ITMS 538 Final Analysis

Alan Palayil
Due Date: 12/11/2022

Introduction

During this Final Analysis Lab, we are assigned a high-profile case which involves an owl trafficking ring. The investigation team has provided us a full computer's hard drive (60+ GB) and smartphone (40+ GB). I am given the logical acquisition of our prime suspect, Sarah McAvoy, smartphone LG Nexus 5.

Our goal is to look over the evidence to find various which can be used for the trial that is scheduled for next week. We go over the logical files to look over three specific evidence categories: interest, motivation, and delivery.

For the investigation we are using Autopsy as our primary forensics tool as it has ingested modules to view smartphone files and data stored in DB.

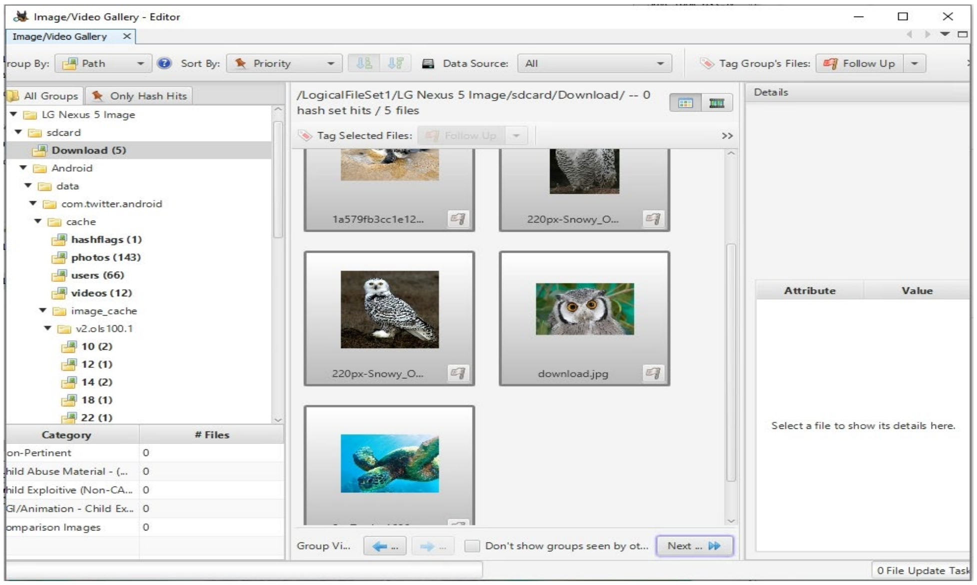
After creating our case in Autopsy and setting up our data source as Logical Files, we then look over to ingest the modules we might be using. I used the following modules to go over the case:

- Android Analyzer Module
- Central Repository Module
- Data Source Integrity Module
- Encryption Detection Module
- File Type Identification Module
- Interesting Files Identifier Module
- Picture Analyzer Module
- Android Analyzer (aLEAPP) Module
- Email Parser Module
- Embedded File Extractor Module
- Extension Mismatch Detector Module
- Hash Lookup Module
- Keyword Search Module
- Recent Activity Module

Once the set up was completed, I then headed to look over for the evidence and along the way add notable tags to the evidence gathered.

Interest Evidence

To prove that user was interested in owls, I first glanced over the images that were present in the files using the Images/Videos scanner. A total of nine jpg images were found including duplicates which were tagged under interest.



roup By: Path

Sort By: Priority

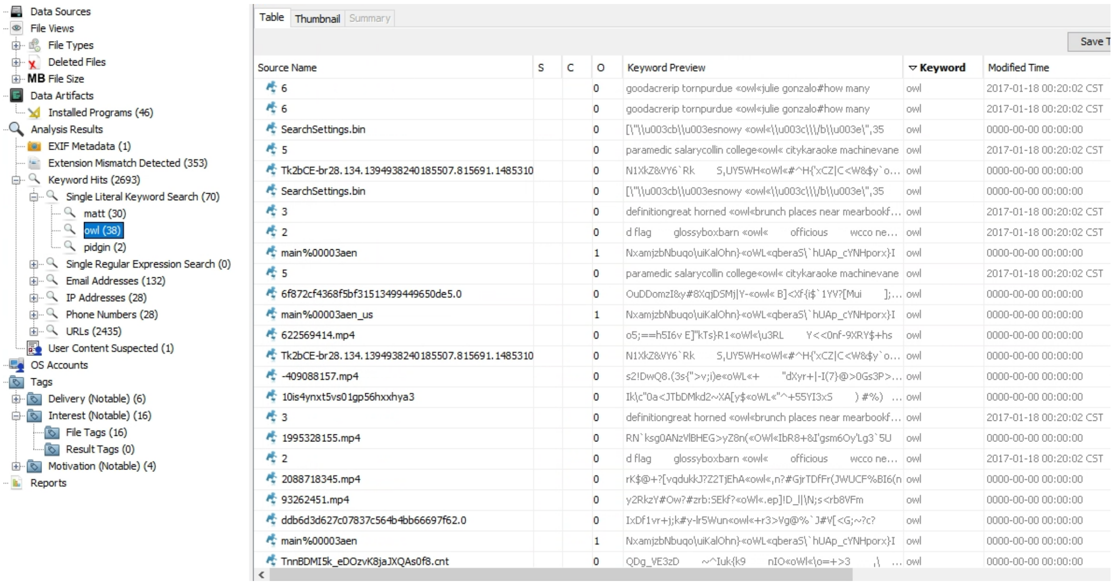
Data Source: All

Tag Group's Files: Follow Up

/LogicalFileSet1/LG Nexus 5 Image/sdcard/Download/ -- 0 hash set hits / 5 files

Category	# Files
on-Pertinent	0
hild Abuse Material - (...	0
hild Exploitive (Non-CA...	0
GI/Animation - Child Ex...	0
omparison Images	0

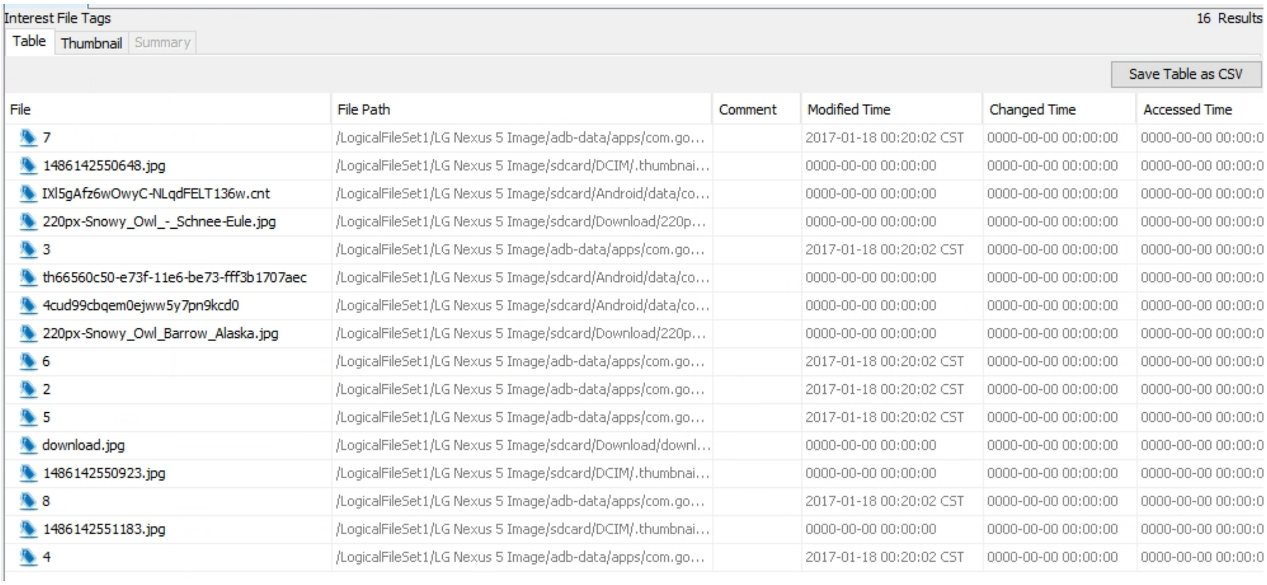
I then did a keyword search on all the files that contained ‘owl’ within them and went over each document to by looking at the text and Analysis Results do determine whether the file belonged to a web-search, document, image, or chat message.



- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Installed Programs (46)
- Analysis Results
  - EXIF Metadata (1)
  - Extension Mismatch Detected (353)
  - Keyword Hits (2693)
    - Single Literal Keyword Search (70)
      - matt (30)
      - owl (38)
      - pidgin (2)
    - Single Regular Expression Search (0)
    - Email Addresses (132)
    - IP Addresses (28)
    - Phone Numbers (28)
    - URLs (2435)
  - User Content Suspected (1)
- OS Accounts
- Tags
  - Delivery (Notable) (6)
  - Interest (Notable) (16)
    - File Tags (16)
    - Result Tags (0)
  - Motivation (Notable) (4)
- Reports

Source Name	S	C	O	Keyword Preview	▽ Keyword	Modified Time
6			0	goodacrerip tornpurdue «owl«julie gonzalo#how many	owl	2017-01-18 00:20:02 CST
6			0	goodacrerip tornpurdue «owl«julie gonzalo#how many	owl	2017-01-18 00:20:02 CST
SearchSettings.bin			0	[\"\\u003cb\\u003esnowy «owl«\\u003c\\\/b\\u003e\",35	owl	0000-00-00 00:00:00
5			0	paramedic salarycollin college«owl« citykaraoke machinevane	owl	2017-01-18 00:20:02 CST
Tk2bCE-br28.134.1394938240185507.815691.1485310			0	N1XkZ&VY6`Rk S,UY5WH«oWl«#^H{'xCZ|C<W&$y`o…	owl	0000-00-00 00:00:00
SearchSettings.bin			0	[\"\\u003cb\\u003esnowy «owl«\\u003c\\\/b\\u003e\",35	owl	0000-00-00 00:00:00
3			0	definitiongreat horned «owl«brunch places near mearbookf…	owl	2017-01-18 00:20:02 CST
2			0	d flag glossyboxbarn «owl« officious wcco ne…	owl	2017-01-18 00:20:02 CST
main%00003aen			1	NxamjzbNbuqo\uiKalOhn}«oWL«qberaS\`hUAp_cYNHporx}I	owl	0000-00-00 00:00:00
5			0	paramedic salarycollin college«owl« citykaraoke machinevane	owl	2017-01-18 00:20:02 CST
6f872cf4368f5bf31513499449650de5.0			0	OuDDomzI&y#8XqjDSMj|Y-«owl« B]<Xf{i$`1YV?[Mui];…	owl	0000-00-00 00:00:00
main%00003aen_us			1	NxamjzbNbuqo\uiKalOhn}«oWL«qberaS\`hUAp_cYNHporx}I	owl	0000-00-00 00:00:00
622569414.mp4			0	o5;==h5I6v E]"kTs}R1«oWl«\u3RL Y<<0nf-9XRY$+hs	owl	0000-00-00 00:00:00
Tk2bCE-br28.134.1394938240185507.815691.1485310			0	N1XkZ&VY6`Rk S,UY5WH«oWl«#^H{'xCZ|C<W&$y`o…	owl	0000-00-00 00:00:00
-409088157.mp4			0	s2!DwQ8.(3s{">v;i)e«oWL«+ "dXyr+|-I(7}@>0Gs3P>…	owl	0000-00-00 00:00:00
10is4ynxt5vs01gp56hxxhya3			0	Ik\c"0a<JTbDMkd2~XA[y$«oWL«"^+55YI3xS) #%) …	owl	0000-00-00 00:00:00
3			0	definitiongreat horned «owl«brunch places near mearbookf…	owl	2017-01-18 00:20:02 CST
1995328155.mp4			0	RN`ksg0ANzVlBHEG>yZ8n(«OWl«IbR8+&I'gsm6Oy'Lg3`5U	owl	0000-00-00 00:00:00
2			0	d flag glossyboxbarn «owl« officious wcco ne…	owl	2017-01-18 00:20:02 CST
2088718345.mp4			0	rK$@+?[vqdukkJ?Z2TjEhA«owl«,n?#GjrTDfFr(JWUCF%BI6(n	owl	0000-00-00 00:00:00
93262451.mp4			0	y2RkzY#Ow?#zrb:SEkf?«oWl«.ep]!D_l|\N;s<rb8VFm	owl	0000-00-00 00:00:00
ddb6d3d627c07837c564b4bb66697f62.0			0	IxDf1vr+j;k#y-lr5Wun«owl«+r3>Vg@%`J#V[<G;~?c?	owl	0000-00-00 00:00:00
main%00003aen			1	NxamjzbNbuqo\uiKalOhn}«oWL«qberaS\`hUAp_cYNHporx}I	owl	0000-00-00 00:00:00
TnnBDMI5k_eDOzvK8jaJXQAs0f8.cnt			0	QDg_VE3zD ~^Iuk{k9 nIO«oWl«\o=+>3 ,\ …	owl	0000-00-00 00:00:00

The files that seemed relevant were tagged to the ‘Interest Tag’ and a total of 16 files were tagged.



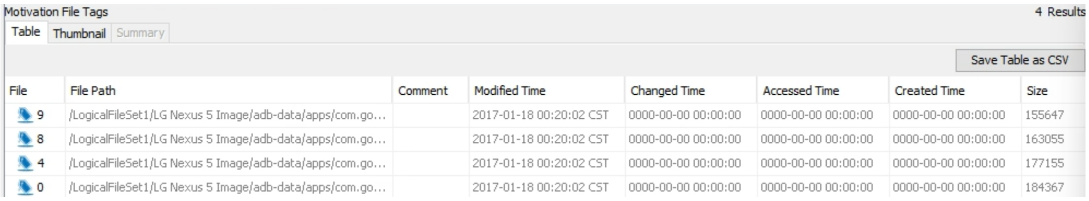
Interest File Tags

16 Results

File	File Path	Comment	Modified Time	Changed Time	Accessed Time
7	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0
1486142550648.jpg	/LogicalFileSet1/LG Nexus 5 Image/sdcard/DCIM/.thumbnai…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
IXl5gAfz6wOwyC-NLqdFELT136w.cnt	/LogicalFileSet1/LG Nexus 5 Image/sdcard/Android/data/co…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
220px-Snowy_Owl_-_Schnee-Eule.jpg	/LogicalFileSet1/LG Nexus 5 Image/sdcard/Download/220p…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
3	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0
th66560c50-e73f-11e6-be73-fff3b1707aec	/LogicalFileSet1/LG Nexus 5 Image/sdcard/Android/data/co…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
4cud99cbqem0ejww5y7pn9kcd0	/LogicalFileSet1/LG Nexus 5 Image/sdcard/Android/data/co…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
220px-Snowy_Owl_Barrow_Alaska.jpg	/LogicalFileSet1/LG Nexus 5 Image/sdcard/Download/220p…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
6	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0
2	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0
5	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0
download.jpg	/LogicalFileSet1/LG Nexus 5 Image/sdcard/Download/downl…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
1486142550923.jpg	/LogicalFileSet1/LG Nexus 5 Image/sdcard/DCIM/.thumbnai…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
8	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0
1486142551183.jpg	/LogicalFileSet1/LG Nexus 5 Image/sdcard/DCIM/.thumbnai…		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
4	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:0

Motivation Evidence

Now the next stage of our investigation is to look for the motivation that our suspect, Sarah, was interested in buying/selling owls. We further investigate the files with the keyword ‘owl’ and look at the web-searches in particular to see what might have influenced the suspect to purchase the owl. The files tagged with motivation included searches that were on an owl game, their living habitat, and which owl would be better.



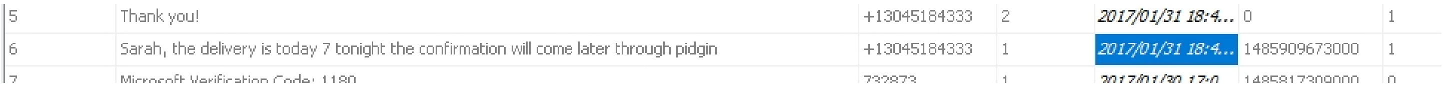
Motivation File Tags

4 Results

File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size
9	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	155647
8	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	163055
4	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	177155
0	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.go…		2017-01-18 00:20:02 CST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	184367

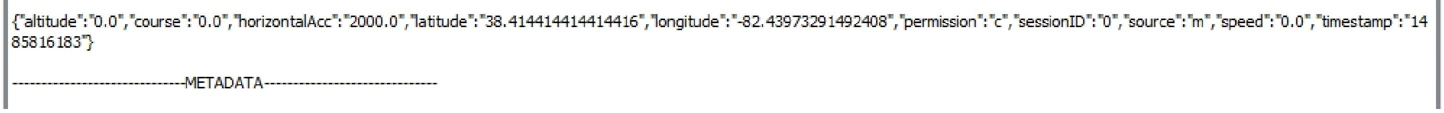
Delivery Evidence

The investigation team also claimed that our suspect had another person-of-interest who received a trafficked owl and was communicating via text to schedule the delivery. We start looking over the databases using the hint given by the investigation team. We start by looking over the text messages and find a message which gives a time of ‘7pm’ for a delivery and the date of the message is ‘01/31/2017’ as displayed below:



5	Thank you!	+13045184333	2	2017/01/31 18:4...	0	1
6	Sarah, the delivery is today 7 tonight the confirmation will come later through pidgin	+13045184333	1	2017/01/31 18:4...	1485909673000	1
7	Microsoft Verification Code: 1180	732873	1	2017/01/30 17:0	1485817309000	0

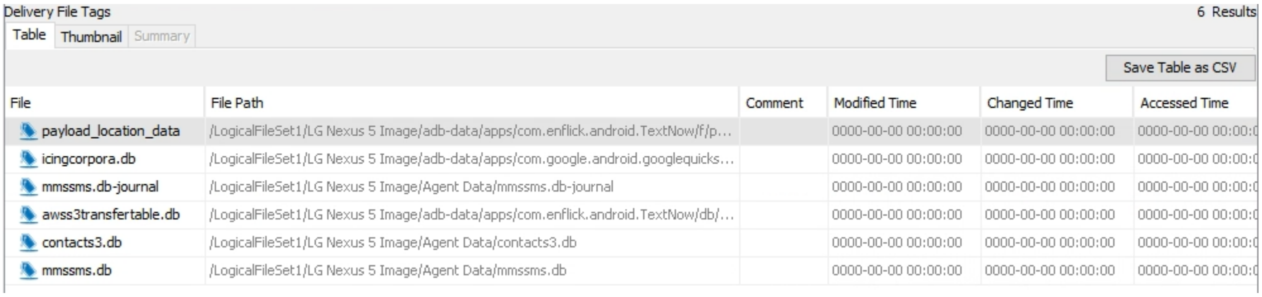
This made me look over other database files which can help us look over the other possible evidence to help us track the evidence. We go over the contacts3.db and come across a contact, ‘Matt Haze’ who seems to be added via Skype. The other detail from text was the ‘pidgin’ which after research is a texting application. So, the next aim for our investigation is to try and find the location of the drop-off. While going over other databases, there is a transfer of contacts done to an application ‘TextNow’. Looking over the files related to TextNow, we find a payload location with the coordinates: (38.414414414414416, -82.43973291492408) which is in Huntington, West Virginia.



{"altitude":"0.0","course":"0.0","horizontalAcc":"2000.0","latitude":"38.414414414414416","longitude":"-82.43973291492408","permission":"c","sessionID":"0","source":"m","speed":"0.0","timestamp":"14
85816183"}

------------------------------METADATA------------------------------

All the files that were found in reference to the evidence related to Delivery were tagged to Delivery.



Delivery File Tags

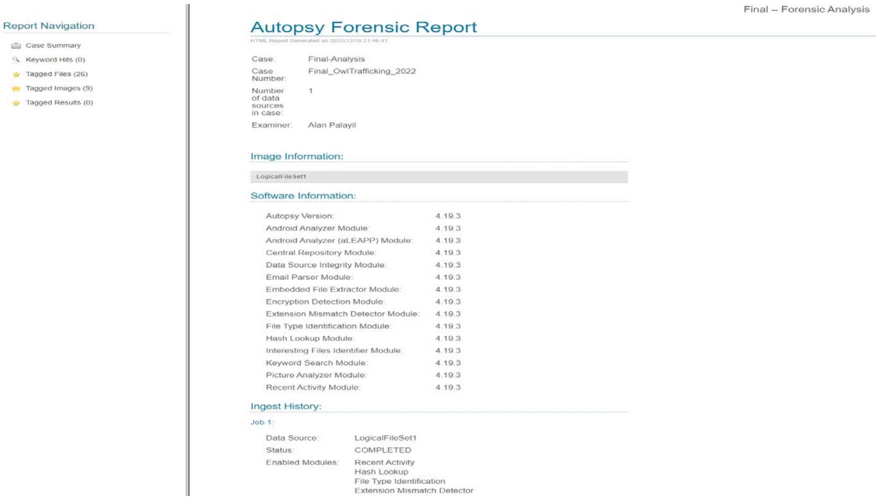
File	File Path	Comment	Modified Time	Changed Time	Accessed Time
payload_location_data	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.enflick.android.TextNow/f/p...		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
icingcorpora.db	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.google.android.googlequicks...		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
mmssms.db-journal	/LogicalFileSet1/LG Nexus 5 Image/Agent Data/mmssms.db-journal		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
awss3transfertable.db	/LogicalFileSet1/LG Nexus 5 Image/adb-data/apps/com.enflick.android.TextNow/db/...		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
contacts3.db	/LogicalFileSet1/LG Nexus 5 Image/Agent Data/contacts3.db		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0
mmssms.db	/LogicalFileSet1/LG Nexus 5 Image/Agent Data/mmssms.db		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0

Conclusion

Thus, we have found the location and schedule of the owl delivery and the possible partner in crime. After gathering all our evidence, we sort the evidence into dedicated directories. Then using Autopsy, we extract the files into our directory which we created.

The next step is to generate the report using Autopsy. We click on the Generate report tab and create a HTML Report as instructed. The html file is saved within the Report directory and when opened, we can look over the report’s homepage and all the tags that have been made.

I don’t know how the html file is viewable through the pdf and thus have just the address location of the file.



Report Navigation

- Case Summary
- Keyword Hits (0)
- Tagged Files (26)
- Tagged Images (9)
- Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2022/12/10 21:46:41

Case:	Final-Analysis
Case Number:	Final_OwlTrafficking_2022
Number of data sources in case:	1
Examiner:	Alan Palayil

Image Information:

LogicalFileSet1

Software Information:

Autopsy Version:	4.19.3
Android Analyzer Module:	4.19.3
Android Analyzer (aLEAPP) Module:	4.19.3
Central Repository Module:	4.19.3
Data Source Integrity Module:	4.19.3
Email Parser Module:	4.19.3
Embedded File Extractor Module:	4.19.3
Encryption Detection Module:	4.19.3
Extension Mismatch Detector Module:	4.19.3
File Type Identification Module:	4.19.3
Hash Lookup Module:	4.19.3
Interesting Files Identifier Module:	4.19.3
Keyword Search Module:	4.19.3
Picture Analyzer Module:	4.19.3
Recent Activity Module:	4.19.3

Ingest History:

Job 1:

Data Source:	LogicalFileSet1
Status:	COMPLETED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification Extension Mismatch Detector

This case files are all archived into a zip file for the submission.

The URL of the HTML Autopsy report is within the file directory:

file:///../Reports/Final-Analysis%20HTML%20Report%2012-10-2022-21-46-41/report.html