

# **CTEC – 5806**

## **Digital Forensics & Investigation**



---

Declaration: I have read and I understand the Department's guidelines on plagiarism and cheating, and I certify that this submission fully complies with these guidelines.

---



CTEC5806  
Digital Forensics: Principles & Practice  
Coursework Template 2022

Cohort:	CEM1
Date Due:	10/06/2022
Time Due:	12:00 noon/midday Leicester UK time

## Table of Contents

<b>1.Introduction.....</b>	<b>4</b>
<b>2. Analysis of Hard Drive Forensic Image .....</b>	<b>6</b>
2.1 Launch FTK 7.4 & Create a New Case .....	6
2.2 Adding and Processing the Evidence.....	8
2.3 Analysing the Evidence .....	11
2.4 Conclusion:.....	12
<b>3. Analysis of USB Drive Forensic Image.....</b>	<b>12</b>
3.1 Launch FTK 7.4 & Create a New Case .....	12
3.2 Adding Evidence & Processing the Data .....	14
3.3 Analysing the Evidence .....	16
3.4 Launching the PRTK.....	19
3.5 Conclusion:.....	23
<b>4. Analysis of Mobile Phone Forensic Image .....</b>	<b>24</b>
4.1 Launching the Cellebrite Physical Analyser .....	24
4.2 Adding Evidence to the Case .....	25
4.5 Conclusion .....	33
<b>6. Critical Reflection on My Learning Journey .....</b>	<b>34</b>
<b>Appendix A - References .....</b>	<b>36</b>
<b>Appendix B – Title.....</b>	<b>37</b>
<b>Appendix C – Title.....</b>	<b>38</b>

## List of Figures

Figure 1:Launching FTK Application .....	6
Figure 2:Creating a new case .....	6
Figure 3:Evidence Processing for the selected Case study .....	7
Figure 4:Carving the Options .....	7
Figure 5:Managing the evidence Item .....	8
Figure 6:Adding / Managing the Evidence.....	8
Figure 7:Processing the Evidence.....	9
Figure 8:Data Processing Status Window .....	9
Figure 9:Evidence added (Laptop) for Investigation .....	10
Figure 10:Search Term .....	10
Figure 11:***** .....	11
Figure 12:***** .....	11
Figure 13:***** .....	11
Figure 14:***** .....	12
Figure 15:Launching FTK 7.4 Application.....	12
Figure 16:Creating USB Case for Analysing .....	13
Figure 17:Processing Evidence for USB Case .....	13
Figure 18:Selecting the Carving Options.....	14
Figure 19:Selecting the Evidence Type.....	14
Figure 20:Adding the USB Evidence to the Case .....	15
Figure 21:FTK Processing the Data .....	15
Figure 22:Data processing Status .....	16
Figure 23:Added Evidence to the USB Case.....	16
Figure 24:Search Term .....	17
Figure 25:Overview tab of the USB Case.....	17
Figure 26:Export the Selected File .....	18
Figure 27:Encrypted xlsx file .....	18
Figure 28:Launching the PRTK Tool Kit & adding the files .....	19
Figure 29:Identifying the Exported file .....	19
Figure 30:Job wizard of the file .....	20
Figure 31:Calculating the Password.....	20
Figure 32:Results of the Encrypted File .....	21
Figure 33:Rules window .....	21
Figure 34>Password/second.....	22

Figure 35:Decrypted excel file with PRTK .....	22
Figure 36:Generating the Report.....	23
Figure 37:Generated DNA/PRTK Report.....	23
Figure 38:Launching the Physical Analyser & Open a case .....	24
Figure 39:Loading the evidence to a case.....	24
Figure 40:Examination of tools .....	25
Figure 41:Cellebrite Home View .....	25
Figure 42:Case Timeline .....	26
Figure 43:Analysed Data.....	26
Figure 44:Contacts from the Analysed Data.....	27
Figure 45:SMS received from the Analysed Data.....	27
Figure 46:SMS from Vodafone .....	28
Figure 47:SMS from +447785373471 .....	28
Figure 48:SMS from 49503 .....	28
Figure 49:Device Locations found .....	28
Figure 50:File Systems .....	29
Figure 51:Image Attachments .....	29
Figure 52:Searching from the HEX Pattern .....	30
Figure 53:Insights View.....	30
Figure 54:Updating the signature database.....	30
Figure 55:Malware Scanner .....	31
Figure 56:Trace Window of malware scanning.....	31
Figure 57:Reports tab View.....	32
Figure 58:Extraction report.....	32
Figure 59:Tags View .....	33

## **1.Introduction**

### **Case Information: What have you got to analyse?**

The continued misuse of the cyberspace has necessitated different methods of ensuring proper usage and security measures of the respective users. This is in different forms including digital forensics which can be described as the examination of digital media of storage to piece together traces of information to lead to a substantial evidence (Mueller, 2020). Digital forensics is mostly focused in law enforcement scenarios where the examiners collect pieces of information to solidify the evidence from the investigation.

As such, this project is geared towards the examination of three storage media; USB drive, laptop and a mobile phone. As described, digital forensics is an investigative science in the vast computer science domain where the examiners seek to solidify pieces of evidence related to a given digital crime as alleged.

The examination involves the use of different tools and techniques depending on the image formats, the availability of the respective tools and the expertise available. In this case, E01 is the image file format as obtained from the digital imaging process. As mentioned, the objective of this examination is to piece together pieces of information from the three digital media to solidify or invalidate the allegations depending on the hypothetical position taken.

### **SANS Framework**

Deploying the SANS framework, this forensic examination is tailored in the following perspective;

#### **Preparation**

Preparation sets the centre-stage for the digital examination, in this stage, the examiners prepare the necessary tools and techniques to commence the forensic examination.

#### **Identification**

Identification is set to identify the specific media and image types to be examined. This entails identifying the appropriate tool to be used. As mentioned, the selection of tools and techniques is informed by diverse factors including expertise and the type of image to be examined.

#### **Containment**

Containment step in digital forensics as per SANS comes after the actual investigations are completed. This is the whole incident response aspect in which the organization/ victim deploys various techniques in deterrence of similar incidents in the future.

## **Eradication**

SANS places eradication aspect of the framework from a security perspective, in this step, the examiners are set to do away with the issues causing the incidents and the related attacks.

## **Recovery**

According to SANS framework, a digital forensic is not complete until the last stable state of the IT infrastructure has been restored. In this sense, if the examination surrounded security breach, the stakeholders must undertake to restore the last stable condition of the system before it was affected or attacked.

## **Lessons Picked**

This is a summary of the important aspects picked from the whole process encompassing the possible causes, impacts and the methods that have been used to navigate through as well as recovering to a stable state as was required.

The SANS framework can also be viewed from the incident response perspective, in this, sense, the framework goes from examination to recovery and documentation of the process as well as the lessons learnt from the entire process. This is critical in ensuring that the users have a strategy to sail through the incident as well as nail the perpetrators of the respective crime.

## **Forensic Imaging**

Involved in digital media, the possibilities of tampering with digital pieces of evidence are high posing an integrity issue in the media under investigation. This necessitates the need to create a copy of the digital media before embarking on the technical investigation. The imaging process is specified on the target media (Carew and Errickson, 2019). As well as the destination location.

## 2. Analysis of Hard Drive Forensic Image

**Software Used:** FTK Imager & PRTK

**Forensic Image File Name:** 22020307\_laptop\_SD. E01

The digital media/ laptop's hard drive contains digital footprints and evidence; a digital image is loaded into the work space in this case as the subject of investigation.

**E01 format** - This format compresses the image file. Image in this format will start with case information in the header and footer, which has an MD5 hash of the entire bit stream. This case information contains the date and time of acquisition, examiner's name, special notes and an optional password.

### 2.1 Launch FTK 7.4 & Create a New Case

The tool is installed on Windows environment with a GUI desktop application for easy navigation in University Lab. Unlike other tools, the GUI interaction makes it easier to navigate the evidence items hence the preferred choice in this case scenario.

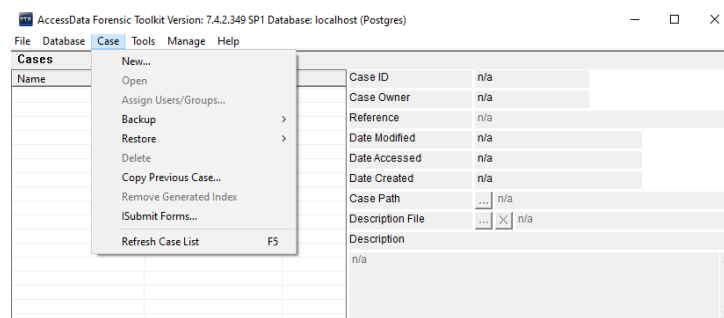


Figure 1: Launching FTK Application

After Launching the FTK 7.4, as shown in figure 1. New window will pop up from the FTK window, select the Case menu, then the New option.

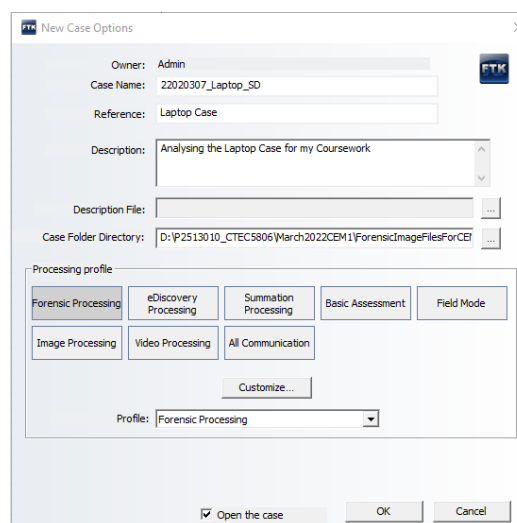


Figure 2: Creating a new case

Enter the Case name, Reference & Description for the case study. Then choose the Processing Profile, click on the Customize button.

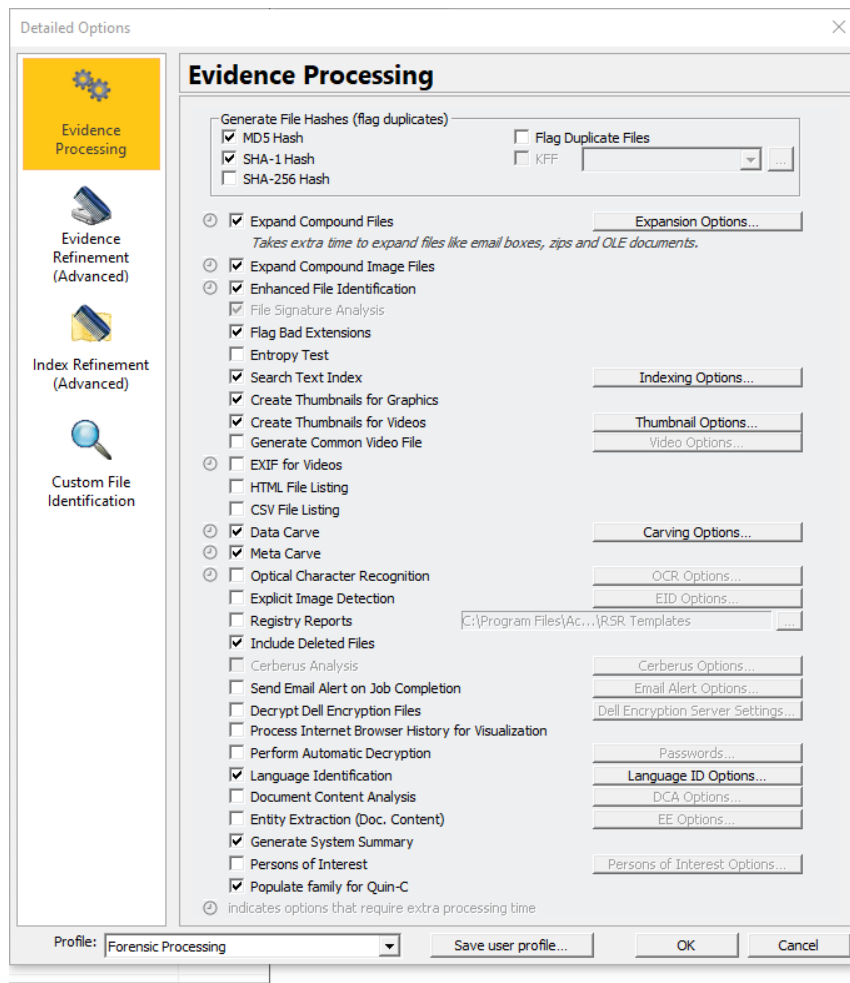


Figure 3: Evidence Processing for the selected Case study

Hence the Forensic Processing profile is selected, A window is popup showing as the evidence processing. we can also customise this further by selecting the check boxes next to the various options as in the above screenshot

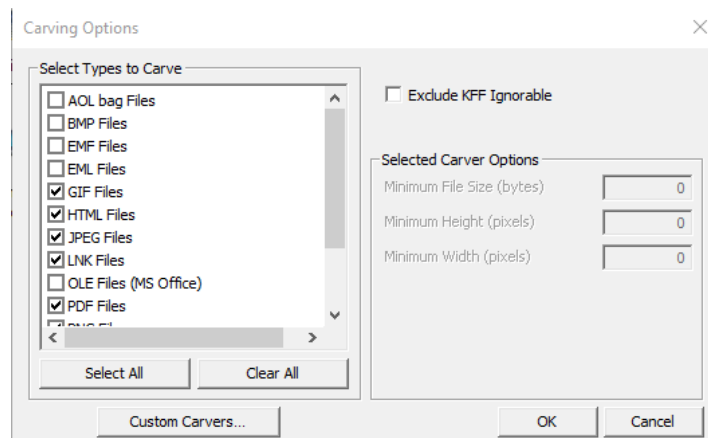


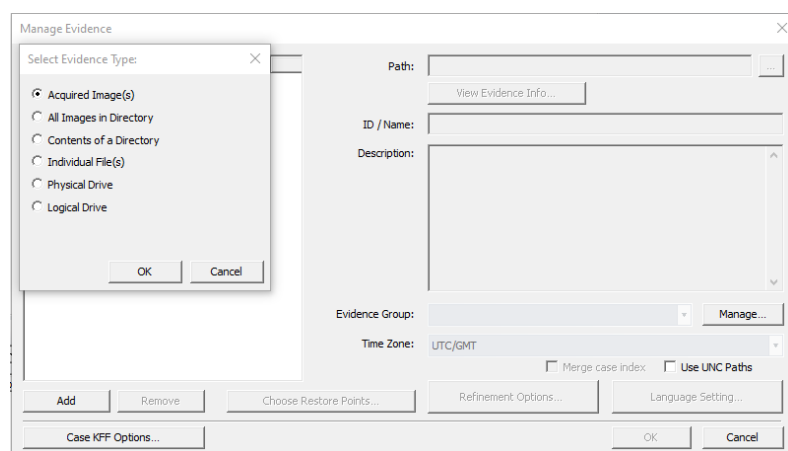
Figure 4: Carving the Options



I've selected the carving options which are listed in the above screenshot.

- HTML Files
- PDF files
- PNG files
- LNK Files etc. Which are listed in the below screenshot.

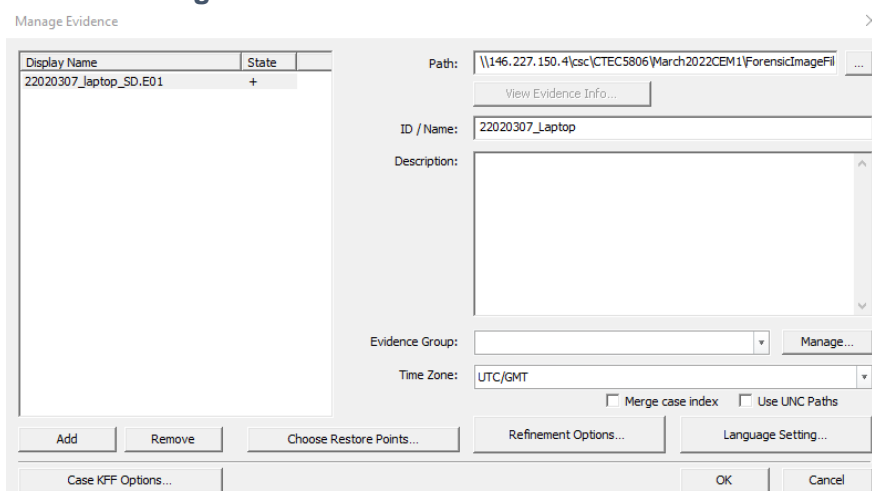
Once done click OK when you have selected the required Carving Options, you will then be returned to the Evidence Processing window and click OK.



*Figure 5:Managing the evidence Item*

Now select the source that you need to acquire. Please make sure that you are selecting the right evidence type, after selecting the Acquired images then click OK option Locate the 22020307\_laptop\_SD. E01 file you saved to the Forensic Image Files folder inside your case.

## 2.2 Adding and Processing the Evidence



*Figure 6:Adding / Managing the Evidence*

Once done with this step then the FTK will start processing the evidence. FTK allows for the import of evidence from which the specific piece of evidence can be selected and loaded into the work space.

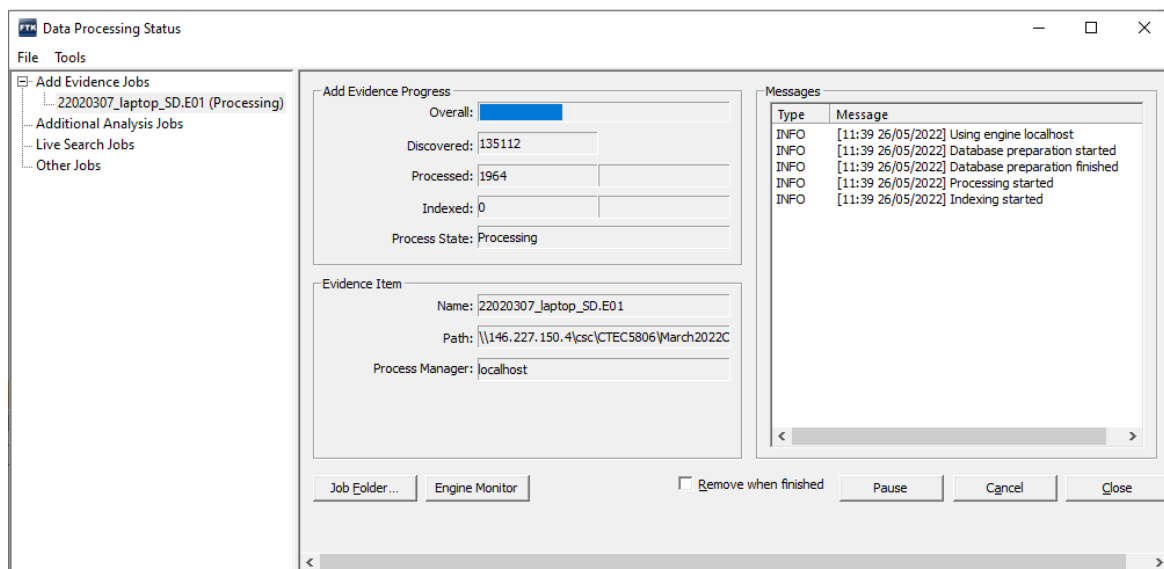


Figure 7: Processing the Evidence

Depending on the size of the forensic image which have added and the processing options customised, this process is taking a bit time & can see the progress bars and numbers changing as the evidence file is processed.

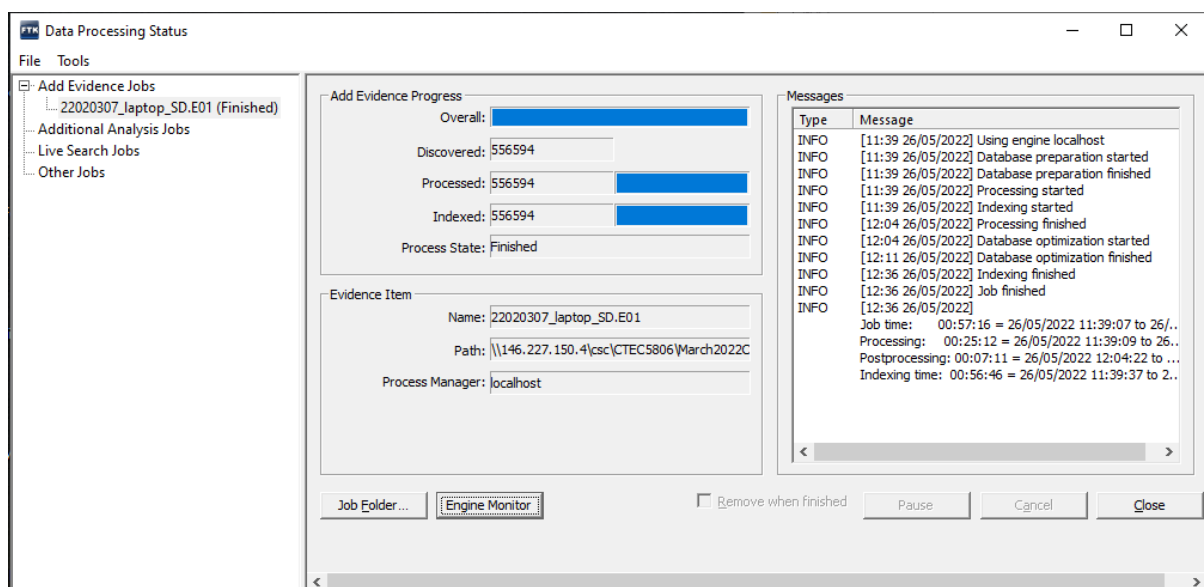


Figure 8: Data Processing Status Window

The processing took about 00:25:12 mins. Once everything processed, you can click the Close button & then you will then be shown the FTK case window and the case is ready to use.

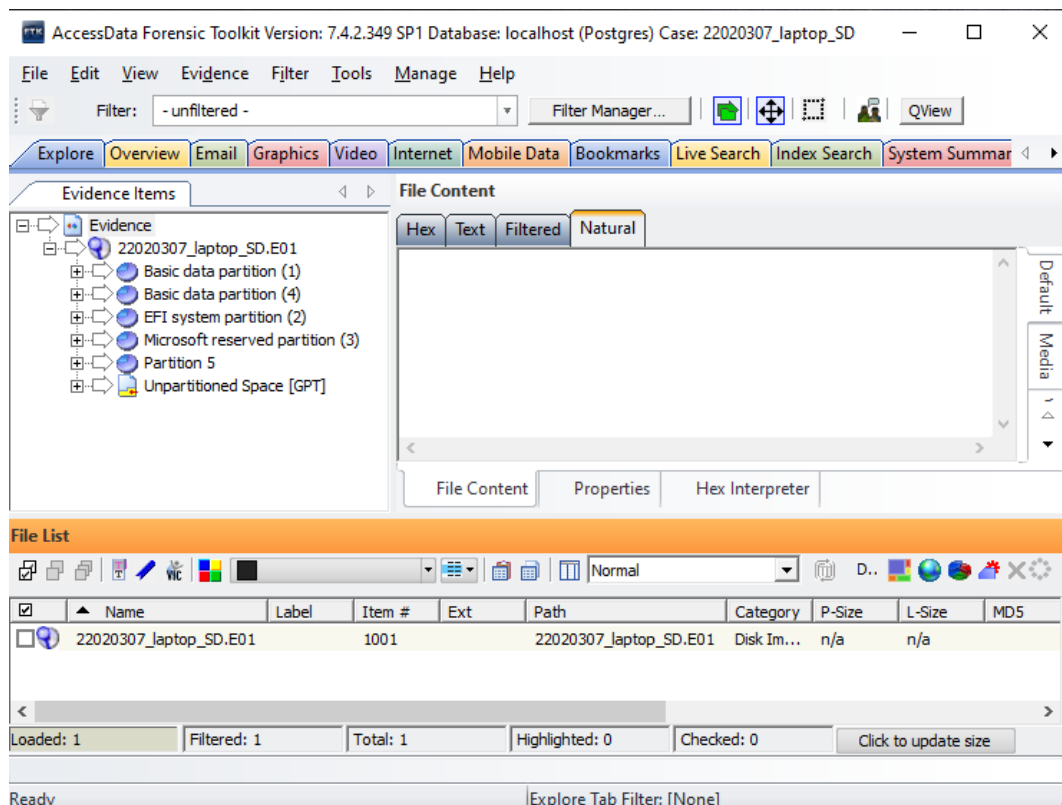


Figure 9:Evidence added (Laptop) for Investigation

We see multiple coloured tabs in the FTK screen. Let's check the explore tab first. Expand the Evidence item (22020307\_laptop\_SD. E01). There I have 5 partitions and some un-partitioned space. Each Space contains some HEX values. Click the Viewer Pane and press the CTRL + F keys to open up the search function & search for Hex or Text term.

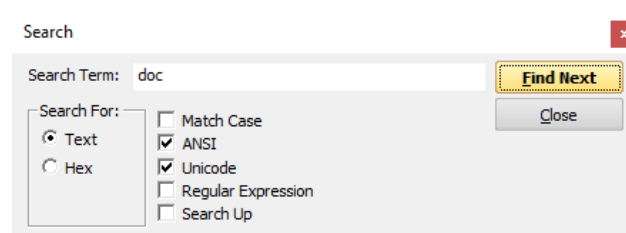


Figure 10:Search Term

### 2.3 Analysing the Evidence

This is the most important aspect of the digital forensic examination. From the Analysed Case something is suspicious that I found some volume type: removable disk.



Figure 11:\*\*\*\*\*



Figure 12:\*\*\*\*\*



Figure 13:\*\*\*\*\*



Figure 14:\*\*\*\*\*

From the Removable disk I found some xlsx file which is moved, renamed or deleted.

## 2.4 Conclusion:

To create a comprehensive report, it is critical to support the evidence with visible evidence, this necessitates the export of the reconstructed pieces of evidence from the digital media as imported into the work space. As illustrated in the workspace, the laptop folder is characterized by the presence of various pieces of evidence to be investigated. This investigation is approached from a black-box perspective such that there is zero hint on what is being sought in the investigation. As part of the investigations, it is important to establish what type of media is involved in the investigation. This can be used to create a concrete case against the subjects involved in the investigations.

## 3. Analysis of USB Drive Forensic Image

**Software Used:** FTK 7.4 & PRTK

**Forensic Image File Name:** USB\_20220703\_001\_SD. E01

The retrieval or recovery of deleted data from USB drives is what we call USB forensics. This paper details the procedure for performing forensics analysis on a USB device.

### 3.1 Launch FTK 7.4 & Create a New Case

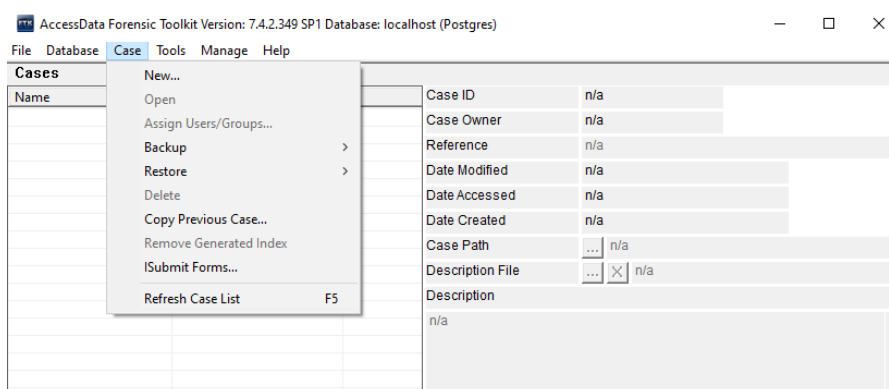


Figure 15:Launching FTK 7.4 Application

After Launching the FTK 7.4, as shown in figure 1. New window will pop up from the FTK window, select the Case menu, then the New option.

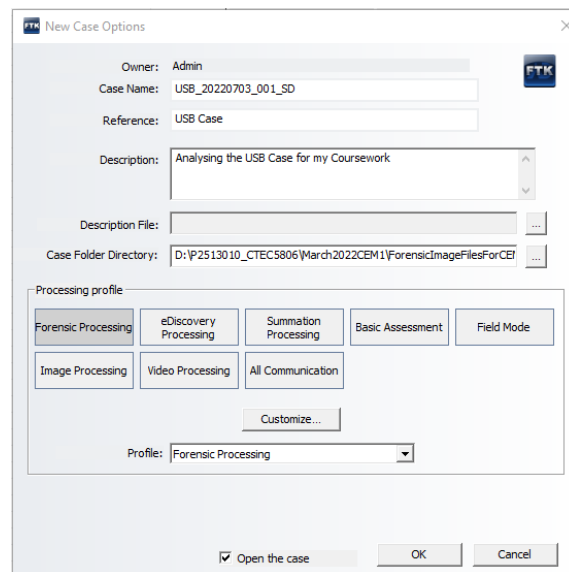


Figure 16: Creating USB Case for Analysing

Enter the Case name, Reference & Description for the case study. Then choose the Processing Profile, click on the Customize button. A window will popup showing as the evidence processing

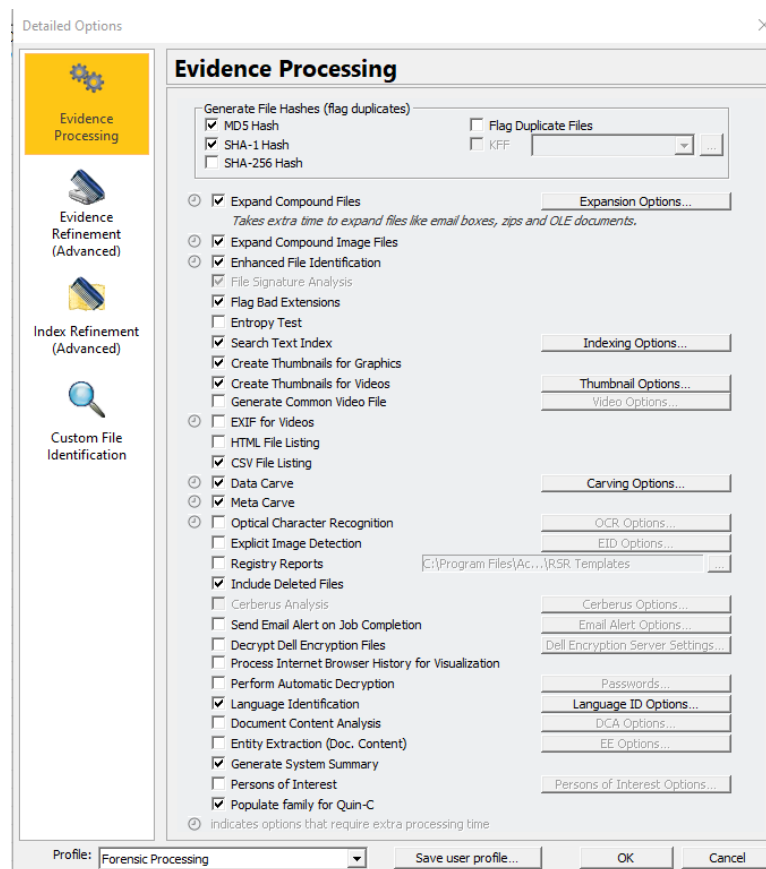


Figure 17: Processing Evidence for USB Case

I've selected the carving options from the above screenshot & selected the options for my case So FTK to automatically recover files that are located in free space or embedded within files.

- HTML Files
- PDF files
- PNG files
- ZIP files
- LNK Files etc. Which are listed in the below screenshot.

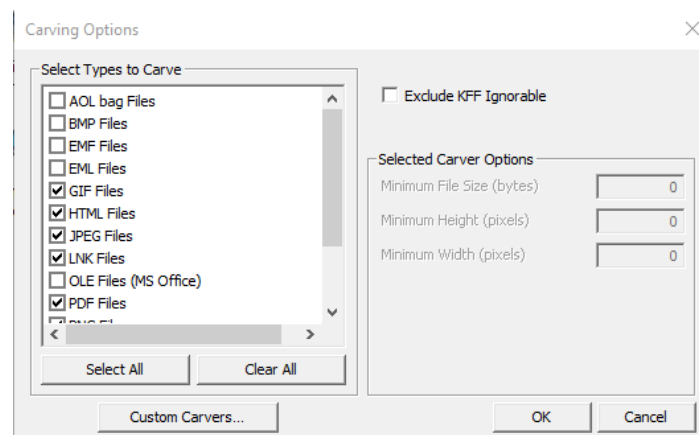


Figure 18:Selecting the Carving Options

Once done click OK when you have selected the required Carving Options, you will then be returned to the Evidence Processing window. Now select the source that you need to acquire. I had chosen the Acquired Images.

### 3.2 Adding Evidence & Processing the Data

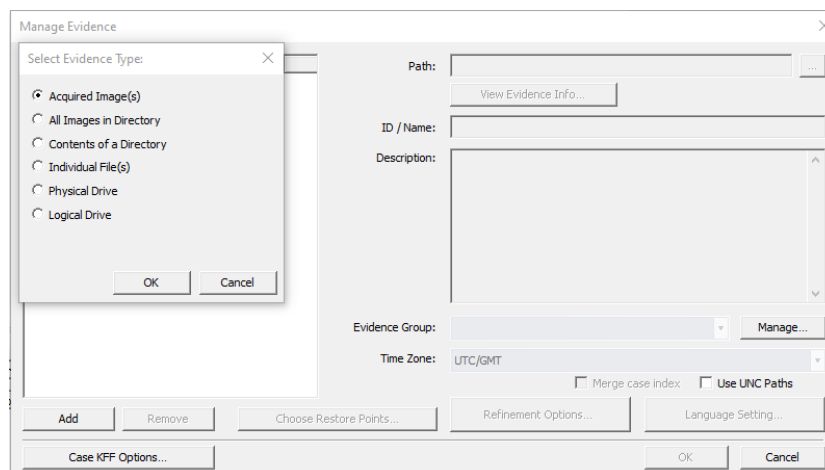


Figure 19:Selecting the Evidence Type

After selecting the Acquired images then click OK option Locate the file for adding evidence  
Here my file is USB\_20220703\_001\_SD. E01 file and after adding evidence click ok button.

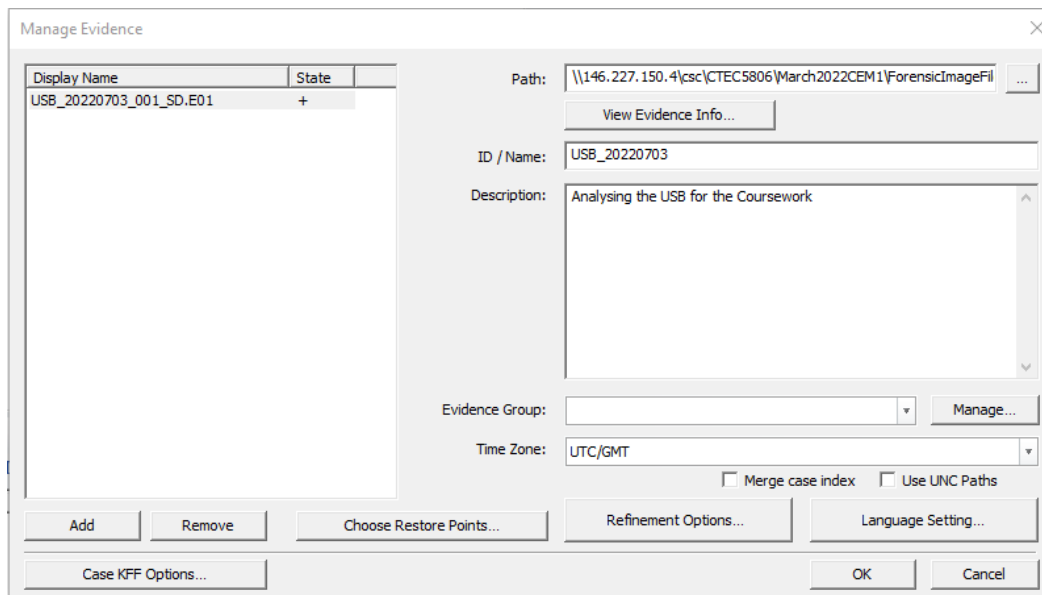


Figure 20: Adding the USB Evidence to the Case

Once done adding the evidence to the Case click OK option & the FTK will Process the Data.

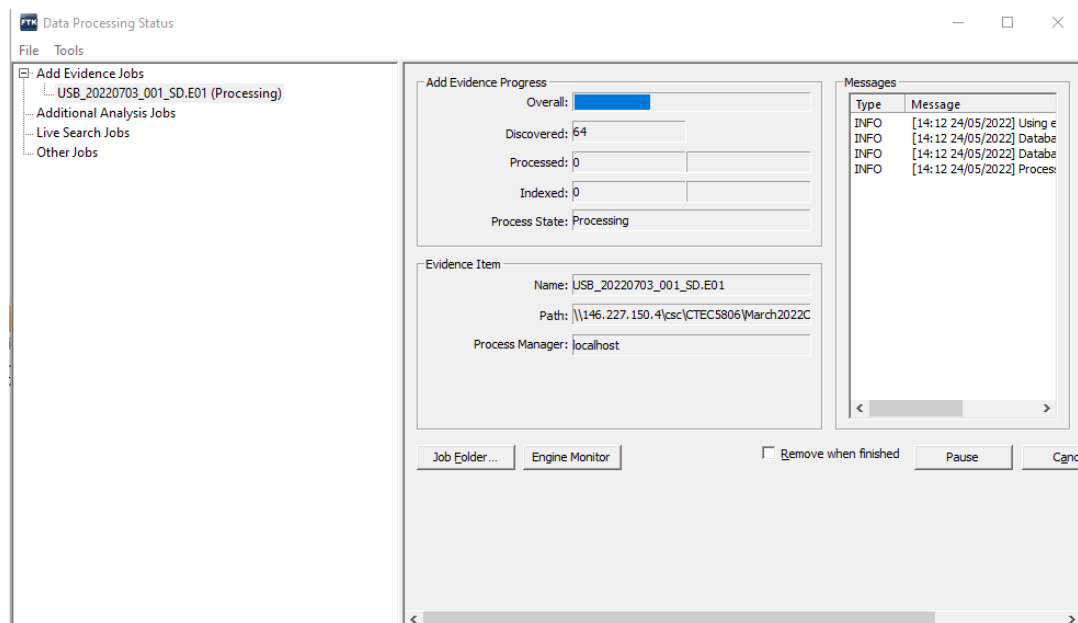


Figure 21: FTK Processing the Data

Depending on the size of the forensic image which have added and the processing options customised, this process will take a couple of minutes & can see the progress bars and numbers changing as the evidence file is processed in the below screenshot.



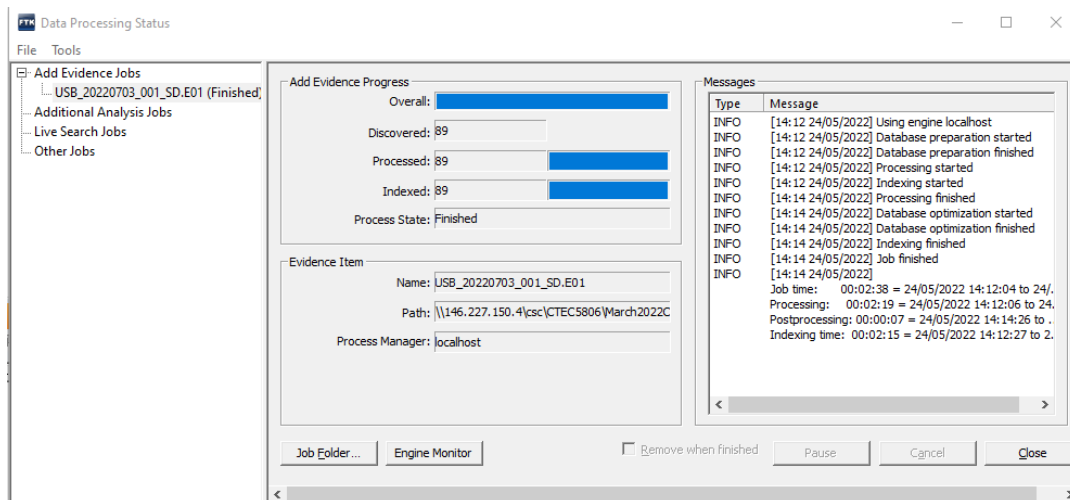


Figure 22:Data processing Status

The entire job for this forensic image took 00:02:38 minutes. Once everything processed, you can click the Close button & then you will then be shown the FTK case window and the case is ready to use.

### 3.3 Analysing the Evidence

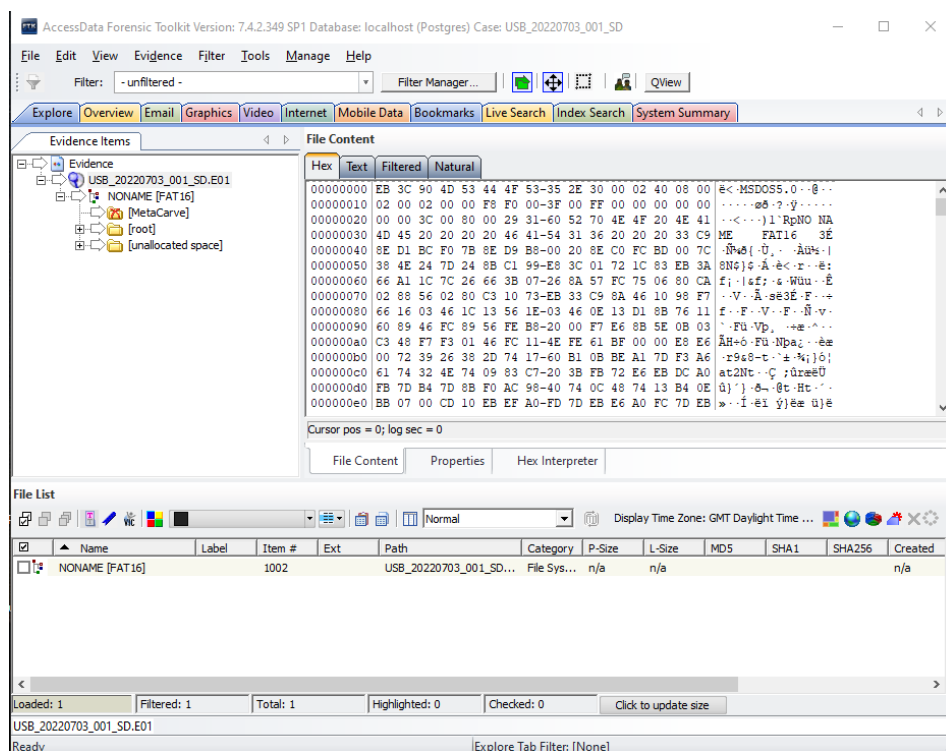


Figure 23:Added Evidence to the USB Case

As illustrated in the figure above, the above illustration adds evidence into the investigation tool. We have 1 partition named NONAME [FAT 16] under that, we can see 2 parts named as MetaCarve, root & some un-allocated space.

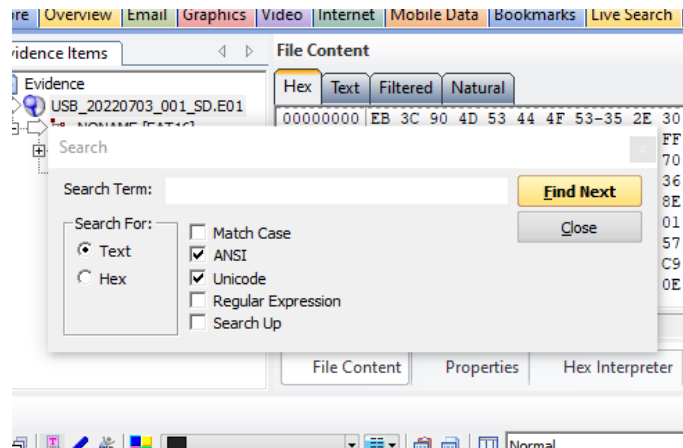


Figure 24: Search Term

The search for specific pieces of information from the vast file can be made easier by the use of the search functionality if the headers are known. We can Find files like Docx, exe, jpg, jpeg Files etc. So that we can find the text using the Hex tab.

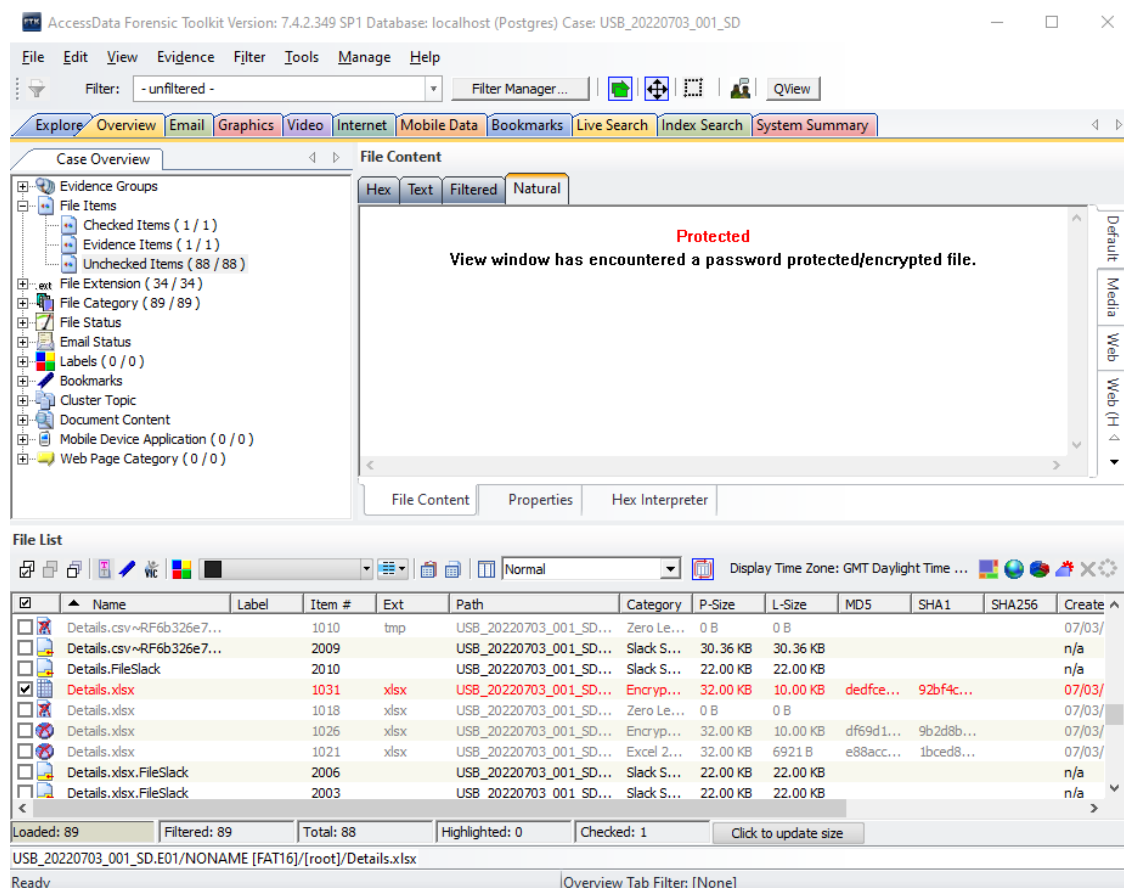


Figure 25: Overview tab of the USB Case

The overview of the Evidence Group contains the above listed items which includes the File items and File groups. After analysing I found Encrypted xlsx. file. Which we need to decrypt and analyse in further. Export the encrypted file to your path.

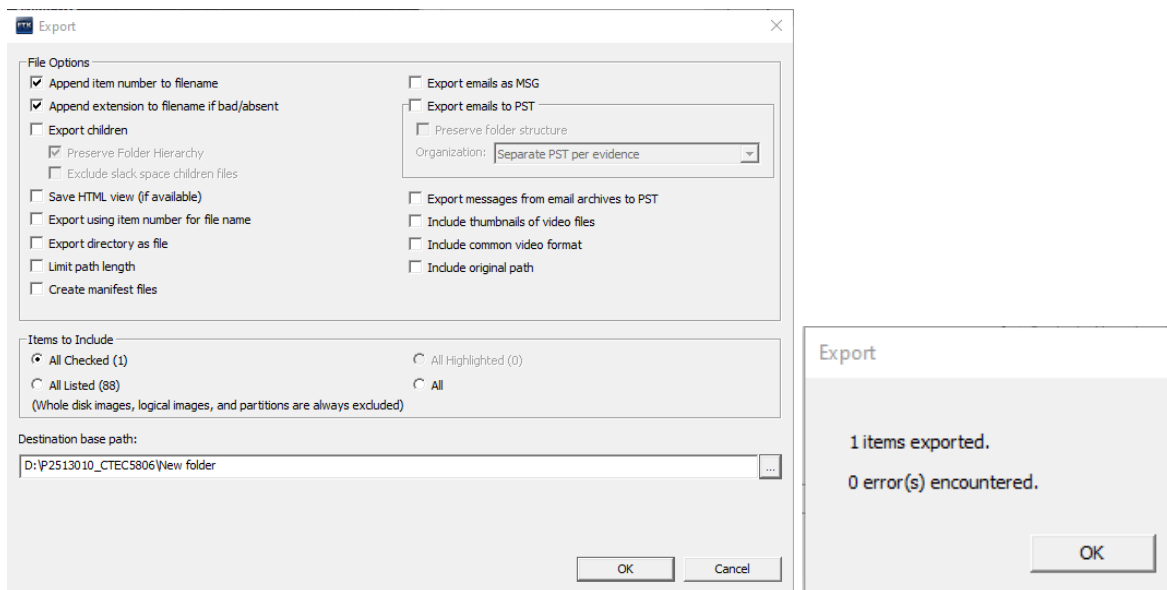


Figure 26:Export the Selected File

Select the Required option when exporting the file & select the Destination path where you want to save it. Then Successfully 1 item has been exported without any errors encountered. Now let's find the Exported file from the Saved destination

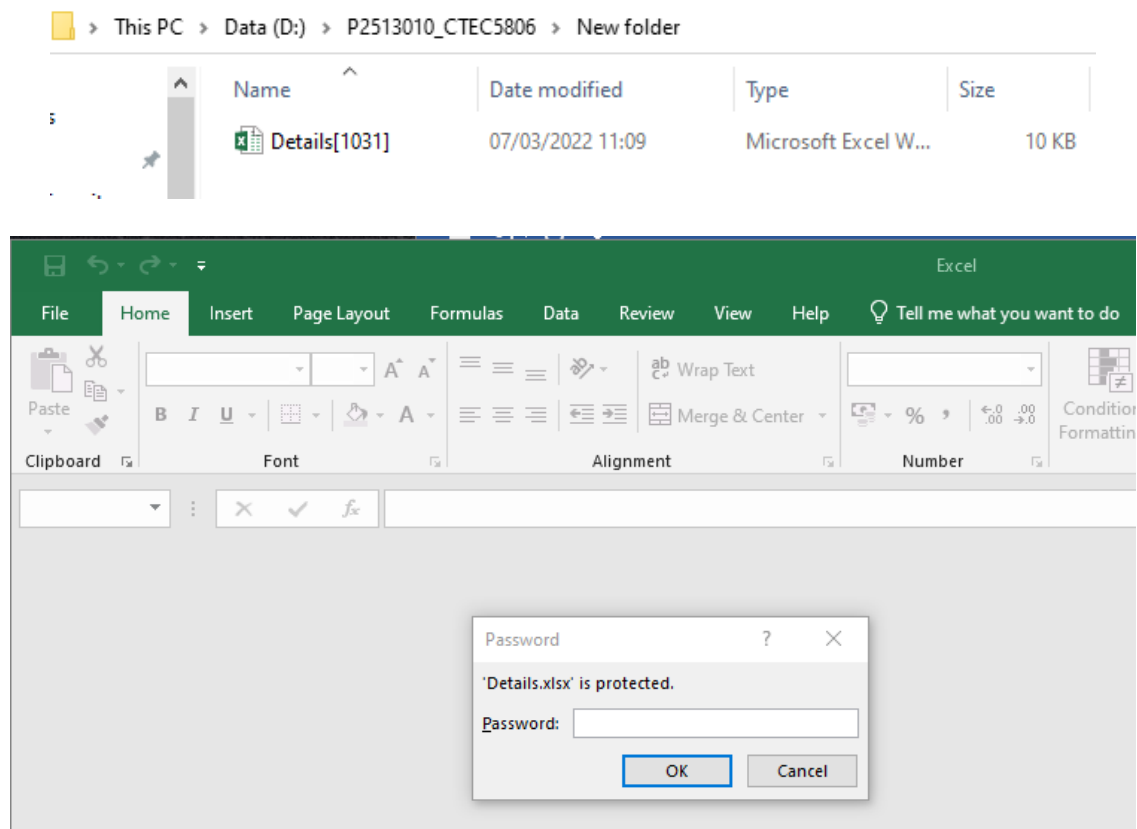


Figure 27:Encrypted.xlsx file

We need to decrypted this Password Protected /Encrypt file. So, for this we are using the PRTK (Password Recovery tool kit) for this process.

### 3.4 Launching the PRTK



Figure 28: Launching the PRTK Tool Kit & adding the files

Add the exported files from the saved destination to the PRTK. Click add button



Figure 29: Identifying the Exported file

In this step it will identify for the add files, then the Job wizard window will popup check the details & click Finish.

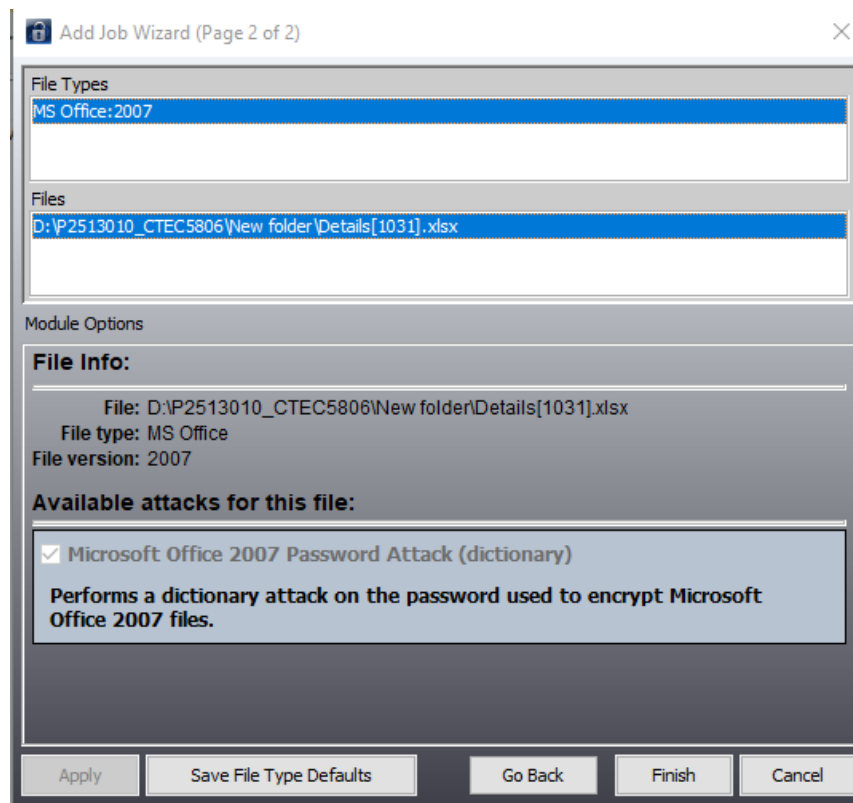


Figure 30:Job wizard of the file

This will calculate the password space for the selected encrypted file. Hence the result is displayed as follows.



Figure 31:Calculating the Password

From the figure 31 the Job information is showing the **Results: alphabet**. Now let's see the Processing rules & Passwords/second tab. For this click on the menu tab and expand the View tab click on the file properties.

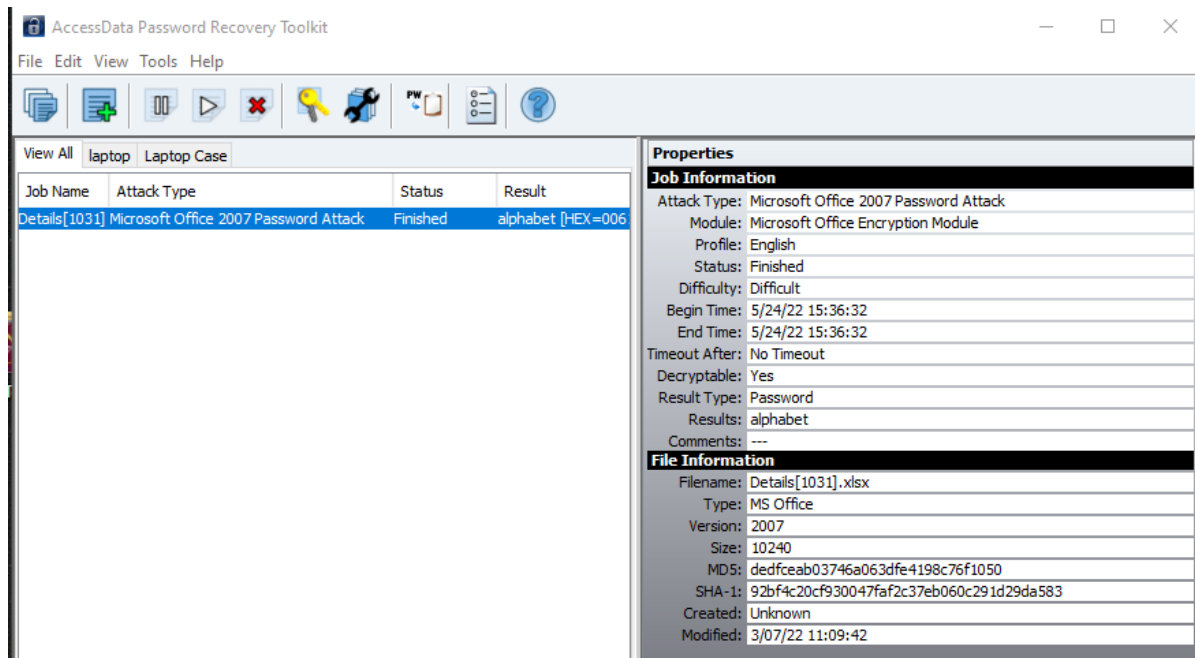


Figure 32:Results of the Encrypted File

To check the properties for details double click on the Job Name then new window will popup as shown in below screenshot.

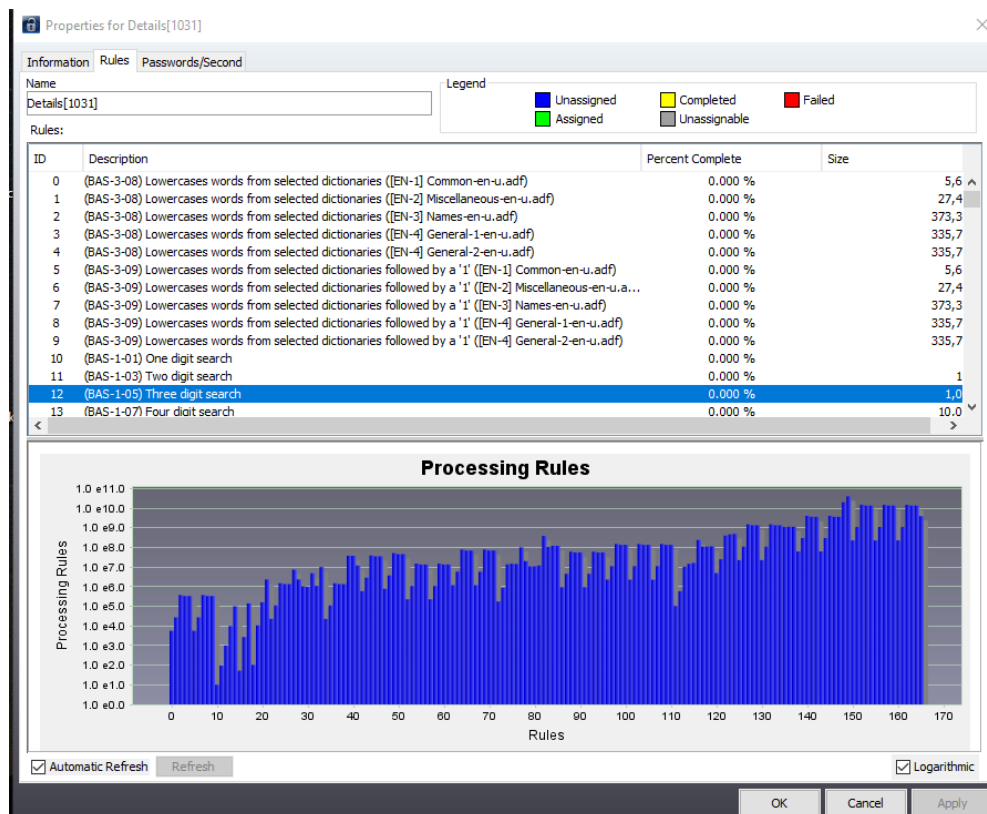


Figure 33:Rules window

From the Above the image we can see the 3 tabs contains information on each tab. Click on the Rules tab there you can find the Details & Processing rules with graph illustration.

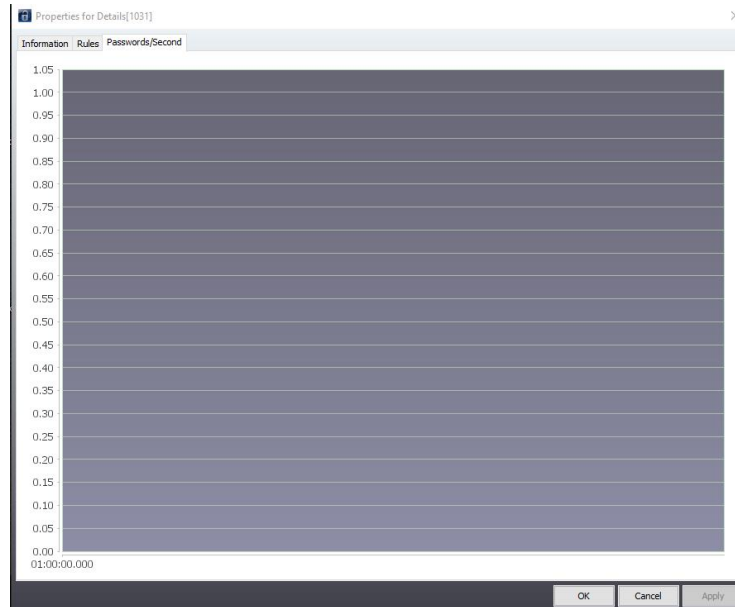


Figure 34:Password/second

We can check how many encryptions has done in the Passwords/second tab. I had done with only 1 encryption so the result is displayed as 00:000

	A	B	C	D	E	F	G	H	I
1	First Name	Surname	Job Title	Pay	Gender	Date of Birth	Favourite Colour	Favourite Song	Pets Name
2	Violet	Afia	CEO	88241	Female	17/06/1987	Cyan	You Got It	Sophia
3	Imogen	Albaz	Software Engineer	65421	Female	21/07/1994	Purple	Don't Feel Like Dancing	Jack
4	Lisa	Arturo	Manager	67421	Female	03/04/1986	Green	A Kind Of Magic	Ruben
5	Kris	Devlin	Chef	24895	Non-binary	12/06/1997	Red	Tequila	Rufus
6	Richard	Donaldson	Reporter	26342	Male	26/12/1990	Pink	Ice Ice Baby	Frank
7	Ibrahim	Duncan	Detective	56894	Male	04/05/1981	Red	Every Little Thing She Does Is Magic	Daria
8	Rebekka	Ford	Doctor	48457	Female	15/07/1992	Gold	Strong Enough	Chrissy
9	Felicity	Green	Publisher	41992	Non-binary	18/05/1988	Yellow	Give Me Everything	Tilly
10	Patrick	Kirk	Pre-School Leader	12.75	Male	16/02/2001	Light Blue	See You Again	Tom
11	Billy	Lemon	Hospitality Assistant	9.8	Male	25/12/2002	Fawn	Starboy	Bruce
12	Helen	Nuffield	Marketing Manager	50000	Female	29/04/1984	Blue	Songbird	Bernie
13	Dolly	Parton	Bus driver	14.35	Female	08/03/1978	Black	The Macarena	Bruno
14	Randeep	Patel	Lawyer	82143	Non-binary	22/10/1996	Orange	Jail House Rock	Ginger
15	Khalil	Riley	Computer Scientist	62120	Male	09/01/1989	Yellow	Alice	Simba
16	Gurvinder	Singh	Bank Clerk	25473	Male	10/09/1998	Jade	Money, Money, Money	Benny
17	Bobby	Smith	HGV driver	22.8	Male	16/11/1989	Brown	Last Christmas	Toto
18	Jessica	Smithian	Teacher	36542	Female	14/04/2002	Purple	Lady in Red	Cadbury
19	Jimmy	Taylor	Book Store Owner	62587	Male	30/08/1978	Silver	Don't Stop Believing	Bobby
20	Sammi	Thornhill	Retail assistant	10	Non-binary	12/11/1998	Yellow	Erasure stop	Bobo

Figure 35:Decrypted excel file with PRTK

Hence with the above result shows that the file is decrypted with the PRTK. I opened the encrypted file with the result shown above with the details listed above.

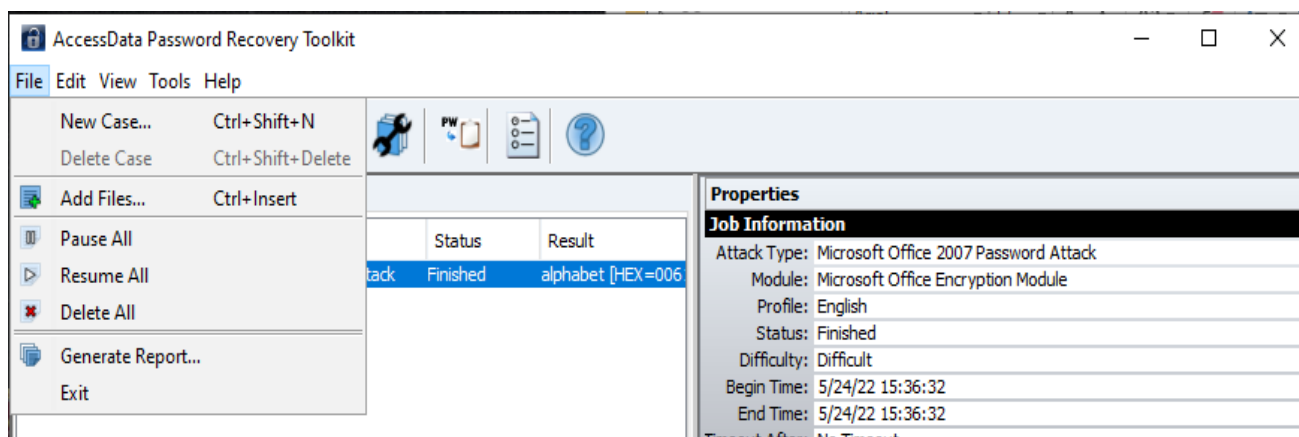


Figure 36: Generating the Report

**Report:** To Generate the report of your analysis click on the menu Option as shown in Figure & generate the report of Analysis.

Saved in my Local system: [file:///C:/Users/cscuser/Desktop/2405/USB\\_Report.pdf](file:///C:/Users/cscuser/Desktop/2405/USB_Report.pdf)

## DNA/PRTK Report

D:\P2513010\_CTEC5806\New folder\Details[1031].xlsx

- Job Status: Finished on 5/24/22 15:36:32
- Commonly Registered Type: Microsoft Office 2007 Password Attack
- Identified Type: MS Office
- File Size: 10240
- File Version: 2007
- Job Started: 5/24/22 15:36:32
- File Modified: 3/07/22 11:09:42
- SHA 1: 92bf4c20cf930047faf2c37eb060c291d29da583
- MD5: dedfceab03746a063dfe4198c76f1050
- Result: alphabet
- Description: Save As
- Password Type: Password
- Where Found: The Golden Dictionary

Figure 37: Generated DNA/PRTK Report

### 3.5 Conclusion:

This investigation is set to examine the Case. FTK allows for the import of evidence containing the pieces of information such that one can select the specific image to be examined as per the case. From the evidence folder, the examiner gets to launch the respective image into the workspace for investigations. Forensic investigation is approached in a structured manner with a glimpse of the objectives of the investigation. This can be to obtain some suspected emails, images or documents.



## 4. Analysis of Mobile Phone Forensic Image

**Software Used:** Cellebrite Physical Analyser

**Forensic Image File Name:** UFED Apple iPhone 5 (A1429) 2022\_03\_07 (001)

The mobile forensics process aims to recover digital evidence or relevant data from a mobile device in a way that will preserve the evidence in a forensically sound condition.

### 4.1 Launching the Cellebrite Physical Analyser

Cellebrite Physical Analyzer is a digital forensic tool which allow examiners and investigators to recover, decrypt, decode, and review digital data and effectively surface actionable intelligence.

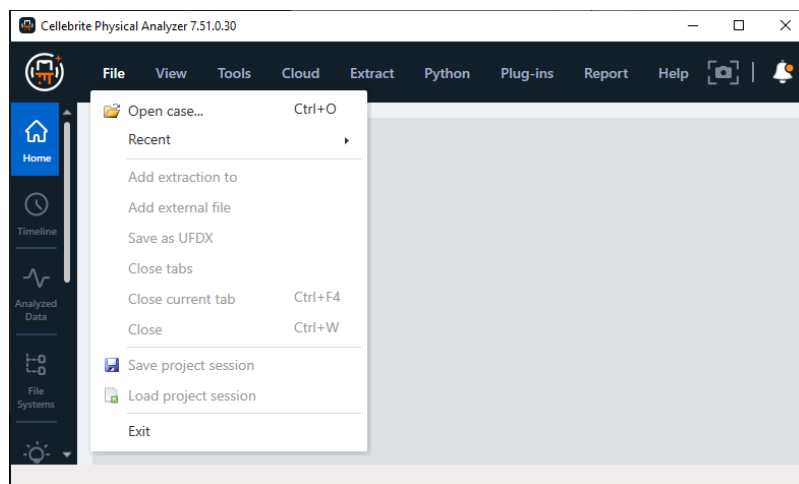


Figure 38: Launching the Physical Analyser & Open a case

After Launching the Cellebrite Physical Analyser a new window will popup. Open a new case from the file Menu and load the evidence from your folder.

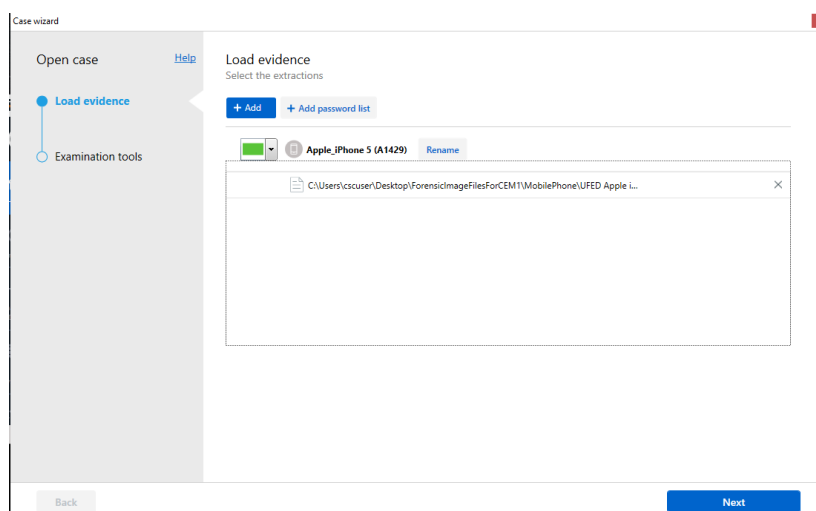


Figure 39: Loading the evidence to a case

Add the Evidence to the Case from your Folder and when you click Next a case wizard option will popup to select the options from the Examination tools screen there you select the required tools & click examine Data for further process

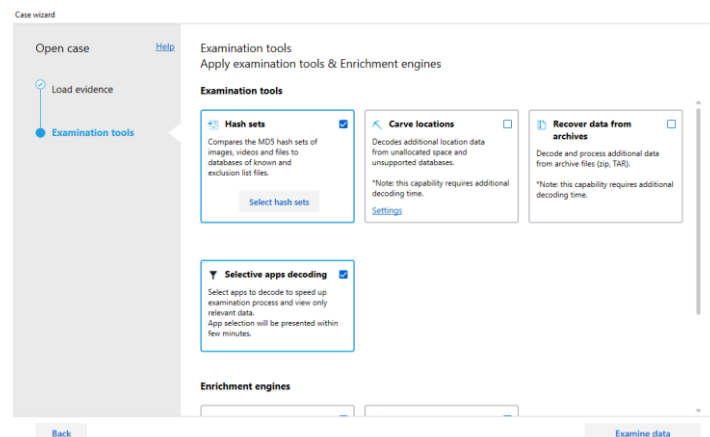


Figure 40:Examination of tools

## 4.2 Adding Evidence to the Case

Once everything is done will be redirected to the Cellebrite physical analyser Home View. Where you can find the Summary of the Loaded evidence.

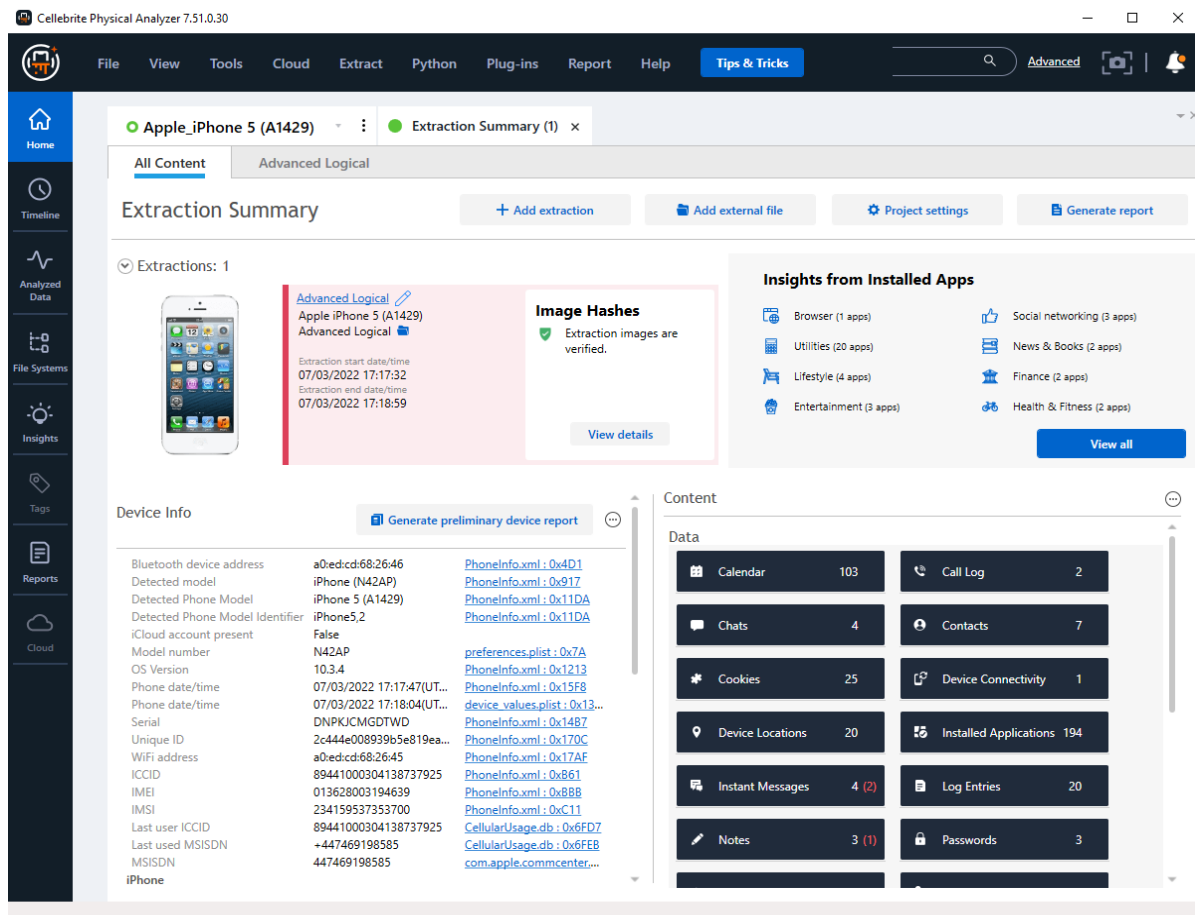


Figure 41:Cellebrite Home View

The Extraction Summary tab includes a summary of the extraction and has the following sub tabs: All Content: Includes information on the extractions, device information and device content, Advanced Logical: All the Extraction Details & device information.

## Timeline View:

The Timeline view that enables you to analyse data in chronological order, to identify the order of events and make connections between them.

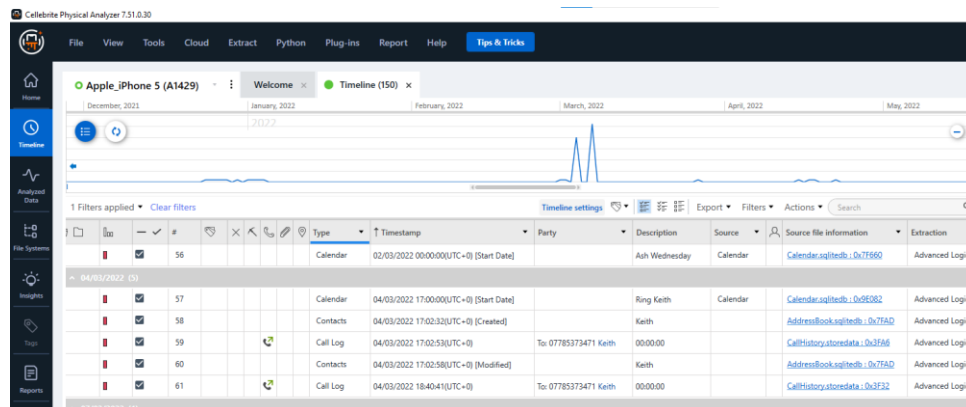


Figure 42:Case Timeline

This Graphical time bar allows you to zoom-in to the timeframe & filter option available to choose the file type. From there I had selected the Calendar, logs, messages and so on.

## Analysed Data View:

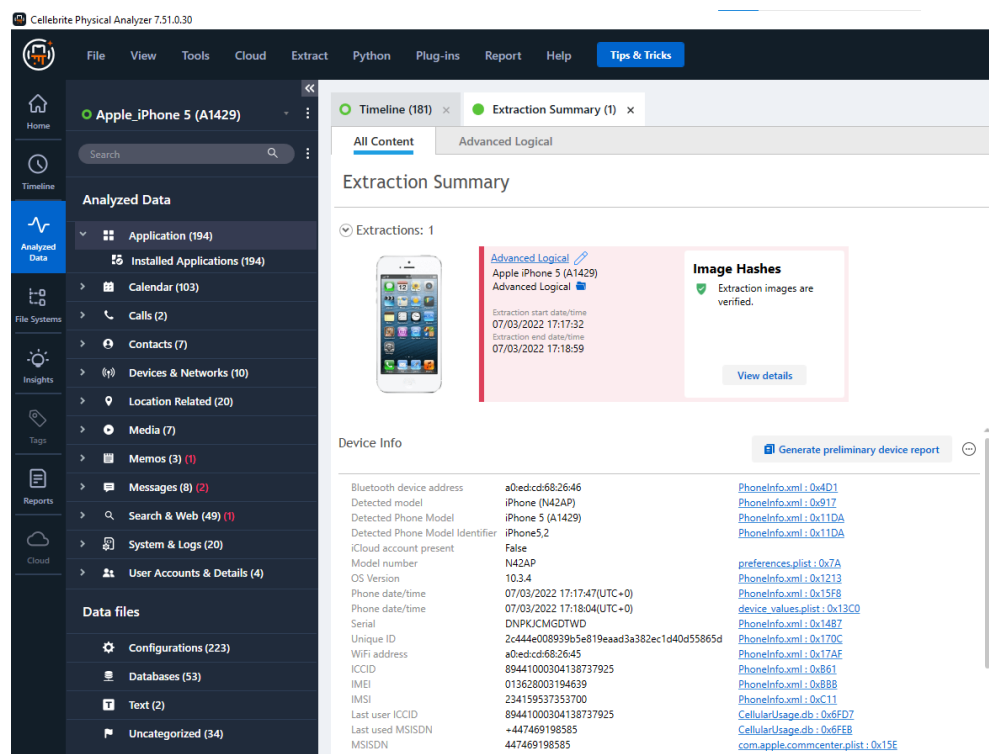


Figure 43:Analysed Data

The Analysed Data view shows a tree with groups of analysed data that are related to device specific features such as contacts, messages, call logs, Device & Networks etc.

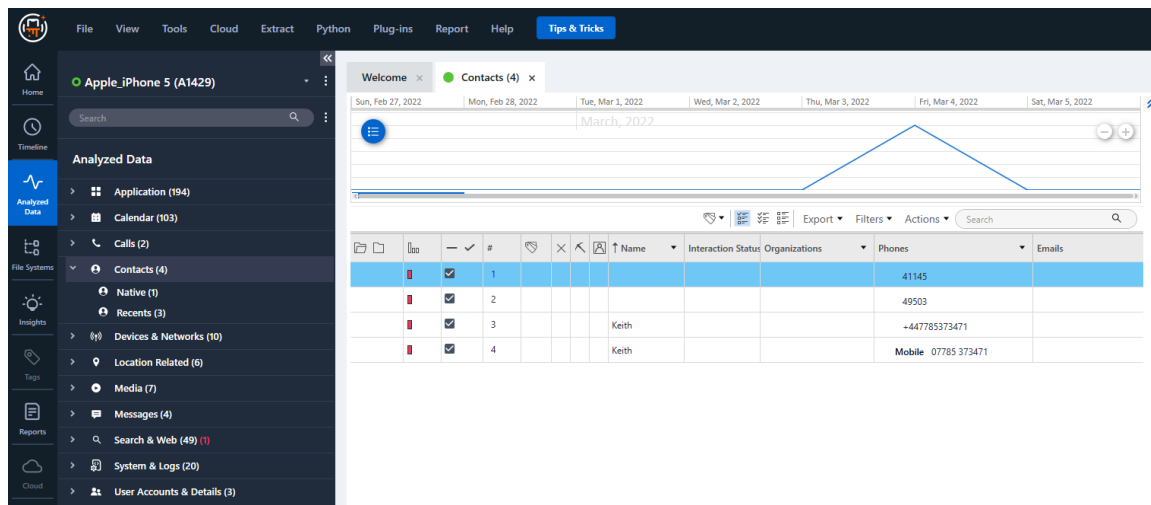


Figure 44: Contacts from the Analysed Data

From the analysis I found 4 contacts with the messages. One contact is from Keith, so I am trying to find out exactly what was there in detail.

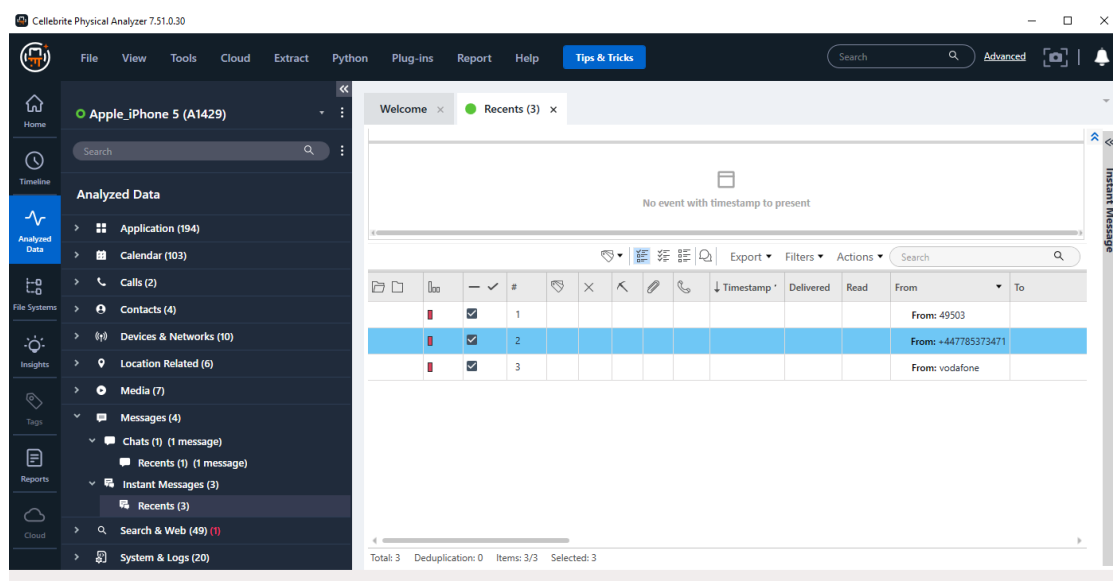


Figure 45: SMS received from the Analysed Data

Click on each displayed data and it will be redirected to the files systems where we can find them from HEX values.

The below image shows the messages for Vodafone, +447785373471 & 49503 numbers. Let's us check them in detail.

```

6 6F 64 61 66 6F 6E 65 63 6F 6D 2E 61 70 70 | m.apple.MobileSMS:SMS:vodafone.com.app
2 0D 00 00 33 25 33 81 17 05 00 4D 09 08 63 | le.MobileSMS1646226.*....3%3....M..c
A 76 6F 64 61 66 6F 6E 65 63 6F 6D 2E 61 70 | om.apple.MobileSMS:SMS:vodafone.com.ap
6 35 30 30 30 3A 31 36 34 | 1646645165000:164658572
4 36 34 31 33 34 36 35 30 | 31000:1646413465000:164
5 41 41 34 35 45 41 32 36 | .; .84BC7EAA45EA2645F030
7 0F F2 0F E4 00 00 00 00 | .....
0 00 00 00 00 00 00 00 00 | .....
2 00 00 00 00 00 00 00 00 | .....

```

InstantMessage.Party.Identifier:  
vodafone

InstantMessage.Party.Identifier: vodafone

Figure 46:SMS from Vodafone

```

3 0D 00 17 33 2F 33 81 17 05 00 4D 09 08 4B 65 69 74 68 63 6F | .....4....3/3....M..Keithco
D 53 53 4D 53 3A 2B 34 34 37 37 38 35 33 37 33 34 37 31 63 6F | m.apple.MobileSMS:SMS:+447785373471co
D 53 31 36 34 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 | m.apple.MobileSMS1646652559000:16466
2 35 30 34 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 | 52504000:1646652504000:1646652483000
F 64 24 0E 98 38 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 | :1646652444000..d$.8ACB882F238CE247
1 6E 05 0C 00 00 33 33 33 33 33 33 33 33 33 33 33 33 33 33 | BED3A2F2D4D1FA31n....3.3'..M..com.ap
3 3A 34 39 35 30 33 33 33 33 33 33 33 33 33 33 33 33 33 33 | ple.MobileSMS:SMS:49503com.apple.Mobi
0 30 30 01 7F 5F E8 0E B0 43 31 38 35 39 37 35 37 32 33 35 42 | leSMS1646581518000...C1859757235B
5 38 33 43 31 7B 04 0C 00 00 5B 00 37 27 05 00 4D 09 08 43 4E | 2D130FADAA37998E83C1{....[.7'..M..CN
9 6F 43 6F 6F 74 61 63 74 44 65 66 61 75 6C 74 41 63 74 69 6F | UICRRecentDomainContactDefaultActio

```

InstantMessage.Party.Identifier:  
+447785373471

InstantMessage.Party.Identifier: +447785373471

Figure 47:SMS from +447785373471

```

0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....phone49503.
0 68 6F 6E 65 34 39 35 30 33 16 | .....%url07785 373471.....'.Keit
9 1D 02 69 6E 73 74 4B 65 69 74 | hphone+447785373471.....)..instantm
2 65 34 31 31 34 35 OD 00 00 00 | essagevodafone.....phone41145.
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....

```

Contact.PhoneNumber.Value: 41145

Contact.PhoneNumber.Value: 41145

Figure 48:SMS from 49503

The screenshot shows the Cellebrite Physical Analyzer interface. On the left, a sidebar lists analyzed data for an Apple iPhone 5 (A1429), including Applications (194), Calendar (103), Calls (2), Contacts (4), Native (1), Recents (3), Devices & Networks (10), Location Related (6), Device Locations (6), Locations (6), Media (7), Images (7), Messages (4), Search & Web (49), System & Logs (20), Log Entries (20), and User Accounts & Details (3). The main window displays a map of Europe with location pins. A table below the map lists the locations found:

#	Origin	Timestamp	End time	Position
1		07/03/2022 11:28:17(UTC+0)		
2		07/03/2022 11:27:05		(52.629383, -1.139478)
3		07/03/2022 11:25:57(UTC+0)		
4		07/03/2022 11:24:28(UTC+0)		

On the right, the 'Location' details panel shows information for a specific location:

- Name: \_BTW-6
- Description: BSSID: Sca1761efb0c0 SSID: \_BTW-6
- Type: Wireless Network
- Origin: Wireless Network
- Timestamp: 07/03/2022 11:28:17(UTC+0)
- End time: 07/03/2022 11:28:17(UTC+0)
- Position: (52.629383, -1.139478)
- Map Address: (52.629383, -1.139478)
- Category: Wireless Networks
- Source: Advanced Logical
- Manually decoded: False
- Source file: [Phone]preferences/SystemConfiguration/com.apple.wifi.plist (Size: 4583 bytes)

The bottom status bar shows: Path: /Phone/mobile/Library/location/user.plist, Size: 170 bytes, Date modified: 25/12/2021 20:32:43(UTC+0).

Figure 49:Device Locations found

## File Systems View:

The File systems view displays a tree with the Memory Images - lists the extraction files generated from the memory modules of the device whereas the Memory Ranges - lists the analysed memory ranges for each of the extracted memory modules of the device (listed under Images).

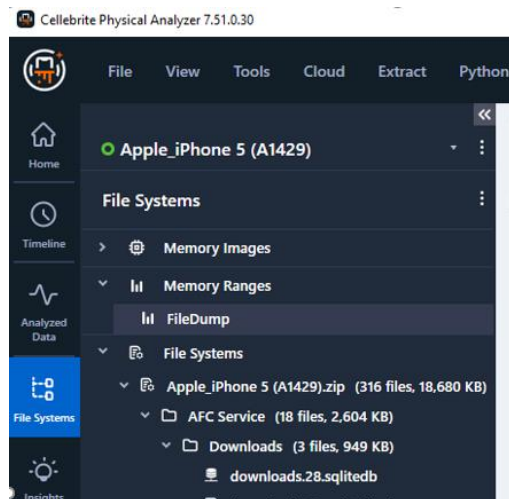


Figure 50:File Systems

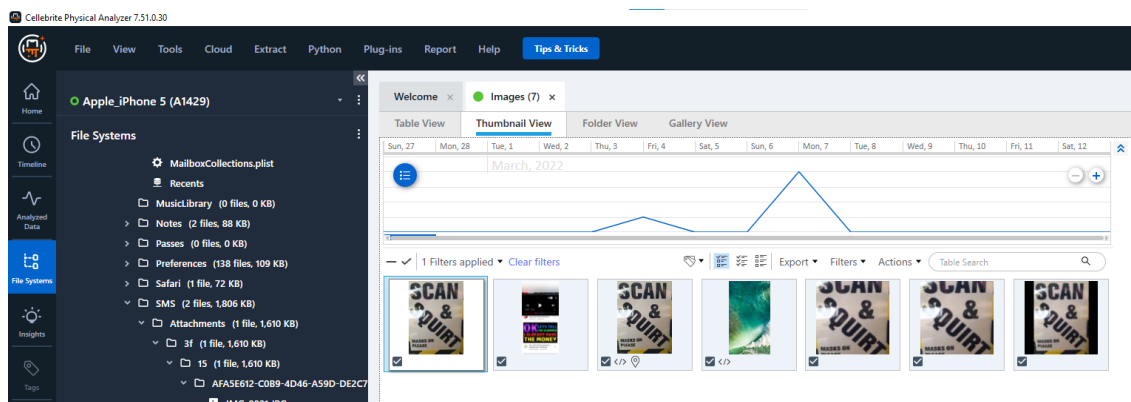


Figure 51:Image Attachments

Use ctrl+F for Searching large memory structures for SMS text strings (7bit PDU) in the Hex data. The Find window has several tabs that enable you to search the Hex data

**Find** - Search for specific parameters, such as strings, bytes, dates, and more.

**RegEx (GREP)** - Search for strings using Regular Expressions.

**SMS 7Bit (PDU)** - Search for SMS text strings.

**Pattern** - Search for text patterns, in cases in which the pattern of the text is understood but not the text itself (mainly used for 7-bit search to locate SMS messages).

**Code** - Specialized search for user codes and passwords.

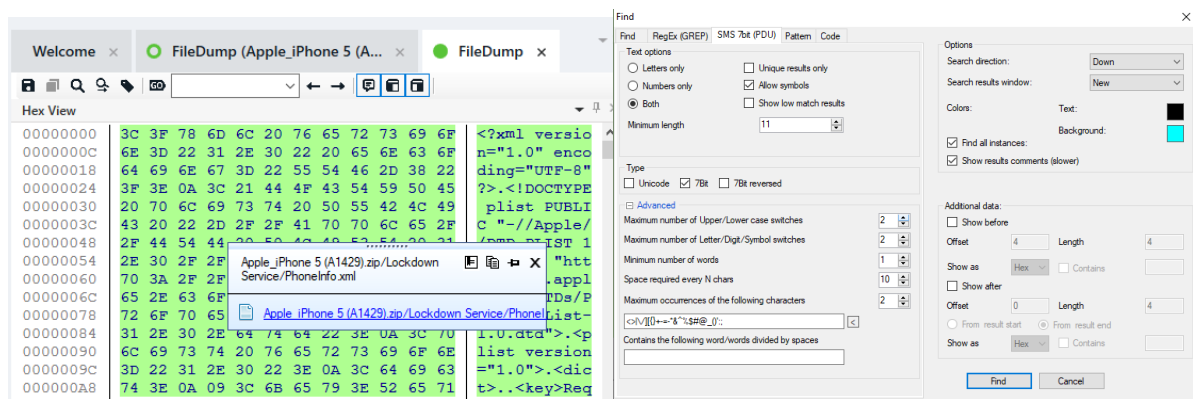


Figure 52: Searching from the HEX Pattern

## Insights View:

The insights View shows the Malware scanner. Which will show you the available Malware on this device

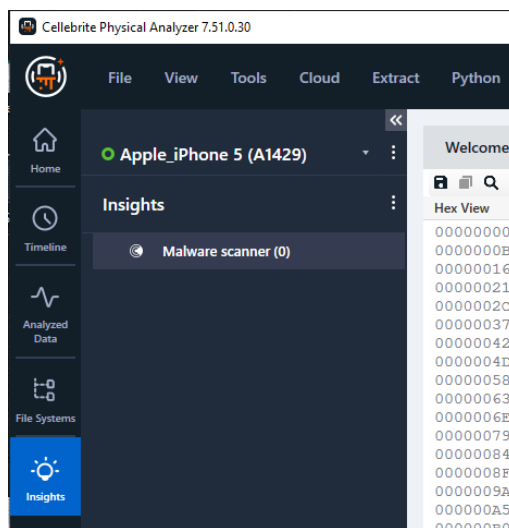


Figure 53: Insights View

In the menu bar click Tools, select Malware scanner > Update signature database. The following window appears.

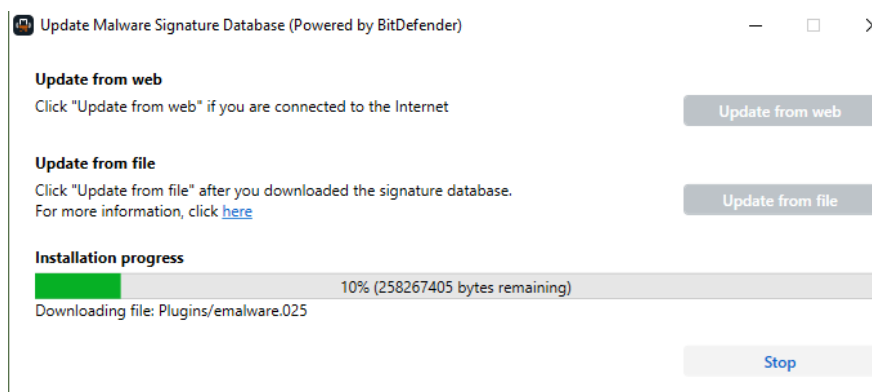


Figure 54: Updating the signature database



After completing this, run malware detection on this extraction to search for malware.

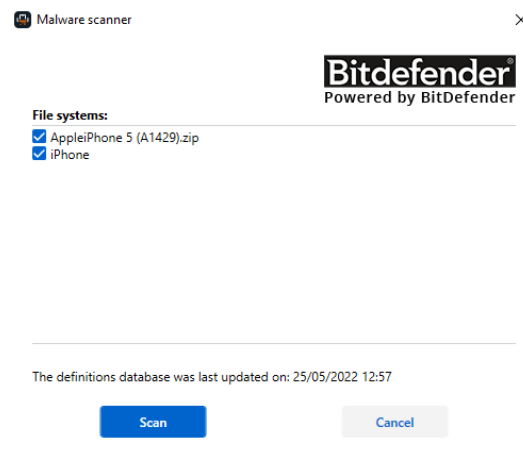


Figure 55: Malware Scanner

After successfully scanning the Malware we found **0 Issues**. The Trace window at the bottom of the data display area shows a log of the actions performed in session by Cellebrite Physical Analyzer

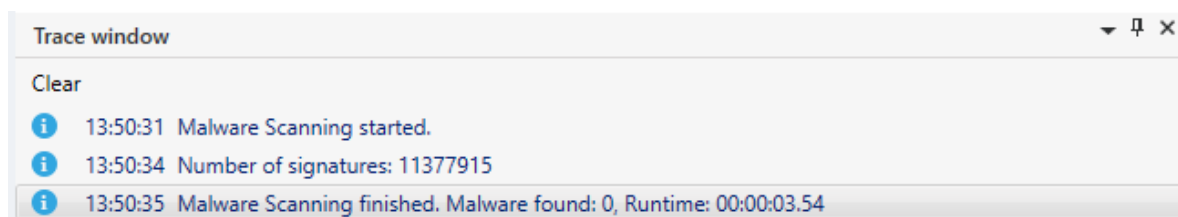


Figure 56: Trace Window of malware scanning

This trace windows shows the results & runtime of the scanning process.

**Report:** Generate the Report from the Home tab

### Reports View:

Since I had generated 1 report from my analysis. So, in the report tab it is showing only 1 report.



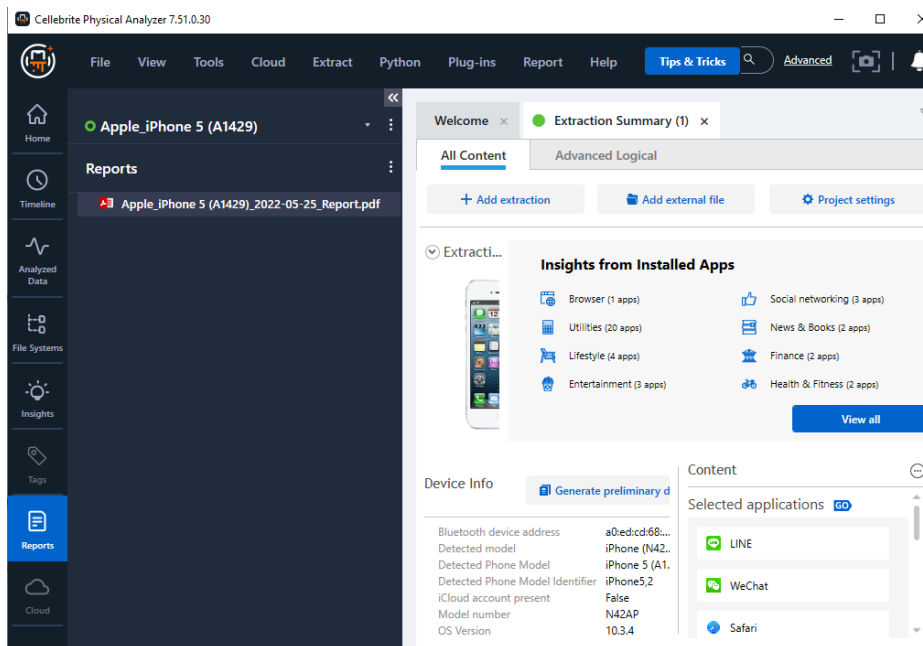


Figure 57: Reports tab View


Extraction Report - Apple iPhone	
	
Summary	
Cellebrite Physical Analyzer version	7.51.0.30
Report creation time	25/05/2022 12:25:57 +01:00
Time zone settings (UTC)	(UTC+00:00) London (Europe)
Report filter used	From: 01/05/2022 To: 25/05/2022
Examiner name	Shamili Mallela
Location	De Montfort University
Department	Cyber Security
Notes	Generating the Sample Report of this case for my Coursework
Source Extraction	
Advanced Logical - Selective apps decoding	
Extraction start date/time	07/03/2022 17:17:32
Extraction end date/time	07/03/2022 17:18:59
Unit identifier	1611330670
UFED version	7.52.0.152
Internal version	7.52.0.152
Selected manufacturer	Apple
Selected device name	iPhone 5 (A1429)
Machine name	DESKTOP-VIIGQHQ
Connection type	Cable No. 210
Is encrypted	Encrypted by Physical/Logical Analyzer during the extraction process for user credentials information
Backup password	1234
Extraction type	Advanced Logical
Extraction ID	3F78366D-6C25-442A-8130-CDDF671D9981
Extraction (UFED) file data integrity	Intact
Device Information	
Name	Value
Advanced Logical	
iPhone	
Detected Phone Model Identifier	iPhone5,2
Detected Phone Model	iPhone 5 (A1429)
OS Version	10.3.4
Serial	DNPKJCMGDTWD
Owner Name	iPhone
Unique ID	2c444e008939b5e819eaad3a382ec1d40d55865d
IMEI	013628003194639
MSISDN	+44 7469 198585
ICCID	89441000304138737925
Is encrypted	True
Phone Settings	

Figure 58: Extraction report

Here the summary report which was generated from the evidence. The extraction report gives you the Details of the evidence including source Extraction & Device Information

## Tags View:

The tag view is showing the 3 tags because in the filesystems I found 4 messages and contact from the analysed data. When analysing them I checked the hex values & tagged them.

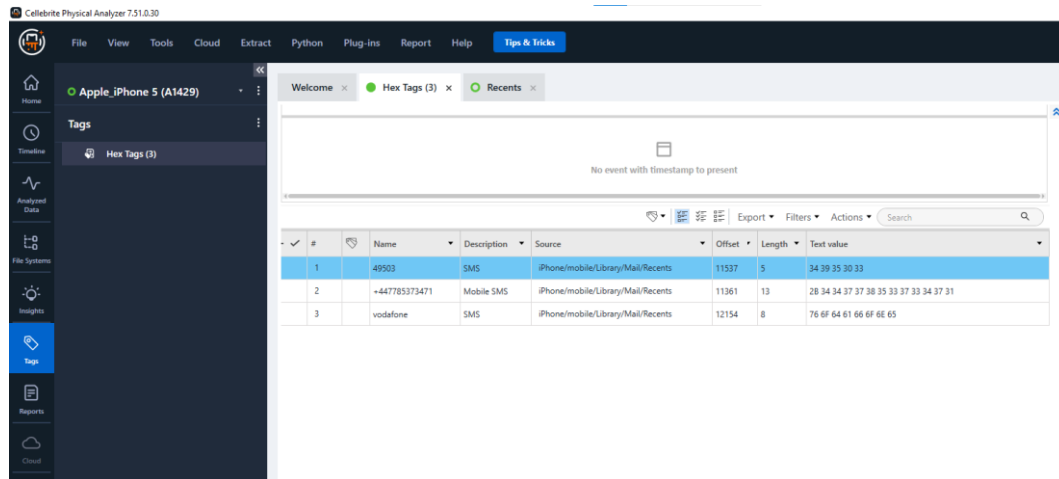


Figure 59:Tags View

## 5 Conclusion

### The facts from the forensic images I have analysed:

The digital space is fast-growing as attributed to the constant need for better communication, storage and collaboration in the world's global village scenario. This has also tagged along various misuse aspects hence the advent of digital forensic as the counter to the computer misuse scenarios. As illustrated, digital forensics is critical not only to reconstruct pieces of evidence in legal cases, it can also be used to recover lost data. Either way, digital forensic is an important aspect of the today's cyberspace for the named reasons. This concept is set to aid in the elimination of computer misuse cases. The investigation process as demonstrated is technical thus requires technical skills, in this essence, imaging is done on the target media (Xiao, Li and Xu 2019). The result can be Raw, E01 or dd. In this illustrations, E01 image formats are used as proprietary to enhance the integrity of the chain of custody. In most cases, E01 would require the examiner to create some sort of authentication by encryption normally implemented in MD5 hashes functions and algorithms.

## 6. Critical Reflection on My Learning Journey

1	What have you done to make this process better or worse for yourself?
<p>Success in any project is informed by how much planning and analysis is put into practice before launching the actual implementation process. Similarly, this investigation is approached from a planned and guided perspective from SANS framework. This entails different phases of SANS of incident response as far as incidents necessitating forensic examination are concerned. In this course (Sachdeva et.al 2020), the importance of digital forensics is clearly brought out in my learning module, the growing need for digital forensics in the society is attributed to the continued misuse of computer systems.</p>	
2	What would you do differently next time if you had to tackle a module like this?
<p>As illustrated, the investigation in this case is quite extensive, however, the lack of proper planning makes it look like a juggled investigation process with unclear phases and steps towards the attainment of the investigation goals. For this reason, I would focus on planning and layout out a clear-cut framework in which my investigation would be founded on, in this way, my investigation would be very procedural such that the readers would easily understand what steps have been taken just by reading the document. I would also give an explicit hypothesis on my allegations.</p>	
3	What did you think of the software you used during the module? Critically evaluate the software, its usefulness and usability.
<p>Whereas there are many digital forensics that can be used, it is certain that the respective tools do not provide similar usability, for this reason, my investigation is based on FTK imager. This is founded on the usability and best user experience from the user interface. FTK imager is quite straight forward with a navigation bar whose widgets are consistent with the functionalities as named. Unlike the command-line tools which require some extensive knowledge of the respective commands to be used in the investigation. This makes the tools exclusive to experienced experts.</p>	
4	What area of digital forensics did you find most interesting, or enjoy the most? Why?
<p>The investigation aspect to obtain the actual evidence is the most interesting part of the whole procedure. Personally, this is fascinating in that the end-result gives the actual evidence to either validate or invalidate the previous position. The fact that I, the examiner gets to dissect the image and obtain evidence that was hidden, deleted or was present in the digital media before the image was captured is just fun in itself, it also gives some sense of satisfaction to achieve this objective as it signifies some sort of success which everybody wants as I am convinced.</p>	
5	What area(s) do you need or want to develop further to be successful in digital forensics in the future?

The computer space is vast, digital forensics is just one of the many areas, in most cases, digital forensics goes hand-in-hand with computer networks, to become a successful forensic expert in this area, computer networks and security is my go-to. Computer networks and security contains aspects that are mostly investigated by digital forensics, an in-depth knowledge in this perspective would thus be critical in distinguishing one as a digital forensic expert (Årnes, 2017). It would also be vital to get some in-depth knowledge in the command-line tools and forensic tools to expand the portfolio.

6 | What could you do to help develop the area(s) you mentioned in question 5?

In this advancing technological world, it would help if one or me as a forensic expert would undertake extra seminar classes, workshops and training in security agencies, private firms specifically to advance skills in different tools including the CLI-driven tools. I would also undertake to train in computer networks and security as an additional to expand my knowledge and understanding in digital forensics. Personal efforts invested in these areas would make a big difference to position oneself as a top-notch digital forensic expert as I would desire.

## **Appendix A - References**

Harvard format used:

- i. Alhassan, J.K., Oguntoye, R.T., Misra, S., Adewumi, A., Maskeliūnas, R. and Damaševičius, R., 2018, January. Comparative evaluation of mobile forensic tools. In *International Conference on Information Technology & Systems* (pp. 105-114). Springer, Cham.
- ii. Akbal, E. and Dogan, S., 2018. Forensics Image Acquisition Process of Digital Evidence. *International Journal of Computer Network & Information Security*, 10(5).
- iii. Arshad, H., Jantan, A.B. and Abiodun, O.I., 2018. Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14(2), pp.346-376.
- iv. Årnes, A. ed., 2017. *Digital forensics*. John Wiley & Sons.
- v. Carew, R.M. and Errickson, D., 2019. Imaging in forensic science: five years on. *Journal of Forensic Radiology and Imaging*, 16, pp.24-33.
- vi. Mueller, M.L., 2020. Against sovereignty in cyberspace. *International Studies Review*, 22(4), pp.779-801.
- vii. Sachdeva, S., Raina, B.L. and Sharma, A., 2020. Analysis of digital forensic tools. *Journal of Computational and Theoretical Nanoscience*, 17(6), pp.2459-2467.
- viii. Xiao, J., Li, S. and Xu, Q., 2019. Video-based evidence analysis and extraction in digital forensic investigation. *IEEE Access*, 7, pp.55432-55442.

## **Appendix B – Title**

### **Content: Glossary**

#### **A**

Advanced logical extraction: An extraction method that combines both the logical and file system extractions into a single extraction method.

#### **C**

Carving: The process of finding data contained within the hexadecimal code, apart from what the forensic software has automatically offered. Carving can become necessary when the forensic tool parses data from unsupported apps, with deleted data including images, and other situations with file system and physical extractions.

Common/Known Image Filter: As part of the decoding process, UFED Physical Analyzer can calculate hash values of any extracted data file, particularly for media files. UFED Physical Analyzer automatically filters out common images.

#### **D**

Decoding: The process of translating raw hexadecimal data into an easily readable format. An automatic process within applications such as Physical Analyzer, decoding renders data easier for the examiner to find and analyse.

#### **L**

Location: Location data is drawn from different locations within the mobile device including Cell towers, WiFi networks, Harvested Cell towers, Harvested WiFi networks, Media locations, Favourites, Reminders, Home, Entered, TomTom, Foursquare, GpsFix, Recent, Frequent, Wireless networks

#### **P**

Physical/Logical Analyzer: An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

#### **S**

SQLite database A database file format often used for data storage. Commonly used storage of mobile and application data, but many smartphones may use .db. files, plists, and other file formats as well.

#### **T**

Tag: An investigator can apply a tag to flag events for future reference. Each event can have multiple tags. Tags can be included in reports or used for filtering.

#### **U**

Unallocated space: The area on a device's memory outside the defined file system that is available to write data to. Very often, deleted data or fragments can be found and carved from unallocated space.

## **Appendix C – Title**

Content:

<https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

<https://ijcsit.com/docs/Volume%206/vol6issue05/ijcsit20150605150.pdf>

<https://eforensicsmag.com/introduction-to-mobile-forensics/>

<https://www.forensicsware.com/blog/e01-file-format.html>

<https://dfprocedures.files.wordpress.com/2013/09/procedure-mounting-a-forensic-image.pdf>

<https://digitalmountain.com/newsletter/taking-the-first-step-data-preservation/>

[https://www.academia.edu/33376134/Step by step guide Live Image FTK.docx](https://www.academia.edu/33376134/Step_by_step_guide_Live_Image_FTK.docx)

<https://technewskb.com/mount-e01-encase-image-windows/>