What's in Your Mobile Device?
Forensic Science in the Portable Digital Age
95% of corporate information is now digital

THE EVIDENCE IS IN ELECTRONIC FORM

“To say electronically stored information (ESI) is on the rise would be a glaring and obvious understatement. But it is also true. The fact is over 95% of corporate information is now digital and more ESI is created each 15 minutes than all written data penned from the beginning of time through the year 2004.

- Michael Swarz
Over Half of the World Population Uses a Cell Phone

Global Digital Snapshot
A Snapshot of the World's Key Digital Statistical Indicators

Total Population: 7.395 Billion
Internet Users: 3.419 Billion
Active Social Media Users: 2.307 Billion
Unique Mobile Users: 3.790 Billion
Active Mobile Social Users: 1.968 Billion

Urbanisation: 54%
Penetration: 46%
Penetration: 31%
Penetration: 51%
Penetration: 27%

Sources: Population: UN, US Census Bureau; Internet: ITU, Internet World Stats, CIA, national government ministries and industry associations; Social & Mobile Social: Facebook, Tencent, Viber, Snapchat, Twitter, LinkedIn, Nokian, VentureBeat, Niki Agilera; Mobile: GSMA Intelligence.
Mobile is on the Rise...

MOBILE’S SHARE OF WEB TRAFFIC
PERCENTAGE OF ALL GLOBAL WEB PAGES SERVED TO MOBILE PHONES IN JANUARY OF EACH YEAR

JAN 2016

2009: 0.7%
2010: 2.9%
2011: 6.1%
2012: 10.9%
2013: 17.0%
2014: 28.9%
2015: 33.4%
2016: 38.6%

Source: StatCounter, Q1 2016.
Cell Phone Forensics – Example Cases

Theft of Trade Secrets
• SMS recovered that undermined provided deposition testimony

Non-Compete / Non-Solicitation
• iPhone backup on PC containing thousands of SMS

Workplace Harassment
• Deleted SMS containing…things you shouldn’t send in a text
Step One – Super Exciting Paperwork

Chain of Custody = the record of what, who, when and where.

With phones, that typically means the make, model and IMEI (serial number) of the device combined with who had possession, who is taking possession, when and where are they taking possession.

This process usually also involves photographs of the device itself and an inventory of associated components (microSD card, cables, etc).
Step Two – Case Context

- Typically the phone should be put “offline” – no wireless signal of any kind, cell, Wi-Fi, Bluetooth, etc.
- If the wireless connections are not blocked, you run the risk of data loss in certain circumstances. Many modern phones are capable of receiving a wipe command.
- Specialized bags and equipment exist to assist with this quickly if the phone cannot be accessed (screen locked).
Step Two – Case Context

- Phone is not screen locked? May want to keep it that way.

- Does the make and model of phone use encryption? That may limit acquisition options.
Extraction Methods

- **Manual** – Scroll and Photo.

- **Logical** – Active data typically in predetermined report formats (html, pdf, etc) Think triage events.

- **File system** – a broader logical collection type (databases). Likely the most common extraction method.
Extraction Methods

- **Physical (Hex Dumping)** – upload modified boot loader into RAM for data extraction of the stored flash memory.

- **JTAG** – partial physical disassembly for hook up of probes. Requires device specific schematics and knowledge.

- **Chip Off** – physical removal of the chip for binary image acquisition. Device is essentially destroyed.
Common Cell Phone Data Types

- SMS (text message)
- MMS (text message with pic/video)
- Call Logs
- Email
- Contacts
- Pictures
- Videos
- Web History
- Notes
- Audio (voicemails)
- 3rd Party applications
- IM

Deleted Information
Data Storage - the Physical Layer

- Internal Memory (NAND / NOR Chips)
- External (SIM, MicroSD cards, etc)
Data Storage – Logical Layer 1

Common File Systems
- YAFFS (Android)
- HFSX (iDevice)
- Brew (Samsung, HTC, etc)

... more importantly SQLite databases
SQLite Databases – Your Final Destination

Think of a spreadsheet (like Excel) but just slightly more complex. Tables and rows of data.

Use of SQLite across applications makes data parsing easier.
Specialized equipment and software tools are used to extract the data from the source device. There is often more than one way to perform the “copy” process, depending on the needs of the case and technical considerations.
Many extraction tools today help the examiner out by automatically blocking write access to the source device *but not all do*. As the forensic expert, you need to know what the tool you are using is going to do.

If uncertain, test it on a spare device first!
If the examination involves uncommon data sources or new software, look beyond what is initially apparent.

A manual review of configuration files or other data may show other relevant content is available but just unknown to the tool at this time.
Tools – What Do They Really Do?

- Examination tools simply read and display data that has already been “understood” by a human. That human (or more likely team) then creates the logic that the software follows to interpret the data.
- Constant cat and mouse between phone operating system and app versions and the tool developers who reverse engineer them.
Data Not There?

- The device may have been backed up to a computer or the cloud.
- Don’t forget to check that extra storage (microSD).
- Call Detail Records may be available from the carrier (Verizon, AT&T, etc) that could provide some context of the use of the phone. *Will not include text message content.*
- Certain data types (email) are likely stored elsewhere and are more accessible from other sources than from the phone anyway.
Depending on the needs of the client, the report could be in many forms:

- Oral report, in person or on the phone
- Email summary with attachments
- Formal “letter” style
- Declaration or Affidavit
For Those Who Like to Dabble…

http://www.cfreds.nist.gov/

• Example cell phone data extractions. Multiple phones that make up a fake case.
• Free (stripped down) Examination Tool
CONTACT US:  

Brett Creasy  
Vice President & Director of Digital Forensics  

bit-x-bit, LLC  
437 Grant Street, Suite 1250  
Pittsburgh, Pennsylvania 15219  

412-325-4033  
info@bit-x-bit.com