A technical look at Phone Extraction

Police officers who operate mobile phone extraction technologies often have little or no forensic training and are increasingly reliant on devices whose capabilities they do not understand, particularly as budgets are cut and the volume of data they have to cope with increases.

In this piece we examine mobile phone extraction, relying on publicly available information and Privacy International's experience from conducting mobile phone extraction using a Cellebrite UFED Touch 2. We welcome input from experts in the field. This is a rapidly developing area. Just as new security features are announced for phones, so too new methods to extract data are found.

General explanation of mobile phone extraction

Mobile Phone Extraction technologies, known also as mobile forensics, entails the physical connection of the mobile device that is to be analysed and a device that extracts, analyses and presents the data contained on the phone. Whilst forensics experts, hackers and those selling spyware[i] may be able to access and extract data, we look at a number of the most well-known commercial companies who sell their products to law enforcement, such as Cellebrite, Oxygen Forensic Detective, and MSAB[ii].

Android and iOS

Our analysis focuses on Android and iOS when looking at extractive technologies. Android is the leading operating system for phones worldwide.[iii] *"According to IDC, in the first quarter of 2017, Android dominated the industry with an 85% market share."*[iv] iOS leads the way in relation to security and presents the biggest forensic challenge. *"...without the passcode we can hardly extract anything from the modern iOS device."*[v] For example iOS's USB restricted mode, which first appeared in iOS 11.4.1[vi], disabled USB communications after one hour of the last unlock which causes issues of those conducting an extraction. As USB restricted mode develops with iOS releases[vii], for many in the world of forensics it is simply a challenge to overcome[viii]. Mobile phone extraction could be characterised as an arms race, where vendors are constantly seeking to overcome obstacles of increased phone security.

> *"We want to start with the bad news: if you are examining an iPhone that runs iOS 8 or newer … chances to unlock it are not good at all...With iOS 11 this problem becomes even more severe - even if the device under examination is not passcode-protected, the examiner will need the passcode anyway as it must be entered to confirm the trust between the device and your workstation."*[ix]

An important differentiator between iOS and Android in terms of forensics capabilities is that whilst Apple can push updates directly to their users, patching vulnerabilities and exploits, Android users are predominantly reliant on the manufacturer and carrier to provide update. This causes many Android phones to be running older versions of the operating systems which means various forms of extraction are viable[x]. *"The variety of the operating system versions and the hardware platforms on which they are used provide a wide range of data extraction methods. "*[xi]

Vulnerabilities

In evaluating MPE technologies, this project looks at some of the vulnerabilities used to obtain data, particularly for Android phones, such as the use of Emergency Download Mode for devices with the Qualcomm chipset.

Vulnerabilities

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved

Figure 1: Extract from Cellebrite Webinar[xii]

Table of Contents

What current technologies are used to access, extract and analyse data from mobile phones?

Context

> *"Mobile device forensics is likely the most rapidly advancing discipline that digital forensics has ever seen or ever will see, primarily because of the rapidly changing environment of the actual devices. Device operating systems have become more advanced, and the storage capacity on the current devices is astronomical. Today's devices are mobile computing platforms, but accessing the data contained on these devices is much more difficult than accessing data from any other digital device."*[xiii]

Accessing and extracting data from phones is nothing new. However, as the volume of data[xiv] on phones explodes and *"the mobile landscape is changing each passing day"* the ability to access, extract and analyse this data is increasingly difficult and complex. Techniques vary depending on the hardware and software of a phone, from the chipset (Qualcomm, MediaTek) to the operating system version. *"Extracting data from a mobile device is half the battle. The operating system, security features, and type of smartphone will determine the amount of access you have to the data."*[xv]

Encryption and other security measures present significant challenges[xvi].

> *"As mobile technology continues to mature, and the amount security and encryption continues to strengthen, it's becoming more of a challenge to know how to access data on smartphones that are password-protected. On top of the encryption challenge is the manufacturing variants that can create different roadblocks along the way."*[xvii]

There are three generic types of extraction: logical, file system and physical, which provide a framework to consider extraction technologies. No one technology can access and extract all data from all phones, and no one type of extraction is guaranteed to be successful. As acknowledged by MobilEdit, a phone forensics company, when commenting on the US National Institute of Standards and Technology (NIST) test results for mobile device acquisition[xviii]:

> *"Tests have also shown that there are significant differences in results between individual data types across the competitive*

> *tools tested. Each tool was able to demonstrate certain strengths over the others, and there is no single tool that demonstrated superiority in all testing categories. Our conclusion is that there is a significant increase in the success rate when performing a cross-reference tool analysis. In the real world, when there is a case, each piece of evidence matters. With a combination of tools you can get up to 89.6% overall success rate.”*[xix]

Physical acquisition is generally the preferred method. As it extracts the raw data at a binary level, from the devices storage (see Figure 2). Even if this is possible there is a view that *“A logical acquisition should always be obtained as it may contain only the parsed data and provide pointers to examine the raw memory image.”*[xx]

Factors such as the status of the mobile device will determine whether logical or physical extraction is attempted. *“The type of examination is contingent on the device’s power status and whether the device is locked, password protected, or disabled (disassembled or broken) ...Not all mobile devices can be collected physically. An iPhone 5 to X, for example, cannot be collected physically using non-invasive methods.”*[xxi]

The reality of carrying out mobile phone extraction is that you will often have to try all types of extraction that the tool you have offers. However, the ability to do this will be limited by time, resources and expertise.

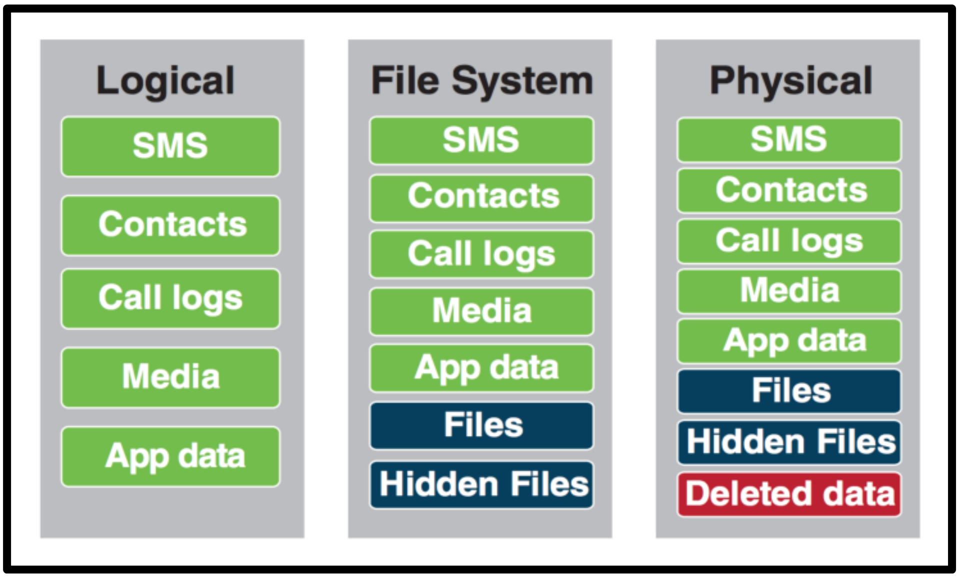
A developing area is Cloud extraction which we look at in more detail in a separate article. This development makes for disturbing reading, as we grasp how much is held in remote servers and accessible to those with no forensic skill but the money to pay for push button technologies that can grab it all. Cloud extraction, a leap from what is on the phone to what is accessible from it, is a reaction to encryption and device locks that make traditional mobile phone forensics hard if not impossible and a response to the volume of information stored in the Cloud.

“Today’s digital investigators should not ignore the significance of the data stored in various cloud services. Without cloud data, the information that can be gathered from traditional sources (such as mobile device, flash media, or computer) is limited, inconclusive, or simply unobtainable.”[xxii]

Once data is extracted there are some impressive products on offer to read and analyse extracted data. Increasingly these are marketed with artificial intelligence capabilities to assist investigators.

Analysis: Access & extraction: physical, logical, file system

First an analysis of the three main types of extraction: logical, file system and physical and the tools used to carry these out. These methods vary in technicality and the type and volume of data they can extract.



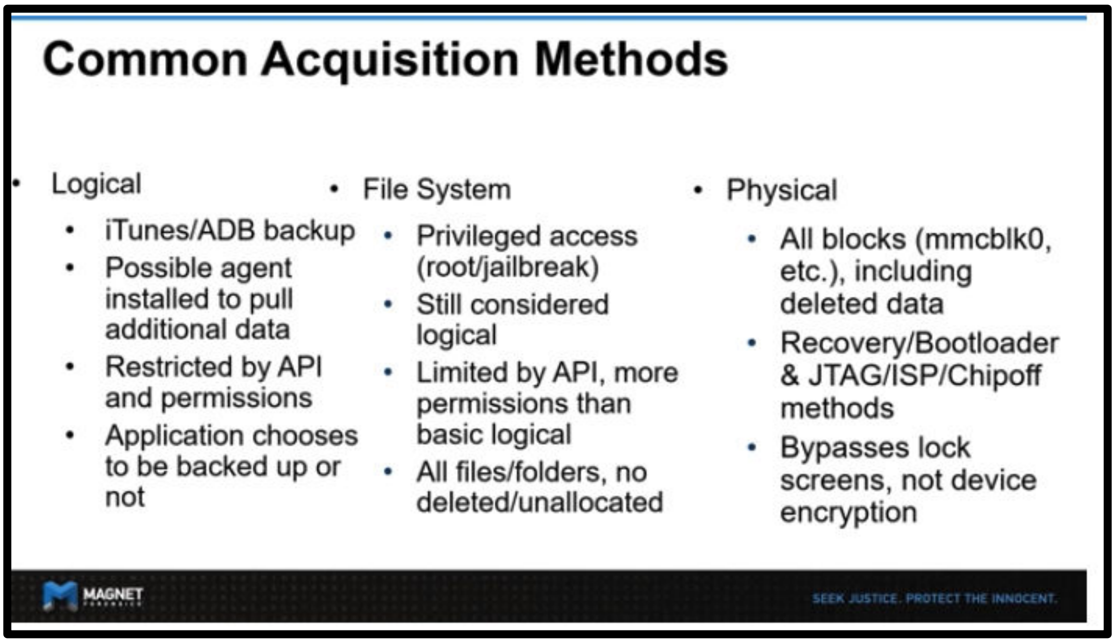
Logical
- SMS
- Contacts
- Call logs
- Media
- App data

File System
- SMS
- Contacts
- Call logs
- Media
- App data
- Files
- Hidden Files

Physical
- SMS
- Contacts
- Call logs
- Media
- App data
- Files
- Hidden Files
- Deleted data

Figure 2: Summary of types of data that can be extracted using logical, file system and physical extraction[xxiii]

Under each generic method, companies may differ on the way they achieve the extraction. As set out in a slide from Magnet Forensics (Figure 3), a logical extraction can be achieved via iTunes/ADB backup or installing an agent to pull additional data; a File System using privileged access such as root or jailbreak; and Physical using recovery or bootloader methods.



Common Acquisition Methods

- Logical
  - iTunes/ADB backup
  - Possible agent installed to pull additional data
  - Restricted by API and permissions
  - Application chooses to be backed up or not
- File System
  - Privileged access (root/jailbreak)
  - Still considered logical
  - Limited by API, more permissions than basic logical
  - All files/folders, no deleted/unallocated
- Physical
  - All blocks (mmcblk0, etc.), including deleted data
  - Recovery/Bootloader & JTAG/ISP/Chipoff methods
  - Bypasses lock screens, not device encryption

MAGNET FORENSICS

SEEK JUSTICE. PROTECT THE INNOCENT.

Figure 3: Common Acquisition Methods[xxiv]

There are other invasive methods to extract data from phones. JTAG (Joint Test Action Group), ISP (In System Programming) and Chip-off (or any associated hardware forensic methodology, such as inter-chip communication interception - If you are dismantling the device, you may be able to intercept the data as it travels from one microcontroller to another/processor, for example I2C or SPI, bypassing a software defined security model) are more reliant on forensics skill as opposed to the newest technology and thus are mentioned briefly.

JTAG is a method named after the industry standard for verifying designs and testing printed circuit boards after manufacture. It involves connecting to the Standard Test Port to transfer raw data from memory chips. *"The JTAG technique involves probing the JTAG Test Access Ports and soldering connectors to the JTAG ports in order to read data from the device memory."*[xxv] ISP *"is the practice of connecting to an eMMC or eMCP flash memory chip for the purpose of downloading a device's complete memory content"*[xxvi]. Chip-off is a destructive method, which is based on the removing of memory chip from system board and a chip reader is used to extract data stored.[xxvii]

Finally, manual extraction which does not require sophisticated tools and:

> *"...involves simply scrolling through the data on the device and viewing the data on the phone directly through the use of the device's keypad or touchscreen. The information discovered is then photographically documented... At this level, it is not possible to recover deleted information and grab all the data. "*[xxviii]

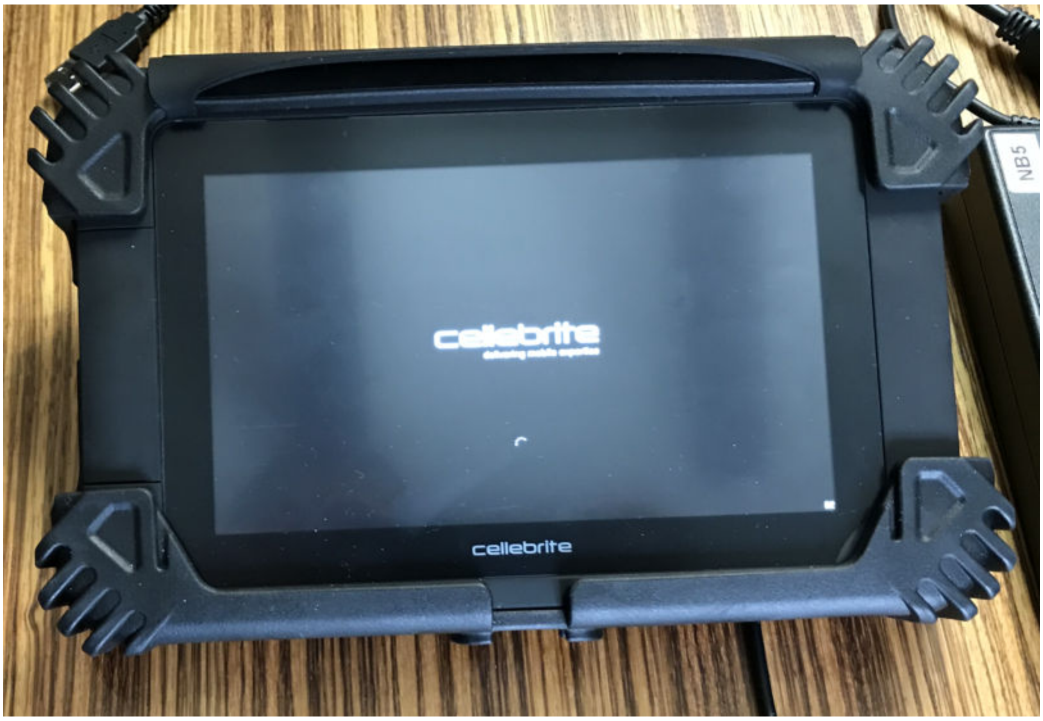


Figure 4: Cellebrite UFED Touch 2

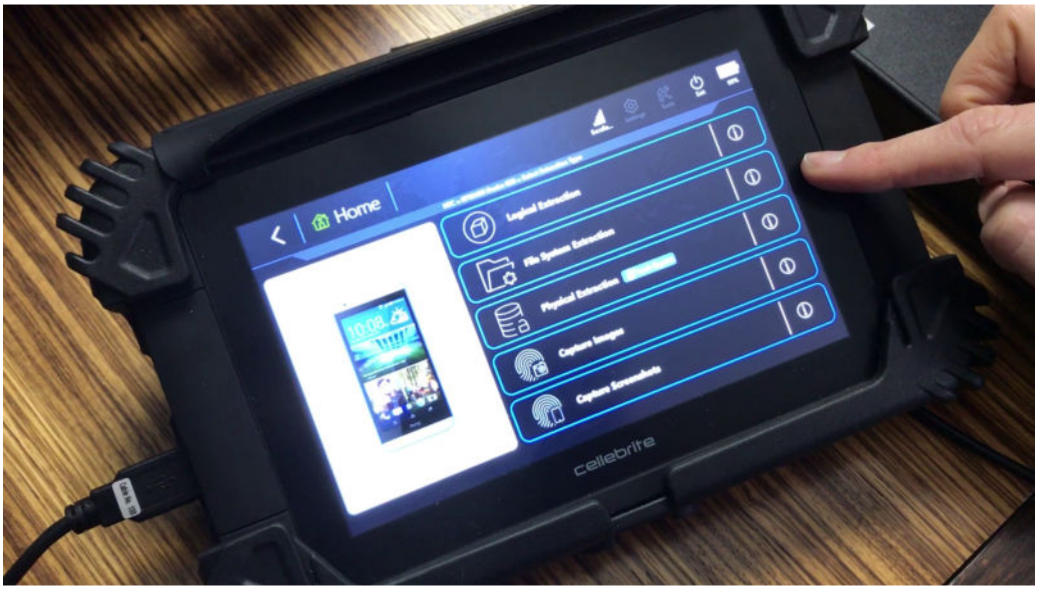


Figure 5: Cellebrite UFED Touch 2 options

Logical extraction

> *“Logical acquisition is about extracting the logical storage objects, such as files and directories that reside on the filesystem. Logical acquisition of mobile phones is performed using the device manufacturer application programming interface to synchronize the phone’s contents with a computer. Many of the forensic tools perform a logical acquisition...A logical acquisition is easy to perform and only recovers the files on a mobile phone and does not recover data contained in unallocated space. “*[xxix]

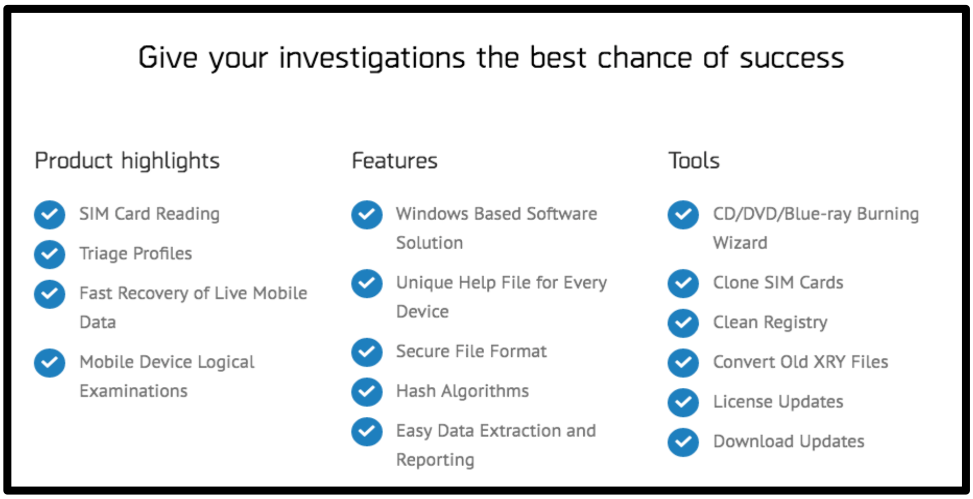
What is it?

Out of the three types of extraction, logical is seen as the quickest, least intrusive, but most limited. It creates a copy of the user accessible files[xxx] such as phonebook, calls, messages, some app data and other data you might expect from an iTunes or Android backup[xxxi]. i.e. what you can see if you manually examine each screen on the device.

MSAB, which describes itself as *‘a pioneer in forensic technology for mobile device examination”*[xxxii] markets their XRY Logical as *“our entry-level solution for forensic investigators and the starting point for our license options”.*[xxxiii]

“XRY Logical enables the user to conduct quick extractions (of iTunes backup, Android backup, Android Agent) and is geared toward “pump-and-dump” examinations.”[xxxiv]

Figure 6: MSAB’s XRY Logical[xxxv]



Give your investigations the best chance of success

Product highlights

- ✓ SIM Card Reading
- ✓ Triage Profiles
- ✓ Fast Recovery of Live Mobile Data
- ✓ Mobile Device Logical Examinations

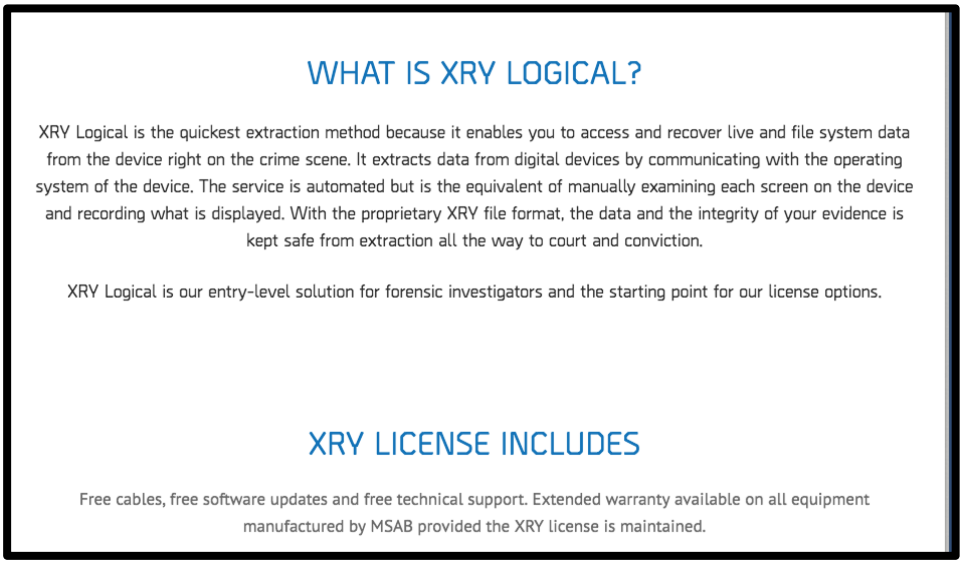
Features

- ✓ Windows Based Software Solution
- ✓ Unique Help File for Every Device
- ✓ Secure File Format
- ✓ Hash Algorithms
- ✓ Easy Data Extraction and Reporting

Tools

- ✓ CD/DVD/Blue-ray Burning Wizard
- ✓ Clone SIM Cards
- ✓ Clean Registry
- ✓ Convert Old XRY Files
- ✓ License Updates
- ✓ Download Updates

Figure 7: MSAB XRY Logical[xxxvi]



WHAT IS XRY LOGICAL?

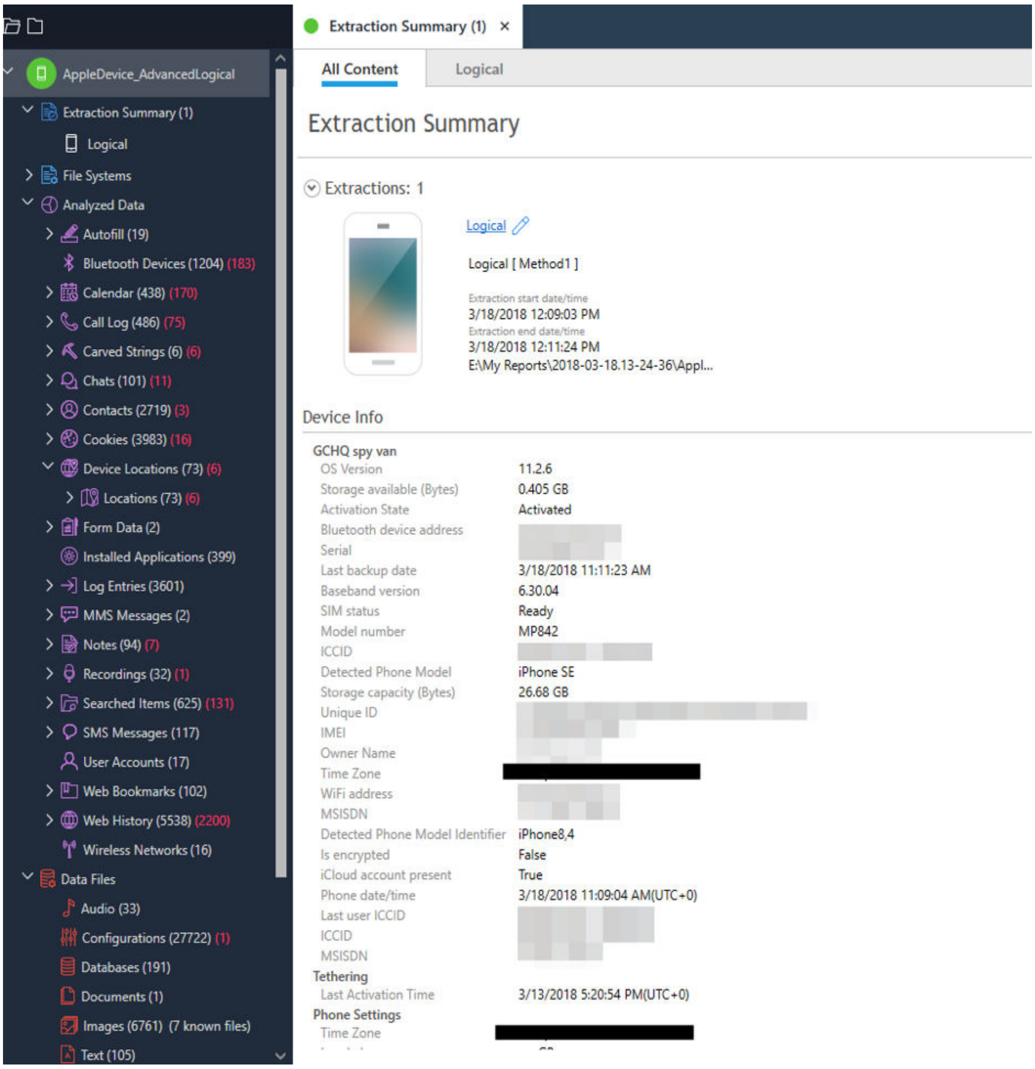
XRY Logical is the quickest extraction method because it enables you to access and recover live and file system data from the device right on the crime scene. It extracts data from digital devices by communicating with the operating system of the device. The service is automated but is the equivalent of manually examining each screen on the device and recording what is displayed. With the proprietary XRY file format, the data and the integrity of your evidence is kept safe from extraction all the way to court and conviction.

XRY Logical is our entry-level solution for forensic investigators and the starting point for our license options.

XRY LICENSE INCLUDES

Free cables, free software updates and free technical support. Extended warranty available on all equipment manufactured by MSAB provided the XRY license is maintained.

Figure 8: MSAB XRY Logical[xxxvii]



- AppleDevice_AdvancedLogical
  - Extraction Summary (1)
    - Logical
  - File Systems
  - Analyzed Data
    - Autofill (19)
    - Bluetooth Devices (1204) (183)
    - Calendar (438) (170)
    - Call Log (486) (75)
    - Carved Strings (6) (6)
    - Chats (101) (11)
    - Contacts (2719) (3)
    - Cookies (3983) (16)
    - Device Locations (73) (6)
      - Locations (73) (6)
    - Form Data (2)
    - Installed Applications (399)
    - Log Entries (3601)
    - MMS Messages (2)
    - Notes (94) (7)
    - Recordings (32) (1)
    - Searched Items (625) (131)
    - SMS Messages (117)
    - User Accounts (17)
    - Web Bookmarks (102)
    - Web History (5538) (2200)
    - Wireless Networks (16)
  - Data Files
    - Audio (33)
    - Configurations (27722) (1)
    - Databases (191)
    - Documents (1)
    - Images (6761) (7 known files)
    - Text (105)

Extraction Summary

Extractions: 1

Logical

Logical [Method1]

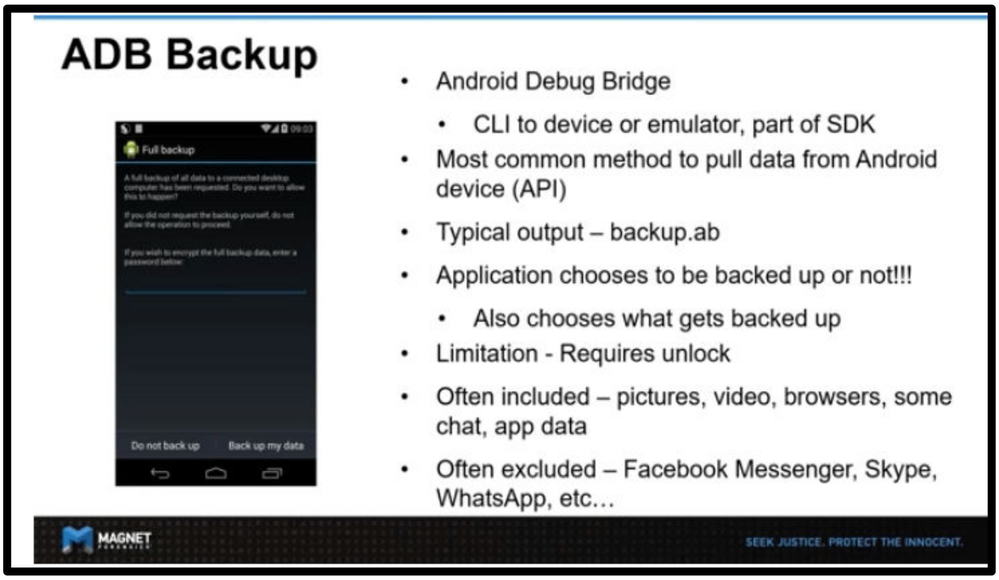
Extraction start date/time
3/18/2018 12:09:03 PM
Extraction end date/time
3/18/2018 12:11:24 PM
E:\My Reports\2018-03-18.13-24-36\Appl...

Device Info

GCHQ spy van	
OS Version	11.2.6
Storage available (Bytes)	0.405 GB
Activation State	Activated
Bluetooth device address	
Serial	
Last backup date	3/18/2018 11:11:23 AM
Baseband version	6.30.04
SIM status	Ready
Model number	MP842
ICCID	
Detected Phone Model	iPhone SE
Storage capacity (Bytes)	26.68 GB
Unique ID	
IMEI	
Owner Name	
Time Zone	[redacted]
WiFi address	
MSISDN	
Detected Phone Model Identifier	iPhone8,4
Is encrypted	False
iCloud account present	True
Phone date/time	3/18/2018 11:09:04 AM(UTC+0)
Last user ICCID	
ICCID	
MSISDN	
Tethering	
Last Activation Time	3/13/2018 5:20:54 PM(UTC+0)
Phone Settings	
Time Zone	[redacted]

Figure 9: Logical extraction of author's iPhone SE using Cellebrite UFED

Logical extraction may exclude data from certain apps if those apps do not backup into the files which form part of the extraction e.g. the default folder. To access these apps you would need access to the file system.



ADB Backup

- Android Debug Bridge
  - CLI to device or emulator, part of SDK
- Most common method to pull data from Android device (API)
- Typical output – backup.ab
- Application chooses to be backed up or not!!!
  - Also chooses what gets backed up
- Limitation - Requires unlock
- Often included – pictures, video, browsers, some chat, app data
- Often excluded – Facebook Messenger, Skype, WhatsApp, etc…

09:03
Full backup
A full backup of all data to a connected desktop computer has been requested. Do you want to allow this to happen?
If you did not request the backup yourself, do not allow the operation to proceed.
If you wish to encrypt the full backup data, enter a password below:
Do not back up
Back up my data
MAGNET FORENSICS
SEEK JUSTICE. PROTECT THE INNOCENT.

Figure 10: Magnet Forensics Webinar[xxxviii]

> *"Note for Android Devices: Non-system Android apps can choose to opt-out of the backup (e.g. WhatsApp). If the app manufacturer selects, then no app data is stored in the backup; a method commonly used for logical data recovery from mobile devices."*[xxxix]

Thus, you obtain only that which is available through a vendor's API. i.e. the phone can restrict what you can access. However, for Android phones, it may be possible to obtain app data by downgrading the target app to an older version where adb backup is allowed[xl]. The ability to do this is reportedly blocked in newer versions of Android[xli]. Although Cellebrite UFED 7.16 update on APK Downgrade method states it *"enables access to file system data from more than 40 applications on Android device running version 6.0 and above."* [xlii]

Logical extractions typically do not include a full bit-by-bit copy of the data or recover deleted data. However, it may be possible to recover deleted records including SMS, chats and browsing history if SQLite databases are used to store the data[xliii] using for example Cellebrite's SQLite Wizard.[xliv] As noted by Reiber (2019:159), *"within a subset of devices such as iOS and Android devices, a logical file extraction can often contain deleted data."*

How does it work?

Logical extraction involves *"connecting the mobile device to forensic hardware or to a forensic workstation via a USB cable, a RJ-45 cable, infrared or Bluetooth"*[xlv]. Once the phone is connected, the forensic tool *"initiates a command and sends it to the device, which is then interpreted by the device processor."*[xlvi] I.e. the forensic tools communicate with the operating system of the mobile device[xlvii]. The data requested as a result of the use of proprietary protocols and queries[xlviii] is:

"…received from the device's memory and sent back to the forensic workstation. Later, the examiner can review the data. Most of the forensic tools currently available work at this level of the classification system."[xlix]

Using the Application Programming Interface ("API"), is one way to carry out logical extraction. Cellebrite, a leading forensics company popular with government agencies[l], states *"From a technical standpoint, API-based logical extraction is straightforward to implement, and the results are provided in a readable format."*[li]

Cellebrite's UFED Touch (hardware with UFED software) and UFED 4PC (software installed on a computer) work by communicating with the operating system of a device using the API.

> *"Logical extraction of data is performed, for the most part, through a designated API, available from the device vendor. Just as the API allows commercial third-party apps to communicate with the device OS, it also enables forensically sound data extraction...Upon connection, the UFED loads the relevant vendor API to the device. The UFED then makes read-only API calls to request data from the phone. The phone replies to valid API requests to extract designated content items such as text messages (SMS), phonebook entries, pictures, etc."*[lii]

Logical extraction on an iPhone using a Cellebrite UFED Touch 2 works similarly to how iTunes or iCloud might take a backup, it displays on the phone screen the various prompts for the data being extracted, for example 'Backup Call Data" (Yes/No).

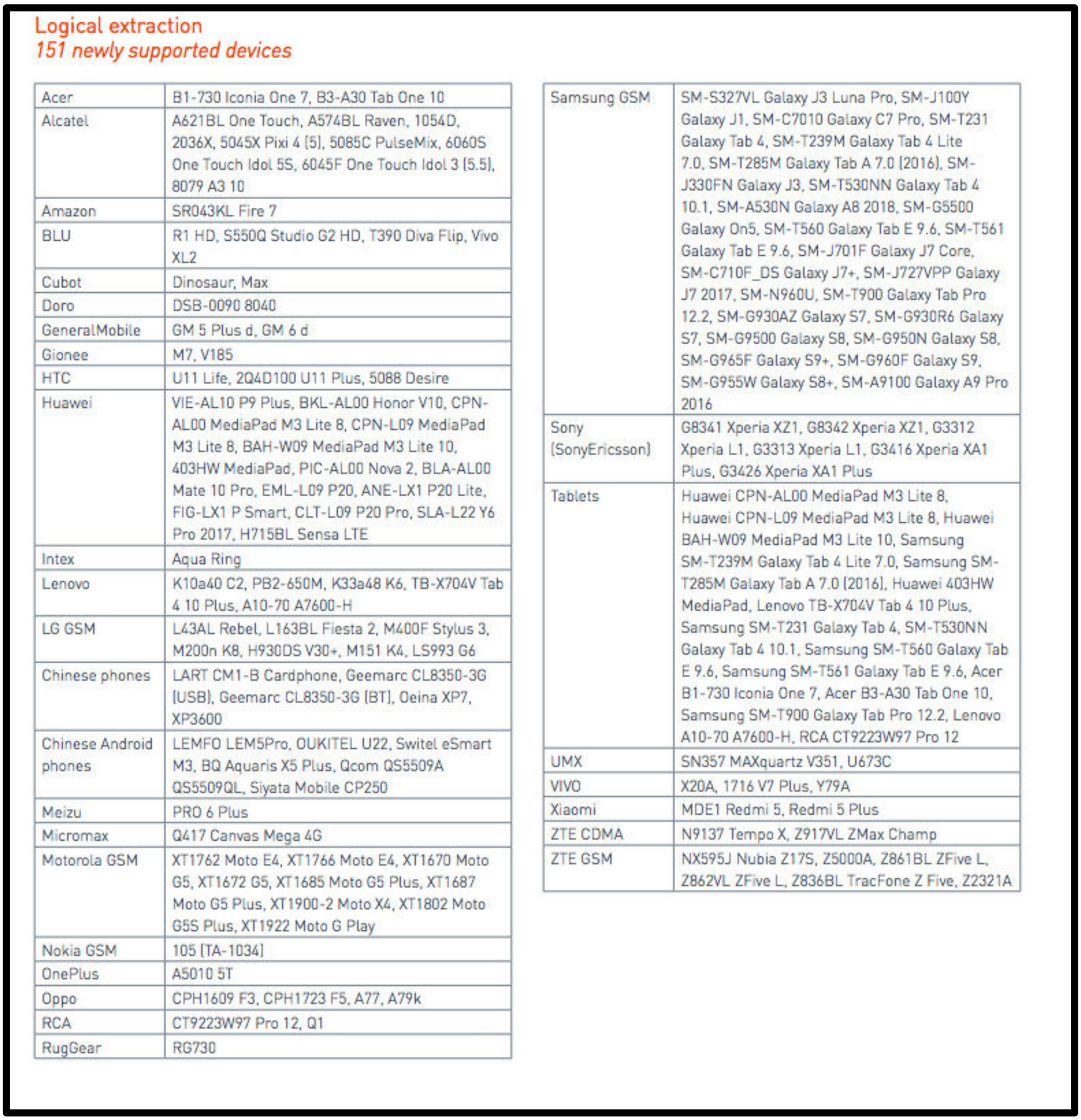
Some forensics tools install an App or agent onto the device to try and pull additional data.

"The best mobile forensic software, such as: UFED (Cellebrite), Oxygen Forensic, XRY (Microsystemation), Secure View (Susteen), MOBILedit Forensic can extract data from Android devices by installing an agent program on the device."[liii]

As noted by Reiber (2019:57) MobileEdit Forensics, scans the connected device and if an Android device is detected, it uploads an agent program Forensic Connector and using this agent, it extracts data from the device.

> *"An example ... would be using a software tool on an Android device with an Android application package (APK) file... The APK queries the Android device's internal databases and returns the data to the software interface. The data is then displayed in the software's user interface. This method does not return a file system, but the data that is represented by the contents of the files on the device."*[liv]

Logical extraction is not guaranteed for all devices, even if unlocked. Cellebrite's Product Updates for example lists supported phones.



Logical extraction
151 newly supported devices

Acer	B1-730 Iconia One 7, B3-A30 Tab One 10
Alcatel	A621BL One Touch, A574BL Raven, 1054D, 2036X, 5045X Pixi 4 [5], 5085C PulseMix, 6060S One Touch Idol 5S, 6045F One Touch Idol 3 [5.5], 8079 A3 10
Amazon	SR043KL Fire 7
BLU	R1 HD, S550Q Studio G2 HD, T390 Diva Flip, Vivo XL2
Cubot	Dinosaur, Max
Doro	DSB-0090 8040
GeneralMobile	GM 5 Plus d, GM 6 d
Gionee	M7, V185
HTC	U11 Life, 2Q4D100 U11 Plus, 5088 Desire
Huawei	VIE-AL10 P9 Plus, BKL-AL00 Honor V10, CPN-AL00 MediaPad M3 Lite 8, CPN-L09 MediaPad M3 Lite 8, BAH-W09 MediaPad M3 Lite 10, 403HW MediaPad, PIC-AL00 Nova 2, BLA-AL00 Mate 10 Pro, EML-L09 P20, ANE-LX1 P20 Lite, FIG-LX1 P Smart, CLT-L09 P20 Pro, SLA-L22 Y6 Pro 2017, H715BL Sensa LTE
Intex	Aqua Ring
Lenovo	K10a40 C2, PB2-650M, K33a48 K6, TB-X704V Tab 4 10 Plus, A10-70 A7600-H
LG GSM	L43AL Rebel, L163BL Fiesta 2, M400F Stylus 3, M200n K8, H930DS V30+, M151 K4, LS993 G6
Chinese phones	LART CM1-B Cardphone, Geemarc CL8350-3G [USB], Geemarc CL8350-3G [BT], Oeina XP7, XP3600
Chinese Android phones	LEMFO LEM5Pro, OUKITEL U22, Switel eSmart M3, BQ Aquaris X5 Plus, Qcom QS5509A QS5509QL, Siyata Mobile CP250
Meizu	PRO 6 Plus
Micromax	Q417 Canvas Mega 4G
Motorola GSM	XT1762 Moto E4, XT1766 Moto E4, XT1670 Moto G5, XT1672 G5, XT1685 Moto G5 Plus, XT1687 Moto G5 Plus, XT1900-2 Moto X4, XT1802 Moto G5S Plus, XT1922 Moto G Play
Nokia GSM	105 [TA-1034]
OnePlus	A5010 5T
Oppo	CPH1609 F3, CPH1723 F5, A77, A79k
RCA	CT9223W97 Pro 12, Q1
RugGear	RG730
Samsung GSM	SM-S327VL Galaxy J3 Luna Pro, SM-J100Y Galaxy J1, SM-C7010 Galaxy C7 Pro, SM-T231 Galaxy Tab 4, SM-T239M Galaxy Tab 4 Lite 7.0, SM-T285M Galaxy Tab A 7.0 [2016], SM-J330FN Galaxy J3, SM-T530NN Galaxy Tab 4 10.1, SM-A530N Galaxy A8 2018, SM-G5500 Galaxy On5, SM-T560 Galaxy Tab E 9.6, SM-T561 Galaxy Tab E 9.6, SM-J701F Galaxy J7 Core, SM-C710F_DS Galaxy J7+, SM-J727VPP Galaxy J7 2017, SM-N960U, SM-T900 Galaxy Tab Pro 12.2, SM-G930AZ Galaxy S7, SM-G930R6 Galaxy S7, SM-G9500 Galaxy S8, SM-G950N Galaxy S8, SM-G965F Galaxy S9+, SM-G960F Galaxy S9, SM-G955W Galaxy S8+, SM-A9100 Galaxy A9 Pro 2016
Sony [SonyEricsson]	G8341 Xperia XZ1, G8342 Xperia XZ1, G3312 Xperia L1, G3313 Xperia L1, G3416 Xperia XA1 Plus, G3426 Xperia XA1 Plus
Tablets	Huawei CPN-AL00 MediaPad M3 Lite 8, Huawei CPN-L09 MediaPad M3 Lite 8, Huawei BAH-W09 MediaPad M3 Lite 10, Samsung SM-T239M Galaxy Tab 4 Lite 7.0, Samsung SM-T285M Galaxy Tab A 7.0 [2016], Huawei 403HW MediaPad, Lenovo TB-X704V Tab 4 10 Plus, Samsung SM-T231 Galaxy Tab 4, SM-T530NN Galaxy Tab 4 10.1, Samsung SM-T560 Galaxy Tab E 9.6, Samsung SM-T561 Galaxy Tab E 9.6, Acer B1-730 Iconia One 7, Acer B3-A30 Tab One 10, Samsung SM-T900 Galaxy Tab Pro 12.2, Lenovo A10-70 A7600-H, RCA CT9223W97 Pro 12
UMX	SN357 MAXquartz V351, U673C
VIVO	X20A, 1716 V7 Plus, Y79A
Xiaomi	MDE1 Redmi 5, Redmi 5 Plus
ZTE CDMA	N9137 Tempo X, Z917VL ZMax Champ
ZTE GSM	NX595J Nubia Z17S, Z5000A, Z861BL ZFive L, Z862VL ZFive L, Z836BL TracFone Z Five, Z2321A

Figure 11: Cellebrite Product Update[lv]

Using vulnerabilities

As with all forms of extraction, there are several components which will influence whether it is possible. First is the operating system. If it's Android, if USB debugging has been enabled, which enables the ADB server on the device and the RSA keys (security prompt) has been accepted and the personal computer ("PC") and phone paired, then a logical extraction can be performed. As noted, this is typically an ADB backup combined with pushing an Android APK to the device and using available commands to extract active records like SMS/MMS, Call Logs and Contacts.

Mikhaylov (2017:39) states that different steps are required to activate USB debugging mode depending on what version of Android is being used. To enable USB debugging the passcode will be required. Although some devices running Android, like the Innotab Max, which Privacy International tested in 2016-17, appear to ship from the factory with debugging enabled by default. Research by Pen

Test Partners confirmed that the Vtech Innotab Max is rooted by default with ADB (auto debugging) enabled from the outset[lvi].

USB debugging mode is a developer mode in Android phones that allows newly programmed apps to be copied via USB to the device for testing[lvii]. It allows an Android device to receive commands, files and the like from a computer and allows the computer to pull crucial information like log files from the Android device[lviii]. Enabling USB debugging leaves the device exposed. The ADB, Android Debug Bridge is a command-line utility included with Google's Android SDK. ADB can control your device over USB from a computer[lix].

Without USB debugging logical extraction is unlikely to be possible, unless a vulnerability could be used. A logical extraction may be available depending on factors such as phone type, vulnerability used, software version and so on. Another way of looking at this is to consider whether user data is stored on the internal flash memory, and if so, whether it is protected and requires root access to read.[lx]

An example of a vulnerability used for logical extraction, since it can only target a specific area of the file system is described by Christopher Vance[lxi] of Magnet Forensics.

"Because this is an MTP extraction, we're only going to be able to grab what's in the / media / directory in the /data/ or /userdata/ partition. This is going to be mostly pictures and video files. However, the /media/ directory can hold more than that. It can also include documents, downloads from web browsers, WhatsApp chat backups, and third-party application data that developers choose to store here."[lxii]

Extracting an encrypted and damaged Samsung Galaxy S7, SM-G930V (could not enter the passcode or turn on USB debugging), using Media Transfer Protocol ("MTP") was one option to get around passcodes and authorization. However, whilst available for some Android phones, Samsung v.6 *"has changed the default connection type to "Charge Only" when it is plugged into a computer, so we would have to enable MTP which isn't going to be possible without our [damaged] screen".*[lxiii] Magnet AXIOM have an 'Advanced MTP bypass method':

"...to grab a quick image of the / media / partition on the device for Samsung devices that have not received either the SMR-OCT-2017 or SMR-NOV-2017 security update (the exact update in which this was patched depends on the device model). Even if this device doesn't have MTP enabled or is even locked with a passcode, this option will allow us to extract some of the data for analysis."[lxiv]

Locked iPhones

Whilst *"...a logical acquisition can be obtained if the iPhone is unlocked,"*[lxv] a locked iPhone is problematic since there are two separate prompts to deal with. One activates pairing mode with the computer and allows for an iTunes backup and one allows for media transfer if the standard iTunes provided driver cannot be found and it defaults back to MTP (Media Transfer Protocol) mode. If the device has a valid pairing record on the PC where the extraction is occurring, then a logical (iTunes style backup) can be obtained from a locked iPhone. Without that unfortunately it cannot be obtained.

In older iOS versions it was possible to gain just MTP extractions from an iPhone that was locked but this has since been patched and is the reason for the second prompt. Without accepting that prompt (hidden by the lock screen) you won't be able to get an MTP extraction from the device.[lxvi]

File system extraction

What is it

File system extraction is often technically seen as a type of logical extraction. As with all forms of extraction, the capabilities of a file system extraction will be device-specific.[lxvii] File System Extraction is slightly more data rich than a logical extraction, in file system extraction the entire filesystem is taken off of the phone.

It *"…contains much more information than the defined logical collection and should be considered a step up from a logical collection. A file system contains the files and folders that the device uses to populate applications, system configurations, and user configurations along with user storage areas."*[lxviii]

It includes files not directly accessible to the user via the device interface and require specialised tools to access file system artefacts. It does not extract unallocated space.

"The information contained [in a file system extraction] far exceeds any data that is collected on the surface. Collecting the "surface" logical data along with file system recovery is what every examination should strive to accomplish. This type of collection should be referred to as a file system collection, not simply a logical extraction."[lxix]

"Feature phones using proprietary file systems can have their file systems collected and displayed to show system files, user databases, media, user files, logs, user settings, and more. … These files are the actual containers queried and parsed by the logical software and displayed in the software interface. By having the actual file, you can conduct a more detailed analysis, which should be considered much more valuable than what "logical" defines."[lxx]

File System Extraction is usually done by a root user so requires (generally soft) rooting the phone. A root user is a superuser, in that a superuser has permission to do anything to any files anywhere in the phone's system. i.e. privileged control over the phone. Rooting a phone is the process to attain root access.

Cellebrite UFED 'advanced logical extraction' combines the logical and file system extractions for iOS and Android devices and is an alternative to where physical extraction is not possible.[lxxi]

"Advanced logical acquisitions are the same as file system acquisitions in which access to the filesystem data is provided. Physical acquisition on iOS devices using the A5-A11 chips (iPhone 4s and newer) is not possible using this tool. Thus the advanced logical acquisition method is the best support and will pull the most data from these devices if they are unlocked (even if they are not jailbroken). If the device is jailbroken, additional data can be extracted."[lxxii]

How does it work?

File system extraction is less identified as a distinct form of extraction by companies. Almost uniquely Cellebrite promotes UFED's file system extraction and is amongst the few who refer to the method:

> *"File system extraction with UFED Physical Analyzer is almost identical to physical extraction in that it relies on a boot loader*

> *to access the device's memory; however, rather than obtain a bit-for-bit image including unallocated space, the software extracts only the device file system. This extraction process is proprietary rather than dependent on Apple's API."*[lxxiii]

MSAB does not have a specific file system product, simply XRY Logical and XRY Physical. Oxygen Forensics refer to obtaining a file system collection as part of 'classic logical'[lxxiv]. Magnet's Acquire tool allows you to choose an extraction process, offering a 'quick extraction' from all iOS and Android devices or 'full extraction through a physical image of rooted Android devices or file system logical images of jailbroken iOS devices.'[lxxv]

"If the device is rooted you can create a physical dump. If the device is not rooted a backup of the device is created and all the files that are in the memory card of the device are extracted."[lxxvi]

File system acquisition is however an alternative where physical extraction of iOS devices is no longer possible. Unfortunately, the passcode is required.

"Since iOS 8, removing the passcode is pointless even on 32-bit devices. The cryptographic key that's needed to decrypt the data partition is calculated dynamically based on user input (the passcode) and keys from Secure Enclave. Without the correct passcode, the iPhone will remain encrypted; there's simply no way around it."[lxxvii]

Secure Enclave *"is a hardware-based key manager that's isolated from the main processor to provide an extra layer of security."*[lxxviii] The consequence is that encryption keys are protected by Secure Enclave and are no longer accessible even if the device is jailbroken[lxxix]. However, a file system extraction can be obtained if you jailbreak the device. To do this you need to boot and unlock the device using the passcode. *"In other words, the passcode must be known in order to perform the (limited) physical acquisition of all iPhone devices starting with iPhone 5s."*

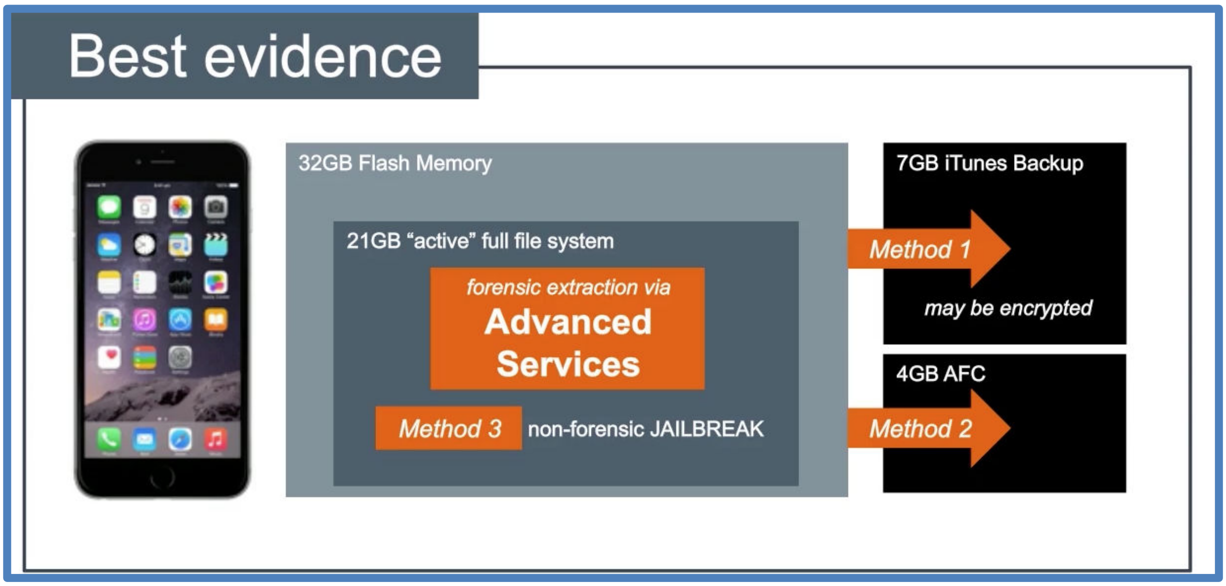
> *"Secure Enclave has brought new challenges to iOS forensic examiners. Now, we can't extract encryption keys required to decrypt the device image, so physical acquisition is useless. But here comes the filesystem acquisition. Unfortunately, it requires the iOS device to be jailbroken."*[lxxx]

Unlike a logical extraction, once the file system has been obtained it will need to be decoded.

"The decoding process translates the raw data within a database file to a recognizable format. Data extracted via APIs and backups require no decoding because it is intrinsic to these methods, which present media files such as pictures and videos as they are seen on the device. However, data within other database files, such as those that contain text messages, must be separately decoded to parse out the messages. UFED Physical Analyzer automatically performs this decoding process, presenting decoded data both in human-readable format, and as raw data is stored in the device's memory."[lxxxi]

Using vulnerabilities

Cellebrite claims its full file system extraction of an iOS device using their in-house labs ‘Cellebrite Advanced Services’, can obtain 21GB from a 32GB Flash Memory[lxxxii]. Cellebrite promotes its ‘Advances Services’ instead of releasing valuable vulnerabilities into the UFED, as this will, for example, give Apple a chance to patch exploits. Thus, what vulnerabilities are used to carry out a full file system extraction of an iOS device are not publicly disclosed.



Best evidence

32GB Flash Memory

21GB “active” full file system

forensic extraction via **Advanced Services**

Method 3 non-forensic JAILBREAK

7GB iTunes Backup

Method 1

may be encrypted

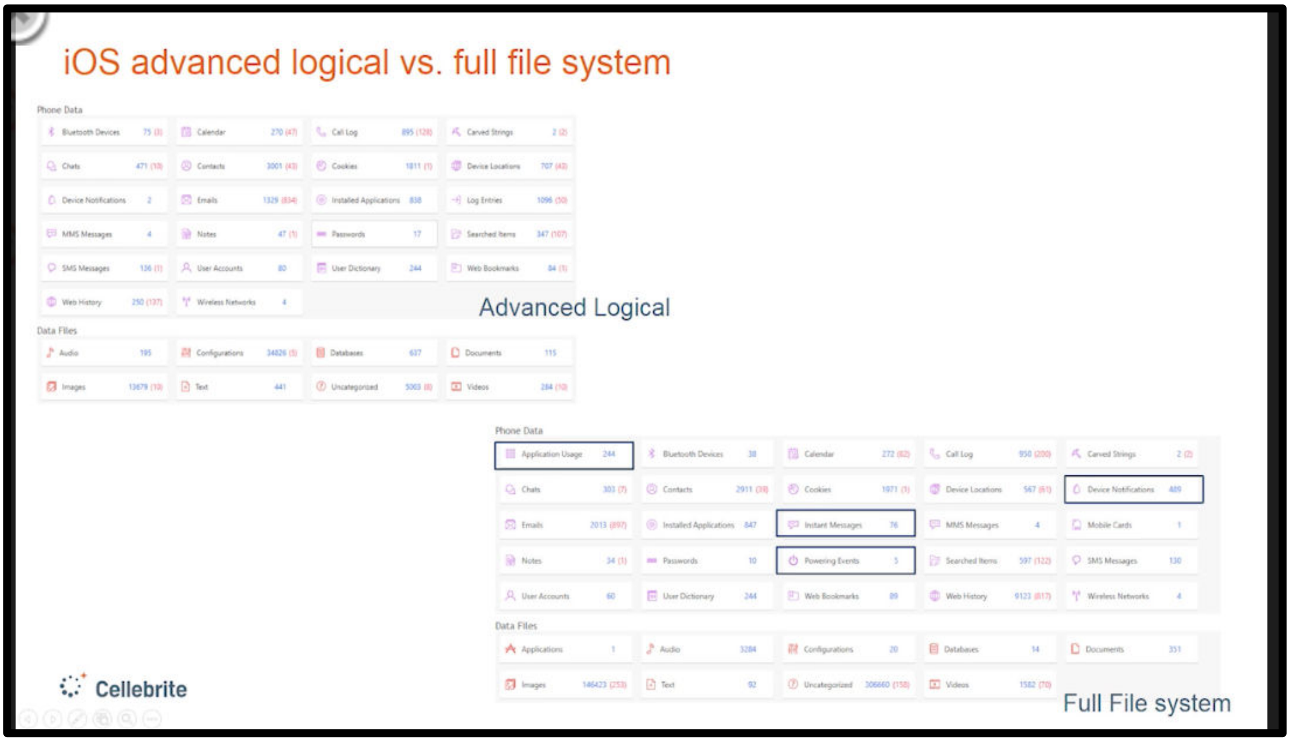
4GB AFC

Method 2

Figure 12: Cellebrite webinar[lxxxiii]

“What is the benefit of performing a full file system extraction instead of logical, file system or even an advanced logical extraction? There are three main benefits. Getting data from third party apps is the first one. WhatsApp, Facebook messenger, telegram. The data cannot be recovered unless a full file system extraction is performed. These apps and many more can hold critical information which can help close your case.”[lxxxiv]

I.e. A full file system extraction can obtain third party apps excluded from an iTunes backup. It can also identify device locations of interest, reveal system logs and application log data.[lxxxv]



iOS advanced logical vs. full file system

Phone Data

Bluetooth Devices	75 (3)	Calendar	270 (47)	Call Log	895 (128)	Carved Strings	2 (2)
Chats	471 (10)	Contacts	3001 (43)	Cookies	1811 (1)	Device Locations	707 (43)
Device Notifications	2	Emails	1329 (834)	Installed Applications	838	Log Entries	1096 (50)
MMS Messages	4	Notes	47 (1)	Passwords	17	Searched Items	347 (107)
SMS Messages	136 (1)	User Accounts	80	User Dictionary	244	Web Bookmarks	84 (1)
Web History	250 (137)	Wireless Networks	4				

Data Files

Audio	195	Configurations	34826 (5)	Databases	637	Documents	115
Images	13679 (10)	Text	441	Uncategorized	5303 (8)	Videos	284 (10)

Advanced Logical

Phone Data

Application Usage	244	Bluetooth Devices	38	Calendar	272 (62)	Call Log	950 (200)	Carved Strings	2 (2)
Chats	303 (7)	Contacts	2911 (38)	Cookies	1971 (1)	Device Locations	567 (61)	Device Notifications	489
Emails	2013 (897)	Installed Applications	847	Instant Messages	76	MMS Messages	4	Mobile Cards	1
Notes	34 (1)	Passwords	10	Powering Events	5	Searched Items	597 (122)	SMS Messages	130
User Accounts	60	User Dictionary	244	Web Bookmarks	89	Web History	9123 (817)	Wireless Networks	4

Data Files

Applications	1	Audio	3284	Configurations	20	Databases	14	Documents	351
Images	146423 (253)	Text	92	Uncategorized	306660 (158)	Videos	1582 (70)		

Full File system

Cellebrite

Figure 13: Cellebrite comparison between iOS advanced logical and full file system extraction

The use of Cellebrite Advanced Services has not been without controversy. In June it was reported[lxxxvi] that UK digital evidence lab Sytech lost its accreditation after a former employee reported concerns about the handling of evidence at the business. This included phones being 'sent abroad to be decrypted without the knowledge of the police'. One former employee said that 'a police force, understood to be Greater Manchester police, raised concerns with Sytech last year after learning that phones had been sent abroad to be unlocked by the Israeli-founded, Japanese owned company Cellebrite.' [lxxxvii]

Magnet Forensics also states that it can obtain a full file system. It has partnered with GrayKey to offer *"the most advanced solution to recover data from an iOS device including the full file system, decrypted keychain and process memory whereas other tools are limited to an iTunes backup only."*[lxxxviii] GrayKey can reportedly unlock iOS devices and get around USB Restricted mode[lxxxix].

Magnet Forensics report that they can then get third-party application data unlike an iTunes backup, aspects of Apple Mail data, web cache and app cache, operating system data, location data, keychain data and some deleted messages:

"GrayKey can obtain a full-file system image of the device which means that temporary or support files that exist with our standard artifacts are now available for review. A prime example of this is the sms.db-wal file that lives in the same directory as the sms.db. The sms.db allows examiners to recover and parse iMessages, SMS messages, and MMS messages. However, because this database utilizes the "write ahead log" functionality of SQLite, messages are in fact written to the sms.db-wal file before being committed into the main sms.db. This can cause issues in recovering potentially deleted messages depending upon how long the messages were on the device before being deleted. If messages are deleted as soon as they are sent/received it's much less likely to be able to recover these messages from a standard iTunes style extraction. However, since GrayKey allows us to extract the full file system, we now have access to this file and AXIOM will attempt to carve for any traces of messages left behind in the write ahead log including potentially deleted messages."[xc]

There is little information around file system extraction, perhaps given the value of iPhone vulnerabilities. There is also not much about other operating systems such as Android, perhaps because it is still possible to carry out the preferred physical extraction.

Physical extraction

What is it?

Physical extraction can obtain *"service data, applications, and user's data. Deleted files can be restored from the physical dump."* [xci] Physical extraction is a bit-by-bit copy of the physical storage / entire filesystem / device memory or as a hex-dump. It usually requires specific cabling, and involves booting the phone into a custom OS, or recovery. Physical Extraction generally takes a long time, because it brings over free space too, however freespace can contain deleted information so may be worthwhile from an investigators point of view.

> "Physical extraction has long been an ideal forensic extraction method for cell phones and embedded devices. This method has traditionally included physical access to the memory chip to obtain a raw reading of the underlying flash blocks. Not only does this method allow access to the digital data, but analyzing the physical storage quickly reveals unused areas and blocks that can contain deleted data and hold significant forensic value."[xcii]

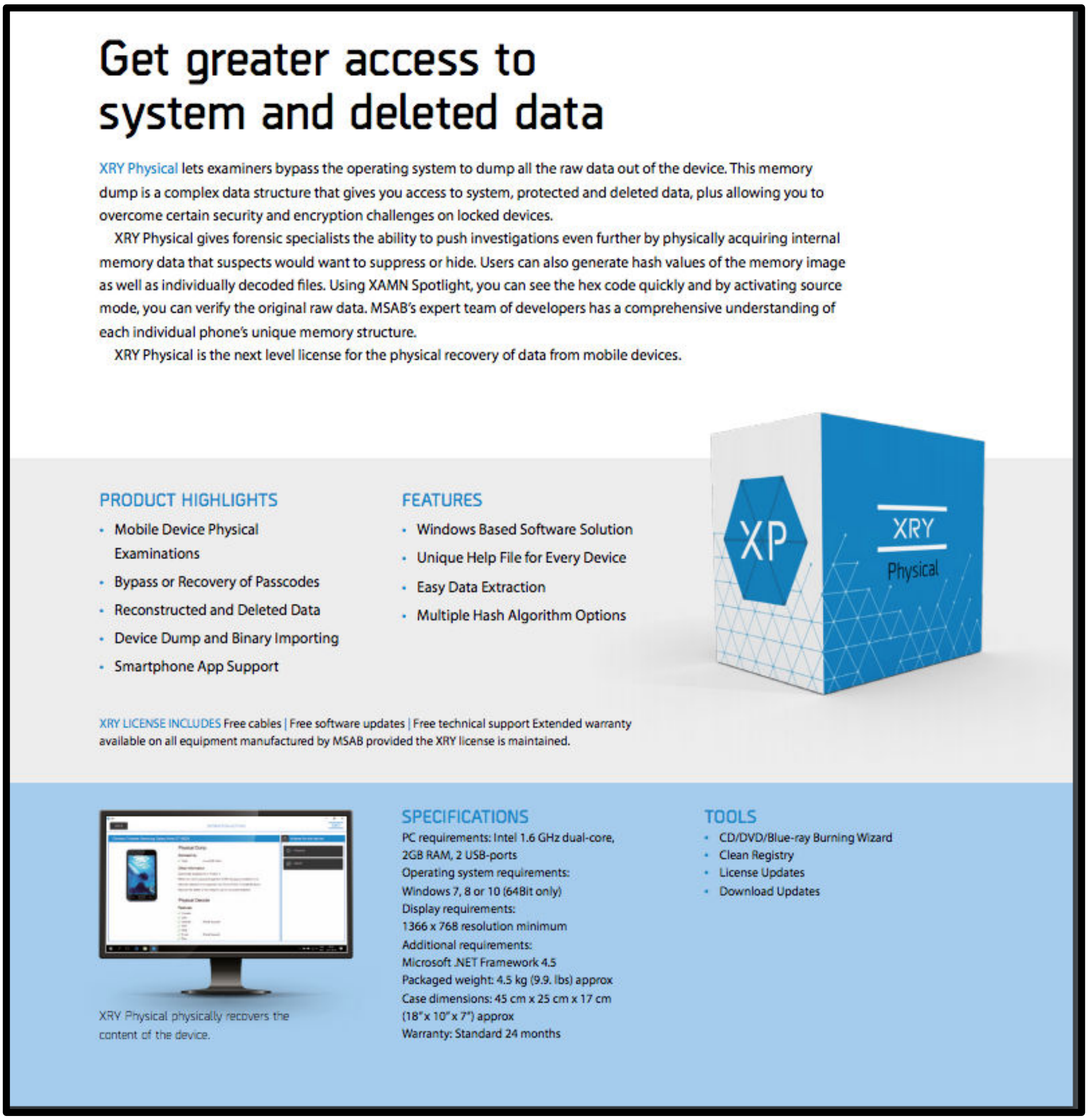
It is the most comprehensive and invasive of all the extractions and includes all unallocated space on the phone which is why it may include deleted files.

"Cellebrite's physical extraction capability accesses the additional data layers, in both allocated and unallocated space, that construct the phone's physical memory. These layers include three different groups of content pertinent to investigators:

"Logical" content unavailable through API (e.g. call logs on smartphones and feature phones)

Deleted content

Content that the phone collects without any user action (and sometimes without user knowledge). For example: wi-fi networks, GPS locations, web history, email headers and EXIF data on images and system data."[xciii]



Get greater access to system and deleted data

XRY Physical lets examiners bypass the operating system to dump all the raw data out of the device. This memory dump is a complex data structure that gives you access to system, protected and deleted data, plus allowing you to overcome certain security and encryption challenges on locked devices.

XRY Physical gives forensic specialists the ability to push investigations even further by physically acquiring internal memory data that suspects would want to suppress or hide. Users can also generate hash values of the memory image as well as individually decoded files. Using XAMN Spotlight, you can see the hex code quickly and by activating source mode, you can verify the original raw data. MSAB's expert team of developers has a comprehensive understanding of each individual phone's unique memory structure.

XRY Physical is the next level license for the physical recovery of data from mobile devices.

PRODUCT HIGHLIGHTS

- Mobile Device Physical Examinations
- Bypass or Recovery of Passcodes
- Reconstructed and Deleted Data
- Device Dump and Binary Importing
- Smartphone App Support

FEATURES

- Windows Based Software Solution
- Unique Help File for Every Device
- Easy Data Extraction
- Multiple Hash Algorithm Options

XRY LICENSE INCLUDES Free cables | Free software updates | Free technical support Extended warranty available on all equipment manufactured by MSAB provided the XRY license is maintained.

XRY Physical physically recovers the content of the device.

SPECIFICATIONS

PC requirements: Intel 1.6 GHz dual-core, 2GB RAM, 2 USB-ports
Operating system requirements:
Windows 7, 8 or 10 (64Bit only)
Display requirements:
1366 x 768 resolution minimum
Additional requirements:
Microsoft .NET Framework 4.5
Packaged weight: 4.5 kg (9.9. lbs) approx
Case dimensions: 45 cm x 25 cm x 17 cm (18"x 10"x 7") approx
Warranty: Standard 24 months

TOOLS

- CD/DVD/Blue-ray Burning Wizard
- Clean Registry
- License Updates
- Download Updates

Figure 14: MSAB's XRY Physical

How does it work

> *"A hex dump, also referred to as a physical extraction, is achieved by connecting the device to the forensic workstation and pushing unsigned code or a bootloader into the phone and instructing the phone to dump memory from the phone to the computer. Since the resulting raw image is in binary format, technical expertise is required to analyze it. The process ... provides more data to the examiner, and allows the recover of*

deleted files from the device-unallocated space on most devices."[xciv]

MSAB state that their XRY Physical product accesses the data through bypassing the operating system to access all system and deleted data. They can overcome security and encryption challenges on (certain) locked devices.

"The physical collection of a mobile device's data should imply that direct communication with a device's internal data storage is made to collect a representation of the data as it is stored on the actual device flash memory. This data is a snapshot in the area of the flash memory store that is accessible using specialized tools and methods."[xcv]

"...with encryption enabled on the full disk, at the block-level, entire physical reading becomes unusable unless an examiner can retrieve a device's encryption key."[xcvi]

The XRY Physical add-on to XRY Logical enables the user to conduct password bypass of some Android devices, on-board memory chip reads, and other advanced mobile forensic tasks."[xcvii]

On an Android phone, this method usually requires the removal of the battery and the turning off of the phone, also the cable is usually specific for this method, rather than using the standard charging cable. The Cellebrite directs throughout what steps must be undertaken and when, including which buttons need to be held at startup to enable FastBoot, Bootloader, Recovery, Factory Reset etc, depending on which devices are being extracted.

Once the device is in fastboot, the Cellebrite works fairly automatedly, it may prompt you at times to select options on the phone screen or restart the phone.

The physical extraction, which we did on a iPhone 4, uses a bug in the iOS bootstrap process which allows for unsigned code to executed (its a technique used to jailbreak older iDevices) the Cellebrite then runs its own OS instead of iOS and extracts the data from the phone.

Physical extraction might use a phone's rescue mode or download mode. *"Operating in this mode, mobile phones are designed to allow the insertion of a small piece of code, called bootloaders, into the RAM during start-up."*[xcviii] The bootloader will read the contents of the device's memory and send it back to extraction device. Cellebrite states that:

"... During the initial stage of the device's booting, the UFED sends the boot loader to the device's RAM memory. The device will start running the boot loader, but will not continue its regular booting procedure into the OS. The Cellebrite boot loaders then execute "read only" actions that extract evidence from mobile devices and leave no artifacts behind."[xcix]

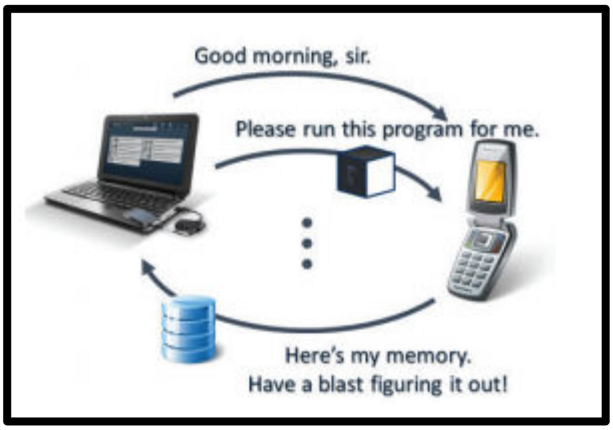

Good morning, sir.
Please run this program for me.
Here's my memory.
Have a blast figuring it out!

Figure 15: Physical extraction using a bootloader[c]

Cellebrite's bootloaders are designed in-house around each individual device platform taking into account the varieties in chipsets, peripherals, memory chip interfaces and USB controllers. Customers will need to send certain phones to Cellebrite.

"UFED has obtained the permission to access operating system internals after the data is already decrypted. It can then extract the raw, block-level reading in decrypted form. This is done, again, by exploiting vulnerabilities identified by Cellebrite. These vulnerabilities are rarely available to the public after they are discovered. Quite often, Cellebrite's Security Research Labs have exclusive knowledge of vulnerabilities and the opportunities they afford.

This knowledge will only become more valuable; as iOS & Android software progresses and privacy protections, sandbox isolation mechanisms and security mitigations advance."[ci]

The iOS challenge

Apple’s iOS presents the biggest hurdle for physical extractions. Before the iPhone 4S you could carry out a physical extraction on an iPhone. But since iPhone 4S and indeed for other devices that have entered the market, it is extremely difficult if not impossible to get into the device due to hardware encryption. Although a number of vendors’ state they can.

> *“Physical acquisition has the greatest potential for recovering data from iOS devices; however, current and evolving security features (secure boot chain, storage encryption, and passcode) on these devices may hinder the accessibility of the data during forensic acquisition. Researchers and commercial forensic tool vendors are continually attempting new techniques to bypass the security features and perform physical acquisition on iOS devices, but for the latest model the only available option is jailbreaking and even this won’t help you to physically acquire devices with Secure Enclave…”*[cii]

Elcomsoft iOS Forensic Toolkit 5.0 states that it can achieve iOS 12 physical extraction. This sounds similar to Cellebrite’s full file system extraction described above. It can extract the content of the file system and decrypt passwords and authentication credentials stored in the iOS keychain. It is possible on devices supported by the ‘rootless jailbreak’[ciii].

“Elcomsoft iOS Forensic Toolkit supports all possible options for extracting and decrypting data from both jailbroken and non-jailbroken 64-bit devices, including the last generations of Apple hardware and software. Without a jailbreak, experts can perform logical extraction though iOS system backups, extract shared app data and media files. In certain cases, logical extraction is even possible if the iPhone is locked. If a jailbreak can be installed, experts can image the file system of 64-bit iPhones, extract protected application data and working datasets.”[civ]

“Physical acquisition offers numerous benefits compared to all other acquisition options by enabling access to protected parts of the file system and extracting data that is not synced with iCloud or included in local backups: In particular, physical acquisition is the only method for decrypting keychain items targeting the highest protection class. File system extraction gains full access to application sandboxes and all system areas, extract secret chats and recover deleted messages. Downloaded email messages, chat databases and secrets from two-factor authentication apps, system logs and detailed location data are just a few things that are exclusively available with file system extraction.”[cv]

“...public jail breaks to gain access to the device’s file system, circumvent iOS security measures and access device secrets allowing us to decrypt the entire content of the keychain including keychain items protected with the highest protection class.”[cvi]

Indeed, Reiber (2019 : 342) states that:

> *"With today's iOS devices containing A5 and later chipsets, a non-jailbroken physical bit-by-bit collection using a USB is impossible, so a logical file system collection is the only available method…Some sources report that a physical collection can be obtained using tools such as Elcomsoft iOS Forensic Toolkit, GrayKey by Grayshift, or Cellebrite's professional services CAIS program, but this is not entirely accurate. These tools cannot be used to perform a physical partition collection as they can with A4 chipsets; they simply enable collecting a jailbroken device's internal file system. Once the device is in a state in which a raw file system can be collected, most commercial tools, including UFED Touch 2, Oxygen Forensic Detective, and XRY, can collect the file system and artifacts."*

Physical acquisition of iOS 11 devices by Elcomsoft iOS Forensics Toolkit uses classic jailbreak.

"Forensic experts use jailbreaks for much different reasons compared to enthusiastic users. A wide-open security vulnerability is exactly what they want to expose the device's file system, circumvent iOS sandbox protection and access protected data. Jailbreaking extracts the largest set of data from the device. During jailbreaking, many software restrictions imposed by iOS are removed through the use of software exploits.

In addition to sandboxed app data (which includes conversation histories and downloaded mail) experts can also extract and decrypt the keychain, a system - wide storage for online passwords, authentication tokens and encryption keys. Unlike keychain items obtained from a password-protected local backup, physical extraction of a jailbroken device gains access to keychain items secured with the highest protection class."[cvii]

Android - Using vulnerabilities: Emergency Download Mode

"It may seem unusual, but it is possible to make a physical dump of an Android device without rooting and it does not require JTAG and Chip-off methods."[cviii]

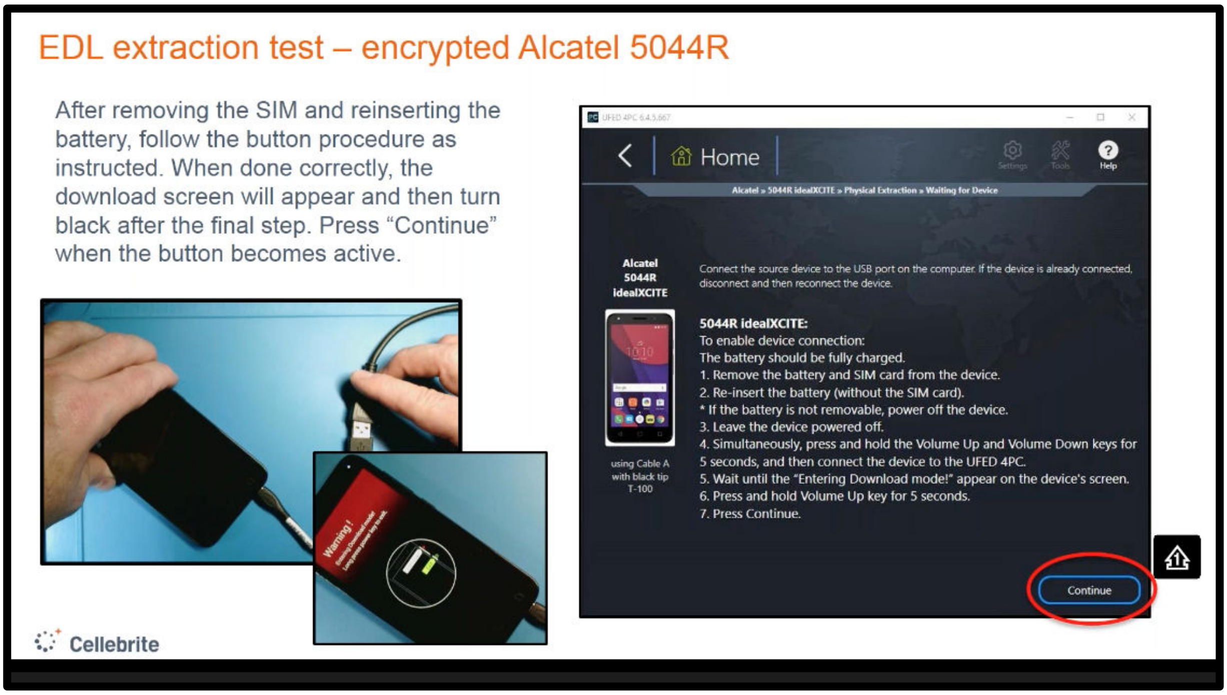
Emergency Download (EDL) mode is a vulnerability used by a number of vendors to carry out physical extractions. It works on some but not all devices that have the Qualcomm chipset. EDL is Qualcomm's rescue mode for phone diagnostics and repair, which is exposed through various triggers or when a device cannot boot. It *"is designed to allow low level access to chipset for device analysis, repair or re-thrashing."*[cix]

Cellebrite has a wide range of ready 'programmers' which are *"pieces of software containing raw flash read/write functionality"*.[cx] Programmers can be digitally signed with a vendor signature that is verified by the device, so for EDL to accept and verify a programmer it must match but the hardware and signature requirement.

When Cellebrite's UFED starts EDL extraction flow, it will automatically attempt to match an existing programmer it has to the hardware and signature requirement. If there is a match, then it will have flash read access. If there is not signature requirement for a particular phone, then it will match the hardware. According to Cellebrite, UFED has a proprietary exploit to bypass the signature requirement for several chipsets.

In addition, raw flash access will enable access to encrypted content, however, without access to encryption keys. To address this problem, Cellebrite UFED will attempt to fully boot the device before the extraction begins.

The way you put a device in EDL mode will differ depending on the phone and ranges from techniques that various technologies such as Cellebrite's UFED can support, to more invasive techniques that require forensic skill. If EDL is supported by Cellebrite, the UFED can guide you through what you need to do, for example, hold vol up and down.



EDL extraction test – encrypted Alcatel 5044R

After removing the SIM and reinserting the battery, follow the button procedure as instructed. When done correctly, the download screen will appear and then turn black after the final step. Press "Continue" when the button becomes active.

UFED 4PC 6.4.5.667

Alcatel » 5044R idealXCITE » Physical Extraction » Waiting for Device

Alcatel 5044R idealXCITE

using Cable A with black tip T-100

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

5044R idealXCITE:
To enable device connection:
The battery should be fully charged.
1. Remove the battery and SIM card from the device.
2. Re-insert the battery (without the SIM card).
* If the battery is not removable, power off the device.
3. Leave the device powered off.
4. Simultaneously, press and hold the Volume Up and Volume Down keys for 5 seconds, and then connect the device to the UFED 4PC.
5. Wait until the "Entering Download mode!" appear on the device's screen.
6. Press and hold Volume Up key for 5 seconds.
7. Press Continue.

Figure 16: Using EDL Mode

Cellebrite's UFED has both a decrypting and non-decrypting EDL extraction option. Both work on pattern or passcode locked devices (if the device is supported), if the device is encrypted. The decryption extraction for encrypted devices will require the device to boot so that the UFED can apply the decrypting bootloader, which is not required for non-decrypting EDL extraction. For both options, when using the UFED, the user will be able to choose placing the device in DFU (handset diagnostic interface) FTM (factory test mode). These both use EDL methods.

An example of using EDL mode, bootloader option is Cellebrite's EDL physical bypass solution for certain Samsung devices with the Qualcomm chipset.[cxi] Most modern phones running Android are encrypted out of the box. In this method Cellebrite uses specified cables for devices with a specific data port connection. When the device is running in bootloader mode, the operating system does not run. It bypasses any user lock.[cxii] When you select the phone you want to download, the UFED will ask you to do a number of things to get the phone into download mode and enable the extraction.

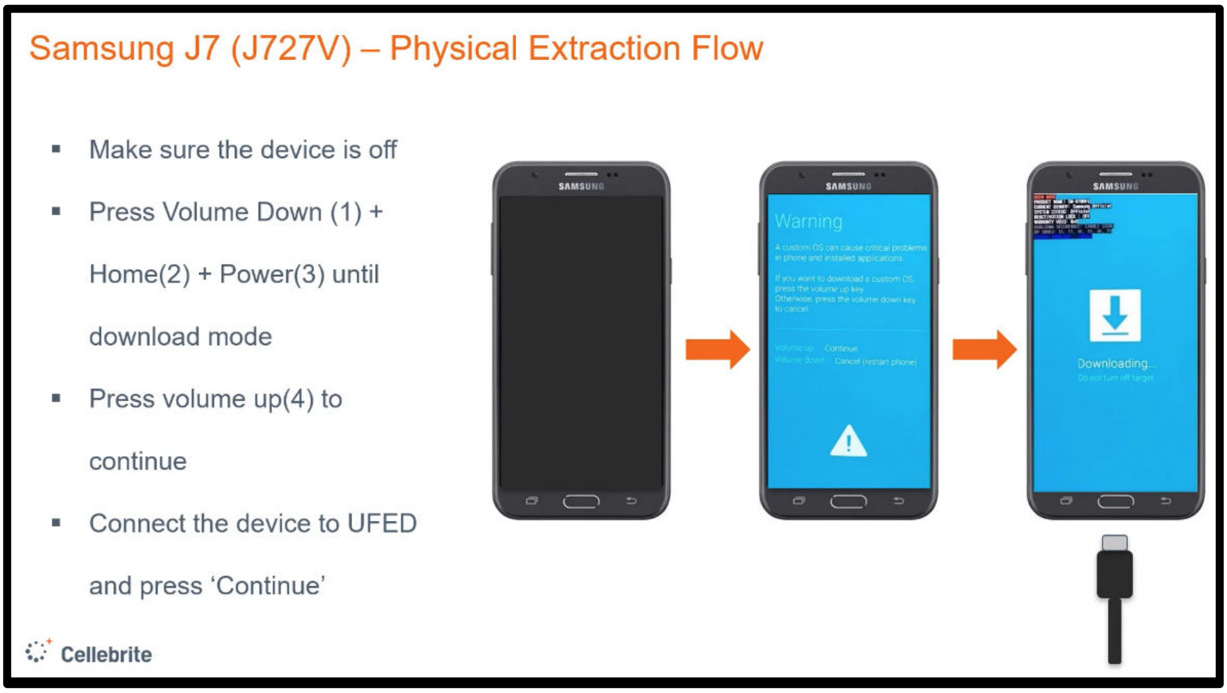
Other methods to achieve EDL mode include the use of cable 523, 'abd reboot edl', 'fastboot oem edl', test point and eMMC fault injection (shorting). The last two require experience with ISP and Chip Off.

Cellebrite are not the only vendor extracting a physical image for devices with Qualcomm chipsets via EDL mode. Magnet Forensics and Oxygen Forensics do this using the ADB method. Both note that ADB access has to be enabled. To do this the phone must be unlocked and USB debugging turned on *"so that you're able to send and received ADB commands to the phone … the method does work quite well in scenarios where the phone is already unlocked and you just want to get a better acquisition."*[cxiii] Oxygen Forensics also use 'fastboot' and describe getting devices into this mode using key combinations e.g. holding Power and Vol- at the same time.[cxiv]

Cellebrite also promotes its ability to use 'smart' ADB:

"With this ground-breaking capability, Cellebrite restores physical extraction access to many new devices with Full-Disk Encryption enabled, when ADB can be enabled. The method requires Android 6 and above and has a wide generic coverage for many vendors."[cxv]

Oxygen Forensic Detective states that use of EDL mode *"allows investigators to utilize this non-invasive physical acquisition technique and screen lock bypass on more than 400 unique devices when the phone can be successfully placed into EDL mode."*[cxvi]



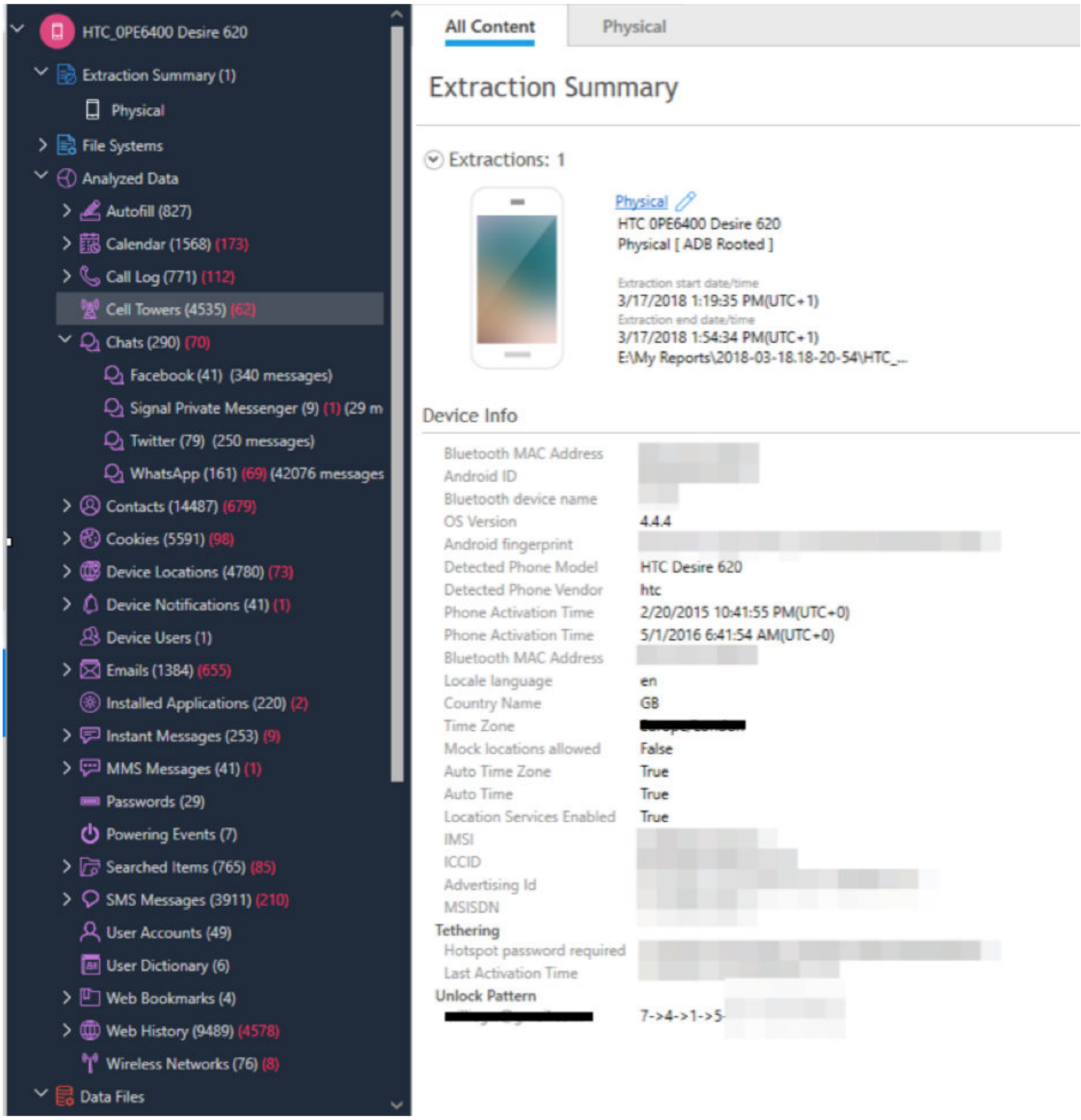
Samsung J7 (J727V) – Physical Extraction Flow

- Make sure the device is off
- Press Volume Down (1) + Home(2) + Power(3) until download mode
- Press volume up(4) to continue
- Connect the device to UFED and press 'Continue'

Cellebrite

SAMSUNG
Warning
Downloading...

Figure: 17: How to get a device into EDL mode[cxvii]



HTC_0PE6400 Desire 620

- Extraction Summary (1)
  - Physical
- File Systems
- Analyzed Data
  - Autofill (827)
  - Calendar (1568) (173)
  - Call Log (771) (112)
  - Cell Towers (4535) (62)
  - Chats (290) (70)
    - Facebook (41) (340 messages)
    - Signal Private Messenger (9) (1) (29 m
    - Twitter (79) (250 messages)
    - WhatsApp (161) (69) (42076 messages
  - Contacts (14487) (679)
  - Cookies (5591) (98)
  - Device Locations (4780) (73)
  - Device Notifications (41) (1)
  - Device Users (1)
  - Emails (1384) (655)
  - Installed Applications (220) (2)
  - Instant Messages (253) (9)
  - MMS Messages (41) (1)
  - Passwords (29)
  - Powering Events (7)
  - Searched Items (765) (85)
  - SMS Messages (3911) (210)
  - User Accounts (49)
  - User Dictionary (6)
  - Web Bookmarks (4)
  - Web History (9489) (4578)
  - Wireless Networks (76) (8)
- Data Files

Extraction Summary

Extractions: 1

Physical
HTC 0PE6400 Desire 620
Physical [ADB Rooted]

Extraction start date/time
3/17/2018 1:19:35 PM(UTC+1)
Extraction end date/time
3/17/2018 1:54:34 PM(UTC+1)
E:\My Reports\2018-03-18.18-20-54\HTC_...

Device Info

Bluetooth MAC Address	[redacted]
Android ID	[redacted]
Bluetooth device name	[redacted]
OS Version	4.4.4
Android fingerprint	[redacted]
Detected Phone Model	HTC Desire 620
Detected Phone Vendor	htc
Phone Activation Time	2/20/2015 10:41:55 PM(UTC+0)
Phone Activation Time	5/1/2016 6:41:54 AM(UTC+0)
Bluetooth MAC Address	[redacted]
Locale language	en
Country Name	GB
Time Zone	[redacted]
Mock locations allowed	False
Auto Time Zone	True
Auto Time	True
Location Services Enabled	True
IMSI	[redacted]
ICCID	[redacted]
Advertising Id	[redacted]
MSISDN	[redacted]
Tethering	
Hotspot password required	[redacted]
Last Activation Time	[redacted]
Unlock Pattern	
[redacted]	7->4->1->5 [redacted]

Figure 18: Physical extraction of author’s HTC Desire using Cellebrite UFED

Analysis: Analytics on extracted data

A number of tools with impressive analytical capabilities are on offer to help investigators deal with extracted data.

> *"There are a lot of tools for analysis of physical dumps and backups of mobile devices running Android operating systems. These tools include all the best mobile forensics tools, such as UFED Physical Analyzer (Cellebrite), Oxygen Forensics (Oxygen Forensics, Inc), XRY (MSAB), MOBILedit Forensic Express (COMPELSON Labs), and Secure View (Susteen)."*[cxviii]

> *"Examination and analysis using third-party tools is generally performed by importing the device's memory dump into a mobile forensics tool which will automatically retrieve the results."*[cxix]

Cellebrite's Physical Analyzer is a user-friendly piece of software that is designed to organise data extracted in different file types from XML, CSV, TXT to CDR, media and text. It can bring together datasets from different devices, recognise and categorise digital media. Physical Analyzer can display all the information that was extracted. It also has considerable data diving and visualisation capabilities.

> *"The analytics system unifies all drone, mobile, cloud, computer and telecommunications data in a centralised view so you don't waste previous time using separate tools."*[cxx]

Link analysis is used to analyze phone calls, emails text messages and location data in order to discover associations between individuals via different types of data.[cxxi] As noted by Professor Peter Sommer in evidence to the UK Parliament:

> *"Use is also made of data visualisation / link analysis techniques to demonstrate frequencies over time of contacts between phone numbers and between IP addresses, financial transactions and chronologies of events among others."*[cxxii]

Police in the UK are trialling Cellebrite's machine learning tools[cxxiii] to interpret images, match faces and analyse patterns of communication. Cellebrite states that:

> *"... data can be extracted along with other sources of critical information, such as online activity from email and social media accounts. These sources can then be filtered, compared and analysed using artificial intelligence and machine learning to generate actionable insights, such as locations...Extracted data can be combined with data from public sources - such as websites or social media accounts - to find crucial information and make comparisons. Investigators can use the combined data to build profiles of attackers, their contacts, and members of wider terror cells. The data can also create timelines of events, helping investigators to determine exactly what has happened and compile the right evidence for a prosecution."*[cxxiv]

Magnet AXIOM is also utilising machine learning techniques:

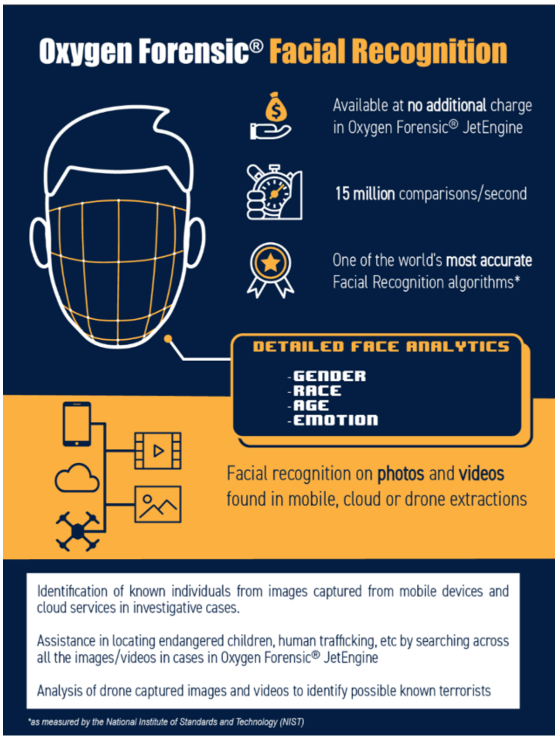
> *"...with features like Connections and Magnet.AI, you can automatically generate insights that could lead to important breakthroughs in your examinations."*[cxxv]

> *"Machine learning, via Magnet.AI, offers … a predictive apparatus "trained" to recognize messages that fall into … categories."*[cxxvi]

> *"With the launch of AXIOM 2.0, the Magnet.AI module now identifies images that may contain depictions of child sexual abuse, nudity, weapons and drugs. We've also expanded our text classification model to detect potential sexual conversations in addition to child luring."*[cxxvii]

In August 2017 Cellebrite introduced what it called "advanced machine learning technology" for its analytics platform, which can be used to analyse data extracted from the cloud and which included face recognition and matching[cxxviii].

From July 2019, Oxygen Forensics JetEngine module, built into Oxygen Forensic Detective, provides the ability to categorise human faces using their own technology. Not only do they provide the categorisation and matching of faces within extract data, facial analytics is included gender, race and emotion recognition[cxxix]. Lee Reiber, Oxygen's chief operating officer said the tool can *"search for a specific face in an evidence trove, or cluster images of the same person together. They can also filter faces by race or age group, and emotions such as "joy" and "anger"."*[cxxx]



Oxygen Forensic® Facial Recognition

Available at no additional charge in Oxygen Forensic® JetEngine

15 million comparisons/second

One of the world's most accurate Facial Recognition algorithms*

DETAILED FACE ANALYTICS
- GENDER
- RACE
- AGE
- EMOTION

Facial recognition on photos and videos found in mobile, cloud or drone extractions

Identification of known individuals from images captured from mobile devices and cloud services in investigative cases.

Assistance in locating endangered children, human trafficking, etc by searching across all the images/videos in cases in Oxygen Forensic® JetEngine

Analysis of drone captured images and videos to identify possible known terrorists

*as measured by the National Institute of Standards and Technology (NIST)

Conclusion

As the use of mobile phone extraction proliferates, whether it is used by law enforcement or border security, the data from these devices will be used to challenge an individual whether in criminal, civil or immigration proceedings and procedures. There is little technical information available to individuals, to those who may represent them and those who campaign on these issues. Whilst mobile forensics is a rapidly changing field, this is an attempt to look at what is going on when those who use powerful extraction tools seek data from devices.

The use of mobile forensics raises issues complex issues relating to the reliability of the extracted data as a form of evidence, particularly if it is used by unskilled individuals who rely on the push button technologies but are not digital forensic analysts[cxxxi].

> *"What I am seeing in the field is that regular police officers are trying to be digital forensic analysts because they are being given these rather whizzy magic tools that do everything, and a regular police officer, as good as he may be, is not a digital forensic analyst. They are pushing some buttons, getting some output and, quite frequently, it is being looked over by the officer in charge of the case, who has no more training in this, and probably less, than him. They will jump to conclusions about what that means because they are being pressured to do so, and they do not have the resources or the training to be able to make the right inferences from those results. That is going smack in front of the court."*[cxxxii]

The delivery of justice depends on the integrity and accuracy of evidence and trust that society has in it. We hope that in starting to unpick some of the complexities in this field, we can inform the debate on this topic.

[i] Cox, J, February 2018, [ONLINE] Available at: https://motherboard.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware [Accessed 23.03.2019]

[ii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.151

[iii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.33

[iv] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.186

[v] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018 p.72

[vi] https://support.apple.com/en-us/HT208857

[vii] https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf

[viii] https://blog.elcomsoft.com/2019/09/usb-restricted-mode-in-ios-13-apple-vs-graykey-round-two/

[ix] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.72

[x] Afonin, O, October 2017, Elcomsoft blog [ONLINE] Available at: https://blog.elcomsoft.com/2017/10/ios-vs-android-physical-data-extraction-and-data-protection-compared/ [Accessed on 5 April 2019]

[xi] Mikhaylov, I, *Mobile Forensics Cookbook*, Birmingham, Packt Publishing, 2017, p.37

[xii] Embury, Woolley, Soh, December 2018, Cellebrite Webinars [ONLINE] Available at: https://www.cellebrite.com/en/webinars/advance-your-toughest-investigations-with-cellebrite-advanced-services/ slide 14 [Accessed on 15 January 2019]

[xiii] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.10

[xiv] See Annex B

[xv] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.11

[xvi] McQuaid, J, February 2018, Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/blog/device-agnostic-mobile-acquisition-who-needs-model-numbers/ [Accessed on 21 April 2019]

[xvii] McQuaid, J 2019, Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/resources/recorded-webinar-an-in-depth-look-at-different-password-bypass-options-2/?submission=https://go.magnetforensics.com/l/52162/2018-11-14/jxklfj [Accessed on 24 March 2019]

[xviii] MOBILedit News (October 2018) MobilEdit [ONLINE] Available at: https://www.mobiledit.com/news [Accessed on 01 April 2019]

[xix] MOBILedit News (October 2018) MobilEdit [ONLINE] Available at: https://www.mobiledit.com/news [Accessed on 01 April 2019]

[xx] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.17

[xxi] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.223

[xxii] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.68

[xxiii] Cellebrite, (2019) Smarter Forensics [ONLINE] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[xxiv] McQuaid, J, (2018) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/resources/recorded-webinar-an-in-depth-look-at-different-password-bypass-options-2/?submission=https://go.magnetforensics.com/l/52162/2018-11-14/jxklfj [Accessed on 24 March 2019]

[xxv] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.238

[xxvi] Teel Technologies, (2019) Teel Technologies [ONLINE] Available at: http://www.teeltech.com/mobile-device-forensics-training/in-system-programming-for-mobile-device-forensics/ [Accessed 27 March 2019]

[xxvii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.24

[xxviii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.23

[xxix] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.25

[xxx] *'live and file system data'* Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.64

[xxxi] See Annex B

[xxxii] MSAB (2019) [ONLINE] Available at: https://www.msab.com/ (Accessed on 28 March 2019)

[xxxiii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.64

[xxxiv] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.189

[xxxv] MSAB (2019) MSAB [ONLINE] Available at:, https://www.msab.com/products/xry/xry-logical/ [Accessed on 28 April 2019]

[xxxvi] MSAB (2019) MSAB [ONLINE] Available at:, https://www.msab.com/products/xry/xry-logical/ [Accessed on 28 April 2019]

[xxxvii] MSAB (2019) MSAB [ONLINE] Available at: https://www.msab.com/products/xry/xry-logical/ [Accessed on 28 April 2019]

[xxxviii] McQuaid, J (2019), Magnet Forensics [ONLINE], Available at: https://www.magnetforensics.com/resources/recorded-webinar-an-in-depth-look-at-different-password-bypass-options-2/?submission=https://go.magnetforensics.com/l/52162/2018-11-14/jxklfj [Accessed on 24 March 2019]

[xxxix] Homeland Security, (November 2018) Homeland Security Science and Technology [ONLINE] Available at: https://www.dhs.gov/sites/default/files/publications/Test%20Report_NIST_Mobile%20Device%20Acquisition%20Tool%20XRY%20v7.8.0_November%202018.pdf p.12, [Accessed on 05.04.2019]

[xl] SalvationData (August 2018) SalvationData [ONLINE] Available at: https://blog.salvationdata.com/2018/08/06/case-study-mobile-forensics-downgrade-extraction-collect-app-data-without-root/ [Accessed on 29 March 2019]

[xli] BeauHD (September 2017) Slashdot [ONLINE] Available at: https://tech.slashdot.org/story/17/09/06/2027200/android-oreos-rollback-protection-will-block-os-downgrades [Accessed on 30 March 2019]

[xlii] Cellebrite Product Updates (March 2019) Cellebrite [ONLINE] https://www.cellebrite.com/en/productupdates/exclusive-access-to-whatsapp-data-and-another-40-apps-on-android-devices/ [Accessed on 30 March 2019]

[xliii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.73 & https://hub.packtpub.com/how-to-extract-sim-card-data-from-android-devices-tutorial/ accessed on 28.03.2019

[xliv] Watson A (March 2018) Cellebrite [ONLINE] Available at: https://www.cellebrite.com/en/blog/access-inaccessible-apps-with-virtual-analyzer-sqlite-wizard/ [Accessed on 1 May 2019]

[xlv] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.23

[xlvi] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.23

[xlvii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018 p.64

[xlviii] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.159

[xlix] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.23

[l] Brewster, T, (April 2017) Forbes [ONLINE] Available at: https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#70936d81a1fc [Accessed on 23 March 2019]

[li] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[lii] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[liii] Mikhaylov, I, *Mobile Forensics Cookbook*, Birmingham, Packt Publishing, 2017, p.51

[liv] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.159

[lv] Cellebrite Product Update (May 2018) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2019/02/ReleaseNotes_UFED_7.15.pdf (Accessed on 28 April 2019)

[lvi] https://vpnpick.com/vtech-innotab-max-tablet-found-easy-hack-may-explain-recent-data-breach/

[lvii] https://www.pcmag.com/encyclopedia/term/64003/usb-debugging-mode

[lviii] https://www.howtogeek.com/258788/what-is-usb-debugging-and-is-it-safe-to-leave-it-enabled-on-android/

[lix] https://www.howtogeek.com/125769/how-to-install-and-use-abd-the-android-debug-bridge-utility/

[lx] Lahoti, S, (February 2019) PacktPublishing [ONLINE] Available at: https://hub.packtpub.com/how-to-extract-sim-card-data-from-android-devices-tutorial/ [Accessed on 20 April 2019]

[lxi] Vance, C (March 2018) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/blog/extracting-data-from-a-samsung-device-using-advanced-mtp/ [Accessed on 27 March 2019]

[lxii] Vance, C (March 2018) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/blog/extracting-data-from-a-samsung-device-using-advanced-mtp/ [Accessed on 27 March 2019]

[lxiii] Vance, C (March 2018) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/blog/extracting-data-from-a-samsung-device-using-advanced-mtp/ [Accessed on 27 March 2019]

[lxiv] Vance, C (March 2018) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/blog/extracting-data-from-a-samsung-device-using-advanced-mtp/ [Accessed on 27 March 2019]

[lxv] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.34

[lxvi] REFERENCE

[lxvii] Cellebrite, (2019) Smarter Forensics [ONLINE] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[lxviii] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.159

[lxix] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.163

[lxx] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.162

[lxxi] Cellebrite Product Updates (February 2019) [ONLINE] Available at: https://www.cellebrite.com/en/productupdates/supporting-new-extraction-methods-and-devices/ [Accessed on 23 March 2019]

[lxxii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.152

[lxxiii] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[lxxiv] Forensics Detective Guide (2019) Oxygen Forensics [ONLINE] Available at: https://www.oxygen-forensic.com/en/uploads/doc_guide/Oxygen_Forensic_Detective_Getting_started2.pdf p.17 [Accessed on 23 March 2019]

[lxxv] Magnet Products (2019) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/products/magnet-acquire/ [Accessed on 28 April 2019]

[lxxvi] Mikhaylov, I, *Mobile Forensics Cookbook*, Birmingham, Packt Publishing, 2017, p.67

[lxxvii] Afonin, O (October 2017) Elcomsoft [ONLINE] Available at: https://blog.elcomsoft.com/2017/10/ios-vs-android-physical-data-extraction-and-data-protection-compared/ [Accessed on 30 March 2019]

[lxxviii] Apple Developer (2019) Apple [ONLINE] Available at: https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave [Accessed on: 28 March 2019]

[lxxix] Afonin, O (October 2017) Elcomsoft [ONLINE] Available at: https://blog.elcomsoft.com/2017/10/ios-vs-android-physical-data-extraction-and-data-protection-compared/ [Accessed on 30 March 2019]

[lxxx] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.83

[lxxxi] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[lxxxii] Whereas an iTunes Backup would only retrieve 7GB and the UFED would only get 4GB. A physical extraction would have obtained the remaining 11G (deleted / unallocated space) which is unobtainable because iOS uses file-based encryption. When a picture or video is deleted for example, the key is thrown away. Each file has a key. There is therefore no way to recover the deleted data as even if you could extract it, you could not decrypt it. Embury, Woolley, Soh, December 2018, Cellebrite Webinars [ONLINE] Available at: https://www.cellebrite.com/en/webinars/advance-your-toughest-investigations-with-cellebrite-advanced-services/ slide 14 [Accessed on 15 January 2019]

[lxxxiii] Embury, Woolley, Soh, December 2018, Cellebrite Webinars [ONLINE] Available at: https://www.cellebrite.com/en/webinars/advance-your-toughest-investigations-with-cellebrite-advanced-services/ slide 14 [Accessed on 15 January 2019]

[lxxxiv] Carmelli, Armon, Embury, Goldberg, Tal, (June 2018) Cellebrite [ONLINE] Available at: https://www.cellebrite.com/en/webinars/decoding-ios-extractions-understanding-analytics-and-future-trends/ [Accessed on 28 March 2019]

[lxxxv] Embury, Soh, Woolley (December 2018) Cellebrite [ONLINE] Available at: https://www.cellebrite.com/en/webinars/advance-your-toughest-investigations-with-cellebrite-advanced-services/ [Accessed on 28 March 2019]

[lxxxvi] https://www.theguardian.com/uk-news/2019/jun/12/police-forensics-contractor-sytech-allegedly-sent-phones-to-fone-fun-shop

[lxxxvii] https://www.theguardian.com/uk-news/2019/jun/12/police-forensics-contractor-sytech-allegedly-sent-phones-to-fone-fun-shop

[lxxxviii]Magnet Forensics (2019) [ONLINE] Available at: https://www.magnetforensics.com/graykey/ [Accessed on 21 April 2019]

[lxxxix] Burgess, M (October 2018) Wired [ONLINE] Available at: https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk [Accessed on 21 April 2019]

[xc] Blog (February 2019) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/blog/maximizing-the-partnership-between-graykey-and-magnet-axiom/ [Accessed on 21 April 2019]

[xci] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.23

[xcii] Tal, S, *Forensic Breakthrough, New Ways to Extract Encrypted Phones*, Cellebrite, 2018

[xciii] Tal, S, *Forensic Breakthrough, New Ways to Extract Encrypted Phones*, Cellebrite, 2018

[xciv] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics, Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.23

[xcv] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.164

[xcvi] Forensic Breakthrough, New Ways to Extract Encrypted Phones, Shahar Tal, VP Research, Security Research Lab, Cellebrite, 2018

[xcvii] Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.189

[xcviii] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23.03.2019]

[xcix] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[c] Cellebrite, (2019) Smarter Forensics [online] Available at: https://smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf [Accessed on 23 March 2019]

[ci] Forensic Breakthrough, New Ways to Extract Encrypted Phones, Shahar Tal, VP Research, Security Research Lab, Cellebrite, 2018

[cii] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.85

[ciii] Afonin, O (February 2019) Elcomsoft [ONLINE] Available at: https://blog.elcomsoft.com/2019/02/physical-extraction-and-file-system-imaging-of-ios-12-devices/ [Accessed on 23 March 2019]

[civ]News (February 2019) Elcomsoft [ONLINE] Available at: https://www.elcomsoft.co.uk/news/716.html [Accessed on 23 March 2019]

[cv] News (February 2019) Elcomsoft [ONLINE] Available at: https://www.elcomsoft.co.uk/news/716.html [Accessed on 23 March 2019]

[cvi] Afonin, O (July 2018), [ONLINE] Available at: https://blog.elcomsoft.com/2018/07/electra-jailbreak-ios-11-2-11-3-1-iphone-physical-acquisition/ Accessed on 1 April 2019

[cvii] Afonin, O (July 2018), [ONLINE] Available at: https://blog.elcomsoft.com/2018/07/electra-jailbreak-ios-11-2-11-3-1-iphone-physical-acquisition/ Accessed on 1 April 2019

[cviii] Mikhaylov, I, *Mobile Forensics Cookbook*, Birmingham, Packt Publishing, 2017, p.72

[cix] Cellebrite Webinar (February 2018) *Safely extract digital evidence with emergency download* [ONLIN] Available at: https://www.cellebrite.com/en/blog/webinar-understand-emergency-download-mode-edl-to-get-forensically-sound-access-to-mobile-devices/

[cx] Cellebrite Webinar (February 2018) *Safely extract digital evidence with emergency download* [ONLIN] Available at: https://www.cellebrite.com/en/blog/webinar-understand-emergency-download-mode-edl-to-get-forensically-sound-access-to-mobile-devices/

[cxi] Kennedy, J (October 2018) Cellebrite [ONLINE] *The convergence of physical and virtual data for faster discovery of evidence* Available at: https://www.cellebrite.com/en/webinars/the-convergence-of-physical-and-virtual-data-for-faster-discovery-of-evidence/

[cxii] INV Solutions (2019) [ONLINE] Available at: https://www.invsolutionsllc.net/physical-extraction-using-enhanced-bootloader/ [Accessed on 23 March 2019]

[cxiii] Magnet Forensics (September 2018) [ONLINE] Available at: https://www.magnetforensics.com/blog/qualcomm-phone-edl-mode/ [Accessed on 23 March 2019]

[cxiv] Oxygen Forensics (undated) [ONLINE] Available at: https://www.oxygen-forensic.com/en/uploads/doc_guide/How_to_extract_data_from_devices_based_on_Qualcomm_chipsets_via_EDL_mode.pdf [Accessed 31 March 2019]

[cxv] Forensic Breakthrough, New Ways to Extract Encrypted Phones, Shahar Tal, VP Research, Security Research Lab, Cellebrite, 2018

[cxvi] Oxygen Forensics (undated) [ONLINE] Available at: https://www.oxygen-forensic.com/en/uploads/doc_guide/How_to_extract_data_from_devices_based_on_Qualcomm_chipsets_via_EDL_mode.pdf [Accessed 31 March 2019]

[cxvii] West, Colangelo, Cole, Lorenz (October 2018) Cellebrite [ONLINE], Available at: https://www.cellebrite.com/en/webinars/the-convergence-of-physical-and-virtual-data-for-faster-discovery-of-evidence [Accessed on 20 December 2018]

[cxviii] Mikhaylov, I, *Mobile Forensics Cookbook*, Birmingham, Packt Publishing, 2017, p.181

[cxix] Tamma, Skulkin, Mahalik, Bommisetty, *Practical Mobile Forensics*, *Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android , and the Windows Phone platforms*, Birmingham, Packt Publishing, 2018, p.27

[cxx] Armon, B (undated) Cellebrite [ONLINE] Available at: https://www.cellebrite.com/en/whitepapers/digital-forensics-is-changing-how-law-enforcement-prevents-and-responds-to-terrorism/ [Accessed on 20 December 2018]

[cxxi] Mena, J, (undated) Info Sec Today [ONLINE] Available at: http://www.infosectoday.com/Articles/Machine_Learning_Forensics/Machine_Learning_Forensics.htm [Accessed on 1 February 2019]

[cxxii] Sommer, P, 'Supplementary written evidence' [ONLINE] Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/92608.html [Accessed on 5 May 2019]

[cxxiii] Bowcott, Devlin (May 2018) The Guardian [ONLINE] Available at: https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence [Accessed on 1 May 2019]

[cxxiv] Cellebrite (2018) White Paper *Digital Forensics is changing how law enforcement prevents and responds to terrorism*, Available at: https://www.cellebrite.com/en/whitepapers/digital-forensics-is-changing-how-law-enforcement-prevents-and-responds-to-terrorism/ [Accessed on 1 February 2019]

[cxxv] Products (2019) Magnet Forensics [ONLINE] Available at: https://www.magnetforensics.com/products/magnet-axiom/ [Accessed on 24 March 2019]

[cxxvi] New Features (April 2017) Magnet Forensics, [ONLINE] Available at: https://www.magnetforensics.com/blog/introducing-magnet-ai-putting-machine-learning-work-forensics/ [Accessed on 23 March 2019]

[cxxvii] New Features (April 2017) Magnet Forensics, [ONLINE] Available at: https://www.magnetforensics.com/blog/introducing-magnet-ai-putting-machine-learning-work-forensics/ [Accessed on 23 March 2019]

[cxxviii] https://www.cellebrite.com/en/press/cellebrite-introduces-advanced-machine-learning-technology-to-analytics-solution-to-accelerate-evidence-discovery/

[cxxix] https://forensicfocus.com/News/article/sid=3567/

[cxxx] https://www.wired.com/story/amazon-detect-fear-face-you-scared/?mbid=social_twitter_onsiteshare

[cxxxi] https://privacyinternational.org/news-analysis/2901/push-button-evidence

[cxxxii] Dr Jan Collie, 27 November 2018, oral evidence http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/oral/93059.html