Android Deep Dive With Chuck Easttom

Lesson 3 Android Forensics

Evidence from phones

- Photo/video
- Texts
- Contacts
- Call Info

Actual cases

- Adam Howe took a “selfie” photo of himself at the scene of a church burglary. This evidence led to a search of the suspect’s property, which turned up the stolen goods from the church.
- A Manchester University student, Mikayla Munn, gave birth to a baby in her dorm room bathtub. She immediately drowned her new born in the bath tub but covered it up stating that she was not aware of her pregnancy and labor pains were felt while taking a bath, followed by the baby’s arrival. On verifying her digital assets, investigators have found that she had searched on Google for “at home abortions” and “ways to cut the umbilical cord of a baby.” Munn pleaded guilty to neglect and was imprisoned for 9 years.

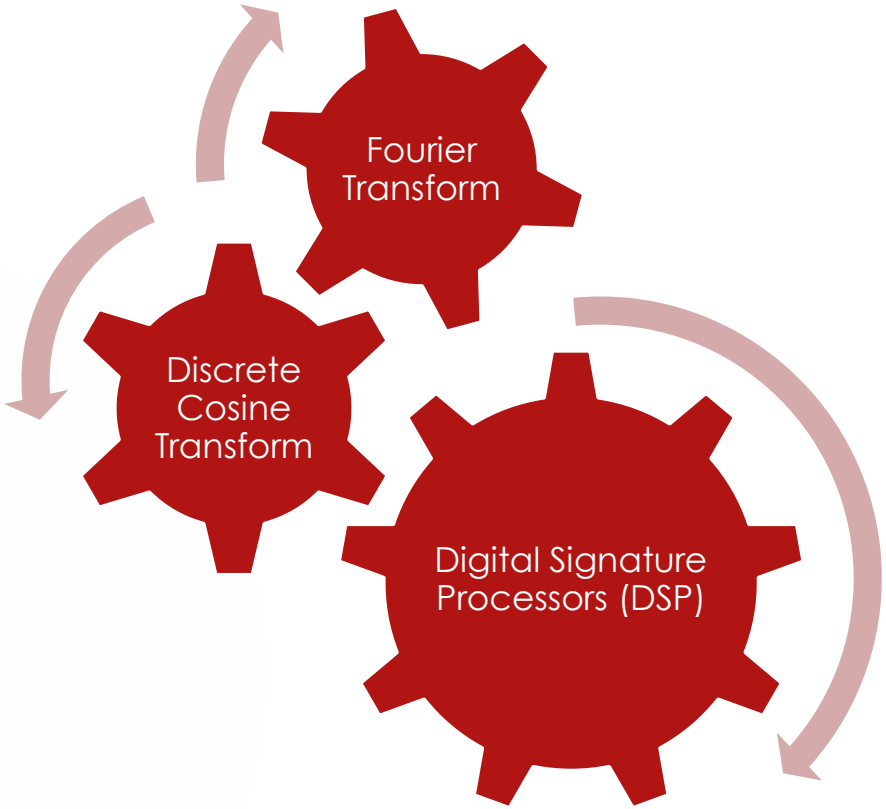
Actual Cases

- A child swore that her stepfather was abusing her and that he would video the alleged molestation with his cell phone. The stepfather denied the allegations and willingly turned over his phone for examination. The local PD examiner used a popular tool but the only videos he found were benign. In subsequent interviews with the investigators the girl continued to stick to her story. A manual file carving examination of the physical image of the phone uncovered 108 deleted video files; proving the child's allegations

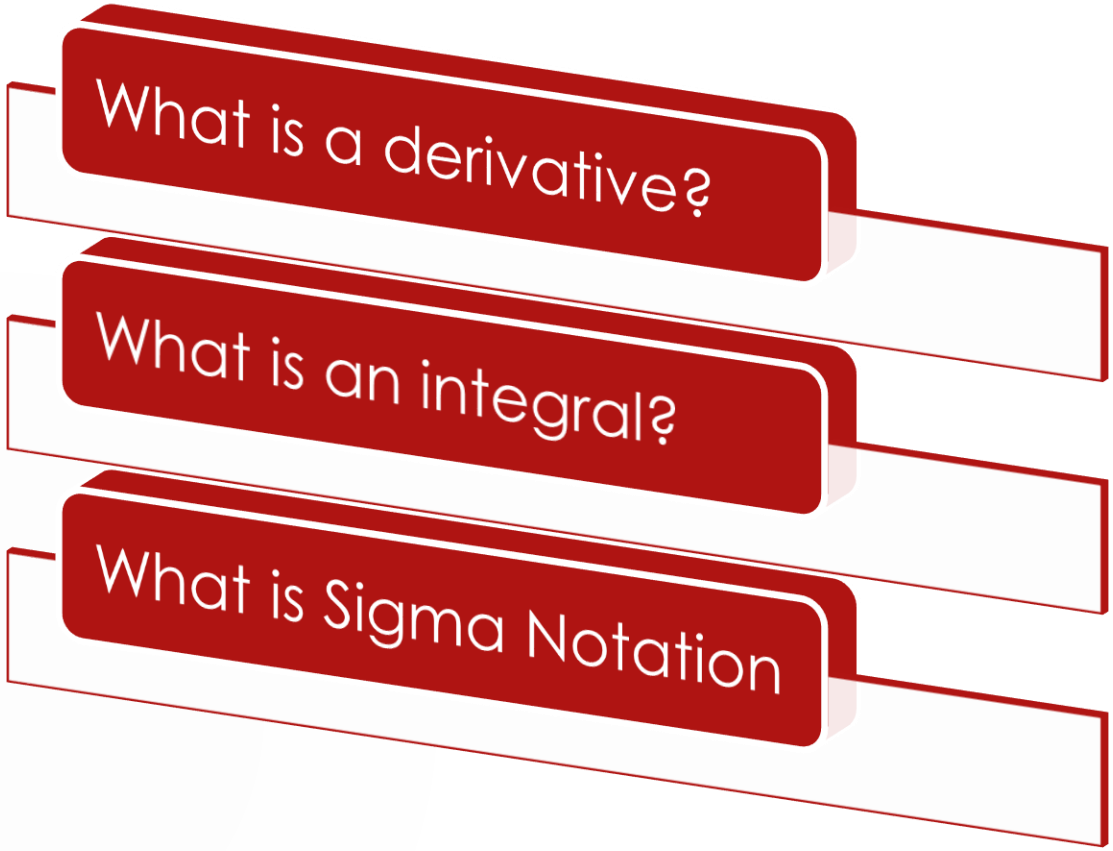
Actual Cases

- Vanity Fair has a disturbing tale about two Canadian teenage boys who tortured, raped, and murdered a classmate, Kim Proctor, after she dumped one of them via text message. While they burned her body, they were unable to eradicate the damning trail of evidence they left behind in the form of Wikipedia searches (for "lithotomy position" among others), instant messages, a confession in a World of Warcraft chat, GPS data associated with an "alibi" text message sent from the scene of the murder, and Google map searches for places to dump the body. The tragic tale, via Wired, is told through that same evidence by journalist David Kushner. His interviews with law enforcement speak to how important digital evidence has become for investigating crimes involving "digital natives":

Cellular Telephony Basics



A little math



Fourier Transform

A Fourier transform basically decomposes a function of time (a signal) into the frequencies that make it up. The term Fourier transform refers to both the frequency domain representation and the mathematical operation that associates the frequency domain representation to a function of time.

Any Real Number

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i x \xi}\,dx,$$

Called a 'circumflex" and represents a definite integral

Discrete Cosine Transform

- This function expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies.

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \qquad k = 0, \ldots, N-1.$$

Cellular Telephony Basics

- Cells and base stations
  - Space is divided into *cells*, and each cell has a *base station* (tower and radio equipment)
  - Base stations coordinate themselves so mobile users can access the network
  - If you move from one cell to another, the first cell notices your signal strength *decreasing*, the second cell notices your signal strength *increasing*, and they coordinate *handover* so your handset switches to the latter cell

Terms

- **Mobile Switching Center (MSC)** This is the switching system for the cell network. These can be used in 3G or in GSM networks (you will learn about both of those terms later in this section). The MSC processes all the connections from both mobile devices and land line calls. It is also responsible for routing calls between base stations and the public switched telephone network (PSTN).
- **Base Transceiver Station (BTS)** This is the part of the cell network responsible for communications between the mobile phone and the network switching system. It consists of a base transceiver station and a base station controller. The BSS Base Station System is radio transceiver equipment that communicates with cellular devices. The BSC is a central controller coordinating the other pieces of the BSS.

Terms

- **Home Location Register (HLR)** The database used by the MSC for subscriber data and service information. It is related to the Visitor Location Register (VLR) which is used for roaming phones.
- **Subscriber Identity Module (SIM)** This is a circuit that stores the International Mobile Subscriber Identity (IMSI). Think of it as how you identify the phone. Many modern phones have removable SIM, which means you could change out the SIM and essentially have a different phone with a different number. A SIM card contains its unique serial number (ICCID), the IMSI, security authentication and ciphering information. This SIM will also usually have network information, services the user has access to and two passwords. Those passwords are the personal identification number (PIN) and the personal unblocking code (PUK).

Terms

- **Electronic Serial Number (ESN)** ESN's were developed by the United States Federal Communications Commission (FCC) to identify cell phones. They are now only used in CDMA phones (CDMA is discussed later in this section) whereas GSM and later phones use the International Mobile Equipment Identity (IMEI) number. The first 8 bits of the ESN identify the manufacturer, and subsequent 24 bits uniquely identify the phone. The IMEI is used with GSM and LTE as well as other types of phones.
- **Personal Unlock Number (PUK)** This is a code used to reset a forgotten PIN. Now using the code, will return the phone to its original state, losing most forensic data. If the code is entered incorrectly 10 times in a row, the device becomes permanently blocked and unrecoverable.

Terms

- **ICCID: Integrated Circuit Card Identification** Each SIM is identified by its integrated circuit card identifier (ICCID). These numbers are engraved on the SIM during manufacturing. This number has sub sections that are very important for forensics. Starting with the Issuer identification number (IIN), which is a seven digit number that identifies the country code and issuer. There is also a variable length individual account identification number to identify the specific phone, and a check digit.
- **IMEI** The International Mobile Equipment Identity or IMEI a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dialpad, or alongside other system information in the settings menu on smartphone operating systems.

ICCID

From ForensicWiki the example 89 91 10 1200 00 320451 0

- The first two digits (89 in the example) refers to the Major Industry Identifier.
- The next two digits (91 in the example) refers to the country code (91-India).
- The next two digits (10 in the example) refers to the issuer identifier number.
- The next four digits (1200 in the example) refers to the month and year of manufacturing.
- The next two digits (00 in the example) refers to the switch configuration code.
- The next six digits (320451 in the example) refers to the SIM number.
- The last digit which is separated from the rest is called the checksum digit.

Networks

- GSM: Global System for Mobile communications. This is a standard developed by the European Telecommunications Standards Institute (ETSI). Basically GSM is the 2G network.
- EDGE: Enhanced Data Rates for GSM Evolution. This one does not fit neatly into the 2g/3g/4g spectrum. It is technically considered pre-3g but was an improvement on GSM (2g). So one could consider it a bridge between 2g and 3g technology.
- UMTS: Universal Mobile Telecommunications Systems. This is a 3g standard based on GSM. It is essentially an improvement of GSM.
- LTE: Long Term Evolution. This is a standard for wireless communication of high-speed data for mobile devices. This is what is commonly called 4G.
- Wi-Fi: All cellular phones and other mobile devices today are able to connect to Wi-Fi networks. Wireless networking has become the norm and free Wi-Fi hot spots can be found in restaurants, coffee shops, and hotels.

5G

- 5th-Generation Wireless Systems (abbreviated 5G)
- Meets ITU IMT-2020 requirements and 3GPP Release 15
- Peak Data Rate 20 Gbit/s
- Expected User Data Rate 100 Mbit/s

NIST Cell Phone Characteristics

- Despite their differences in technology, cellular networks are organized similarly to one another, in a manner illustrated in Figure 1. The main components are the radio transceiver equipment that communicates with mobile phones, the controller that manages the transceiver equipment and performs channel assignment, and the switching system for the cellular network. The technical names for these components are respectively the Base Transceiver Station (BTS), the Base Station Controller (BSC), and the Mobile Switching Center (MSC). The BSC and the BTS units it controls are sometimes collectively referred to as a Base Station
- Subsystem. The transceivers at the BTS can be configured in a variety of ways. A typical configuration involves three distinct sectors of 120 degree coverage: 0 degrees North to 120 degrees Southeast, 120 degrees Southeast to 240 degrees Southwest, and 240 degrees Southwest to 360 degrees North. A cell identifier uniquely identifies the BTS and sector involved in servicing a call.

NIST Cell Phone Organization

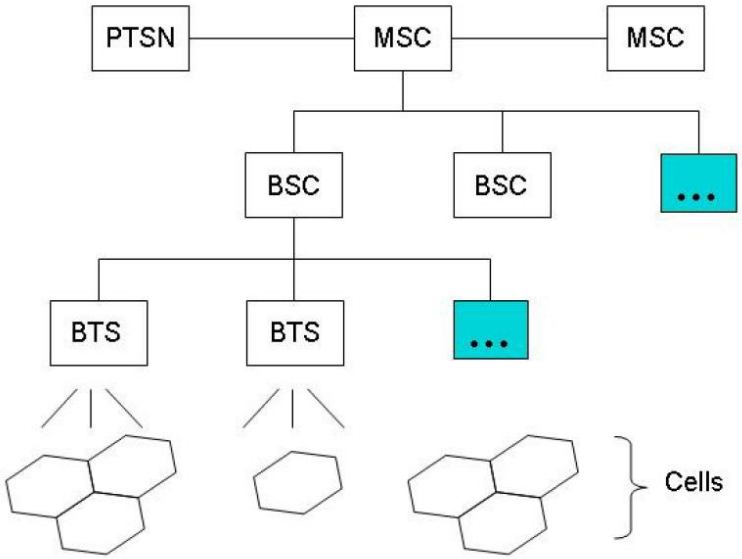


Figure 1: Cellular Network Organization

Source: NIST Guidelines on Cell Phone Forensics

RFC 3227 - Continued

The following is a direct quote from the RFC

- - Don't shutdown until you've completed evidence collection. Much evidence may be lost and the attacker may have altered the startup/shutdown scripts/services to destroy evidence.

- - Don't trust the programs on the system. Run your evidence gathering programs from appropriately protected media

- - Don't run programs that modify the access time of all files on the system (e.g., 'tar' or 'xcopy‘)

RFC 3227 - Continued

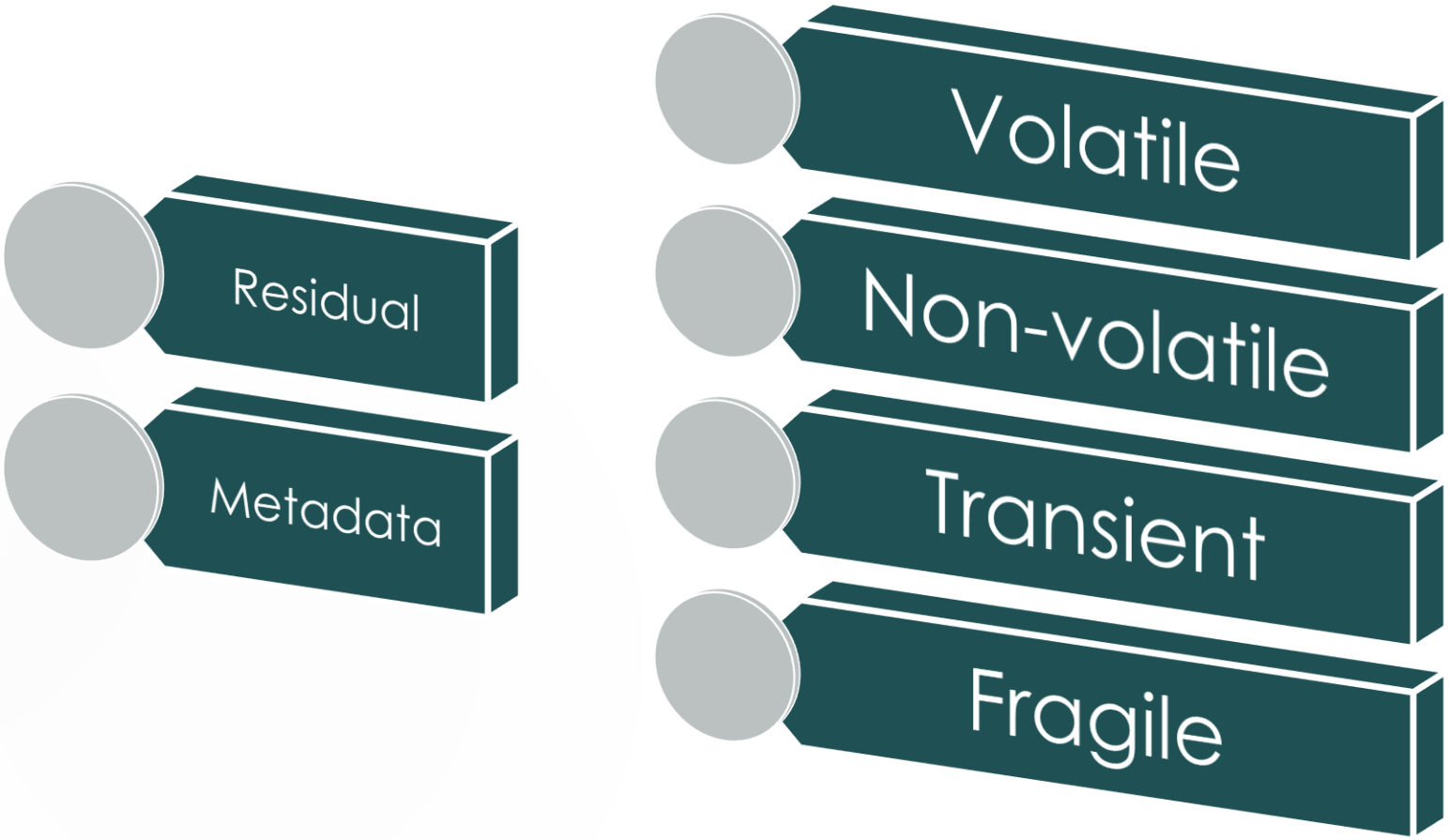
The following is a direct quote from the RFC

- - Admissible: It must conform to certain legal rules before it can be put before a court.
- - Authentic: It must be possible to positively tie evidentiary material to the incident.
- - Complete: It must tell the whole story and not just a particular perspective.
- - Reliable: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- - Believable: It must be readily believable and understandable by a court.

Order of Volatility - CHFI

- Registers/Cache
- Routing Table, process table, memory, kernel statistics
- Temp files
- Disk or other storage
- Remote logging
- Configuration/Network Topology
- Archive Media

Types of Evidence



Organizations

- SWGDE – Scientific Working Group on Digital Evidence - CCFP
- IOCE - International Organization on Computer Evidence - CHFI

The Scientific Method

- First let us examine how science works. One always begins with an hypothesis. Contrary to popular misconception, an hypothesis is not a guess. It is a question that is testable. If a question cannot be tested, then it has no place in science whatsoever. Once one has tested an hypothesis, one has a fact. For example if I suspect that confidential documents where on your computer and subsequently moved to a USB device and deleted (my hypothesis), I can conduct a forensic examination of your computer (my test). If that examination finds that a USB drive was connected to the computer and an undelete program recovers the deleted documents, I now have a fact.

The Scientific Method Continued

- The next step is to build a theory of the crime, based on multiple facts. The fact that confidential documents where on your computer, while very interesting evidence, is not in and of itself enough. Is it possible someone else used your computer? Yes it is. Is it possible that you accidently had confidential information (i.e. you mistakenly took home documents you should not have) and then immediately deleted them? Yes it is. So we must find additional facts. For example we would want to know if your username was the one logged in when the files were deleted. Once we recover the deleted files we would want to know when they were last accessed and modified (this might tell us if you were using the files). We might also want to check your email to see if there is any communication with a third party that might have an interest in these documents.

The Scientific Method Continued

- Falsifiability – This means that it is possible to falsify a question, or to get a false answer. In other words it is possible to get a negative answer. This rules out questions of opinion, or questions that cannot be refuted.

Occam's Razor

A problem-solving principle devised by William of Ockham (c. 1287–1347)

"Entities should not be multiplied unnecessarily."

"The principle states that among competing hypotheses that predict equally well, the one with the fewest assumptions should be selected"

"when you have two competing theories that make exactly the same predictions, the simpler one is the better."

Sometimes called Ontological parsimony or: asa rule of thumb, which obliges us to favor theories or hypotheses that make the fewest unwarranted, or ad hoc, assumptions about the data from which they are derived.

Locard's principle of transference

- Dr. Edmond Locard was a forensic scientist who formulated what has become known as Locard's exchange principle or Locard's principle of transference. This principle was first applied to physical forensics, and it essentially states that one cannot interact in any environment without leaving something behind

Daubert

- In Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1994), the Supreme Court held that the Federal Rules of Evidence superseded Frye as the standard for admissibility of expert evidence in federal courts

Daubert

- Standard used by a trial judge to make a preliminary assessment of whether an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Under this standard, the factors that may be considered in determining whether the methodology is valid are:
- (1) whether the theory or technique in question can be and has been tested;
- (2) whether it has been subjected to peer review and publication;
- (3) its known or potential error rate;
- (4) the existence and maintenance of standards controlling its operation; and
- (5) whether it has attracted widespread acceptance within a relevant scientific community.
- The Daubert standard is the test currently used in the federal courts and some state courts.

Three Dimensions of a crime

- **Motive**: does the suspect have motive to have perpetrated the attack? Conversely do alternate suspects have equal or greater motive?
- **Means**: Does it appear that the suspect has the skillset to have perpetrated the attack. It is not always possible to ascertain the skills of a given attacker, nor the minimum skills required for a specific attack. However, some estimation should be formed of the attacker's skills as compared to the sophistication of the attack. This should also be compared to a skillset analysis of other viable suspects, if any exist. This is often referred to as 'means', in traditional criminal investigations, but in cyber forensics can also be considered simply as 'suspect skillset'.
- **Opportunity**: Did the suspect have the opportunity to have been responsible for some or all of the suspect traffic

Time Line Analysis

- Lists all system events, files, activities in chronological order
  - Multiple data sources
  - Multiple systems
- One approach to forensics
- Approaches
  - Automatically gather everything
  - Selective representation

TLN Format

- Pipe “ | ” delimited text file
- 5 fields
  - Time | Source | System | User | Description
- This is one approach, it is easy to follow. The Description field should be lengthy and free form.

Time Formats

- 64-bit FILETIME (UTC)
  - Number of 100 nanosecond intervals since 1/1/1601
- 32-bit Unix time format (UTC)
  - Number of seconds since 1/1/1970
- String based format (local time)
  - 01/01/2014 7:00 PM

Tools

Cellebrite

XRY

Magnet

Oxygen

Black Bag

Mobile Edit

Paraben

Guidelines for PDA/Phone forensics

- NIST guidelines http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf
  - Most Common Operating Systems
    - iOS
    - Android/Linux
    - Windows Mobile (formerly Windows CE)
- SIM: Subscriber Identity Module
- ESN: Electronic Serial Number
- PUK: Personal Unlock Number

Phone states

(taken from NIST guidelines)

- **Nascent State/Factory Default State –** Devices are in the nascent state when received from the manufacturer – the device contains no user data and observes factory configuration settings
- **Active State –** Devices that are in the active state are powered on, performing tasks, and able to be customized by the user and have their filesystems populated with data.
- **Semi-Active State –** The semi-active state is a state partway between active and quiescent. The state is reached by a timer, which is triggered after a period of inactivity allowing battery life to be preserved by dimming the display and taking other appropriate actions.
- **Quiescent State –** The quiescent state is a dormant mode that conserves battery life while maintaining user data and performing other background functions. Context information for the device is preserved in memory to allow a quick resumption of processing when returning to the active state.

GPS

As you travel, you move from one cell to another, and the base stations monitor the strength of your phone's signal. As you move toward the edge of one cell, your **signal strength** diminishes. At the same time, the base station in the cell you are approaching notices the strength of your signal increasing. As you move from cell to cell, the towers transfer your signal from one to the next

GPS

Advanced systems determine the sector in which the mobile phone resides and roughly estimate also the distance to the base station. Further approximation can be done by interpolating signals between adjacent antenna towers. It is possible to achieve a precision of down to 50 meters in urban areas

GPS

Handset-based technology requires the installation of client software on the handset to determine its location

SIM based uses the SIM card signal

WiFi augments cellular signal with wifi

GPS

In a best-case-scenario, a cell phone's signal may be picked up by three or more cell towers, enabling the "triangulation" to work. From a geometric/mathematical standpoint, if you have the distance to an item from each of three distinct points, you can compute the approximate location of that item in relation to the three reference points

Basically average cell phone (without wifi) GPS accuracy is 100 meters or 328.1 feet

NOTE: Some phones now have actual GPS

How does WiFi improve ?

Various organizations, including Google track the BSSID used by wireless routers, and correlate with physical addresses.

An SSID is the Name of a Network

BSSIDs Basic Service Set Identifier. A unique address that identifies the access point/router that creates the wireless network. Identify Access Points and Their Clients. The access points MAC address is used

https://wigle.net/

Pinging

- To “ping” in this context means to send a signal to a particular cell phone and have it respond with the requested data (GPS location and if available Wifi). This is done by the cell phone carrier, usually in response to a law enforcement request citing exigent circumstances.

Cell Phone GPS concepts

- Bearing – directionality of the cell phone to the cell site
- Distance – physical distance between cell phone and the cell site
- Free-Space Path Loss – is the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction

Calculations

Free-space path loss is proportional to the square of the distance between the transmitter and receiver, and also proportional to the square of the frequency of the radio signal.

$$\text{Free Space Path Loss} = \left(\frac{4\pi d}{\lambda}\right)^2$$

d is the distance of the receiver from the transmitter (meters)

λ is the signal wavelength (meters)

f is the signal frequency (Hertz)

c is the speed of light in a vacuum (meters/ sec)

Core Requirements - Examples

Internal Memory

- Device Recognition
  - Cable, Bluetooth, IrDA
- Non-Supported Devices
  - Error message
- Connectivity Errors
- Report Generation
  - GUI, Report
- Logical Acquisition
  - Tool supported data objects

SIM

- Media Recognition
  - PC/SC, proprietary reader
- Non-Supported SIMs
  - Error message
- Connectivity Errors
- PIN
- Report Generation
  - GUI, Report
- Logical Acquisition
  - Tool supported data objects

Optional Requirements - Examples

Internal Memory / SIM Acquisition

- Data Presentation
  - GUI, Report
- Case Data Protection
- Physical Acquisition
- Access Card Creation
- Log File Generation
- Foreign Language
- Remaining Number of PIN/PUK attempts
- Stand-alone Acquisition
- Hashing
  - Overall Case File, Individual Acquired Files

backup with adb

```
C:\projects\teaching\Android\tools>cd platform-tools

C:\projects\teaching\Android\tools\platform-tools>adb devices
List of devices attached
LGL16C9f11b9bf  device
```

```
C:\projects\teaching\Android\tools\platform-tools>adb backup -all -f c:\phonebackup.ab
Now unlock your device and confirm the backup operation...

C:\projects\teaching\Android\tools\platform-tools>
```

Where is the best data?

Call logs register	/data/data/com.android.providers.contacts/databases/contacts2.db
Call logs register (Samsung)	/data/data/com.sec.android.provider.logsprovider/databases/logs.db
Default Browser Passwords	/data/data/com.android.browser/databases/webview.db
Default Browsers History	/data/data/com.android.browser/databases/browser2.db
Dolphin Web Browser History	/data/data/mobi.mgeek.TunnyBrowser/db/browser.db
Facebook App messages	/data/data/com.facebook.katana/databases/threads_db2
Facebook Messenger messages	/data/data/com.facebook.orca/databases/threads_db2
Google Chrome History	/data/data/com.android.chrome/app_chrome/Default/History
Google Chrome Login Data (Passwords)	/data/data/com.android.chrome/app_chrome/Default/Login Data

Where is the best data?

Kik Messenger chat messages	/data/data/kik.android/databases/kikDatabase.db
MeowChat Messages	/data/data/com.minus.android/databases/com.minus.android
Phonebook Contacts	/data/data/com.android.providers.contacts/databases/contacts2.db
Samsung SMS snippets	/data/data/com.sec.android.provider.logsprovider/databases/logs.db
Skype Calls / Messages	/data/data/com.skype.raider/files/<account_name>/main.db
SMS messages	/data/data/com.android.providers.telephony/databases/mmssms.db
Synchronised Accounts	/data/system/users/0/accounts.db
Tinder messages & users	/data/data/com.tinder/databases/tinder.db
Viber calls register	/data/data/com.viber.voip/databases/viber_data
Viber chat messages	/data/data/com.viber.voip/databases/viber_messages
WhatsApp Contacts	/data/data/com.whatsapp/databases/wa.db
WhatsApp Messages & Calls	/data/data/com.whatsapp/databases/msgstore.db
Wi-Fi passwords (WPA-PSK/WEP)	/data/misc/wifi/wpa_supplicant.conf

Databases and SQLite

SQLite is not a client–server database engine. Rather, it is embedded into the end program
SQLite is a popular choice as embedded database software for local/client storage in application software such as web browsers.

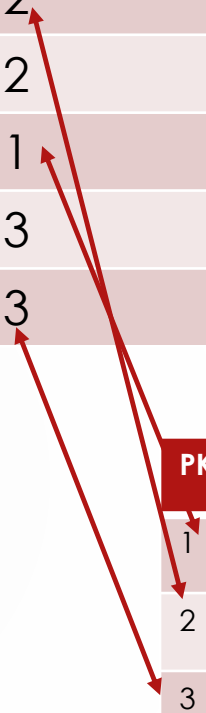
SQLite stores the entire database (definitions, tables, indices, and the data itself) as a single cross-platform file on a host machine. It implements this simple design by locking the entire database file during writing. SQLite read operations can be multitasked, though writes can only be performed sequentially.

D. Richard Hipp designed SQLite in the spring of 2000 while working for General Dynamics on contract with the United States Navy

Relational DB

- SQL Server, Oracle, MySQL, PostGres, MS Access

PK	LNAME	FNAME	JobCode	Hire Date
1	Smith	Jane	2	1/10/2010
2	Perez	Juan	2	1/14/2011
3	Kent	Clark	1	3/2/2005
4	Euler	Leonard	3	3/5/2009
5	Plank	Max	3	4/2/2012



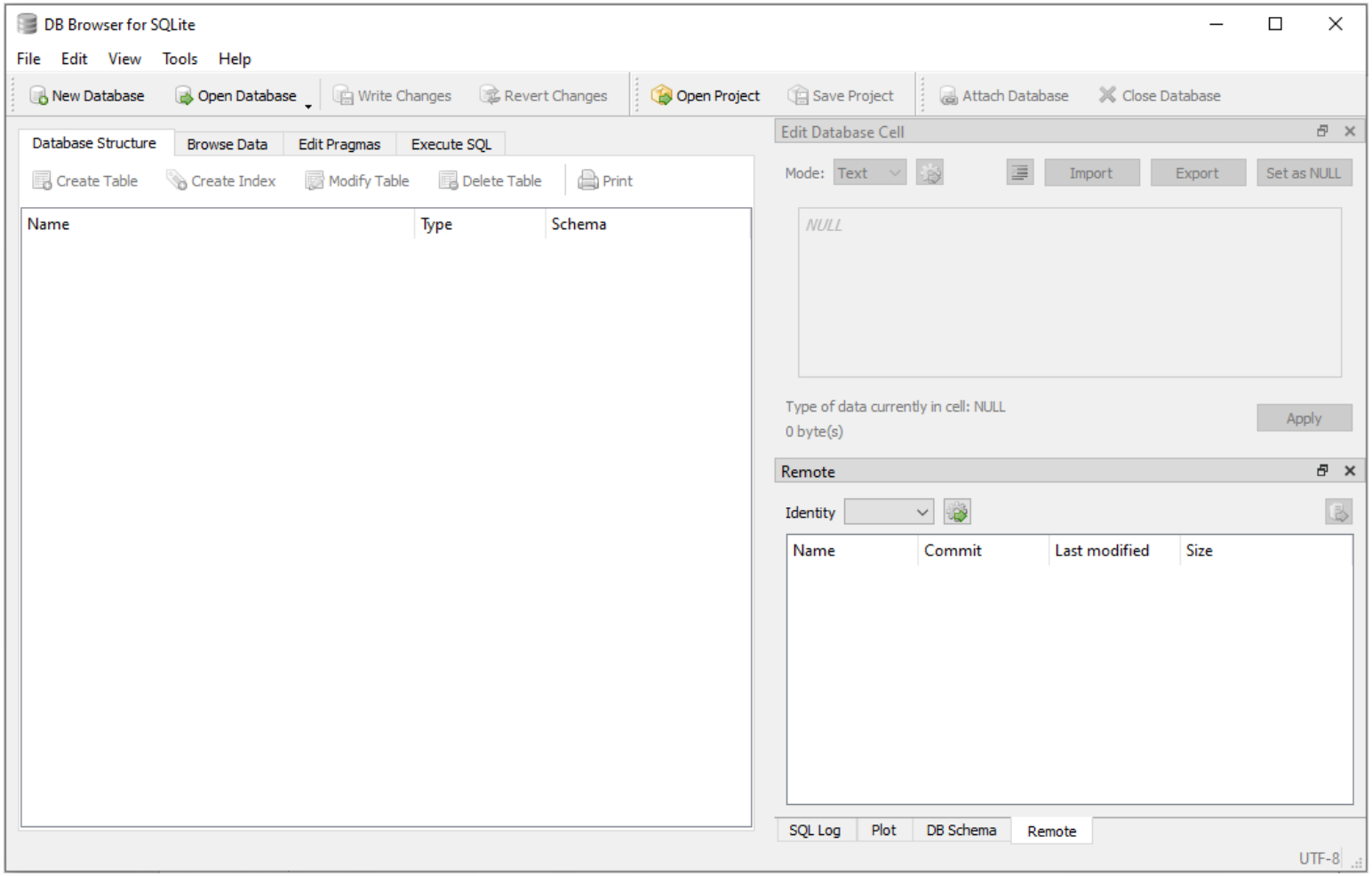
PK	Job Name	Min Edu.	Min Salary	Max Salary
1	Super hero	None	100,000	1,000,000
2	Programmer	BA/BS	70,000	95,000
3	Math / Scientist	Ph.D.	80,000	110,000
4	Manager	BA/BS	140,000	220,000

DBMS Should Provide:

- Transaction persistence
- Fault tolerance and recovery
- Sharing by multiple users
- Security controls

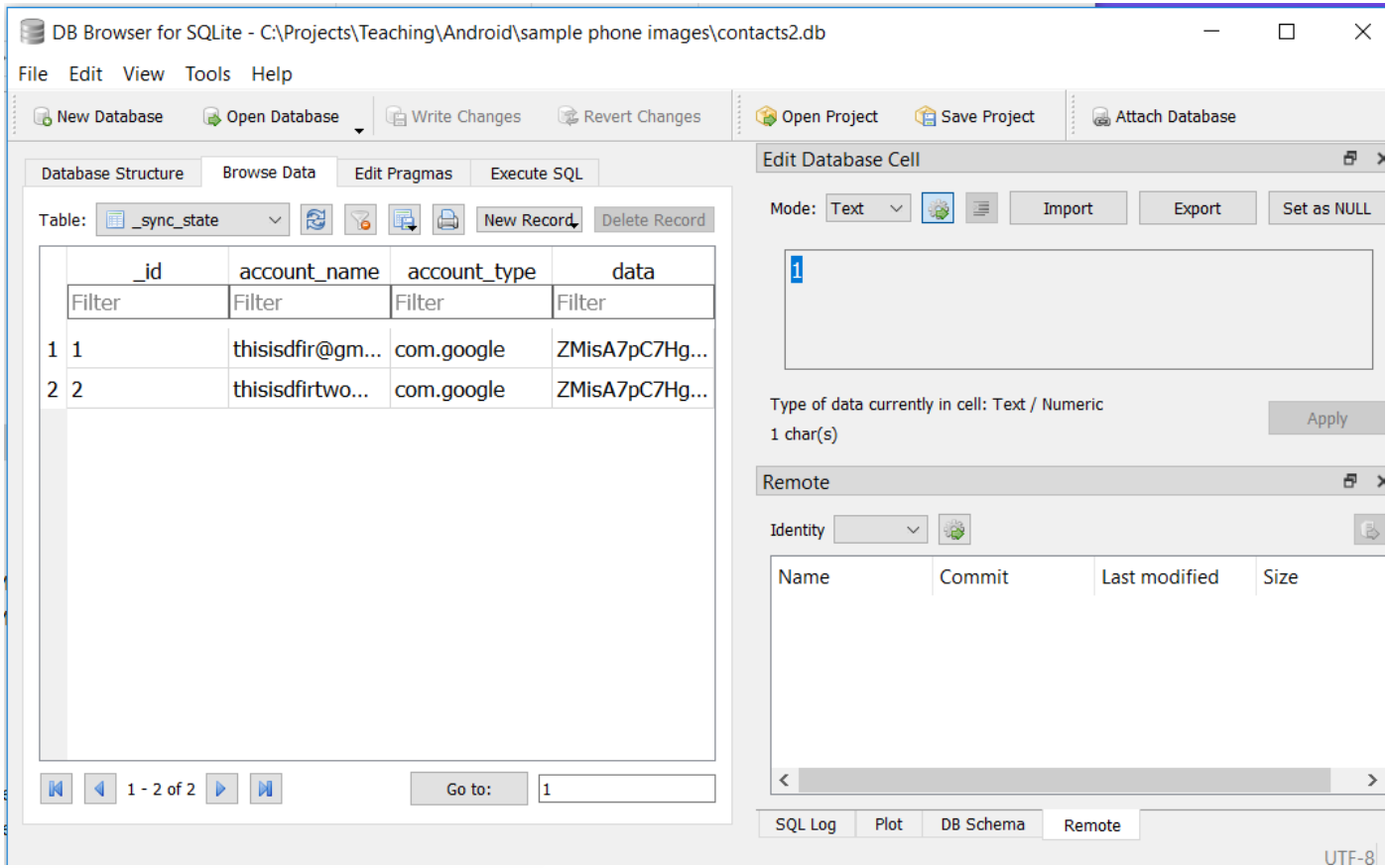
DB Browser

- https://sqlitebrowser.org/



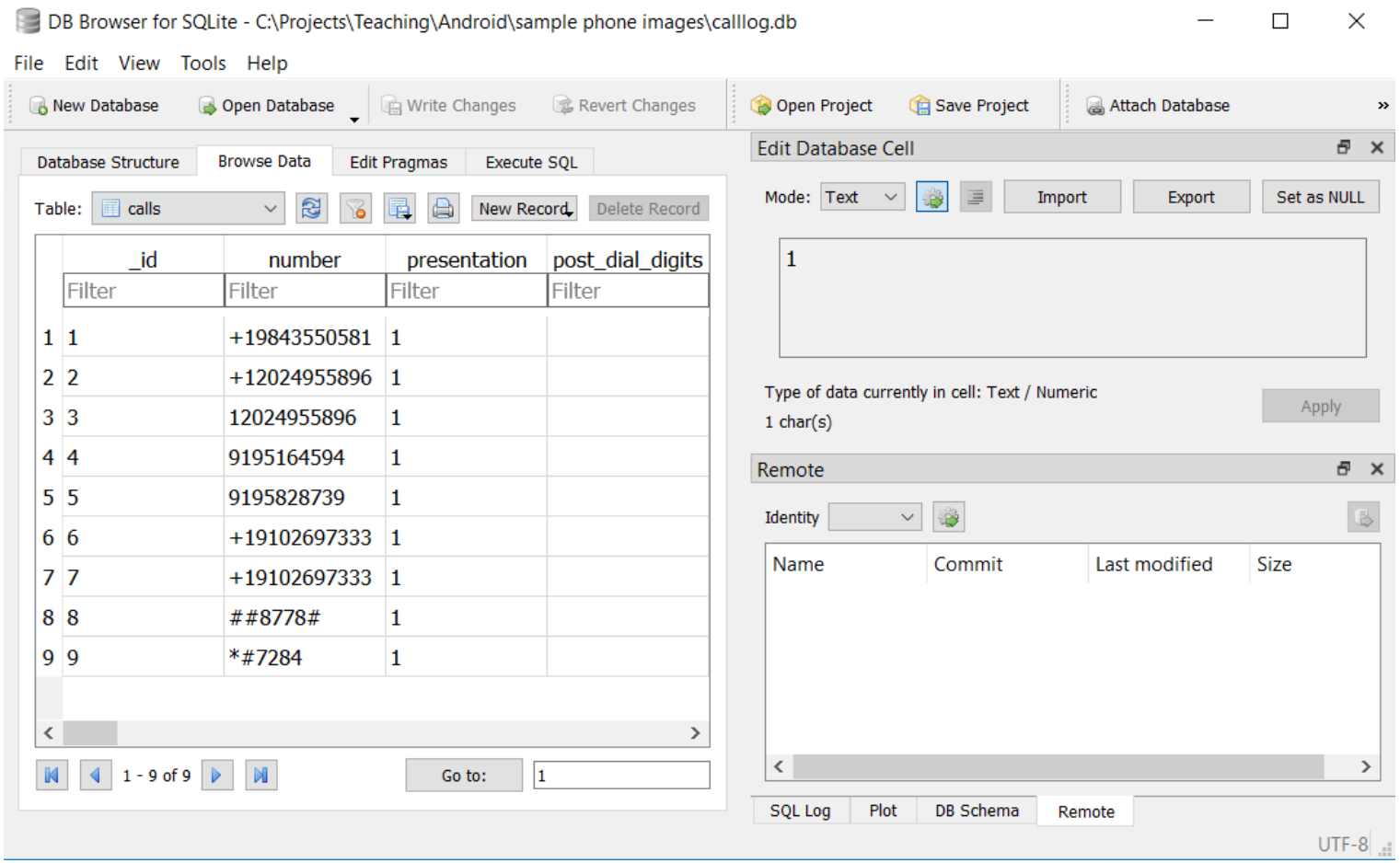
DB Browser

- Contacts2.db



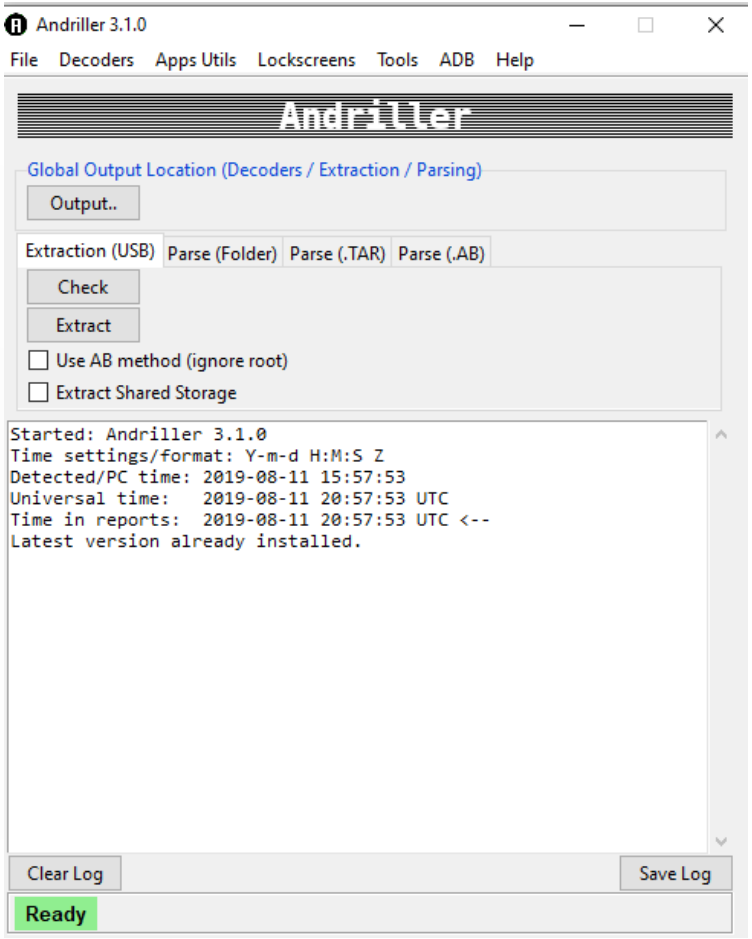
DB Browser

- callog.db



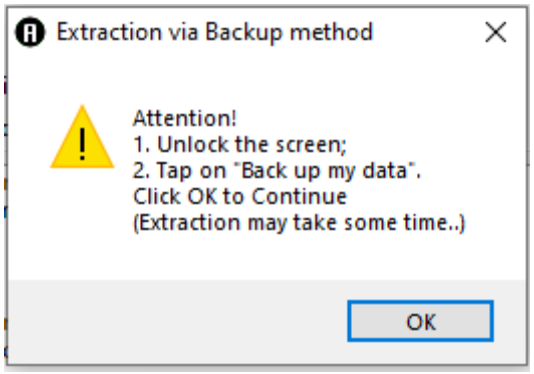
Andriller

- https://www.andriller.com/
- Free 30-day trial or 99 USD for 1-year license



Andriller

- Under settings you will find back up my data



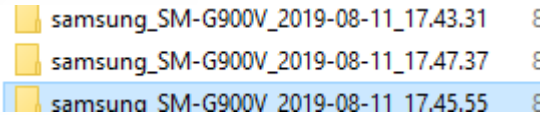
Andriller

This report was generated using Andriller # (This field is editable in Preferences)

[Andriller Report]

Type	Data
Serial	a5c44a58
Status	device
Permisson	shell
Ro.Product.Manufacturer	samsung
Ro.Product.Model	SM-G900V
Ro.Build.Version.Release	6.0.1
Ro.Build.Display.Id	MMB29M.G900VVRS2DQD1
Wifi Mac	60:f1:89:09:75:2b
Local_Time	2019-08-11 17:43:30 Central Daylight Time
Device_Time	2019-08-11 17:43:30 CDT

 # andriller.com # (This field is editable in Preferences)



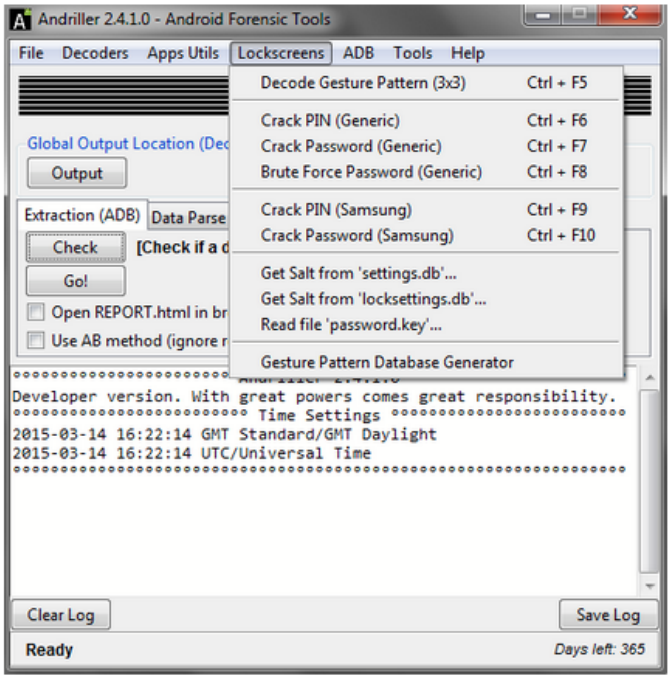
Andriller

Lockscreens Decoding

Andriller has the means of decoding pattern locks, and cracking PIN codes and Passwords.

Pattern, PIN and Password Cracking These features require a little more processing power, so are best to be performed locally on your own machine. The methods are explained below.

Get Salt from... Salt is an integer value, which is required for cracking the passwords. Salt can be positive as well as negative integers. The salt value can be obtained by parsing setting.db or locksettings.db files; when successfully fetched, the Salt value will be printed into the main terminal window.



Andriller

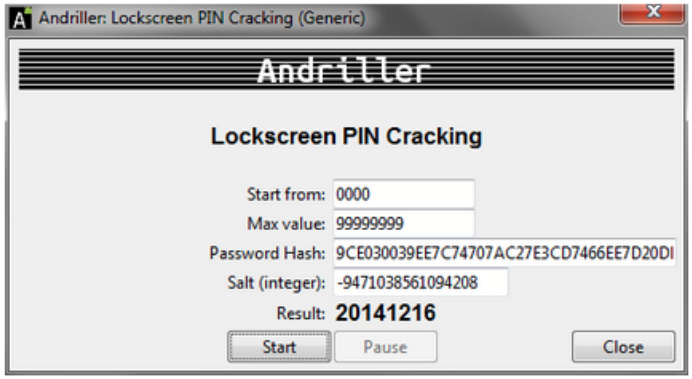
Lockscreen PIN code cracking

1. Select start and max value of the PIN code. By default, the max value is set to 9999, increase if required
2. Enter the value of password.key file
3. Enter the salt value as an integer
4. Press Start for cracking to begin

Once Start is clicked, a percentage progress will be displayed.

You can pause and resume cracking at any time. Last tried PIN will be shown just to let you know how far you've gone.

Also includes Samsung cracking, which uses different type of password hashing than other Android vendors.

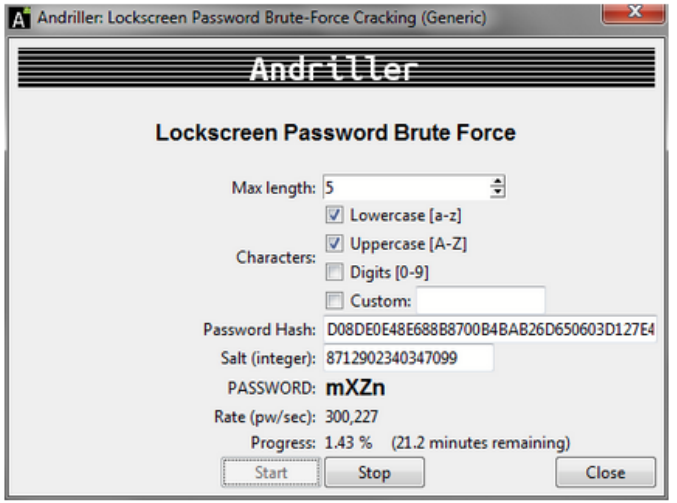


Andriller

Lockscreen Password brute force

1. Select the maximum length of a password
2. Select characters believed to have been used in the password. Select combinations of lower/upper case characters, digits, or custom characters
3. Enter the value of password.key file
4. Enter the salt value and an integer
5. Press Start for cracking to begin

This cracking method cannot be paused/resumed like with other methods.



Andriller

Decrypt Encrypted Databases

Andriller supports decryption of encrypted WhatsApp databases:

1. msgstore.db.crypt
2. msgstore.db.crypt5
3. msgstore.db.crypt7
4. msgstore.db.crypt8
5. msgstore.db.crypt9
6. msgstore.db.crypt10
7. msgstore.db.crypt12

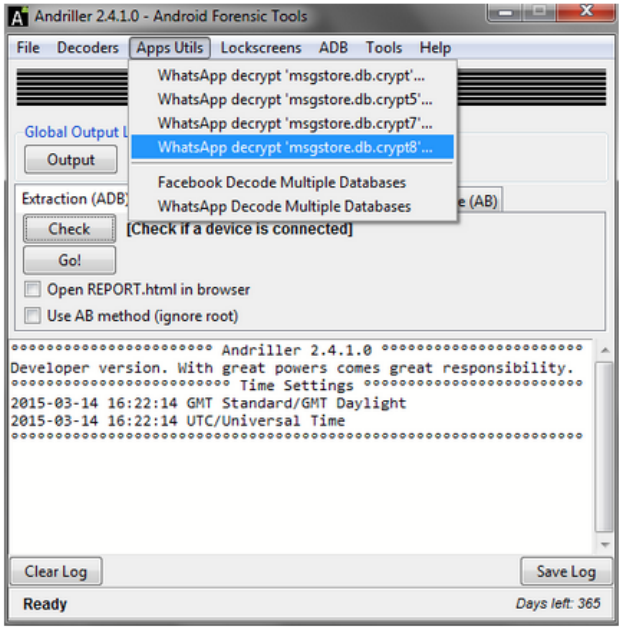
Plain Crypt (msgstore.db.crypt) The encrypted database is automatically decrypted into an SQLite3 database. Browse and select the encrypted file, Andriller will decode to a new file in the same directory.

msgstore.db.crypt ==> msgstore.db

Crypt5 (msgstore.db.crypt5) To successfully decrypt this type of database, an email address is required, which is synchronised with the Android device. Browse and select the encrypted file, you will be prompted to enter the email address. Once successful, it will decode to a new file in the same directory.

msgstore.db.crypt5 ==> msgstore.db

Crypt7-12 (msgstore.db.crypt7-12) To successfully decrypt this type of database, an encryption key file is required for the following location: '/data/data/com.whatsapp /files/key' <-- absolute path 'apps/com.whatsapp/f/key' <-- from Android backup This file should be automatically extracted during normal Andriller extraction (root and AB), and saved in the 'db' folder of the extraction



Create image

- Use open source tools to create an image.

Step 1 Mount

- From ADB Shell

```
shell@y25c:/dev $ mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,seclabel,nosuid,relatime,size=208520k,nr_inodes=52130,mode=755 0 0
devpts /dev/pts devpts rw,seclabel,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,seclabel,relatime 0 0
selinuxfs /sys/fs/selinux selinuxfs rw,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
none /sys/fs/cgroup tmpfs rw,seclabel,relatime,size=208520k,nr_inodes=52130,mode=750,gid=1000 0 0
tmpfs /mnt/asec tmpfs rw,seclabel,relatime,size=208520k,nr_inodes=52130,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,seclabel,relatime,size=208520k,nr_inodes=52130,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/platform/msm_sdcc.1/by-name/system /system ext4 ro,seclabel,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/userdata /data ext4 rw,seclabel,nosuid,nodev,noatime,discard,noauto_da_alloc,resu
id=1000,errors=continue,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/persist /persist ext4 rw,seclabel,nosuid,nodev,relatime,nodelalloc,data=ordered 0
 0
/dev/block/platform/msm_sdcc.1/by-name/cache /cache ext4 rw,seclabel,nosuid,nodev,noatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/drm /persist-lg ext4 rw,seclabel,nosuid,nodev,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/sns /sns ext4 rw,seclabel,nosuid,nodev,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/modem /firmware vfat ro,relatime,uid=1000,gid=1000,fmask=0337,dmask=0227,codepage
=cp437,iocharset=iso8859-1,shortname=lower,errors=remount-ro 0 0
/dev/fuse /mnt/shell/emulated fuse rw,nosuid,nodev,relatime,user_id=1023,group_id=1023,default_permissions,allow_other 0
 0
shell@y25c:/dev $ _
```

Step 2 df

- From ADB Shell

```
shell@y25c:/ $ df
Filesystem                Size      Used      Free    Blksize
/dev                    203.63M   132.00K   203.50M      4096
/sys/fs/cgroup          203.63M    12.00K   203.62M      4096
/mnt/asec               203.63M     0.00K   203.63M      4096
/mnt/obb                203.63M     0.00K   203.63M      4096
/system                   1.17G     1.14G    31.92M      4096
/data                     1.80G    58.45M     1.74G      4096
/persist                 31.46M     4.02M    27.43M      4096
/cache                  295.09M     4.75M   290.34M      4096
/persist-lg               7.83M     4.17M     3.66M      4096
/sns                      7.83M     4.03M     3.80M      4096
/firmware                63.95M    36.02M    27.94M     16384
/mnt/shell/emulated       1.80G    58.45M     1.74G      4096
shell@y25c:/ $
```

Step 3

- Use a different command window to setup port forwarding on some obscure port

```
C:\projects\teaching\Android\tools\platform-tools>adb forward tcp:7000 tcp:7000

C:\projects\teaching\Android\tools\platform-tools>
```

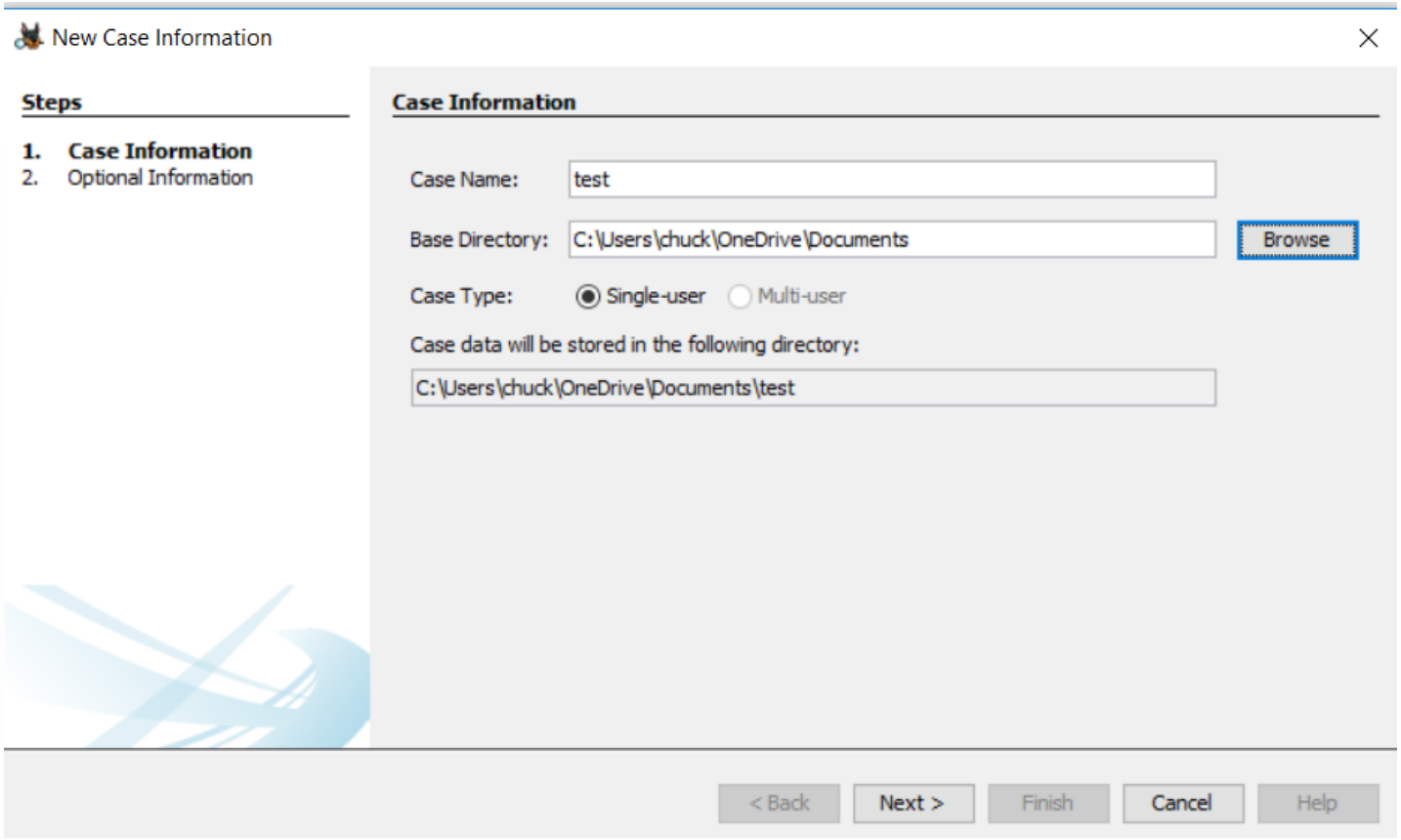
Step 5

- Send the command via busy box to the host
- Su
- dd if=/dev/block/sda1 | nc 192.168.1.1 -l -p 7000

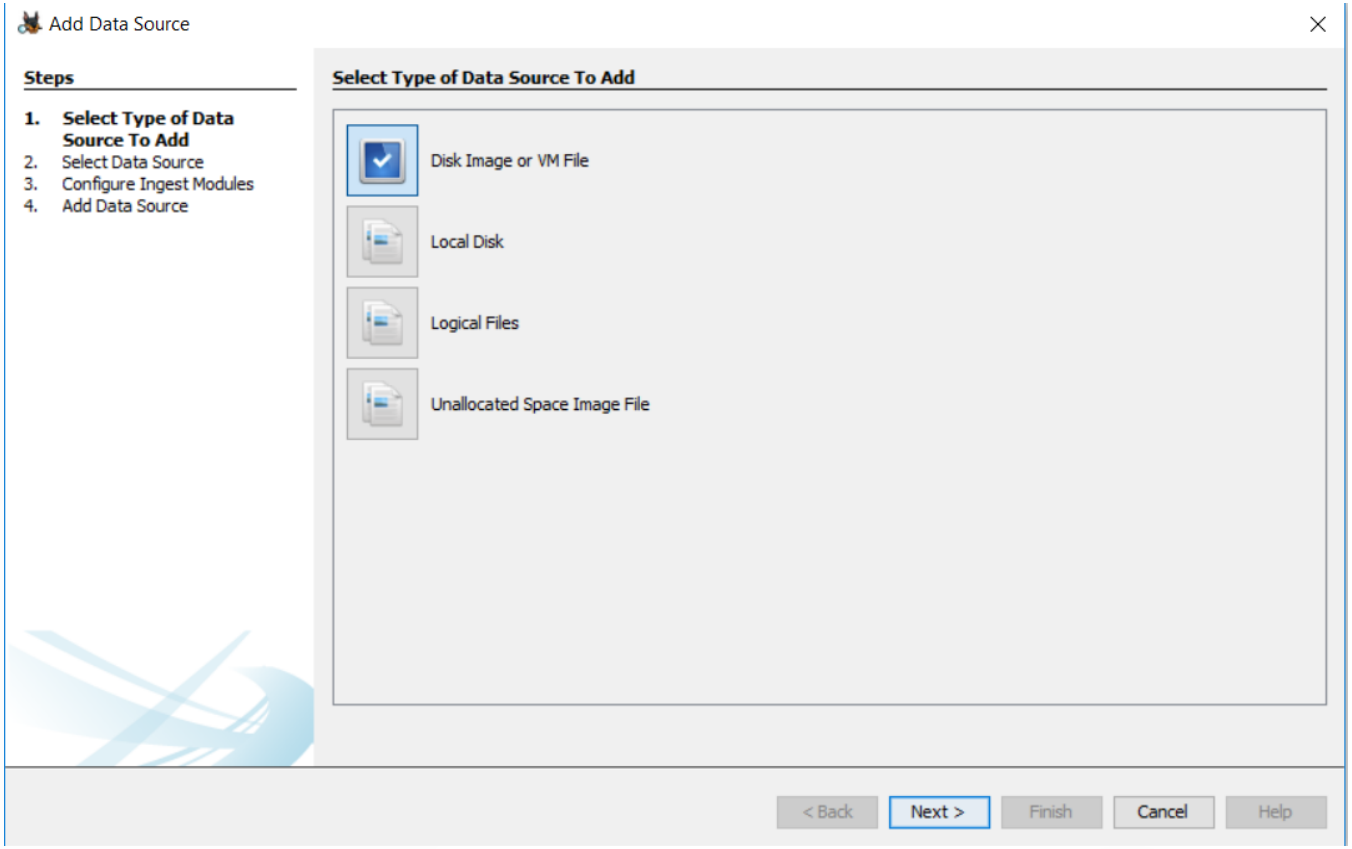
- Note replace /dev/block/sda1 with the appropriate block and replace the ip address with your host PC ip

- Common issue: permission denied. You can try rooting the phone first

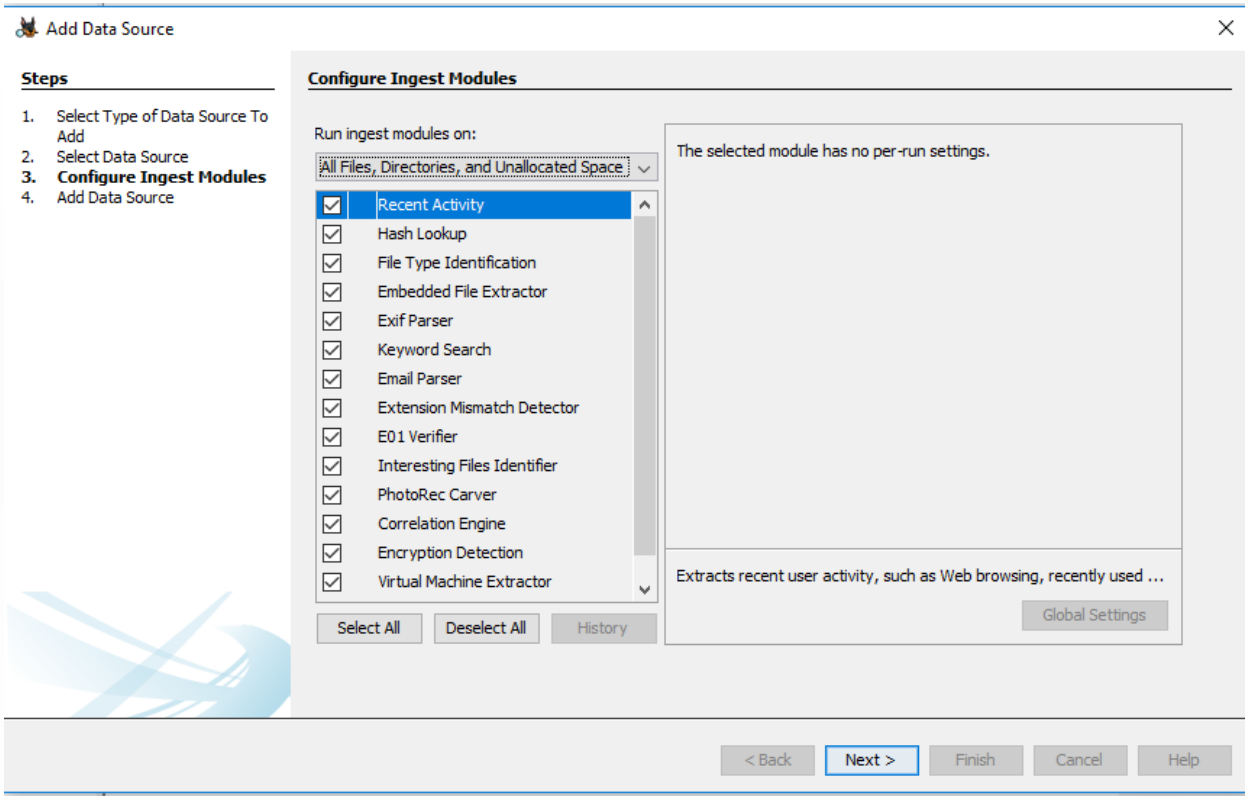
Using Open Source Autopsy



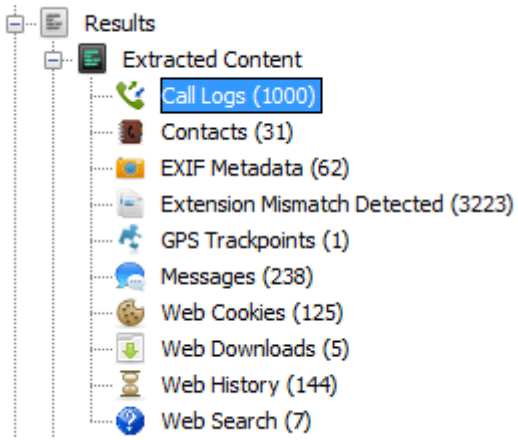
Using Open Source Autopsy



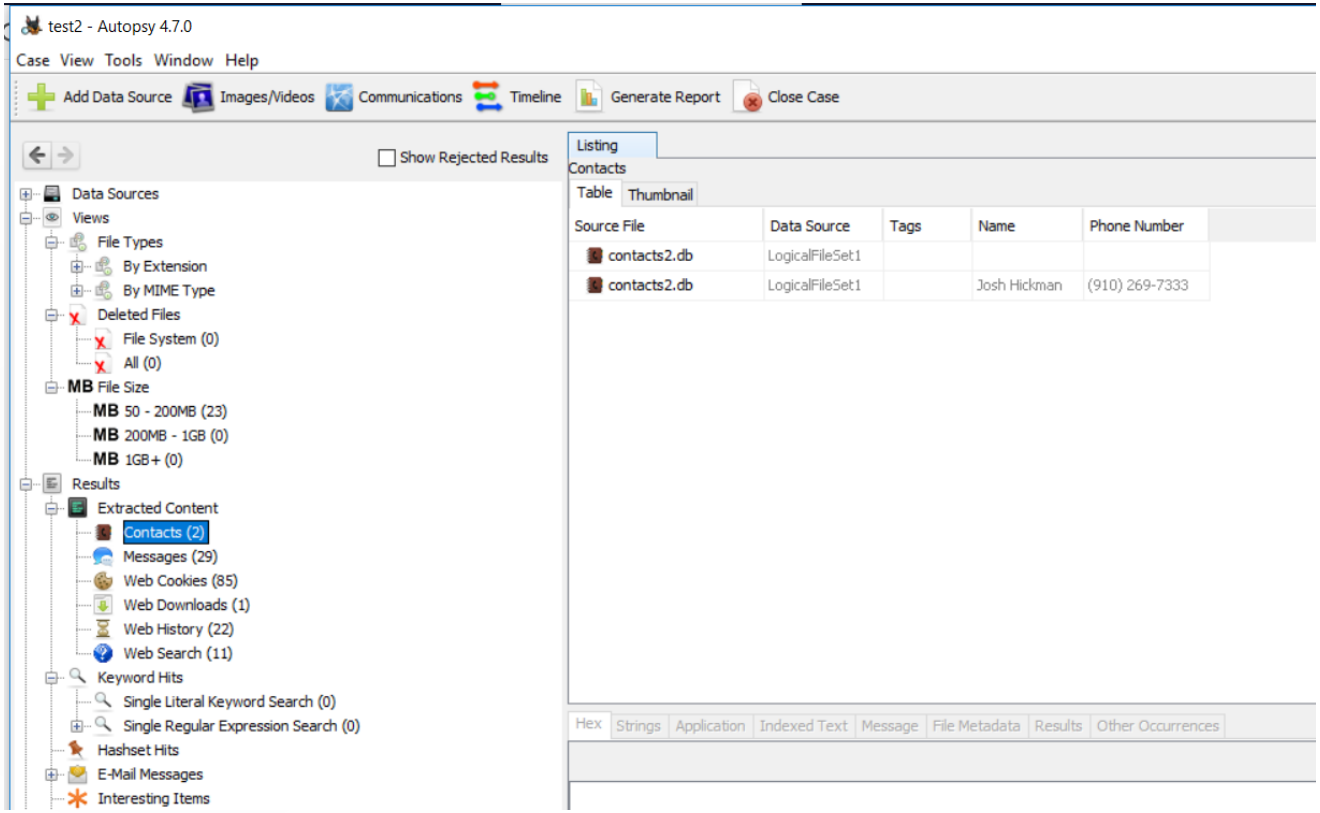
Using Open Source Autopsy



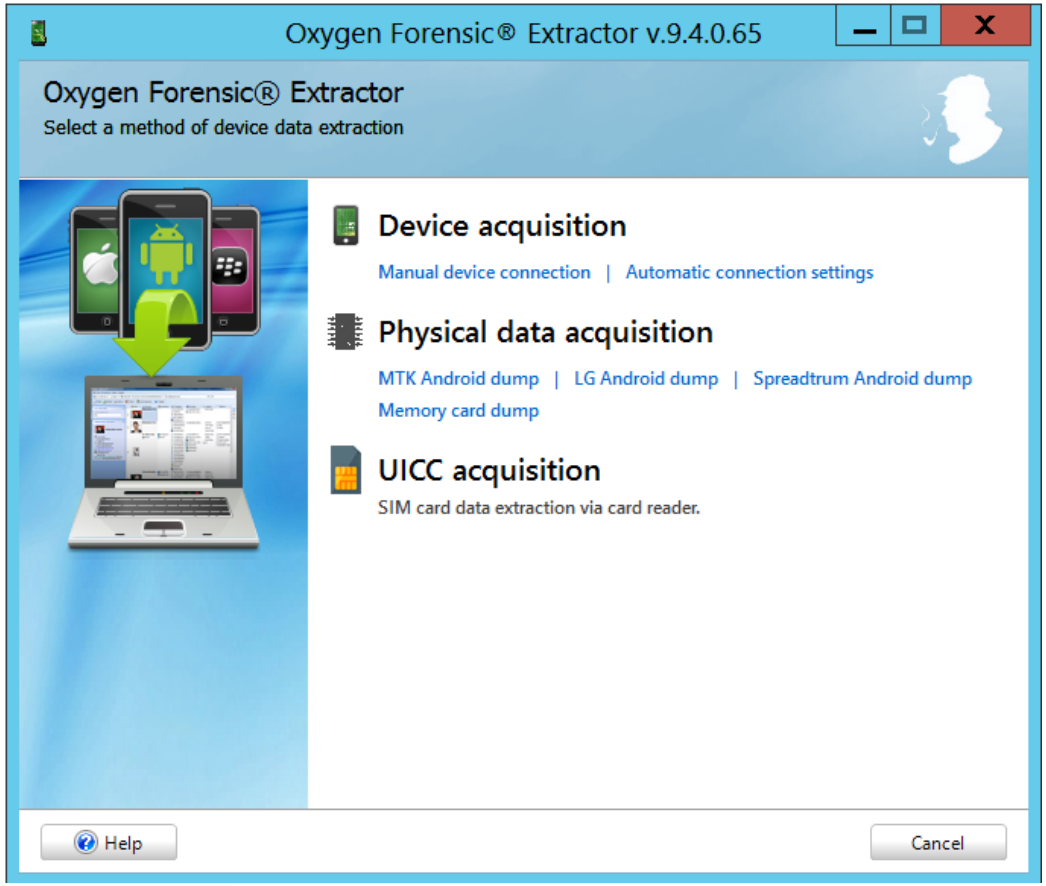
Using Open Source Autopsy



Using Open Source Autopsy

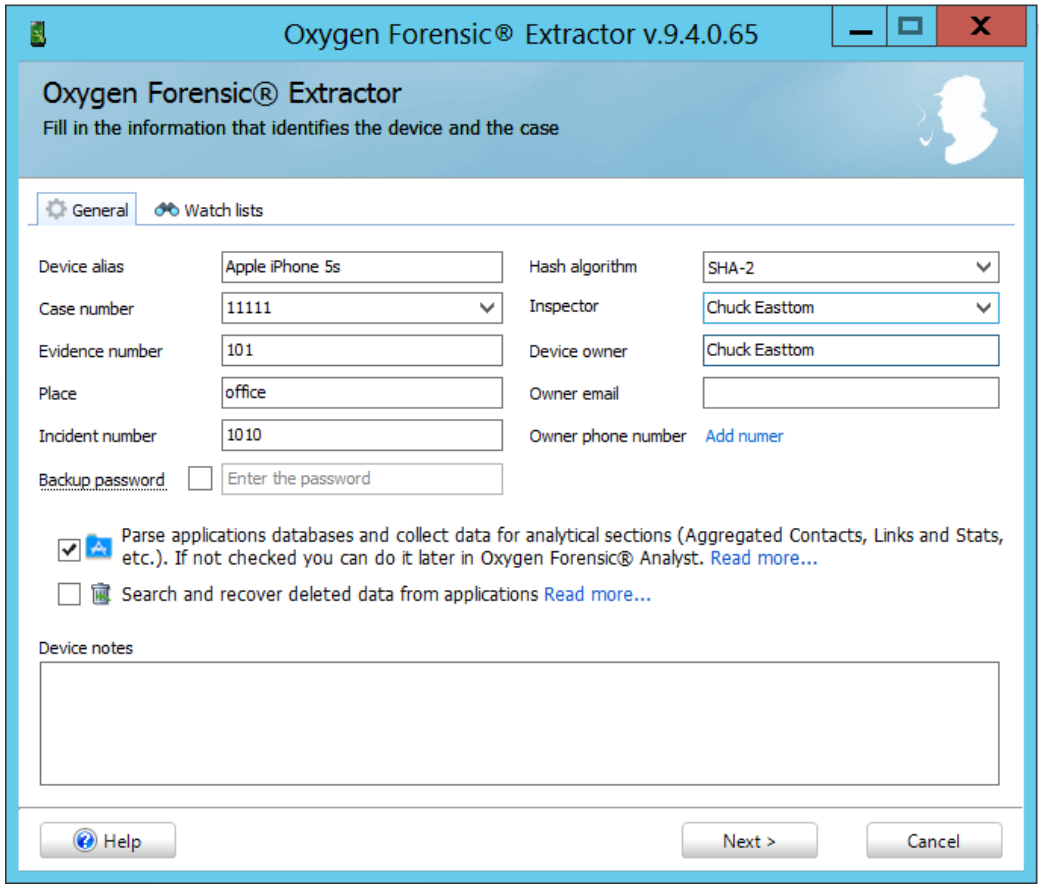


Oxygen Initial iPhone extraction - 1



Oxygen Initial iPhone extraction - 2

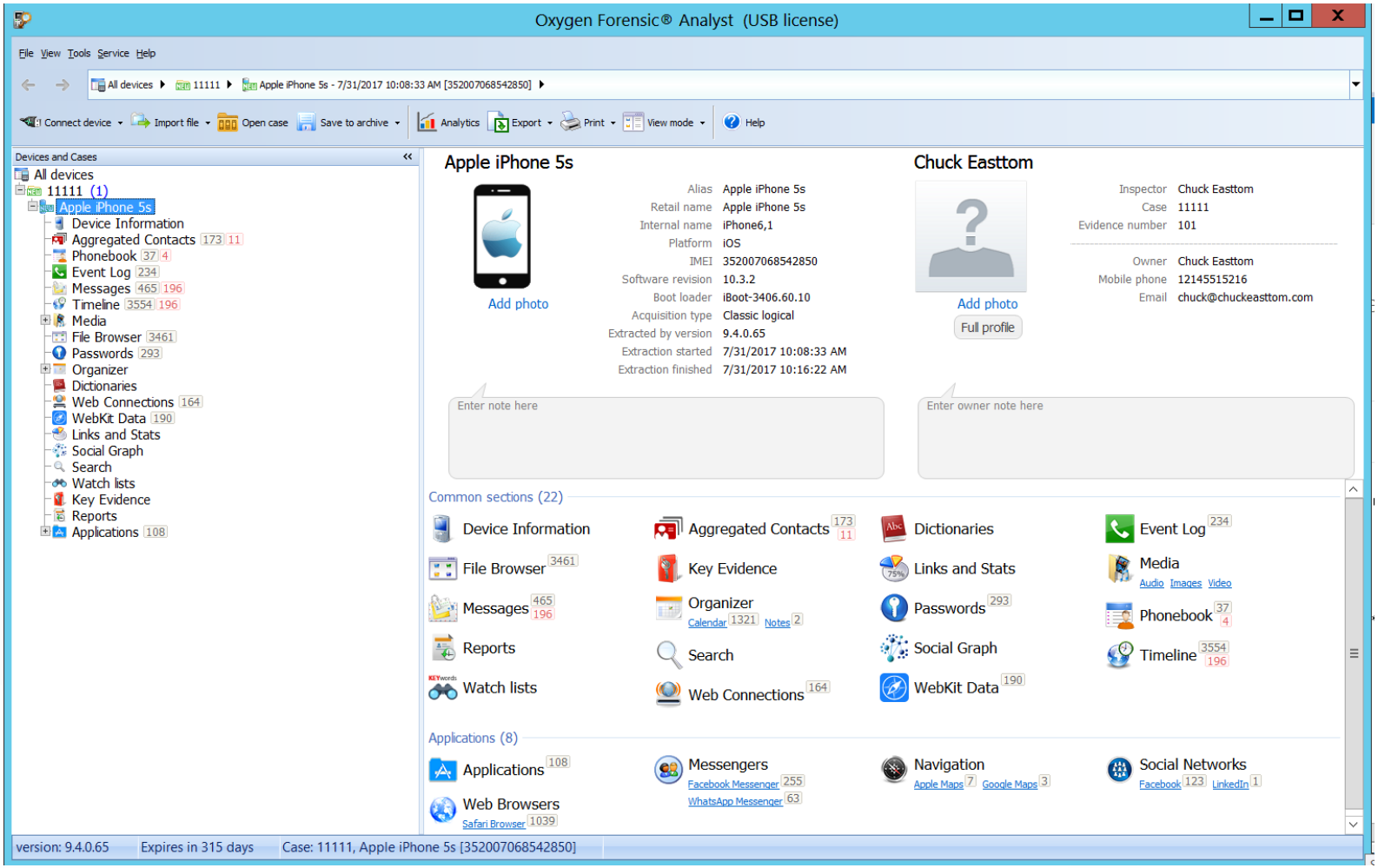
Oxygen Initial iPhone extraction - 3



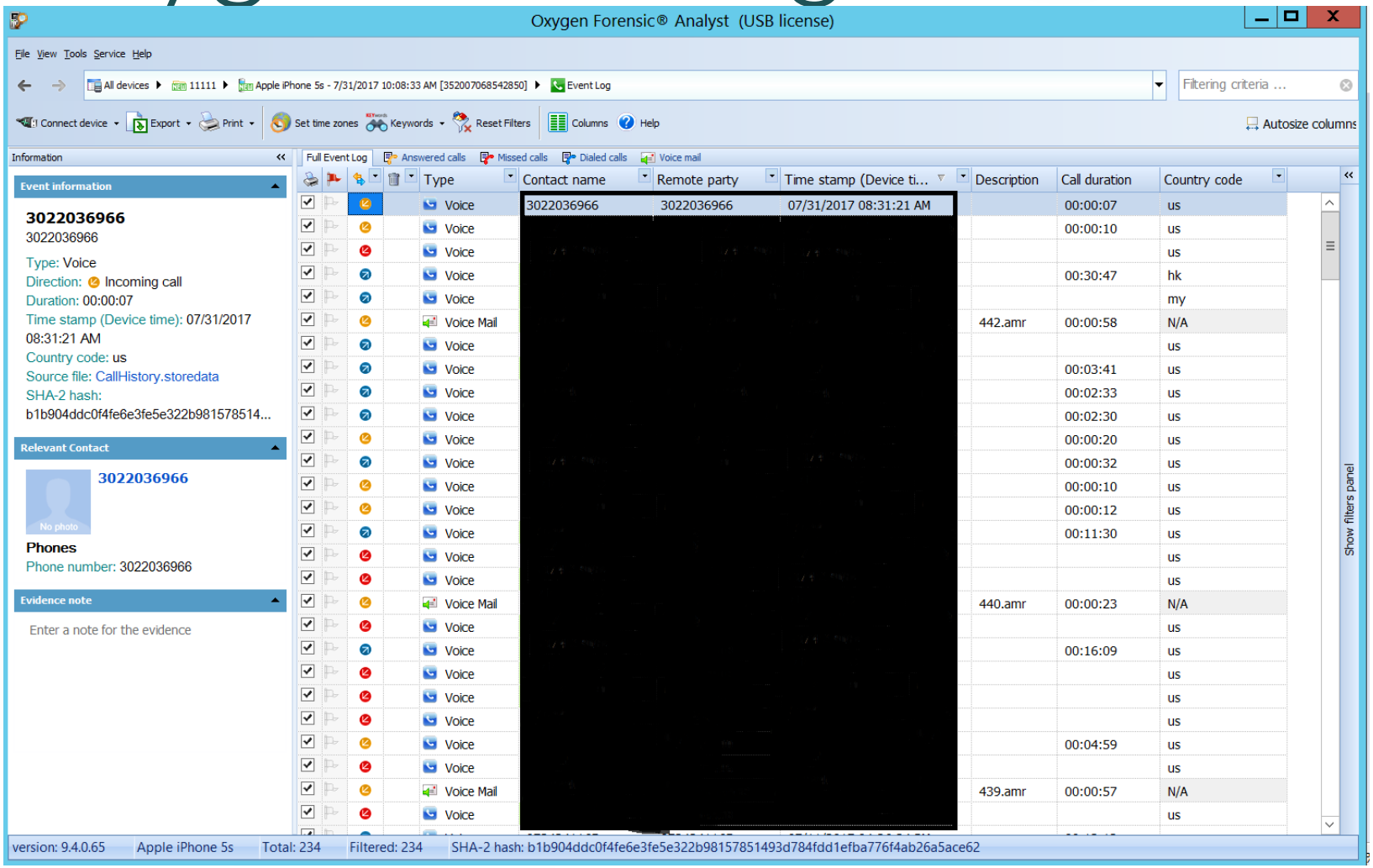
Oxygen Results

- In some cases Oxygen won't be able to get all the data, and will prompt you if you wish it to do an MTP extraction.

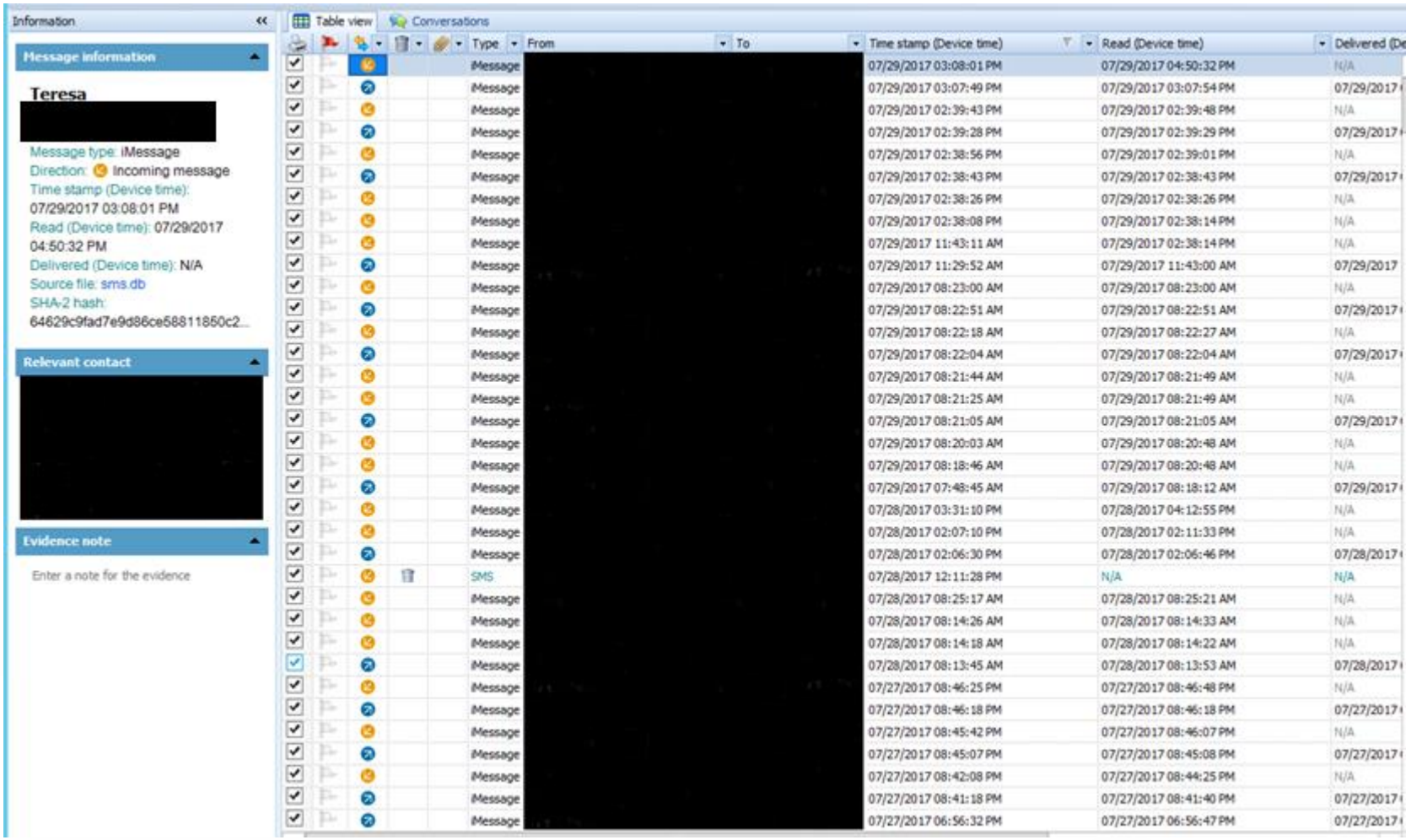
Oxygen Results



Oxygen Event log



Oxygen Messages



iPhone deleted messages

- Deleted messages are automatically recovered in Messages section, highlighted with blue color and marked by recycle bin icon
- Deleted calls are automatically recovered in Event Log section, highlighted with blue color and marked by recycle bin icon.
- Deleted email messages can be viewed in Envelope Index file (the file has no extension). Envelope Index file is only accessible on jailbroken devices.
- Deleted contacts are automatically recovered in Phonebook section and marked by recycle bin icon.
- Deleted calendar events are stored in Calendar.sqlite file that can be

Android deleted messages

- Deleted messages are automatically recovered in Messages section, highlighted with blue color and marked by recycle bin icon.
- Deleted calls are automatically recovered in Event Log section, highlighted with blue color and marked by recycle bin icon.
- Deleted contacts are automatically recovered in Phonebook section and marked by recycle bin icon.
- Deleted calendar events are stored in Calendar.db file that can be viewed on Database files tab in File Browser section.

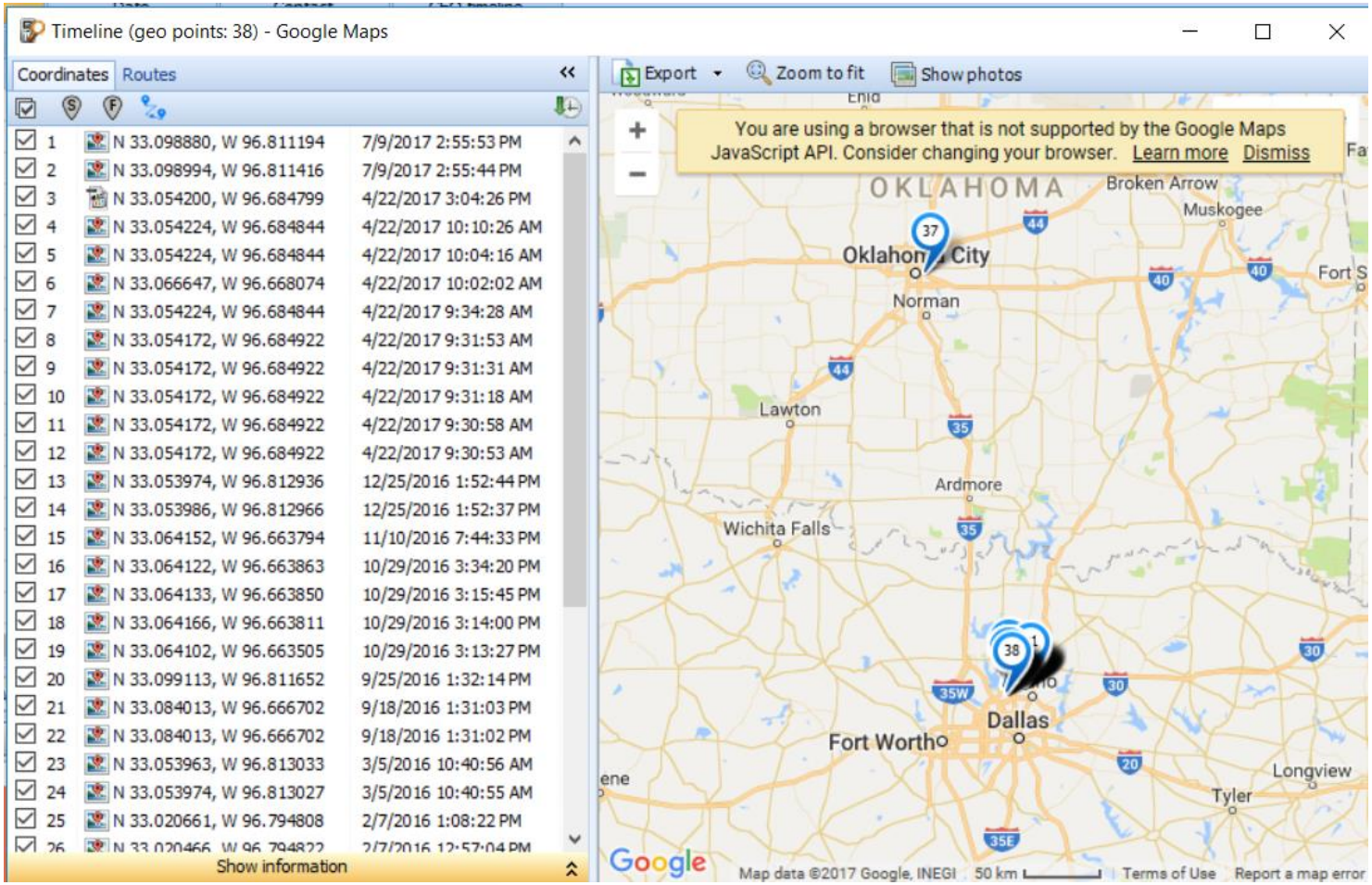
Blackberry deleted messages

- Deleted messages are automatically recovered in Messages section, highlighted with blue color and marked by recycle bin icon.
- Deleted calls are automatically recovered in Event Log section, highlighted with blue color and marked by recycle bin icon.
- Deleted contacts are automatically recovered in Phonebook section and marked by recycle bin icon.
- Deleted calendar events are stored in Calendar.db file that can be viewed on Database files tab in File Browser section.

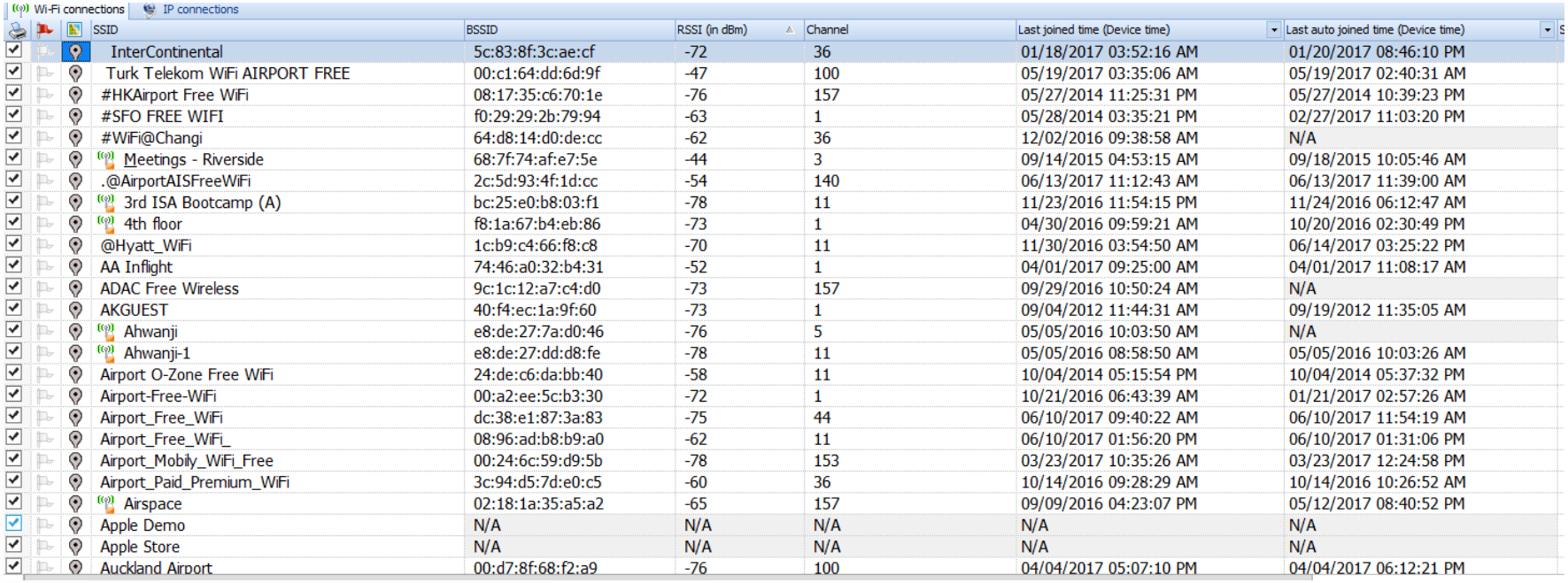
Windows deleted messages

- Only recoverable via JTAG

Oxygen Map data for Images

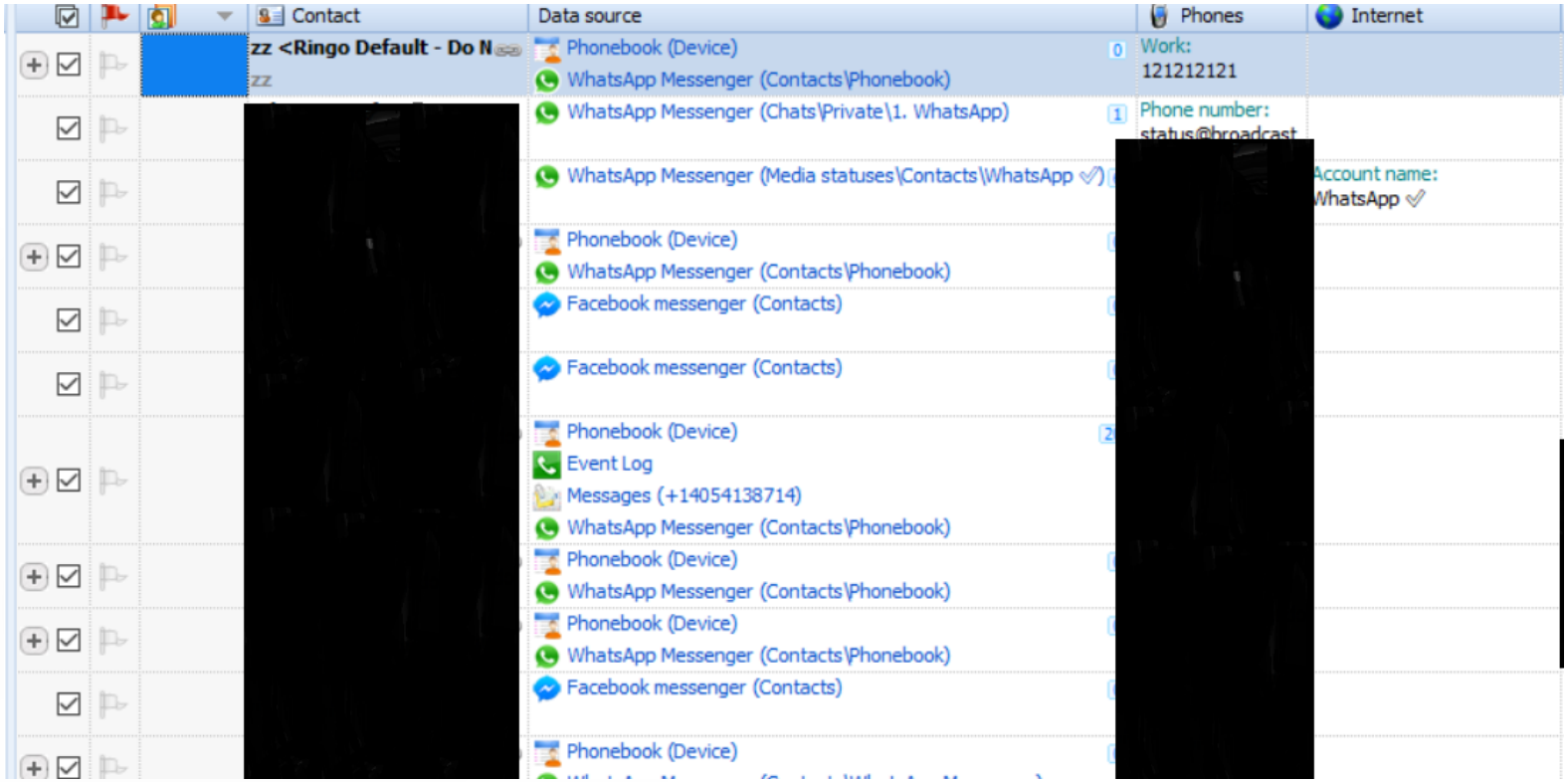


Oxygen Web connections

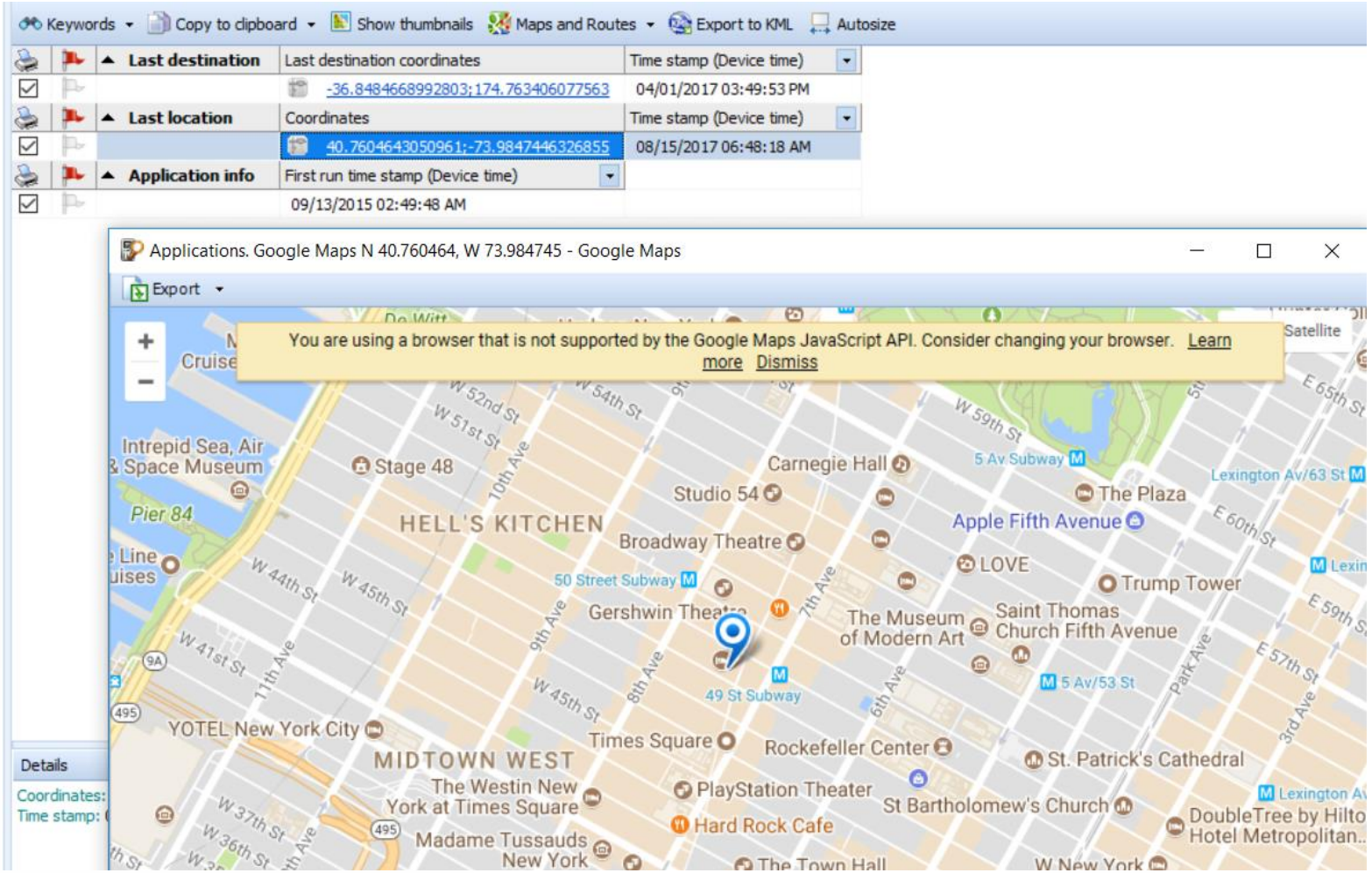

Wi-Fi connections | IP connections

SSID	BSSID	RSSI (in dBm)	Channel	Last joined time (Device time)	Last auto joined time (Device time)
InterContinental	5c:83:8f:3c:ae:cf	-72	36	01/18/2017 03:52:16 AM	01/20/2017 08:46:10 PM
Turk Telekom WiFi AIRPORT FREE	00:c1:64:dd:6d:9f	-47	100	05/19/2017 03:35:06 AM	05/19/2017 02:40:31 AM
#HKAirport Free WiFi	08:17:35:c6:70:1e	-76	157	05/27/2014 11:25:31 PM	05/27/2014 10:39:23 PM
#SFO FREE WIFI	f0:29:29:2b:79:94	-63	1	05/28/2014 03:35:21 PM	02/27/2017 11:03:20 PM
#WiFi@Changi	64:d8:14:d0:de:cc	-62	36	12/02/2016 09:38:58 AM	N/A
Meetings - Riverside	68:7f:74:af:e7:5e	-44	3	09/14/2015 04:53:15 AM	09/18/2015 10:05:46 AM
.@AirportAISFreeWiFi	2c:5d:93:4f:1d:cc	-54	140	06/13/2017 11:12:43 AM	06/13/2017 11:39:00 AM
3rd ISA Bootcamp (A)	bc:25:e0:b8:03:f1	-78	11	11/23/2016 11:54:15 PM	11/24/2016 06:12:47 AM
4th floor	f8:1a:67:b4:eb:86	-73	1	04/30/2016 09:59:21 AM	10/20/2016 02:30:49 PM
@Hyatt_WiFi	1c:b9:c4:66:f8:c8	-70	11	11/30/2016 03:54:50 AM	06/14/2017 03:25:22 PM
AA Inflight	74:46:a0:32:b4:31	-52	1	04/01/2017 09:25:00 AM	04/01/2017 11:08:17 AM
ADAC Free Wireless	9c:1c:12:a7:c4:d0	-73	157	09/29/2016 10:50:24 AM	N/A
AKGUEST	40:f4:ec:1a:9f:60	-73	1	09/04/2012 11:44:31 AM	09/19/2012 11:35:05 AM
Ahwanji	e8:de:27:7a:d0:46	-76	5	05/05/2016 10:03:50 AM	N/A
Ahwanji-1	e8:de:27:dd:d8:fe	-78	11	05/05/2016 08:58:50 AM	05/05/2016 10:03:26 AM
Airport O-Zone Free WiFi	24:de:c6:da:bb:40	-58	11	10/04/2014 05:15:54 PM	10/04/2014 05:37:32 PM
Airport-Free-WiFi	00:a2:ee:5c:b3:30	-72	1	10/21/2016 06:43:39 AM	01/21/2017 02:57:26 AM
Airport_Free_WiFi	dc:38:e1:87:3a:83	-75	44	06/10/2017 09:40:22 AM	06/10/2017 11:54:19 AM
Airport_Free_WiFi_	08:96:ad:b8:b9:a0	-62	11	06/10/2017 01:56:20 PM	06/10/2017 01:31:06 PM
Airport_Mobily_WiFi_Free	00:24:6c:59:d9:5b	-78	153	03/23/2017 10:35:26 AM	03/23/2017 12:24:58 PM
Airport_Paid_Premium_WiFi	3c:94:d5:7d:e0:c5	-60	36	10/14/2016 09:28:29 AM	10/14/2016 10:26:52 AM
Airspace	02:18:1a:35:a5:a2	-65	157	09/09/2016 04:23:07 PM	05/12/2017 08:40:52 PM
Apple Demo	N/A	N/A	N/A	N/A	N/A
Apple Store	N/A	N/A	N/A	N/A	N/A
Auckland Airport	00:d7:8f:68:f2:a9	-76	100	04/04/2017 05:07:10 PM	04/04/2017 06:12:21 PM

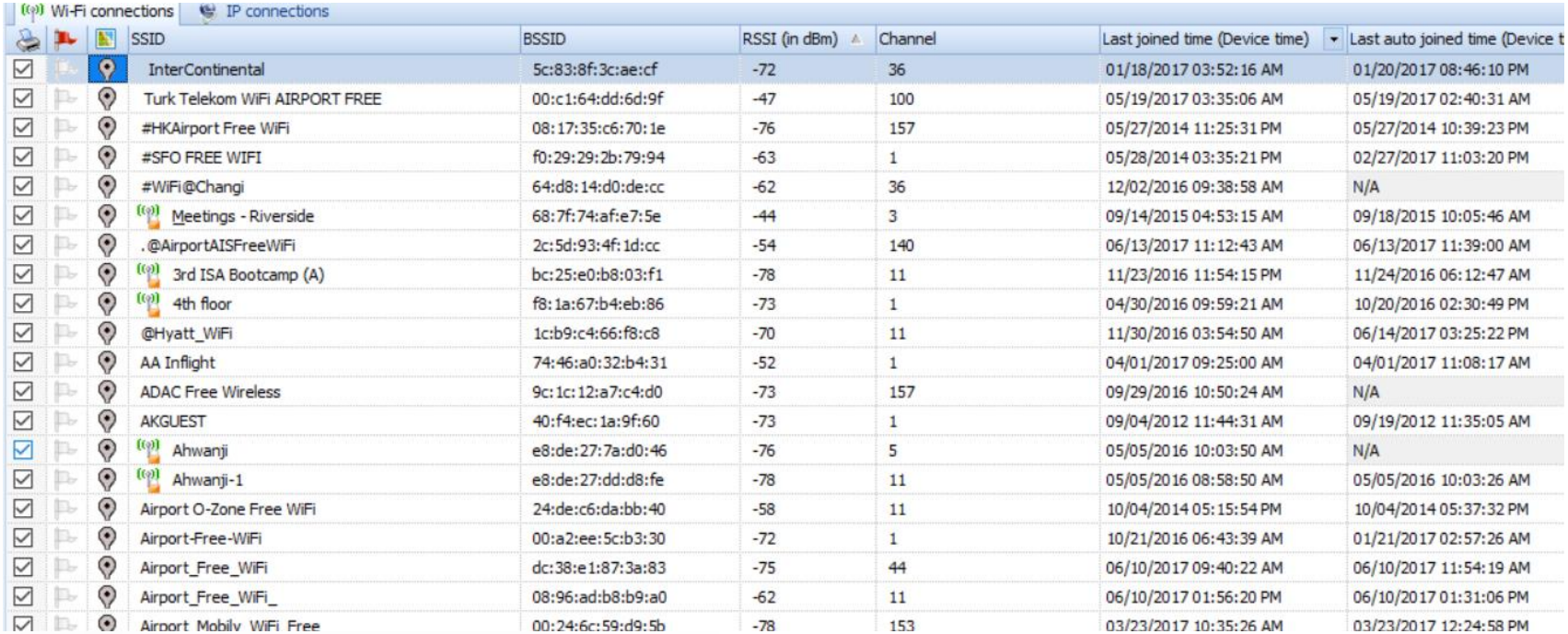
Oxygen Aggregated Contacts



Oxygen Navigation



Oxygen Web Connections



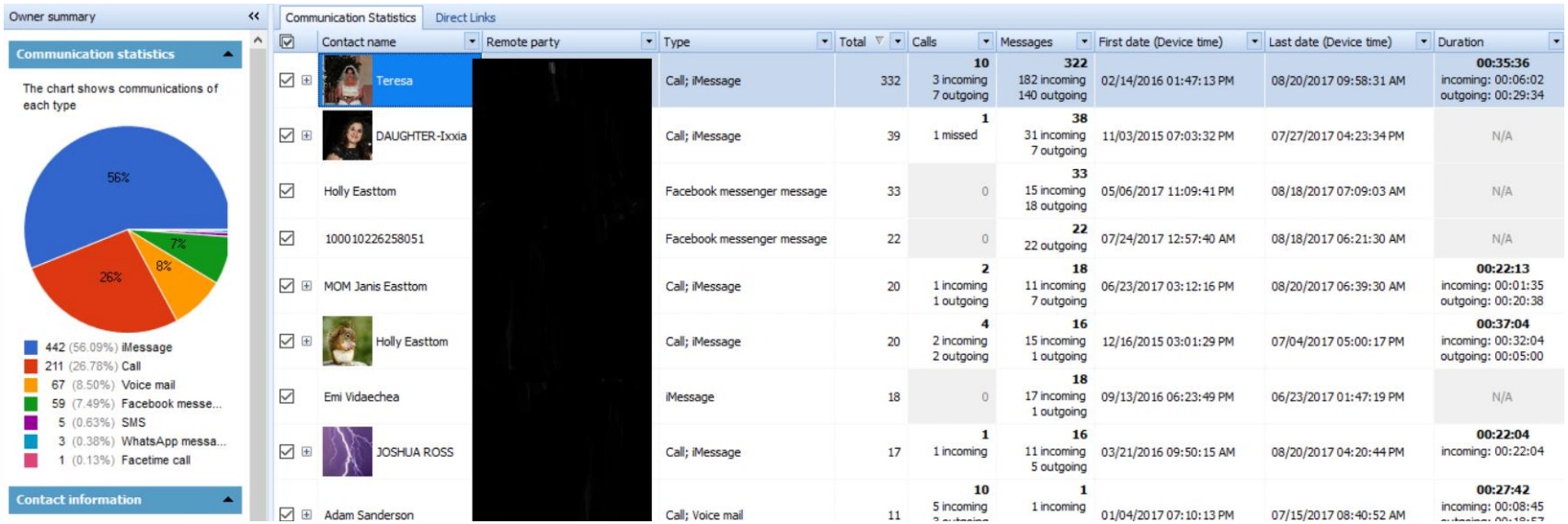
Wi-Fi connections | IP connections

SSID	BSSID	RSSI (in dBm)	Channel	Last joined time (Device time)	Last auto joined time (Device t
InterContinental	5c:83:8f:3c:ae:cf	-72	36	01/18/2017 03:52:16 AM	01/20/2017 08:46:10 PM
Turk Telekom WiFi AIRPORT FREE	00:c1:64:dd:6d:9f	-47	100	05/19/2017 03:35:06 AM	05/19/2017 02:40:31 AM
#HKAirport Free WiFi	08:17:35:c6:70:1e	-76	157	05/27/2014 11:25:31 PM	05/27/2014 10:39:23 PM
#SFO FREE WIFI	f0:29:29:2b:79:94	-63	1	05/28/2014 03:35:21 PM	02/27/2017 11:03:20 PM
#WiFi@Changi	64:d8:14:d0:de:cc	-62	36	12/02/2016 09:38:58 AM	N/A
Meetings - Riverside	68:7f:74:af:e7:5e	-44	3	09/14/2015 04:53:15 AM	09/18/2015 10:05:46 AM
.@AirportAISFreeWiFi	2c:5d:93:4f:1d:cc	-54	140	06/13/2017 11:12:43 AM	06/13/2017 11:39:00 AM
3rd ISA Bootcamp (A)	bc:25:e0:b8:03:f1	-78	11	11/23/2016 11:54:15 PM	11/24/2016 06:12:47 AM
4th floor	f8:1a:67:b4:eb:86	-73	1	04/30/2016 09:59:21 AM	10/20/2016 02:30:49 PM
@Hyatt_WiFi	1c:b9:c4:66:f8:c8	-70	11	11/30/2016 03:54:50 AM	06/14/2017 03:25:22 PM
AA Inflight	74:46:a0:32:b4:31	-52	1	04/01/2017 09:25:00 AM	04/01/2017 11:08:17 AM
ADAC Free Wireless	9c:1c:12:a7:c4:d0	-73	157	09/29/2016 10:50:24 AM	N/A
AKGUEST	40:f4:ec:1a:9f:60	-73	1	09/04/2012 11:44:31 AM	09/19/2012 11:35:05 AM
Ahwanji	e8:de:27:7a:d0:46	-76	5	05/05/2016 10:03:50 AM	N/A
Ahwanji-1	e8:de:27:dd:d8:fe	-78	11	05/05/2016 08:58:50 AM	05/05/2016 10:03:26 AM
Airport O-Zone Free WiFi	24:de:c6:da:bb:40	-58	11	10/04/2014 05:15:54 PM	10/04/2014 05:37:32 PM
Airport-Free-WiFi	00:a2:ee:5c:b3:30	-72	1	10/21/2016 06:43:39 AM	01/21/2017 02:57:26 AM
Airport_Free_WiFi	dc:38:e1:87:3a:83	-75	44	06/10/2017 09:40:22 AM	06/10/2017 11:54:19 AM
Airport_Free_WiFi_	08:96:ad:b8:b9:a0	-62	11	06/10/2017 01:56:20 PM	06/10/2017 01:31:06 PM
Airport_Mobily_WiFi_Free	00:24:6c:59:d9:5b	-78	153	03/23/2017 10:35:26 AM	03/23/2017 12:24:58 PM

Oxygen Web Browser

Title	URL
N/A	http://172.19.128.1/
Avoid Joe Mccray/Strategic Security | Forgotten ...	http://blog.forgottensec.com/2015/03/21-avoid-joe/
Free PDF BookIntroduction to Tactical Hacking A ...	http://bookpdfo0tradams.blogspot.com/2017/03/free-pdf-bookintroduction-to-tactical.html?m=1
Redirect	http://capture.onboard.onair.aero/redir2?requestedHost=172.19.128.1%2F
Department of Chemistry | M. A. Program (1 year)	http://chem.virginia.edu/graduate-studies/the-m-a-program/
Biomedical Neuroscience - Distance Learning - Uni...	http://distance.ufl.edu/biomedical-neuroscience/
Biomedical Neuroscience - Distance Learning - Uni...	http://distance.ufl.edu/biomedical-neuroscience/
Biomedical Neuroscience - Distance Learning - Uni...	http://distance.ufl.edu/biomedical-neuroscience/#prereq
N/A	http://edx.org/
Job Title "Engineer" without PE? - General Engine...	http://engineerboards.com/index.php?/topic/4328-job-title-engineer-without-pe/
Build Your Professional Value | UMUC	http://learn-more.umuc.edu/search/degree-programs/?marketcode=WB200482&gclid=EAIaIQobCh
Become a Software Developer! - Edge Tech Acad...	http://learn.edgetechacademy.com/?utm_source=google&utm_term=schools%20for%20computer
N/A	http://portal.inflight.onair.aero/ac/UAE/capture/QTYtRUVW/MTcyLjE5LjEzMi4xOTg=
Emirates Internet ONAIR	http://portal.inflight.onair.aero/ac/UAE/en/browse
Emirates Internet ONAIR	http://portal.inflight.onair.aero/ac/UAE/en/connect
MS in Artificial Intelligence | Institute for Artificial ...	http://www.ai.uga.edu/content/ms-artificial-intelligence
N/A	http://www.airportterminalmaps.com/Dallas-Fort-Worth-DFW-airport-terminal-map
N/A	http://www.airportterminalmaps.com/Dallas-Fort-Worth-DFW-airport-terminal-map#TERMD
N/A	http://www.airportterminalmaps.com/Dallas-Fort-Worth-DFW-airport-terminal-map/#TERMD
Online Doctorate Degree in Computer Science | A...	http://www.aspen.edu/degrees/doctoral-degree/doctorate-of-science-in-computer-science
Online Doctorate Degree in Computer Science | A...	http://www.aspen.edu/degrees/doctoral-degree/doctorate-of-science-in-computer-science
Welcome | Capitol Technology University	http://www.capitol-college.edu/

Oxygen Link Stats



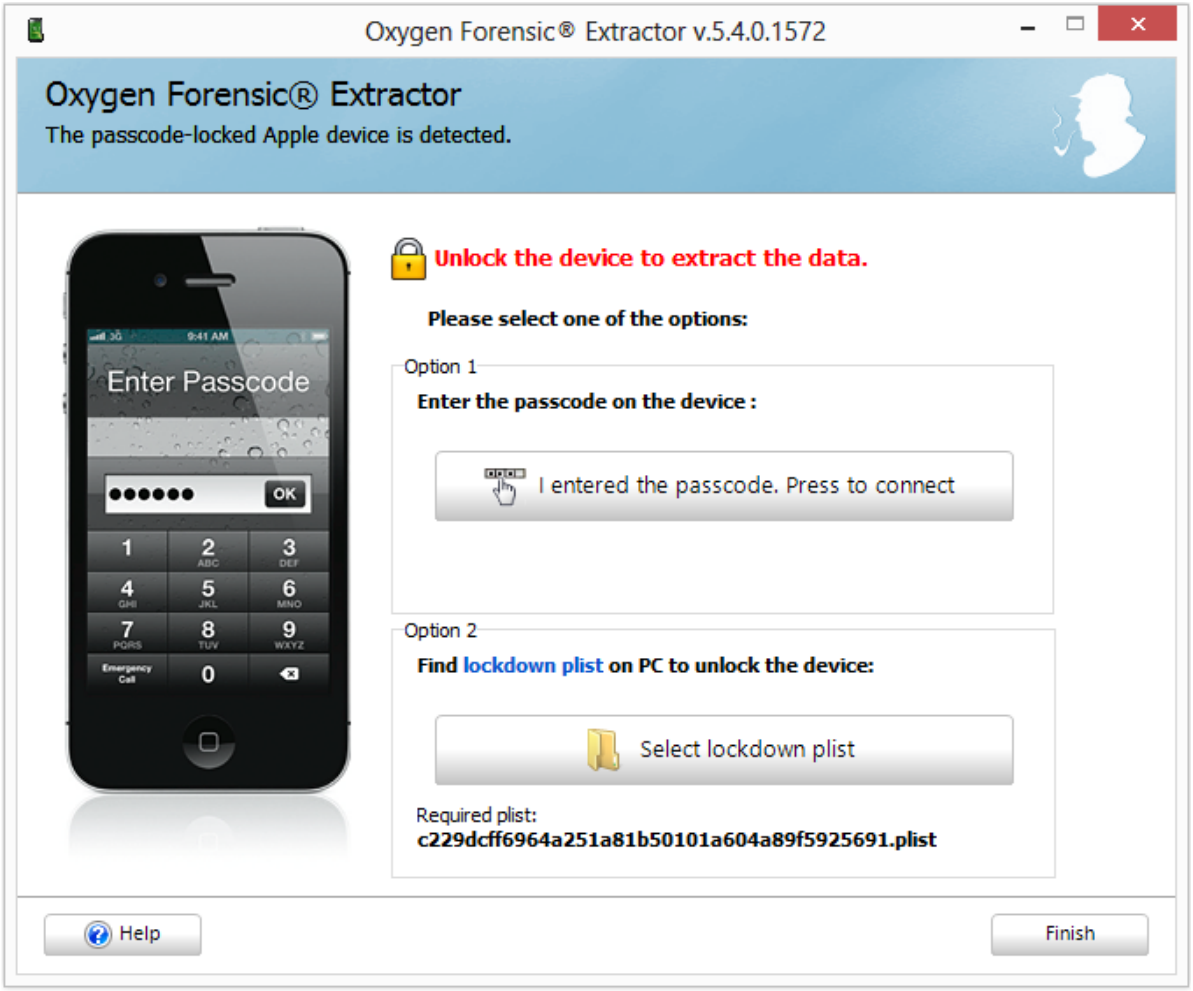
iPhone lock screen

Look for lockdown.pslist on the machine the iphone was synched with

Where to search:

- Windows 98/ME/2000/XP:
  - Documents and Settings\All Users\Application Data\Apple\Lockdown\
- Windows Vista/7:
  - Users\<User Name>\AppData\Roaming\Apple Computer\Lockdown\
- Windows 8/10:
  - ProgramData\Apple\Lockdown
- Mac OS X:
  - X (VolumeName)\Users\<User Name>\Library\Lockdown\

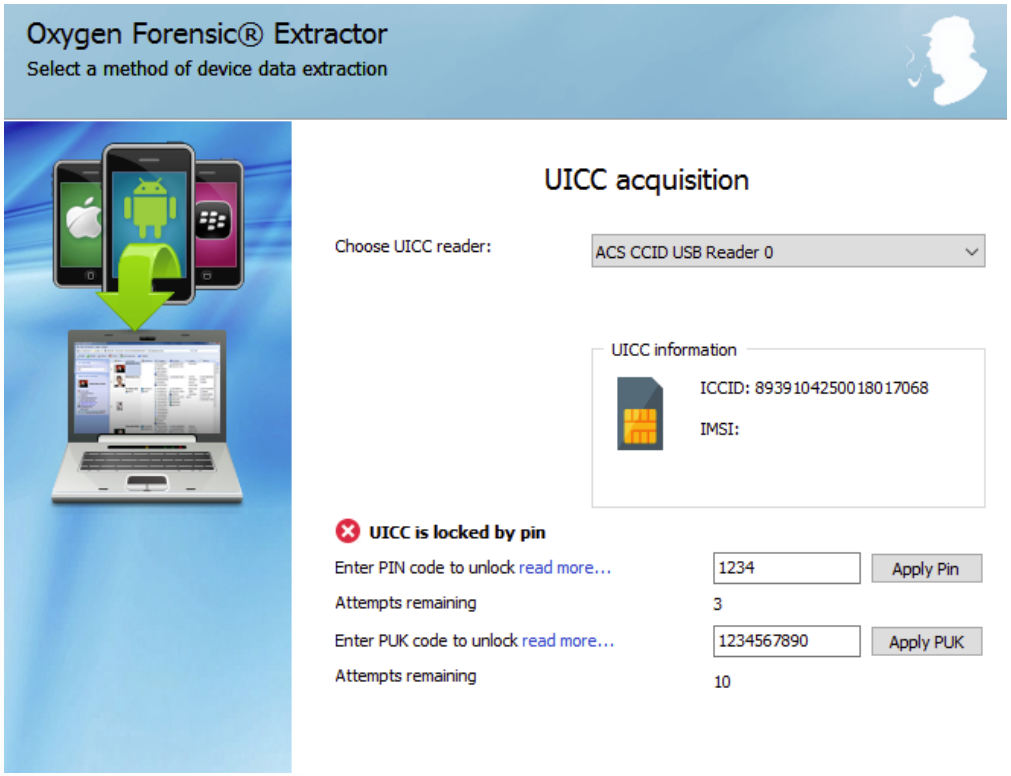
Oxygen iPhone lock screen



Oxygen iPhone lock screen

Oxygen Acquire from a SIM

- You can extract data from a SIM using a SIM card reader. If it is locked with a PIN code you will be given a chance to enter that with the Forensic Extractor.



Acquire from a Backup

- You can import several backup types including
  - iTunes Backup
  - Apple Backup/Image (many types)
  - Android Backup
  - UFED Physical Image
  - Windows 8 or Android JTAG image
  - Blackberry backup
  - Nokia backup

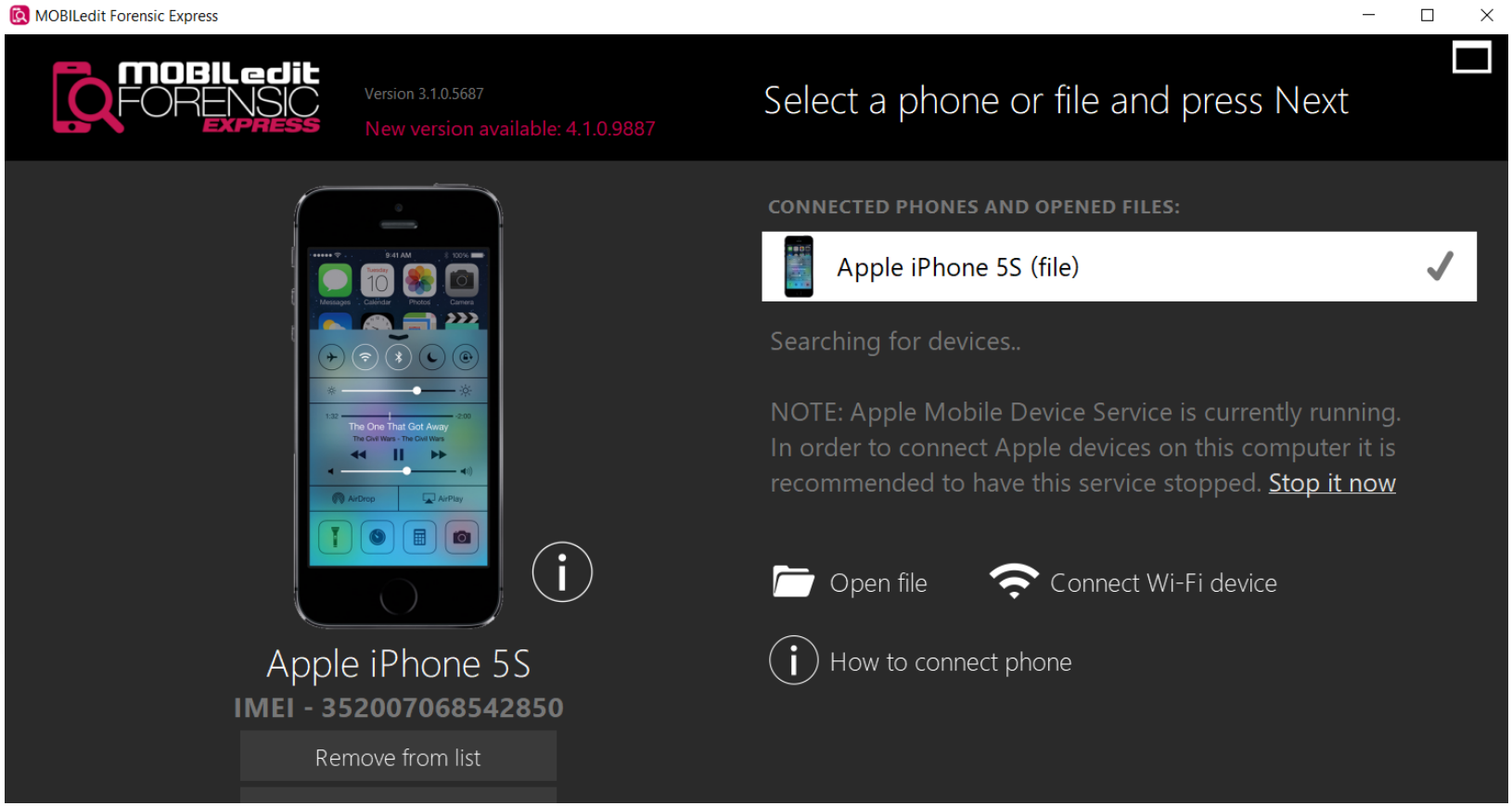
Acquire from a Backup

- Finding iTunes backup on PC
  - Find the Search bar:
  - In Windows 7, click Start.
  - In Windows 8, click the magnifying glass in the upper-right corner.
  - In Windows 10, click the Search bar next to the Start button.
- In the Search bar, enter %appdata%
- Press Return.
- Double-click these folders: Apple Computer > MobileSync > Backup.

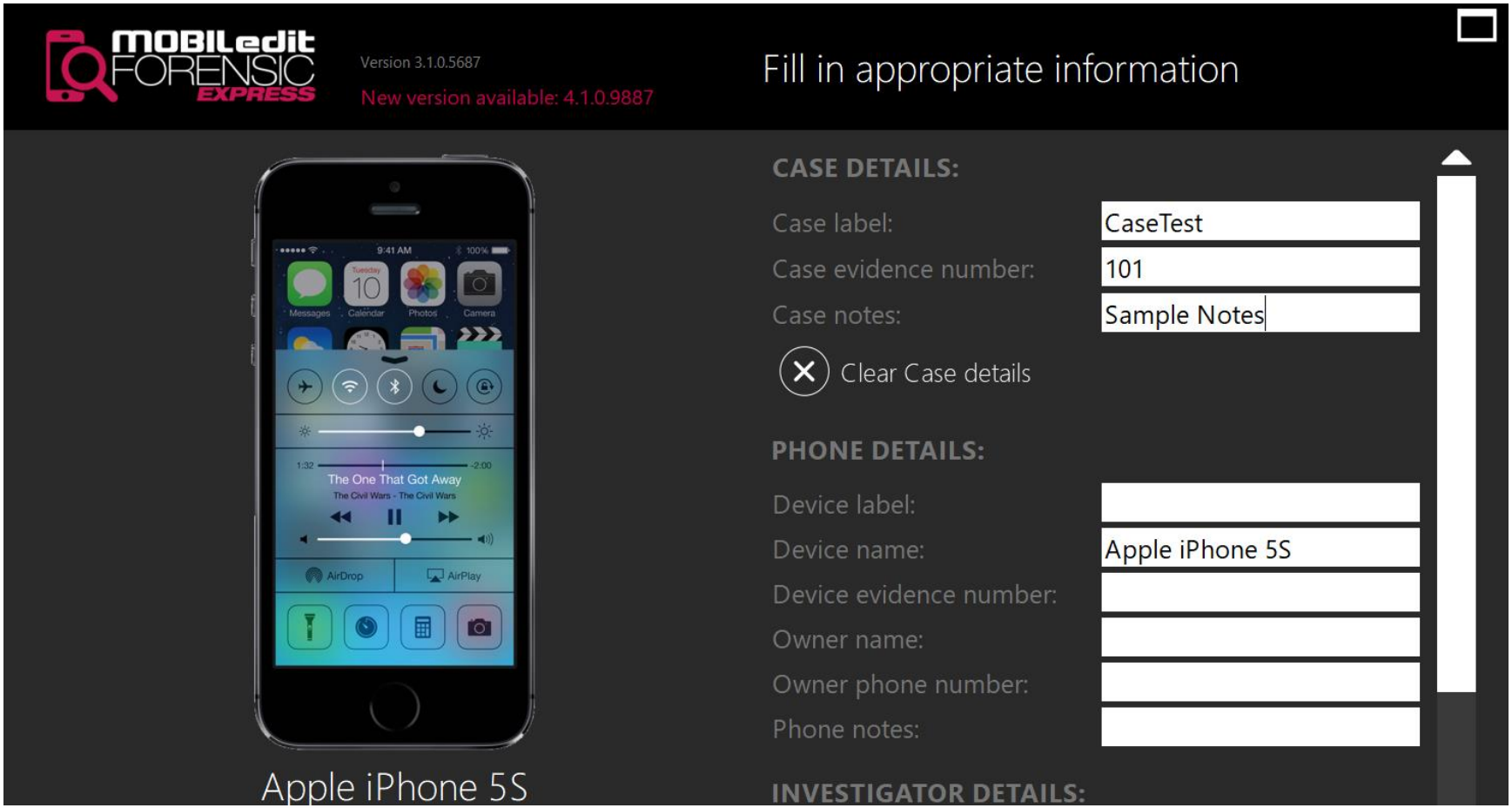
Mobile Edit

- Several versions
  - Get Forensic Express (top version $1500 for the license. $600 to renew)
  - Forensic Express Single Phone only $99

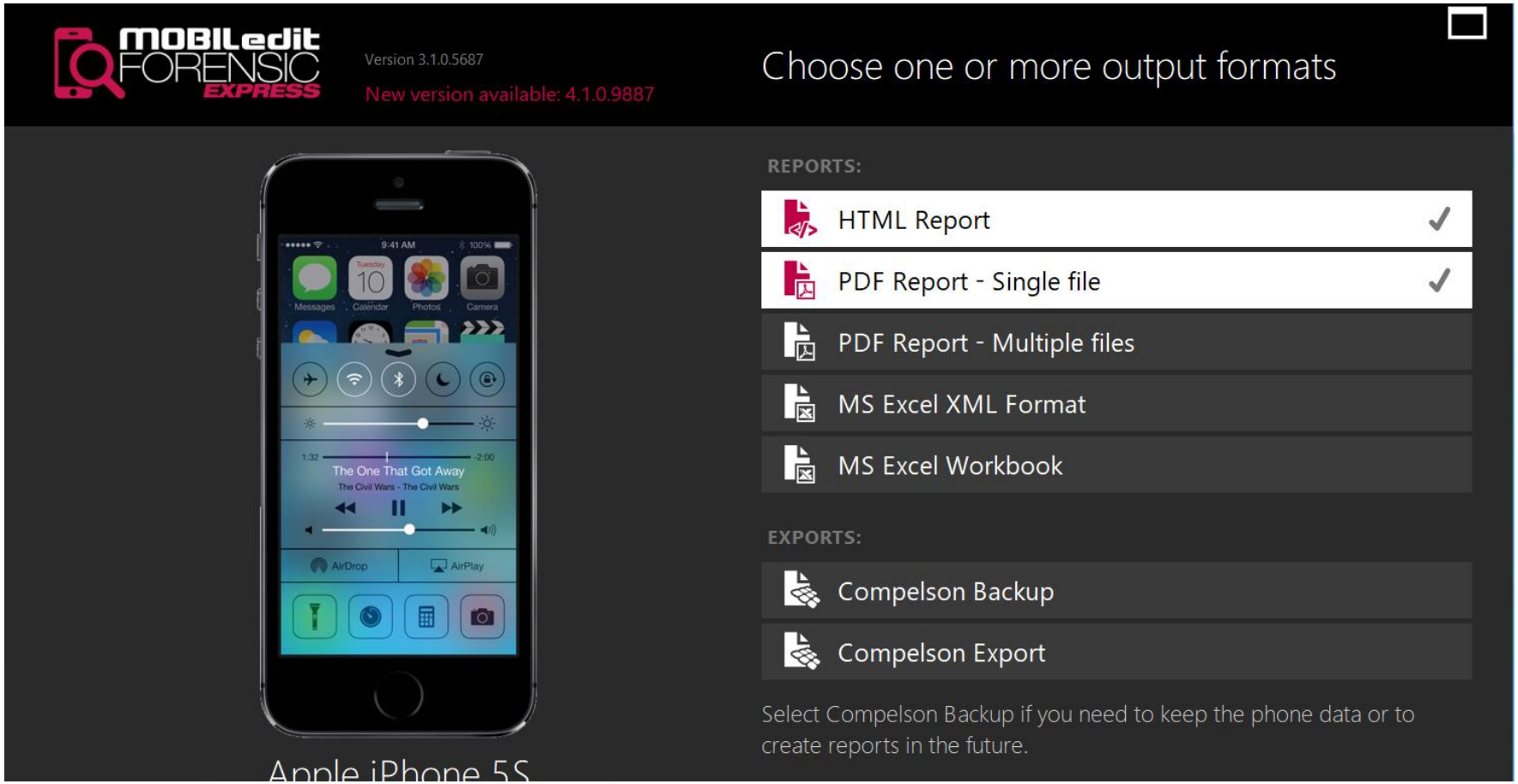
Mobile Edit Connect



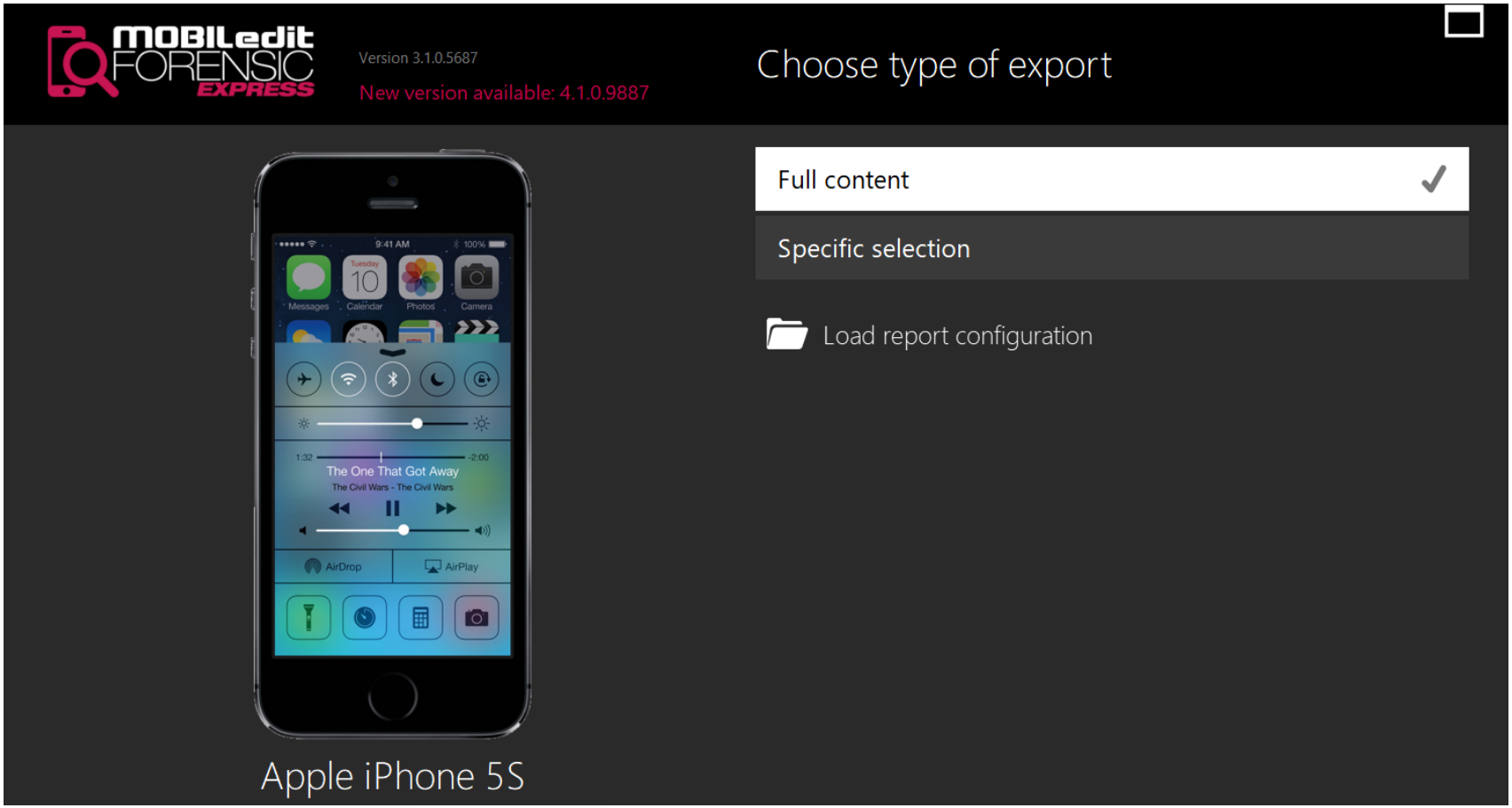
Mobile Edit Case Details



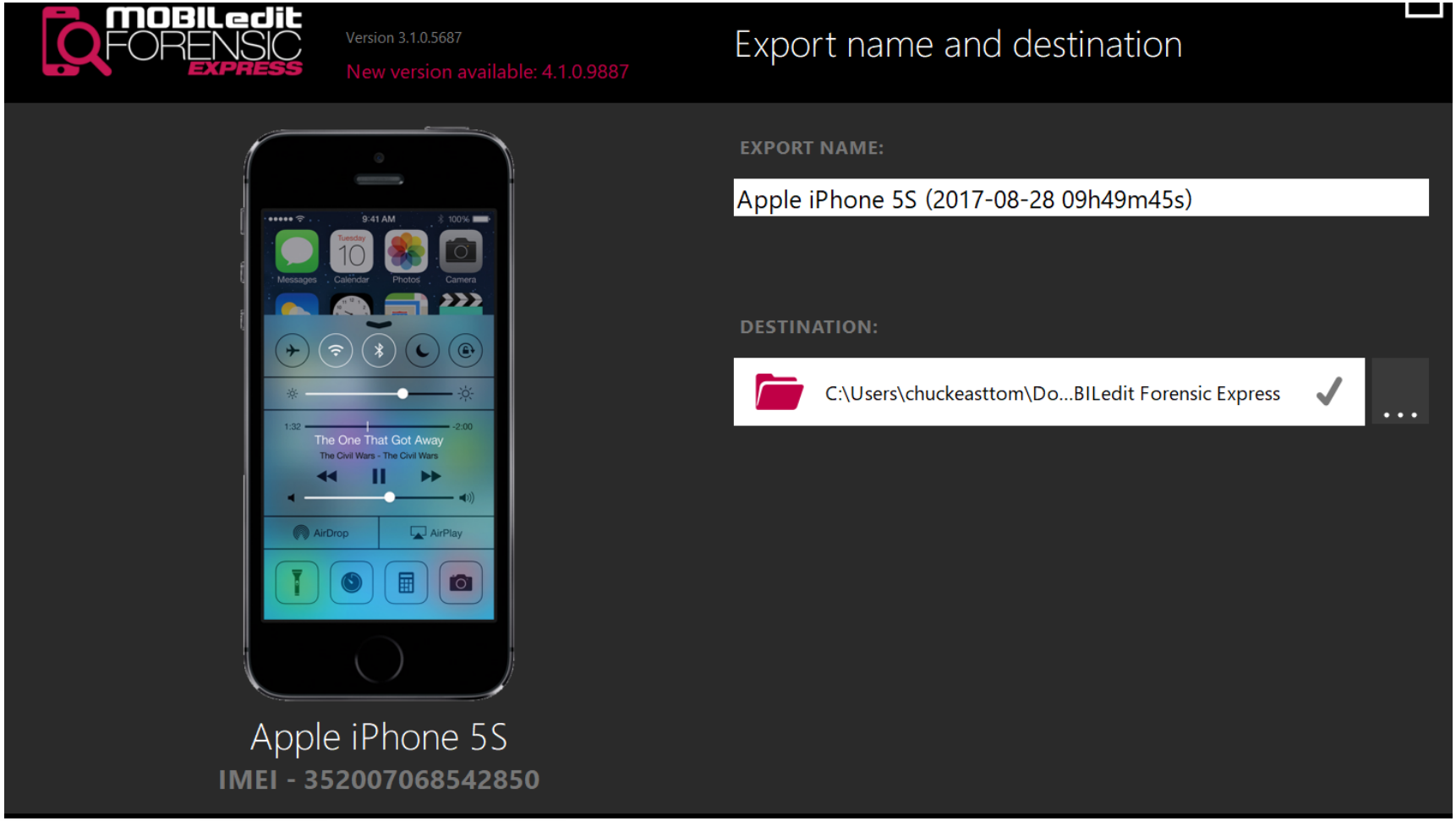
Mobile Edit Report Type



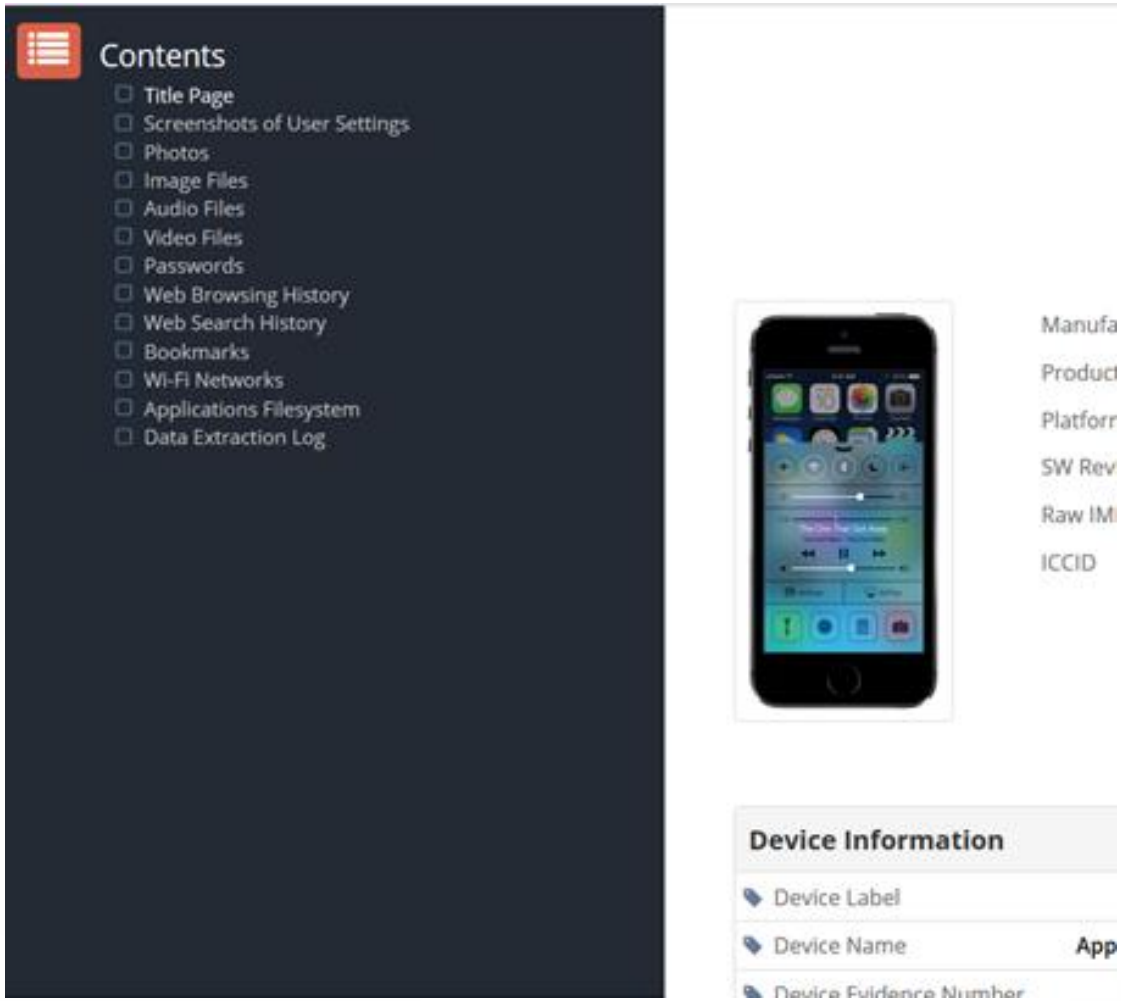
Mobile Edit Case Export Type



Mobile Edit Case Export Type



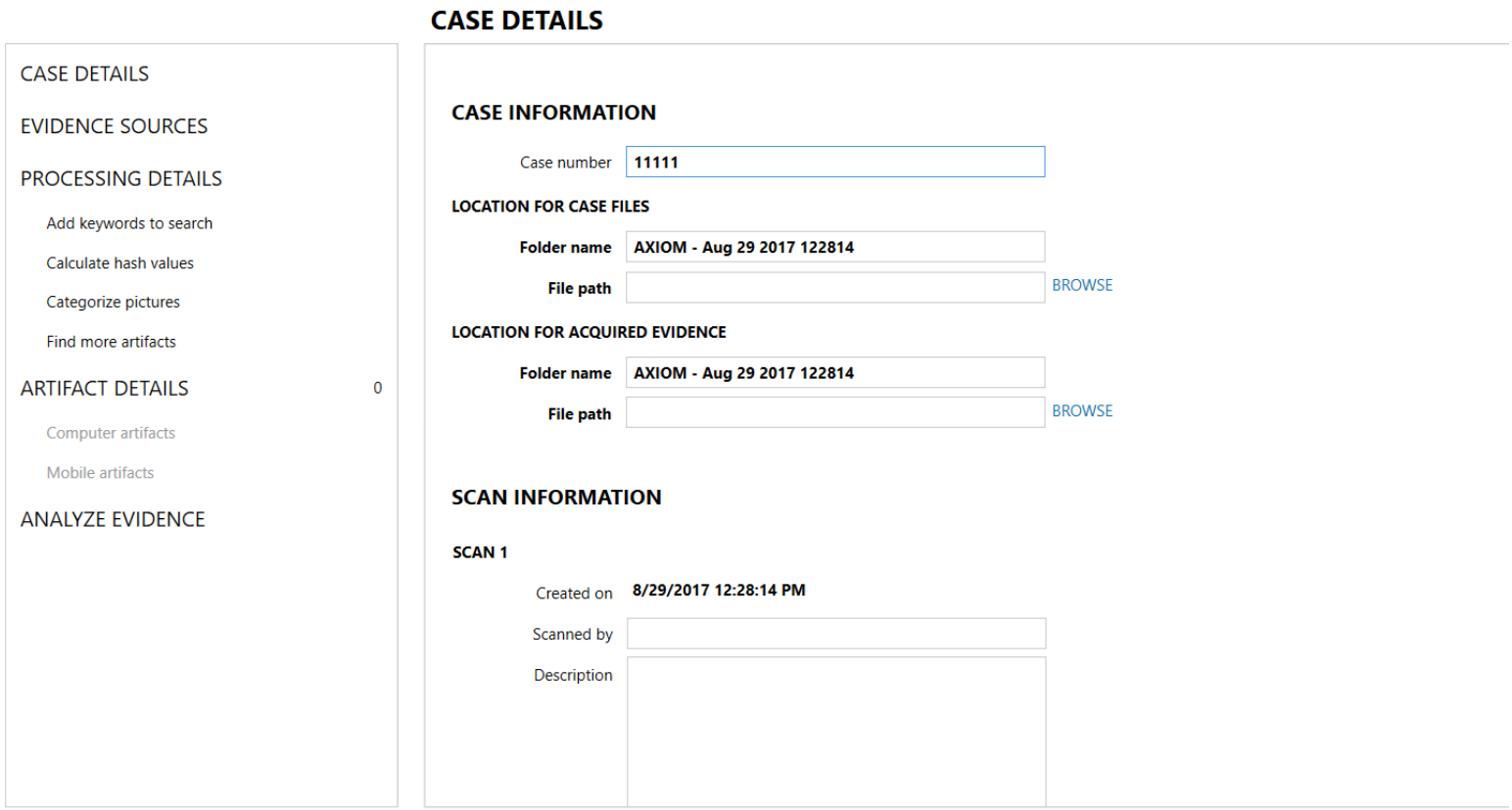
Mobile Edit Report



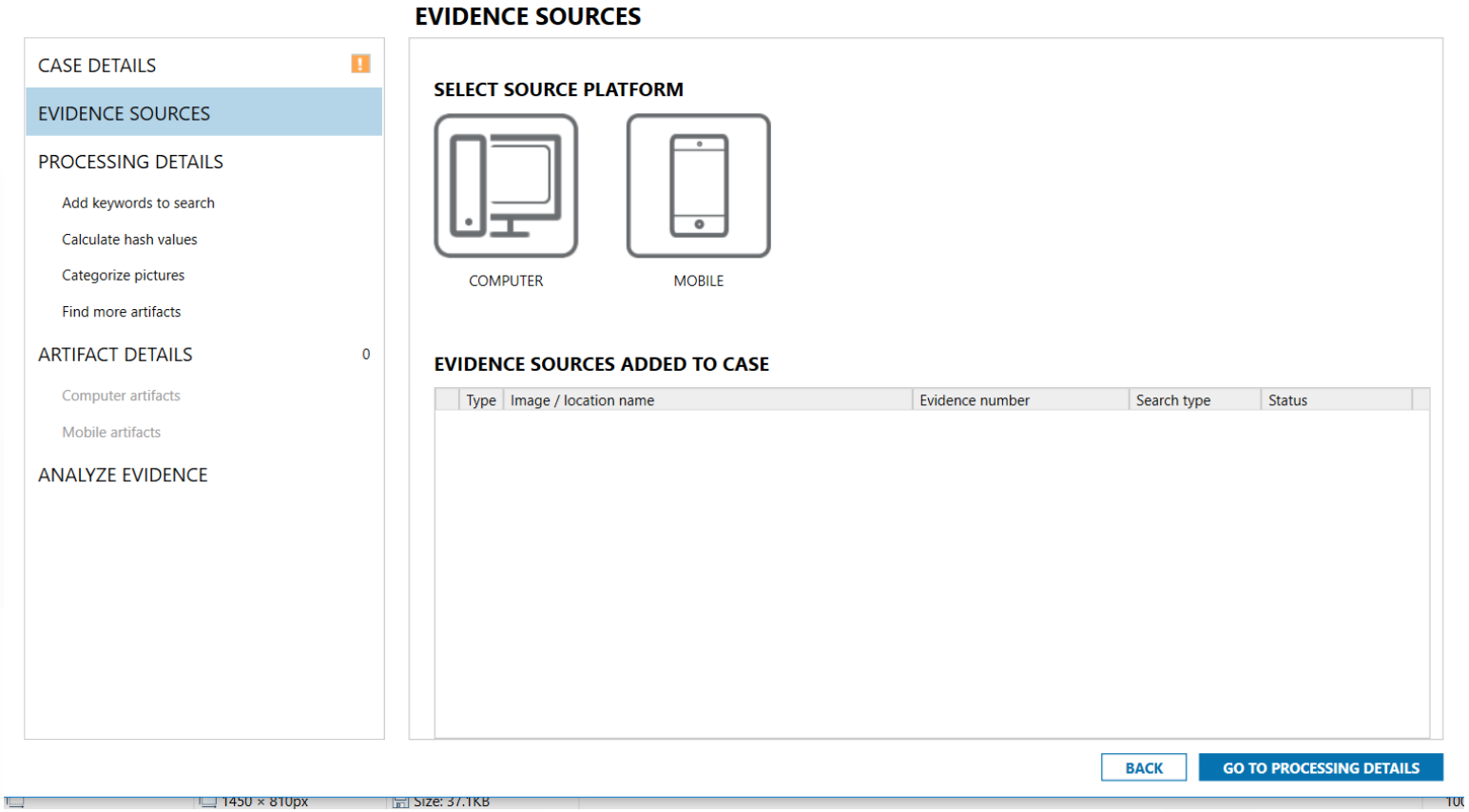
Magnet Axiom

- Several versions
  - Axiom process can do computers or phones
  - Price unknown

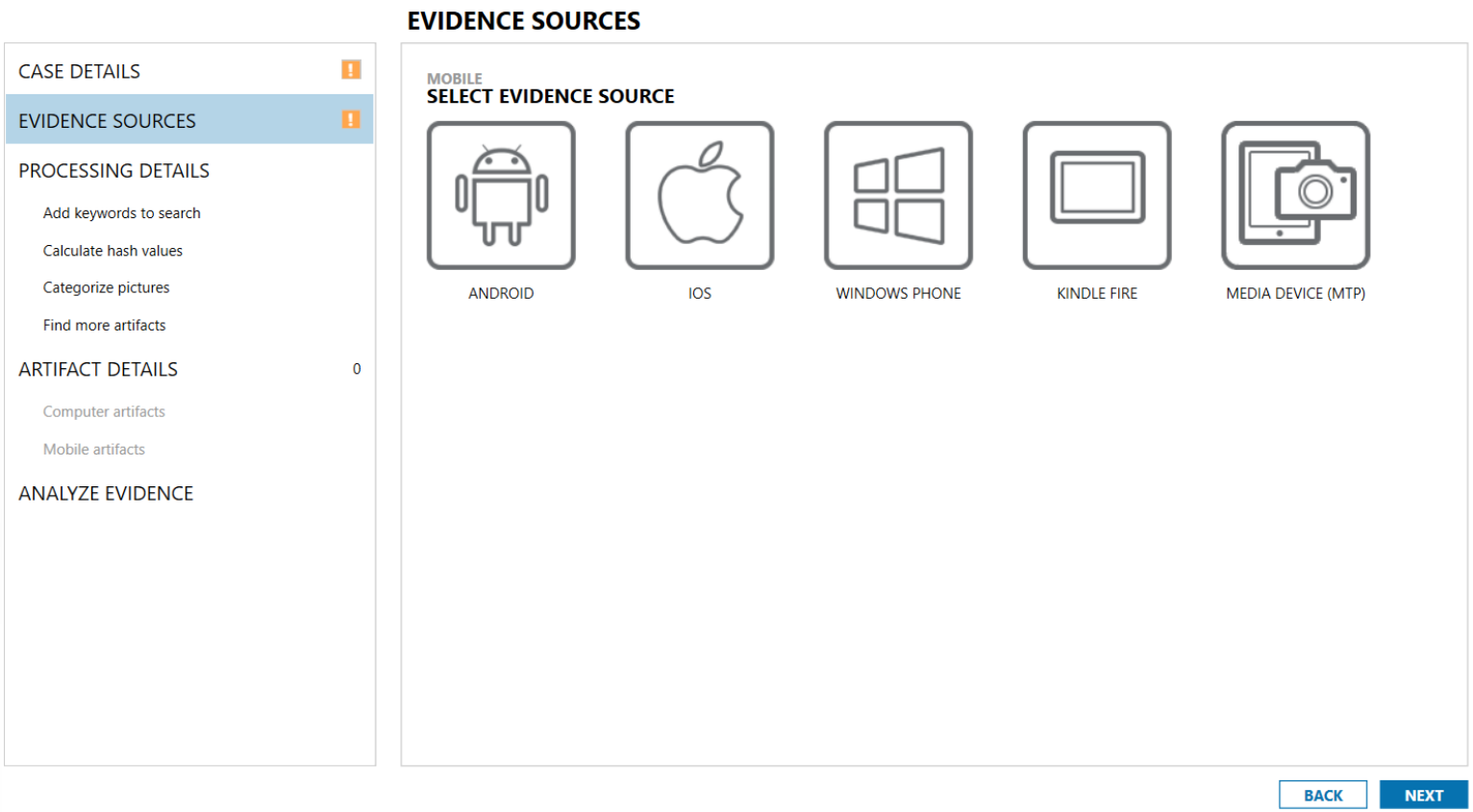
Axiom – start a case



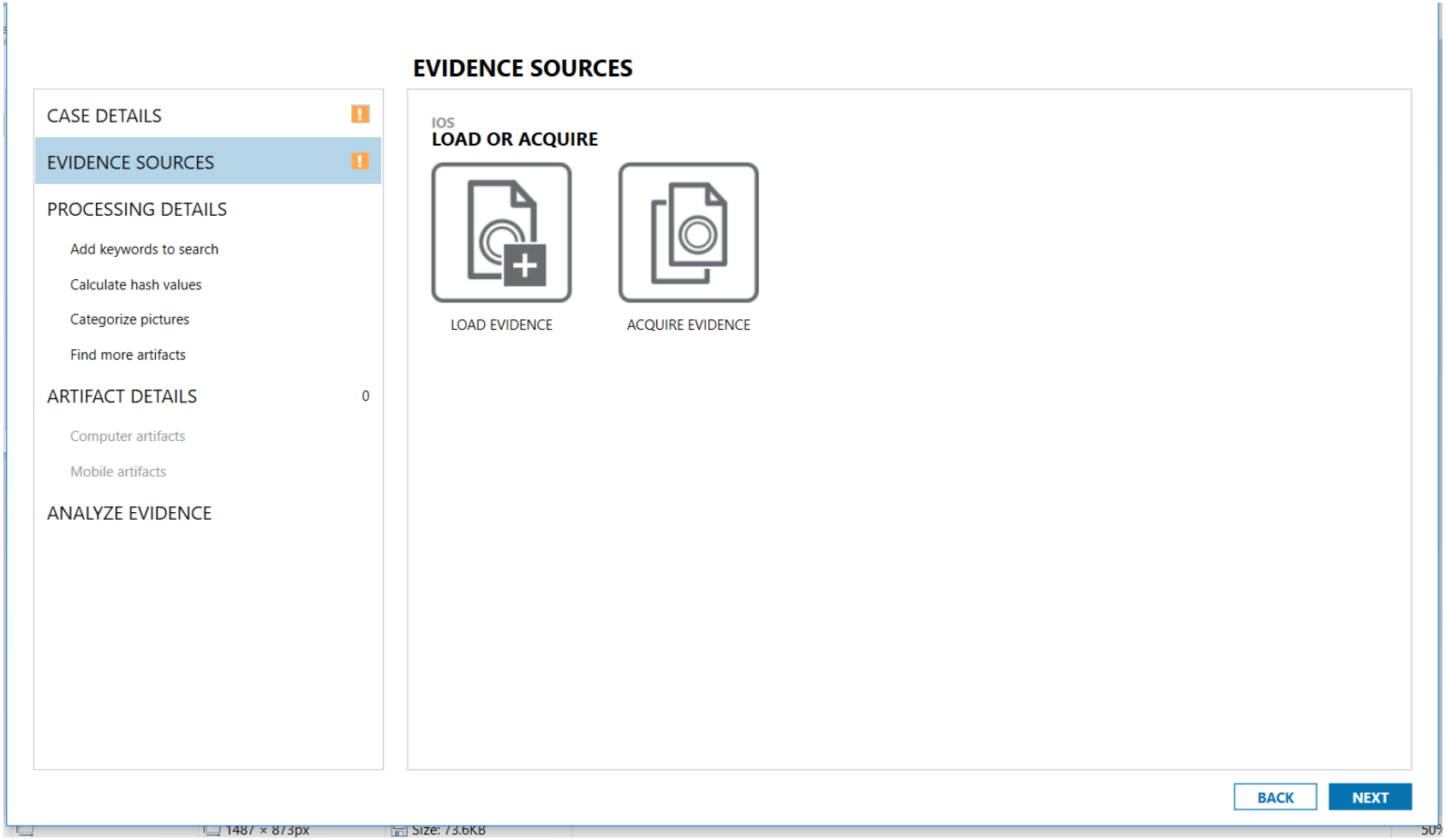
Axiom – Evidence Source



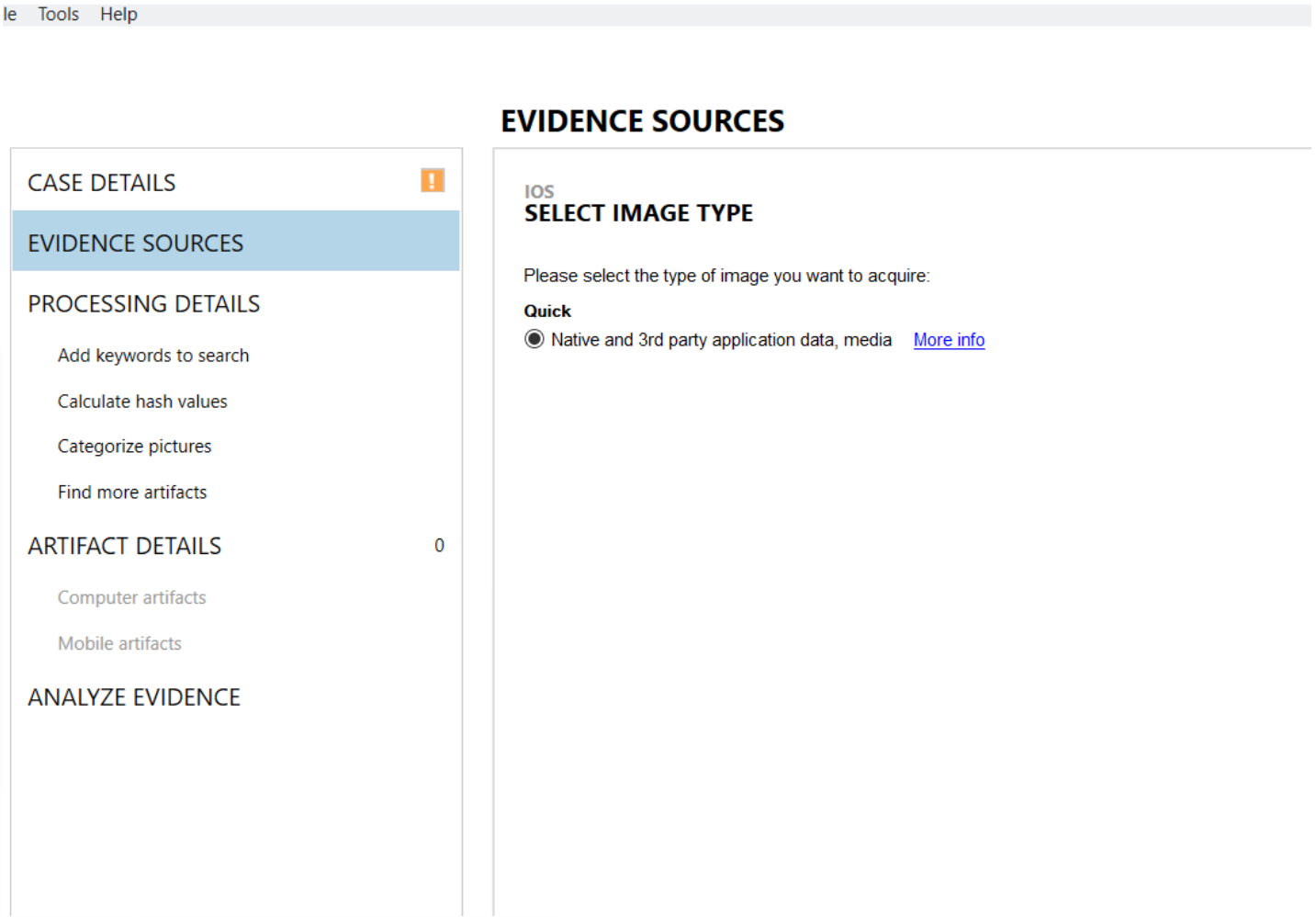
Axiom – Phone Type



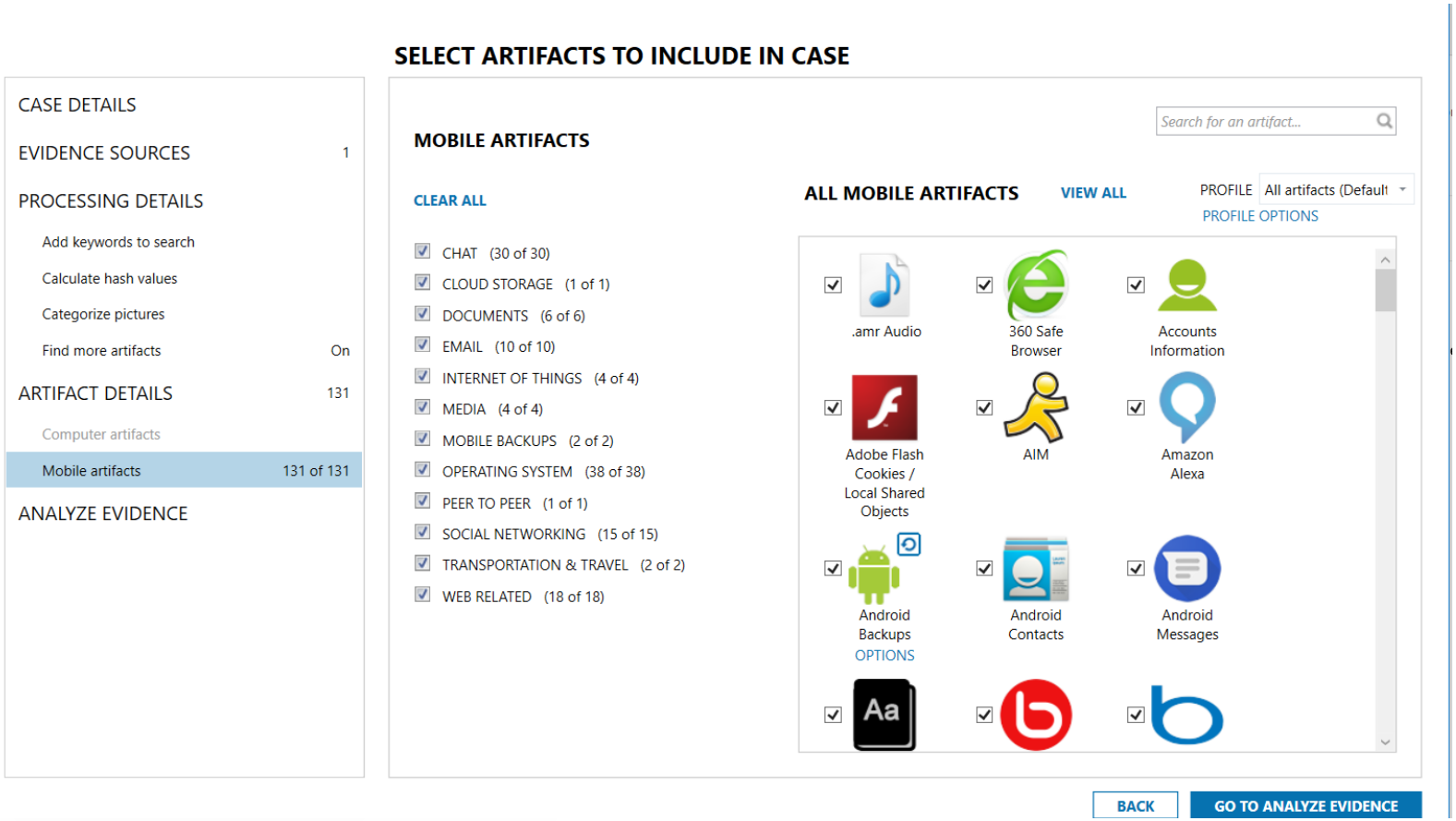
Axiom – Load or Acquire



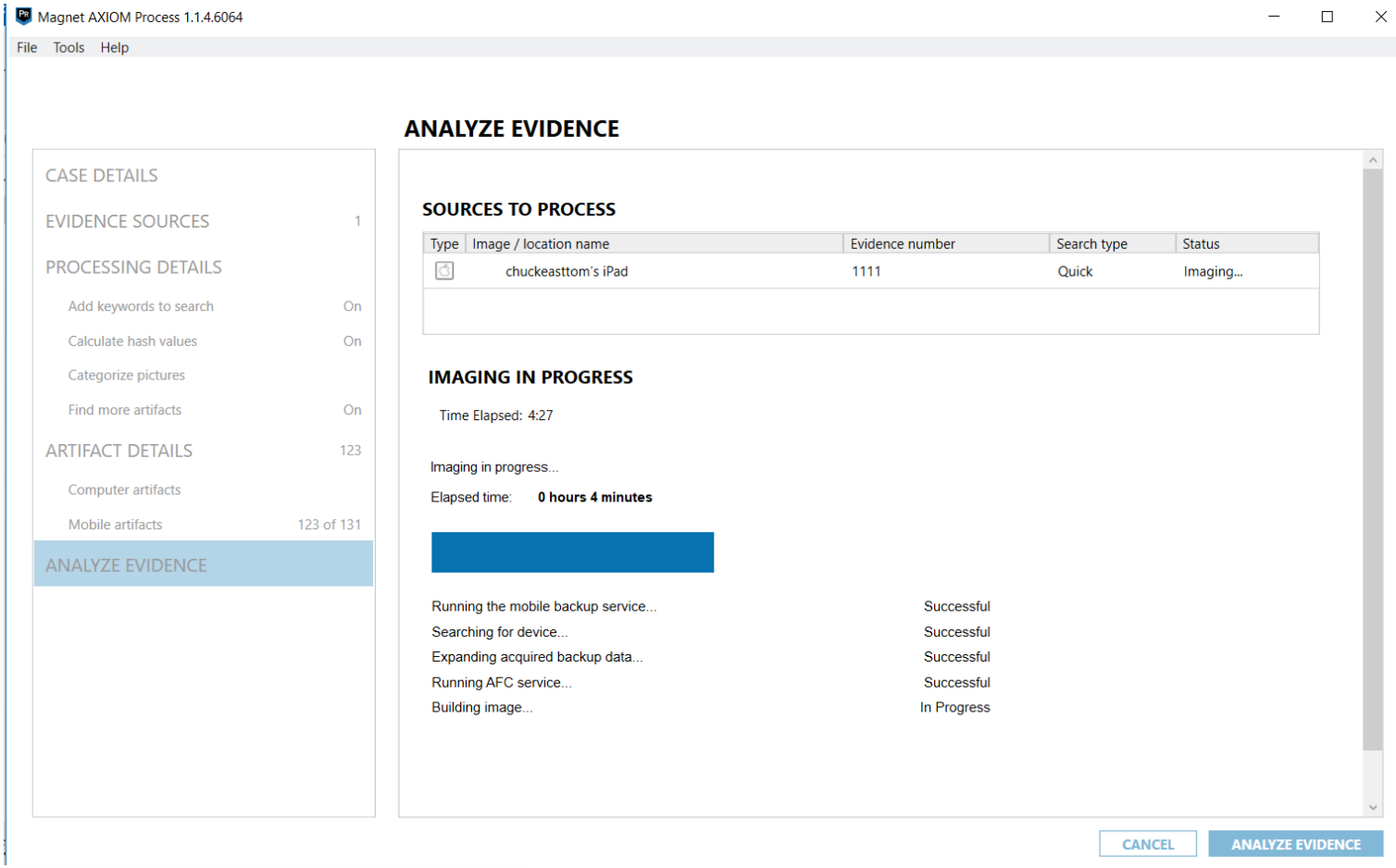
Axiom – How to Acquire



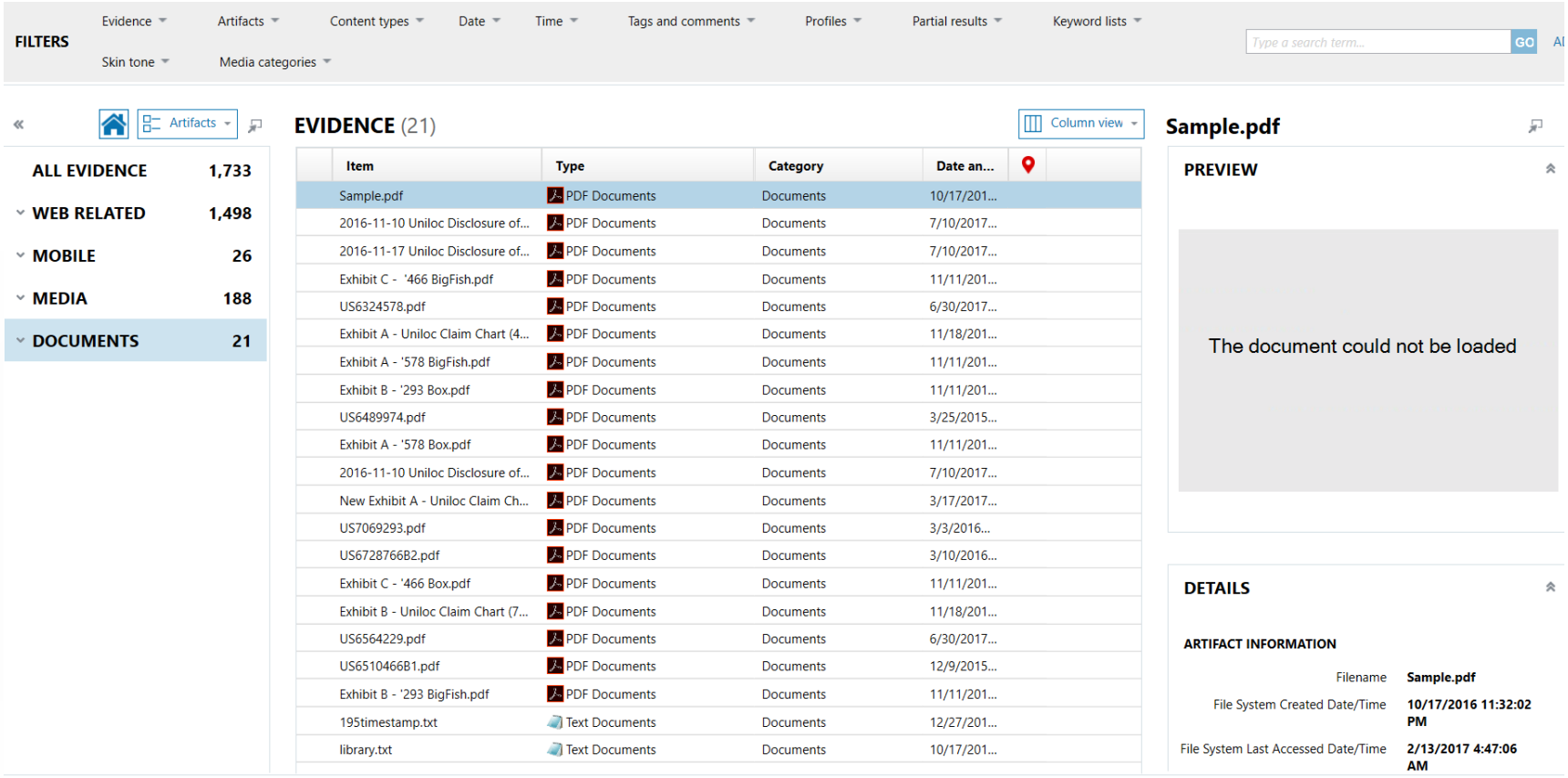
Axiom – Artifacts



Axiom – Analyze Evidence



Axiom – Analyze Evidence



MPE+

- Mobile Phone Examiner
- Same people who make FTK

MPE+ - Android Extraction

To extract data from an Android device

1. Install the proper driver for your Android phone. See the MPE+ Quick Install Guide for more information on installing drivers.
2. Ensure the phone has at least a 50% charge.
3. Activate USB Debugging mode on the phone. Activating USB Debugging mode depends on the version of Android from which you are extracting. To activate Debugging mode:
   - On most devices running Android 3.2 or older, select **Settings > Applications > Development**.
   - On Android 4.0 and newer, select **Settings > Developer options**.

   Note: On Android 4.2 and newer, Developer options is hidden by default. To unhide *Developer options*, open **Settings > About phone** and tap *Build number* seven times. Return to the previous screen and *Developer options* is available.

4. Connect the device using the correct cable. To see a list of cables, click **Supported Devices** from the *Manage* ( ) tab.
5. In *MPE+*, click **Select Device** from the *Main* ribbon.
6. Select "Android" as the **Manufacturer** and "dLogical" as the **Model** of the phone.

   Note: You can also select your specific Manufacturer and Model.

7. Click **Connect**.
8. In the *Select Data for Extraction* dialog, check the data type to extract from the connected device and click **Extract**.

MPE+ - dSOLO

dSOLO™ allows you to provision a MicroSD card to extract pre-configured user data types from any Android device that has an SD card slot. With this mode, you can create an extraction profile containing the items to extract within MPE+ and then compile that profile to a MicroSD card. You can then insert the provisioned card into an Android device independent of any connection to MPE+. The configured application initiates on the Android device and the previously selected extraction capabilities are extracted from the device onto the SDCard in a format that only MPE+ can read.

MPE+ - dSOLO

the target device.

Note: Make sure that the SDCard has a large enough capacity to store the extracted data of the target device or devices.

MPE+ then creates the dSOLO agent (`MPE.apk`) onto the SDCard.

To configure dSOLO Mode

1. Click **Configure dSOLO Mode** from the *Tools* ribbon.
2. Select the configuration options for dSOLO Mode.
3. Select the device from the *Device Selection* menu. This is the device where MPE+ creates the dSOLO Mode file.
4. Click **Create APK**.

Note: When writing to a device that already contains a dSOLO Configuration File, clicking **Create APK** with replace the older configuration file. To retain the older configuration file while adding configuration options, click **Refresh**.

MPE+ - Apple Screen 1

To acquire data from an Apple device

1. Power on your Apple device and connect it to the MPE+ system via a USB cable. Your device should now be booted into normal mode.
2. Launch MPE+ and click **Select Device**.
3. In the *Device Selection* dialog, select **Apple** from the Manufacturer drop-down list, **i[DEVICE] (Physical)** as the Model, and click **Connect**.
4. Click **Connect**.
   The DFU wizard launches.
5. Press and hold the sleep button (the button on the top of device).
6. Slide the red button to power off and wait 10 seconds after the device has powered off completely.
7. Click **Connect**.
8. Click **Next**. You have 3 seconds to position your hands over the device's buttons.
9. At that end of the 3 second "Get Ready" count-down, press and hold the *Sleep* and the *Home* buttons simultaneously. Hold both buttons down until the countdown reaches zero.
   This is the first step towards powering on the device into DFU mode.

   Note: Press the *Sleep* button (top) before the *Home* button (bottom) if it is not possible to press both at the same time.

10. As the 10 seconds expire, prepare to release the *Sleep* button (top) while still holding the *Home* button (bottom). Release the button when prompted.
11. The wizard will automatically transition to the next slide and will begin a new countdown.

MPE+ - Apple Screen 2

12. If successful, the wizard will say Complete!

> **Note:** If the device boots into recovery mode, you must unplug the device, and boot the device back into normal mode by holding both buttons until you see the apple logo. Then, click the yellow **Restart** button to start the wizard over again. For help see "Troubleshooting Apple Driver Mode" on page 32.

13. At this point the screen turns white, and then black (on some devices, an AccessData custom splash screen displays). Lastly, an MPE+ logo with an empty progress meter appears.
14. If the device has a passcode, MPE+ prompts you to do one of the following and click **OK**:
    - **Use Brute Force**: Select this if it is a SIMPLE passcode and you do not know the passcode of the phone. SIMPLE passcodes are commonly a 4 digit number. Upon completion, MPE will tell you the SIMPLE passcode of the device.
    - **Use Passcode**: Select this if you know the SIMPLE or COMPLEX passcode. You can then enter the SIMPLE or COMPLEX passcode and bypass the brute force methods.
    - **Get Logical Partition Only**: Select this if you are prompted with a COMPLEX passcode and are unsure of the password. You will still be able to recover data not protected by the Apple API.
15. MPE+ prompts you to choose which partitions you would like to acquire from the device. Check the items you want to extract and click **OK**.
    See Acquiring Apple Device Partitions on page 31.

> **Note:** From this point on, if you make any mistake, no cancel options will be provided. The only recourse will be to unplug the device, boot the device back into normal mode, and start the connect process again from the beginning.

MPE+ - Apple Partitions

Acquiring Apple Device Partitions

Before you can proceed with these steps, you must be properly connected to the device.

See Connecting to an Apple Device for Physical Acquisition on page 30..

1. When prompted to select which partitions you would like to acquire, choose one of the following:
   - Full Disk (gets user partition, OS Partition, and slack space).
   - OS partition (usually quite small, about 1GB).
   - User partition (Device storage capacity minus OS partition).
   - Decrypted user partition (Same size as user partition. This option will only be available for devices that support encrypted user partitions).
   - Logical OS Partition
   - Logical User Partition

Note: During physical Apple device acquisition, once you have confirmed which partitions you want to extract, you cannot cancel the "Browse for folder" dialog in order to change the selected partitions.

2. When prompted, browse to the desired destination to save the device image.
3. When the acquisition is complete, you will receive a message indicating that the process completed successfully.

MPE+ - Storage

MPE+ can extract data from mass storage devices including SD cards, Flash Drives, Hard Drives, and so forth.

To extract data from a mass storage device

1. Click **Mass Storage** on the Main toolbar.
2. Select and enter either a *Physical Image* or *Logical Image*.
3. Click **Next**.
4. Click **Add** to add *Image Destination(s)*. You can also edit or remove existing image destinations.
5. Select the *Destination Image Type*. You can also add notes or a description (optional).
6. Click **Next**.
7. Enter the *Image Destination Folder*, the *Image FileName*, and the *Image Details*.
8. Click **Finish**.

MPE+ - Image files you can import

- AD1
- FAT
- E01
- YAFFS
- YAFFS2
- EXT
- EXT2
- EXT3
- EXT4
- TAR
- RFS
- DD4
- DD8
- DD4.001
- DD8.001

MPE+ - Data Carving

To run a data carve

1. Click the **Carve Data** button on the *Main* ribbon.

   Note: If you have already done a data carve on the collected phone data, you will be asked if you want to discard the data and do a new carve; click Yes to continue.

2. In the *Data Carve Options* dialog, check the folders in the file system that you want to include in your search, as well as the data types to carve.
3. Click **Continue**.
   The Data Carving progress dialog displays.
4. When carving is complete, the **Cancel** button deactivates and the **Close** button activates. Click **Close**.
   The carved data list is displayed in the *Carved Data*, *Data View*.

Cell Site Analysis

- Historical call records from the carrier
- The National Institute of Standards (NIST) states that cell phone towers can be servicing phones as far away as 35 kilometers (21.74 miles).
- "While plotting call record locations and information onto a map can sometimes be useful, it does not necessarily provide a complete and accurate picture. Cell towers can service phones at distances of up to 35 kilometers (approximately 21 miles) and may service several distinct sectors."

Cell Site Analysis

"Recourse to the CCR Cell ID is useful only to establish a possible area in which a sending mobile was locate when a call was made from that mobile and 'picked up' by a receiving telephone [19]. Herbert Dixon goes even further in his article "Scientific Fact or Junk Science; Tracking a Cell Phone without GPS" [20] describing the use of cell phone usage records to determine location of a cell phone as "junk science".

TABLE I. TABLE 1: CELL PHONE TOWER AREA COVERED

Radius (km)	*Radius (miles)*	*Area (km)*	*Area (miles)*
5	3.16	78.5	31.35
10	6.32	314	121.2
35	21.74	3846.5	1484.05

Cell Site Analysis

- Figure 1, shown below, has a map of part of New York City, showing cell phone tower locations.

Cell Site Analysis

Montana

Cell Site Analysis

How to estimate

Time	Cell Tower Connected to	Distance to Next Tower in the path	Mean distance to handoff to next tower
01/01/18 09:12:52	A	1.5 km	.75 km
01/01/18 09:14:54	B	2.0 km	1.0 km
01/01/18 09:17:52	C	2.0km	1.0 km

Given D_i = mean distance for hand off ; E_i = margin of error per hand off

$$\sum_{i=1}^{n} D_i \quad +/- \quad \sum_{i=1}^{n} M_i$$

Easttom, C. (2018). A Method For Using Historical GPS Phone Records. Digital Forensics Magazine, 36.

Logical Acquisition

- Logical imaging refers to copying the active file system from the device into another file. Through this method, allocated data from the actual device is recovered and can later be analyzed. Logical techniques are often the first type of examination forensic analysts will run because they are easier to execute and often provide sufficient data for the case.
  - Data extracted using common PC-to-mobile communication protocols:
  - Smartphone connected to PC with a standard cable (or Bluetooth/IR adapter)

- iPhone forensics physical techniques can provide far more data; however, they are more difficult to execute successfully and also take considerably more effort to analyze.
  - Data extracted using direct memory reading (hex dump)

Physical

Physical imaging has been widely used in forensics for many years, but is relatively new to the mobile device world. A physical acquisition creates a physical bit-by-bit copy of the file system, similar to the way a hard drive would be forensically imaged. For this reason, it has the greatest potential to recover large amounts of data, including deleted files. The release of iOS 4 brought up many issues from a mobile forensics standpoint. Hardware encryption is offered with iOS versions 4 and beyond. What this means is that even if a full physical disk image is possible, all the data may be encrypted.

Comparison

Logical

- Some information Extracted
- Faster
- Easy to analyze
- All tools can get at least this information

Physical

- All information extracted
- Slower
- Harder to analyze
- Not all tools can get this information

Chip-off & JTAG

- The chip-off technique describes the practice of removing a memory chip, or any chip, from a circuit board and reading it. Literally unsoldering it
  - Need specialized equipment to read the chip
- IEEE Joint Test Action Group (JTAG) methods
- mobile devices that are implementing the BGA-style memory incorporate JTAG for test and debugging. That means the JTAG ports can be used to retrieve a physical image of the data without requiring the removal of the chip

What JTAG can (and can't) do

- It can bypass login
- It can work on Android and Windows phones
- It cannot (at least not now) work in iPhone
- It cannot bypass encrypted drives
- It is not fast
- It is not a phone forensics panacea

What is JTAG?

JTAG = Joint Test Action Group – method for testing circuits

IEEE codified the JTAG efforts – IEEE Standard 1149.1

Technique used to acquired data directly from a mobile device's Printed Circuit Board (PCB)

Terms

JTAG = Joint Test Action Group – method for testing circuits
IEEE Standard 1149.1 – JTAG standard
PCB - Printed Circuit Board
TAP – Test Access Port
DCC – Debug Communications Channel
BSR – Boundary Scan Register
TDI (Test Data In)
TDO (Test Data Out)
TCK (Test Clock)
TMS (Test Mode Select)
TRST (Test Reset) optional
ETM – Embedded Trace Module
DSCR – Debug Status and Control Register
ETB – Embedded Trace Buffer
ITR – Instruction Transfer Register

What is JTAG?

"Circuitry that may be built into an integrated circuit to assist in the test, maintenance and support of assembled printed circuit boards and the test of internal circuits is defined. The circuitry includes a standard interface through which instructions and test data are communicated. A set of test features is defined, including a boundary-scan register, such that the component is able Circuitry that may be built into an integrated circuit to assist in the test, maintenance and support of assembled printed circuit boards and the test of internal circuits is defined. The circuitry includes a standard interface through which instructions and test data are communicated. A set of test features is defined, including a boundary-scan register, such that the component is able to respond to a minimum set of instructions designed to assist with testing of assembled printed circuit boards. Also, a language is defined that allows rigorous structural description of the component-specific aspects of such testability features, and a second language is defined that allows rigorous procedural description of how the testability features may be used."

-1149.1-2013 - IEEE Standard for Test Access Port and Boundary-Scan Architecture

What is JTAG?

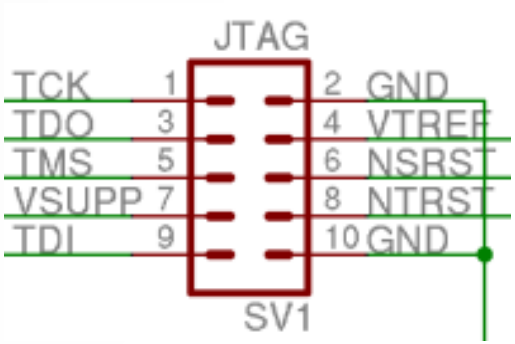
"To perform a JTAG extraction, the device must be taken apart down to the circuit board. The circuit board will contain multiple taps (physical contacts on the device circuit board), though they are commonly unlabeled and there are usually far more taps than required for JTAG. To determine the correct taps, an examiner would have to either find a pin-out online (or included with their tool of choice), or use electronic test equipment to determine what each tap is. The examiner will then have to solder a wire to each tap, or use adapters (sometimes called jigs) that are commercially available, and connect to their JTAG box through a provided adapter."

-Tamma, Rohit; Tindall, Donnie. Learning Android Forensics

How does it work?

"In order to perform a JTAG recovery, one must connect the appropriate JTAG pins (Image 1 below) to the memory flasher. Once the board is powered on, the flasher software can then a full memory dump of the NAND flash. This takes a significant amount of time. The connections can then be broken and the phone can be reassembled.

Although this captures a full physical image, it is not normally used as logical means can perform sufficient coverage. Also, any errors in soldering or voltages can destroy the very small PCB connections & the device itself."
-Do-It-Yourself Mobile Forensics by Lewis Sykalski



What are TAPs for?

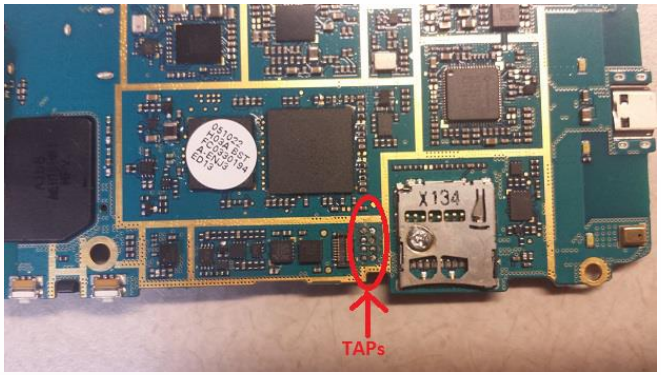
- **Debug Target** A CPU TAP can be used as a GDB debug target.
- **Flash Programming** Some chips program the flash directly via JTAG. Others do it indirectly, making a CPU do it.
- **Program Download** Using the same CPU support GDB uses, you can initialize a DRAM controller, download code to DRAM, and then start running that code.
- **Boundary Scan** Most chips support boundary scan, which helps test for board assembly problems like solder bridges and missing connections.

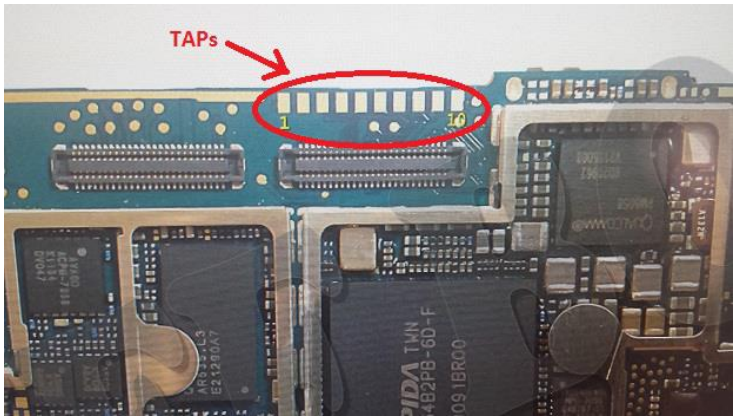
-http://openocd.org/doc/html/TAP-Declaration.html

Note: GDB is the GNU project debugger

What do the TAPs look like?

- **These are generic pictures of TAPs from NIST and AAFS**





What is Boundary Scanning?

The signals are represented in the boundary scan register (BSR) accessible via the TAP.

IEEE 1149.1 defines these connector pins

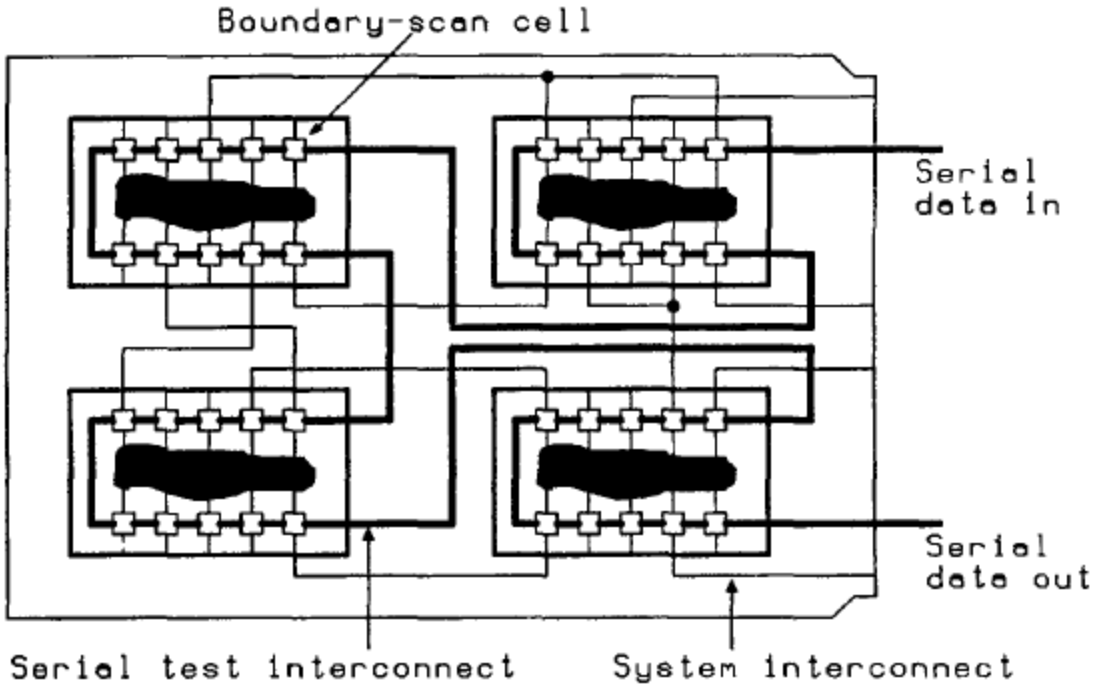
- **TDI** (Test Data In)
- **TDO** (Test Data Out)
- **TCK** (Test Clock)
- **TMS** (Test Mode Select)
- **TRST** (Test Reset) optional.

TAPS

Abbreviation	Signal	Description
TCK	Test Clock	Synchronizes the internal state machine operations.
TMS	Test Mode Select	Sampled at the rising edge of TCK to determine the next state.
TDI	Test Data In	Represents the data shifted into the device's test or programming logic. It is sampled at the rising edge of TCK when the internal state machine is in the correct state.
TDO	Test Data Out	Represents the data shifted out of the device's test or programming logic and is valid on the falling edge of TCK when the internal state machine is in the correct state.
TRST	Test Reset	An optional pin which, when available, can reset the TAP controller's state machine.

-JTAG Tutorial Corolis

What is Boundary Scanning?



-1149.1-2013 - IEEE Standard for Test Access Port and Boundary-Scan Architecture

How to get GPS from Photo

- Download the **image** file to your computer, right-click it, select Properties, and click the Details tab. Look for the Latitude and Longitude coordinates under **GPS**. On a Mac, download the file, right-click it (or Control-click it), and select **Get** Info. You'll see the Latitude and Longitude coordinates under More details

Extract Data from Garmin

- Export your activity for upload to other programs. From the Details page you can export a .TCX file for other fitness programs and .KML for Google Earth. From the Splits page you can export a CSV file with the details of your activity.

- Garmin Connect
- https://connect.garmin.com/features/export
- Or use this
- http://freegeographytools.com/2007/exporting-gps-data-to-gis-i-garmin-gps-units

Clone a phone

- This is a phone you have access to and just want the data
- Step 1: Go to https://my.Copy9.com/ and clicking on "Sign Up".
- Step 2: Download the copy9 app from copy9.com and open it to install.
- Step 3: Log into your account and activate account
- Step 4: Accept (tap Allow) them and Copy9 will be installed automatically.
- Step 5: Go to my.copy9.com-> settings. Choose SMS, Calls, GPS... any information you need and then click on 'Save & Sync Now' to begin the cloning.
- Step 6: From my.Copy9.com –> Settings –> Select tab Export Data –> Choose Features or tick all Features –> Sent to email or Download

OSForensics

- Free Trial
- Low cost for the fill version (Under $1000 per license)
- Does Windows, Mac, and now Android

Image a phone with OSForensics

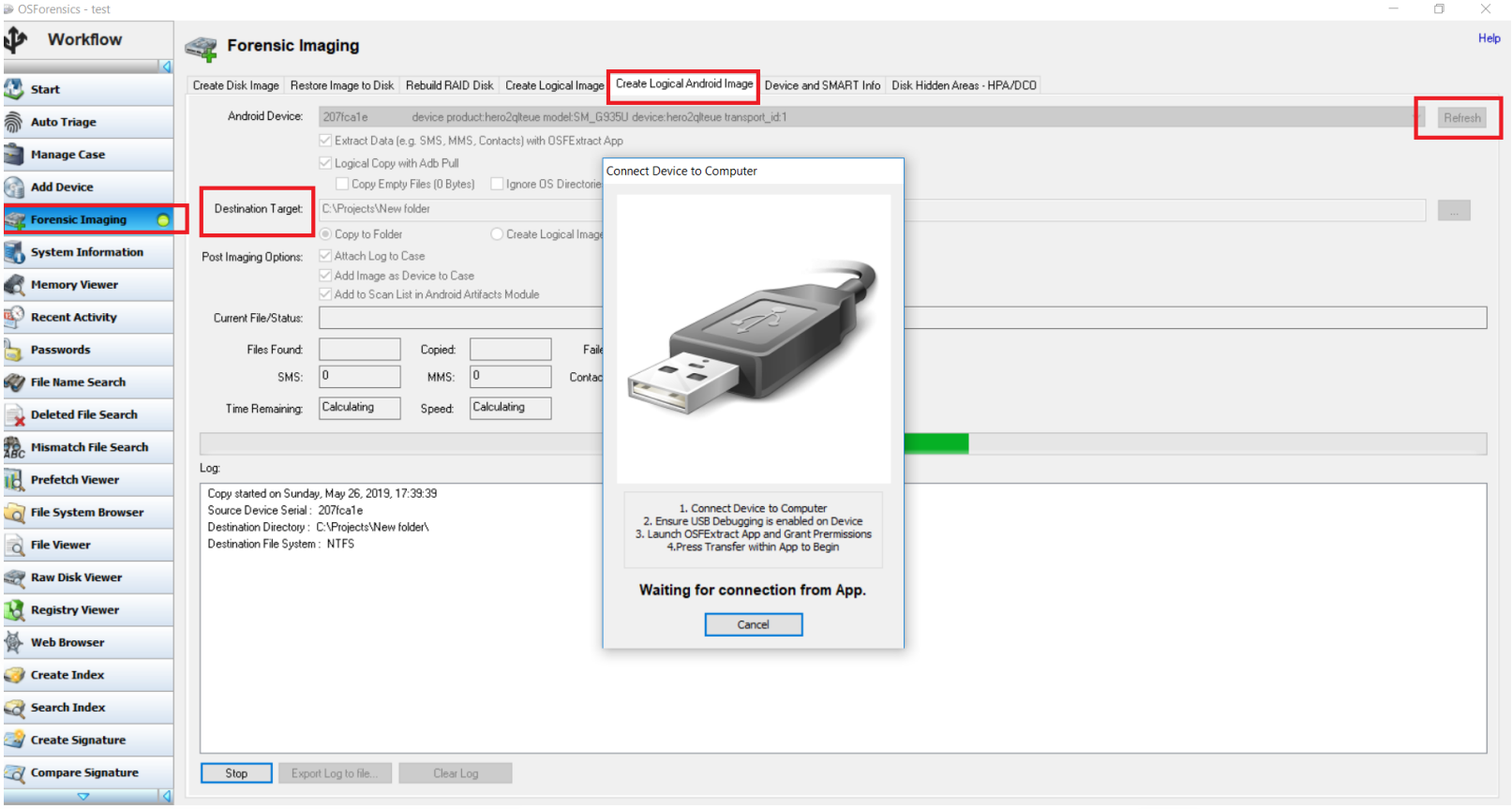
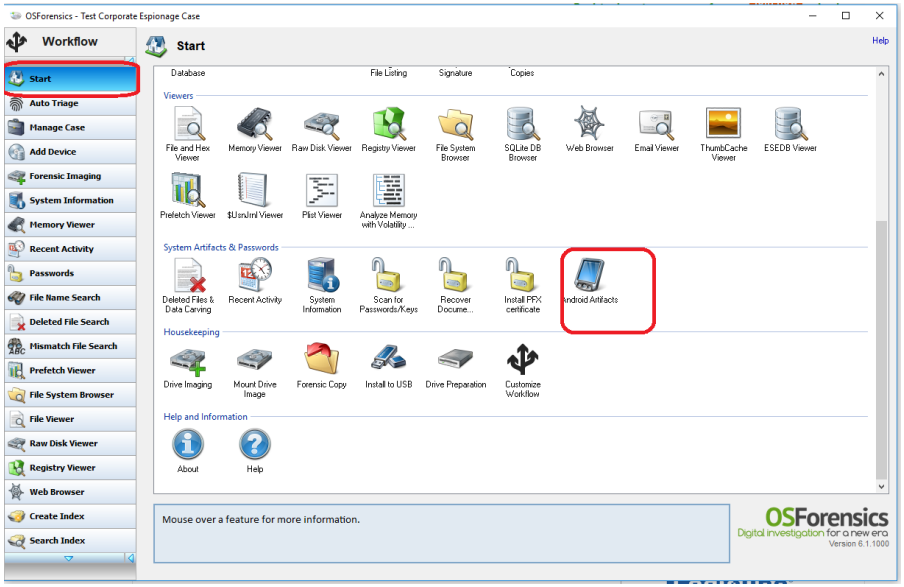


Image a phone with OSForensics

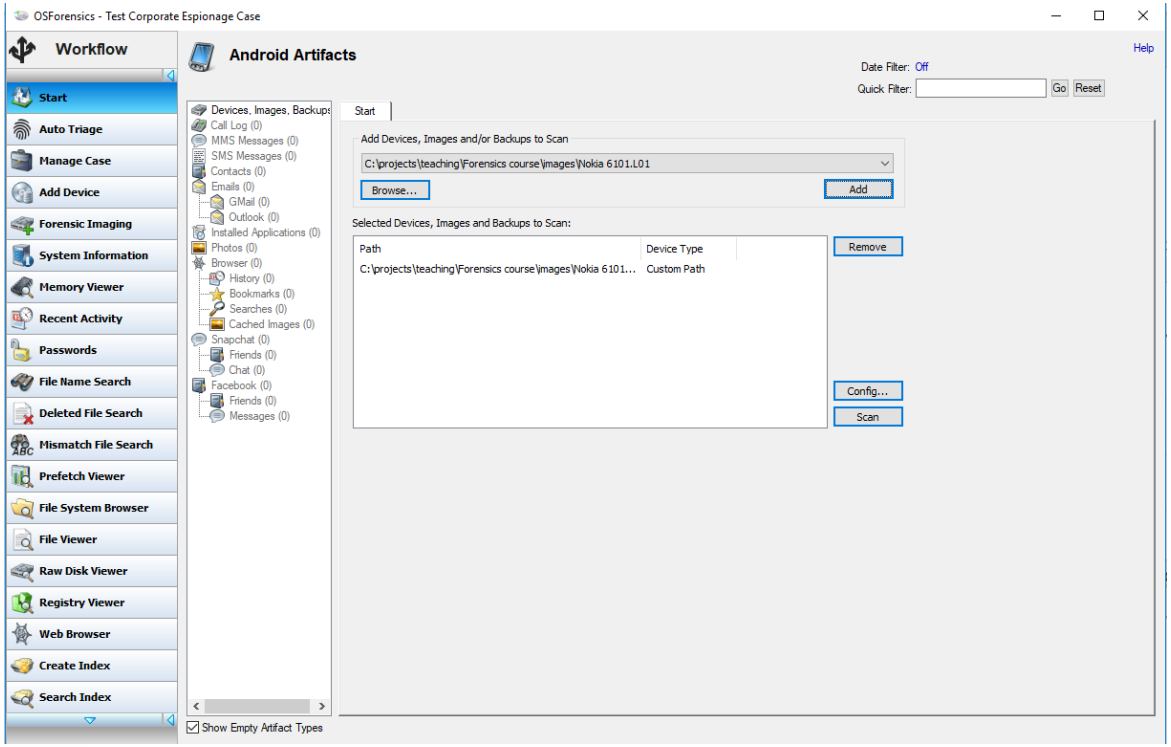
Android Artifacts

You can also scan Android images for artifacts.



Android Artifacts

OSForensics can extract quite a bit of data.



Android Artifacts

You can configure what you want to collect and analyze.