showing information on the installed program USBPcap 2024/01/11 09:48:58 GMT

Type	Value
Program Name	USBPcap 1.5.4.0 v.1.5.4.0
Date/Time	2024-01-11 09:48:58 GMT
Source File Path	/img_CrypticWilds.000/vol_vol6/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854775519

Figure J.1.3- Screenshot of Autopsy showing information on the installed program AnalogExif v0.04.1 2024/02/08 13:48:15 GMT

Type	Value
Program Name	AnalogExif v.0.0.4.1
Date/Time	2024-02-08 13:48:15 GMT
Source File Path	/img_CrypticWilds.000/vol_vol6/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854775492

Figure J.1.4- Screenshot of Autopsy showing information on installed program Mozilla Thunderbirds 2024/02/21 19:16:10 GMT

Type	Value
Program Name	Mozilla Thunderbird (x64 en-GB) v.115.8.0
Date/Time	2024-02-21 09:16:10 GMT
Source File Path	/img_CrypticWilds.000/vol_vol6/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854775522

J.2 - Run Programs Investigator MF

index	Source Name	Program Name	Path	Date/Time	Count
1	CERTUTIL.EXE-79A712E5.pf	CERTUTIL.EXE	/WINDOWS/SYSWOW64	2024/01/11 09:48:06 GMT	7
2	CERTUTIL.EXE-79A712E5.pf	CERTUTIL.EXE	/WINDOWS/SYSWOW64	2024/01/11 09:48:07 GMT	7
3	CERTUTIL.EXE-79A712E5.pf	CERTUTIL.EXE	/WINDOWS/SYSWOW64	2024/01/11 09:48:13 GMT	7
4	NPFINSTALL.EXE-5577DC1C.pf	NPFINSTALL.EXE	/PROGRAM FILES/NPCAP	202401/11 09:48:14 GMT	3
5	NPFINSTALL.EXE-5577DC1C.pf	NPFINSTALL.EXE	/PROGRAM FILES/NPCAP	2024/01/11 09:48:15 GMT	3
6	STEGHIDE.EXE-0E315A11.pf	STEGHIDE.EXE	/USERS/SONYA/DOWNLOADS/STEGHIDE-0.5.1-WIN32/STEGHIDE	2024/01/24 13:40:27 GMT	1
7	VERACRYPT SETUP 1.26.7.EXE-58BC9A34.pf	VERACRYPT SETUP 1.26.7.EXE	/USERS/SONYA/DOWNLOADS	2024/02/19 09:22:00 GMT	1
8	GPG4WIN-4.3.0.EXE-C3A18CBB.pf	GPG4WIN-4.3.0.EXE	/USERS/SONYA/DOWNLOADS	2024/02/19 09:24:37 GMT	1
9	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/19 09:25:09 GMT	7

10	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/19 09:25:16 GMT	10
11	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/19 09:25:18 GMT	15
12	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/19 09:25:19 GMT	15
13	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/19 09:42:44 GMT	7
14	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/19 09:42:44 GMT	15
15	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/20 09:07:37 GMT	7
16	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:07:40 GMT	15
17	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:07:41 GMT	15
18	GPG-CONNECT-AGENT.EXE-78A78391.pf	GPG-CONNECT-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:07:44 GMT	3
19	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:07:44 GMT	10
20	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:07:48 GMT	10
21	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:07:56 GMT	13
22	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 09:10:26 GMT	13
23	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 10:10:26 GMT	13
24	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 10:51:25 GMT	19
25	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 11:22:18 GMT	19
26	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 11:22:18 GMT	13
27	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/20 11:32:41 GMT	19
28	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 08:07:15 GMT	13
29	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 08:07:56 GMT	19
30	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 09:06:44 GMT	19
31	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 09:06:44 GMT	13
32	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 09:18:48 GMT	19
33	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/21 16:19:38 GMT	7

34	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/21 16:19:39 GMT	7
35	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:19:54 GMT	15
36	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:19:54 GMT	19
37	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:19:54 GMT	13
38	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:19:55 GMT	15
39	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:19:57 GMT	10
40	GPG-CONNECT-AGENT.EXE-78A78391.pf	GPG-CONNECT-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:19:58 GMT	3
41	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/21 16:20:02 GMT	7
42	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:20:03 GMT	10
43	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/21 16:20:04 GMT	10
44	KLEOPATRA.EXE-458747A6.pf	KLEOPATRA.EXE	/PROGRAM FILES (X86)/GPG4WIN/BIN	2024/02/22 14:13:53 GMT	7
45	GPGCONF.EXE-BFC8F1C0.pf	GPGCONF.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/22 14:13:56 GMT	15
46	GPG.EXE-2D33AE2A.pf	GPG.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/22 14:13:56 GMT	19
47	GPGSM.EXE-3A25A152.pf	GPGSM.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/22 14:13:56 GMT	13
48	GPG-CONNECT-AGENT.EXE-78A78391.pf	GPG-CONNECT-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/22 14:13:59 GMT	3
49	GPG-AGENT.EXE-D575FAC6.pf	GPG-AGENT.EXE	/PROGRAM FILES (X86)/GNUPG/BIN	2024/02/22 14:13:59 GMT	10

Appendix K - Shell Bags

Figure K.1- Screenshot of Autopsy showing "mission spec" file created, modified, and accessed on 2024/01/26 at 09:21:32 GMT

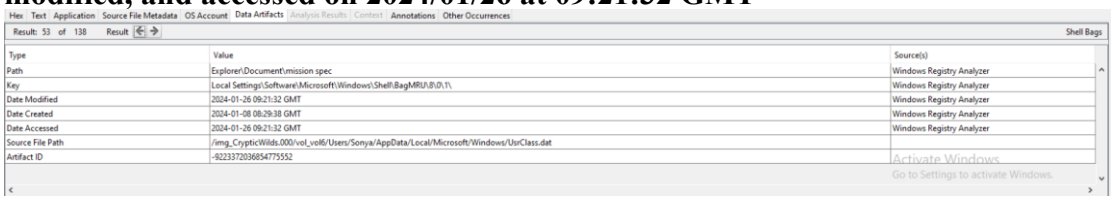


Figure K.2- “steghide-0.5.1-win32.zi” was created. This file was extracted on the same date at 13:40:20 GMT and became “steghide-0.5.1-win3”. Items were then written to the file “steghid” 2024/01/24 13:36:20 to 13:40:42 GMT.

UsrClass.dat			Explorer\steghide-0.5.1-win32.zi	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-01-24 13:36:24 GMT	2024-01-24 13:36:20 GMT	2024-01-24 13:36:24 GMT
UsrClass.dat			Explorer\steghide-0.5.1-win32.zi	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-01-24 13:36:24 GMT	2024-01-24 13:36:20 GMT	2024-01-24 13:36:24 GMT
UsrClass.dat			Explorer\steghide-0.5.1-win3	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-01-24 13:40:20 GMT	2024-01-24 13:40:20 GMT	2024-01-24 13:40:22 GMT
UsrClass.dat			Explorer\steghide-0.5.1-win3\steghid	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-01-24 13:40:42 GMT	2024-01-24 13:40:22 GMT	2024-01-24 13:40:20 GMT	2024-01-24 13:40:22 GMT
UsrClass.dat			Explorer\steghide-0.5.1-win3	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-01-24 13:40:20 GMT	2024-01-24 13:40:20 GMT	2024-01-24 13:40:22 GMT
UsrClass.dat			Explorer\steghide-0.5.1-win3\steghid	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-01-24 13:40:42 GMT	2024-01-24 13:40:22 GMT	2024-01-24 13:40:20 GMT	2024-01-24 13:40:22 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 4 of 138 Result Shell Bags

Type	Value	Source(s)
Path	Explorer\steghide-0.5.1-win32.zi	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\0\	Windows Registry Analyzer
Date Modified	2024-01-24 13:36:24 GMT	Windows Registry Analyzer
Date Created	2024-01-24 13:36:20 GMT	Windows Registry Analyzer
Date Accessed	2024-01-24 13:36:24 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775601	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 5 of 138 Result Shell Bags

Type	Value	Source(s)
Path	Explorer\steghide-0.5.1-win3	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\1\	Windows Registry Analyzer
Date Modified	2024-01-24 13:40:20 GMT	Windows Registry Analyzer
Date Created	2024-01-24 13:40:20 GMT	Windows Registry Analyzer
Date Accessed	2024-01-24 13:40:22 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775600	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 6 of 138 Result Shell Bags

Type	Value	Source(s)
Path	Explorer\steghide-0.5.1-win3\steghid	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\1\0\	Windows Registry Analyzer
Last Write	2024-01-24 13:40:42 GMT	Windows Registry Analyzer
Date Modified	2024-01-24 13:40:22 GMT	Windows Registry Analyzer
Date Created	2024-01-24 13:40:20 GMT	Windows Registry Analyzer
Date Accessed	2024-01-24 13:40:22 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775599	

Figure K.3- file called “mission pic” was created and placed in the documents folder. 2024/01/26 at 09:07:42

UsrClass.dat			Explorer\mission pic	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-01-26 09:07:52 GMT	2024-01-26 09:07:42 GMT	2024-01-26 09:21:22 GMT
UsrClass.dat			Explorer\Document\mission pic	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-16 07:12:46 GMT	2024-01-26 09:07:42 GMT	2024-01-26 09:07:42 GMT	2024-01-26 09:07:42 GMT

Type	Value	Source(s)
Path	Explorer\mission pic	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\6\0\	Windows Registry Analyzer
Date Modified	2024-01-26 09:07:52 GMT	Windows Registry Analyzer
Date Created	2024-01-26 09:07:42 GMT	Windows Registry Analyzer
Date Accessed	2024-01-26 09:21:22 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775586	

Type	Value	Source(s)
Path	Explorer\Document\mission pic	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\0\	Windows Registry Analyzer
Last Write	2024-02-16 07:12:46 GMT	Windows Registry Analyzer
Date Modified	2024-01-26 09:07:42 GMT	Windows Registry Analyzer
Date Created	2024-01-26 09:07:42 GMT	Windows Registry Analyzer
Date Accessed	2024-01-26 09:07:42 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775553	

Figure K.4- a file called “elephant” was created then moved to the documents folder On 2024/02/06 at 10:17:44

UsrClass.dat			Explorer\elephant	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-06 10:17:48 GMT	2024-02-06 10:17:44 GMT	2024-02-06 10:17:44 GMT	2024-02-06 10:17:44 GMT
UsrClass.dat			Explorer\Document\elephant	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-06 10:18:34 GMT	2024-02-06 10:17:44 GMT	2024-02-16 07:04:18 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 20 of 138 Result Shell Bags

Type	Value	Source(s)
Path	Explorer\elephant	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\6\1\	Windows Registry Analyzer
Last Write	2024-02-06 10:17:48 GMT	Windows Registry Analyzer
Date Modified	2024-02-06 10:17:44 GMT	Windows Registry Analyzer
Date Created	2024-02-06 10:17:44 GMT	Windows Registry Analyzer
Date Accessed	2024-02-06 10:17:44 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775585	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 56 of 138 Result Shell Bags

Type	Value	Source(s)
Path	Explorer\Document\elephant	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\4\	Windows Registry Analyzer
Date Modified	2024-02-06 10:18:34 GMT	Windows Registry Analyzer
Date Created	2024-02-06 10:17:44 GMT	Windows Registry Analyzer
Date Accessed	2024-02-16 07:04:18 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775549	

Figure K.5- a folder was created called “backup_07022”and placed in the documents folder. Then three files were added to the folder - “mission spec”, “mission pic” and “elephant”. 2024/02/07 at 09:26:54 to 09:27:04 GMT

UsrClass.dat	CLSID_Users\Document\backup_07022	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-16 07:11:38 GMT	2024-02-07 09:27:06 GMT	2024-02-07 09:26:54 GMT	2024-02-13 13:48:06 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_07022	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-07 09:27:02 GMT	2024-02-07 09:26:54 GMT	2024-02-07 09:26:54 GMT	2024-02-07 09:26:54 GMT
UsrClass.dat	CLSID_Users\Document\backup_07022	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-16 07:11:38 GMT	2024-02-07 09:27:06 GMT	2024-02-07 09:26:54 GMT	2024-02-13 13:48:06 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_07022	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-07 09:27:02 GMT	2024-02-07 09:26:54 GMT	2024-02-07 09:26:54 GMT	2024-02-07 09:26:54 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 16 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	CLSID_Users\Document\backup_07022	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\5\0\0\	Windows Registry Analyzer
Last Write	2024-02-16 07:11:38 GMT	Windows Registry Analyzer
Date Modified	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Date Accessed	2024-02-13 13:48:06 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775589	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 33 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\	Windows Registry Analyzer
Last Write	2024-02-07 09:27:02 GMT	Windows Registry Analyzer
Date Modified	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Date Accessed	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775572	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 85 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	CLSID_Users\Document\backup_07022	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\5\0\0\	Windows Registry Analyzer
Last Write	2024-02-16 07:11:38 GMT	Windows Registry Analyzer
Date Modified	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Date Accessed	2024-02-13 13:48:06 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854710938	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 102 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\	Windows Registry Analyzer
Last Write	2024-02-07 09:27:02 GMT	Windows Registry Analyzer
Date Modified	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Date Accessed	2024-02-07 09:26:54 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854710921	

UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-07 09:27:06 GMT	2024-02-07 09:27:06 GMT	2024-02-07 09:27:06 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-07 09:27:06 GMT	2024-02-07 09:27:06 GMT	2024-02-07 09:27:06 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-20 09:16:37 GMT	2024-02-07 09:27:06 GMT	2024-02-07 09:27:06 GMT	2024-02-07 09:27:06 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 34 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\elephant	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\0\	Windows Registry Analyzer
Date Modified	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Accessed	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775571	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 35 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\mission pic	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\1\	Windows Registry Analyzer
Date Modified	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Accessed	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775570	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 36 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\mission spec	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\2\	Windows Registry Analyzer
Last Write	2024-02-20 09:16:37 GMT	Windows Registry Analyzer
Date Modified	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Accessed	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775569	

Figure K.6- files "mission spec" and "mission pic" were created. 2024/02/07 at 09:27:06

UsrClass.dat	My Computer\E:\mission spec	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-20 09:16:56 GMT	2024-02-07 09:27:06 GMT	2024-02-20 09:16:56 GMT
UsrClass.dat	My Computer\E:\mission pic	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-20 09:16:56 GMT	2024-02-07 09:27:06 GMT	2024-02-20 09:16:56 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 47 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\E:\mission spec	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\1\1\	Windows Registry Analyzer
Date Modified	2024-02-20 09:16:56 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Accessed	2024-02-20 09:16:56 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775558	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 48 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\E:\mission pic	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\1\2\	Windows Registry Analyzer
Date Modified	2024-02-20 09:16:56 GMT	Windows Registry Analyzer
Date Created	2024-02-07 09:27:06 GMT	Windows Registry Analyzer
Date Accessed	2024-02-20 09:16:56 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775557	

Figure K.7- files "lion", "antelop", and "giraff" added to "backup_07022". 2024/02/14 07:15:56 to 2024/02/16 07:12:06 GMT

UsrClass.dat	CLSID_Users\Document\backup_07022\lion	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-20 09:24:15 GMT	2024-02-14 07:18:02 GMT	2024-02-14 07:15:56 GMT	2024-02-14 07:18:02 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-14 07:15:56 GMT	2024-02-14 07:15:56 GMT	2024-02-14 07:15:56 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 17 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	CLSID_Users\Document\backup_07022\lion	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.5\.0\.0\.0\	Windows Registry Analyzer
Last Write	2024-02-20 09:24:15 GMT	Windows Registry Analyzer
Date Modified	2024-02-14 07:18:02 GMT	Windows Registry Analyzer
Date Created	2024-02-14 07:15:56 GMT	Windows Registry Analyzer
Date Accessed	2024-02-14 07:18:02 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775588	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 37 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\lion	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.7\.0\.0\.0\.3\.0\.3\	Windows Registry Analyzer
Date Modified	2024-02-14 07:15:56 GMT	Windows Registry Analyzer
Date Created	2024-02-14 07:15:56 GMT	Windows Registry Analyzer
Date Accessed	2024-02-14 07:15:56 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775568	

UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-16 07:04:54 GMT	2024-02-16 07:04:34 GMT	2024-02-16 07:04:34 GMT	2024-02-19 09:09:18 GMT
UsrClass.dat	Explorer\Document\antelop	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-16 07:04:34 GMT	2024-02-16 07:04:34 GMT	2024-02-16 07:04:38 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 41 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\antelop	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.7\.0\.0\.0\.3\.0\.7\	Windows Registry Analyzer
Date Modified	2024-02-16 07:04:54 GMT	Windows Registry Analyzer
Date Created	2024-02-16 07:04:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:09:18 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775564	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 54 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\Document\antelop	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.8\.0\.2\	Windows Registry Analyzer
Date Modified	2024-02-16 07:04:34 GMT	Windows Registry Analyzer
Date Created	2024-02-16 07:04:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-16 07:04:38 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775551	

UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-16 07:10:00 GMT	2024-02-16 07:09:52 GMT	2024-02-16 07:09:52 GMT	2024-02-19 09:09:18 GMT
UsrClass.dat	Explorer\Document\giraff	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000		2024-02-16 07:09:52 GMT	2024-02-16 07:09:52 GMT	2024-02-16 07:09:52 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 43 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\giraff	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.7\.0\.0\.0\.3\.0\.9\	Windows Registry Analyzer
Date Modified	2024-02-16 07:10:00 GMT	Windows Registry Analyzer
Date Created	2024-02-16 07:09:52 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:09:18 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775562	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 55 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\Document\giraff	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.8\.0\.3\	Windows Registry Analyzer
Date Modified	2024-02-16 07:09:52 GMT	Windows Registry Analyzer
Date Created	2024-02-16 07:09:52 GMT	Windows Registry Analyzer
Date Accessed	2024-02-16 07:09:52 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775550	

UsrClass.dat	Explorer\Document\lion	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-16 07:12:06 GMT	2024-02-16 07:12:06 GMT	2024-02-16 07:12:06 GMT	2024-02-16 07:12:08 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 57 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\Document\lion	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.8\.0\.5\	Windows Registry Analyzer
Date Modified	2024-02-16 07:12:06 GMT	Windows Registry Analyzer
Date Created	2024-02-16 07:12:06 GMT	Windows Registry Analyzer
Date Accessed	2024-02-16 07:12:08 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775548	

Figure K.8- On 2024/02/19 at 09:11:34 GMT 5 files created and added to "backup_07022" - "incident_", "incident_", "nois", "buffal" and "hippo" 2024/02/19 at 09:11:34 GMT

UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:12:12 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:12:16 GMT
UsrClass.dat	My Computer\C:\User\Sony\Document\backup_0702...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:11:52 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:34 GMT	2024-02-19 09:11:52 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 38 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\incident_	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.7\.0\.0\.0\.3\.0\.4\	Windows Registry Analyzer
Date Modified	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775567	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 39 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\incident_	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\.7\.0\.0\.0\.3\.0\.5\	Windows Registry Analyzer
Date Modified	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775566	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 40 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\nois	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\6\	Windows Registry Analyzer
Date Modified	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775565	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 42 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\buffal	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\8\	Windows Registry Analyzer
Date Modified	2024-02-19 09:12:12 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:12:16 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775563	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 44 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\C:\User\Sony\Document\backup_07022\hippo	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0\3\0\10\	Windows Registry Analyzer
Date Modified	2024-02-19 09:11:52 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:11:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:11:52 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775561	

Figure K.9- file "VeraCrypt_1.26" installed, a folder was placed within the VeraCrypt files called "sr", and the release and setup folders of VeraCrypt were created and accessed. 2024/02/19 at 09:20:12 - 09:21:00 GMT

UsrClass.dat	Explorer\VeraCrypt_1.26.	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:21:06 GMT	2024-02-19 09:20:12 GMT	2024-02-19 09:20:12 GMT	2024-02-19 09:20:12 GMT
UsrClass.dat	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:21:18 GMT	2024-02-19 09:20:34 GMT	2024-02-19 09:20:12 GMT	2024-02-19 09:20:34 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 7 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\VeraCrypt_1.26.	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\2\	Windows Registry Analyzer
Last Write	2024-02-19 09:21:06 GMT	Windows Registry Analyzer
Date Modified	2024-02-19 09:20:12 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:20:12 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:20:12 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775598	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 8 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\2\0\	Windows Registry Analyzer
Last Write	2024-02-19 09:21:18 GMT	Windows Registry Analyzer
Date Modified	2024-02-19 09:20:34 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:20:12 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:20:34 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775597	

UsrClass.dat	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.\sr	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:21:23 GMT	2024-02-19 09:21:06 GMT	2024-02-19 09:20:34 GMT	2024-02-19 09:21:06 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 9 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.\sr	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\2\0\0\	Windows Registry Analyzer
Last Write	2024-02-19 09:21:23 GMT	Windows Registry Analyzer
Date Modified	2024-02-19 09:21:06 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:20:34 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:21:06 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775596	

UsrClass.dat	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.\sr\Releas	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:21:24 GMT	2024-02-19 09:21:00 GMT	2024-02-19 09:21:00 GMT	2024-02-19 09:21:00 GMT
UsrClass.dat	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.\sr\Releas\Se...	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-19 09:21:29 GMT	2024-02-19 09:21:00 GMT	2024-02-19 09:21:00 GMT	2024-02-19 09:21:02 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 10 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.\sr\Releas	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\2\0\0\0\	Windows Registry Analyzer
Last Write	2024-02-19 09:21:24 GMT	Windows Registry Analyzer
Date Modified	2024-02-19 09:21:00 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:21:00 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:21:00 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775595	

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 11 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	Explorer\VeraCrypt_1.26.\VeraCrypt_1.26.\sr\Releas\Setup File	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\2\0\0\0\0\	Windows Registry Analyzer
Last Write	2024-02-19 09:21:29 GMT	Windows Registry Analyzer
Date Modified	2024-02-19 09:21:00 GMT	Windows Registry Analyzer
Date Created	2024-02-19 09:21:00 GMT	Windows Registry Analyzer
Date Accessed	2024-02-19 09:21:02 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775594	

Figure K.10- folder called "ke" was created on the computer 2024/02/20 at 10:28:16 GMT.

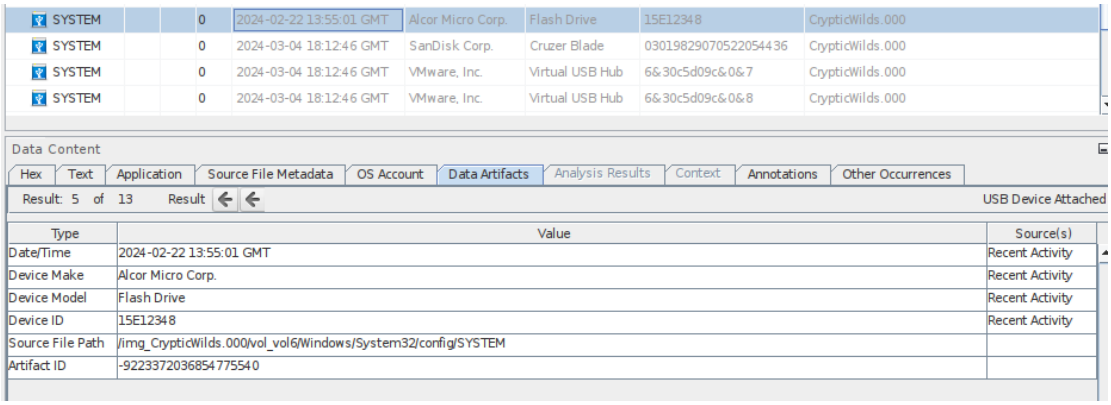
UsrClass.dat	My Computer\E:\ke	Local Settings\Software\Microsoft\Windows\Shell\Ba...	CrypticWilds.000	2024-02-20 10:36:45 GMT	2024-02-20 10:28:16 GMT	2024-02-20 10:28:16 GMT	2024-02-20 10:28:16 GMT

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 46 of 138 | Result | Shell Bags

Type	Value	Source(s)
Path	My Computer\E:\ke	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\1\0\	Windows Registry Analyzer
Last Write	2024-02-20 10:36:45 GMT	Windows Registry Analyzer
Date Modified	2024-02-20 10:28:16 GMT	Windows Registry Analyzer
Date Created	2024-02-20 10:28:16 GMT	Windows Registry Analyzer
Date Accessed	2024-02-20 10:28:16 GMT	Windows Registry Analyzer
Source File Path	/img_CrypticWilds.000/vol_vol6/Users/Sonya/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775559	

Figure K.11- External USB of model Alcor micro corp Flash Drive 2024/02/22 at 13:55:01 GMT



SYSTEM	0	2024-02-22 13:55:01 GMT	Alcor Micro Corp.	Flash Drive	15E12348	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	SanDisk Corp.	Cruzer Blade	0301982907052205443 6	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	VMware, Inc.	Virtual USB Hub	6&30c5d09c&0&7	CrypticWilds.000
SYSTEM	0	2024-03-04 18:12:46 GMT	VMware, Inc.	Virtual USB Hub	6&30c5d09c&0&8	CrypticWilds.000

Data Content

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 5 of 13 Result USB Device Attached

Type	Value	Source(s)
Date/Time	2024-02-22 13:55:01 GMT	Recent Activity
Device Make	Alcor Micro Corp.	Recent Activity
Device Model	Flash Drive	Recent Activity
Device ID	15E12348	Recent Activity
Source File Path	/img_CrypticWilds.000/vol_vol6/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775540	

Appendix L Glossary

Term	Definition
Autopsy	A forensic software suite used to analyse digital evidence such as emails, images, system logs, and web history. It also includes timeline and hashing modules.
BitLocker / BitLocker To Go	A Microsoft encryption tool used for securing entire drives or portable media like USBs. BitLocker To Go applies to USB devices.
BrowsingHistoryView	A tool used to extract and view browsing history from browsers such as Chrome and Edge.

CERTUTIL.EXE	A Windows command-line tool that can be used to encode files, manage certificates, and sometimes exfiltrate data.
Command Line Interface (CLI)	A text-based interface where forensic tools and scripts are executed, especially in Linux.
Custom Script	In this report, refers to personally written scripts (e.g., hash_cracker_SHA1.sh, photots_searcher.cpp) to automate forensic tasks.
DB Browser for SQLite	A GUI-based tool used to analyse SQLite databases, such as those storing web browser artifacts.
Disk Audit	A process using tools like fdisk, mmls, and parted to inspect drive structure, sectors, and hidden partitions.
Email Thread	A sequence of related emails, analysed in this report to determine communication chains between suspects.

Encrypted File (.gpg, .pgp)	Files that were protected using GPG/PGP encryption, requiring a private key to decrypt.
Encryption	The process of transforming data into a secure format. Used in the report for securing documents and communication.
Exif Metadata	Embedded data in images indicating details like time taken, device used (e.g., Canon EOS), and location.
FDISK / MMLS / PARTED	Tools used to analyse disk partitions and identify hidden or unallocated space.
File Extraction	The act of copying files from a forensic image for deeper analysis, typically preserving integrity via hashing.
FTK Imager	A forensic acquisition tool used for imaging drives and viewing evidence in a forensically sound manner.

GPG / GPG4Win	Encryption tools used for securing files. GPG is the engine; Gpg4win is the Windows package.
Hash Function (MD5 / SHA1 / SHA256)	Algorithms used to create digital fingerprints for verifying file integrity and detecting tampering.
Hash Verification	Comparing hash values before and after copying to ensure no modification occurred.
Image Previewing	Refers to Autopsy's ability to show thumbnails of images found on the drive, often used in manual review.
Incident Numbering	A systematic way of labelling events (e.g., Incident #4 – Emails), used throughout the report.
Kleopatra	The graphical user interface for managing encryption keys in the Gpg4win suite.

Loopback Device	A virtual device used to mount a forensic image on a Linux system for safe, read-only analysis.
Malware Scan	A check for malicious software (e.g., via volatility malfind) to confirm if the system was compromised.
MD5 / SHA1 / SHA256	Cryptographic hashing algorithms used for file integrity checks. SHA256 is stronger than MD5 or SHA1.
Mounting	Attaching a disk image to a system in a read-only mode for analysis, often through Linux or FTK Imager.
Npcap / USBPcap	Tools for capturing network and USB traffic. Used to investigate possible communications or data exfiltration.
Poetry Obfuscation	The act of hiding meaning or intentions using poetry or symbolic language, often combined with translation (e.g., Afrikaans).

Public Key / Private Key	The cryptographic pair used in GPG encryption. Public keys encrypt data; private keys decrypt it.
Registry / Registry Explorer / Regripper	The Windows Registry is a database of configuration settings. Regripper and Registry Explorer are used to extract and analyze it.
SHA1 Hash Cracking	The process of trying to recover a password from a known SHA1 hash using scripts or tools.
SQLite	A lightweight database format used by browsers to store cookies, login data, and autofill records.
Steghide	A tool used to hide data within images or audio files. It was found installed but inconclusive in usage.
System Artifacts	Data such as installed programs, run commands, user profiles, and login data that provide insight into user behavior.

Timeline Analysis	Using timestamps across different artifacts to reconstruct the sequence of suspect actions.
Volatility (v3)	A memory forensics tool used to analyse RAM dumps, often for hidden processes or suspicious behaviour.
Whitelist	A list of safe or known-good file hashes used to filter out irrelevant or benign system files during analysis.
Windows 11	The operating system version confirmed on the suspect's device. Helps determine compatibility and expected artifacts.