

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Digital Forensics: Mobile Device Forensic Handling

Digital Forensics
(ACCA7031)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

- *This lecture is aligned with Cellebrite Certified Operator Certification.*

Talk to your Lecturer to book your Cellebrite Certification Exam



Cellebrite

Digital intelligence
for a safer world

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk





➤ **Mobile Device Forensics Handling**

Lab/ Tutorials

➤ **Handson Activity 6**

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

In continuation to our earlier lecture, we discussed about History of Digital Forensics and its attributes. Understood the importance of Incident Response and discussed about the principles of Digital Forensics, its process, different roles and finally getting to understand the technology's role in the crime and the law framed around it to prevent various crimes. We also discussed about various digital forensics capabilities and the appropriate method to acquire data. We looked at the challenges in acquiring data and the area in which keen attention is required. We further discussed digital evidences storage formats, Acquisition Methods, Contingency Planning for Data Acquisition, Use and Validate Data Acquisition, RAID Acquisition, Remote Network Acquisition and Forensic Tools used for Data Acquisition.

Earlier during our last lecture, we introduced Mobile Forensics, its scope and its architecture.





➤ *Mobile Device Forensics Handling*

Lab/ Tutorials

- *Handson Activity 6 will help you to review and identify, shield and isolate various and legally, ethically, handling the obstacles during acquisition.*

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

During this session, we will deep dive into four phases of examination process for digital devices, selecting appropriate tools, applying techniques required to document the forensic examination of Mobile Devices before, during and after the extraction.

Phases of Forensic Process

Locate, Identify, Seize

Forensic Acquisition

Analyze

Report



- + The Civil/ Criminal cases, will involve well-trained personnel to conduct the investigation. However, in a real time scenario: a mixture of trained and untrained helpers may interact with digital, physical evidences.
- + What would be the best to avoid this situation?

Phases of Forensic Process

Locate, Identify, Seize



Forensic Acquisition



Analyze



Report



+ Reports are critical

- Reports need to be developed based on the reader's needs and expectations.
- Accurately portray evidentiary findings
- Be well written and articulate
- Provide pertinent answers



- + Examiners and investigators must ensure they have the appropriate legal authority to seize and search for electronic devices.

Judicial Order Owner's Consent

- + What about examination of Cloud-based electronic data?
- + The law varies from jurisdiction to jurisdiction as to what can be accessed and how it can be accessed.



Discussion: If a warrant is issued. However, on close scrutiny, it only allows for a search for and seizure of the device, without providing authority for the actual examination of the device.

+ **Person giving consent,**

- + must have possessory rights over the device
- + Consent must be knowingly and voluntarily given
- + Person can restrict the areas to be searched
- + Rescind, revoke the consent any time

Discussion: What if, a person giving consent only to look in the SMS Messages, but not the Photos?



- + EU – GDPR is the body of law regarding data protection and privacy for all individuals within the EU and the EEA
- + Ensure that the examination is done in strict compliance with all applicable laws regarding search, seizure and the examination of electronic devices.
- + If a warrant is required, ensure the warrant provides sufficient legal authority for the examination.
- + Examiners are obliged to research the local laws to ensure they comply with the legal processes.
- + **Violations not only subject the evidence to intense judicial scrutiny but cast doubt upon the integrity of the examiner and the entire investigative process**



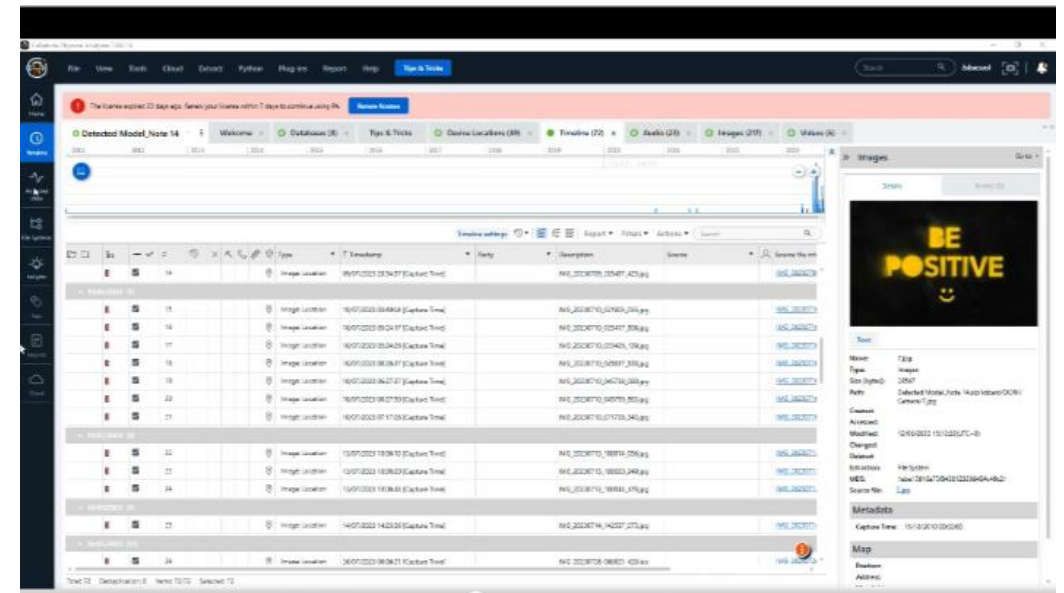
Documentation of evidence is critical to investigative integrity and establishing the chain of custody.

Document:

- + How was it located? Location
- + Where was it discovered? Identification
- + Possible investigative significance, Relationship of evidence

Methods

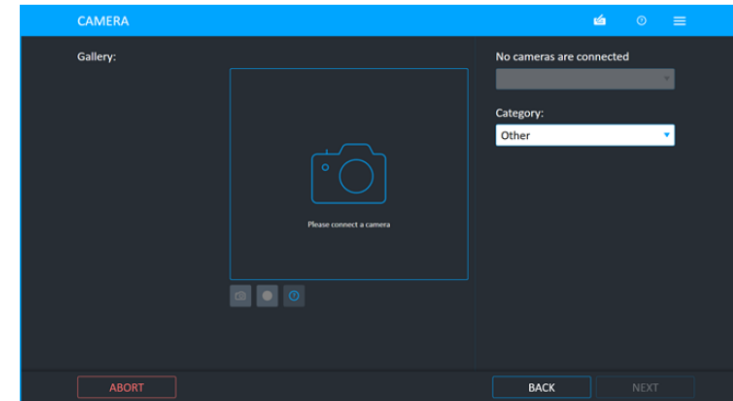
- + Reports and notes
- + Photographs and video
- + Sketching and mapping





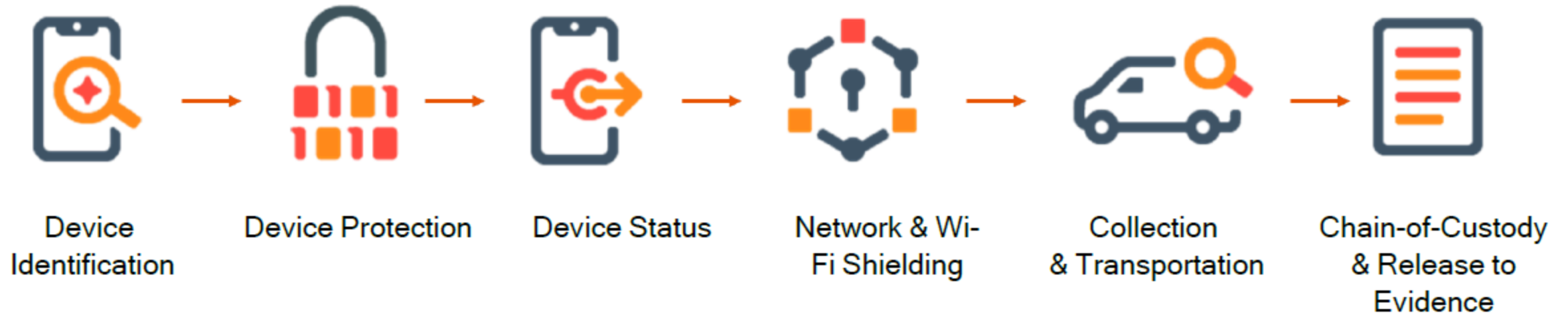
- + Examiner should understand the offenses and elements of proof
- + Physical, File System and Logical Extractions conducted whenever possible
- + Search/Documentation of pertinent evidence
- + Tagging pertinent evidence or items of interest

Tools like Cellebrite UFED 4PC together with UFED Camera will allow you to collect the evidence by taking pictures or videos of the device.



Evidence Handling

- + Take immediate steps to preserve the evidence
- + Consider legal authority
- + Maintain data integrity and admissibility of evidence
 - + Ensure Investigative integrity
 - + Evidence is not modified or destroyed
 - + Successful extraction of the device data



Evidence Handling

Identifying Devices

- + Make and Model of the device.
- + A critical component in ensuring validation of a search warrant.
- + Identifying Mobile Device is done prior to seizure and examination.
- + Challenging when the device is extremely damaged.
- + SD Cards

There are numerous reasons to ensure the mobile device has been properly identified:

Device Components /
Capabilities



Implementation of
Proper Shielding



The Existence of Additional
Evidence



Visual
Inspection



Evidence Handling

IMEI

- + The devices are identified by IMEI
- + They are Unique identification
- + They are hardcoded into the handset and broadcasted when during use of handset.
- + The first 8 digit are the type allocation code (TAC).
- + TAC will identify the Phone model.

Discussion: What can be determined by the investigator with the call records?

Evidence Handling

IMSI

- + GSM Subscriber Identification
- + Stored in the SIM Card
- + 15 Digit Number with
 - + MCC, MNC, MSIN

Discussion: What is the Phone Number?

- + The local area identity may be recovered from a SIM Card

	GSM	CDMA	SIM
Serial Number	IMEI	MEID	ICCID
Telephone Number	MSISDN	MDN	
Identifies Subscriber	IMSI	MIN	Stores IMSI

How do secure startup and screen locks impact the device identification?

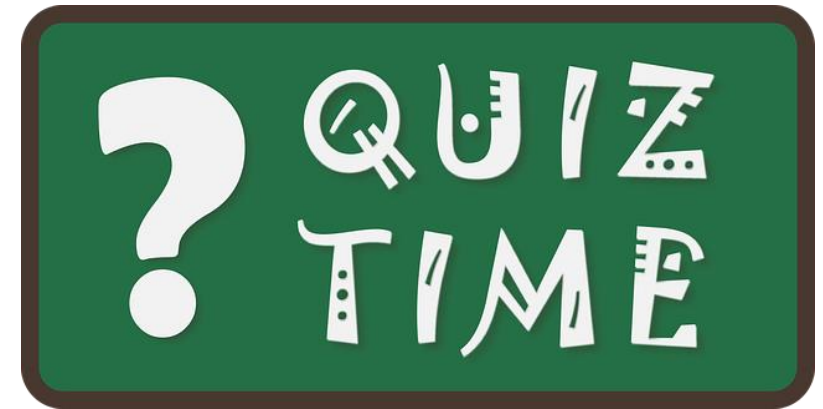
- a. They prevent access to the contents of a device
- b. They do not affect device identification
- c. They provide access to the device contents
- d. They can be used to retrieve device data

What does the IMSI provide in the device identification process?

- a. Visual identification of the device
- b. Device protection status
- c. Unique identification number of the device
- d. Unique identification of the user account

MSISDN is

- a. The device Identifier
- b. The Subscriber Identifier
- c. The Devices phone identifier
- d. The Network identifier



Task 1

You have been granted the legal authority to seize a device. When you have received the device, it was switched off. It is believed that the user of the phone is involved in several scamming in the community. The phone has a case and screen protector.

- + What are you confirming at this point?
- + What action will you take now?

Back in your workstation, after removing the protective case, you notice a worn-out sticker with the following information in addition to 256 GB, IMEI 1 and IMEI 2.

SM-A137F/DS

XT2245

SM-G998U

- + Use phonescoop.com and collect as much as information as possible

Task 1

SM-A137F/DS

XT2245

SM-G998U

- + What do the above letters refer to?
- + Storage Capacities?
- + Processor?
- + OS version?
- + Expandable Storage?
- + 5G Capable?
- + Type of connector?
- + How do you confirm if the details listed are for the same phone you investigate?

Evidence Handling

Protecting the Evidence

- + Shield/ Isolate the device from receiving and transmitting data
- + Remove SIM Card → Power Off → Place in a Faraday Bag

From what to protect?

- + Human Interference
- + Rain, Snow, Extreme Heat/Cold
- + Isolate from cellular, Bluetooth and Wi-Fi Connections

Discussion: What will you do to properly protect a device?

Evidence Handling

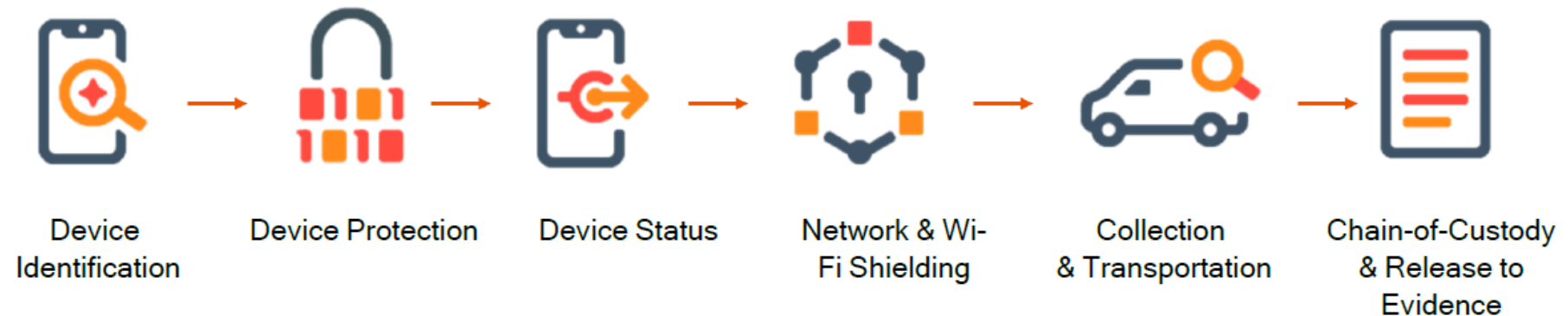
- + Isolate by enabling Airplane Mode.
- + What if?
 - + Wi-Fi or Bluetooth is not disabled in Airplane mode
 - + Wi-Fi turns on automatically upon restart
 - + Initialize USB Tethered connection
 - + Airplane mode cannot be enabled due to conditions like locked phone, no airplane mode etc
 - + FARADAY BAGS!!!
 - + You don't have FARADAY Bags?
 - + Inside Faraday bags, the device will continuously attempt to connect to the carrier. Will that affect the evidence?

Discussion: Why not power off the device?

Evidence Handling

Device Status

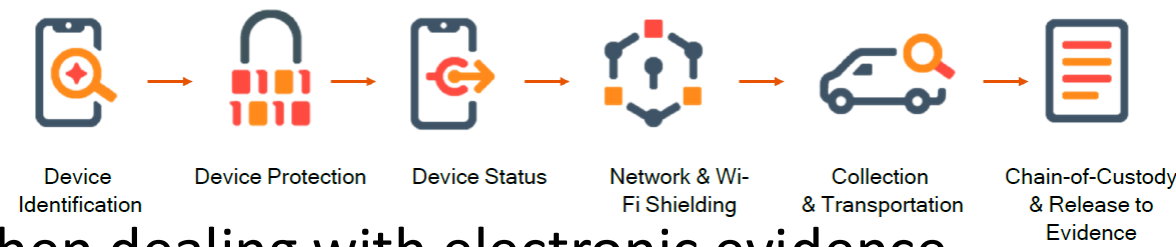
- + Determine whether the device is on or off.
- + If the device is powered off, there is no urgency, provided that the device is protected from environmental factors.
- + Immediate action must be taken regarding a device that is powered on.
- + A powered-on device must be placed in an isolated state to avoid remote intrusions or alterations to the integrity of the data on the device.



Evidence Handling

Evidence Issues

- + Environmental factors present unique issues when dealing with electronic evidence.
- + Examiners should not overlook the presence of other physical evidence.
- + When handling and processing mobile devices, it is not uncommon to encounter trace hair, Fiber, blood, or other body fluids, which could contain valuable DNA evidence.
- + In these instances, care should be taken to protect the physical evidence from alteration or destruction.



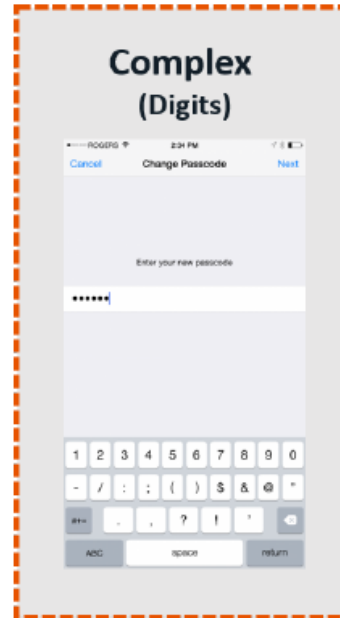
Discussion Point

- Implementation of encryption in devices has a huge impact unlocking and the extraction ability.
- Do a quick search on the following and discuss within your class and present your understanding:
 - After First Unlock (AFU)
 - Before First Unlock (BFU)
 - Brute Forcing
 - FDE (Full Disk Encryption)
 - FBE (File Based Encryption)



Evidence Handling

Locks



Face Lock



Fingerprint



Voice Recognition



Knock Pattern



Smart Location



Iris Scan



PIN/Password and Pattern Lock



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

Evidence Extraction



Logical

Advanced Logical

File System

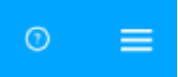
Full File System

Physical Read

Other Areas

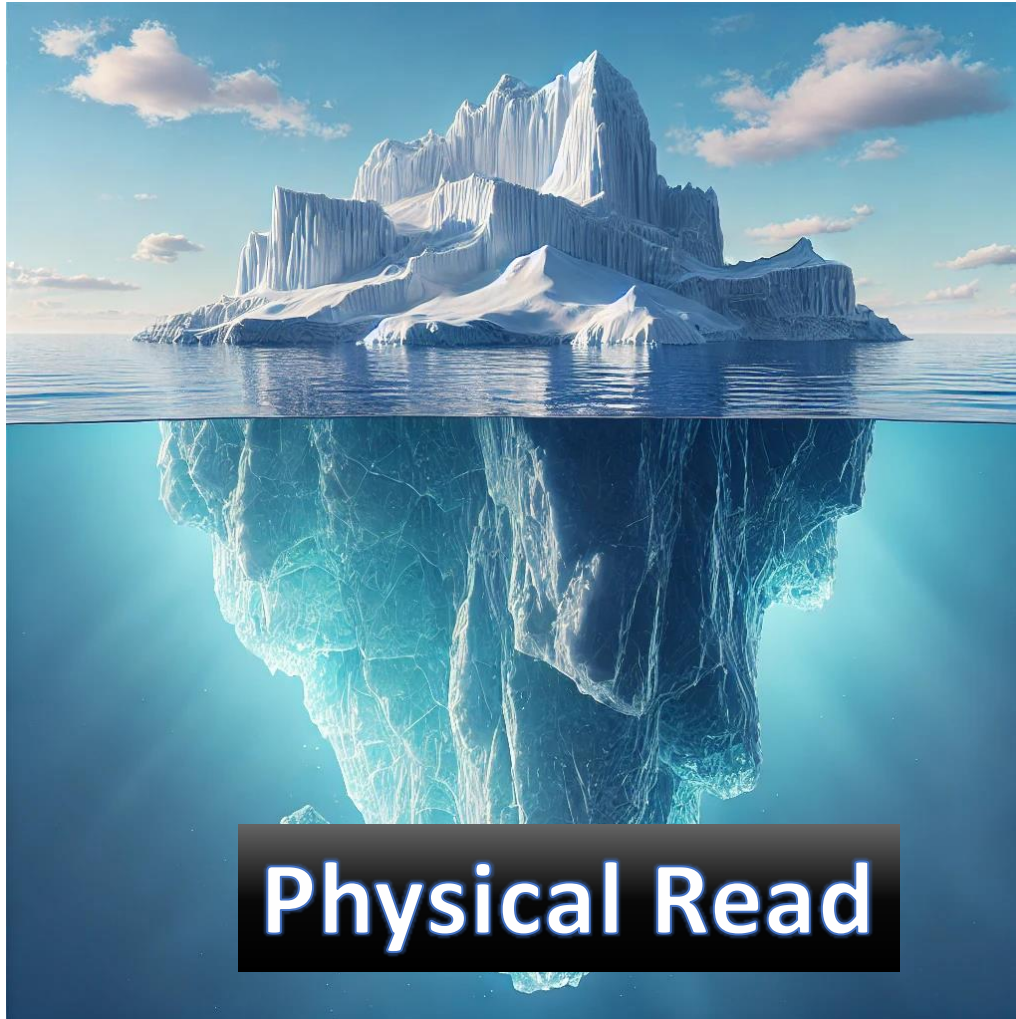
Task 2

Working with UFED 4PC

1. Open Cellebrite UFED 4PC (On top of the App, click on the 3 Lines  and navigate to settings.
 - + Always confirm the date and time settings before each use of the tool.
 - + Navigate to General, Reports, System, License, Version, Activity Log and User Permissions
2. Take screenshots of EACH setup and write a brief note about each options and submit in Moodle.

Discussion: Have you noticed Android Backup APK Downgrade? What is it?

Evidence Extraction



- SMS
- Contacts
- Call Logs
- Audio
- Files
- Hidden Files
- Deleted Files
- Deleted Data

Physical

Task 3 Extract with UFED 4PC

1. Open Cellebrite UFED 4PC (*Ensure the licenses are updated and active*)
2. Click on Mobile Device. Skip when it asks for Connect phone to Auto Detect
3. Manually select the Phone you want to Extract
4. Select Physical Extraction to extract information like Device File System, Deleted Information, Hidden Files, Unallocated Space, User Data, Select the Physical Extraction Type
5. Select the Extraction Location Type
6. Verify, if the USB Debugging is enabled and Continue
7. Once the extraction is completed, open with UFED Physical Analyser

Attention

Verify that USB Debugging is enabled on the source device and then press Continue. If USB Debugging cannot be verified press Abort.

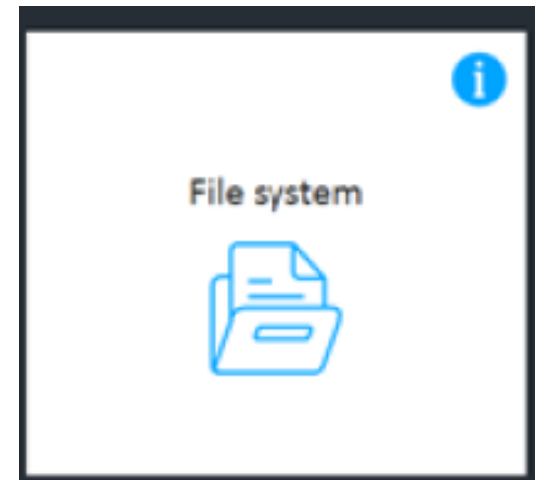
ABORT

CONTINUE

EXTRACTION IN PROGRESS

Task 4 Extract with UFED 4PC

1. Completely power cycle the device used in previous activity before beginning this activity
2. Open Cellebrite UFED 4PC (*Ensure the licenses are updated and active*)
3. Click on Mobile Device. Skip when it asks for Connect phone to Auto Detect
4. Manually select the Phone you want to Extract
5. Select File System Extraction to extract information like Application Data, Files (Internal Files, File System, All accessible Files)
6. Select Android Backup
7. Select the Extraction Location Type
8. Follow Instructions from UFED 4PC



Task 4 Extract with UFED 4PC

1. Completely power cycle the device used in previous activity before beginning this activity
2. Open Cellebrite UFED 4PC (*Ensure the licenses are updated and active*)
3. Click on Mobile Device. Skip when it asks for Connect phone to Auto Detect
4. Manually select the Phone you want to Extract
5. Select Advanced Logical Extraction to extract information like Audio, Images, Ringtones, Video Folders
6. Check if: Enable Developer Options, USB Debugging and Stay Awake Options are enabled.

Device Tools

Android Debug Console:

This tool uses Android Debug Bridge (ADB) and requires that the "USB Debugging" mode is enabled.

To use this tool:

1. Go to the device settings > About/Information > tap the "Build number" 7 times. A message is displayed that you're now a developer.
2. Go back to the Developer options menu, select "USB debugging" and "Stay awake" (if available).
3. Approve the "Allow USB debugging" connection to the computer by selecting "Always allow".

OK

In the absence of a Developers Options choice, look for **About phone** or **About tablet**.

Scroll to the bottom of the menu and locate the **Build Number** field.

Tapping the **Build Number** field seven times should enable Developer Options.

Exit the About menu and select Developer Options.

In the Developer Options menu scroll to the **USB Debugging** entry and place a check in the box.

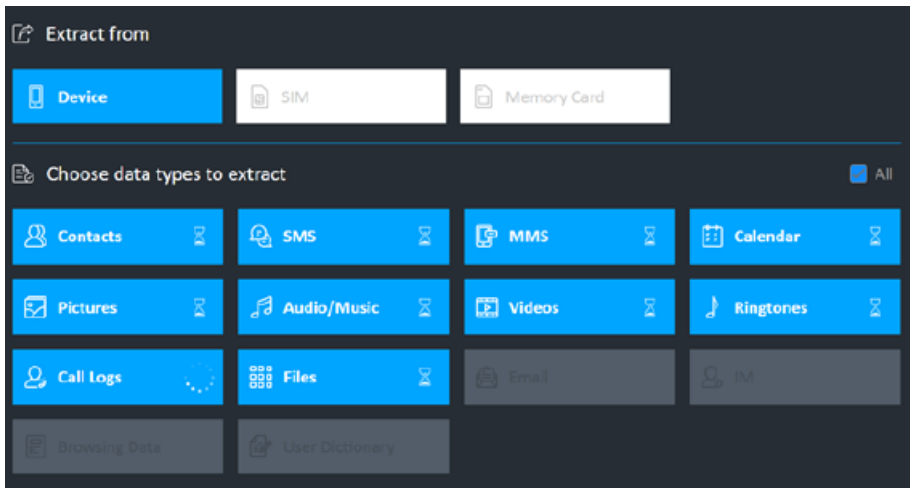
Task 4 Extract with UFED 4PC

Advanced Logical Extraction

The Advanced logical extraction uses other extraction protocols and can potentially extract additional data compared to the standard logical extraction.

A quick extraction method that supports the largest number of devices. The data types that can be extracted from a source device include: Call logs, phone books, SMSs, calendar events, multimedia files (images, videos, audio), and apps data.

The available types of extracted data may vary depending on the source device make and model. In most cases, a logical extraction is not possible for locked devices.

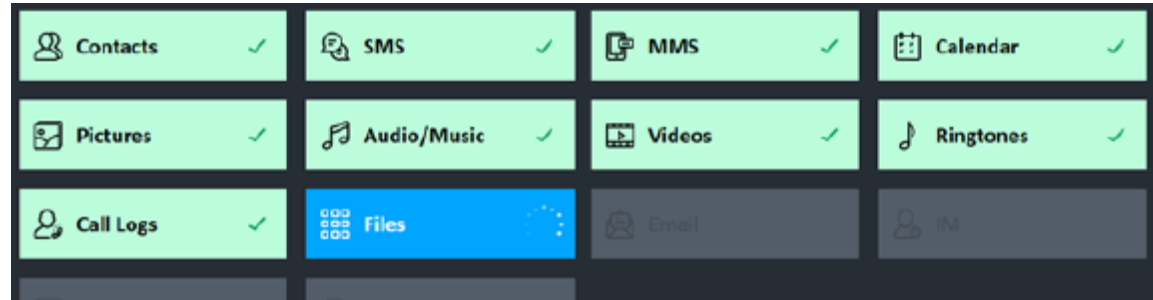


Warning

The following content types may require a device restart during the extraction process:
Files.
Select "Continue" to continue with the extraction.
Select "Exclude content" and avoid a device restart during the extraction.

EXCLUDE CONTENT

CONTINUE



Extraction

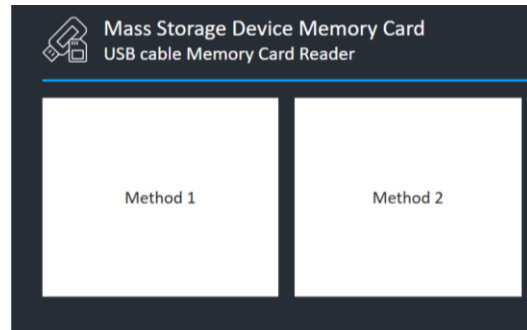
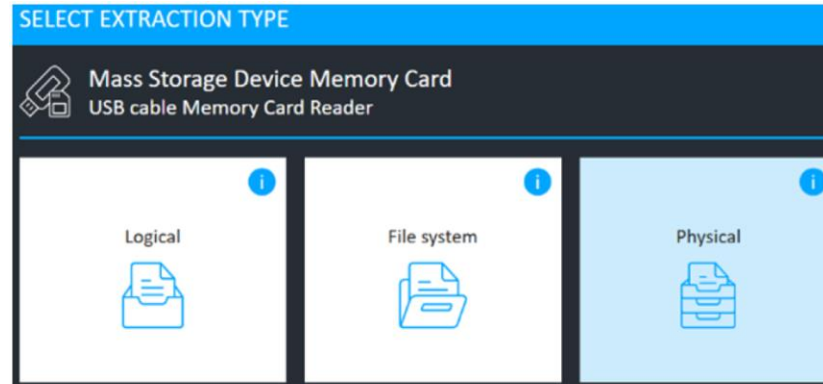
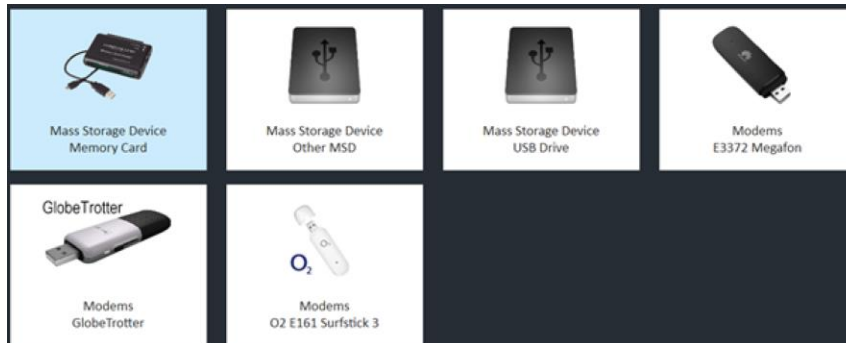
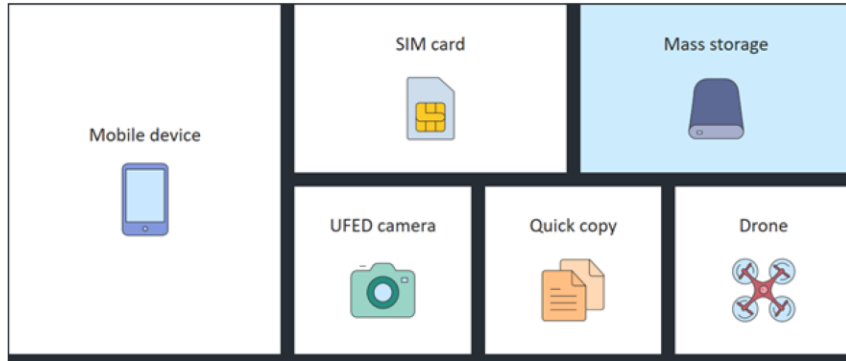
Advanced Extraction Techniques

- + Extract Data stored in the memory of electronic devices
- + Requires unique software, hardware and advanced skills to complete.

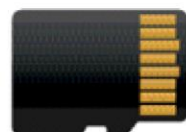
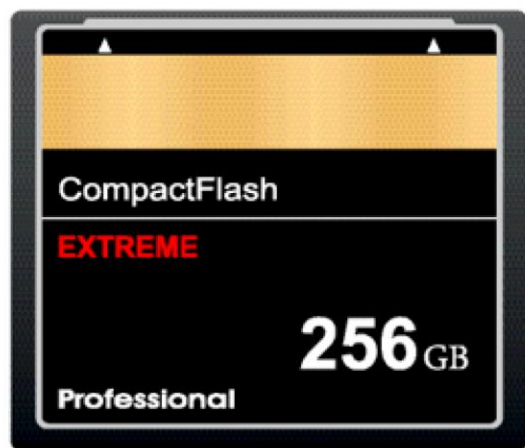
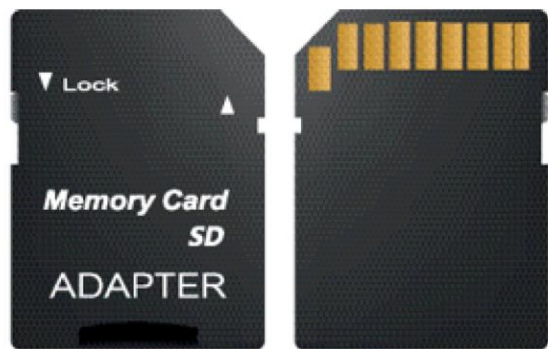
Task 5 Ensure Integrity

1. Record the hash value created at the time of extraction
2. Record the hash value verification
3. Record the hash value of all extractions using a third-party tool

Task 6 Storage: Physical and Logical



SIM



SDXC
host device



SDXC card
64GB - 2TB



SDHC card
4GB - 32GB



SD card
2GB and less



SDHC
host device



SDHC card
4GB - 32GB



SD card
2GB and less

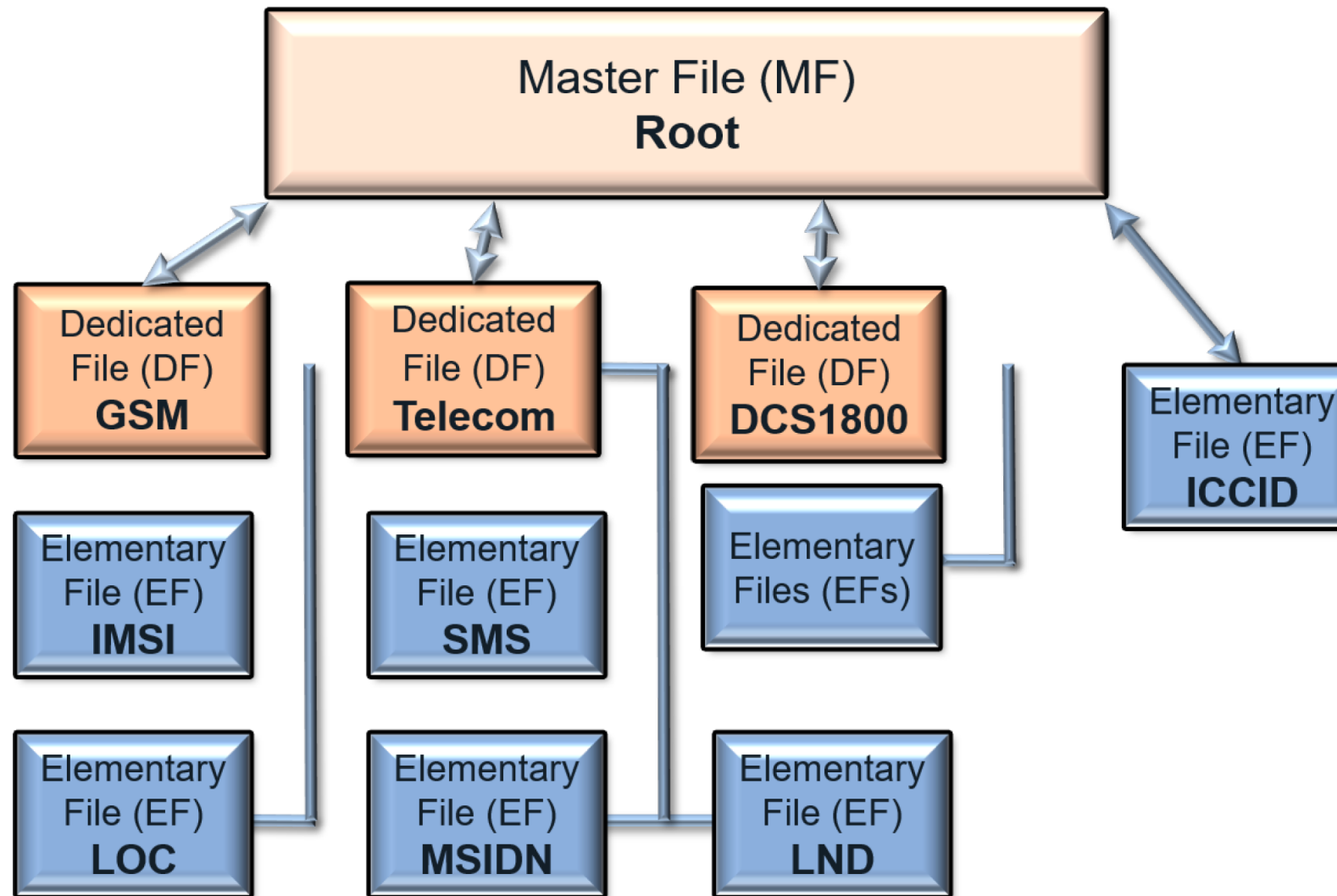


SD
host device

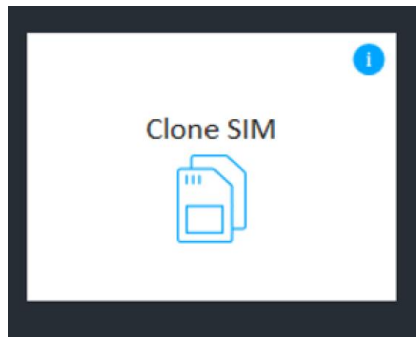
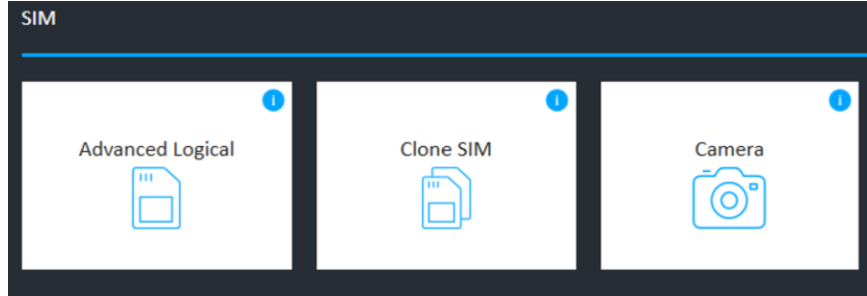


SD card
2GB and less





SIM



- Backup 2022_03_20 (001).clog
- Logical.ufd
- Report.html
- Report.xml
- Report_CallLogsSection.html
- Report_ContactsSection.html
- Report_SMSSection.html

Purpose



Produce a Cellular Network Isolation Card (CNIC)

How



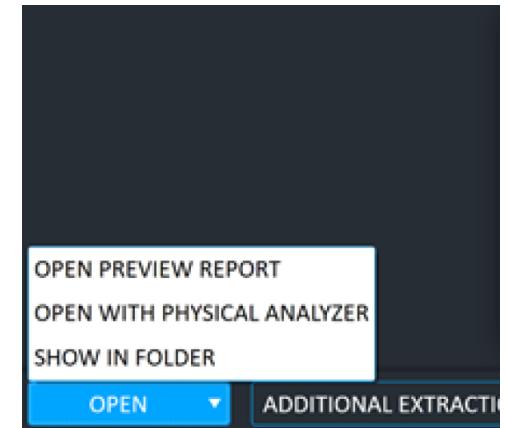
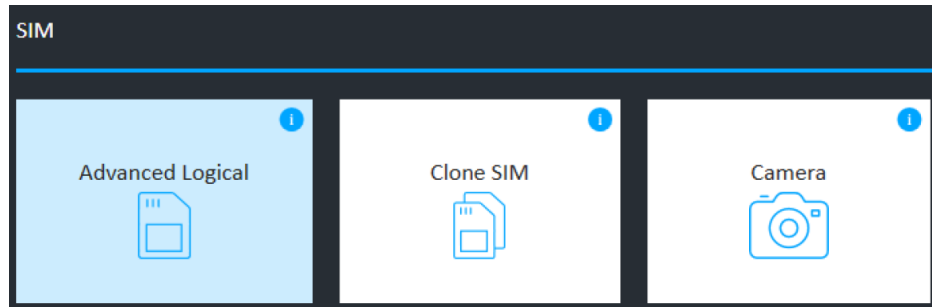
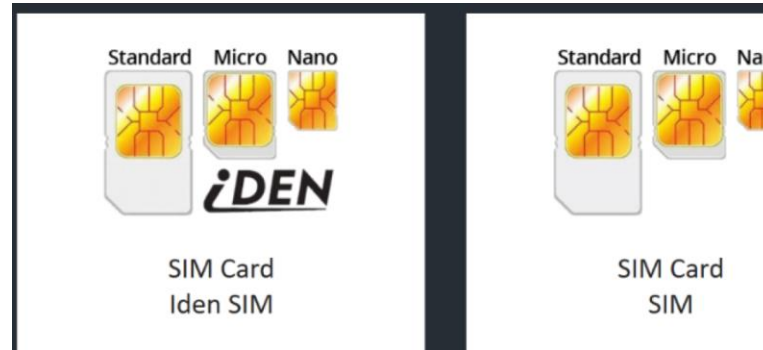
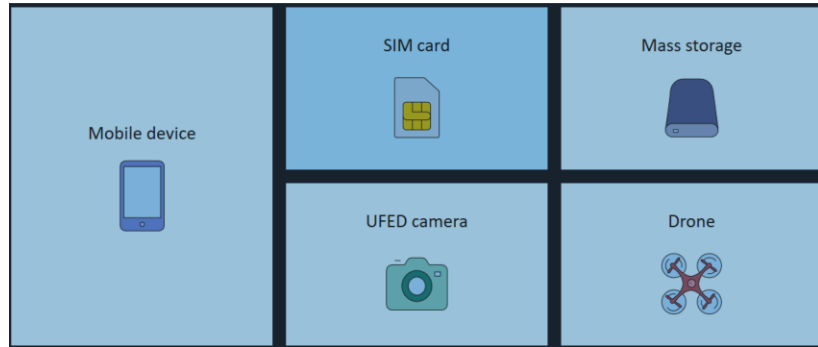
Copies a subset of data from the SIM to the CNIC

Benefit



Allows mobile devices to function without connecting to a cellular network

Task 7 SIM Extraction



Task 8 SIM Clone

1. From the Home screen, select **SIM Card**.
2. On the next screen, SELECT SIM, choose **SIM Card SIM**.
3. From the SELECT EXTRACTION TYPE, press **Clone SIM**.
4. Insert the SIM card into the slot on the MultiSIM adapter (as indicated), with the card contacts facing down and the clipped corner facing out. The SIM card should be inserted up to the stopper point, without applying pressure.
5. Select **CONTINUE**.
6. The screen SELECT SOURCE appears. Choose "**Clone an existing SIM card**".
7. You will receive the following message: "Insert Source SIM into the UFED Device Adapter with the SIM card's contacts facing down and the clipped corner pointing toward you", which should have been done in Step 4. Press **CONTINUE**.
8. After UFED 4PC has completed reading the SOURCE SIM card, a message will appear to insert the TARGET card. ****NOTE: Failure to remove the SOURCE SIM card prior to pressing CONTINUE will result in ERASING the SOURCE SIM****
9. After removing the SOURCE SIM card, insert the TARGET CNIC card provided by the instructor and press **continue**.

Task 9 Compare and Contrast SIM Extraction and Cloning

1. Do a SIM Extraction and SIM Clone
2. Analyse both the data and come with a Comparison.
3. The comparison is expected to be in a Tabulated format.

A sample is given here. Your comparison is expected like this with more features

		1	2
		AT&T SIM Card	Cloned AT&T SIM Card
1	Extraction start date/time:	25/09/2018 18:27:28 (GMT-5)	25/09/2018 18:25:30 (GMT-5)
2	Extraction end date/time:	25/09/2018 18:29:44 (GMT-5)	25/09/2018 18:25:53 (GMT-5)
3	ICCID:	89014104275850066794	89014104275850066794
4	IMSI:	310410585006679	310410585006679
5	SPN:	N/A	N/A

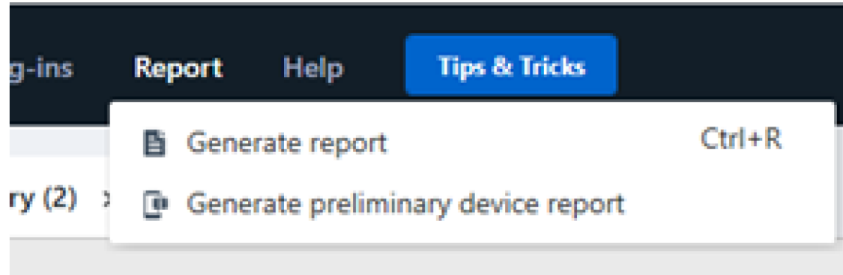
Task 10: Report

10.1

1. Launch Physical Analyzer.
2. From the Application Menu bar, select **File > Open Case**.
3. From Case Wizard screen select **Add > Load Extraction**.
4. Navigate to the Desktop and select the .ufd file associated with the Physical extraction conducted on the Android device provided by the instructor.
5. Repeat Step 4 for the remaining associated extractions for this device (Files System & Advanced Logical) to include the SIM card and Micro SD card extractions.
6. Select **Next** (lower right corner of the Case Wizard screen).
7. Select **Examine Data** (lower right corner of the Case Wizard screen).

Task 10: Report

- 10.2 1. Select **Generate Report** from the **Report** tab in Cellebrite Reader.



2. Name the report **The Investigation**.
3. Select the **Browse** button and save the report to the Desktop.
4. Type **The InvestigationReader Report** in the **Report sub-directory** field.
5. Click the **Browse** button and save the report to the **Desktop**.
6. Select the drop-down for **Format**. Notice the various formats available.
7. Select the box for **UFDR**.

Format

UFDR (For Cellebrite Reader or Cellebrite Pathfinder)

Case Information

8. Type the case information relevant to the case in the fields provided. Select **Next**.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

Digital Forensics
(ACCA7031)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- CCO - Cellebrite Certified Operator Participant Guide

Digital Forensics
(ACCA7031)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk