Digital Investigations Coursework 2

Maks Miketa 2020 (N0945100)

Case 2
Aim 2
Ethical Considerations 2
Analysis 2
Analysis 4
20/01/1970 4
31/10/2010 to 25/10/2021 6
09/03/2022 8
08/09/2023 8
13/09/2023 10
14/09/2023 13
15/09/2023 17
16/09/2023 21
18/09/2023 23
22/09/2023 24
26/09/2023 25
27/10/2023 32
Conclusion 34
Software Documentation 35
References 36

Case

A mobile phone identified as Samsung GSM SM-A320FL Galaxy A3 (2017) was seized from an individual called Tom Biddle and the seizure took place on Canal Street in Manchester's "gay village".

Aim

The aim is to identify any laws that have been or may have been broken on the seized device.

Ethical Considerations

Before proceeding with the investigation, consent to investigate the device was given from the individual that the device was obtained from, and the individual was fully aware of the data extracted and the impact on their privacy. Only data relevant to the case was extracted and if there were to be any identified child pornography then the case would be paused, and the case investigator would have been contacted immediately. The data investigated within the investigation and report was kept confidential and not shared to any individuals that were not involved with the case.

Analysis

Cellebrite Physical Analyzer 7.63.0.126 was used to analyse for evidence on the seized phone: Samsung GSM SM-A320FL Galaxy A3 (2017). Cellebrite is a mobile phone analyser tool used to extract and investigate data from the device. The devices physical image was

investigated which contained all the information from that was within the logical image. The physical image was extracted on 27/10/2023 and selected:

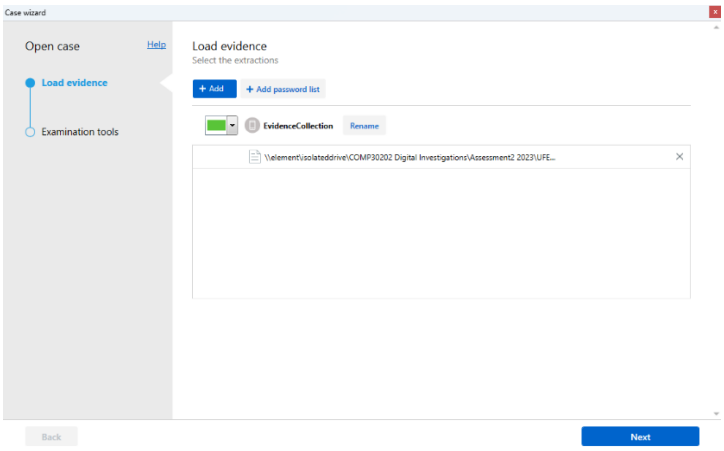
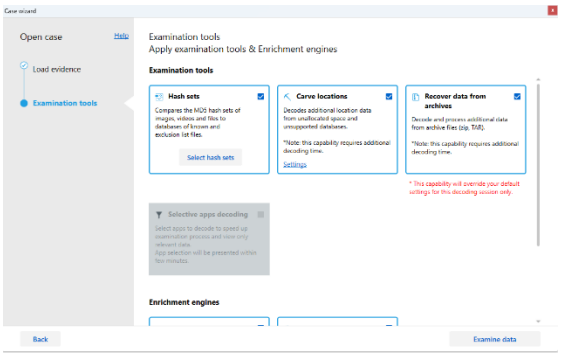


Figure 1 Loading case on Cellebrite.

Next, all available examination tools were selected for extraction. Hash sets compare files MD5 hash sets for known files within the Cellebrite database saving time searching for MD5 files on the internet. Carve locations can provide additional evidence for location data. Recover data from archives decodes archived data that can potentially reveal evidence and save time. Media classification aids in searching for specific files and cryptocurrency identifies any crypto wallets used on the device.



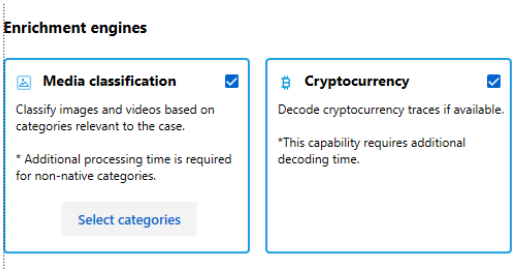


Figure 2 Selecting examination tools.

Figure 3 Selecting enrichment engines.

After the Cellebrite analysis completed, the first step taken was checking the timeline history of the device to see all the data from the start to the end. The devices evidence was

obtained on UTC +0 time zone. The device analysing the evidence was within the same time zone, so it did not require time zone alteration.

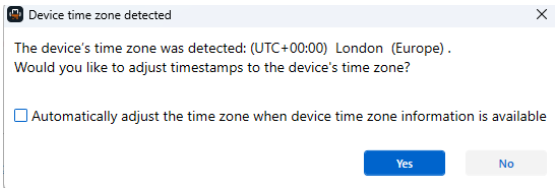


Figure 4 Time zone alteration.

Analysis

In this section, only data relevant to the case is shown as well as any steps and processes that were taken to identify for evidence. The timeline used was UTC + 0.

20/01/1970

23 items were identified from the social media platform Facebook.

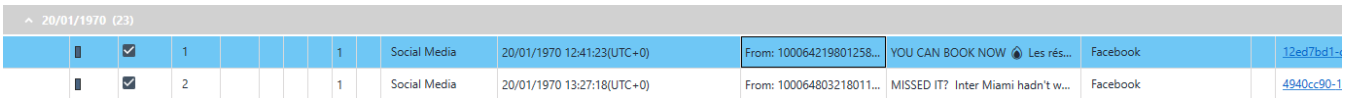


Figure 5 Facebook data.

All items appear to be posts from the news feed. The reason of this timestamp can be due to Facebook using the Unix epoch date therefore, the time stamp is not accurate. However, from this information, a Facebook account is used on the device (dotnet-bot, n.d.).

One of the files hex data was saved and opened using HxD Editor. The search tool was used to type in key words to identify the account holder which was “Tom Biddle” from looking up the users ID.

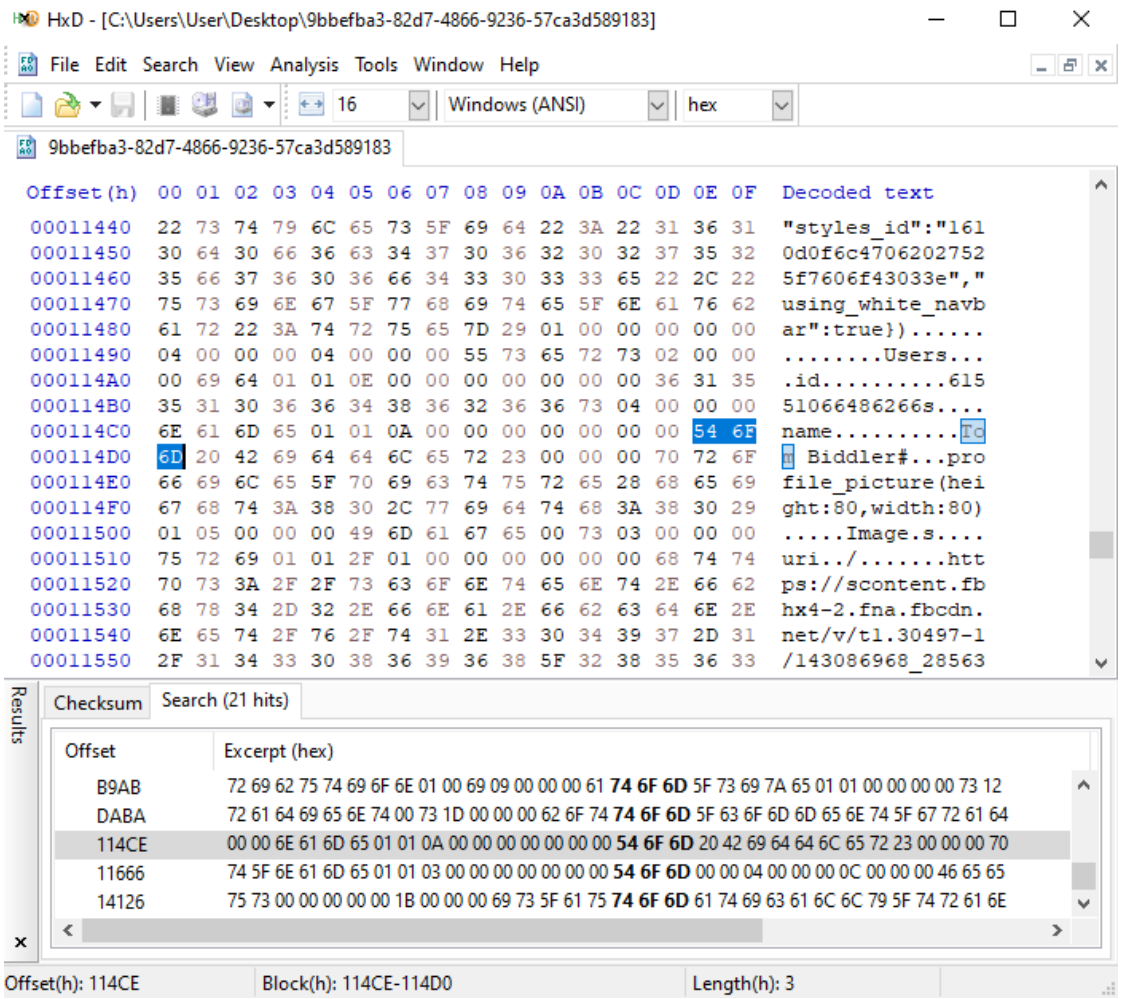


Figure 6 HxD Identifying ID.

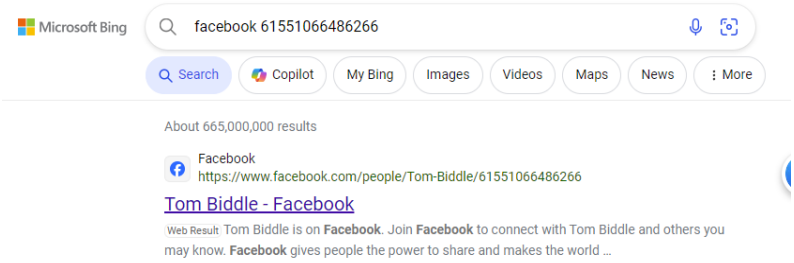


Figure 7 Searching Facebook ID

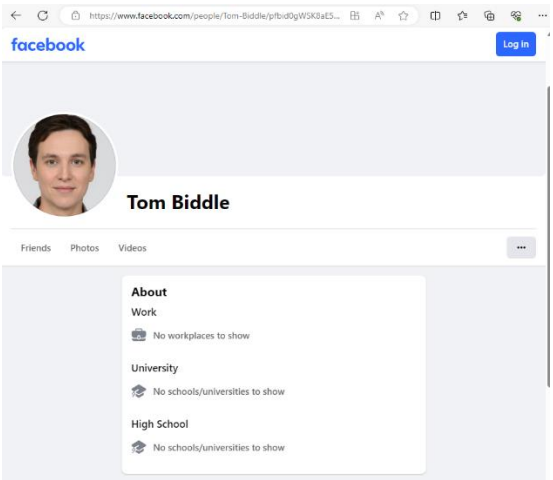


Figure 8 Tom Biddle Facebook ID

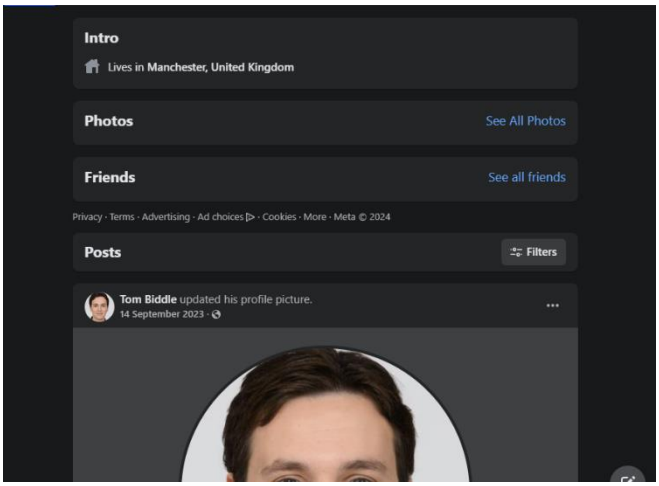


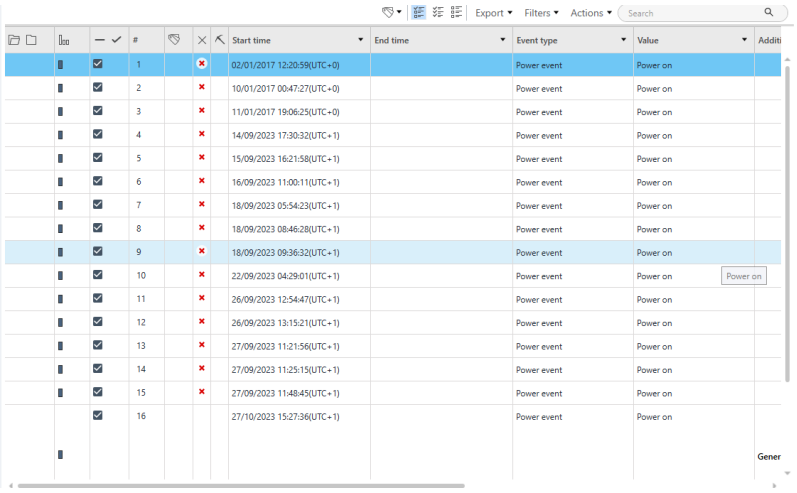
Figure 9 Tom Biddle Facebook information.

After logging into Facebook to search for more details, the page shows that Tom lives in Manchester, and he updated his profile picture on the 14th of September 2023.

31/10/2010 to 25/10/2021

Many images of which most were women were identified. Some of which are children are identified from cached browser. After looking into the hex of the source file, the URL for the images is found to be all from www.vista.com.

The device bootup time itself appears to show the device powering on from 02/01/2017 however many of the files appear to be deleted and the only evidence of the device booting is from 2023.



#	Start time	End time	Event type	Value
1	02/01/2017 12:20:59(UTC+0)		Power event	Power on
2	10/01/2017 00:47:27(UTC+0)		Power event	Power on
3	11/01/2017 19:06:25(UTC+0)		Power event	Power on
4	14/09/2023 17:30:32(UTC+1)		Power event	Power on
5	15/09/2023 16:21:58(UTC+1)		Power event	Power on
6	16/09/2023 11:00:11(UTC+1)		Power event	Power on
7	18/09/2023 05:54:23(UTC+1)		Power event	Power on
8	18/09/2023 08:46:28(UTC+1)		Power event	Power on
9	18/09/2023 09:36:32(UTC+1)		Power event	Power on
10	22/09/2023 04:29:01(UTC+1)		Power event	Power on
11	26/09/2023 12:54:47(UTC+1)		Power event	Power on
12	26/09/2023 13:15:21(UTC+1)		Power event	Power on
13	27/09/2023 11:21:56(UTC+1)		Power event	Power on
14	27/09/2023 11:25:15(UTC+1)		Power event	Power on
15	27/09/2023 11:48:45(UTC+1)		Power event	Power on
16	27/10/2023 15:27:36(UTC+1)		Power event	Power on

Figure 10 Power Events

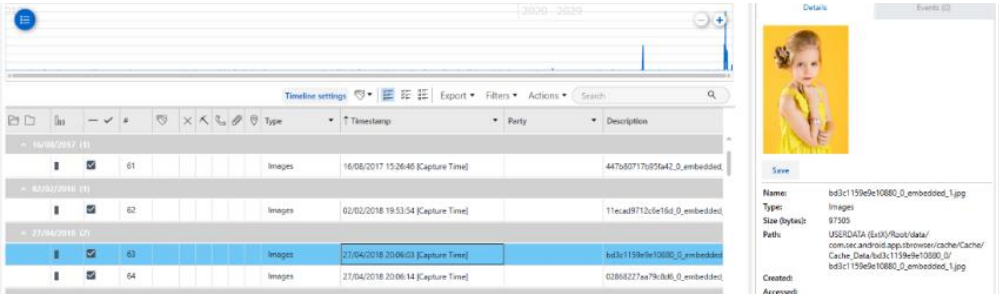


Figure 11 Images of children

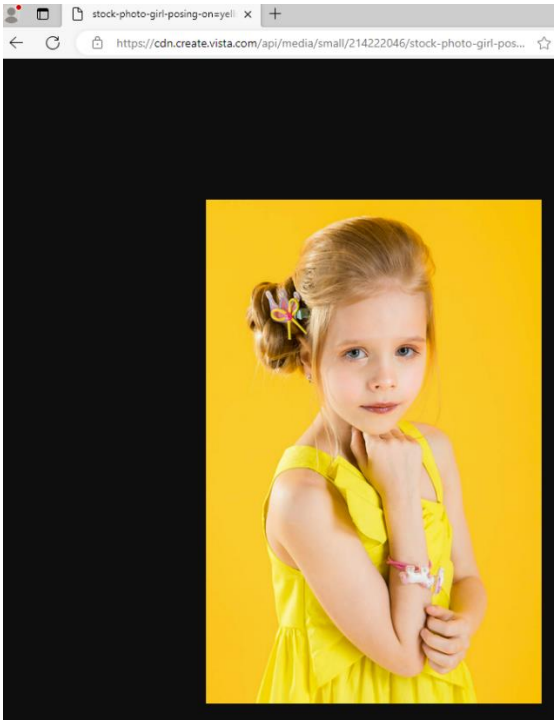


Figure 12 Image of child found on website.

09/03/2022

There was a sim swap at 13:23:00 and a connection to the SSID “Steve” shortly after. Downloads occurred from the phone’s browser.

SIM Change Time	09/03/2022 13:23:00(UTC+0)	SimCard.dat : 0xE

Figure 13 SIM swap.

09/03/2022 (7)

		☑	112						Wireless Network...	09/03/2022 13:23:34(UTC+0)		SSId: Steve BSSId: 22:b0:01:9ff2:d9	
		☑	113						Installed Applicat...	09/03/2022 13:24:29(UTC+0) [Purchase date]		Google Play services	
		☑	114						Downloads	09/03/2022 13:30:28(UTC+0) [Start time]		/storage/emulated/0/Download/A...	Samsung Internet Browser
		☑	115						Downloads	09/03/2022 13:30:29(UTC+0) [End time]		/storage/emulated/0/Download/A...	Samsung Internet Browser
		☑	116						Cookies	09/03/2022 13:31:38(UTC+0) [Creation time]		.android.com	Samsung Internet Browser
		☑	117						Downloads	09/03/2022 13:31:38(UTC+0) [Start time]		/storage/emulated/0/Download/A...	Samsung Internet Browser
		☑	118						Downloads	09/03/2022 13:31:39(UTC+0) [End time]		/storage/emulated/0/Download/A...	Samsung Internet Browser

Figure 14 Downloads.

08/09/2023

A new SSID was used to connect to an access point and there was more network usage within that day. Many searches related to dating websites have been accessed as well as photos of teenage girls. A teenage girl was downloaded from pixabay.com

08/09/2023 (311)

		☑	1112						Network Usages	08/09/2023 15:00:00(UTC+1) [Date started]		SSId: BT-QMATW3

Figure 15 New SSID connection.

Web History	08/09/2023 16:21:09(UTC+1) [Last Visited]		free dating sites uk - Google Searc
Searched Items	08/09/2023 16:21:09(UTC+1)		free dat
Searched Items	08/09/2023 16:21:09(UTC+1)		free dating sites uk
Web History	08/09/2023 16:21:10(UTC+1) [Last Visited]		free dating sites uk - Google Searc
Searched Items	08/09/2023 16:21:10(UTC+1)		free dat
Searched Items	08/09/2023 16:21:10(UTC+1)		free dating sites uk
Web History	08/09/2023 16:22:16(UTC+1) [Last Visited]		free dating sites uk - Google Searc
Searched Items	08/09/2023 16:22:16(UTC+1)		free dat
Searched Items	08/09/2023 16:22:16(UTC+1)		free dating sites uk
Web History	08/09/2023 16:22:27(UTC+1) [Last Visited]		OkCupid Paid Features & Subscrip.
Cookies	08/09/2023 16:22:29(UTC+1) [Creation time]		.help.okcupid.com
Cookies	08/09/2023 16:24:52(UTC+1) [Creation time]		.stockfreeimages.com
Cookies	08/09/2023 16:24:52(UTC+1) [Creation time]		.stockfreeimages.com

Figure 16 Dating site search.

Web History	08/09/2023 16:24:52(UTC+1) [Last Visited]		18,000+ Teen girl Free Stock Phot...	Samsung Internet Browser

Figure 17 Search for teenage girls.

Searched Items	08/09/2023 16:28:15(UTC+1)		teen girl royalty free	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		create.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		create.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		create.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		create.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		create.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Accessed]		create.vista.com	Samsung Internet Browser
Cookies	08/09/2023 16:28:15(UTC+1) [Creation time]		.vista.com	Samsung Internet Browser
Web History	08/09/2023 16:28:37(UTC+1) [Last Visited]		teen girl royalty free - Google Sea...	Samsung Internet Browser
Searched Items	08/09/2023 16:28:37(UTC+1)		teen girl royalty free#ip=1	Samsung Internet Browser

Figure 18 Web search.

An image of a child is downloaded from the internet.

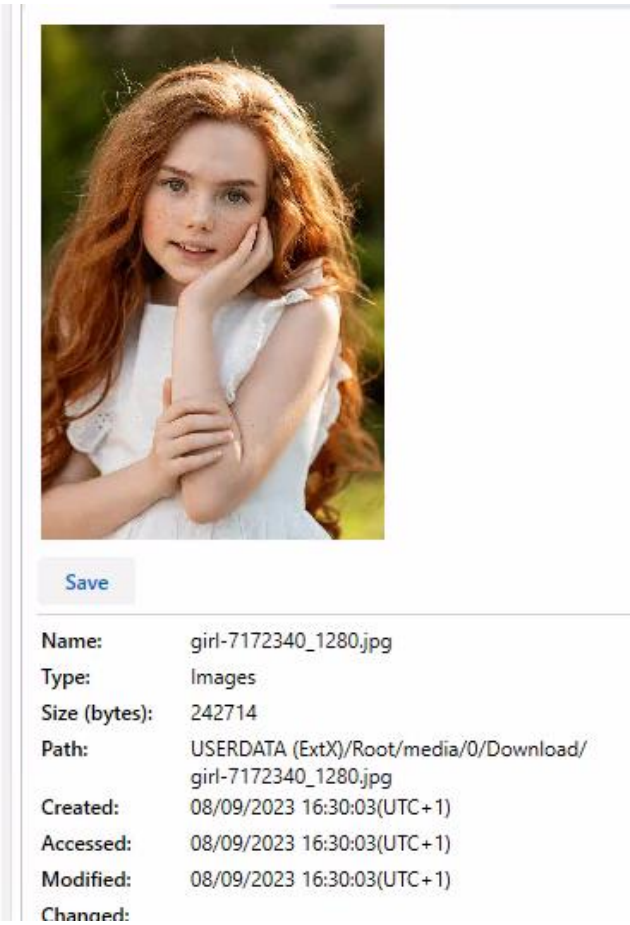


Figure 19 Image of child downloaded from internet.

13/09/2023

Tom Biddle received an SMS message from ASDA Mobile which is a sim provider. Tom Biddle created his Gmail account as well as an account on a dating profile on match.com and ASDA Mobile.

1459						Instant Messages	13/09/2023 15:41:44(UTC+1)	From: ASDAMobile To:	To browse the mobile internet and...	Android CallLog database	
1460						Instant Messages	13/09/2023 15:41:44(UTC+1)	From: ASDAMobile	To browse the mobile internet and...	Native Messages	

Figure 20 Asda Mobile message.

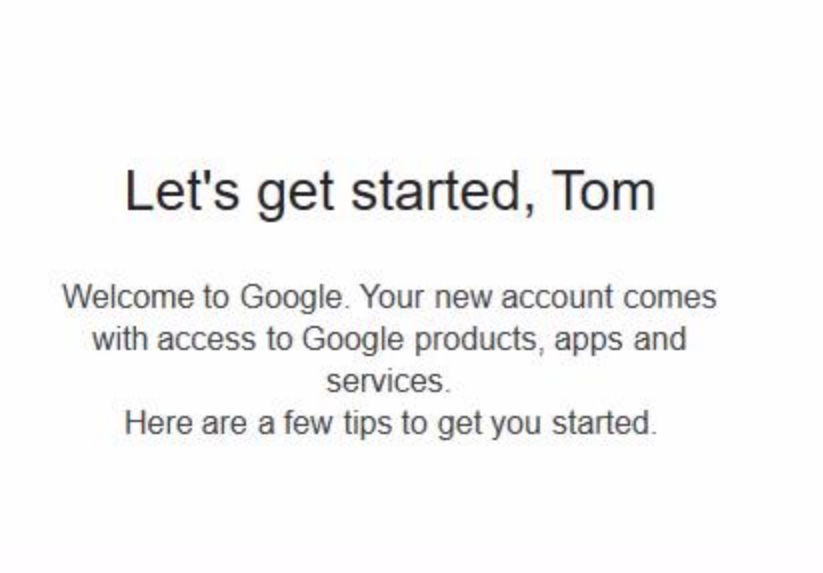


Figure 21 Google account registration.

Emails	13/09/2023 16:03:15(UTC+1)	From: match@e1.match.... To: tombiddle029@gmai...	<u></u><div bgcolor="#eef0f5"...	Gmail

Figure 22 Dating profile registration.

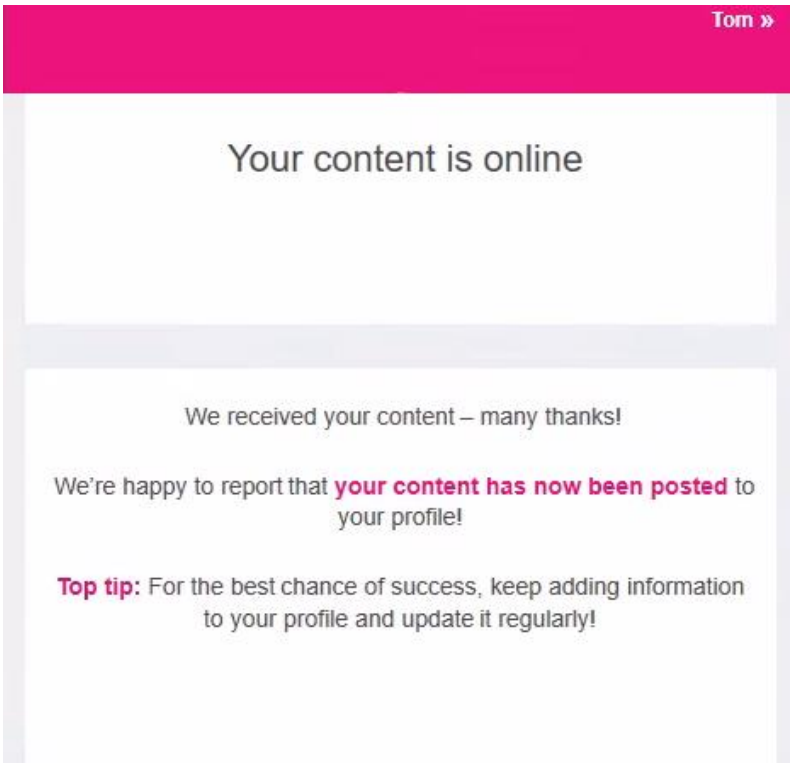


Figure 23 Match.com registration.

A phone number +447520601004 was messaged with an “error message” in the body and then called. This number was from Google’s verification message.

	☑	1631						Instant Messages	13/09/2023 16:13:10(UTC+1)	From: To: +447520601004
	☑	1632						Call Log	13/09/2023 16:13:25(UTC+1)	To: +447520601004

Figure 24 Tom sending message and calling.

Tom Biddle’s google account was identified so his google location tag photo and reviews were checked by accessing his Gmail account (tombiddle029@gmail.com) on google chat and checking the data-person-id option in the inspect window that checks his google ID. The google ID was used to check the data using this link: https://www.google.com/maps/contrib/105053130270568608678

The data showed no results for reviews and contributions.

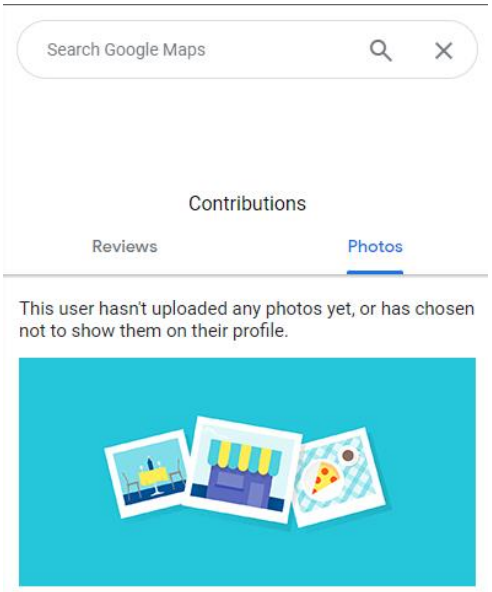


Figure 25 Google Maps contributions.

```
<div jsaction="rcuQ6b:npT2md; keydown:mAamLc" jsname="kIV4t
b" jscontroller="vIMXmd" data-person-id="105053130270568608
78"></div> == $0
```

Figure 26 Google ID used to find contributions.

Web History	13/09/2023 16:28:15(UTC+1) [Last Visited]		Purchase a top-up | Asda Mobile	Samsung Internet Browser
Web History	13/09/2023 16:28:20(UTC+1) [Last Visited]		Purchase a top-up | Asda Mobile	Samsung Internet Browser
Web History	13/09/2023 16:28:28(UTC+1) [Last Visited]		Top-up payment | Asda Mobile	Samsung Internet Browser
Web History	13/09/2023 16:28:29(UTC+1) [Last Visited]		Top-up payment | Asda Mobile	Samsung Internet Browser
Autofill	13/09/2023 16:29:02(UTC+1)		cardholderName : John Kingston	Samsung Internet Browser
Autofill	13/09/2023 16:29:02(UTC+1)		expiryDate.expiryMonth : 08	Samsung Internet Browser
Autofill	13/09/2023 16:29:02(UTC+1)		expiryDate.expiryYear : 28	Samsung Internet Browser

Figure 27 John Kingston top up.

Tom Biddle signed up to another dating account on internationalcupid.com. A £5 top up was provided for the ASDA sim card. The card holder name was "John Kingston" within the autofill.

14/09/2023

Tom Biddle creates his Facebook account revealing his birth date which is 6/6/1994 from the autofill data. A phone number 07818027905 is also provided in the reg_email autofill.

Web History	14/09/2023 10:19:17(UTC+1) [Last Visited]		Join Facebook	Samsung Internet Browser
Autofill	14/09/2023 10:20:06(UTC+1)		firstname : Tom	Samsung Internet Browser
Autofill	14/09/2023 10:20:06(UTC+1)		lastname : Biddle	Samsung Internet Browser
Autofill	14/09/2023 10:20:06(UTC+1)		birthday_day : 6	Samsung Internet Browser
Autofill	14/09/2023 10:20:06(UTC+1)		birthday_month : 6	Samsung Internet Browser
Autofill	14/09/2023 10:20:06(UTC+1)		birthday_year : 1994	Samsung Internet Browser
Autofill	14/09/2023 10:20:06(UTC+1)		reg_email__ : 07818027905	Samsung Internet Browser

Figure 28 Autofill data revealing date of birth.

Tom Biddle receives a message from Katie Cameron on Facebook Messenger with a message saying she saw his profile and would want to chat to him. Her Facebook ID is provided and searched on the internet.

Source:	Facebook Messenger
Subject:	
Timestamp:	14/09/2023 10:39:02(UTC+1)
Status:	Sent
Message Type:	App Message
SMSC:	
Device description:	
Folder:	
Priority:	
Service Identifier:	
Extraction:	Physical
Source file:	USERDATA (ExtX)/Root/data/com.facebook.orca/databases/msys_database_61551066486266-wal : 0x58AF (Table: messages; Size: 2776912 bytes)

From

From: 61551066486266 Tom Biddle

Participants

61550864656601	Katie Cameron
61551066486266	Tom Biddle (owner)

Label

Attachment

SharedContacts

Body

Activate Windows
Go to Settings to activate Windows.

Hi! I saw your profile on Match.com and I found you here. I'd love to chat to you.

Figure 29 Katie Cameron Message

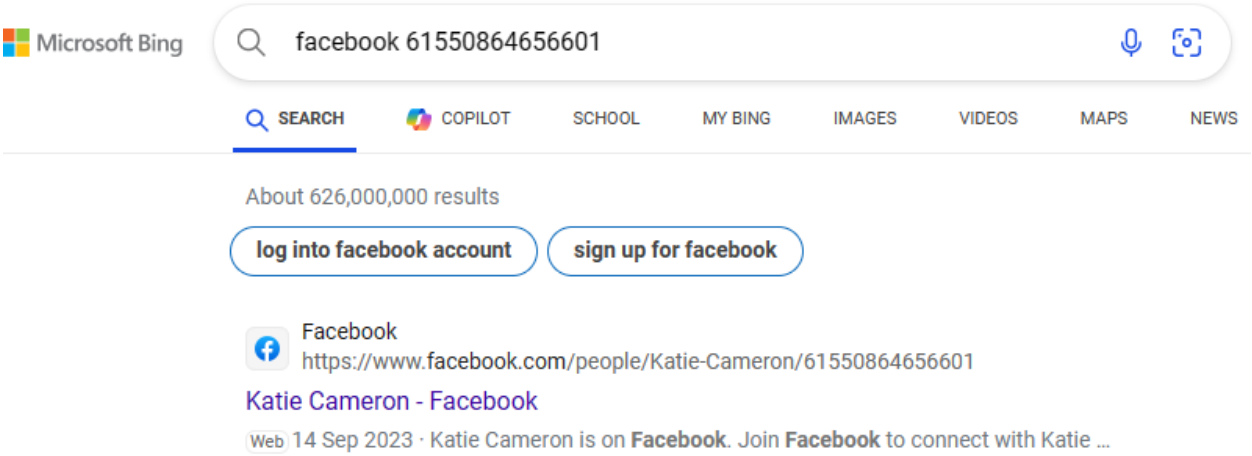


Figure 30 Facebook ID searched on google.

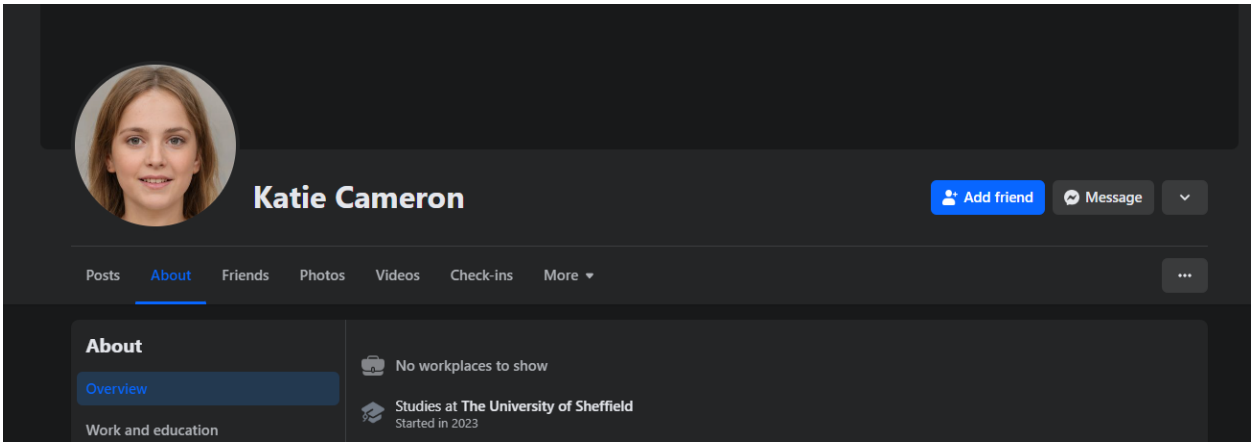


Figure 31 Katie Cameron FB profile.

The profile reveals that Katie studies at University of Sheffield and her profile picture was uploaded on 14/09/2023. They both exchange messages with each other on Facebook Messenger until Katie asks Tom to chat on text and provided her phone number. Katie provided her phone number in two different messages to Tom. Tom reveals to her that he lives near Manchester during their exchange in messages on Facebook Messenger. Tom added the number to his contacts which is showing as deleted.

			Instant Messages	14/09/2023 11:14:11(UTC+1)	From: System Message S...	You can now call each other and s...	Facebook Messenger
			Web History	14/09/2023 11:20:41(UTC+1) [Last Visited]		Facebook	Samsung Internet Browser
			Web History	14/09/2023 11:20:47(UTC+1) [Last Visited]		Facebook	Samsung Internet Browser
			Instant Messages	14/09/2023 11:22:55(UTC+1)	From: 61551066486266...	Great! R U into sports, or music, o...	Facebook Messenger
			Instant Messages	14/09/2023 11:24:31(UTC+1)	From: 61550864656601...	I luv music... Specially Justin Biebe...	Facebook Messenger
			Instant Messages	14/09/2023 11:28:44(UTC+1)	From: 61550864656601...	Oh wow! You know there's one thi...	Facebook Messenger
			Instant Messages	14/09/2023 11:30:38(UTC+1)	From: 61550864656601...	That's a funny question.I think Do...	Facebook Messenger
			Instant Messages	14/09/2023 11:32:13(UTC+1)	From: 61551066486266...	I love Doctor Who!	Facebook Messenger
			Instant Messages	14/09/2023 11:32:59(UTC+1)	From: 61550864656601...	Hey do you wanna chat on text?...	Facebook Messenger
			Instant Messages	14/09/2023 11:33:09(UTC+1)	From: 61550864656601...	103687	Facebook Messenger

Figure 32 Tom and Katie messaging each other on FB Messenger.

Tom and Katie exchange messages on text and Katie reveals she faked her age and name. She also says that she runs a secret agency, and she wants to send secure messages by emailing Tom instructions which he sends his email for. Tom is then advised to delete the email after reading the instructions which he did as the email was found in the deleted folder.

Instant Messages	14/09/2023 11:35:59(UTC+1)	From: +447437103687 To:	Great! Hey Tom, I'm so glad UR int...	Android CallLog database
Instant Messages	14/09/2023 11:35:59(UTC+1)	From: +447437103687	Great! Hey Tom, I'm so glad UR int...	Native Messages
Instant Messages	14/09/2023 11:36:35(UTC+1)	From: To: +447437103687	You look young, free, single and b...	Android CallLog database
Instant Messages	14/09/2023 11:36:35(UTC+1)	From: To: +447437103687	You look young, free, single and b...	Native Messages
Instant Messages	14/09/2023 11:37:36(UTC+1)	From: +447437103687 To:	Ha ha. Do you like young women,...	Android CallLog database
Instant Messages	14/09/2023 11:37:36(UTC+1)	From: +447437103687	Ha ha. Do you like young women,...	Native Messages
Instant Messages	14/09/2023 11:38:08(UTC+1)	From: To: +447437103687	Don't tell me you faked your age?	Android CallLog database
Instant Messages	14/09/2023 11:38:08(UTC+1)	From: To: +447437103687	Don't tell me you faked your age?	Native Messages

Figure 33 Tom and Katie exchanging text messages.

Instant Messages	14/09/2023 11:46:56(UTC+1)	From: +447437103687	Tom, we need a more secure meth...	Native Messages
Instant Messages	14/09/2023 11:47:28(UTC+1)	From: To: +447437103687	Tombiddle029@gmail.com	Android CallLog database
Instant Messages	14/09/2023 11:47:28(UTC+1)	From: To: +447437103687	Tombiddle029@gmail.com	Native Messages

Figure 34 Tom sending his email.

Tom received an email from Katie which he deleted after being told to within the email. The email asked Tom to install an application called Pixelknot. Katie later sends pictures for Tom to process the pictures with the password being Katie. Tom was asked to delete all emails and Pixelknot after.

From

From: katiecam211@gmail.com Kate Cameron

To

To: tombiddle029@gmail.com tombiddle029@gmail.cc

CC

BCC

Attachments

Body HTML Text

Install an application called Pixelknot on your phone. Then I will send you some pictures -process them with Pixelknot.

Password will be Katie

Remember to delete this message and, when you are done, delete all emails from me and Pixelknot too

Figure 35 Email from Kate.

The katiecam211@gmail.com email was checked just like for Tom's email for location data which was provided no results.

```
data-person-id="115787382459232465798"
```

Figure 36 Katie email being checked.

The Pixelknot application was searched and installed from the play store. The application hides secret messages in an image that can be revealed from a given password.

Searched Items	14/09/2023 17:31:46(UTC+1)		pixelknot	Play Store
Installed Applicat...	14/09/2023 17:32:44(UTC+1) [Purchase date]		PixelKnot: Hidden Messages	

Figure 37 Pixelknot installed.

15/09/2023

Katie sent an email to Tom containing only an image of a tree. Pixelknot was installed on an android device and the image was checked to see if it was used by the application to hide secret messages. The password Katie was used to reveal the message for IMG_20230915_144429.jpg

Figure 38 Email from Katie of a tree.

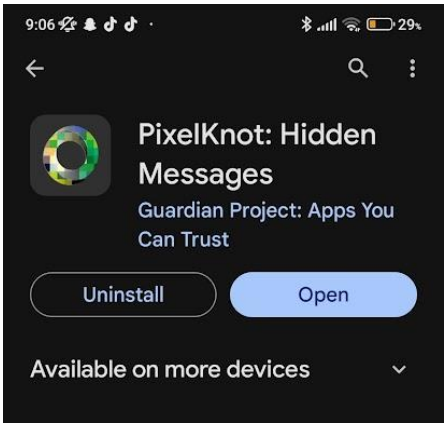


Figure 39 Pixelknot installed on android device.

The message contained the message in figure 40:

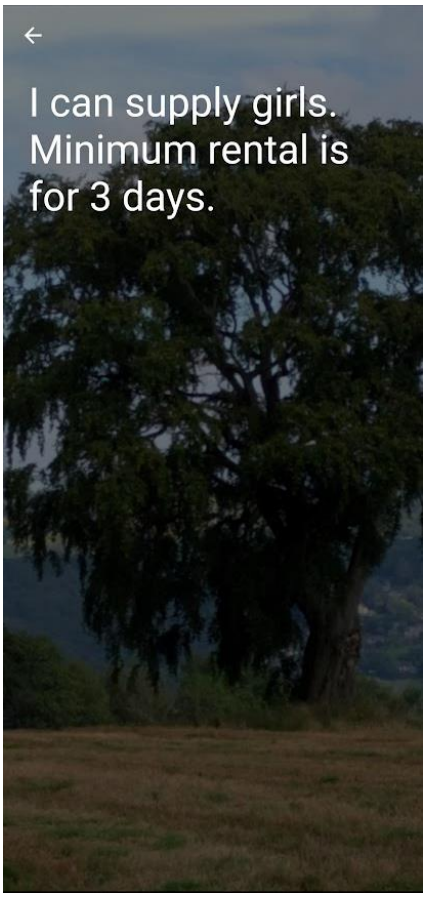


Figure 40 Secret message from IMG_20230915_144429.jpg

Tom sent an email shortly after with an image of a ginger haired girl which he downloaded previously as girl-7172340_1280.jpg. The secret message was revealed in figure 42.

Figure 41 Email sent to Katie from Tom

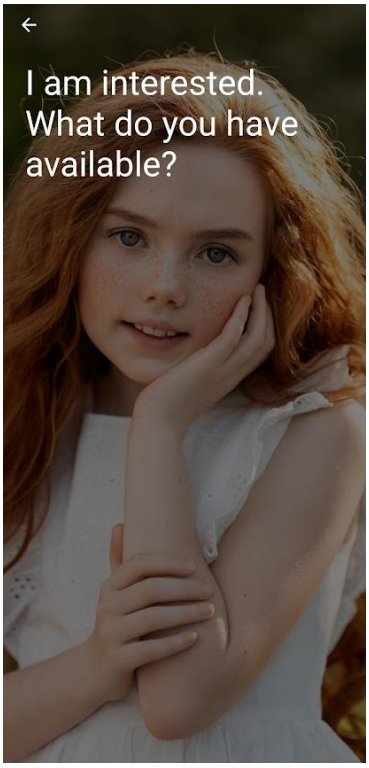


Figure 42 Secret message from girl-7172340_1280.jpg

Kate later sent an email with an image of a wall IMG_20230915_144729.jpg which revealed a secret message to download another app and to use images named after numbers for that in figure 44.

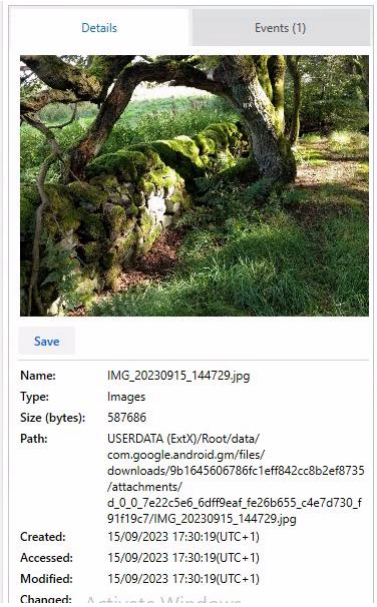


Figure 43 Kate email with image of wall.

Figure 44 Secret message from IMG_20230915_144729.jpg

16/09/2023

Tom received another email from Kate. This time the email contains a hyperlink called one.jpg to google drive which requires access. Kate sends a similar email shortly after but this time two.jpg with a Google Drive link that also requires access.

Folder: Inbox, Personal
Subject: One
Timestamp: 16/09/2023 07:43:54(UTC+1)
Priority:
Source: Gmail
Status:
Extraction: Physical
Source file: USERDATA (ExtX)/Root/data/com.google.android.gm/databases/bigTopDataDB.598685270 : 0xD0175 (Size: 1454080 bytes)

From

From: katiecam211@gmail.com Kate Cameron

To

To: tombiddle029@gmail.com tombiddle029@gmail.cc

CC

BCC

Attachments

Body HTML Text

one.jpg

Figure 45 Email from Kate containing hyperlink to Google Drive

https://drive.google.com/file/u/0/d/1b3Xdd0V0NdwmgpFro1vO2xq-0hJXTtBA/view?usp=drivesdk&pli=1

Google Drive

You need access

Request access, or switch to an account with access.
Learn more

Message (optional)

Request access

Figure 46 one.jpg hyperlink results.

To

To: tombiddle029@gmail.com tombiddle029@gmail.cc

CC

BCC

Attachments

Body HTML Text

two.jpg

Email header

ource

Web History Translate Go to

Title:

Last Visited: 16/09/2023 07:44:42(UTC+1)

URL: https://drive.google.com/file/d/1wpMGRR8hnpFMnuanqSKYkElYBnoCfeWy/view?usp=drivesdk

Visits:

Activate Windows
Go to Settings to activate Windows.

Figure 47 Email from Kate containing hyperlink to Google Drive

https://drive.google.com/file/d/1wpMGRR8hnpFMnuanqSKYkElYBnoCfeWy/view?usp=drivesdk

Google Drive

You need access

Request access, or switch to an account with access.
Learn more

Message (optional)

Request access

Figure 48 two.jpg hyperlink results.

18/09/2023

Tom searches an application called Stephanie on the play store with an identifier of com.piekarskipiotr.stephanie

Searched Items	18/09/2023 06:04:03(UTC+1)		stephanie	Play Store
Installed Applicat...	18/09/2023 06:04:14(UTC+1) [Purchase date]			

Figure 49 Stephanie application searched and installed.

A google search found the application which is a steganography application to hide messages and files in a file as it was not found in the play store.

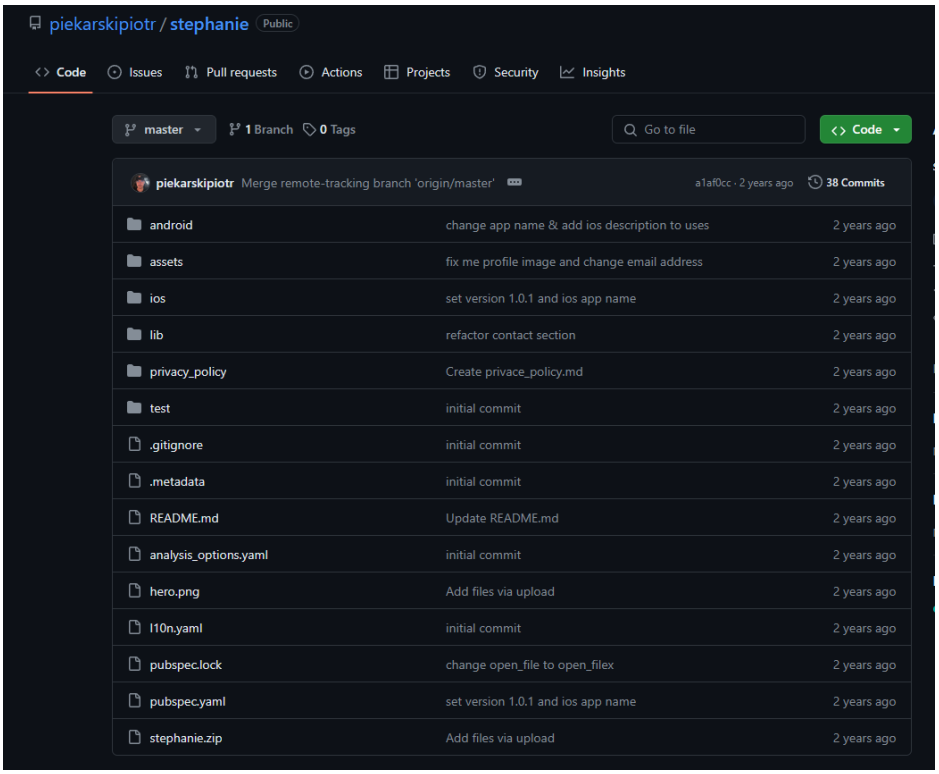


Figure 50 Stephanie application.

Kate sends another one.jpg hyperlink by email and shares it with Tom. The link requires access however, it is similar to the link from the previous one.jpg email.

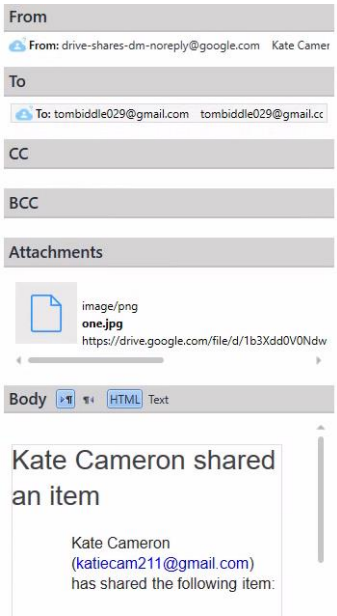


Figure 51 one.jpg shared with Tom.

Tom sends an SMS to Kate suggesting that he could not access the files as there is no evidence that he accessed them, so he sent the message to Kate.

Instant Messages	18/09/2023 09:40:51(UTC+1)	From: To: +447437103687	That didn't work
Instant Messages	18/09/2023 09:40:51(UTC+1)	From: To: +447437103687	That didn't work

Figure 52 Tom sending message to Kate.

22/09/2023

Figure 53 suggests that Kate sent the message to Tom to work on allowing access to the drive folder.

Instant Messages	22/09/2023 04:28:59(UTC+1)	From: +447437103687 To:	I am working on it
Instant Messages	22/09/2023 04:28:59(UTC+1)	From: +447437103687	I am working on it

Figure 53 Kate responding to Tom's message.

Images of children were downloaded. The search also contained teenage girls:

Downloads	22/09/2023 04:34:29(UTC+1) [Start time]		/storage/emulated/0/Download/a...	Samsung Internet Browser
Downloads	22/09/2023 04:36:09(UTC+1) [Start time]		/storage/emulated/0/Download/j...	Samsung Internet Browser
Downloads	22/09/2023 04:36:27(UTC+1) [Start time]		/storage/emulated/0/Download/s...	Samsung Internet Browser
Downloads	22/09/2023 04:37:27(UTC+1) [Start time]		/storage/emulated/0/Download/o...	Samsung Internet Browser
Downloads	22/09/2023 04:37:28(UTC+1) [End time]		/storage/emulated/0/Download/o...	Samsung Internet Browser
Downloads	22/09/2023 04:37:42(UTC+1) [Start time]		/storage/emulated/0/Download/a...	Samsung Internet Browser

26/09/2023

Tom receives a shared folder called “KT” from Kate. Opening the google drive folder revealed images of children. These images are also numbers mentioned previously that were used by the Stephanie application. The application was installed on the android device after finding it in the GitHub zip file and extracting and installing the apk file.

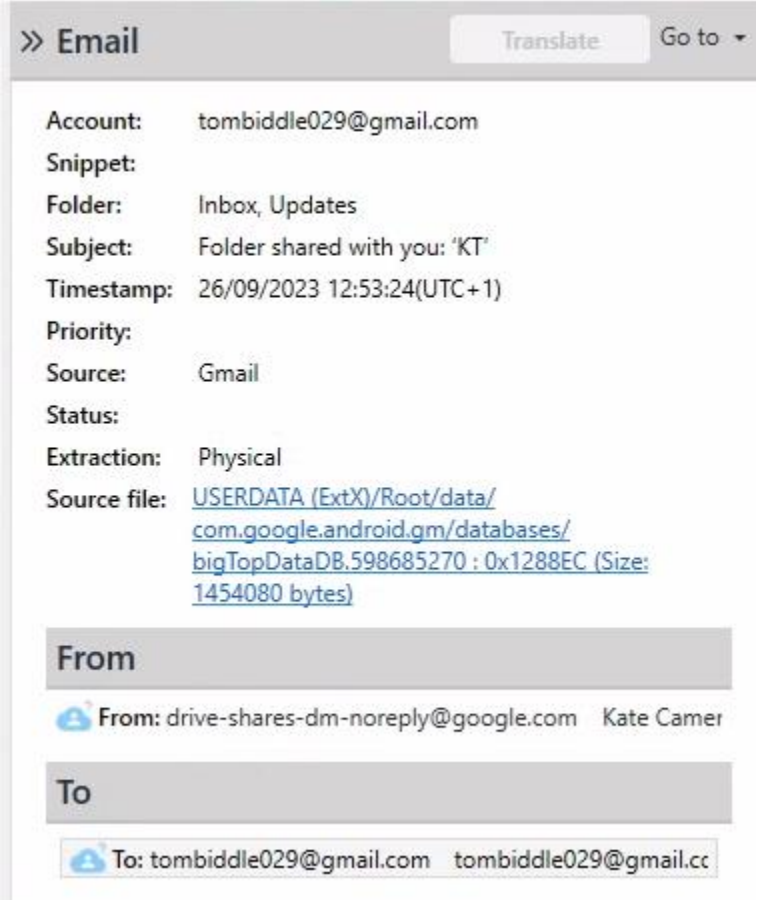


Figure 54 Shared "KT" Folder email.

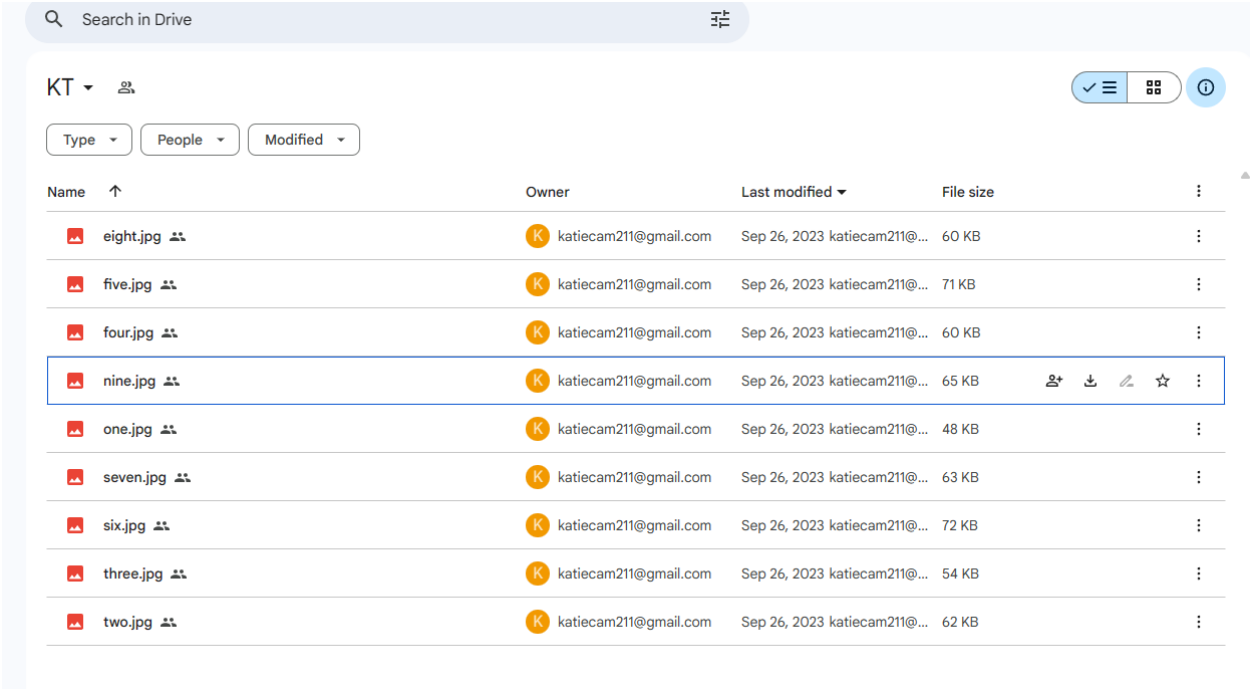


Figure 55 Shared "KT" folder.

All the images from the drive were checked on the application and they all provided an mp3 file of 0.19MB size however, none were able to be played.

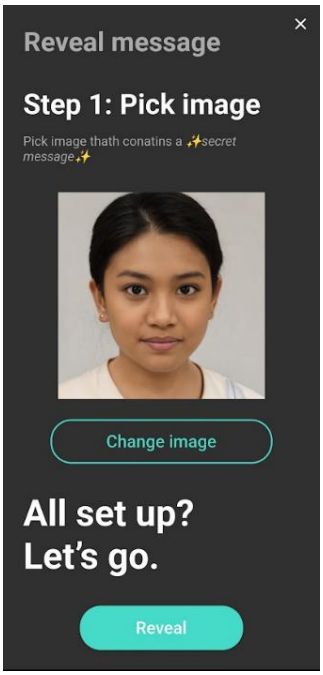


Figure 56 Image reveal process from KT folder.

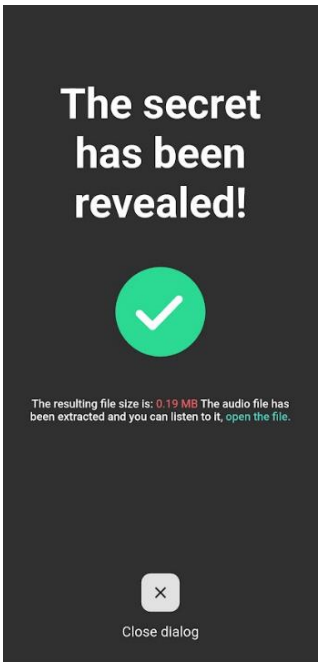


Figure 57 Revealed secret.

Figure 58 mp3 file not playing.

Tom sends an email containing image 0_one.jpg and Kate sends an email containing an image IMG_20230915_152522.jpg shortly after. Tom then searches for a file manager application and installs it.

Emails	26/09/2023 13:18:27(UTC+1)	From: tombiddle029@g... To: katiecam211@gmail....		Gmail
Emails	26/09/2023 13:27:18(UTC+1)	From: katiecam211@gm... To: tombiddle029@gmai...		Gmail
Searched Items	26/09/2023 13:28:02(UTC+1)		file manager	Play Store
Installed Applicat...	26/09/2023 13:28:33(UTC+1) [Purchase date]			

Figure 59 Emails containing image attachments between Tom and Kate

Image 0_one.jpg is checked on Pixelknot and the message reveals that Tom wants “Seven” which is most likely the female number 7 within the “KT” shared folder.

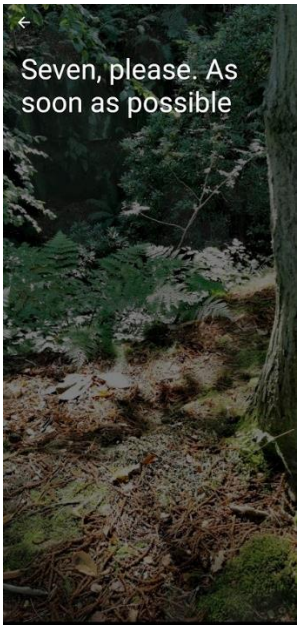


Figure 60 Pixelknot revealing 0_one.jpg message.

The image IMG_20230915_152522 .jpg from Kate’s email was attempted to be revealed. The image was stuck on 0% on Pixelknot and did not work on Stephanie application. The image file name was searched to find the image stored elsewhere and the same process

was applied to reveal the message. One file did not work in Pixelknot, but it worked on Stephanie however, the audio did not play.

#	Type	Fields	Content
Emails (1)			
1	Emails	Attachments	**katiecam211@gmail.com** (No subject) (26/09/2023 13:27:18(UTC+1))
Files (4)			
2	Files	Path Name	**/USERDATA (ExtX)/Root/data/com.google.android.gm/files/downloads/9b1645606786fc1eff842cc8b2...** 0 Bytes (USERDATA (ExtX))
3	Files	Path Name	**/USERDATA (ExtX)/Root/data/info.guardianproject.pixelknot/cache/pixelknot_selected_35507598-9ec6...** 618808 Bytes (USERDATA (ExtX))
4	Files	Path Name	**/USERDATA (ExtX)/Root/media/0/Download/IMG_20230915_152522.jpg** 618808 Bytes (USERDATA (ExtX))
5	Files	Path Name	**/Media/Phone/Download/IMG_20230915_152522.jpg** 618808 Bytes (Media)

Figure 61 IMG_20230915_152522.jpg searched on device.

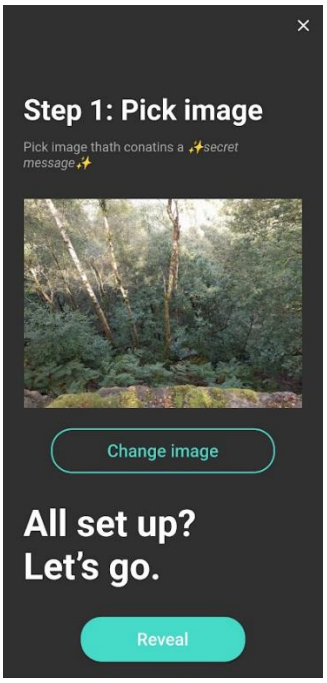


Figure 62 Image revealed but no audio.

The file path in figure 63 revealed the secret message in Pixelknot.

Figure 63 Secret message from Kate.

Figure 64 Image from number 7 in "KT" folder found on device.

Save

Name:	IMG_20230915_152522.jpg
Type:	Images
Size (bytes):	618808
Path:	Media/Phone/Download/ IMG_20230915_152522.jpg
Created:	26/09/2023 13:35:57
Accessed:	
Modified:	
Changed:	
Deleted:	
Extraction:	Advanced Logical
MD5:	c0921ac5dd0acbd117157836de369e7e
Source file:	IMG_20230915_152522.jpg

Figure 65 Image with secret message.

Tom searches vigenere cipher on google. Vigenere cipher is an encryption technique that adds complexity to the traditional cipher.

Searched Items	26/09/2023 13:31:22(UTC+1)		vigenere cipher
Web History	26/09/2023 13:31:22(UTC+1) [Last Visited]		vigenere cipher - Google Search
Cookies	26/09/2023 13:31:25(UTC+1) [Creation time]		www.google.com
Cookies	26/09/2023 13:31:27(UTC+1) [Creation time]		.google.com
Cookies	26/09/2023 13:31:28(UTC+1) [Creation time]		.google.com
Cookies	26/09/2023 13:31:28(UTC+1) [Creation time]		.google.com
Cookies	26/09/2023 13:31:28(UTC+1) [Creation time]		.google.com
Cookies	26/09/2023 13:31:28(UTC+1) [Creation time]		www.google.com
Web History	26/09/2023 13:31:31(UTC+1) [Last Visited]		Vigenere Cipher - Online Decoder,...
Web History	26/09/2023 13:31:31(UTC+1) [Last Visited]		Vigenere Cipher - Online Decoder,...

Figure 66 vigenere cipher searched on google.

Tom created a note on Samsung Notes. The context is unreadable. The context is typed into the Vigenere cypher decrypter on www.dcode.fr/vigenere-cipher and the results are "KATIE – Canal Street 10am. Bring Credit Card."

Title:	
Creation time:	26/09/2023 13:35:15(UTC+1)
Modification Time:	26/09/2023 13:35:15(UTC+1)
Last Modifier :	
Source:	Samsung Notes
Account:	
Extraction:	Physical
Manually decoded:	False
Source file:	USERDATA (ExtX)/Root/data/com.samsung.android.app.notes/databases/sdoc.db : 0x3FA7 (Table: sdoc; Size: 49152 bytes)

Summary

Body HTML Text

Magip Ctkmid 10af. Jvsnz kvodbb gkrw.

Figure 67 Content from Samsung Notes.

Figure 68 Decrypted vigenere cipher.

27/10/2023

The last power event was performed which ended the timeline.

Figure 69 Power Event

Manual evidence within Cellebrite was checked, and the carved image results provided no useful information. The screenshots in the media classification identified images that support the analysed evidence.

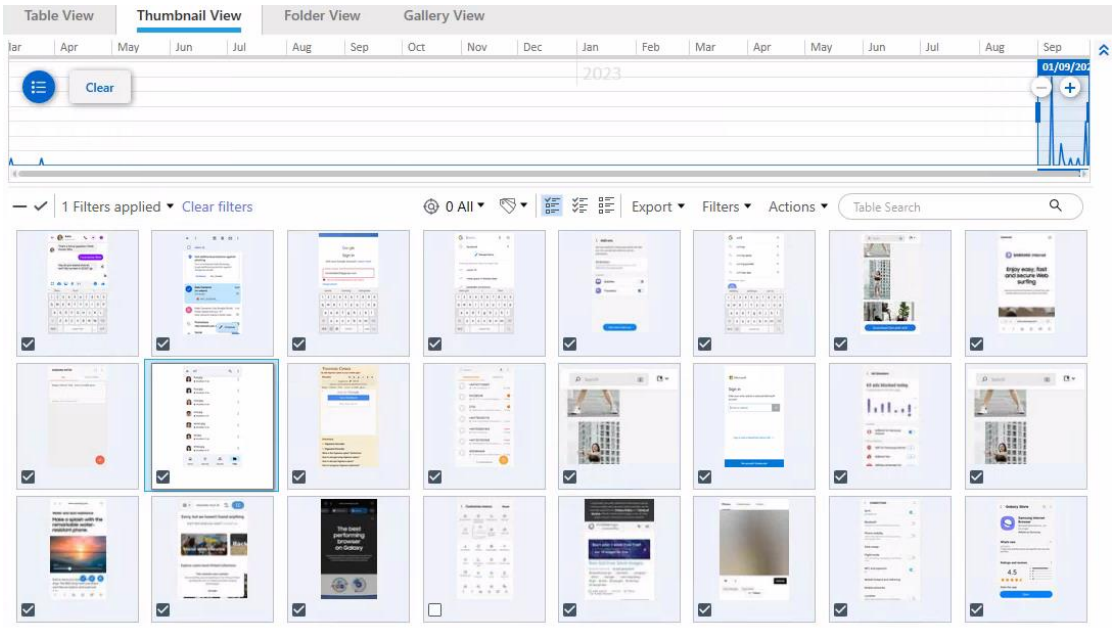


Figure 70 Screenshots from media classification.

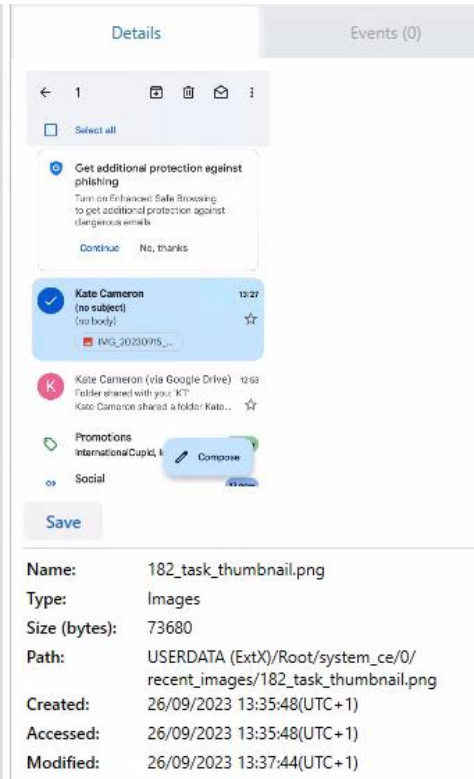


Figure 71 Katies email.

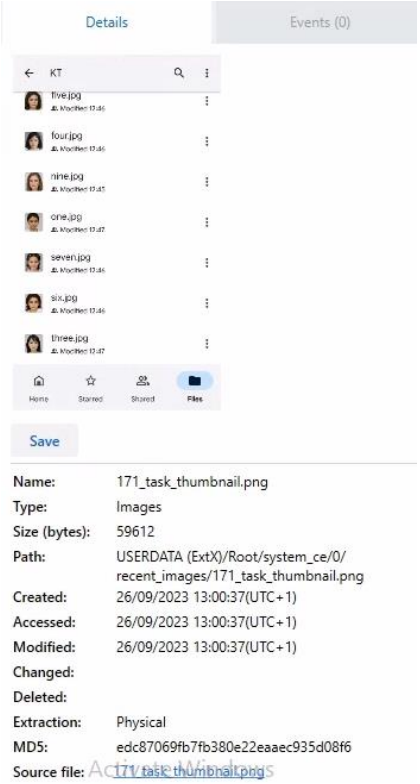


Figure 72 Shared KT folder screenshot.

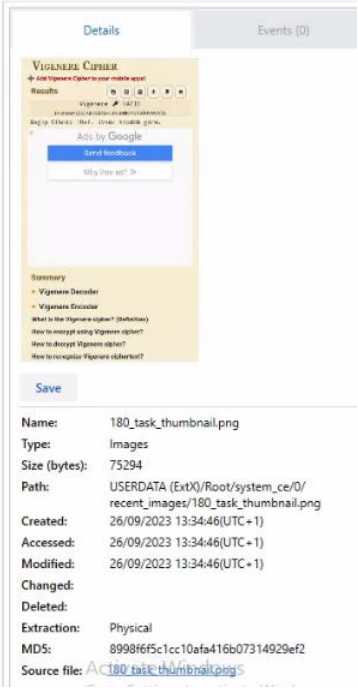


Figure 73 Vigenere Cipher website.

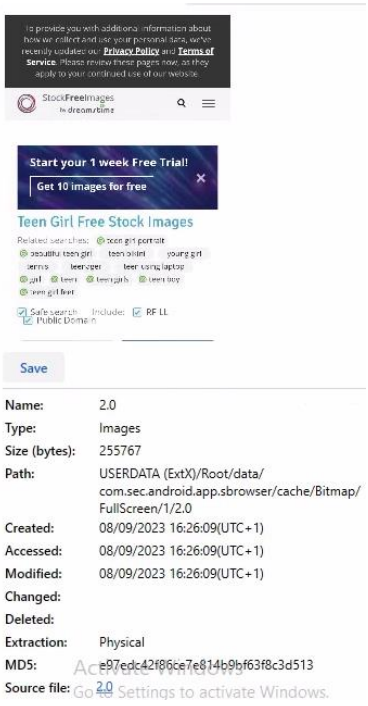


Figure 74 Stock image filters.

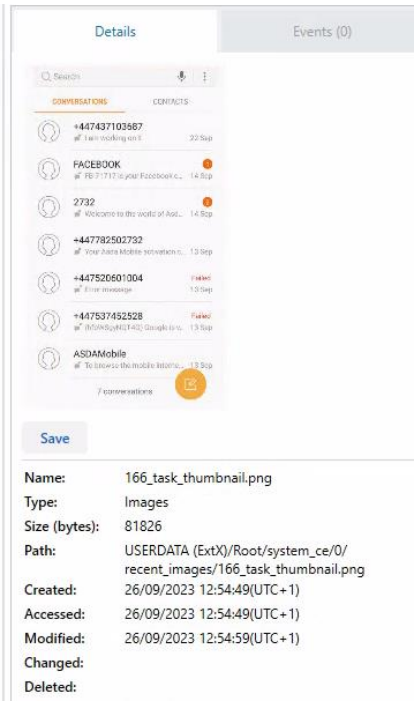


Figure 75 Messages.

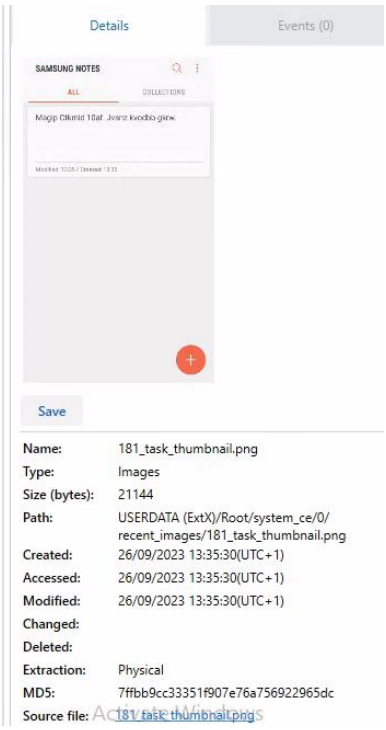


Figure 76 Notes.

Conclusion

In conclusion, the investigation into Tom Biddle's actions reveals several concerning legal implications. While the images of children that were downloaded from stock image websites did not depict indecent or sexually explicit content and were obtained with the consent of the individuals portrayed, Tom's subsequent interactions and intentions raise significant legal concerns.

Tom's engagement with Katie Cameron, despite being informed of her false identity and age, demonstrates a disregard for legal and ethical boundaries. His willingness to continue communicating with her, even secretly, indicates a potentially exploitative intent.

After Tom encountered Katie Cameron, he continued to message her even despite being informed that she is lying her age and name and identifying that he is above the age of 18. He also agrees to continue messaging her secretly after sending her his email and following instructions demonstrating a disregard for legal and ethical boundaries. His willingness to continue communicating with her even secretly, indicates a potentially exploitative intent.

Tom communicates with Kate over email by sending secret messages that are decrypted with the intention to rent children. He agreed to rent “number 7” which is a minor and to meet at Canal Street in Manchester where the device was seized. Tom noted the meeting date in his notes using Vigenere Cipher to hide evidence. These actions constitute a violation of the Modern Slavery Act 2015 (Legislation.gov, 2015). Section 1 of this act criminalises human trafficking, slavery, servitude, and forced or compulsory labour. Renting a child for any form of exploitation falls squarely within this prohibition.

Furthermore, Tom's actions potentially contravene provisions of the Sexual Offences Act 2003 (Legislation.gov.uk, 2003). Section 15A of this act criminalises sexual communication with a child under 16 years of age. Tom wanted to meet up in a location to rent a child where sexual communication may have been involved.

Additionally, Section 16 of the Sexual Offences Act 2003 prohibits sexual activity with a child under the age of 16. Tom's expressed intention to engage in such activity with the rented child further compounds the gravity of his offenses.

Finally, the Criminal Attempts Act 1981 (Legislation.gov.uk, 2010) may be broken even if Tom did not meet at the location as he would be attempting to commit a crime. Section 1 of this act outlines the offence of attempting to commit a criminal act. It states that "If, with intent to commit an offence to which this section applies, a person does an act which is more than merely preparatory to the commission of the offense, he is guilty of attempting to commit the offence." Tom would have committed a crime due to planning to meet someone to rent a child in exchange for money.

In summary, Tom's actions not only violate laws designed to protect vulnerable individuals from exploitation and abuse but also reflect a disturbing disregard for the well-being of minors.

Software Documentation

Cellebrite Physical Analyzer 7.63.0.126: https://cellebrite.com/en/physical-analyzer/

HxD: https://mh-nexus.de/en/hxd/

Pixelknot: https://play.google.com/store/apps/details?id=info.guardianproject.pixelknot&hl=en_GB&gl=US&pli=1

Stephanie: https://github.com/piekarskipiotr/stephanie

References

dotnet-bot (n.d.). DateTime.UnixEpoch Field (System). [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/dotnet/api/system.datetime.unixepoch?view=net-8.0 [Accessed 25 Apr. 2024].

Legislation.gov (2015). Modern Slavery Act 2015. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2015/30/section/1/enacted.

Legislation.gov.uk (2003). Sexual Offences Act 2003. [online] legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2003/42/contents.

legislation.gov.uk (2010). Criminal Attempts Act 1981. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1981/47.