Nottingham Trent University

COMP40571

Computer Forensics

Investigation Computer Forensics

N1334679 – Karunakar Reddy Machupalli

Table of contents

1. Introduction

1.1 Brief Overview of the Case and Objectives

This investigation involves examining a confiscated phone in response to a report concerning a suspicious Craigslist post. The deleted post was advertising a painting for sale. My aims are to ascertain whether any laws were violated or attempted to be violated using Craigslist, to investigate if the painting was promoted in other platforms, and to discern any motives or discover any accomplices. The inquiry entails examining a forensic image of the mobile device and assessing files located on a memory stick at the same location.

1.2 Importance of Computer Forensics in the Investigation

Computer forensics is essential in contemporary investigations, particularly in matters with digital data. It enables us to discover, examine, and present digital data in a legally admissible format. In this instance, computer forensics is crucial for:

Data Recovery: Despite the deletion of the suspicious post, forensic techniques can assist in retrieving this and other possibly valuable information.

Analyzing Digital Footprints: By examining the mobile device and memory stick, we can delineate the suspect's activity and interactions, uncovering additional evidence or accomplices.

Ensuring Data Integrity: Forensic techniques guarantee that the obtained data is retained in its original condition, sustaining its integrity for judicial processes.

Detecting Legal Infractions: Through the examination of digital evidence, we can ascertain particular statutes that may have been breached, establishing a definitive foundation for legal proceedings.

2. Analysis Procedures

2.1 Technical and Business Integration

The processes I employed in this inquiry closely align with business priorities by ensuring that digital evidence is managed in a manner that satisfies both legal and organizational objectives. This integration is essential for preserving the integrity of the inquiry and guaranteeing that the findings are admissible in court. By following best practices in computer forensics, we can deliver credible proof that bolsters the organization's IT security policy and aids in managing risks related to system misuse, fraud, intellectual property theft, or harassment.

2.2 Tools and Techniques

For my experiment, I used the Cellebrite Physical Analyser, an advanced tool for extracting and analyzing data from mobile devices. This instrument is important for:

Data Acquisition: Obtaining a forensic image of the device to guarantee the preservation of all data in its unaltered condition.

Data Analysis: Analyzing the contents of the mobile device, encompassing deleted files, messages, and application data.

Reporting: Producing comprehensive reports that elucidate the results and substantiate the conclusions of the investigation.

Furthermore, I employed many tools and procedures as required, including:

Memory Stick Examination: Analyzing the files on the memory stick (Document One.docx and password.txt) to extract pertinent information.

Analysis of Android programs: Installation and execution of requisite Android programs to retrieve specified data from the forensic image.

2.3 Step-by-Step Process

2.3.1 Data Acquisition

Explicitly outline the parameters of the investigation and assemble the requisite tools. This involves ensuring that all equipment is prepared and that we possess a precise plan of action. Upon arrival, secure the site to avert any alteration of the evidence. This may entail the utilization of police tape or conducting operations during the night in a corporate environment. Conduct a comprehensive examination and document the scene. This encompasses capturing images, recording videos, and creating sketches of the region. Examine beneath tables and desks and inspect for any devices that may store information. Obtain the computing equipment and generate a picture of them on-site, if feasible. This includes the phone and all pertinent information, including memory sticks. Activate Airplane mode before placing it into the Faraday bag. This inhibits the phone from establishing connections to any networks and potentially modifying data. Utilize the

Cellebrite Physical Analyser to generate a forensic image of the mobile device. This guarantees the preservation of data in its original condition and precludes any alteration. Transfer the files from the USB drive for subsequent analysis.

2.3.2 Data Preservation

Safeguard the forensic image and copied information to preserve their integrity. This procedure is essential for maintaining the admissibility of the evidence in court. Thoroughly record the chain of custody, noting each instance of access and transfer of the evidence. This encompasses the time, date, and the parties involved. Conduct integrity assessments utilizing hash methods like MD5 or SHA-1 to verify that the evidence remains unaltered since its collection.

Hash Type	Hash Value
MD5	**9420674cb784f6f3c726fbf5b84887a2**
SHA1	**487c2e53d8f38f07aefe5792e9724387ec7ab5bd**
CRC32	**17d0aedd**
SHA256	**bda6e5014f863c7216760374893b982b506253eb73ae8b9d22502ce08c0df75a**
SHA512	**996f7ab082eb495c92965505ee9b07b38f451981e1b22798d4411a2c5faf300bc58da1cdf00facbab254e9574c75db05f5301e828915b67e0dc1a1823441f0b1**
SHA384	**15300f6481a043740f7305b62faaf0f1b29601cc2dae1eb66cd1a738d2857c43b25fd5ef640f2a32e2c9e6c110fe2b8f**

2.3.3 Critical Evaluation

The Cellebrite Physical Analyser was selected for its specialized capabilities in mobile device forensics, despite the availability of similar forensic tools such as EnCase or FTK. It offers extensive data extraction and analytical capabilities that are crucial for this inquiry. The selected approach conforms to industry's best standards and guarantees the integrity and admissibility of the evidence. Alternative methods, such as manual data extraction, were considered less dependable and more susceptible to errors. The procedures were

designed to bolster the organization's IT security strategy and comply with legal mandates. Utilizing proven forensic tools and methodologies, I guaranteed that the study fulfilled both technical and business objectives.

3. Evidence Report

3.1 Evidence Collection

3.1.1 Evidence Collection from the Phone

Type	Included in Report	Total
Autofill	**6**	**6**
Calendar	**179 (179 Deleted)**	**179 (179 Deleted)**
Call Log	**1**	**1**
Chats	**3**	**3**
Native Messages	**3**	**3**
Contacts	**47 (20 Deleted)**	**47 (20 Deleted)**
Cookies	**510 (1 Deleted)**	**510 (1 Deleted)**
Device Events	**1**	**1**
Device Users	**1**	**1**
Downloads	**12**	**12**
Emails	**32**	**32**
Installed Applications	**430**	**430**
Instant Messages	**16 (1 Deleted)**	**16 (1 Deleted)**
Locations	**47**	**47**
Network Usages	**1059**	**1059**
Passwords	**269**	**269**
Searched Items	**12**	**12**
Social Media	**25**	**25**
User Accounts	**23**	**23**
Web Bookmarks	**2**	**2**
Web History	**233**	**233**
Wireless Networks	**46**	**46**

Timeline	**3503 (181 Deleted)**	**3503 (181 Deleted)**
Data Files	**18849 (550 Deleted)**	**18849 (1169 Deleted)**
Applications	**3882 (380 Deleted)**	**3882 (380 Deleted)**
Archives	**246 (117 Deleted)**	**246 (117 Deleted)**
Audio	**189 (11 Deleted)**	**189 (11 Deleted)**
Configurations	**48 (3 Deleted)**	**48 (3 Deleted)**
Databases	**961 (51 Deleted)**	**961 (51 Deleted)**
Documents	**16**	**16**
Images	**8424 (67 Deleted)**	**8424 (67 Deleted)**
Text	**4962 (537 Deleted)**	**4962 (537 Deleted)**
Videos	**121 (3 Deleted)**	**121 (3 Deleted)**

3.1.2 Evidence Collection from the Memory Stick

Artist Name	Nationality
Gerhard Richter	**German**
Bridget Riley	**British**
Damien Hirst	**British**
Sam Gilliam	**American**
Brice Marden	**American**
Christopher Wool	**American**

3.2 Analysis of Evidence

3.2.1 Messages

Evidence:

Session Information:

Start Time: 10/10/2024 16:17:09 (UTC+1)
Last Activity: 10/10/2024 17:34:16 (UTC+1)
Participants: +44 7393207567, (owner)

Timestamp (UTC+1)	From	Source App	Body
10/10/2024 16:17:09	+447393207567	Native Messages	HI, I saw your wooden plate advertised on Craigslist
10/10/2024 17:13:41	(owner)	Native Messages	Hey! Finally! Are you interested in it?
10/10/2024 17:16:51	+447393207567	Native Messages	I just wondered why you are asking such a high price for it
10/10/2024 17:23:09	(owner)	Native Messages	Look, I can't bring the price down much. I need the money.
10/10/2024 17:33:15	+447393207567	Native Messages	Yeah, that's not what I meant
10/10/2024 17:33:55	+447393207567	Native Messages	I have an idea that might help you make more money. Can we switch to email?
10/10/2024 17:34:16	(owner)	Native Messages	Umm, yeah. Waynemoon1400@gmail.com

Relevance:

The evidence from the native messages is particularly pertinent to the investigation. The evidence substantiates the suspect's active participation in the sale of the wooden plate on Craigslist, underscores a potential financial incentive, and implies the existence of a strategy to generate additional revenue. The messages demonstrate a connection between the suspect's phone number and email address, which is crucial for further inquiry into their communications and activities. This evidence substantiates the investigation's aim of comprehending the suspect's objectives, identifying any accomplices, and revealing any illicit activity associated with the sale.

3.2.2 Email

Evidence:

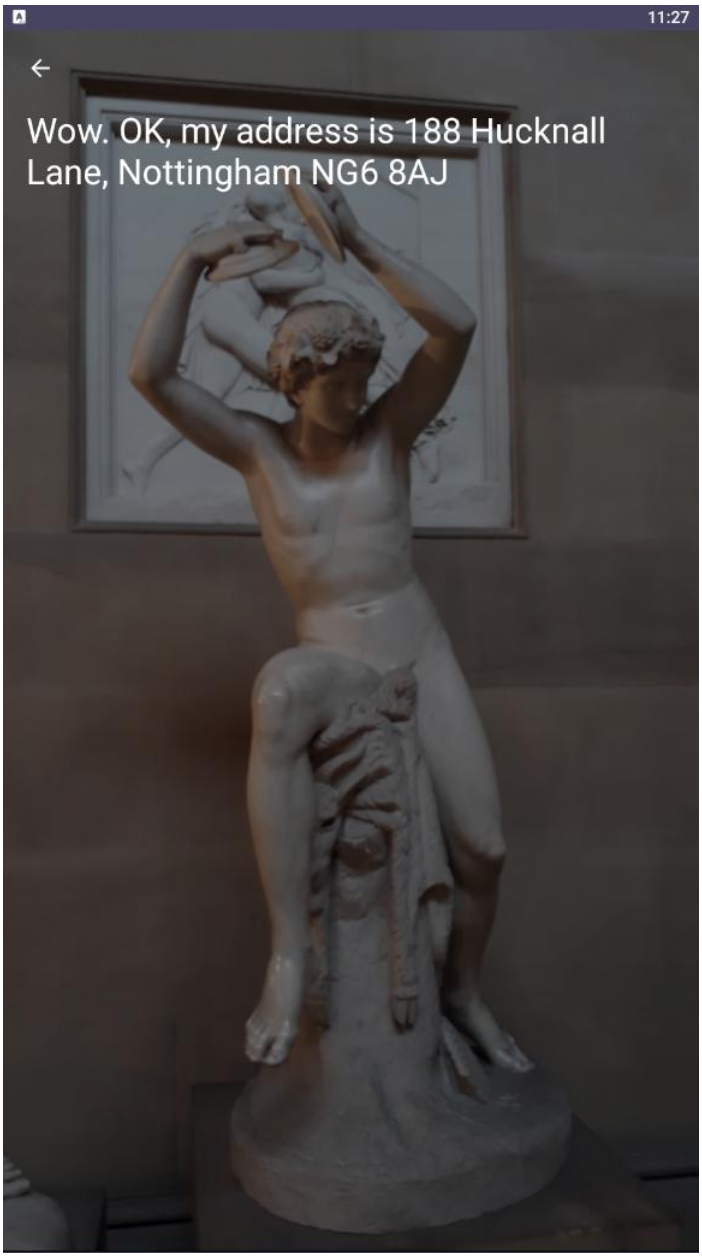
Timestamp	From	To	Subject	Body
25/10/2024 19:44:54	robot@craigslist.org	waynemoon1400@gmail.com	craigslist email verification	to complete your craigslist posting "Abstract painting" complete your posting: link
17/10/2024 09:52:17	waynemoon1400@gmail.com	tombiddle029@gmail.com	No subject	Attachment: 20241012_160934.jpg
16/10/2024 15:52:22	tombiddle029@gmail.com	waynemoon1400@gmail.com	No subject	Attachment: Ash*Tree-geograph.org.uk*-_590710.jpg
16/10/2024 15:46:45	tombiddle029@gmail.com	waynemoon1400@gmail.com	No subject	Attachment: 20241016_154350.jpg
16/10/2024 15:38:32	tombiddle029@gmail.com	waynemoon1400@gmail.com	No subject	Attachment: one.jpg
16/10/2024 15:35:00	tombiddle029@gmail.com	waynemoon1400@gmail.com	No subject	Attachment: image:84 (Empty File)
16/10/2024 15:30:39	tombiddle029@gmail.com	waynemoon1400@gmail.com	Re: Money making idea	You will shortly get a photo from me. Run it through Pixelknot. Password is Artwork. Then delete this message.
16/10/2024 15:27:05	waynemoon1400@gmail.com	tombiddle029@gmail.com	Re: Money making idea	Okay, done that
16/10/2024 14:54:36	tombiddle029@gmail.com	waynemoon1400@gmail.com	Re: Money making idea	I can tell you but it's a secret. Before I tell you you need to download an app called Pixelknot.
16/10/2024 14:51:54	waynemoon1400@gmail.com	tombiddle029@gmail.com	Re: Money making idea	Great :) So what should I learn about abstract art?
16/10/2024 14:43:41	tombiddle029@gmail.com	waynemoon1400@gmail.com	Re: Money making idea	Yeah, abstract art is good

16/10/2024 14:41:23	waynemoon1400@gmail.com	tombiddle029@gmail.com	Re: Money making idea	There are lots of types of art. Any on particular I should look at?
10/10/2024 17:42:44	waynemoon1400@gmail.com	tombiddle029@gmail.com	Re: Money making idea	A bit. I will get back to you in a while
10/10/2024 17:38:23	tombiddle029@gmail.com	waynemoon1400@gmail.com	Money making idea	Hi, this is about my money making idea for you. Do you know much about art?
10/10/2024 15:13:12	robot@craigslist.org	waynemoon1400@gmail.com	cl posting: Wooden carved plate	you created posting #7792130858 Wooden carved plate (for sale) view posting [link] edit or delete posting [link] help pages [link] stay safe [link] avoid scams [link] thanks for using craigslist try the app: Android [link] iPhone and iPad [link]
10/10/2024 15:07:13	(unknown sender)		No subject	
10/10/2024 15:06:04	robot@craigslist.org	waynemoon1400@gmail.com	craigslist login link	you requested a craigslist login link: log in as waynemoon1400@gmail.com
16/08/2024 13:01:43	robot@craigslist.org	waynemoon1400@gmail.com	cl posting: Wooden carved plate	you created posting #7775948717 Wooden carved plate (for sale) view posting [link] edit or delete posting [link] help pages [link] stay safe [link] avoid scams [link] thanks for using craigslist try the app: Android [link] iPhone and iPad [link]
16/08/2024 12:57:57	robot@craigslist.org	waynemoon1400@gmail.com	cl posting: Carved wooden plate	you created posting #7775948187 Carved wooden plate (for sale) view posting [link] edit or delete posting [link] help pages [link] stay safe [link] avoid scams [link] thanks for using craigslist try the app: Android [link] iPhone and iPad [link]
16/08/2024 12:47:05	robot@craigslist.org	waynemoon1400@gmail.com	craigslist account sign-up	to complete your craigslist account: complete account sign-up

14/08/2024 16:55:31	**mailerdaemon@googlemail.com**	**waynemoon1400@gmail.com**	**Delivery Status Notification (Failure)**	**Address not found. Your message wasn't delivered to manager@pretamanger.eastmidlandsairport.com because the domain couldn't be found. Check for typos or unnecessary spaces and try again.**
14/08/2024 16:55:16	**waynemoon1400@gmail.com**	**manager@pretamanger.eastmidlandsairport.com**	**My job**	**Dear sir, I was told this week after I got back from holiday that I have been fired from my job with Pret a Manger. This is supposed to be because I left the place in a mess when I closed the store on Thursday 1 August. I attach two pictures taken on Friday 2 August in the morning showing a clean store. There was a mess but I tidied it all up before I left. Please can I have my job back. Yours sincerely, Wayne Moon**

Attachments:

20241012_160934.jpg

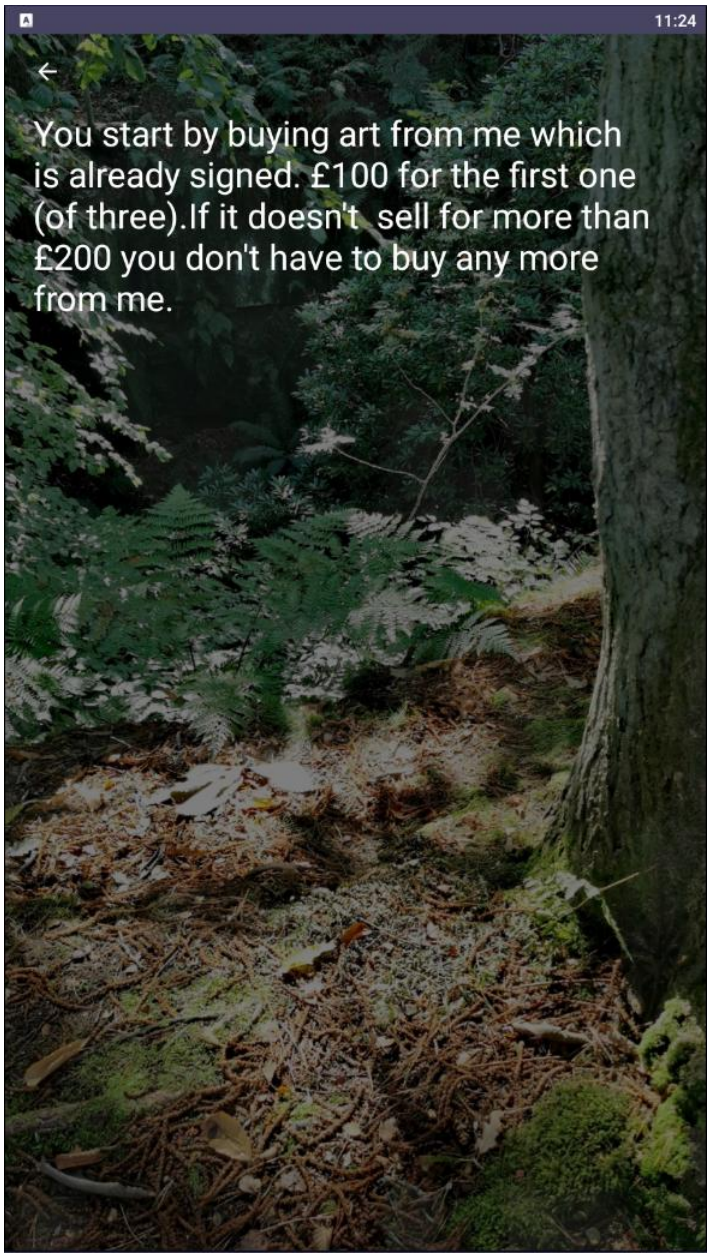


geograph.org.uk-_590710.jpg

20241016_154350.jpg


11:25
I ask you to buy from me so I make some profit out of this... and you wouldn't want anyone to tell the authorities what you are doing, would you?

One.jpg



Relevance:

The suspect, using the email waynemoon1400@gmail.com, received numerous emails from Craigslist verifying the establishment of ads for items such "Wooden carved plate," "Carved wooden plate," and "Abstract painting." The emails substantiate the suspect's

active participation in advertising items for sale on Craigslist. The suspect corresponded often with tombiddle029@gmail.com. The emails contained discussions of a "money-making idea" pertaining to art, directives for utilizing the Pixelknot application for steganography, and the exchange of photographs. This signifies a concerted effort to market products and obscure information. Correspondence between the suspect and tombiddle029@gmail.com indicates the utilization of Pixelknot, an application designed for concealing information within photographs. This implies an effort to obscure actions and denotes a degree of expertise in their operations. An email from the suspect to manager@pretamanger.eastmidlandsairport.com reveals that the suspect was just terminated from employment and is requesting reemployment. This offers insight into a possible financial incentive for the suspect's actions. Numerous communications contained image attachments that could be pertinent to the investigation. These photographs may offer additional evidence regarding the things being sold or the techniques employed to obscure information.

3.2.3 Images

Evidence:

Image Files
20181212_103512.jpg
20241012_151931.jpg
20241012_154423.jpg
20181212_103515.jpg
20241012_152029.jpg
20241012_154528.jpg
20181212_103518.jpg
20241012_152053.jpg
20241012_154659.jpg
20181212_103614.jpg
20241012_152119.jpg
20241012_154741.jpg
20220211_022318.jpg
20241012_152135.jpg

20241012_154908.jpg
20220211_022329.jpg
20241012_152151.jpg
20241012_155009.jpg
20220217_005833.jpg
20241012_152426.jpg
20241012_155208.jpg
20220217_005854.jpg
20241012_152520.jpg
20241012_155334.jpg
20220217_005935.jpg
20241012_152609.jpg
20241012_155418.jpg
20240802_084603.jpg
20241012_152633.jpg
20241012_155505.jpg
20240802_084626.jpg
20241012_152653.jpg
20241012_155933.jpg
20240816_124457.jpg
20241012_152722.jpg
20241012_155954.jpg
20240816_124537.jpg
20241012_152953.jpg
20241012_160041.jpg
20241012_151607.jpg
20241012_153016.jpg
20241012_160445.jpg
20241012_151638.jpg
20241012_153335.jpg
20241012_160717.jpg
20241012_151704.jpg
20241012_153541.jpg
20241012_160733.jpg
20241012_151723.jpg
20241012_153620.jpg
20241012_160934.jpg
20241012_151739.jpg
20241012_153838.jpg

20241016_154350.jpg
pending_media_1335190818613069302.WEBP

Relevance:

Visual representations of the artwork may confirm its existence and state. Offers visual documentation corroborating the sale and characterization of the artwork.

3.2.4 AutoFill

Evidence:

Posting Title	Source	Source file	Data	Timestamp	Last used date
Wooden carved plate	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Web	0x275C (Table: autofill; Size: 110592 bytes)	16/08/2024 13:01:15(UTC+1)	16/08/2024 13:01:15(UTC+1)
	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Web	0x26E3 (Table: autofill; Size: 110592 bytes)	16/08/2024 12:56:47(UTC+1)	16/08/2024 12:56:47(UTC+1)
	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Web	0x2719 (Table: autofill; Size: 110592 bytes)	16/08/2024 12:56:47(UTC+1)	16/08/2024 12:56:47(UTC+1)
Carved wooden plate	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Web	0x26BB (Table: autofill; Size: 110592 bytes)	16/08/2024 12:56:47(UTC+1)	16/08/2024 12:58:24(UTC+1)
	Chrome	USERDATA (ExtX)/Root/data/com.andro	0x27AD (Table: autofill; Size: 110592 bytes)	16/08/2024 12:55:38(UTC+1)	16/08/2024 12:55:38(UTC+1)

		id.chrome/app_chrome/Default/Web			
	Chrome	**USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Web**	**0x27F8 (Table: autofill; Size: 110592 bytes)**	**16/08/2024 12:47:01(UTC+1)**	**16/08/2024 12:47:01(UTC+1)**

Relevance:

The autofill data from the Chrome browser is important to the study. It indicates a trend of activity associated with the selling of items, specifically "Wooden carved plate" and "Carved wooden plate." The timestamps suggest a concentrated interval of activity on 16/08/2024, implying that the suspect was actively involved in online transactions or advertisements during this period. This evidence substantiates the investigation's aim of ascertaining the suspect's participation in the sale of goods and identifying any accomplices or supplementary things being sold.

3.2.5 Cookies

Evidence:

#	Name	Value	Domain	Source App	Source File	Creation Time (UTC+1)	Expires (UTC+0)	Accessed (UTC+1)
1	cl_session	fQOq12lYLhEXWFg0sCjvbDVNvBnDbp4KDnEDTzWS2ra53gevKDOXWofaF87g6GUu	.craigslist.org	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Cookies : 0x17C20 (Table: cookies; Size: 98304 bytes)	25/10/2024 19:49:15	24/11/2024 18:49:15	25/10/2024 19:49:15

2	cl_login	394772902%3Awaynemoon1400%40gmail.com	.craigslist.org	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Cookies : 0x17B19 (Table: cookies; Size: 98304 bytes)	25/10/2024 19:49:15	24/11/2024 18:49:15	25/10/2024 19:54:17
3	cl_session	UlaoVWwaE080SjOq9imE3kugmTcmEQFE42BzBt9g6kDnbhhtD0MHBQHOuFUqKVOP	.craigslist.org	Samsung Internet Browser	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/Cookies : 0x73E0 (Table: cookies; Size: 32768 bytes)	10/10/2024 15:07:20	09/11/2024 14:07:20	25/10/2024 13:24:02
4	cl_login	394772902%3Awaynemoon1400%40gmail.com	.craigslist.org	Samsung Internet Browser	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/Cookies : 0x7473 (Table: cookies; Size: 32768 bytes)	10/10/2024 15:07:20	09/11/2024 14:07:20	25/10/2024 13:24:02
5	cl_b	4	13b72cec6c0079c84f61c6b073c4a05393ac2506	1723808905uZMcI	.craigslist.org	Samsung Internet Browser	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/Cookies : 0x67C3 (Table: cookies; Size:	16/08/2024 12:48:24

							32768 bytes)	
6	cl_b	4	3add4a00e05c20dc85fdd2af57bd62075540bb9a	1723808777KmSwU	.craigslist.org	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Cookies : 0x148A2 (Table: cookies; Size: 98304 bytes)	16/08/2024 12:46:16
7	cl_def_hp	nottingham	.craigslist.org	Chrome	USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/Cookies : 0x14842 (Table: cookies; Size: 98304 bytes)	16/08/2024 12:46:16	25/10/2024 19:54:17	25/10/2024 19:54:17

Relevance:

The cookie evidence is significantly pertinent to the investigation. It verifies the suspect's ongoing and regular utilization of Craigslist across various browsers over an extended duration. The cookies associate the suspect's email address with the Craigslist account, so validating their identity. Moreover, the cookies provide timestamps that correspond with additional evidence, confirming the chronology of the suspect's actions. This evidence

establishes a definitive connection between the suspect and the Craigslist posts, so reinforcing the investigation's aims.

3.2.6 Installed Applications

Evidence:

#	Name	Description	Timestamp (UTC+1)	Source File	Purchase Date
1	PixelKnot	Application ID: info.guardianproject.pixelknot Version: 1.0.2.1 Operation Mode: Foreground Application Size (bytes): 0	USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db : 0x36E9F (Table: appstate; Size: 458752 bytes) USERDATA (ExtX)/Root/data/com.android.vending/databases/verify_apps.db : 0x4C710 (Size: 364544 bytes) USERDATA (ExtX)/Root/app/info.guardianproject.pixelknot-HSpksbvyidpgK5fHOCF9KA==/base.apk/AndroidManifest.xml : 0x3E2 (Size: 6472 bytes)	16/10/2024 15:24:49	Social Networking
2	Indeed Job Search	Application ID: com.indeed.android.jobsearch Version: 183.0 Operation Mode: Foreground Application Size (bytes): 0	USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db : 0x519CB (Table: appstate; Size: 458752 bytes) USERDATA (ExtX)/Root/data/com.android.vending/databases/verify_apps.db : 0x42227 (Size: 364544 bytes) USERDATA (ExtX)/Root/app/com.indeed.android.jobsearch-ByNpS1kpsPMumCKKlsQwAw==/base.apk/AndroidManifest.xml : 0xF98 (Size: 64440 bytes)	05/07/2024 09:29:50	Business

Relevance:

The applications loaded on the Samsung SM-A320FL Galaxy A3 offer significant context for the inquiry. PixelKnot, an application designed for steganography, enables users to conceal messages within photographs. The existence of this application on the suspect's cellphone is pertinent, indicating the suspect may have employed steganography to obscure information. This corresponds with email evidence indicating that the suspect was directed to utilize PixelKnot to conceal information within photographs. The acquisition date of 16/10/2024 suggests that the application was installed contemporaneously with the suspicious activity, so reinforcing its pertinence to the inquiry. Furthermore, Indeed Job Search, an application utilized for employment searches, was discovered on the suspect's cellphone. This suggests that the suspect was actively seeking employment, offering insight into the suspect's financial circumstances and motive. The purchase date of 05/07/2024 indicates that the suspect had been pursuing employment for several months, potentially elucidating the financial necessity highlighted in the texts and emails. These applications underscore the suspect's potential employment of steganography to obscure information and their financial circumstances as a plausible motive for their actions.

3.2.7 Web History

Evidence:

No.	Title	URL	Browser
1	**Abstract painting - arts & crafts - by owner craigslist**	https://nottingham.craigslist.org/art/7796506569.html	**Chrome**
2	**Abstract painting - arts & crafts - by owner craigslist**	https://nottingham.craigslist.org/art/d/cliftonnorth-ward-abstractpainting/7796506569.html?lang=en&cc=gb	**Chrome**
3	**Nottingham posting confirmation**	https://post.craigslist.org/k/_qMIOgCT7xGQqfTaq1ruOA/WulbO?lang=en&cc=gb	**Chrome**
4	**Nottingham posting confirmation**	https://accounts.craigslist.org/login/onetime?key=261387990NfiytN5VQh2eLOLleGYUWfBMcifkcB	**Chrome**

5	Nottingham posting confirmation	https://www.google.com/url?q=https://accounts.craigslist.org/login/onetime?key%3D261387990NfiytN5VQh2eLOLleGYUWfBMcifkcB&source=gmail&ust=1729968547133000&usg=AOvVaw3_yyVaSCdx1sO-ljCNhyqG	Chrome
6	nottingham posting confirmation	https://post.craigslist.org/k/AiG4qRGH7xGvqu0rEJqiow/UQkbW	Samsung Internet Browser
7	nottingham preview	https://post.craigslist.org/k/AiG4qRGH7xGvqu0rEJqiow/UQkbW?s=preview	Samsung Internet Browser
8	nottingham add map	https://post.craigslist.org/k/AiG4qRGH7xGvqu0rEJqiow/UQkbW?s=geoverify	Samsung Internet Browser
9	nottingham posting details	https://post.craigslist.org/k/AiG4qRGH7xGvqu0rEJqiow/UQkbW?s=edit	Samsung Internet Browser
10	nottingham posting confirmation	https://post.craigslist.org/k/AiG4qRGH7xGvqu0rEJqiow/UQkbW	Samsung Internet Browser
11	nottingham manage posting	https://post.craigslist.org/manage/7775948717	Samsung Internet Browser
12	nottingham manage posting	https://post.craigslist.org/k/mJxS_hCH7xGn_0SdVU7CyA/GB3X3	Samsung Internet Browser
13	nottingham posting details	https://post.craigslist.org/k/mJxS_hCH7xGn_0SdVU7CyA/GB3X3?s=edit	Samsung Internet Browser
14	nottingham manage posting	https://post.craigslist.org/k/mJxS_hCH7xGn_0SdVU7CyA/GB3X3	Samsung Internet Browser
15	craigslist account	https://accounts.craigslist.org/login/onetime?key=260005686fIKCKc4Nnt7yYb6lF12x1qfCdJcdBH	Samsung Internet Browser
16	craigslist account	https://www.google.com/url?q=https://accounts.craigslist.org/login/onetime?key%3D260005686fIKCKc4Nnt7yYb6lF12x1qfCdJcdBH&source=gmail&ust=1728655631669000&usg=AOvVaw3YFdL6-qwZ3_SHscGrwc3j	Samsung Internet Browser
17	craigslist account	https://accounts.craigslist.org/login/home	Samsung Internet Browser
18	nottingham for sale "polish wooden plate" craigslist	https://nottingham.craigslist.org/search/sss?query=polish%20wooden%20plate#search=1~grid~0~0	Samsung Internet Browser
19	nottingham for sale "polish wooden plate" craigslist	https://nottingham.craigslist.org/search/sss?query=polish%20wooden%20plate#search=1~grid~0~0	Samsung Internet Browser

20	nottingham for sale "polish wooden plate" craigslist	https://nottingham.craigslist.org/search/sss?query=polish%20wooden%20plate	Samsung Internet Browser
21	nottingham for sale "polish wooden plate" craigslist	https://nottingham.craigslist.org/search/sss?query=polish%20wooden%20plate	Samsung Internet Browser
22	Nottingham posting confirmation	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?lang=en&cc=gb	Chrome
23	Nottingham preview	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?s=preview&lang=en&cc=gb	Chrome
24	Nottingham choose images	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?s=editimage&lang=en&cc=gb	Chrome
25	Nottingham add map	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?s=geoverify&lang=en&cc=gb	Chrome
26	Nottingham posting details	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?s=edit&lang=en&cc=gb	Chrome
27	Nottingham copy from previous	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?s=copyfromanother&lang=en&cc=gb	Chrome
28	Nottingham posting confirmation	https://post.craigslist.org/k/7AtgJcdb7xGbtmsoZU7CyA/dDR17?lang=en&cc=gb	Chrome
29	Nottingham copy from previous	https://post.craigslist.org/c/not?lang=en&cc=gb	Chrome
30	Nottingham choose images	https://post.craigslist.org/k/Zpx3zMZb7xGTrdFLvCKPvw/hmwMj?s=editimage&lang=en&cc=gb	Chrome
31	Nottingham add map	https://post.craigslist.org/k/Zpx3zMZb7xGTrdFLvCKPvw/hmwMj?s=geoverify&lang=en&cc=gb	Chrome
32	Nottingham posting details	https://post.craigslist.org/k/Zpx3zMZb7xGTrdFLvCKPvw/hmwMj?s=edit&lang=en&cc=gb	Chrome
33	Nottingham posting details	https://post.craigslist.org/k/Zpx3zMZb7xGTrdFLvCKPvw/hmwMj?s=edit&lang=en&cc=gb	Chrome

34	Nottingham copy from previous	https://post.craigslist.org/k/Zpx3zMZb7xGTrdFLvCKPvw/hmwMj?s=copyfromanother&lang=en&cc=gb	Chrome
35	Nottingham copy from previous	https://post.craigslist.org/k/Zpx3zMZb7xGTrdFLvCKPvw/hmwMj?lang=en&cc=gb	Chrome
36	Nottingham copy from previous	https://post.craigslist.org/c/not?lang=en&cc=gb	Chrome
37	Nottingham posting confirmation	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?lang=en&cc=gb	Chrome
38	Nottingham preview	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?s=preview&lang=en&cc=gb	Chrome
39	Nottingham choose images	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?s=editimage&lang=en&cc=gb	Chrome
40	Nottingham add map	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?s=geoverify&lang=en&cc=gb	Chrome
41	Nottingham posting details	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?s=edit&lang=en&cc=gb	Chrome
42	Nottingham choose category	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?s=cat&lang=en&cc=gb	Chrome
43	Nottingham choose type	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?s=type&lang=en&cc=gb	Chrome
44	Nottingham posting confirmation	https://post.craigslist.org/k/MjgTecZb7xG3vtUghlruOA/z4nlX?lang=en&cc=gb	Chrome
45	Nottingham copy from previous	https://post.craigslist.org/c/not?lang=en&cc=gb	Chrome
46	nottingham add map	https://post.craigslist.org/k/GDayv8Vb7xGgOgj2fFIjLA/JFDRR?s=geoverify	Samsung Internet Browser
47	nottingham posting details	https://post.craigslist.org/k/GDayv8Vb7xGgOgj2fFIjLA/JFDRR?s=edit	Samsung Internet Browser
48	nottingham choose category	https://post.craigslist.org/k/GDayv8Vb7xGgOgj2fFIjLA/JFDRR?s=cat	Samsung Internet Browser
49	nottingham choose type	https://post.craigslist.org/k/GDayv8Vb7xGgOgj2fFIjLA/JFDRR?s=type	Samsung Internet Browser

50	**nottingham choose type**	**https://post.craigslist.org/k/GDayv8Vb7xGgOgj2fFIjLA/JFDRR**	**Samsung Internet Browser**
51	**nottingham choose type**	**https://post.craigslist.org/c/not**	**Samsung Internet Browser**
52	**craigslist account**	**https://accounts.craigslist.org/login/home**	**Samsung Internet Browser**

Relevance:

The inquiry into the dubious Craigslist advertisement concerning the sale of an artwork has uncovered substantial browser history data from the confiscated phone. The gathered data comprises multiple visits to Craigslist, with URLs reflecting diverse advertisements and confirmations pertaining to the painting's sale. The browsing history indicates the utilization of both Chrome and Samsung Internet Browser, implying that the user actively curated and modified postings during various sessions. This information is essential since it delineates a behavioral pattern and furnishes evidence of the user's intention to sell the picture. The frequent engagement with Craigslist ads may suggest efforts to obscure or alter the listing, potentially pertinent to assessing any legal violations. The existence of numerous URLs associated with posting confirmations and revisions indicates collaborators or additional measures undertaken to promote the transaction. This information will assist in detecting illicit activity and comprehending the user's intentions and techniques.

3.2.8 CSS Cache

Evidence:

#	Name	Path	MD5	Size (bytes)	Source file	Additional file info	Deleted

1	craigslist.css	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/cache/Cache/Cache_Data/cabf3a92c2f8ce5d_0/craigslist.css	40dbbfe9ab6c73d53432f6228088e63b	5312	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/cache/Cache/Cache_Data/cabf3a92c2f8ce5d_0 : 0x0 (Size: 5928 bytes)		1

Relevance:

Craigslist.css is vital to the investigation. The browser cache (com.sec.android.app.sbrowser) shows Craigslist was accessed during web browsing. The file name mentions Craigslist, where the suspicious behavior was reported, increasing its connection to the investigation. This CSS file may reveal Craigslist sites or elements accessed, providing clues or metadata for the inquiry. This file can also establish a timeline of Craigslist access, which can be used with other data to build a complete picture of the suspect's online actions. This file and additional data can support the assertion that Craigslist was used for criminal activities. The file's path and MD5 hash must be specified to validate its legitimacy. Analysis of the file may reveal unique identifiers or timestamps that enhance the inquiry.

3.2.9 Searched Items

Evidence:

#	Timestamp	Source	Value	Origin	Service Identifier
1	10/10/2024 15:04:43	Samsung Internet Browser	craigslist nottingham	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History: 0xEC01 (Size: 229376 bytes)	Deleted Account

2	10/10/2024 15:04:41	Samsung Internet Browser	craigslist nottingham	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History: 0xEC29 (Size: 229376 bytes)	Deleted Account
3	10/10/2024 15:04:39	Samsung Internet Browser	craigslist	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History: 0xEC4E (Size: 229376 bytes)	Deleted Account
4	10/10/2024 15:04:32	Samsung Internet Browser	craigslist#sbfbu=1	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History: 0xEC72 (Size: 229376 bytes)	Deleted Account
5	10/10/2024 15:04:26	Samsung Internet Browser	craigslist#sbfbu=1	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History: 0xEC97 (Size: 229376 bytes)	Deleted Account
6	10/10/2024 15:04:21	Samsung Internet Browser	craigslist	USERDATA (ExtX)/Root/data/com.sec.android.app.sbrowser/app_sbrowser/Default/History: 0xECBC (Size: 229376 bytes)	Deleted Account

Relevance:

The recurrent enquiries for "craigslist nottingham" and "craigslist" indicate a specific intention to either post or seek things in the Nottingham region. This behavioral pattern is essential for determining the user's activities and interests at the time of the dubious post. The proximate timestamps (all occurring within seconds of one another) suggest a concerted attempt to access Craigslist. This may indicate urgency or a particular objective, such as publishing or altering a listing, which corresponds with the investigation's emphasis on the sale of a painting. The reference to "Deleted Account" in the service identification implies that the user may have sought to eliminate evidence of their activity. This is noteworthy as it may suggest an acknowledgement of misconduct or an effort to conceal potentially incriminating behavior. The queries for "craigslist#sbfbu=1" may signify particular features or segments within Craigslist that are being utilized, potentially aiding in the comprehension of the user's behaviors and motives.

3.2.10 Document from Memory Stick

Evidence:

Artist Name	Nationality	Relevance to Investigation
Gerhard Richter	**German**	**The reference to Gerhard Richter, a renowned abstract artist, may suggest the suspect's interest in high-value art, connected to the selling of valuable or counterfeit paintings.**
Bridget Riley	**British**	**The presence of Bridget Riley indicates the suspect's familiarity with notable abstract artists, which could be pertinent if the artwork in issue is said to be by a renowned artist.**
Damien Hirst	**British**	**Damien Hirst is renowned for his valuable artwork. The suspect's mention of Hirst may suggest an endeavor to sell or forge valuable artworks.**
Sam Gilliam	**American**	**The reference to Sam Gilliam, a distinguished abstract artist, substantiates the hypothesis that the suspect is engaged in the art market, handling valuable or counterfeit artworks.**
Brice Marden	**American**	**The presence of Brice Marden suggests the suspect's acquaintance with high-value abstract art, potentially pertinent to the investigation of art sales.**
Christopher Wool	**American**	**Christopher Wool is recognized for his abstract creations. The suspect's mention of Wool may imply participation in the sale or forgery of valuable artworks.**

Relevance:

The document enumerates some renowned contemporary abstract artists, suggesting the suspect's knowledge of valuable art. This is pertinent to the investigation since it indicates that the suspect may be engaged in the sale or forgery of valuable artworks. The presence of renowned artists such as Gerhard Richter, Bridget Riley, Damien Hirst, Sam Gilliam, Brice Marden, and Christopher Wool suggests that the suspect possesses familiarity with the art market, which may be pertinent if the painting in question is purported to be by one of these artists or if the suspect is endeavoring to sell counterfeit art attributed to them.

This information aids the investigation's objective of comprehending the suspect's actions and possible intentions about art sales.

3.3 Legal Implications

The evidence obtained from the phone and memory stick suggests potential violations of multiple laws. The suspect's participation in the sale of a painting under deceptive circumstances may constitute fraud, contravening Section 2 of the Fraud Act 2006 in the UK, which addresses fraud by false representation. Furthermore, if the suspect used another individual's identity or personal information without permission, this may amount to identity theft, infringing the Identity Documents Act 2010. The sale of stolen or counterfeit goods would violate intellectual property legislation, particularly the Copyright, Designs and Patents Act 1988. The illicit utilization of personal data without consent may violate the Data Protection Act 2018, which enforces GDPR. The utilization of steganography tools such as PixelKnot for information concealment may be perceived as an endeavor to obscure illicit activity, potentially infringing the Computer Misuse Act 1990.

Law	Relevant Section	Details
Fraud Act 2006 (UK)	**Section 2 - Fraud by false representation**	**The suspect's participation in the sale of a painting under deceptive circumstances may constitute fraud. This is creating a deceptive assertion with the purpose of securing an advantage for oneself or another, or inflicting a detriment onto another, or subjecting another to a potential loss.**
Identity Documents Act 2010 (UK)	**Various sections**	**If the suspect used another individual's identity or personal information without authorization, this may amount to identity theft. This encompasses the illicit possession or utilization of identity documents.**
Copyright, Designs and Patents Act 1988 (UK)	**Various sections**	**The selling of stolen or counterfeit goods would violate intellectual property legislation. This legislation safeguards against the illicit utilization of copyrighted content.**
Data Protection Act 2018 (UK)	**Various sections implementing GDPR**	**The illicit utilization of personal data without consent may violate data protection legislation. This encompasses the illicit handling of personal data and the inability to safeguard personal data from unauthorized access.**

Computer Misuse Act 1990 (UK)	**Various sections**	**Using steganography tools such as PixelKnot for information concealment may be seen as obscuring illicit activity. This legislation addresses unauthorized access to computer resources and unauthorized actions aimed at disrupting computer functionality.**

3.4 Motive and Collaborators

The evidence indicates other motives for the suspect's behavior. The suspect's communications regarding financial necessity and a recent job loss referenced in an email to Pret a Manger suggest that financial gain is a principal motive. The utilization of PixelKnot to embed information into photographs implies an effort to obscure illicit activity, signifying an intention to evade detection. The regular correspondence with another individual (tombiddle029@gmail.com) regarding a "money-making idea" and the utilization of steganography tools indicate that the suspect may be involved in a broader conspiracy. This collaborator offered guidance on utilizing PixelKnot and elaborated on the strategy, signifying a strong partnership and synchronized efforts to execute the tasks.

4. Discussion

4.1 Interpretation of Findings

The data obtained from the suspect's phone and memory stick offers a thorough insight into their behavior and possible legal infractions. The communications suggest that the suspect was engaged in the sale of items on Craigslist, including a painting. The dialogues indicate a financial incentive, as the suspect articulated a necessity for funds and deliberated on a "profit-generating concept" with an associate. The utilization of PixelKnot for embedding information into photographs implies an effort to obscure illicit operations, reflecting a degree of sophistication and a deliberate intention to evade detection.

The browser history and autofill data indicate a pattern of behavior associated with placing and maintaining advertisements on Craigslist, so reinforcing the suspect's engagement in online transactions. The cookies and cached data corroborate the suspect's regular access to Craigslist, associating their email address with the account utilized for placing advertisements. The installed software, especially PixelKnot, underscores the suspect's utilization of steganography tools for concealing information, aligning with the email evidence.

The information indicates multiple possible legal infractions, including fraud, identity theft, intellectual property theft, data protection breaches, and computer misuse. The suspect's behavior indicates a calculated attempt to perpetrate fraud, obscure their conduct, and possibly conspire with others in a broader conspiracy.

4.2 Recommendations

Identify and examine the individual associated with the email tombiddle029@gmail.com, as they are actively engaged in the plan. This entails examining their digital trace and conversations to identify their role and any potential accomplices. Initiate legal proceedings against the suspect for possible infringements of the Fraud Act 2006, Identity Documents Act 2010, Copyright, Designs and Patents Act 1988, Data Protection Act 2018, and Computer Misuse Act 1990, as supported by the evidence. Establish surveillance of the suspect's online conduct, especially on platforms such as Craigslist, to identify any current or potential fraudulent actions. Enhance IT security protocols within the organization to avert analogous incidents in the future. This entails the establishment of stringent data protection policies, periodic audits, and employee education on cybersecurity best practices.

5. Conclusion

5.1 Key Findings and Their Significance

The inquiry into the suspect's actions uncovered other significant discoveries. The suspect was engaged in selling items on Craigslist, including a painting, under perhaps deceptive circumstances. The correspondence revealed a financial incentive since the suspect articulated a necessity for funds and deliberated a "money-making concept" with an associate. The utilization of PixelKnot to embed information into photos implies an effort to obscure illicit acts, reflecting a degree of skill and a deliberate intention to evade detection.

The browser history, autofill data, cookies, and cached files corroborated the suspect's regular access to Craigslist and associated their email address with the account utilized for posting advertisements. The installed software, notably PixelKnot, indicated the suspect's utilization of steganography tools for concealing information, aligning with the email evidence. The evidence indicated multiple possible legal infractions, including fraud, identity theft, intellectual property theft, data protection breaches, and computer misuse.

These findings are substantial as they offer an extensive overview of the suspect's actions and possible legal infractions. Their acts underscore the suspect's intentional participation in fraudulent activities, efforts to obscure their conduct, and possible collaboration with others in a broader conspiracy. The gathered evidence substantiates the necessity for additional inquiry and legal measures to address the suspect's conduct and avoid future occurrences.

5.2 Reflection on the Effectiveness of the Methodologies Used

The methodologies employed in this investigation were highly effective in revealing the suspect's activity and any legal infractions. The application of Cellebrite Physical Analyser for data gathering and analysis guaranteed the preservation of all pertinent data in its original state and subjected it to comprehensive examination. The sequential methodology of data collecting, preservation, and rigorous examination offered a systematic framework for the investigation, guaranteeing comprehensive evidence collection and analysis.

The amalgamation of technical and business priorities in the analytical processes guaranteed that the results were both technically robust and congruent with legal and

organizational goals. The application of sophisticated forensic technologies and methodologies, including steganography analysis via PixelKnot, facilitated the identification of hidden information, which was essential for comprehending the suspect's actions and intentions.

The employed procedures were effective in fulfilling the investigation's objectives, yielding reliable and legally admissible evidence that underpins further actions and enquiries. The systematic methodology, along with advanced forensic instruments, facilitated a meticulous and exhaustive examination, underscoring the need to adhere to best practices in computer forensics.

6. References

1. **Fraud Act 2006 (UK)**
    a. **Legislation.gov.uk, 2006. *Fraud Act 2006*. [online] Available at: https://www.legislation.gov.uk/ukpga/2006/35/contents [Accessed 7 January 2025].**
2. **Identity Documents Act 2010 (UK)**
    a. **Legislation.gov.uk, 2010. *Identity Documents Act 2010*. [online] Available at: https://www.legislation.gov.uk/ukpga/2010/40/contents [Accessed 7 January 2025].**
3. **Copyright, Designs and Patents Act 1988 (UK)**
    a. **Legislation.gov.uk, 1988. *Copyright, Designs and Patents Act 1988*. [online] Available at: https://www.legislation.gov.uk/ukpga/1988/48/contents [Accessed 7 January 2025].**
4. **Data Protection Act 2018 (UK)**
    a. **Legislation.gov.uk, 2018. *Data Protection Act 2018*. [online] Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents [Accessed 7 January 2025].**
5. **Computer Misuse Act 1990 (UK)**
    a. **Legislation.gov.uk, 1990. *Computer Misuse Act 1990*. [online] Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 7 January 2025].**
6. **Supreme Court of the United States, 2023.**
    a. Brief of Craigslist, Inc. as Amicus Curiae in Support of Respondent. Available at: https://www.supremecourt.gov/DocketPDF/21/21-1333/252677/20230119145528517_21-1333_CRAIGSLIST%20INC.%20Amicus%20Brief.pdf [Accessed 5 January 2025].