



# 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**

Introduction .....	1
Searching and finding all artifacts.....	2
Analysis .....	13
Conclusion.....	20
Expert Opinion .....	20
References .....	21
Activity Log.....	21

## Table of Figures

Figure 1 OS Information .....	2
Figure 2 Crypto Token Extension .....	2
Figure 3 Cryptography-Keys.....	3
Figure 4 Recent Documents.....	3
Figure 5 Recycle Bin .....	4
Figure 6 Shell Bag-Explorer\SanDisk Secure Access .....	4
Figure 7 USB Device Attached.....	5
Figure 8 Web Accounts .....	5
Figure 9 Web Caches-owl .....	6
Figure 10 Tumblr-Hashtags.....	6
Figure 12 Web Cookies-bird.....	7
Figure 13 Web Cookies-owl .....	7
Figure 14 Web Downloads.....	7
Figure 15 Web Form Autofill.....	8
Figure 16 Web History-barn owl.....	9
Figure 17 Web History-bird-trader .....	9
Figure 18 Web History-keyword-buy.....	9
Figure 19 Email with title owl for sale .....	10
Figure 20 Web History-How to own an owl.....	10
Figure 21 Web History Adopt a Snowy Owl.....	11
Figure 22 Web History-Baby Owl.....	11
Figure 23 Web History Sea-Turtle.....	12
Figure 24 Web Searches .....	12
Figure 25 OS-user accounts .....	13
Figure 26 Recycle Bin Pictures .....	14
Figure 27 Shell Bag-SecureAccess.....	15
Figure 28 Web History-YouTube take care baby owl .....	17
Figure 29 Amazon-owl-eggs.....	17
Figure 30 Web History-harry potter with owl .....	18
Figure 31 Web History 19 times search .....	18
Figure 32 Gmail credentials .....	19
Figure 33 Pidgin installed.....	19

## 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.

Timeline		Discovery		Generate Report		Close Case		File		Keyword Lists		Search									
Listing		Keyword search 1 - "McAvoy587@gmail.com"										Keyword Search									
Chromium Extensions																					
Table			Thumbnail			Summary						Save Table as CSV									
Source Name	S	C	O	Name	Description	Version	Flag	ID													
Secure Preferences				Google Docs Offline	Get things done offline with the Google Docs family of...	1.4	Enabled	pharmenmgbpckjgmcnmbm...													
Secure Preferences				CryptoTokenExtension	CryptoToken Component Extension	0.9.46	Enabled	kmendfppggjehhodnlflmmaggbamhfd													
Secure Preferences				Cloud Print	Cloud Print	0.1	Enabled	mflngggpbpcpnccgcnjgi													
Secure Preferences				Chrome PDF Viewer		1	Enabled	mlhfbmgdpgjbbpaegofchod													
Secure Preferences				HP Client Security Manager	Provides secure and convenient logon to Web sites	1.3.0.6309	Disabled	ncffjgbcdlgbidchlmji/cnb...													
Secure Preferences				Google Network Speech	Component extension providing speech via the Google...	1.0	Enabled	neajdpdcidpbafelcoefld													
Secure Preferences				Google Hangouts		1.3.2	Enabled	nikemhqjgdpccpimflma...													
Secure Preferences				Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.1	Enabled	nnmmhkgelcgajdgimdepic													
Secure Preferences				Gmail	Fast, searchable email with less spam.	8.1	Enabled	pjkljhepgnpkigbcnhdjjeo...													
Secure Preferences				Chrome Media Router	Provider for discovery and services for mirroring of Chr...	5616.1120.1.0.3	Enabled	pkedcjkegdppdrjpbcmh...													

*Figure 2 Crypto Token Extension*

### 3. Email Messages

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

/img\_HD1.E01/vol\_vol6/ProgramData/Hewlett-Packard/HP Registration Service/Openssl-1....

Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Hex	Text	Application	File Metadata	OS Account
<b>Strings</b>	<b>Extracted Text</b>	<b>Translation</b>		
Page: 1 of 1 Page	Matches on page: - of - Match	100%		Reset
Text Source: File Text				
{if (err != 1) { _ER_Pprint_errors_fp (stderr); exit (1); }				
EV_PKEY_free (pkey);				
printf ("Signature Verified Ok\n");				
}				
/* EOF */				
----- plain-cert.pem -----				
-----BEGIN CERTIFICATE-----				
MIICLCDAgYCAQoDQYKjZlhvhNAQEEBQAwgaAxCzABgNBVAYTAiBUMRmwEYQD				
VQJlQwpRdWlbhNysWQmQbWQDyVQhWzMaXnb2ExFzAVBgvNBVAoTDk5ldXv				
bmlvCBLMGEuLrgWfgyDFQQLLe9EZXnlbnZhzbPwVvdGbzGzAzbgnVBAMTEmly				
dRtX1cy5UzyVp2b5py5wbDeMBKGCSgS1b3DQEJARyMc2FcG9AaWtpLmZpMB4X				
DTk2DlxWntAZ1ND01m1xDt2MTAwNTA2ND01m1owgaCzAzbJbgNBVAYTAiBUMR				
EVQ/DQVWpIwpRwDmQbWQDyVQhWzMaXnb2ExFzAVBgvNBVAoTDk5l				
d3xlvbmlvCBLMGEuLrgWfgyDFQQLLe9EZXnlbnZhzbPwVvdGbzGzAzbgnVBAMT				
EmjdYXR1cy5UzyVp2b5py5wbDeMBKGCSgS1b3DQEJARyMc2FcG9AaWtpLmZp				
MfwDQYKjZlhvhNAQEEBQAQDsWwA5/BA+7at+y3S1/BA+-yxjx4q1MuTd1knJw				
11YKbpz2zIMCbaeQx02RgkGMxtXw+1mDw9tjtVHOK3DpVK7TCsGruCawEAATAN				
BgkqhQh9w0BAQGFAAnABqFj6T6CKThveQeAsXo/0/8YPh9Qf/9ahJnruWx				
9EcBcd6vgVNh7Xka6d5f7dm5bsBwxb+pJduMoqx4=				
-----END CERTIFICATE-----				
----- plain-key.pem -----				
----- BEGIN RSA PRIVATE KEY -----				
MIIBPAIBAAJBAl+at3y51BA/+yxjx4q1MuTd1kjhNl4YKbzplzImC5beaQxQe				
2rRgmtXm+DuqvjtVHOK3DpVK7TCsGruCawEAQjBALjk+Jc+iih98riEF				
oudmNsIRytwym8comA/PwiBv3c742e03fG4/s01/d9A59hlfOXfzu0zneer				
8E1C0D3B5 +0/688/6d761Qun0A8/8dJGtzvnxCycnxPQyQdQlhAMXt4rUl3nc				
a+U8Y1L2HPFA3grmhBsCIcq2OptOcm7hAiEAx3JlQEcob8WkrJ29DU3/4WYD7				
WLpqwoPwQpoSwPEcICGsrINWh5oea979jFoSfhvW0lZmxdlpRpCspeWBBAiEA				
6/588/0G9wJq99Hweg/H12evUuy5/aD6sgcm=0Av=				
-----END RSA PRIVATE KEY-----				

*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

File	Timeline	Discover	Generate Report	Close Case	Help	Keyboard Shortcuts	Keyword Search
Recent Documents					10 items		
Table		Thumbnail	Summary		Save Table as CSV		
Page 1 of 1	Pages	Go to Page	S	C	D	Paths	
Source Name	Date Accessed	Data Source	Comment				
10 items	2017-02-20 09:52:00	HDI-EMR					
10 items	2017-02-20 09:52:00	HDI-EMR					
Cool picture of a tiger maybe we'll change link	2017-02-20 09:52:00	HDI-EMR					
Unresolved	2017-02-20 09:52:00	HDI-EMR					
Great Hornbill link.xls	2017-02-20 09:52:00	HDI-EMR					
Unresolved	2017-02-20 09:52:00	HDI-EMR					
http://go.microsoft.com/fwlink/?LinkId=2147701.xls	No preferred path found	2017-02-19 09:46:00	HDI-EMR				
no-preferred-path.xls	No preferred path found	2017-02-07 08:00:00	HDI-EMR				
New Pet Cards.xls	2017-01-19 09:02:00	HDI-EMR					
Old Devignacy_Care.xlsx	2017-01-19 09:02:00	HDI-EMR					
Old Devignacy_Care.xls	2017-01-19 09:02:00	HDI-EMR					
pet.xls	2017-02-17 17:00:00	HDI-EMR					
Piggy.Doxfile	2017-02-17 11:20:00	HDI-EMR					
Snowy.Doxfile	2017-02-13 09:00:00	HDI-EMR					
Unresolved	No preferred path found	2017-02-13 09:00:00	HDI-EMR				
Unresolved	2017-02-10 09:00:00	HDI-EMR					
My New Pet.xls	2017-02-06 21:55:00	HDI-EMR					
No path.xls	2017-01-19 02:04:00	HDI-EMR					
Old Devignacy_Care.xls	2017-01-19 02:04:00	HDI-EMR					
Snowy.Doxfile	2017-01-18 19:00:00	HDI-EMR					
whet.Doxfile	2017-02-23 03:05	HDI-EMR					
WOW! Awesome.xls	2017-02-23 03:05	HDI-EMR					
http://go.microsoft.com/fwlink/?LinkId=2147701.xls	No preferred path found	2017-02-17 11:20:00	HDI-EMR				
Unresolved.xls	2017-02-17 11:20:00	HDI-EMR					
Picture.xls	2006-04-06 00:00:00	HDI-EMR					
No preferred path found.xls	No preferred path found	2006-04-06 00:00:00	HDI-EMR				
Unresolved	2006-04-06 00:00:00	HDI-EMR					
Unresolved	2006-04-06 00:00:00	HDI-EMR					
Green Hornet.Outlook.xls	No preferred path found	2006-04-06 00:00:00	HDI-EMR				
Old_Lunatic.xls_Care.pdf	2017-02-23 03:05	HDI-EMR					
Old_Awesome.xls	2017-02-23 03:05	HDI-EMR					
Old_Awesome.xls	2017-02-23 03:05	HDI-EMR					
Snowy.Outlook.xls	2006-04-06 00:00:00	HDI-EMR					
Out Unresolved_Care.pdf	2006-04-06 00:00:00	HDI-EMR					

#### *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.

Source Name	S	C	O	Path	Time Deleted	Username	Data Source
\$R92VOBX.pdf				C:\Users\Sarah M\Desktop\Snowy_Owl.pdf	2017-01-31 19:13:41 GMT	HD1.E01	
\$REEE3NR.jpg				C:\Users\Sarah M\Desktop\pets\Pygmy Owl.jpg	2017-01-27 17:35:45 GMT	HD1.E01	
\$RGH.G2.pdf				C:\Users\Sarah M\Downloads\Great Horned Owl Info.pdf	2017-01-27 17:35:56 GMT	HD1.E01	
\$RIWINIE2.jpg				C:\Users\Sarah M\Desktop\Next pet.jpg	2017-01-31 19:27:38 GMT	HD1.E01	
\$RNWBBH8.jpg				C:\Users\Sarah M\Downloads\Luna Owl.jpg	2017-01-27 17:35:49 GMT	HD1.E01	
\$RW737Y.jpg				C:\Users\Sarah M\Desktop\Great Horned Owl.jpg	2017-01-27 17:35:43 GMT	HD1.E01	

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

Source Name	S	C	O	Path	Key	Last Write	Value
UseClass.dat				My Computer\d3162b92-9365-467a-956b-92703aca0faf	Local Settings\Software\Microsoft\Windows\Shell\Bag		
UseClass.dat				My Computer\30df296-0bce-4f64-81d1-6a343b0cf4de	Local Settings\Software\Microsoft\Windows\Shell\Bag		
UseClass.dat				My Computer\24ad3a4d-a569-98b1-a02079417aa8	Local Settings\Software\Microsoft\Windows\Shell\Bag		
UseClass.dat				My Computer\00be3905-0323-4602-9826-5d99428e115f	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 01:05:46 GMT	
UseClass.dat				My Computer\00be3905-0323-4602-9826-5d99428e115f	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 17:23:43 GMT	
UseClass.dat				My Computer\CLSID/Desktop/jet	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-02-02 22:51:31 GMT	
UseClass.dat				My Computer\CLSID/Desktop	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 17:19:25 GMT	
UseClass.dat				My Computer\C:\User\Sarah\Downloads	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 17:19:25 GMT	
UseClass.dat				My Computer\C:\User\Sarah	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 17:19:25 GMT	
UseClass.dat				My Computer\C:\User	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 17:19:25 GMT	
UseClass.dat				My Computer\C:\	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-02-02 22:39:06 GMT	
UseClass.dat				My Computer	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-01-27 01:05:46 GMT	
NTUSER.DAT				Install HP RG5 Link	Settings\Software\Microsoft\Windows\Shell\Bag\1\Desktop	2017-02-02 22:52:21 GMT	
NTUSER.DAT				Google Chrome link	Software\Microsoft\Windows\Shell\Bag\1\Desktop	2017-02-02 22:52:21 GMT	
UseClass.dat				Explorer\SanDisk SecureAccess	Local Settings\Software\Microsoft\Windows\Shell\Bag	2017-02-02 22:38:19 GMT	
UseClass.dat				Explorer	Local Settings\Software\Microsoft\Windows\Shell\Bag		

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.

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM	1			2017-02-07 14:01:47 GMT	Validity Sensors, Inc.	VFS405 Fingerprint Reader	000a04cb3d9a	HD1.591
SYSTEM	1			2017-02-27 00:41:47 GMT	Validity Sensors, Inc.	VFS405 Fingerprint Reader	000a04cb3d9a	HD1.591
SYSTEM	0			2017-01-07 14:01:38 GMT	Silicon Motion, Inc. - Taiwan (formerly Iweya Technology)	Flash Drive	0315216040016502	HD1.591
SYSTEM	0			2017-02-02 22:38:09 GMT	Sandisk Corp.	Cruzer Glide	200517399111ACCE1DNC29	HD1.591
SYSTEM	1			2017-02-07 14:01:34 GMT	Lite-On Technology Corp.	HP HD Webcam	200901010001	HD1.591
SYSTEM	1			2017-02-07 14:01:34 GMT	Lite-On Technology Corp.	HP HD Webcam	682f6a0d48c060000	HD1.591
SYSTEM	1			2017-02-27 00:55:44 GMT	Lite-On Technology Corp.	HP HD Webcam	200901010001	HD1.591
SYSTEM	1			2017-02-06 19:42:00 GMT	Intel Corp.	Bluetooth wireless interface	5837e919ec0c0512	HD1.591
SYSTEM	1			2017-02-27 00:41:13 GMT	Intel Corp.	Bluetooth wireless interface	5837e919ec0c0512	HD1.591
SYSTEM	1			2017-02-07 14:01:31 GMT	ROOT_HUB30	4829aa77f660000	HD1.591	
SYSTEM	1			2017-01-27 00:41:31 GMT	ROOT_HUB30	4829aa77f660000	HD1.591	

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](mailto:McAvoyS87@gmail.com) was used to access Twitter and Yahoo.

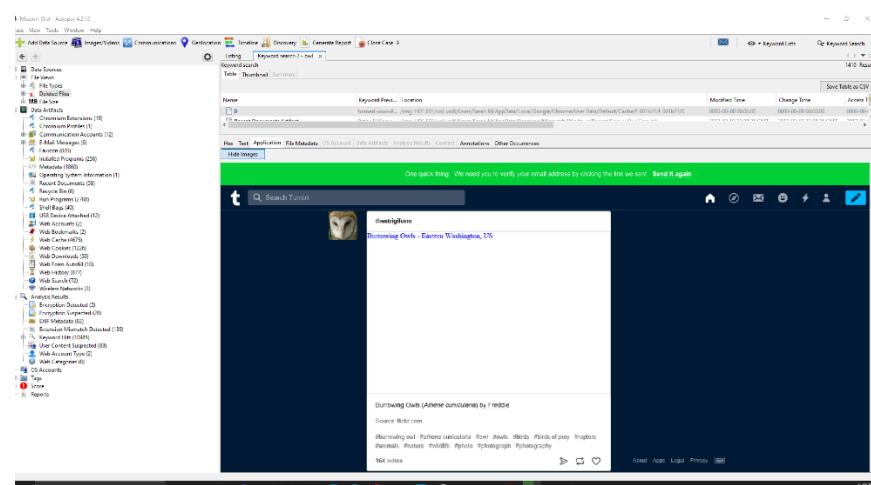
Source Name	S	C	O	URL	Date Created	Decoded URL	Username	Realm	Domain	F
Login Data				https://accounts.google.com/ServiceLogin	2017-01-27 17:07:18 GMT	google.com	Default	https://accounts.google.com/	google.com	G
Login Data				https://www.facebook.com/	2017-01-27 17:14:19 GMT	facebook.com	Default	https://www.facebook.com/	facebook.com	G

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](http://www.barnowltrust.org.uk), [www.owl-help.org.uk](http://www.owl-help.org.uk), and many more.
  - Multiple posts in the Tumblr cache contain owl-related photos and hashtags.

*Figure 9 Web Caches-ow*



*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*

The screenshot shows the Microsoft Edge browser interface. In the address bar, the URL 'internationallawcenter.org' is entered. Below the address bar, the status bar displays '8 results Found'. The main content area shows a table of 446 cookies. The columns in the table are 'Name', 'Value', 'SameSite', 'Path', 'Expires', 'Domain', 'HostOnly', 'Secure', 'HttpOnly', and 'Origin'. The 'Origin' column shows the source of each cookie as 'Web Cookies'. The 'SameSite' column contains values like 'lax', 'strict', and 'none'. The 'Path' column includes paths such as '/', '/.well-known', and '/.well-known/acme-challenge'. The 'Expires' column shows dates ranging from 2017-02-01 to 2024-06-20. The 'Domain' column consistently shows 'internationallawcenter.org'. The 'HostOnly' and 'Secure' columns are mostly checked. The 'HttpOnly' column has mixed values. The 'Origin' column is also present in this view.

*Figure 12 Web Cookies-ow*

## 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

Source Name	S	C	O	Path	Domain	URL
Snowy Owl 2.jpg.Zone.Identifier				/Users/Sarah/M/Desktop/pets/Snowy Owl 2.jpg		
Snowy Owl 3.jpg.Zone.Identifier				/Users/Sarah/M/Desktop/pets/Snowy Owl 3.jpg		
Snowy Owl 4.jpg.Zone.Identifier				/Users/Sarah/M/Desktop/pets/Snowy Owl 4.jpg		
Snowy Owl 5.jpg.Zone.Identifier				/Users/Sarah/M/Desktop/pets/Snowy Owl.jpg		
Owl_Emergency_Care.pdf.Zone.Identifier				/Users/Sarah/M/Documents/New Pet Care/Owl_Emerg...		
Owl_Keeping.pdf.Zone.Identifier				/Users/Sarah/M/Documents/New Pet Care/Owl_Keepin...		
Sightings2005 (1).xsl.Zone.Identifier				/Users/Sarah/M/Documents/New Pet Care/Sightings20...		
Snowy_Owl.pdf.Zone.Identifier				/Users/Sarah/M/Documents/New Pet Care/Snowy_Owl...		
Owl_Keeping.pdf.Zone.Identifier				/Users/Sarah/M/Documents/Owl_Keeping.pdf		
ChromeSetup.exe.Zone.Identifier				/Users/Sarah/M/Downloads/ChromeSetup.exe		
History	1			C:\Users\Sarah\M\Desktop\Next pet.jpg	nef.org	http://www.nef.org/~media/Content/Anim...
History	1			C:\Users\Sarah\M\Desktop\Snowy_owl.pdf	maryland.gov	http://dnr2.maryland.gov/wildlife/Docume...
History	1			C:\Users\Sarah\M\Desktop\WOLF_Awesome.html	flickr.com	https://www.flickr.com/photos/142118881@N...
History	1			C:\Users\Sarah\M\Desktop/what is this.html	flickr.com	https://www.flickr.com/photos/9594327@N...
History	0			C:\Users\Sarah\M\Downloads\Background.jpg	data:image/jpeg;base64,PAACZB9gS...	data:image/jpeg;base64,PAACZB9gS...
History	1			C:\Users\Sarah\M\Downloads\Bibliography - Snowy_owl.globalowlpix.com	https://www.globalowlpix.com/Project...	https://www.globalowlpix.com/Project...
History	1			C:\Users\Sarah\M\Downloads\Cool picture of a tiger ma...ping.com	https://media.cache.e6.alpinetech.com/2...	https://media.cache.e6.alpinetech.com/2...
History	1			C:\Users\Sarah\M\Downloads\Great Horned Owl Info...rcwildlife.org	https://rcwildlife.org/Portals/0/Anim...	https://rcwildlife.org/Portals/0/Anim...
History	1			C:\Users\Sarah\M\Downloads\Great Horned Owl...google.com	https://mail.google.com/mail/?#=/m/...	https://mail.google.com/mail/?#=/m/...
History	1			C:\Users\Sarah\M\Downloads\Great Horned Owl...microsoftmedia.org	https://mail.attachment.googleapis.c...	https://mail.attachment.googleapis.c...
History	0			C:\Users\Sarah\M\Downloads\Luna Owl.jpg	wikimedia.org	https://upload.wikimedia.org/wikipedia...
History	1			C:\Users\Sarah\M\Downloads\Owl_Emergency.pdf	owlpages.com	http://www.owlpages.com/download/Owl...
History	1			C:\Users\Sarah\M\Downloads\Owl_Keeping.pdf	owlpages.com	http://www.owlpages.com/download/Owl...

*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.

The screenshot displays the 'Web Form Autofill' analysis results from a digital forensic tool. At the top, there are tabs for 'Listing', 'Keyword search 1 - "McAvoyS87@gma...', 'Keyword search 3 - "pidgin"', and 'Save Table as CSV'. Below the tabs is a table with columns: Source Name, S, C, O, Name, Value, Count, Date Created, Date Accessed, Username, and Program Name. The table contains numerous entries, many of which are highlighted in blue. A 'Save Table as CSV' button is located at the top right of the table area. Below the table is a search bar with fields for 'Hex', 'Text', 'Application', 'Source File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'Text' tab is selected. Underneath the search bar is a command-line interface showing the word 'autofill'. At the bottom of the interface is a toolbar with various icons and system status indicators like temperature (22°C), battery level (650 PM 4/30/2025), and signal strength.

Source Name	S	C	O	Name	Value	Count	Date Created	Date Accessed	Username	Program Name
Web Data				name	Sarah McAvoy	1	2017-01-27 01:04:17 GMT	2017-01-27 01:04:17 GMT	Default	Google Chrome
Web Data				email	McAvoyS87@gmail.com	2	2017-01-27 01:04:17 GMT	2017-01-28 22:21:05 GMT	Default	Google Chrome
Web Data				session[username_or_email]	McAvoyS87@gmail.com	1	2017-01-27 01:10:44 GMT	2017-01-27 01:10:44 GMT	Default	Google Chrome
Web Data				query	owls	1	2017-01-27 01:42:36 GMT	2017-01-27 01:42:36 GMT	Default	Google Chrome
Web Data				Email	mcavoy87	1	2017-01-27 17:07:04 GMT	2017-01-27 17:07:04 GMT	Default	Google Chrome
Web Data				email	13046388446	2	2017-01-27 17:14:05 GMT	2017-01-28 21:48:30 GMT	Default	Google Chrome
Web Data				freeformGender	Female	1	2017-01-28 22:21:45 GMT	2017-01-28 22:21:45 GMT	Default	Google Chrome
Web Data				tumblelog[name]	Sarah McAvoy	1	2017-01-28 22:22:28 GMT	2017-01-28 22:22:28 GMT	Default	Google Chrome
Web Data				Email	mcavoy87@gmail.com	3	2017-01-28 22:26:31 GMT	2017-01-28 22:28:06 GMT	Default	Google Chrome
Web Data				determine_email	Mcavoy87@gmail.com	1	2017-02-02 22:49:38 GMT	2017-02-02 22:49:38 GMT	Default	Google Chrome

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

Page: 1 of 1 Page    Matches on page: - of - Match    100%    Reset    Text Source: File Text

autofill

```
name value value._lower_date_created_date._last_used_count
name Sarah McAvoy sarah mcavoy 1485479057 1485479057
email McAvoyS87@gmail.com mcavoy87@gmail.com 1485479057 1485642065 2
session[username_or_email] McAvoyS87@gmail.com mcavoy87@gmail.com 1485479444 1485479444 1
query owls owls 1485481356 1485481356 1
Email mcavoy87 mcavoy87 1485536824 1485536824
email 13046388446 13046388446 1485537245 1485640110 2
freeformGender Female female 1485642105 1485642105 1
tumblelog[name] Sarah McAvoy sarah mcavoy 1485642148 1485642148 1
Email mcavoy87@gmail.com mcavoy87@gmail.com 1485642391 1485642486 3
determine_email Mcavoy87@gmail.com mcavoy87@gmail.com 1486075778 1486075778 1
```

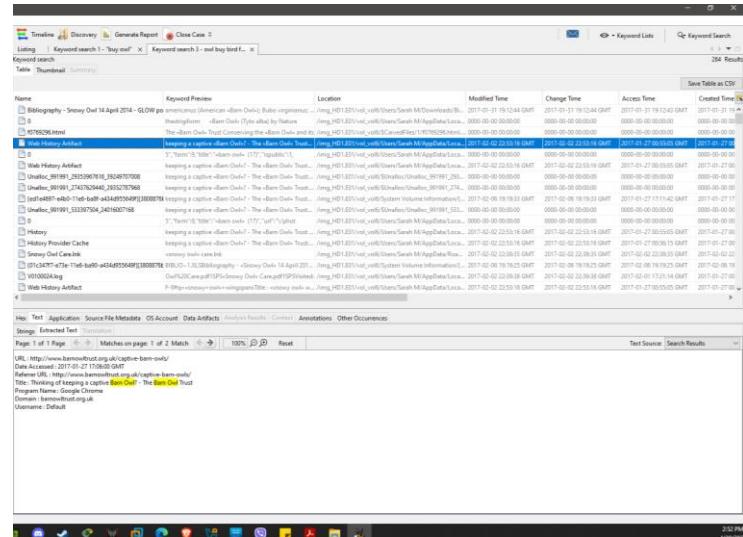
credit\_cards

Figure 14 Web Form Autofill

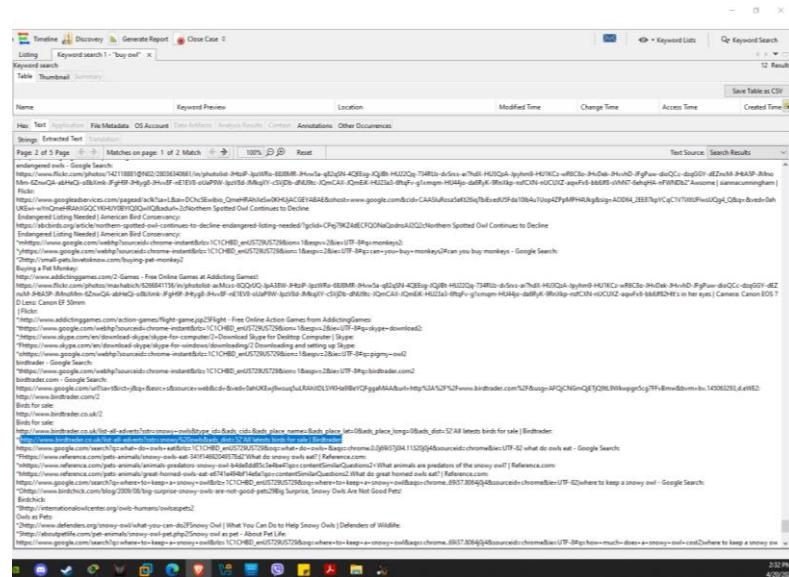
## 13. Web History

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*

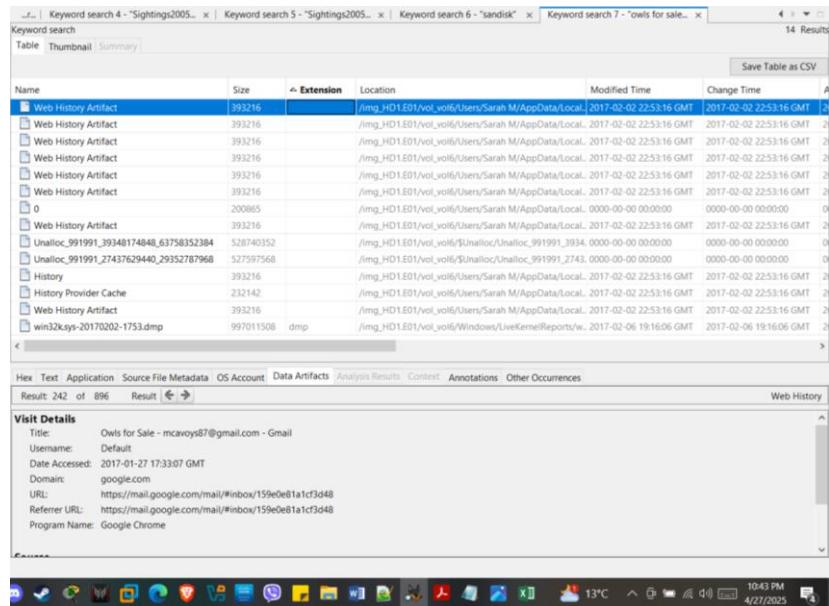


Figure 18 Email with title owl for sale

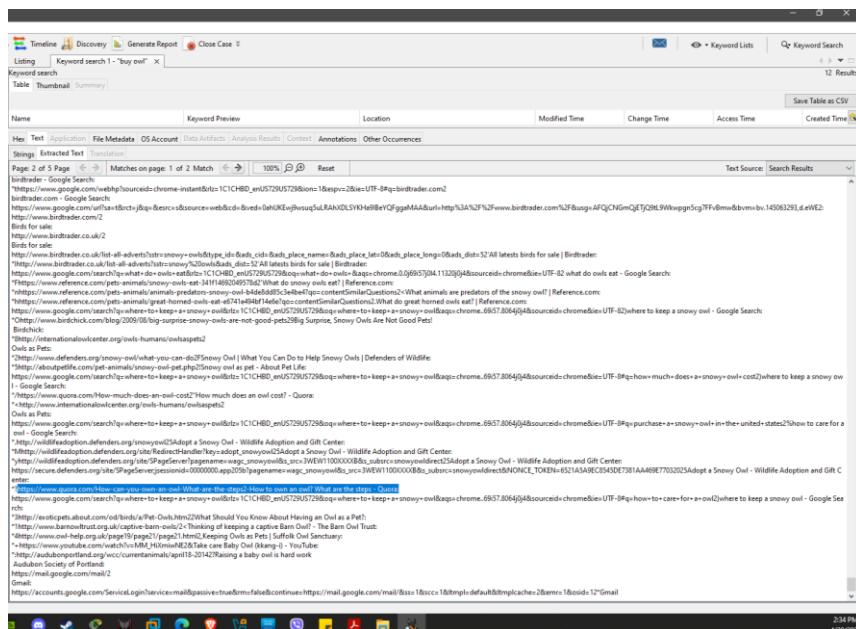
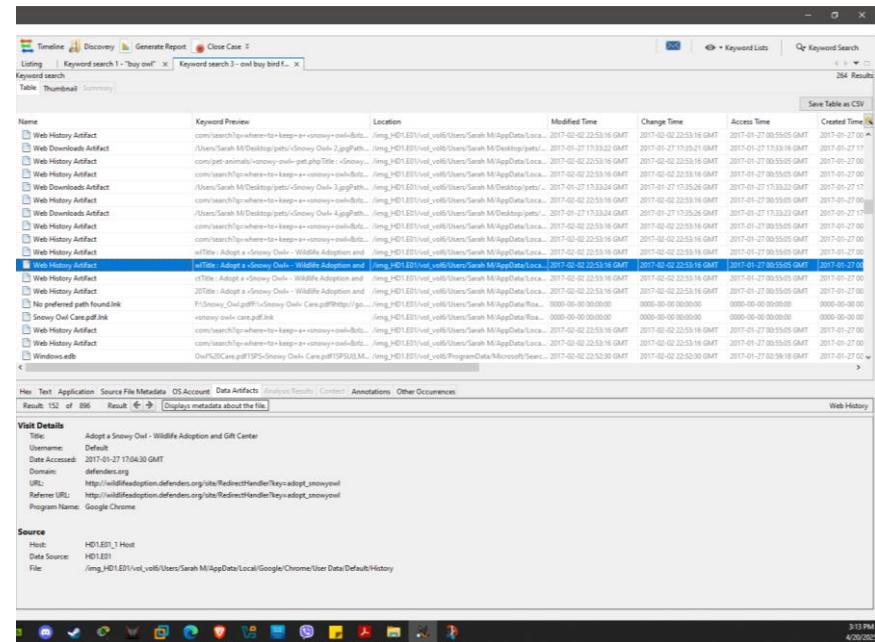
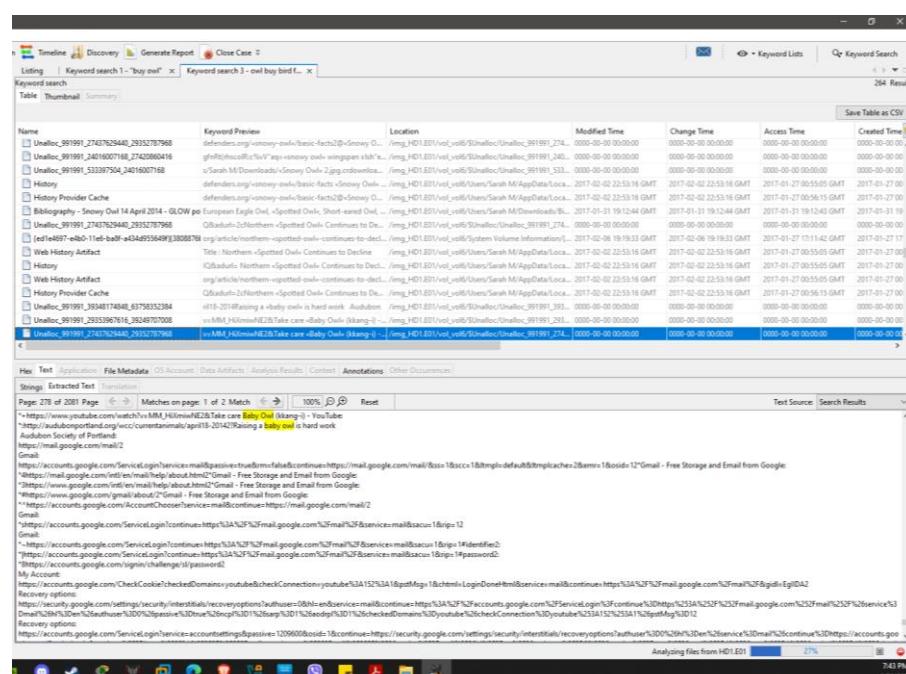


Figure 19 Web History-How to own an owl



*Figure 20 Web History Adopt a Snowy Owl*



*Figure 21 Web History-Baby Owl*

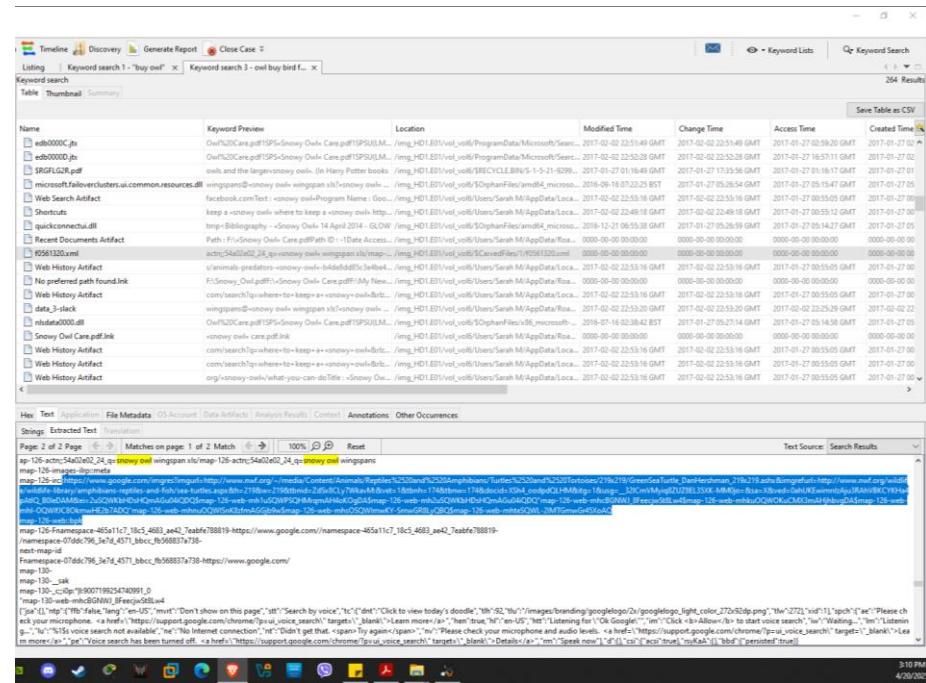


Figure 22 Web History Sea-Turtle

## 14. Web Search

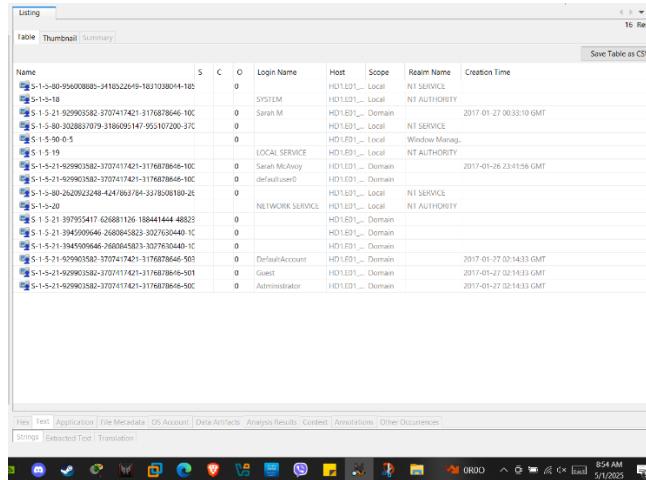
- Some of the web searches are:
- Where to keep a snowy owl
  - harry potter owl
  - how to care owls
  - Athena with an owl artistic
  - trippy owl pictures

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	game theory	Google Chrome	2017-01-28 22:07:45 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?i=9Cme...	Google Chrome	2017-01-28 22:26:36 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				youtube.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

Figure 23 Web Searches

## 15. OS Account

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



The screenshot shows a Windows operating system interface with a table titled "User Accounts" listing 16 user accounts. The columns include Name, S, C, O, Login Name, Host, Scope, Realm Name, and Creation Time. The accounts listed are:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-95600880-341022649-1031038049-1482	0	0	0		HOST1	Local	NT SERVICE	
S-1-5-18	0	0	0	SYSTEM	HOST1	Local	NT AUTHORITY	
S-1-5-21-329903582-3707417421-317687846-10C	0	0	0	Sarah M	HOST1	Domain	NT SERVICE	2017-01-27 00:33:09 GMT
S-1-5-80-302883709-3186095147-955107200-37C	0	0	0		HOST1	Domain	NT SERVICE	
S-1-5-90-0-5	0	0	0		HOST1	Local	Windows Manag.	
S-1-5-19	0	0	0	LOCAL SERVICE	HOST1	Local	NT AUTHORITY	
S-1-5-21-329903582-3707417421-317687846-10C	0	0	0	Sarah McAvoy	HOST1	Domain	NT SERVICE	2017-01-26 23:41:56 GMT
S-1-5-21-329903582-3707417421-317687846-10C	0	0	0	defaultUser0	HOST1	Domain	NT AUTHORITY	
S-1-5-20	0	0	0		HOST1	Local	NT SERVICE	
S-1-5-21-37975417-62688126-188441444-4882	0	0	0	NETWORK SERVICE	HOST1	Local	NT AUTHORITY	
S-1-5-21-3945099446-2680845823-392763040-1C	0	0	0		HOST1	Domain	NT AUTHORITY	
S-1-5-21-3945099446-2680845823-397763040-1C	0	0	0		HOST1	Domain	NT AUTHORITY	
S-1-5-21-329903582-3707417421-317687846-503	0	0	0	DefaultAccount	HOST1	Domain	NT AUTHORITY	2017-01-27 07:14:53 GMT
S-1-5-21-329903582-3707417421-317687846-503	0	0	0	Guest	HOST1	Domain	NT AUTHORITY	2017-01-27 02:14:53 GMT
S-1-5-21-329903582-3707417421-317687846-50C	0	0	0	Administrator	HOST1	Domain	NT AUTHORITY	2017-01-27 02:14:53 GMT

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.

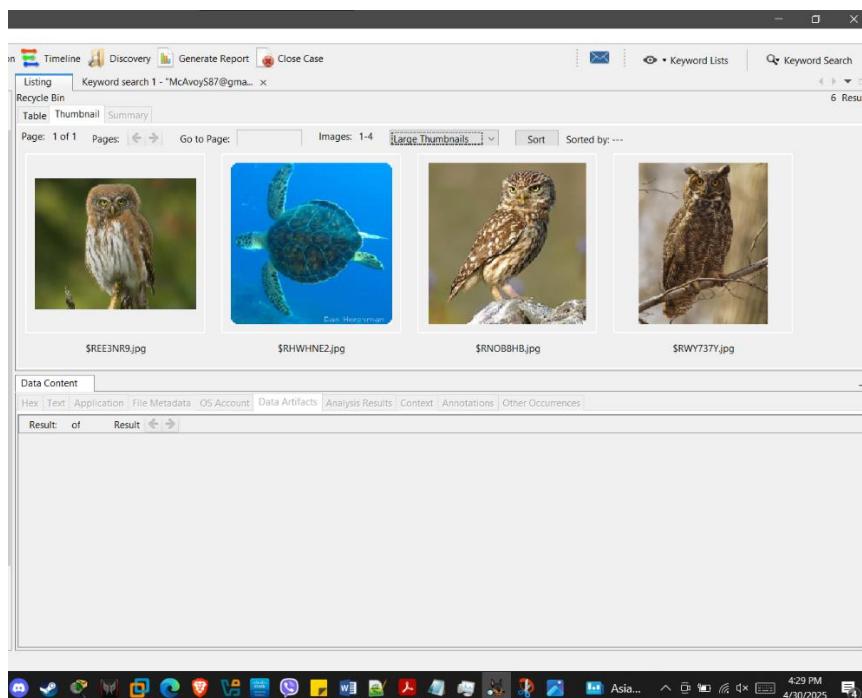


Figure 25 Recycle Bin Pictures

- **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.

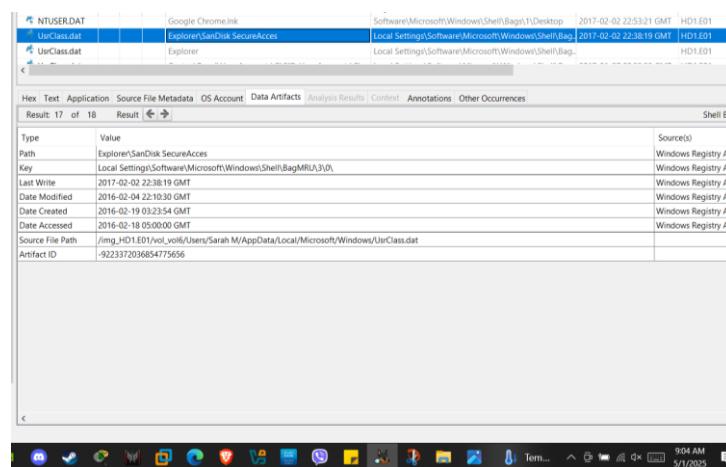


Figure 26 Shell Bag-SecureAccess

- **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](mailto: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.

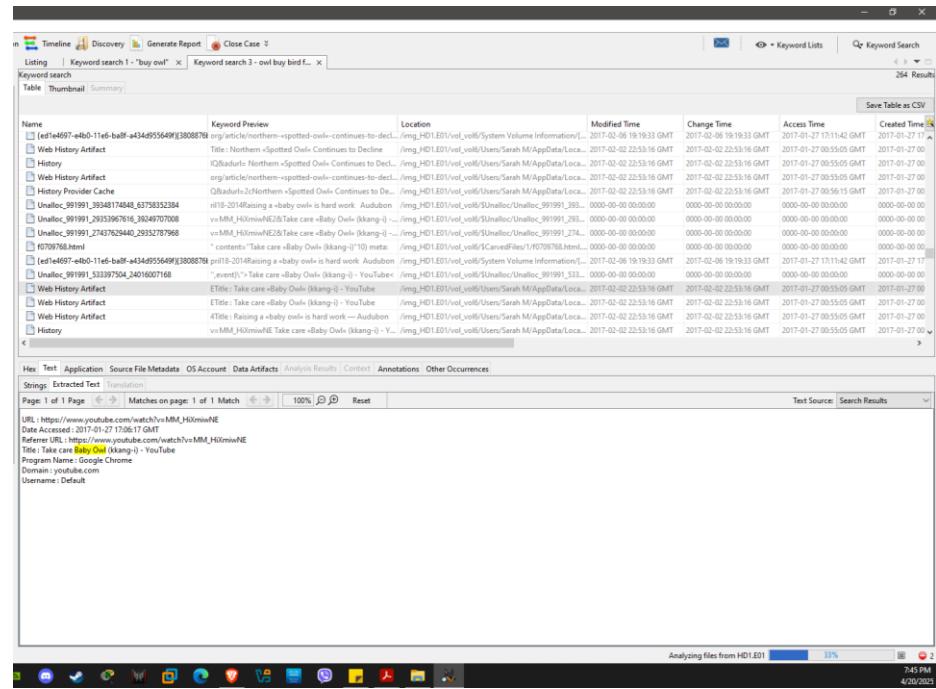


Figure 27 Web History-YouTube take care baby owl

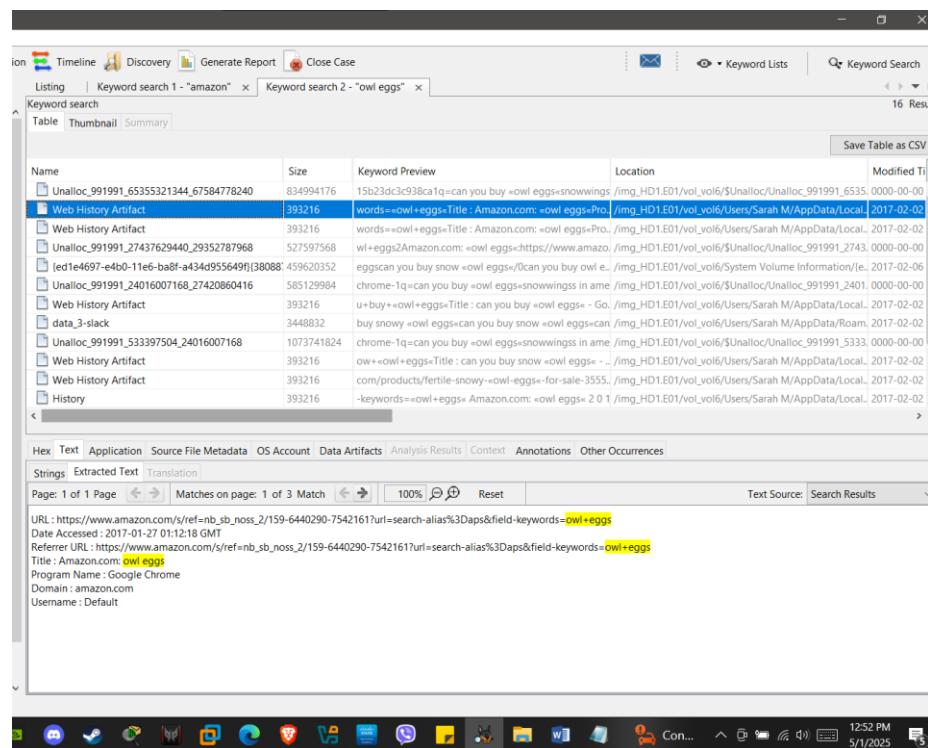


Figure 28 Amazon-owl-eggs

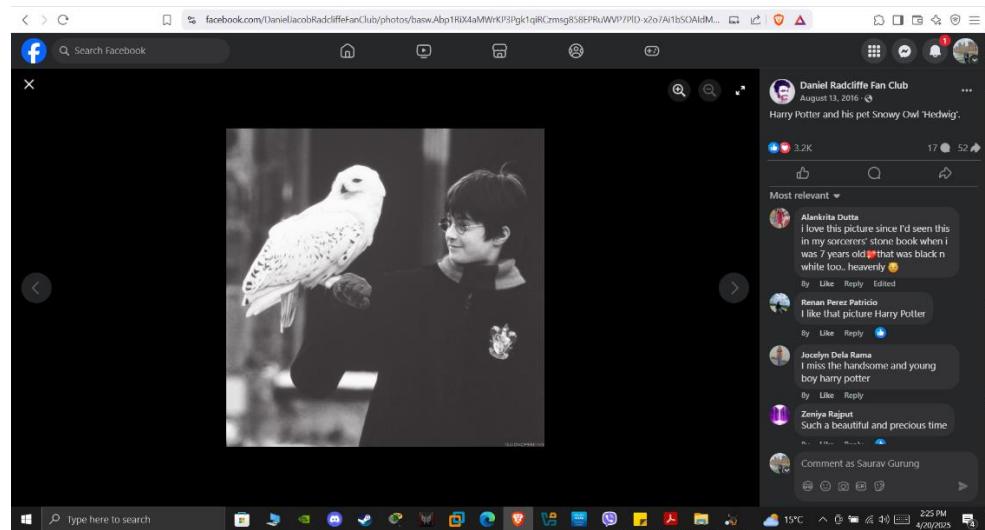


Figure 29 Web History-harry potter with owl

- **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.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	sirius the dog	Google Chrome	2017-01-27 01:08:48 GMT	HD1.E01
History				google.com	sirius the dog	Google Chrome	2017-01-27 01:08:50 GMT	HD1.E01
History				google.com	what do owls eat	Google Chrome	2017-01-27 17:00:54 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:03:50 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:04:12 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:04:12 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:05:58 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:05:58 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:06:32 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:06:32 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:06:32 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:06:32 GMT	HD1.E01
History				google.com	where to keep a snowy owl	Google Chrome	2017-01-27 17:06:32 GMT	HD1.E01
History				facebook.com	https://twitter.com/i/redirect?url=https%3A%2F%2Ftw...	Google Chrome	2017-01-27 17:07:52 GMT	HD1.E01
History				facebook.com	terry bunch	Google Chrome	2017-01-27 17:15:24 GMT	HD1.E01

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](mailto:McavoyS87@gmail.com) was discovered from “f0010712.xml”.

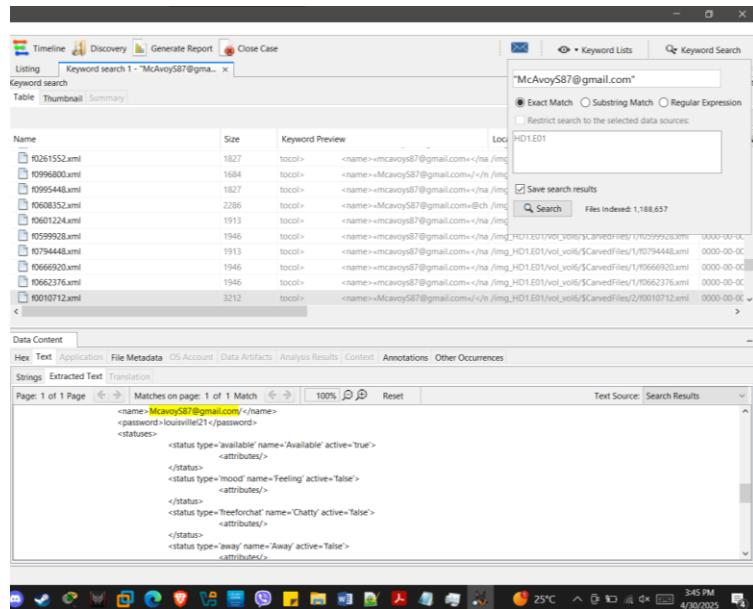


Figure 31 Gmail credentials

#### 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.

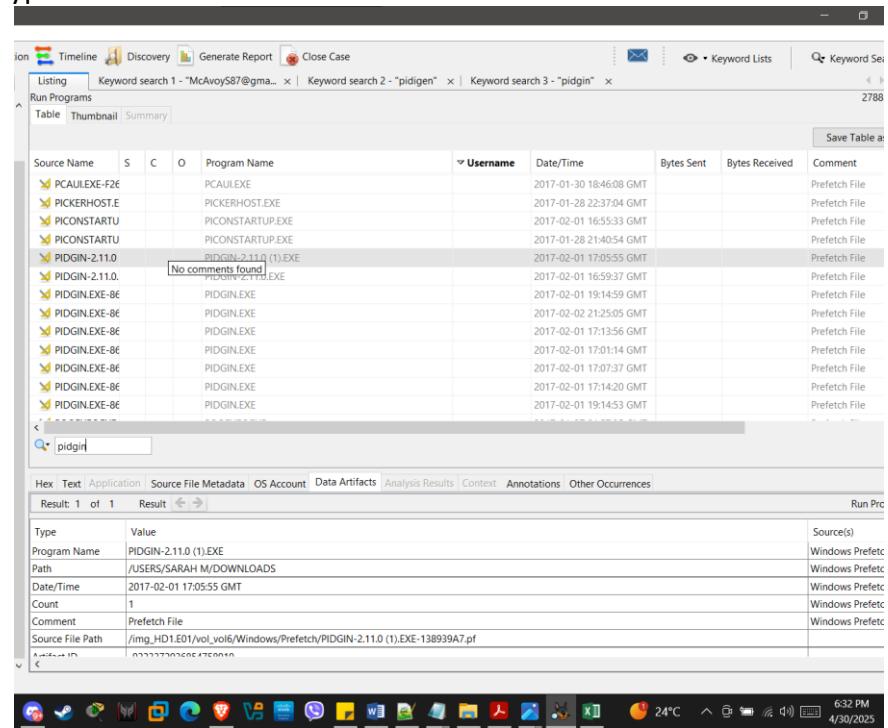


Figure 32 Pidgin installed

## 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](mailto: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](mailto: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.