

COMPUTER FORENSICS – SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

by Chris Thomas

Submission date: 27-Apr-2023 11:07AM (UTC+0100)

Submission ID: 203641212

File name: 37652_Chris_Thomas_COMPUTER_FORENSICS_-
_SYNTHESIZE_A_SOLUTION_TO_A_POTENTIAL_REAL-LIFE_SCENARIO_497079_494053618.docx (9.6M)

Word count: 5114

Character count: 31734

COMPUTER FORENSICS – SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

Christopher John Thomas

Student University of Wales Trinity St David, Swansea, Wales

1252344@student.uwtsd.ac.uk

Abstract-

For this report, the author has been asked to compare and contrast some forensic tools.

What is the best tool to use? Is there a clear winner, or do all tools have a specific niche? Much research has taken place, and there is no clear winner, whether it is an open-source application or a commercial product, not one glove fits all.

I. Task 1 Research

Introduction

Computer Forensics is the most commonly known name for what is now called Digital Forensics. The first known department was created in 1984 by the Federal Bureau of Investigation (FBI) known as CART (Computer Analysis and Response Team), and a short time later the Metropolitan Police had then also setup similar unit called the Fraud Squad, but it wasn't until the later part of 1990s that standardization was needed. In 1994 and 1995 the creation of the modern British digital forensics' methodology was formed and in 1998 the first version of the 'Good Practice Guide for Digital Evidence' was released. [1]

The Field of digital forensics is underpinned by three principles: (1) Collection, (2) Analysis, (3) Presentation. In the upcoming sections further, explanation and clarification on the distinct functions of each principle and how they rely on each other will be provided.

Quality Management System (QMS)

The Forensic Science Regulators Code of Practice March 2023 states there is a need to have an effective quality management system in place (QMS). A QMS system provides the researcher a framework to produce results that would be reliable, consistent and easy to understand and that meet the requirements of the internationally recognised QMS standards ISO/IEC 17025:2017 & ILAC-G19:06/2022. [2]

The code of practice follows from the QMS requirements and states that any forensic science activity is met with impartiality, independence and integrity; what this means is for the forensic analyst is that;

- No vested interest in the case that they are working on.
- That they remain independent, with no relationship with any parties involved in the case.
- Being asked to leave information out of a case that could support either party in the case.
- Being compelled to provide false data by a third party.

QMSs provide a framework that has been designed so that a forensic process can be carried out consistently and reliably. As with any other QMS systems, there has to be involvement of policies, procedures and

quality control with training and development and documentation control at the forefront. If these steps are not implemented, then, for example;

- Lower or no reliability
- No constancy
- Lack of credibility
- Reduced potential for risk management
- Potential for reputational damage

With these implemented, the forensic work would enhance credibility, consistency and reliability.[3]

Documentation Control

Documentation control is the process of managing and maintaining the documents e.g. defined processes and procedures and supporting records of all activities taking place during a forensic investigation. Its purpose is to ensure the integrity, accuracy and reliability of the evidence that has been collected, as well as authorisation and control of the actual processes and procedures that are involved.

The information that will need to be taken must include detailed notes, photographs, and any videos that may have been recorded, by following the correct process will create an audit trail which will allow another examiner to follow in 'the footsteps' of how the previous investigation steps.

Furthermore, confidentiality and document control are critical factors in a forensic environment. The business tasked with forensically analysing an item must ensure they have and follow all the documented policies and that all members of staff adhere to them, and that regular training is provided.

Robust documentation control is needed to ensure that all evidence that has been collected during the examination is

admissible in a court setting, and it's to ensure that the integrity of the investigative process.[2]

Chain of Custody

Chain of Custody in a computer forensic setting is an act of documenting, maintaining the history of evidence, this process starts from its discovery right through to when it is presented in court. The initial process starts when the device that has been seized and then transported and then stored and at each step it is kept secure to preserve the integrity of the evidence. Chain of custody is critical this is to ensure that the admissibility and the integrity of the evidence is usable in the court of law, by following the set processes and documenting each step the forensic expert takes they can then establish the authenticity of the evidence that they have gathered. [4]

Identification and Seizure.

This is the initial step of the process, it is where the identification and then subsequent seizure of an electronic device or media that may contain potential evidence. This has to be done in such a way that preserves the evidence and prevents loss of data, damage etc. From the point of seizure information such as: [4]

- Time & date.
- Location.
- Individuals involved I.E names etc.
- Items taken.

Transportation and Storage.

Once the item has been seized, it will then need to be transported and stored in a secure environment this needs to be done to prevent any form of evidence tampering and any unauthorized tampering. As with the identification procedure document control is also followed. [4]

Analysis.

Once the forensic team begin the examination of the device/s the need to identify the relevant information, to do this they employ a number of techniques and use a range of tools to accomplish the task.

Some methods that are used to recover information:

- **Data Carving**

Data carving is a process in which a forensic expert identifies and extracts specific data from a dataset. [5]

- **Keyword Searching**

Keyword searching is a method in which the expert searches for keywords in the collected data, this can help the investigators to quickly search for key terms and ignore irrelevant data quickly.[6]

- **Timeline Analysis**

Timeline analysis is a technique that is used during the analysis stage, and it creates a chronological timeline of events to help identify when specific actions have occurred. [7]

The information that is held on a device or media is then analysed to identify relevant evidence again as while following the previous step's documentation control.[4]

Presentation in a court setting.

The evidence that has been gathered during the forensic examination is then presented in court with all the relevant documentation to provide authenticity and of course reliability. [4]

In the forthcoming section we compare and discuss three forensic software platforms, their pros and cons and how they would hold up in a legal setting.

A brief overview of the steps in forensic investigations has been explained, the following section will compare and contrast the roles of Forensic Tool Kit (FTK), Forensic Disk Controllers, Wireshark and The Sleuth kit in facilitating the execution of a task in a forensic environment.

1. Forensic Toolkit (FTK)

Exterro is the owner and distributor of the Forensic Toolkit (FTK); FTK is a digital forensic platform that allows a deep forensic analysis of a device. FTK is world-renowned as the most used digital forensic software in court proceedings worldwide. [8]

- FTK Imager
- FTK Enterprise
- FTK Central
- The Original FTK
- FTK Lab
- FTK Connect

FTK Imager

FTK Imager is a tool that has the ability to perfectly clone a target drive such as a hard disk drive, USB drive and even a mobile device, the reason you would want to clone the device is to keep the original evidence intact so that no party has the ability to say that the "original" evidence has been compromised.

FTK Enterprise

FTK Enterprise is the only forensically capable tool that allows use of parallelization, which uses all of the cores of a Central Processing Unit (CPU) to process the data. [9]

- **Multi-Threading**

Multi-Threading (MT) allows the division of work for example FTK Imager software cloning the target device utilises every core of the (CPU) allowing for a quicker run

times in its programme. Below is an image of multiple threads being used and being broken down to be processed by the CPU. [10]

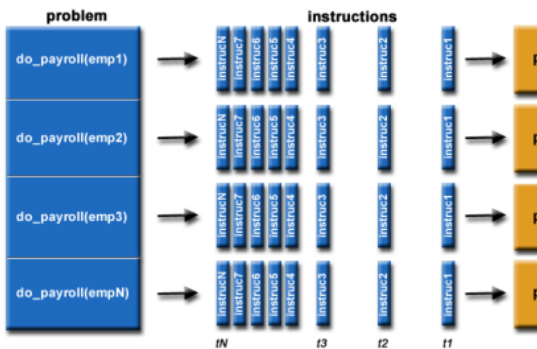


Figure 1 Data Parallelism Diagram

FTK Enterprise allows the forensic team live interaction with the target device, this package is more aimed at the business level, HR investigations, post security incidents and at all times making sure that the chain of custody is kept at all times.[11]

2. Forensic Disk Controllers

Forensic disc controllers are also known as Write blockers; they are hardware and can also be a software program. They can lock a drive such as discs, USB drives and hard drives; by doing this, the forensic collector can ensure that the data on that device will remain intact and prevent data loss and manipulation.

The National Institute of Standards and Technology (NIST) requirements for hardware and software write blockers state that:

- Protected drives cannot be changed.
- The Write blocker cannot prevent the collection of data

Software Write Blocker (SWB) Tools have a strict set of rules that they must follow to ensure that all information on the target device is forensically sound.

SWB tools use a Bios interrupt called INT 0x13; without this Bios call, the disk drives would be inaccessible; SWBs intercept the original 0x13 call and replace it with an altered version of the interrupt. The replaced interrupt will allow or deny an application or device to read/write to the target disk. [12]

SWBs need to meet a strict set of requirements, these are:

- The software tool is required to block all commands to the protected drive if it is in the write mode.
- The software tool is required to block all commands to the protected drive if it is in the read mode.
- The software needs to alert the protection status of all drives that it covers.
- The software needs to be able to report back any commands that have been blocked, if it is configured to do so. [13]

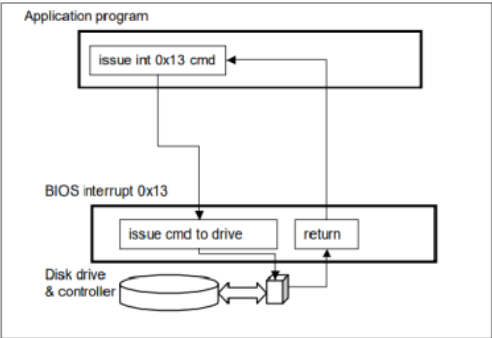


Figure 2 Drive access via 0x13 Bios [13]

3. Wireshark

Wireshark is a very versatile tool, that has the ability to run on multiple operating systems such as Windows, Linux and MacOS. This software is used by a multitude of professionals such as Network Engineers, security personnel. With forensic tool kits such as FTK and Sleuth kit that forensically inspect hard drives and other devices, Wireshark is a different kind of forensic tool, this tool does not inspect

hardware and recover its data. Wireshark is a network analysing tool. [14]

Wireshark inspects packets it does this by utilising what is called a ‘Capture Driver’ called WinPcap what this driver does is act as a ‘go between’ between the Operating System and Wireshark to capture the packets from the Network Interface card (NIC). [15]

The most common protocols that you will see while using Wireshark are:

- Address Resolution Protocol (ARP).
- Dynamic Host Configuration Protocol (DHCP).
- Transmission Control Protocol/Internet Protocol (TCP/IP).
- SYN Packets.

ARP

ARP is a protocol that is able to translate IP addresses (Layer 3) into Media Access Control (MAC) addresses (Layer 2). ARP works by sending two packets a “Who has” and a “Reply”, PC1 (192.168.1.1) wants to send data to PC3(192.168.1.4), PC1 does not know where to send the data with the help from a switch or a router the ARP protocol locates PC3, PC1 will sent a “Who has ARP packet – Who has 192.168.1.4 IP address” and the switch receives this packet and it is able to check it’s ARP table to see who has 192.168.1.4 and reply to say (with MAC address of PC3) to say it’s thought port X. [16]

DHCP

DHCP is a protocol that hands out IP addresses and network related information such as NTP, Subnet, Gateway details. [17]

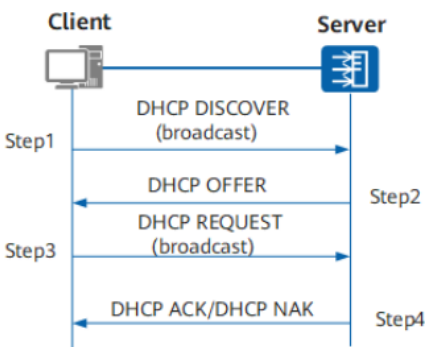


Figure 2 Client asking for an IP (DHCP Request) [17]

4. The Sleuth Kit

Just like FTK, there are opensource projects one such project is Sleuth Kit. Sleuth Kit has two parts;

- Autopsy
- The Sleuth Kit

a) Autopsy

Autopsy is much like any other forensic recovery tool except for one major difference it is an open source project, updates and version changes and plugins are now written by Basis Technology but was the responsibility of one developer named Brian Carrier with testing and debugging being completed by users.

Autopsy’s feature list is very extensive [18]

Here are some analysis features that Autopsy has:

- Multi-User cases – This is to allow forensics teams to collaborate on large scale projects.
- Registry Analysis – This uses a specific plugging to access recently close/active documents.
- File Type sorting – This function groups images, files and documents together.
- Media Playback – Allows for viewing of media files.
- Thumbnail viewer – Allows the viewing of images.

- A Robust File System Analysis – Allows for support of the most common file systems in use.
- Android Support – Allows for the extraction of data from Android devices. [19]

b) The Sleuth Kit

The Sleuth Kit (TSK) is a collection of tools that run at the command line level that will allow the examiner to investigate the file system and the volume system of the target device.

Some tools which are part of TSK;

- The Mactime tool – Allows for the creation of a timeline based on the FLS tool. [20]
- The FLS Tool - Lists all the files and directories in the file system, it will then process the directory and can display the information on deleted items. [21]
- The ICAT tool – Outputs the contents of the recovered file in a disk image. [22]

A) Conclusion

The digital forensic tools discussed within this report are all specialised tools, they all have different purposes and capabilities.

FTK is a software program used in digital forensics to retrieve evidence from various file systems. This commercial tool has advanced features, including integrated case management, the ability to utilise parallelism, data visualisation, advanced search capabilities, and a user-friendly graphical interface.

In contrast, TSK is a collection of open-source command-line tools for file system analysis, disk imaging, keyword searching, and data carving. Its versatility, reliability, and open-source nature have made it popular among digital forensics experts.

Wireshark is a network protocol analyser that lets users capture and analyse network traffic in real-time, commonly used by network administrators and security professionals for network troubleshooting and security.

Forensic disk controllers are specialised hardware devices that allow the creation of bit-by-bit copies of storage devices, such as hard drives and USB drives while ensuring the original data is protected and not altered. These devices ensure the original data is preserved and unaltered, providing a reliable and forensically sound way to acquire digital evidence.

As its stated in this report, there are different strengths and different weaknesses for each product, FTK has the ability to use parallelism where as The Sleuth Kit does not. But allowing parallelism you are giving the forensic recovery the ability to complete its tasks quicker due to the software having more resources available. What would be advantageous is the ability of other programs such as TSK to have the ability to use parallelism.

References

- [1] (). *Digital forensics*. Available: <https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2>.
- [2] (). *The forensic Science Regulators Code of Practice*. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1141863/FINAL_Code_of_Practice.pdf [Accessed 23.03. 2023].
- [3] Dr Rebecca Nix, "Quality Management Systems," 10/04, 10/04.
- [4] Assoc. Professor Carlene Campbell, "DIGITAL FORENSICS INVESTIGATION PHASES - Lecture 3 ," pp. 2-26, .
- [5] V. Roussev, *Digital Forensic Science : Issues, Methods, and Challenges*, San Rafael, California: Morgan & Claypool Publishers, 2017. DOI: 10.2200/S00738ED1V01Y201610SPT019 .
- [6] D. Paul Joseph and P. Viswanathan, "SDOT: Secure Hash, Semantic Keyword Extraction, and Dynamic Operator Pattern-Based Three-Tier Forensic Classification Framework," *IEEE Access*, vol. 11, pp. 3291-3306, 2023. . DOI: 10.1109/ACCESS.2023.3234434.
- [7] B. Inglot and L. Liu, "Enhanced Timeline Analysis for Digital Forensic Investigations," *Information Security Journal.*, vol. 23, (1-2), pp. 32-44, 2014. . DOI: 10.1080/19393555.2014.897401.
- [8] Exterro, "FTK® Suite Version 7.6 Product Brief ," pp. 2, 2021.
- [9] (). *FTK® Imager*. Available: [https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,\(FTK%C2%AE\)%20is%20warranted](https://www.exterro.com/ftk-imager#:~:text=FTK%C2%AE%20Imager%20is%20a,(FTK%C2%AE)%20is%20warranted). [Accessed 27/03/ 2023].
- [10] (). *What Is Hyper-Threading?*. Available: <https://www.intel.co.uk/content/www/uk/en/gaming/resources/hyper-threading.html> [Accessed 27/03/ 2023].
- [11] (). *exterro*. Available: <https://www.exterro.com/ftk-enterprise> [Accessed 27/03/ 2023].
- [12] James R. Lyle and Paul E. Black, "Testing BIOS Interrupt 0x13 Based Software Write Blockers," 2005. Available: https://hissa.nist.gov/~black/Papers/testSWB_ECCE05.pdf.
- [13] Nist, "Software Write Block Tool Specification & Test Plan ," pp. 1-7, 2003. Available: https://www.nist.gov/system/files/documents/2017/05/09/swb-stp-v3_1a.pdf.
- [14] G. Jain and Anubha, "Application of SNORT and Wireshark in Network Traffic Analysis," *IOP Conference Series.Materials Science and Engineering*, vol. 1119, (1), pp. 12007, 2021. . DOI: 10.1088/1757-899X/1119/1/012007.
- [15] C. Sanders, *Practical Packet Analysis*, 3rd Edition, .
- [16] C. Sanders, "Address resolution protocol," in *Practical Packet Analysis* Anonymous 2007, pp. 62.
- [17] (-12-20). *How a DHCP Server Allocates Network Parameters to New DHCP Clients*. Available: <https://support.huawei.com/enterprise/en/doc/EDOC1100195158/bb57bdaa/how-dhcp-works> [Accessed 04/04/ 2023].
- [18] (). *History*. Available: <https://www.sleuthkit.org/about.php> [Accessed 06/04/ 2023].

[19] (). *Analysis Features*. Available:
<https://www.sleuthkit.org/autopsy/features.php> [Accessed 06/04/ 2023].

[20] (). *Mactime*. Available:
<https://wiki.sleuthkit.org/index.php?title=Mactime> [Accessed 10/04/ 2023].

[21] (). *FLS Tool*. Available:
<https://wiki.sleuthkit.org/index.php?title=FLS> [Accessed 10/04/ 2023].

[22] (). *Icat*. Available:
<https://wiki.sleuthkit.org/index.php?title=Icat> [Accessed 10/04/ 2023].

II. Task Two – Case study: Sabotage

Professional Forensic Report

Digital Forensic Investigation Report.

Case Number: 123789.

Investigation Date: March 27, 2023 - April 27, 2023.

Investigator: Barry Lynch, Computer Hacking Forensic Investigator (CHFI).

Overview

On 27th April 2023, Ms Dee Rod of CEC Ltd contacted Barry Lynch from Mentor Forensics. CEC senior management was notified that a former employee Rob Jengelly had deleted millions of pounds worth of designs for a Graphical Interface (GUI) for a mobile phone (Samsung Galaxy S20 Plus).

Objectives

Mentor Forensics has been tasked to generate a report detailing the steps taken to analyse the evidence that CEC Ltd has provided with the potential for usage in a criminal proceeding.

Evidence Analysed

CEC Ltd has shown the Mentor Forensics team the location of the device, and Mentor Forensics has been to the site to collect the machine to be investigated. The Device specifications are as follows:

- Desktop Tower Brand ICON
- Computer Name: SC-IQ205-08
- It has an Intel® Core™ i7-7700 CPU @3.60GHz
- Western Digital 2TerraByte Hard Drive.
- Device ID: 9E687286-B544-4423-BF95-13C48C8FE9D4
- Product ID: 00329-00000-00003-AA222
- Operating System – Windows 10 Version 21H2

Mentor Forensics has used the appropriate techniques and procedures to make a forensically sound bit-for-bit image of a CEC LTD-affected Hard disk drive (HDD). The bit-for-bit image was collected for PC name SC-IQ205-08; a Crucial X8 2 Terabyte Solid State drive was used to make the copy of the affected device HDD.

Investigation Steps

The investigation was conducted by Barry Lynch following the best practices of NIST in digital forensics, adhering to the industry-wide guidelines in the NIST publication 800-86, which can be found [Here](#). Mentor Forensics' approach to evidence collection is forensically sound.

Mentor began to investigate the device provided by CEC Ltd by obtaining a forensic image of Rob Jengelly's business-issued desktop computer's Hard Disk Drive using a write-blocking device. A thorough investigative analysis of the desktop was then performed using FTK 7.5.2.173 on Rob Jengelly's account.

During the investigation Mr Lynch method will focus on the recovery of the images that have been lost this process will filter and conduct keyword searches for images that have been lost this will identify quickly the lost material. As part of the NIST guidelines, a chain of custody record for all of the digital evidence collected during the investigation has been created, documenting the investigative process we have undertaken.

Findings

Our investigation revealed that Rob Jengelly had accessed and downloaded some confidential images from the company's server; we found evidence that Rob Jengelly had used a USB HDD to make copies of the images. During our analysis, we discovered that Rob Jengelly had deleted the images and many others. However, we recovered deleted files using the digital forensic tools mentioned in this report.

Several images were recovered from the device in question, but five images were explicitly requested to be recovered if possible; these have been highlighted in the attached report from FTK.

The Object ID for each image is as follows:

- 2453 – File name; Samsung S20 Plus look.jpg
- 2454 – File name; Samsung S20 Plus GUI Two.jpg
- 2455 – File name; Samsung S20 Plus GUI One.jpg
- 2456 – File name; Samsung S20 Plus GUI Four.jpg
- 2457 – File name; Samsung S20 Plus GUI Five.jpg

Based on the investigation, it is our opinion that Rob Jengelly, did in fact, steal confidential company data and attempt to sell it to a competitor. Our findings are supported by digital evidence that was collected using a sound forensic approach and analysed following the NIST best practices.

The recovered files have been saved onto a clean USB pen drive ready to be viewed, during the forensic image a number of other folders and images/files etc have been recovered and will be available upon request, all information will be held for a period of two years, NIST stipulates that there is no specific time frame to hold user data.

Recommendations

Mentor Forensics recommends that CEC Ltd take legal action against Rob Jengelly to recover the original images and to seek potential damages for the loss of potential income from their intellectual property. It is also a strong recommendation that CEC Ltd implements more robust security measures to prevent similar incidents from occurring in the future.

There are a few ways to prevent further incidents (1) to implement network segmentation to restrict sensitive data. (2) implement data loss prevention software such as Varonis to monitor and prevent unauthorised data transfers. (3) a group policy that will lock down access to USB Dis Drives. (4) Employee security awareness training.

Conclusion

This report has been prepared for CEC Ltd in accordance with best practices. It presents as an authentic and precise summary of Mentor Forensics investigation and its outcomes. If Mentor Forensics can be of further assistance please contact Barry Lynch.

Signed,



Barry Lynch, Computer Hacking Forensic Investigator, Mentor Forensics.

Appendix

Invoice

Mentor Forensics

INVOICE

12B Forensics House,
Forensics Way
Forensics.

INVOICE #177
DATE: 27/03/2023

TO:
CEC Mobile Manufacturing
11 Fabian Way
Swansea SA11TD
cecinfo@cecmobile.com

COMMENTS OR SPECIAL INSTRUCTIONS:
Priority - Full Data Analysis and recovery needed

SALESPERSON	P.O. NUMBER	REQUISITIONER	SHIPPED VIA	F.O.B. POINT	TERMS
Barry Lynch	123789	Dee Rod	N/A	Enter here	Due on receipt

QUANTITY	DESCRIPTION	UNIT PRICE	TOTAL
Quantity 1	Device Investigation	£250	£250
Quantity 1	Software – Clone of Device – To keep original evidence intact.	£1500	£1500
Quantity 1	Software – Analysis of recovered files	£750	£750
Quantity 1	Software – Report creation	£500	£500
		SUBTOTAL	£3000
		SALES TAX	20%
		SHIPPING & HANDLING	N/A
		TOTAL DUE	£3600

Make all checks payable to Mentor Forensics.
If you have any questions concerning this invoice, contact: Dave Smith at Phone or Barry.Lynch@mentor.com
THANK YOU FOR YOUR BUSINESS!

Comparison

Software Name	Mobile Data Processing	Multi-Thread/Multi-Core	Scalability	Windows Agent Indexing	Collaborative	File Decryption	Password Cracking and Recovery	Data preview	Remote collection	Email Analysis	File Type Sorting	Web Artifacts	File System Analysis	Full Disk Forensic Imaging	Network Analysis
FTK Suite	IOS/Android	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Autopsy/Sleuth Kit	Android Only	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Wireshark	N/A	No	Yes	No	No	No	Yes	Yes	Yes	No	No	No	No	No	Yes

Findings for CEC LTD	
Organization	Mentor Forensics
Author	Barry Lynch
Date	17/04/2023

Table Of Contents

Case Summary	15
Evidence List.....	15
All Bookmarks.....	15
Image 1.....	15
File Category (Bookmarks)	15
General	16
Documents.....	17
Graphics.....	21
test1.....	26
File Category (Bookmarks)	26
General	26
Graphics.....	27
Documents.....	33

Case Summary

Mon Apr 17 2023 09:32:41 (GMT Standard Time)

Evidence List

Display Name	: WDC WD10EZEX-00MFC A0 [1000 GB]
Evidence Path	\\.\PHYSICALDRIVE0
ID Number/Name	1
Evidence Type	Disk Image Folder
Time	14/04/2023 16:06:46
Size	1971.6 GB

All Bookmarks

Mon Apr 17 2023 09:32:56 (GMT Standard Time)

Image 1

File Category (Bookmarks)

File Category	Report Count	Case Count
📁 Folder	3	252788
XML	1	120729
Adobe Acrobat	1	64
* Index Allocation	1	34663
JPEG	4	5668
JPEG EXIF	1	1230
Unknown	26	518981
File Category	Report Count	Case Count
7 bit text	7	84522
* SQLITE Database	1	752
* Windows NT Registry	2	2194
* Windows Shortcut	8	1667
* OLE Archive	3	299
Bitmap	1	3367

GIF	1	1300
PNG	4	62524
Text	3	1707

General

Object Id	Name	Type	Size	CreatedDate	Export As
2146	Temp	Folder	672 Byte(s)	2022-0906T07:16:29.780106	ReportFiles\2146
2331	Report_Files	Folder	56 Byte(s)	2023-0414T14:33:40.54266	ReportFiles\2331
2451	CEC Ltd	Folder	56 Byte(s)	2023-0414T14:54:57.01757	ReportFiles\2451
2452	\$I30	Index Allocatio n	4 KB	2023-0414T14:54:57.01757	ReportFiles\2452
134222	ActivitiesCache.db	SQLITE Database	1 MB	2023-0414T11:19:27.868205	ReportFiles\134222.html
143322	UsrClass.dat	Windows NT Registry	3.5 MB	2023-0414T11:19:16.243269	ReportFiles\143322.dat
147057	NTUSER.DAT	Windows NT Registry	1.5 MB	2023-0414T11:19:14.821378	ReportFiles\147057.dat
Object Id	Name	Type	Size	CreatedDate	Export As
146194	Samsung S20 Plus GUI Two.Ink	Windows Shortcut	704 Byte(s)	2023-0414T14:52:12.768827	ReportFiles\146194.html
146195	Samsung S20 Plus look.Ink	Windows Shortcut	850 Byte(s)	2023-0414T14:47:33.583297	ReportFiles\146195.html
146196	Samsung S20 Plus GUI Four.Ink	Windows Shortcut	709 Byte(s)	2023-0414T14:54:11.861662	ReportFiles\146196.html

146197	Samsung S20 Plus GUI One.Ink	Windows Shortcut	704 Byte(s)	2023-0414T14:49:42.895031	ReportFiles\146197.html
146199	CEC Ltd.Ink	Windows Shortcut	564 Byte(s)	2023-0414T14:44:00.584927	ReportFiles\146199.html
146351	Images 2.Ink	Windows Shortcut	695 Byte(s)	2023-0414T14:44:41.131448	ReportFiles\146351.html
146352	Images 1.Ink	Windows Shortcut	695 Byte(s)	2023-0414T14:44:37.647149	ReportFiles\146352.html
146355	Samsung S20 Plus GUI Three.Ink	Windows Shortcut	881 Byte(s)	2023-0414T14:52:51.955931	ReportFiles\146355.html
146370	9b9cdc69c1c24e2b.automaticDestinations-ms	OLE Archive	6.5 KB	2023-0414T12:51:02.686065	ReportFiles\146370.automaticdestinations-ms
146371	12dc1ea8e34b5a6.automaticDestinations-ms	OLE Archive	8 KB	2023-0414T14:47:33.428487	ReportFiles\146371.automaticdestinations-ms
146374	f01b4d95cf55d32a.automaticDestinations-ms	OLE Archive	12 KB	2023-0414T11:20:04.63369	ReportFiles\146374.automaticdestinations-ms

Documents

Object Id	Name	Type	Size	CreatedDate	Export As
2147	Report.fo	XML	43.92 KB	2023-0414T14:33:42.214532	ReportFiles\2147.fo
2148	Report.pdf	Adobe Acrobat	45.66 KB	2023-0414T14:34:24.870721	ReportFiles\2148.tiff
13652	65331	Unknown	1.1 MB	2023-0414T14:57:20.73138	ReportFiles\13652.unknown
14142	64300	Unknown	0 Byte(s)	2023-0414T14:57:08.687426	ReportFiles\14142.unknown

24754	\$MFT	Unknown	1004 MB	2022-0909T00:32:26.731554	ReportFiles\24754.unknown
122541	ntuser.dat.LOG2	Unknown	429 KB	2023-0414T11:19:16.415301	ReportFiles\122541.log2
122542	ntuser.dat.LOG1	Unknown	472 KB	2023-0414T11:19:16.415301	ReportFiles\122542.log1
134221	ActivitiesCache.db-wal	Unknown	3.93 MB	2023-0414T11:19:28.884353	ReportFiles\134221.db-wal
143323	UsrClass.dat.LOG1	Unknown	1.01 MB	2023-0414T11:19:16.243269	ReportFiles\143323.log1
574802	\$UI0A89.jpg	Unknown	120 Byte(s)	2023-0414T14:48:01.708513	ReportFiles\574802.html
574803	\$IWYDC40.png	Unknown	114 Byte(s)	2023-0414T14:48:01.708513	ReportFiles\574803.html
574804	\$I1SDI37.jpg	Unknown	130 Byte(s)	2023-0414T14:48:01.708513	ReportFiles\574804.html
574805	\$IWHRXI.jpg	Unknown	116 Byte(s)	2023-0414T14:48:01.630457	ReportFiles\574805.html

Object Id	Name	Type	Size	CreatedDate	Export As
574806	\$IC5EDRR.jpg	Unknown	116 Byte(s)	2023-0414T14:48:01.630457	ReportFiles\574806.html
574808	\$IJ407U2	Unknown	108 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574808.html
574809	\$IJGTMR9.raw	Unknown	126 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574809.html

574810	\$IB8PRFL.png	Unknown	128 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574810.html
574811	\$IL4Z0QF.jpg	Unknown	120 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574811.html
574812	\$IE2I82M.jpg	Unknown	152 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574812.html
574813	\$IAN9TPE.gif	Unknown	112 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574813.html
574814	\$IF6QCQD.jpg	Unknown	120 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574814.html
574815	\$IDJH95Z.jpg	Unknown	156 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574815.html
574816	\$IA4NI4M.jpg	Unknown	126 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574816.html
574817	\$I4MISDO.bmp	Unknown	124 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574817.html
574818	\$IMRCU07.png	Unknown	116 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574818.html
574819	\$I81SVMY.png	Unknown	118 Byte(s)	2023-0414T14:47:57.599076	ReportFiles\574819.html
Object Id	Name	Type	Size	CreatedDate	Export As
574820	\$IKXG6ON	Unknown	120 Byte(s)	2023-0414T14:47:57.599076	ReportFiles\574820.html
835667	AgRobust.db	Unknown	917.09 KB	2022-0909T04:28:24.815388	ReportFiles\835667.db
130109	AppCache133259583528383192.txt	7 bit text	134 KB	2023-0414T15:05:53.10687	ReportFiles\130109.txt

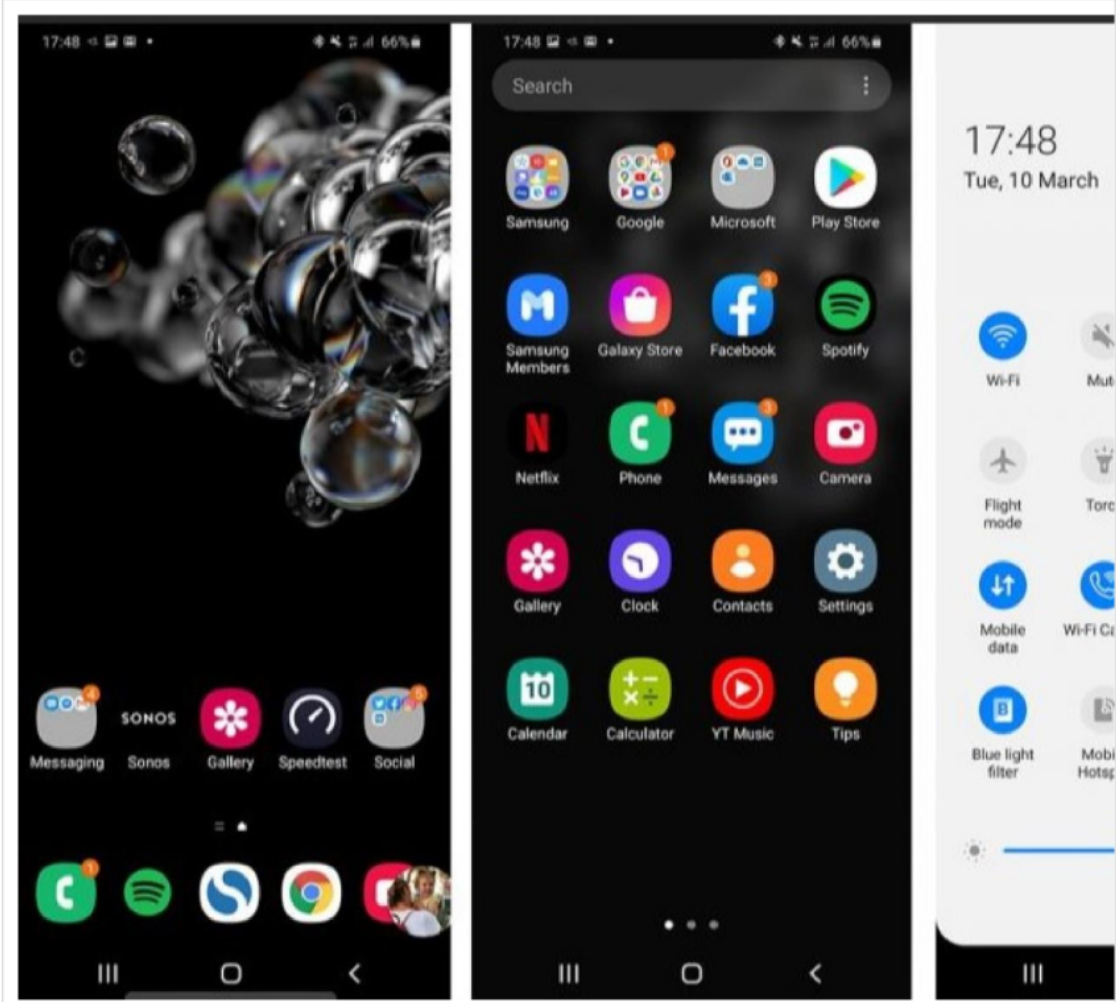
574376	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.080086	ReportFiles\574376
574378	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.064493	ReportFiles\574378
574380	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574380
574382	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574382
574384	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574384
574386	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574386
574807	\$IS7M5ZO.txt	Text	122 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574807.html
574821	\$IJ7YTEM.txt	Text	118 Byte(s)	2023-0414T14:47:57.505359	ReportFiles\574821.html
574822	\$I32473H.txt	Text	122 Byte(s)	2023-0414T14:47:57.505359	ReportFiles\574822.html

Graphics

Object Id	Name	Type	Size	Export As
2453	Samsung S20 Plus look.jpg	JPEG	90.53 KB	ReportFiles\2453.jpg



Object Id	Name	Type	Size	Export As
2454	Samsung S20 Plus GUI Two.jpg	JPEG	124.71 KB	ReportFiles\2454.jpg



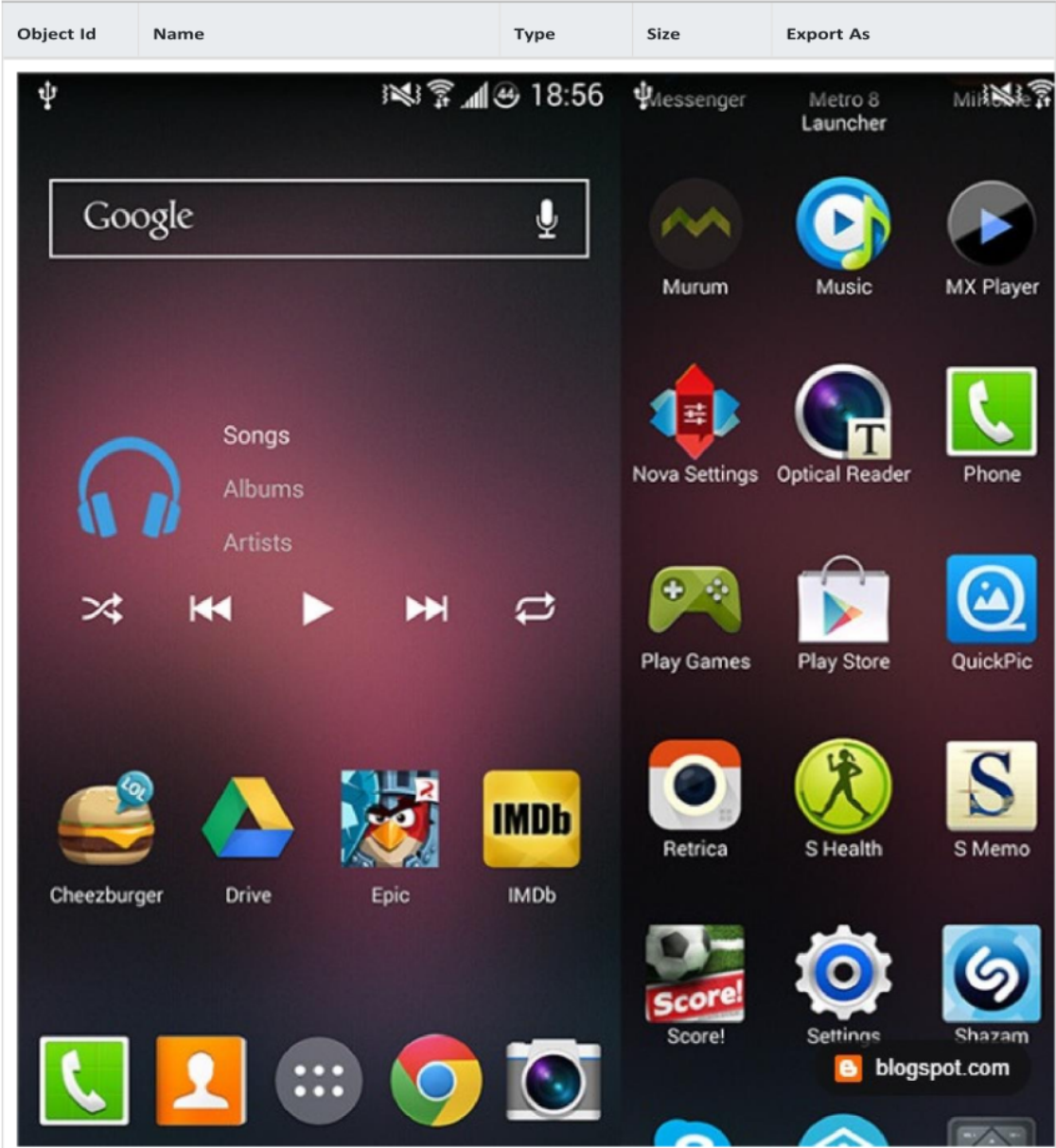
2455	Samsung S20 Plus GUI Three.jpg	JPEG	38.48 KB	ReportFiles\2455.jpg
------	--------------------------------	------	----------	--------------------------------------

Object Id	Name	Type	Size	Export As
-----------	------	------	------	-----------



2456	Samsung S20 Plus GUI One.jpg	JPEG	77.66 KB	ReportFiles\2456.jpg
------	------------------------------	------	----------	--------------------------------------

Object Id	Name	Type	Size	Export As
				
2457	Samsung S20 Plus GUI Four.jpg	JPEG EXIF	200.79 KB	ReportFiles\2457.jpg



574375	computer.bmp	Bitmap	267.87 KB	ReportFiles\574375.bmp
574377	Cat1.gif	GIF	30.29 KB	ReportFiles\574377.GIF
574379	Care-Eric.png	PNG	31.21 KB	ReportFiles\574379.png
574381	Building1.png	PNG	49.61 KB	ReportFiles\574381.png
574383	Building.png	PNG	52.82 KB	ReportFiles\574383.png
Object Id	Name	Type	Size	Export As
574385	Blackberry.png	PNG	345.86 KB	ReportFiles\574385.png

test1

File Category (Bookmarks)

File Category	Report Count	Case Count
📁 Folder	2	252788
JPEG	4	5668
JPEG EXIF	1	1230
Unknown	26	518981
7 bit text	7	84522
* SQLITE Database	1	752
* Windows NT Registry	2	2194
* Windows Shortcut	8	1667
* OLE Archive	3	299
Bitmap	1	3367
GIF	1	1300
PNG	4	62524
Text	3	1707

General

Object Id	Name	Type	Size	CreatedDate	Export As
2146	Temp	Folder	672 Byte(s)	2022-0906T07:16:29.780106	ReportFiles\2146

Object Id	Name	Type	Size	CreatedDate	Export As
2451	CEC Ltd	Folder	56 Byte(s)	2023-0414T14:54:57.01757	ReportFiles\2451
134222	ActivitiesCache.db	SQLITE Database	1 MB	2023-0414T11:19:27.868205	ReportFiles\134222.html
143322	UsrClass.dat	Windows NT Registry	3.5 MB	2023-0414T11:19:16.243269	ReportFiles\143322.dat

147057	NTUSER.DAT	Windows NT Registry	1.5 MB	2023-0414T11:19:14.821378	ReportFiles\147057.dat
146194	Samsung S20 Plus GUI Two.Ink	Windows Shortcut	704 Byte(s)	2023-0414T14:52:12.768827	ReportFiles\146194.html
146195	Samsung S20 Plus look.Ink	Windows Shortcut	850 Byte(s)	2023-0414T14:47:33.583297	ReportFiles\146195.html
146196	Samsung S20 Plus GUI Four.Ink	Windows Shortcut	709 Byte(s)	2023-0414T14:54:11.861662	ReportFiles\146196.html
146197	Samsung S20 Plus GUI One.Ink	Windows Shortcut	704 Byte(s)	2023-0414T14:49:42.895031	ReportFiles\146197.html
146199	CEC Ltd.Ink	Windows Shortcut	564 Byte(s)	2023-0414T14:44:00.584927	ReportFiles\146199.html
146351	Images 2.Ink	Windows Shortcut	695 Byte(s)	2023-0414T14:44:41.131448	ReportFiles\146351.html
146352	Images 1.Ink	Windows Shortcut	695 Byte(s)	2023-0414T14:44:37.647149	ReportFiles\146352.html
146355	Samsung S20 Plus GUI Three.Ink	Windows Shortcut	881 Byte(s)	2023-0414T14:52:51.955931	ReportFiles\146355.html
146370	9b9cdc69c1c24e2b.automaticDestinations-ms	OLE Archive	6.5 KB	2023-0414T12:51:02.686065	ReportFiles\146370.automaticdestinations-ms
Object Id	Name	Type	Size	CreatedDate	Export As
146371	12dc1ea8e34b5a6.automaticDestinations-ms	OLE Archive	8 KB	2023-0414T14:47:33.428487	ReportFiles\146371.automaticdestinations-ms
146374	f01b4d95cf55d32a.automaticDestinations-ms	OLE Archive	12 KB	2023-0414T11:20:04.63369	ReportFiles\146374.automaticdestinations-ms

Graphics

Object Id	Name	Type	Size	Export As
-----------	------	------	------	-----------

2453	Samsung S20 Plus look.jpg	JPEG	90.53 KB	ReportFiles\2453.jpg
------	---------------------------	------	----------	--------------------------------------

Object Id	Name	Type	Size	Export As
				
2454	Samsung S20 Plus GUI Two.jpg	JPEG	124.71 KB	ReportFiles\2454.jpg

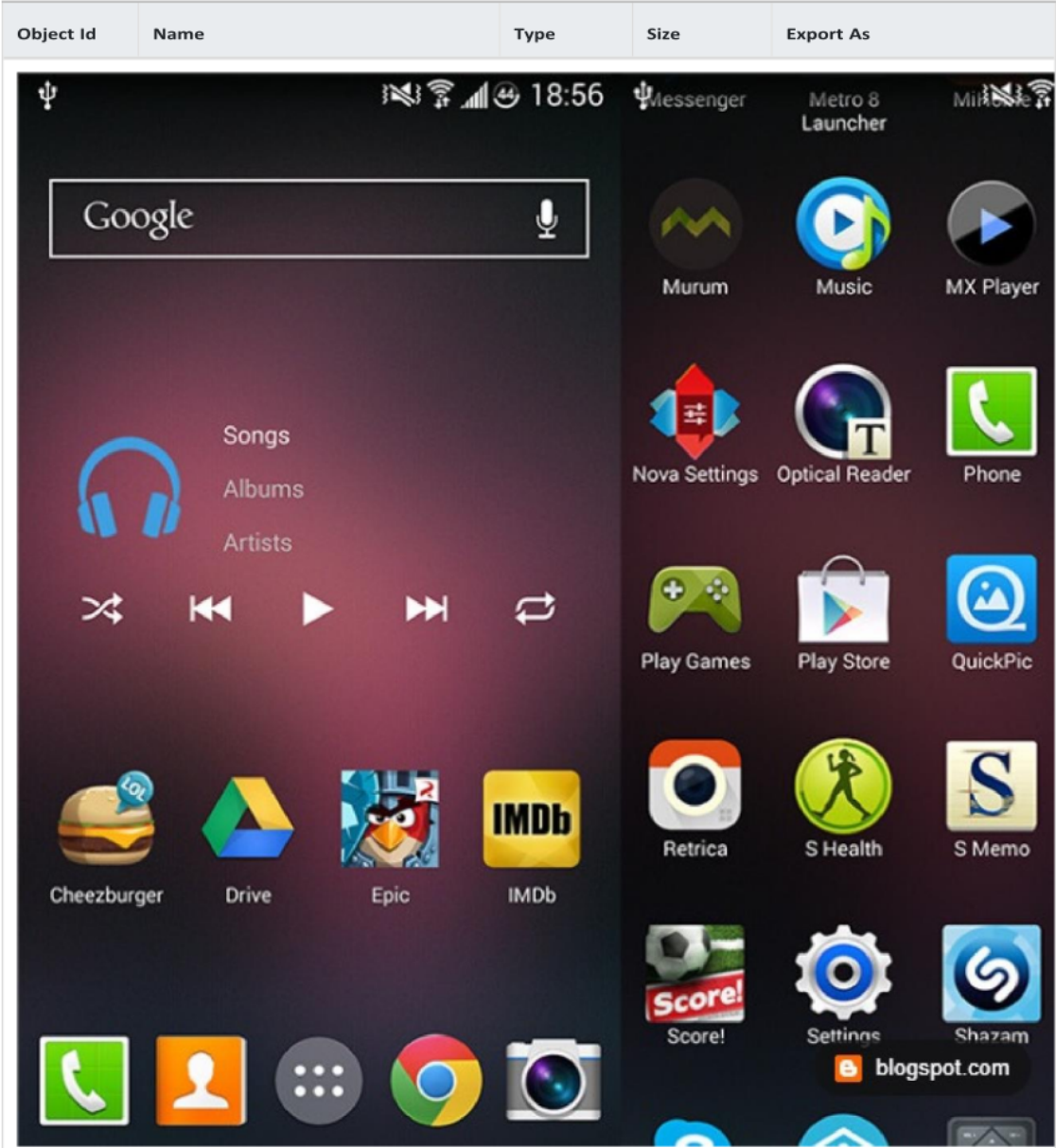
Object Id	Name	Type	Size	Export As
				
2455	Samsung S20 Plus GUI Three.jpg	JPEG	38.48 KB	ReportFiles\2455.jpg

Object Id	Name	Type	Size	Export As
-----------	------	------	------	-----------



2456	Samsung S20 Plus GUI One.jpg	JPEG	77.66 KB	ReportFiles\2456.jpg
------	------------------------------	------	----------	--------------------------------------

Object Id	Name	Type	Size	Export As
				
2457	Samsung S20 Plus GUI Four.jpg	JPEG EXIF	200.79 KB	ReportFiles\2457.jpg



574375	computer.bmp	Bitmap	267.87 KB	ReportFiles\574375.bmp
574377	Cat1.gif	GIF	30.29 KB	ReportFiles\574377.GIF
574379	Care-Eric.png	PNG	31.21 KB	ReportFiles\574379.png
574381	Building1.png	PNG	49.61 KB	ReportFiles\574381.png
574383	Building.png	PNG	52.82 KB	ReportFiles\574383.png
Object Id	Name	Type	Size	Export As
574385	Blackberry.png	PNG	345.86 KB	ReportFiles\574385.png

Documents

Object Id	Name	Type	Size	CreatedDate	Export As
-----------	------	------	------	-------------	-----------

13652	65331	Unknown	1.1 MB	2023-0414T14:57:20.73138	ReportFiles\13652.unknown
14142	64300	Unknown	0 Byte(s)	2023-0414T14:57:08.687426	ReportFiles\14142.unknown
24754	\$MFT	Unknown	1004 MB	2022-0909T00:32:26.731554	ReportFiles\24754.unknown
122541	ntuser.dat.LOG2	Unknown	429 KB	2023-0414T11:19:16.415301	ReportFiles\122541.log2
122542	ntuser.dat.LOG1	Unknown	472 KB	2023-0414T11:19:16.415301	ReportFiles\122542.log1
134221	ActivitiesCache.db-wal	Unknown	3.93 MB	2023-0414T11:19:28.884353	ReportFiles\134221.db-wal
143323	UsrClass.dat.LOG1	Unknown	1.01 MB	2023-0414T11:19:16.243269	ReportFiles\143323.log1
574802	\$IU0A89.jpg	Unknown	120 Byte(s)	2023-0414T14:48:01.708513	ReportFiles\574802.html
574803	\$IWYDC40.png	Unknown	114 Byte(s)	2023-0414T14:48:01.708513	ReportFiles\574803.html
574804	\$I1SDI37.jpg	Unknown	130 Byte(s)	2023-0414T14:48:01.708513	ReportFiles\574804.html
574805	\$IIWHRXI.jpg	Unknown	116 Byte(s)	2023-0414T14:48:01.630457	ReportFiles\574805.html

Object Id	Name	Type	Size	CreatedDate	Export As
574806	\$IC5EDRR.jpg	Unknown	116 Byte(s)	2023-0414T14:48:01.630457	ReportFiles\574806.html

574808	\$IJ407U2	Unknown	108 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574808.html
574809	\$IJGTMR9.raw	Unknown	126 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574809.html
574810	\$IB8PRFL.png	Unknown	128 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574810.html
574811	\$IL4Z0QF.jpg	Unknown	120 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574811.html
574812	\$IE2I82M.jpg	Unknown	152 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574812.html
574813	\$IAN9TPE.gif	Unknown	112 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574813.html
574814	\$IF6QCQD.jpg	Unknown	120 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574814.html
574815	\$IDJH95Z.jpg	Unknown	156 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574815.html
574816	\$IA4NI4M.jpg	Unknown	126 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574816.html
574817	\$I4MISDO.bmp	Unknown	124 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574817.html
574818	\$IMRCU07.png	Unknown	116 Byte(s)	2023-0414T14:47:57.724228	ReportFiles\574818.html
574819	\$I81SVMY.png	Unknown	118 Byte(s)	2023-0414T14:47:57.599076	ReportFiles\574819.html

Object Id	Name	Type	Size	CreatedDate	Export As
-----------	------	------	------	-------------	-----------

574820	\$IKXG6ON	Unknown	120 Byte(s)	2023-0414T14:47:57.599076	ReportFiles\574820.html
835667	AgRobust.db	Unknown	917.09 KB	2022-0909T04:28:24.815388	ReportFiles\835667.db
130109	AppCache133259583528383192.txt	7 bit text	134 KB	2023-0414T15:05:53.10687	ReportFiles\130109.txt
574376	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.080086	ReportFiles\574376
574378	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.064493	ReportFiles\574378
574380	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574380
574382	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574382
574384	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574384
574386	Zone.Identifier	7 bit text	93 Byte(s)	2023-0414T14:54:58.017633	ReportFiles\574386
574807	\$IS7M5ZO.txt	Text	122 Byte(s)	2023-0414T14:47:57.739587	ReportFiles\574807.html
574821	\$IJ7YTEM.txt	Text	118 Byte(s)	2023-0414T14:47:57.505359	ReportFiles\574821.html
574822	\$I32473H.txt	Text	122 Byte(s)	2023-0414T14:47:57.505359	ReportFiles\574822.html

COMPUTER FORENSICS – SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

74/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

GRADING FORM: L5 CF (ACCD5000)

CHRIS THOMAS

74

ENGAGEMENT WITH LITERATURE SKI

Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as how, wiki, forums, etc. will not be accepted. (20 marks)

 Key concepts discussed. Try to use/engage with more updated peer reviewed articles and journals in your research /literature areas, especially for general background research. Some research information was irrelevant for task 1.

14

KNOWLEDGE AND UNDERSTANDING SK

On chosen topic, your work must demonstrate understanding of concepts and underlying principles. You should explain and analyse the tools you have chosen from the research in a meaningful way. The

IEEE report format must be used for the research aspect (task 1) but not mandatory for the case study (task 2). (10 marks)



You have demonstrated sound knowledge and understanding. See comments above to improve this section.

7

COGNITIVE AND INTELLECTUAL SKI

Your work must demonstrate critical analysis and evaluation of the investigation and reporting documentation. Your work must also justify Computer Forensics Investigation procedures. The labs you do in class should help you to complete the processes or forensic methods Barry would have used. (45 marks)



Abstract should be the last to be written to outline the key finding or contribution that would interest key players of what was done.

Tools discussed were categorised. The case study was discussed but making a lot of assumptions.

The key was to list the methodology steps. You could outline/list/document the forensics methodology steps/stages Barry would take.

Example step 1: He would visited Rob's desk and seized all the hardware devices such as hard disks, CDROM, iPods, and DVD disks etc.

Step 2: He placed all the seized devices carefully in anti-static bags and transported them to a forensics laboratory. Etc.

You have done the invoice for services provided

30

PRACTICAL SKILLS

Marks will be awarded based on the sample professional forensics report generated by a forensics tool. AccessData FTK tool is recommended as this tool is on the computers in room IQ 205 or any other of your choice will be accepted. Use sample evidence file(s) from the shared folder. Less than 40% will be awarded for Internet downloaded report. (15 marks)



You have used FTK tool to generate a report and demonstrate your understanding.

15

TRANSFERABLE SKILLS FOR LIFE A

The report should be presented in an academic way (IEEE/ACM format) and therefore must include an abstract, an introduction, a conclusion and a list of references. The report must be submitted via Turnitin as well. (10 marks)



Presentable and professional report.

8