University of East London

Pioneering Futures Since 1898

School of Architecture, Computing and Engineering

Module code: CN7019

Module Title: Digital Forensics (Term 2)

Module Leader: Dr. Tauseef Ahmed
Moses Bankole, Dr Halima Kure, Dr Athirah Mohd Ramly

Assignment Title: Digital Crime Scene Investigation

BY:

SAURAV GURUNG - U2773653

Table of Contents

Table of Figures

Introduction

The results of a computer forensic investigation into the illegal owl trafficking have been provided in this study. In this case, owls are a protected species and it is completely prohibited to trade them. When a suspect tried to buy owls via illegitimate means, a computer was seized.

In this scenario, I am a part of a team of digital forensic consultants to provide necessary help in investigation for a government law enforcement agency in examining the digital evidence. A forensic image of the suspect's computer had already been created for further analysis.

The main aim of this investigation was to identify the suspect's digital footprint, including web activity, communications records, owl-related files, or any user-created content inside the computer, to determine involvement in illegal wildlife trade.

While going through the evidence manually, various items were found, including downloaded files, internet browsing history, search terms, and signs of USB devices being used. Deleted files from the recycle bin, cached web pages, and social media details also came up. There were several files and pictures which directly indicates the user intention and curiosity toward different types of owls, trade of owls and wildlife trade laws.

All investigation steps were carried out following ethical procedures to ensure the evidence remained original and unaltered.

The investigation was carried out using open-source forensic tools:

- Autopsy (V 4.21.0) (Technology, 2000)
- HxD (Hörz, 2003)
- Microsoft Excel (Cooperation, 2013)

Searching and finding all artifacts

The following data artifacts were found and noted during the investigation:

1. Operating System Information
   - OS: Windows 10 Pro
   - Owner: Sarah McAvoy
   - Manufacturer: Hewlett-Packard Company (HP)

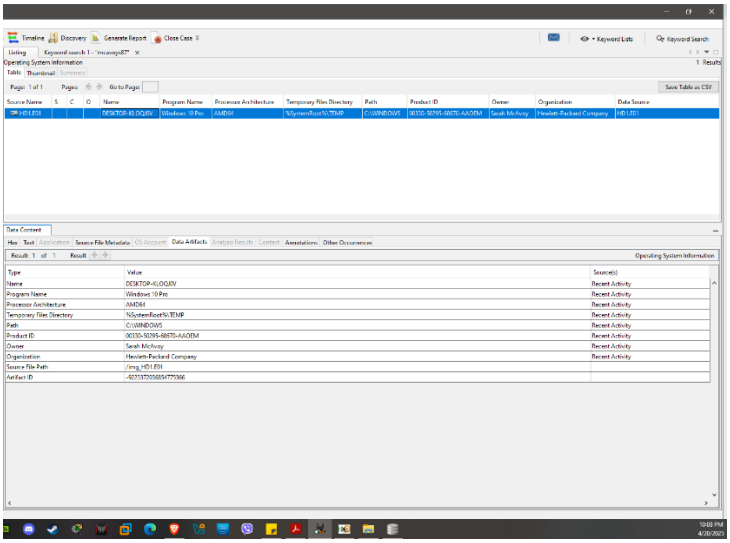


Figure 1 OS Information

2. Chromium Extensions
   A Chromium extension named Crypto Token Extension was discovered.

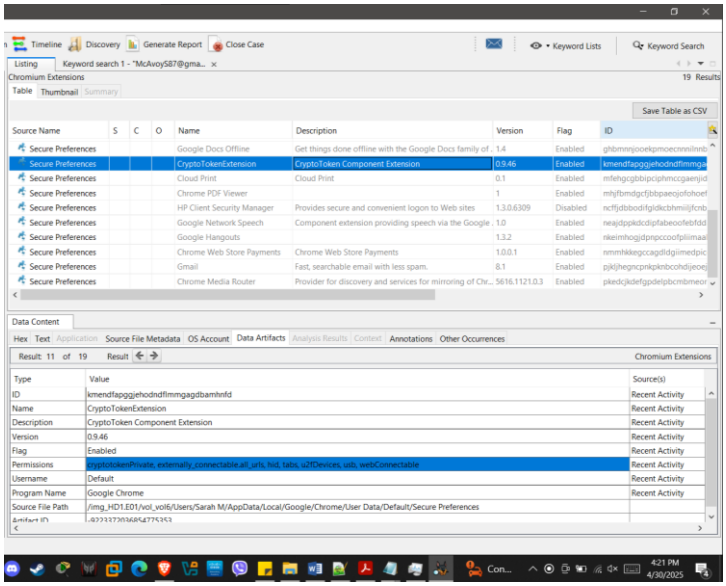


Figure 2 Crypto Token Extension

3. Email Messages
   A set of emails referencing the exchange of private and public keys was discovered.

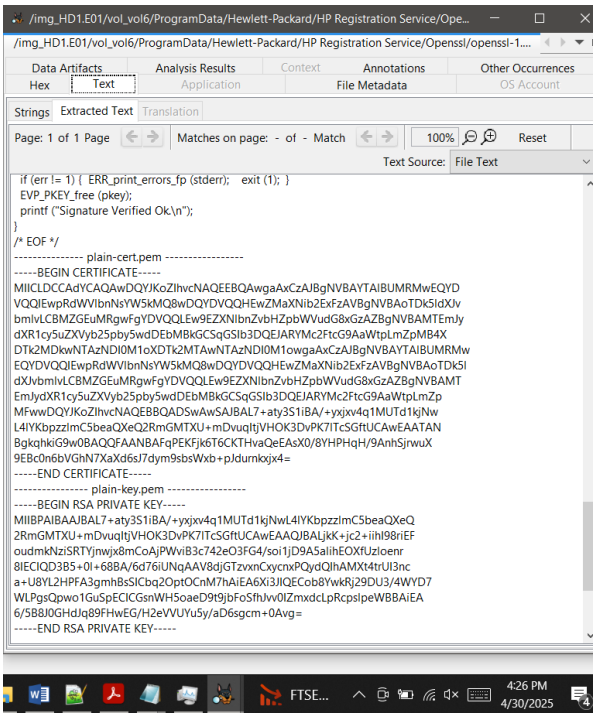


Figure 3 Cryptography-Keys

4. Recent Documents
   There were 58 recent files discovered and some of them are:
   - Great Horned Owl Info.lnk
   - Great Horned Owl.lnk
   - Owl_Emergency_Care.pdf.lnk
   - Owl_keeping.lnk
   - Snowy Owl.jpg.lnk
   - Pygmy Owl.jpg.lnk

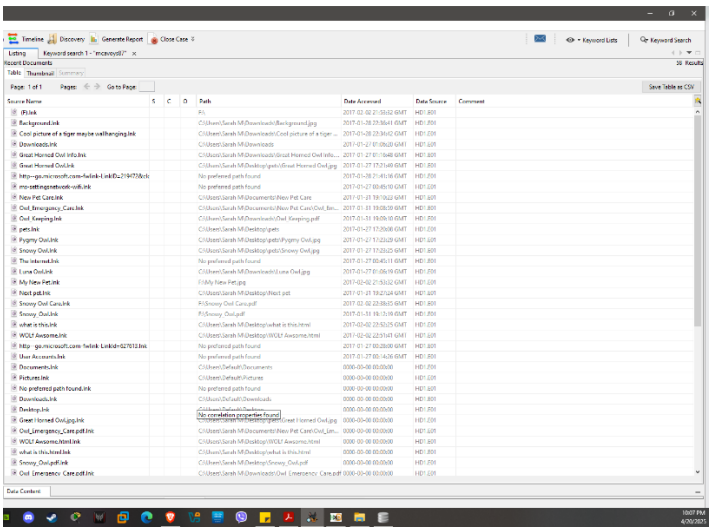


Figure 4 Recent Documents

5. Recycle Bin
   There were 6 files discovered in the Recycle Bin.
   - Pygmy owl.jpg
   - Next pet.jpg
   - Luna Owl.jpg
   - Great Horned Owl.jpg
   - Snowy_Owl.pdf
   - Great Horned Owl Info.pdf.

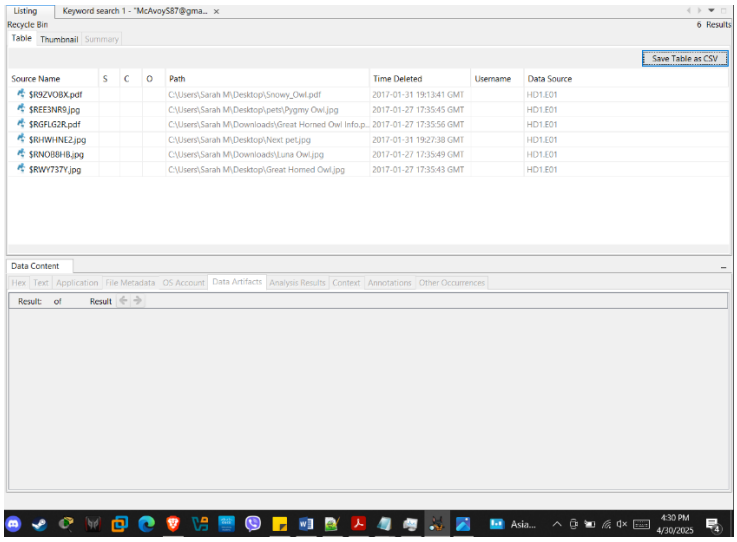


Figure 5 Recycle Bin

6. Shell Bags
   During further searching, Shell Bags showing the following paths were discovered.
   - Explorer\SanDisk Secure Access
   - C:\User\Sarah\Desktop\pets stored owl images like Great Horned Owl.jpg

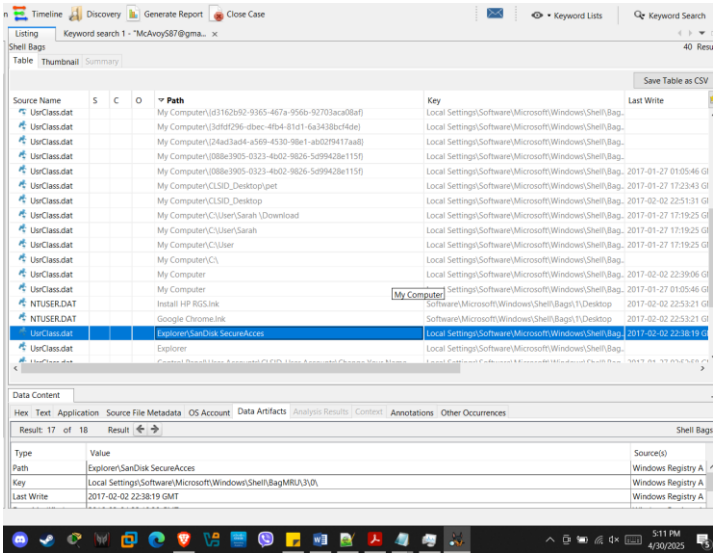


Figure 6 Shell Bag-Explorer\SanDisk Secure Access

7. USB Device Attached
   There were multiple devices identified:
   - 1 SanDisk Cruzer Glide
   - 1 Silicon Motion flash drive.
   - 2 fingerprint readers from Validity Sensor.
   - 4 HP HD webcams.

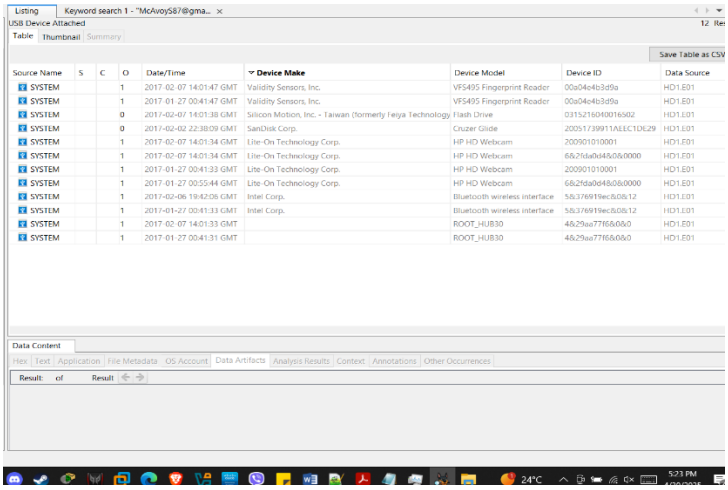


Figure 7 USB Device Attached

8. Web Accounts
   Multiple login details from several websites were discovered.
   - Google's login portal (accounts.google.com) was found with the username "mcavoys87."
   - In Facebook, the username "13046388446" was discovered.
   - The email address McAvoyS87@gmail.com was used to access Twitter and Yahoo.

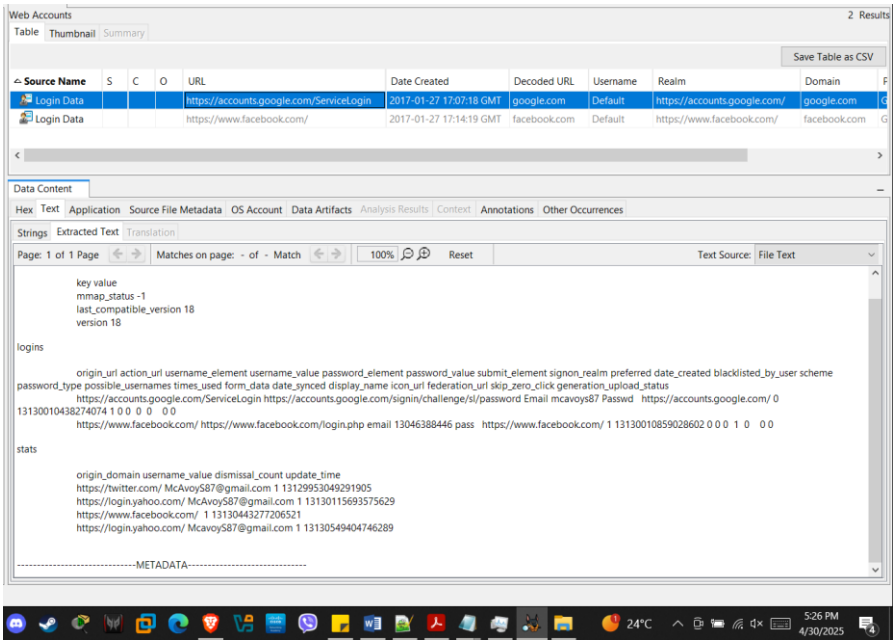


Figure 8 Web Accounts

9. Web Cache
   - Among 4675 web caches, 60 web caches contained the keyword owl on them.
     - Some of the websites are www.barnowltrust.org.uk, www.owl-help.org.uk, and many more.
   - Multiple posts in the Tumblr cache contain owl-related photos and hashtags.

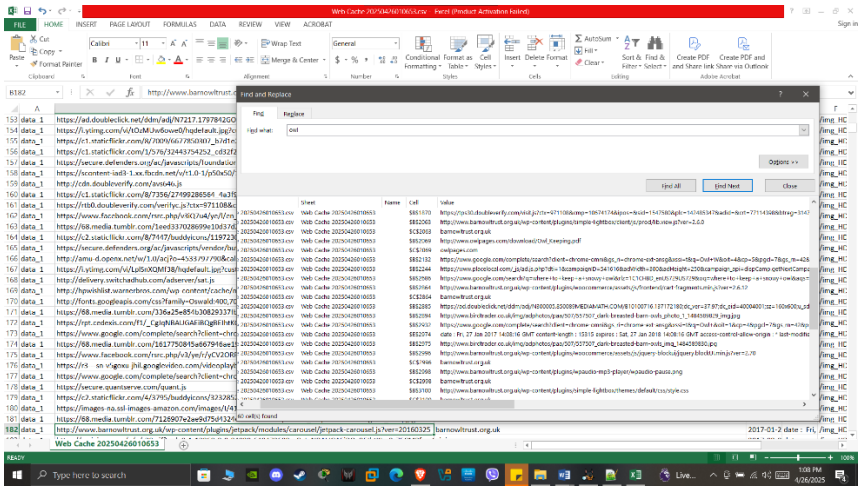


Figure 9 Web Caches-owl

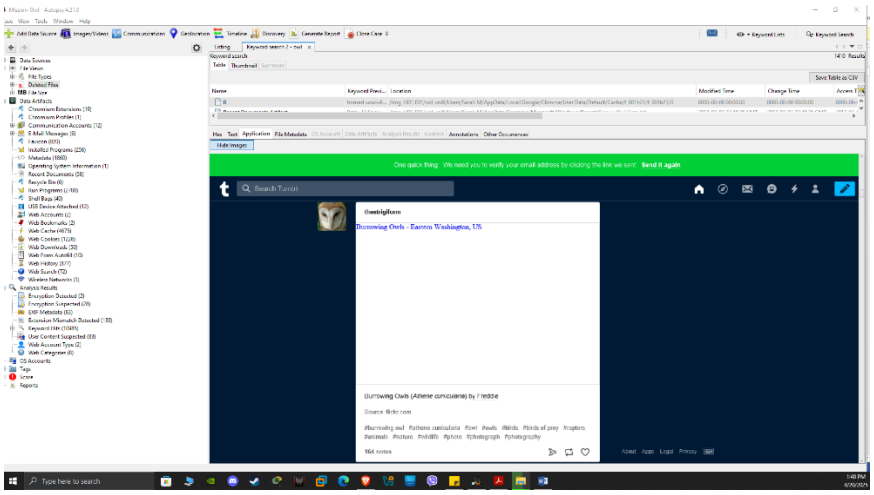


Figure 10 Tumblr-Hashtags

10. Web Cookies

    The keyword “bird” resulted in 46 matching cookies, and “owl” resulted in 8 matching cookies. Some of the website owl-related are:
    - Birdtrade.co.uk
    - Internationalowl.center.org, abcbirds.org and audubonportland.org
    - Defenders.org
    - Ncwildlife.org

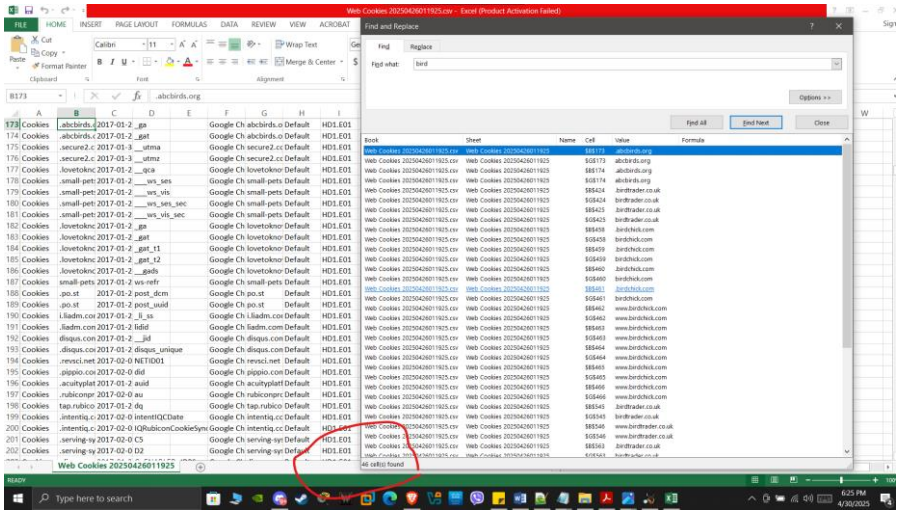


Figure 11 Web Cookies-bird

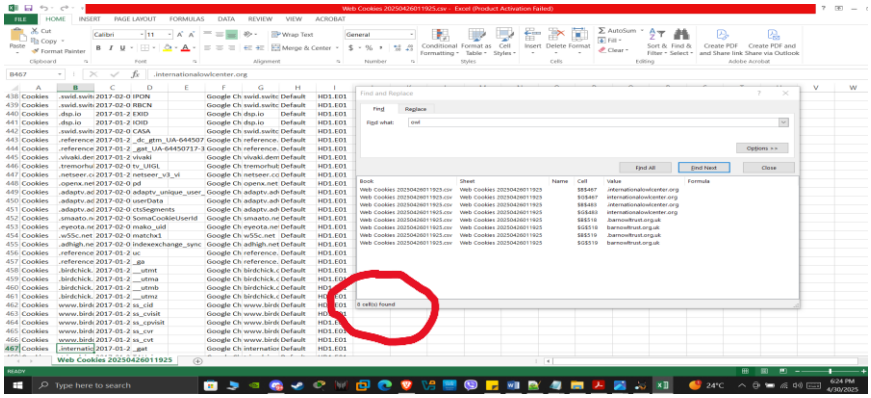


Figure 12 Web Cookies-owl

11. Web Downloads

A total of 51 downloaded files were identified. Some of them are:

- Luna Owl.jpg
- Owl_Emergency_Care.pdf
- Bibliography-Snowy Owl 14 April 2014-GLOW Posting.xls
- Owl_Keeping.pdf

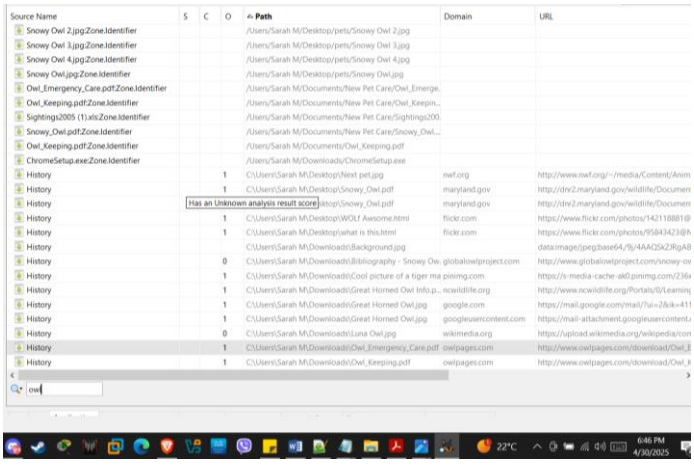


Figure 13 Web Downloads

12. Web Form Autofill

Personal information such as the username i.e., Sarah McAvoy, email address i.e., McAvoyS87@gmail.com, and, most importantly, the search query for “owl” were discovered.

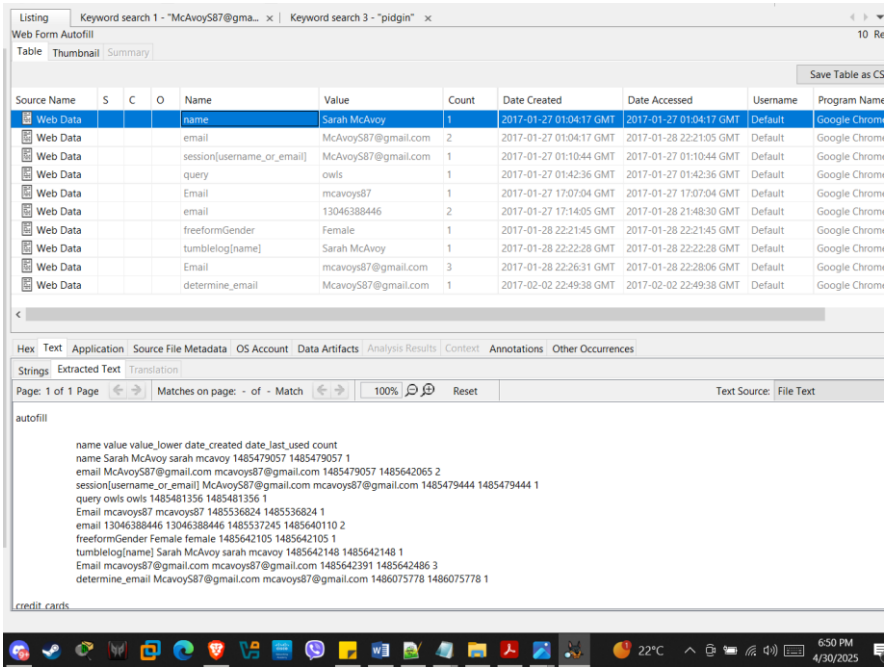


Figure 14 Web Form Autofill

13. Web History

A total of 877 web history entries were recovered. Keyword searches revealed 96 results for "bird," 376 results for "owl," and 5 results related to buying monkeys and owls. Some of them are:

- can you buy owl eggs
- can you buy monkey
- buying pet monkey
- can you buy snowy owls

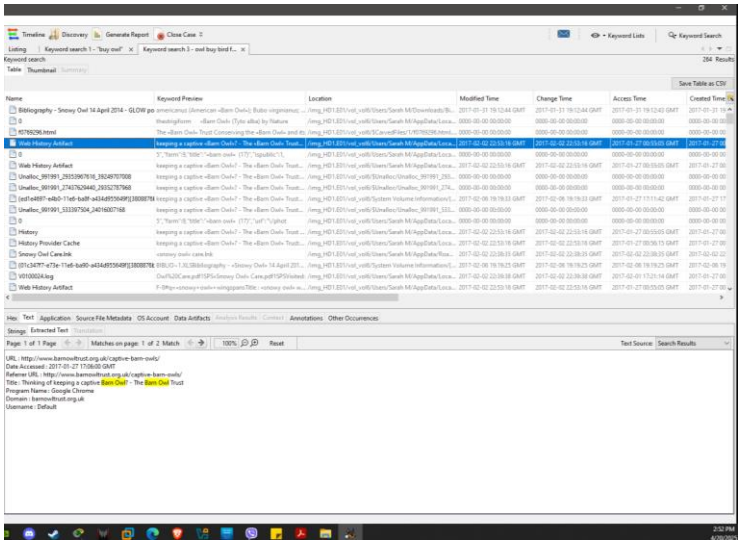


Figure 15 Web History-barn owl

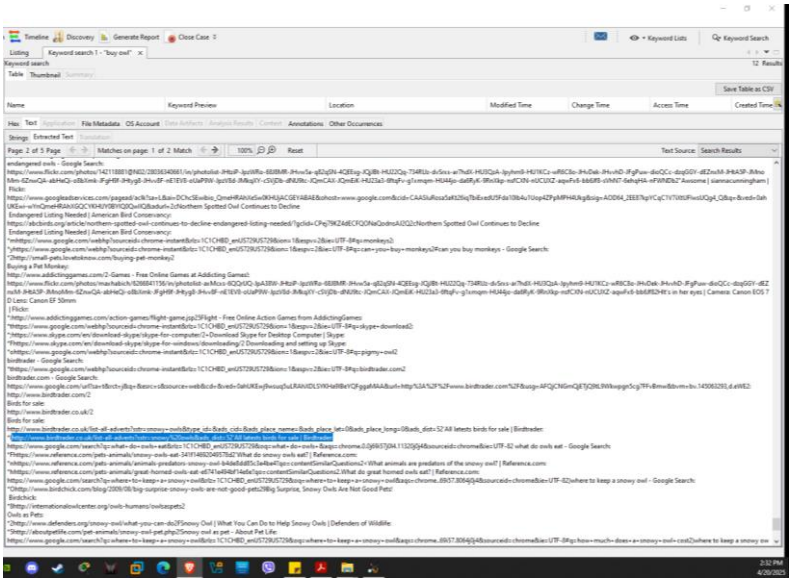


Figure 16 Web History-bird-trader

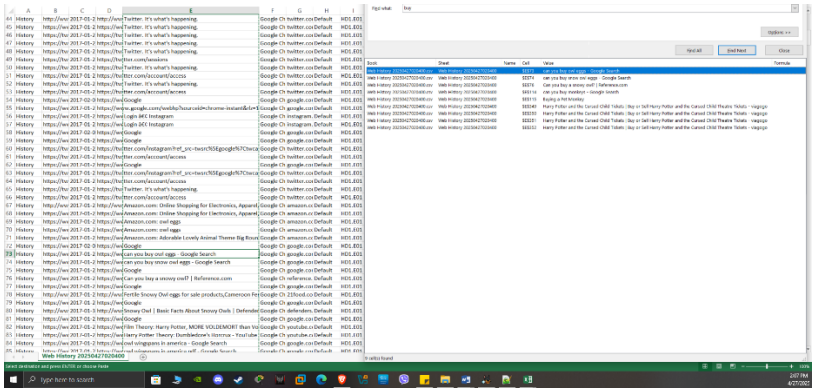


Figure 17 Web History-keyword-buy

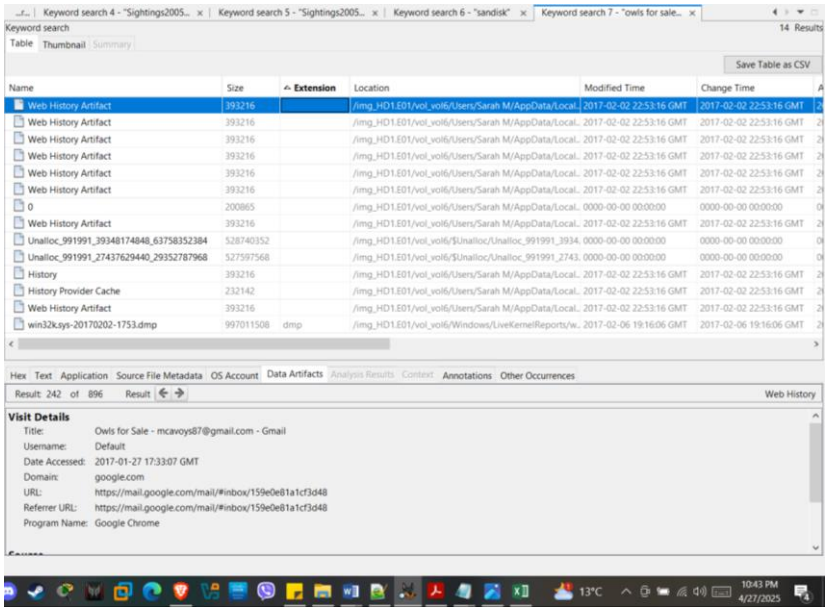


Figure 18 Email with title owl for sale

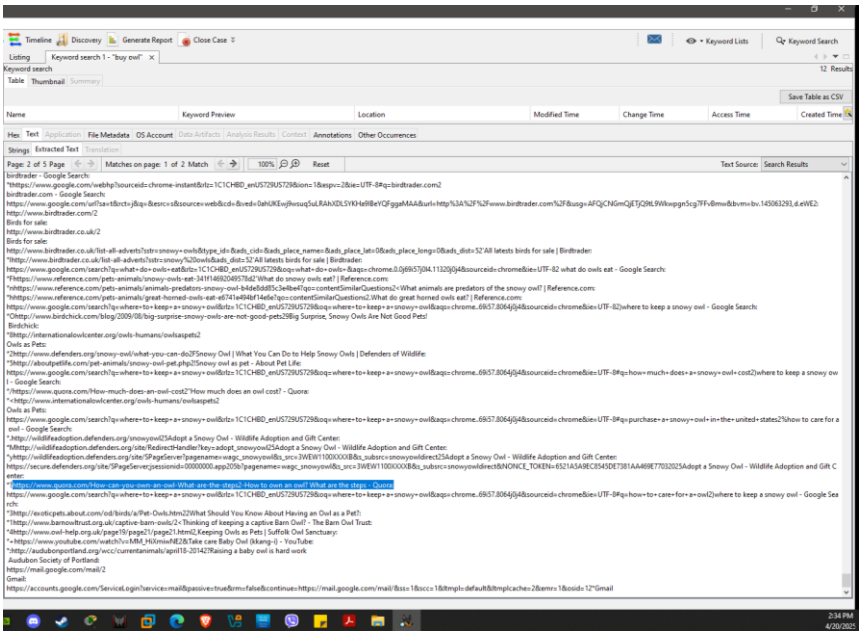


Figure 19 Web History-How to own an owl

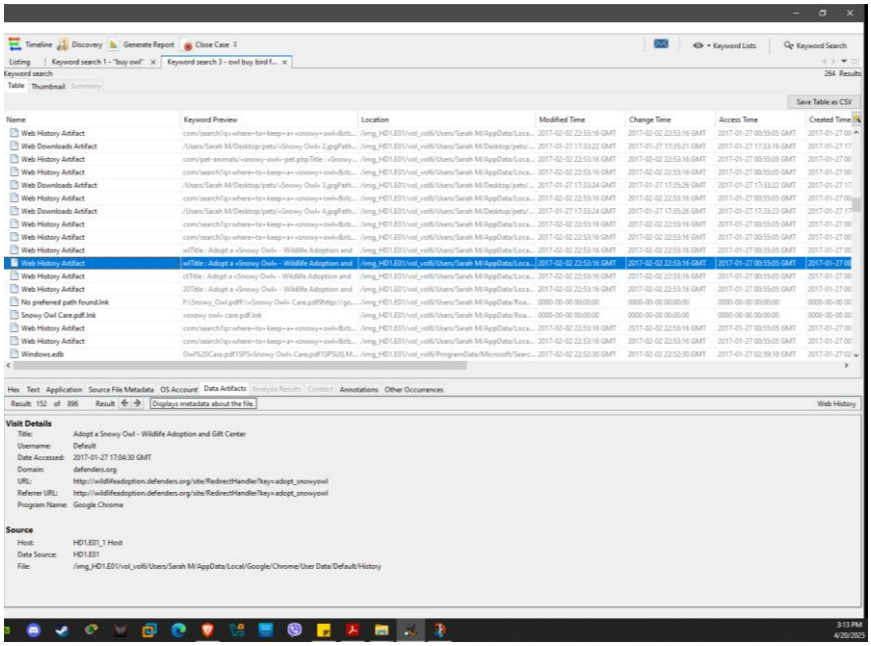


Figure 20 Web History Adopt a Snowy Owl

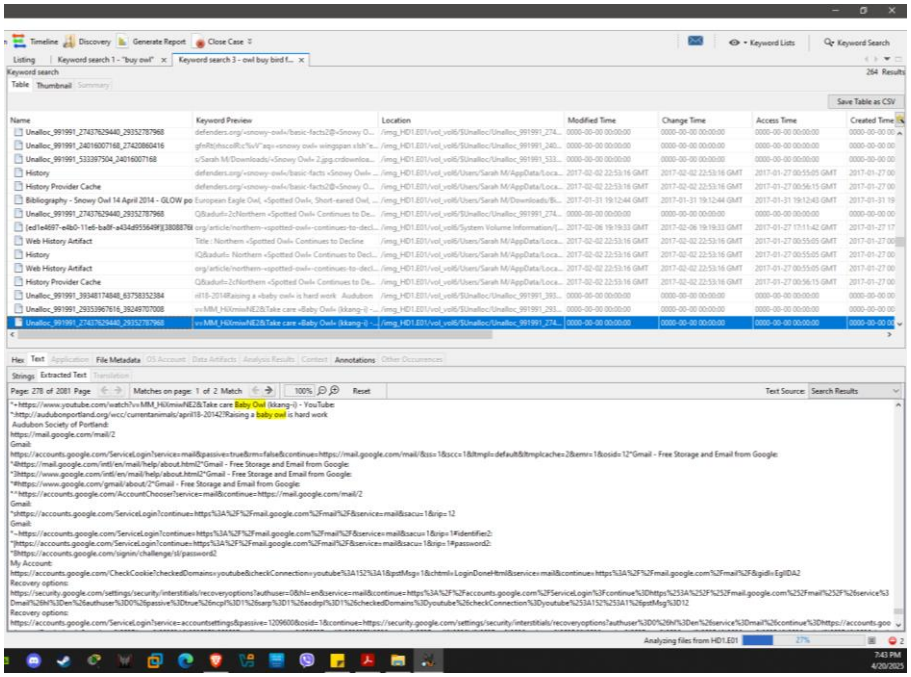


Figure 21 Web History-Baby Owl

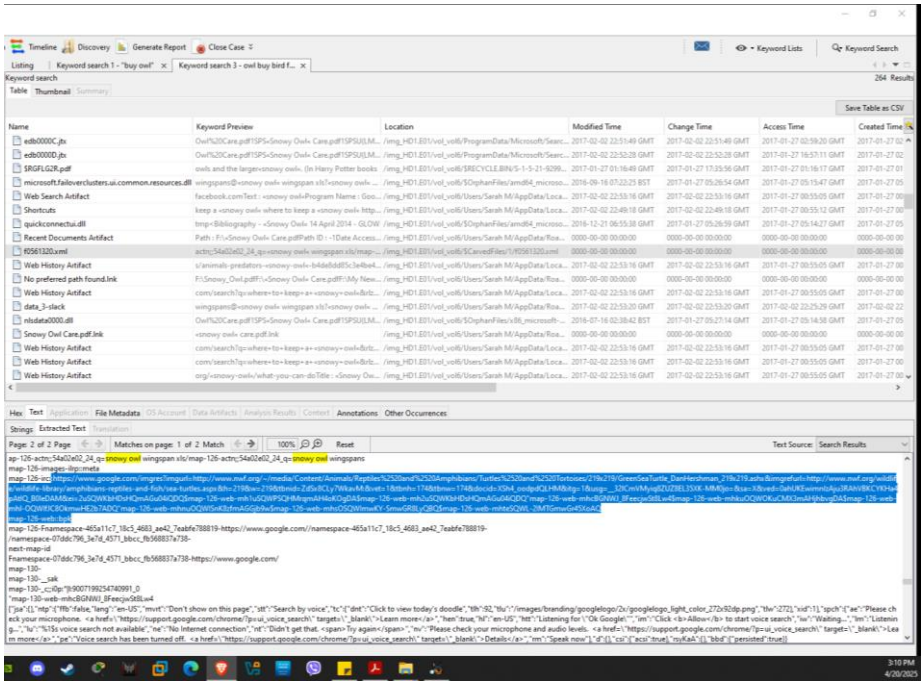
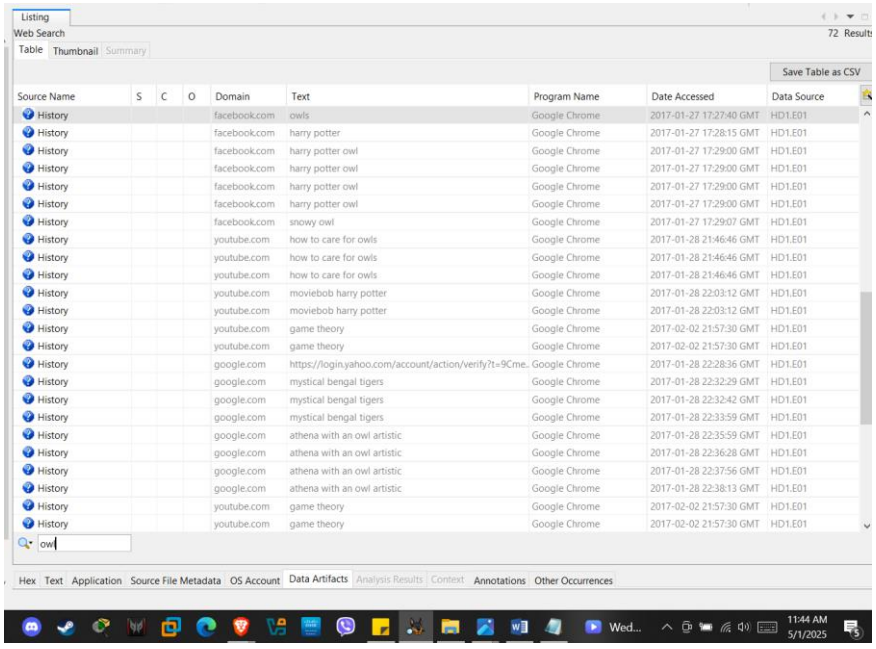


Figure 22 Web History Sea-Turtle

14. Web Search

Some of the web searches are:

- Where to keep a snowy owl
- harry potter owl
- how to care owls
- Athena with an owl artistic
- trippy owl pictures



Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				facebook.com	owls	Google Chrome	2017-01-27 17:27:40 GMT	HD1.E01
History				facebook.com	harry potter	Google Chrome	2017-01-27 17:28:15 GMT	HD1.E01
History				facebook.com	harry potter owl	Google Chrome	2017-01-27 17:29:00 GMT	HD1.E01
History				facebook.com	harry potter owl	Google Chrome	2017-01-27 17:29:00 GMT	HD1.E01
History				facebook.com	harry potter owl	Google Chrome	2017-01-27 17:29:00 GMT	HD1.E01
History				facebook.com	harry potter owl	Google Chrome	2017-01-27 17:29:00 GMT	HD1.E01
History				facebook.com	snowy owl	Google Chrome	2017-01-27 17:29:07 GMT	HD1.E01
History				youtube.com	how to care for owls	Google Chrome	2017-01-28 21:46:46 GMT	HD1.E01
History				youtube.com	how to care for owls	Google Chrome	2017-01-28 21:46:46 GMT	HD1.E01
History				youtube.com	how to care for owls	Google Chrome	2017-01-28 21:46:46 GMT	HD1.E01
History				youtube.com	moviebob harry potter	Google Chrome	2017-01-28 22:03:12 GMT	HD1.E01
History				youtube.com	moviebob harry potter	Google Chrome	2017-01-28 22:03:12 GMT	HD1.E01
History				youtube.com	game theory	Google Chrome	2017-02-02 21:57:30 GMT	HD1.E01
History				youtube.com	game theory	Google Chrome	2017-02-02 21:57:30 GMT	HD1.E01
History				google.com	https://login.yahoo.com/account/action/verify?t=9Cme...	Google Chrome	2017-01-28 22:28:36 GMT	HD1.E01
History				google.com	mystical bengal tigers	Google Chrome	2017-01-28 22:32:29 GMT	HD1.E01
History				google.com	mystical bengal tigers	Google Chrome	2017-01-28 22:32:42 GMT	HD1.E01
History				google.com	mystical bengal tigers	Google Chrome	2017-01-28 22:33:59 GMT	HD1.E01
History				google.com	athena with an owl artistic	Google Chrome	2017-01-28 22:35:59 GMT	HD1.E01
History				google.com	athena with an owl artistic	Google Chrome	2017-01-28 22:36:28 GMT	HD1.E01
History				google.com	athena with an owl artistic	Google Chrome	2017-01-28 22:37:56 GMT	HD1.E01
History				google.com	athena with an owl artistic	Google Chrome	2017-01-28 22:38:13 GMT	HD1.E01
History				youtube.com	game theory	Google Chrome	2017-02-02 21:57:30 GMT	HD1.E01
History				youtube.com	game theory	Google Chrome	2017-02-02 21:57:30 GMT	HD1.E01

15. OS Account
    - 2 personal accounts are “Sarah McAvoy” and “Sarah M”
    - 3 administrative accounts
    - 1 guest account
    - 10 system/service accounts

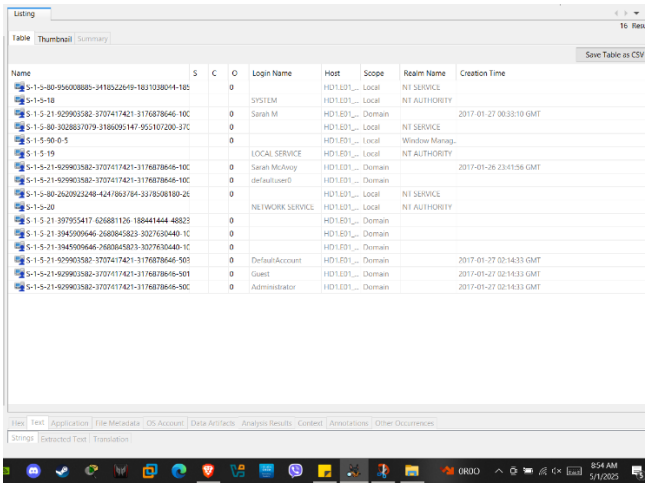


Figure 24 OS-user accounts

Analysis

For further investigation analysis, HxD and Microsoft Excel are used.

1. **Operating System and User Profile Analysis**

- Windows 10 Pro version (HP Computer) registered to “Sarah McAvoy”.
- 16 user accounts were found, and there are some findings:
    - ➢ The user “Sarah M” was created just 51 minutes after creating user “Sarah McAvoy” leading to suspicious timing and could indicate identity separation (one for normal use and one for illegal activity).
    - ➢ Files relating to owls from Recent Documents were accessed by user Sarah M.
    - ➢ The deleted owl-related files from the Recycle Bin, like Snowy_Owl.jpg were also logged in from Sarah M user.

2. **Key Evidence of Illegal Activity**

- ***Recent Documents Analysis***
- Repeated Access to Owl-Specific Files
- Approximately 58 recent documents were found during the analysis, which were identified through LNK (shortcut) files.
    - ➢ The picture of Owl inside the cage named My New Pet.jpg was also discovered.
    - The findings demonstrate the suspect’s curiosity regarding the care, species identification, and handling of owls, which indicates the suspect/user’s interest in buying owls. As the files were recently accessed, these shortcuts provide strong circumstantial evidence.

- External Drive Usage
    - ➢ F:\My New Pet.jpg and F:\Snowy Owl Care.pdf

- Findings of external storage drive.

- ***Recycle Bin Analysis***
- Deletion of Owl-Related Files
  - Snowy_Owl.pdf
  - Pygmy Owl.jpg
  - Great Horned Owl.jpg
  - Luna Owl.jpg
  - Great Horned Owl Info.pdf
  - Next Pet.jpg
  - Great Horned Owl Info.pdf was downloaded on 2017-01-27 and deleted the same day.
- The presence of owl-related material inside the Recycle Bin strongly indicates that the user/suspect may have attempted to avoid detection, which also highlights the user/suspect's awareness and intention to remove potential evidence.

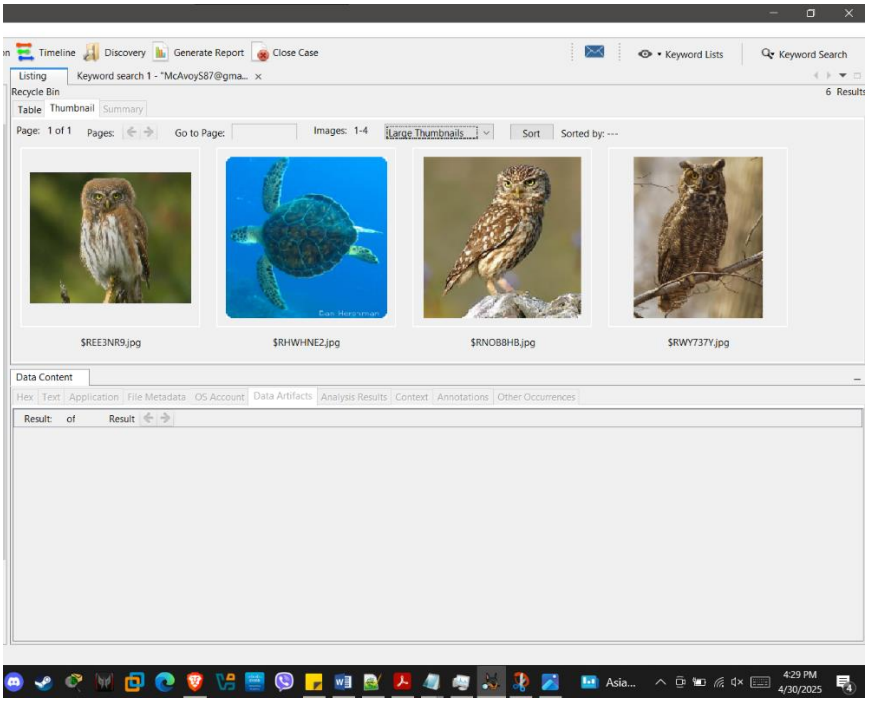


Figure 25 Recycle Bin Pictures

- ***Shell Bags Analysis***
- Shell Bags are the parts of the Windows registry that help the system remember a user's folder settings and activity. All the directories are tracked and recorded in registry (Eastwood, 2020).
- Folder Paths:
  - A folder named "Pet" consists of guides related to owl care and pictures of owls, which indicates the suspect has managed folders for owl-related topics.
- Use of Encrypted Storage
  - Path: Explorer\SanDisk Secure Access (last accessed February 2, 2017)
  - SanDisk SecureAccess has been used to store files in an encrypted and password-protected environment. Even though the files have been deleted,

the Shell Bags artifacts prove that the device/folder was last written on 2017-02-22 22:38:19 GMT.

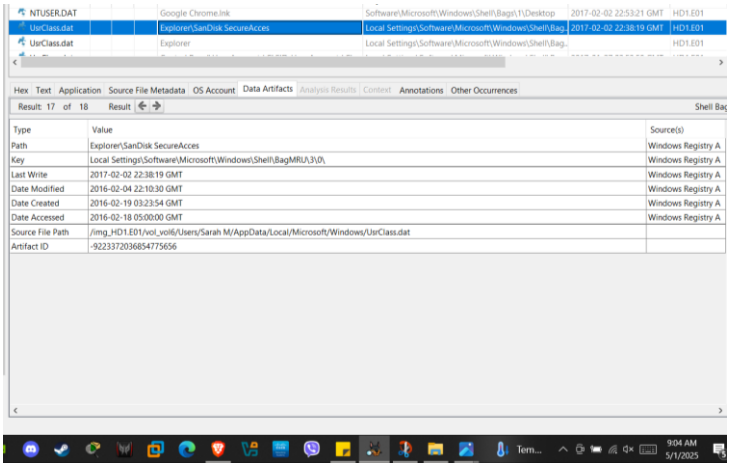


Figure 26 Shell Bag-SecureAccess

- ***USB Device Attached Analysis***
- SanDisk Cruzer Glide (Connected: 2017-02-02 22:38:09 GMT)
  - It could have been used to transfer or back up any illegal files before deleting them from the main system.
- Validity Sensors
  - Multiple connections (2017-01-27 and 2017-02-07)
  - It indicates biometric protection for devices or files.

- ***Web Accounts Analysis***
  - Different social media profiles such as Twitter, Facebook, and Yahoo were discovered.
  - A USA-based phone number was used for the Facebook profile.

- ***Web Cache Analysis***
  - Multiple Tumblr caches with posts containing owl photos and with the hashtag #borrowing_owl were discovered, which indicates the suspect/user has interest in owl trade.
  - 60 web caches containing the keyword “owl” were discovered, which indicates the user has visited the websites related to owl content.

- ***Web Cookies Analysis***
- Bird/Owl-Related and Wildlife regulation sites:
  - The suspect frequently visited Birdtrade.co.uk which is a site to trade birds that points to an active interest in the bird market. At the same time, the suspect also browsed conservation-focused resources like internationalowl.center.org, abcbirds.org and audobonportland.org which seems suspect to learn about protection laws and guidelines around trading owls.

- ***Web Downloads Analysis***
- Owl-related downloads:

- Multiple owl's images (snowy, great horned, and pygmy) and care guides (Owl Emergency Care) were downloaded.
- The suspect/user was likely researching about owl care, habitats or species.

- Exotic Pet Consideration
  - The suspect has also downloaded cool pictures of tigers or named the image file with next pet.jpg of Turtle, which indicates the suspect may be also exploring pets beyond owls.
- Extra Owl Data:
  - The suspect has also downloaded a file named “Sightings2005.xls” from fosc.org (wildlife tracking organization).
  - While analyzing the file, there are the details of the Eastern Screech Owl with its location and behavioral notes. The suspect might visit the place from these details.

- ***Web Form Analysis***
  - The name Sarah McAvoy has been used in multiple fields of social media like Tumblr.
  - The USA-based phone number 13046388446 was discovered, which could be the personal number of the suspect.

- ***Web History Analysis***
  - While investigating the web history of the suspect’s web browser, it has discovered strong evidence of keyword searches regarding illegal acquisition of owls. The suspect/user Sarah M has researched on purchasing owls visiting various platforms including Amazon, Craigslist and specialized bird-trading sites.
  - Keywords Searches like “purchase a snowy owl in the united states” strongly reflect that the suspect was searching to buy the owl inside the United States.
  - The suspect has also visited Amazon product listings with the search query “owl eggs”, visiting huntington.craigslist.org with the query “owls”, birdtrader.com and birdtrader.co.uk with the query of “owls” which shows the suspect to be visiting every site possible to buy owl eggs.
  - The email has been sent titled “Owls for sale” with the email address mcavoys87@gmail.com which shows the communication has been made using Gmail for the trade of owl.
  - Further investigating the web history, the suspect seems to watch Harry Potter, and there was Facebook search where the page named Daniel Radcliffe Fan Club has uploaded photo with owl with the caption Harry Potter and his pet Snowy Owl ‘Hedwig’. There were many Harry Potter web histories which also indicates that it may had influenced the suspect to buy owl.
  - The suspect has also visited the YouTube video titled “take care baby owl (kkang-i)” which indicates that the suspect was curious to learn to take care of the owl.

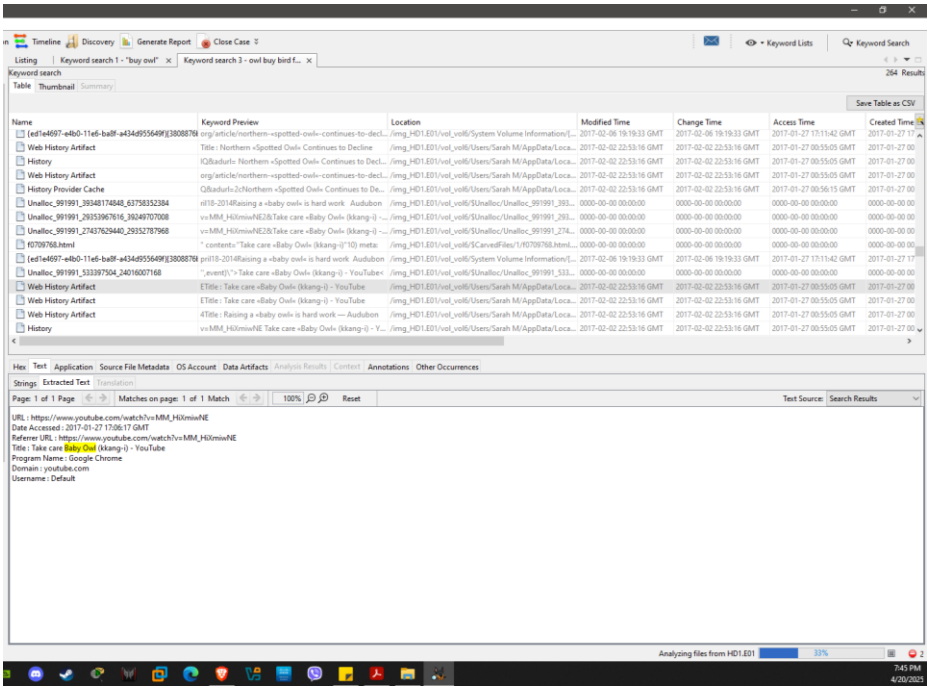


Figure 27 Web History-YouTube take care baby owl

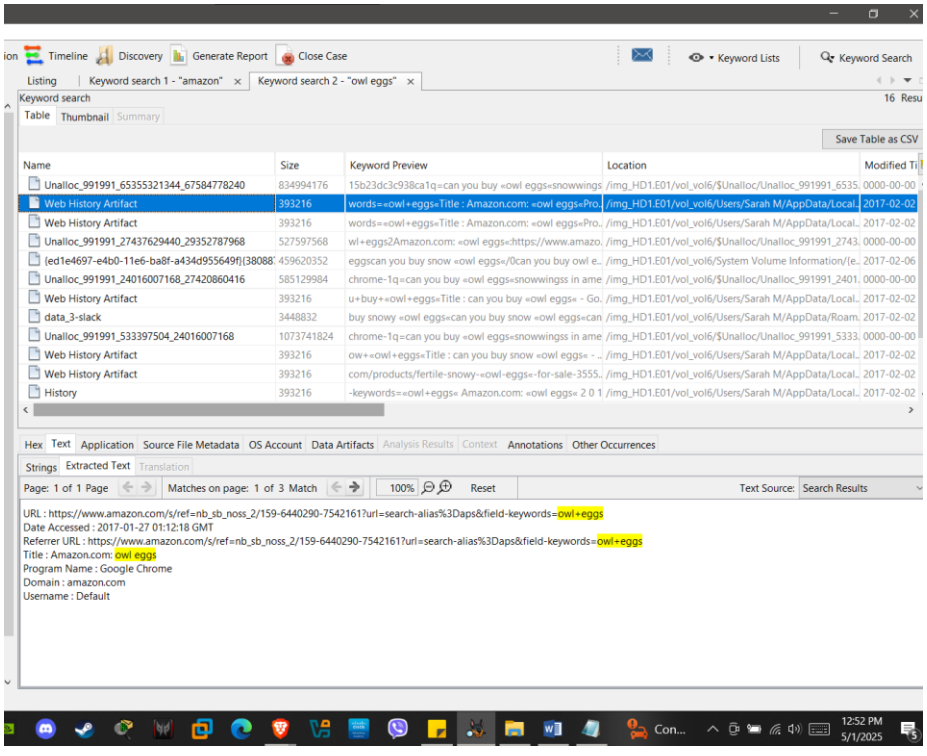


Figure 28 Amazon-owl-eggs

Figure 29 Web History-harry potter with owl

- ***Web Search Analysis***
  - The Facebook search for “terry bunch” and “monica neff” alongside “harry potter owl” could be contacts to trade owls illegally.
  - The suspect’s repeated search **“**where to keep a snowy owl” for 19 times indicates the active preparation to own snowy owl.

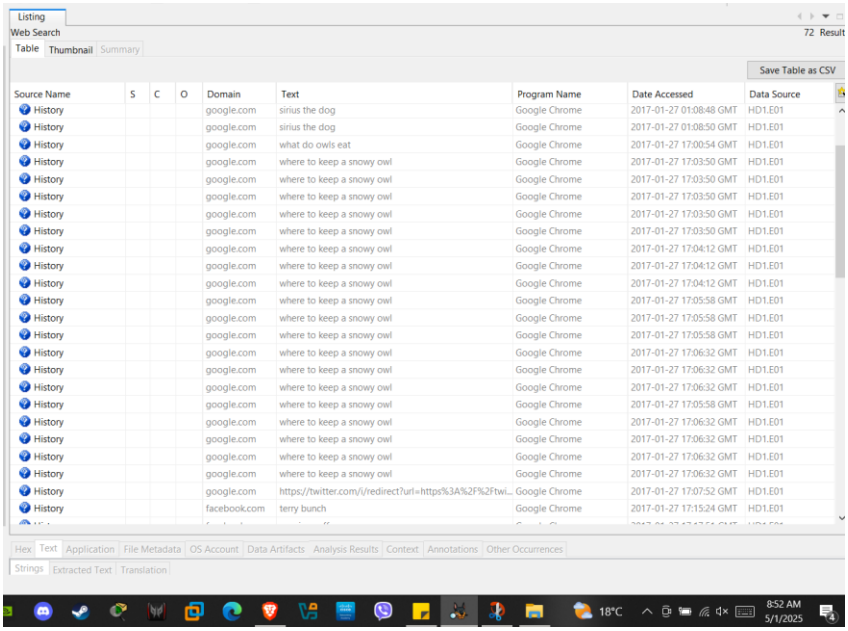


Figure 30 Web History 19 times search

3. *Deleted Files*

A total of 354125 files were deleted on this system. In deep analysis, the suspect has deleted some core cryptographic key that requires administrator privileges. The deletion may be to prevent recovery of encrypted chats or files. The plaintext password of the email McavoyS87@gmail.com was discovered from “f0010712.xml”.

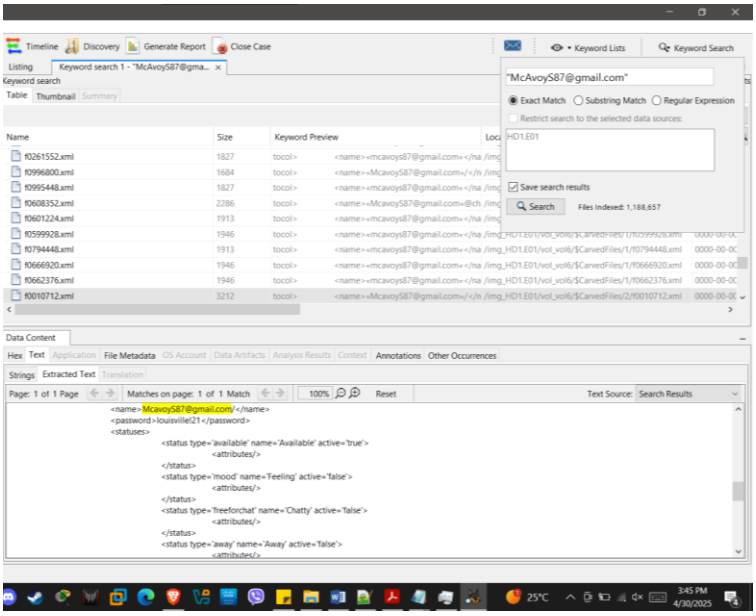


Figure 31 Gmail credentials

4. *Encryption*

The presence of both the Crypto Token Extension and key exchange emails suggests that encryption mechanisms were actively enabled by the user. The software Pidgin was installed on the system, which is an open-source application that offers end-to-end encryption.

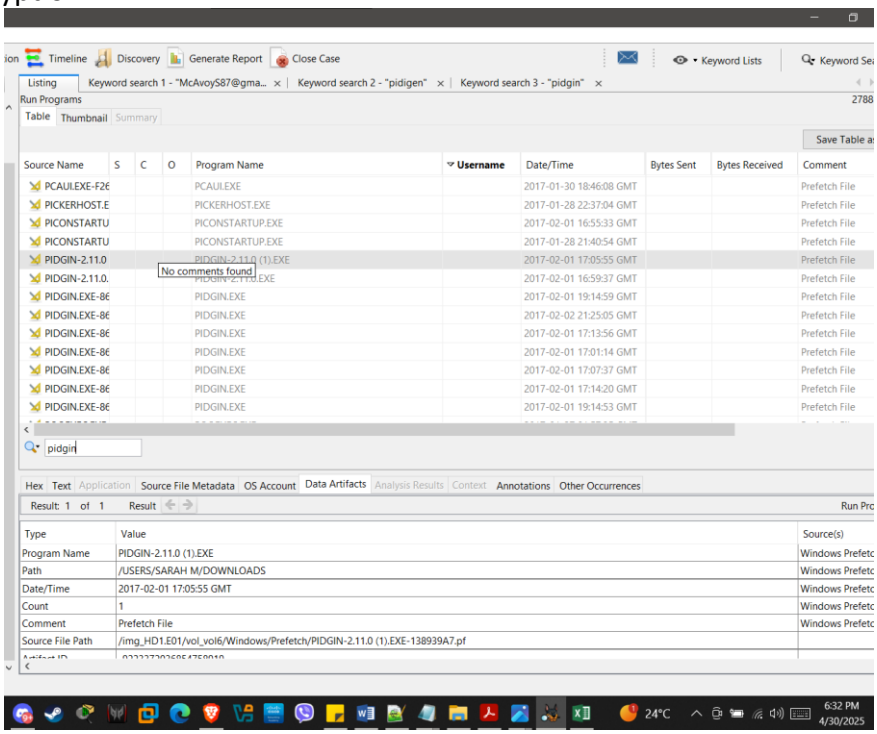


Figure 32 Pidgin installed

Conclusion

The digital forensic examination of suspect Sarah McAvoy's system reveals a suspicious pattern of intention, which indicates engagement in the illegal trade of owls. Findings of owl/bird-related artifacts such as web searches, repeated access to owl care manuals and images, deleted files in the Recycle Bin, encrypted storage via SanDisk SecureAccess and use of secondary user (Sarah M) aggregate the evidence of the suspect's preparation to acquire owls unlawfully. Furthermore, analysis reveals the evidence of encrypted communications (Crypto Token Extension and key-exchanged emails) and external device usage (USB device connection, deleted files and Robocopy installation) suggests the suspect's awareness of illegal activity and efforts to destroy the evidence after backup. However, there was no evidence of any payment made to buy an owl. In order to conclude the case, even though no financial evidences were discovered but the digital evidences that were discovered strongly points to an intentional violation of wildlife protection laws.

Expert Opinion

As a digital forensic investigator, this is my professional judgement that the evidence discovered from the suspect's system demonstrates the intention of research, preparation for and potentially engagement with illegal trade of owls. Key findings such as access to owl-related files in recent documents, owl-related searches in web histories, emails sent with the title Owls for Sale from mcavoys87@gmail.com, encrypted communications and efforts to delete owl-related files from the system indicate conscious effort to trade owls and bypass legal restrictions. The suspect could have visited the physical locations of Owl, which was on the downloaded file "Sightings2005.xls" from fosc.org (wildlife tracking organization). There was the photo of owl inside the cage named "My New Pet.jpg" inside the Pet folder which directs the suspect has been raising the owl but there was no evidence of any financial transaction, which has created doubt in the case. There are recommendations for further investigation:

- Request for legal search of Android Vortex HD65 android phone which is linked MFA to the Gmail access of "mcavoys87@gmail.com".
- Interview the suspect regarding external storage devices (SanDisk Cruzer Glide and Silicon Motion flash drive).
- Inspect the suspect's bank records from periods correlating with owl-related searches to trace any suspicious transactions.
- Re-examine external devices for any encrypted or deleted files.

References

Cooperation, M., 2013. *Microsoft Excel 2013.* [Online] Available at: https://www.microsoft.com/ [Accessed 17 04 2025].

Eastwood, C., 2020. *Medium.* [Online] Available at: https://medium.com/ce-digital-forensics/shellbag-analysis-18c9b2e87ac7 [Accessed 20 04 2025].

Hörz, M., 2003. *mh-nexus.* [Online] Available at: https://mh-nexus.de/en/hxd/ [Accessed 17 04 2025].

Technology, B., 2000. *Autopsy Digital Forensics.* [Online] Available at: https://www.autopsy.com/download/ [Accessed 17 04 2025].

Activity Log

Date	Duration	Activity Performed
28/3/2025	30 minutes	Downloaded the CW Image.
28/3/2025	10 minutes	Downloaded/Installed Autopsy and Hxd.
5/4/2025-7/4-2025	48 hours approx.	Setup forensic image in Autopsy.
10/4/2025	3 hours	Researched digital forensic investigation steps and created a basic roadmap for the case.
15/4/2025-20/4/2025	2 hours per day	Searched for the findings and recorded it on screenshot for reference.
21/4/2025-23/4/2025	3 hours per day	Reviewed the Artifacts.
24/4/2025-27/4/2025	2 hours per day	Began preparing documents.
28/4/2025	3 hours	Rechecked the documents.
2/5/2025	----------	Submitted the report.