FOCUSED ON THE FACTS

I.R.I.S. LLC

Information Retrieval Investigative Services

MOBILE DEVICE FORENSICS

Smart phones and other handheld electronics have become an important part of our everyday lives and the ever changing technology is making these devices a major source of digital evidence. Cell phones have evolved from simple telephones to powerful computing devices for internet browsing, GPS mapping, photo and video cameras, music players and can be used for banking and merchant payments.

Currently there are over 20,000 models of cell phones and smart phones operating on multiple networks and utilizing Apple iOS, Android, Windows Mobile, Blackberry and other proprietary operating systems.

Obtaining digital evidence from mobile devices can present many challenges in conducting forensically sound investigations in this constantly evolving field. Early identification of sources of evidence, not only from the device itself, but from other sources such as service providers, cloud sources and backup files can result in the successful preservation of key evidence.

Common Mobile Device Forensics Scenarios:

- In criminal cases
- Theft of intellectual property such as customer lists or trade secrets
- Preservation orders/e-Discovery
- Employment issues
- Fraud or embezzlement
- Divorce
- Loss of data

Best Practices & Industry Standards

The prevailing governing standards regarding digital evidence are set forth by The Scientific Working Group of Digital Evidence (SWGDE) and The National Institute of Justice (NIJ).

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

SCIENTIFIC WORKING GROUP FOR DIGITAL EVIDENCE
SWGDE

Principles of Digital Evidence

1. Investigation and analysis of digital evidence must be done in accordance with governing industry standards.
2. Actions taken to secure or analyze the digital evidence should not change the integrity of the evidence.
3. Persons conducting an examination of digital evidence should be trained for that purpose.
4. Activity relating to the seizure, examination, storage or transfer of digital evidence should be documented, preserved and available for review.

International Organization Standardization - ISO

ISO is an independent, non-governmental international organization that sets specifications for products, services and systems, to ensure that they follow statutory and regulatory requirements related to a product or program quality, safety and efficiency. Pursuant to the best practices and industry standards, the examination of digital evidence should be conducted in accordance with a quality management system such as ISO 17020 or 17025.

Data Integrity

Operating a cell phone or mobile device or accessing files on the device can change the metadata and change the evidence. Digital evidence should never be accessed as this can change data such as dates and times. Steps should be taken to ensure the integrity of the data acquired; this may include one or more of the following:

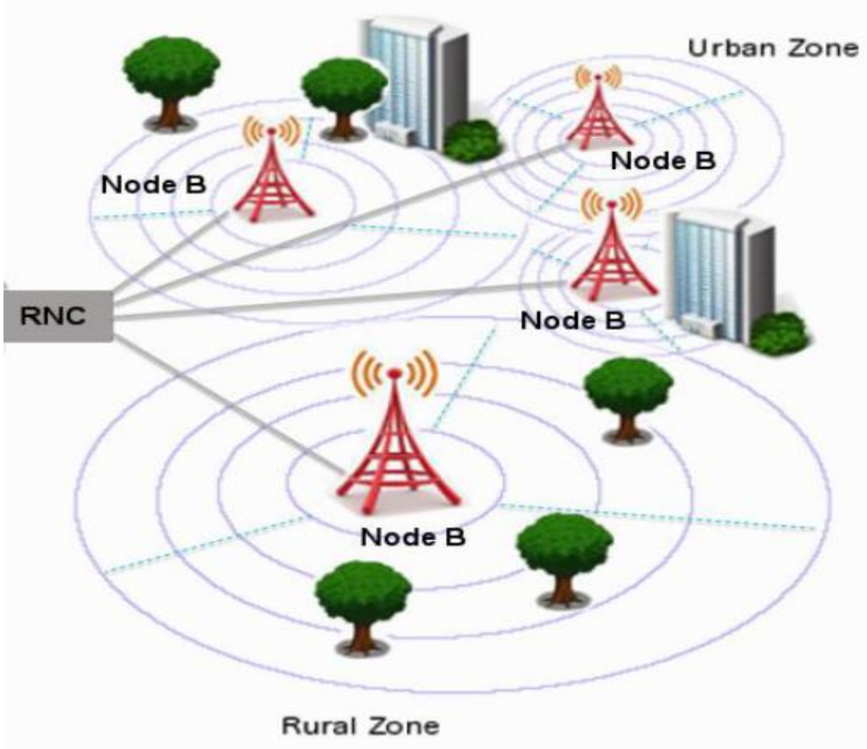
- Hash values (e.g., MD5, SHA-1 and SHA-256)
- Stored on read-only media (e.g., CD-R and DVD-R)
- Sealed in tamper-evident packaging

Training Levels

Mobile device examination training levels are dictated by Industry Standards and Best Practices which suggest examiners should be trained as discussed in *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.

Mobile Device Basics

Mobile devices are tablets, GPS units, cell phones and smart phones. Early personal digital assistants (PDA's) were handheld pocket-sized personal organizers for storing notes, contacts and calendar items and needed a physical connection to a computer to exchange data. PDA's were joined after the year 2000 by larger but otherwise similar tablet computers with Wi-Fi capabilities. Early cell phones were phones only capable of initiating or receiving telephone calls on a cellar network and were powered by a car plug or a battery pack.



The cellular network consists of cell sites, which are antennas which transmit and receive the two-way communication signals from the device. If a device user is moving, the communication is maintained by the device switching to other cell sites in the network.

Although basic cell phones are still available, current mobile devices are typically a small computing device. These have an operating system capable of running mobile applications and may provide a diverse range of functions. Many such devices can connect to the Internet and interconnect with other devices such as car entertainment systems or headsets via Wi-Fi, Bluetooth or near field communication (NFC). Integrated cameras, digital media players, cellular phone and GPS capabilities are common. Power is typically provided by an internal rechargeable battery. Today's mobile devices often contain sensors such as accelerometers, compasses, magnetometers and gyroscopes allowing detection of orientation and motion. Mobile devices may provide biometric user authentication such as face recognition or fingerprint recognition.

Mobile Device Memory Type

Mobile devices store data in electronic circuits known as flash memory. Most computers use hard drives that use magnetic memory, although some newer higher end computers use flash memory in solid state drives. Unlike magnetic memory found in most computer systems, flash memory will actively erase data that has been deleted to make space for new data.

Data Recovery

Flash memory must first erase the old data by resetting the entire allocation unit area to be reused to binary “zeros.” When a file is deleted, the space occupied by the deleted data is marked as available for reuse. At some point, the operating system will “clean up” deleted data on the solid state drive making it ready to be re-written to. Until then, the data may remain intact and can often be recovered by forensic techniques.

Complete or partial data from a deleted file may still exist within a database file and be recovered.

Much of the user data on mobile devices is stored in database files (similar to an Excel spreadsheet). A user could have hundreds of text messages currently on the device, which are stored in the database. If the user deletes one or more of the messages, the deleted message(s) remain in the database, but it is marked deleted and the device does not display the message. With most forensic extractions, these deleted messages are fully recoverable.

When the size of the database grows, the operating system will check if there is deleted information stored in the database. If the size of the file can be reduced, the database will be copied without the deleted data to “clean” allocation units. The original database may remain until the operating system cleans up the allocation units used by the original database file. Data from the original database may be partially or fully recovered.

Rapid Assessment and Preservation

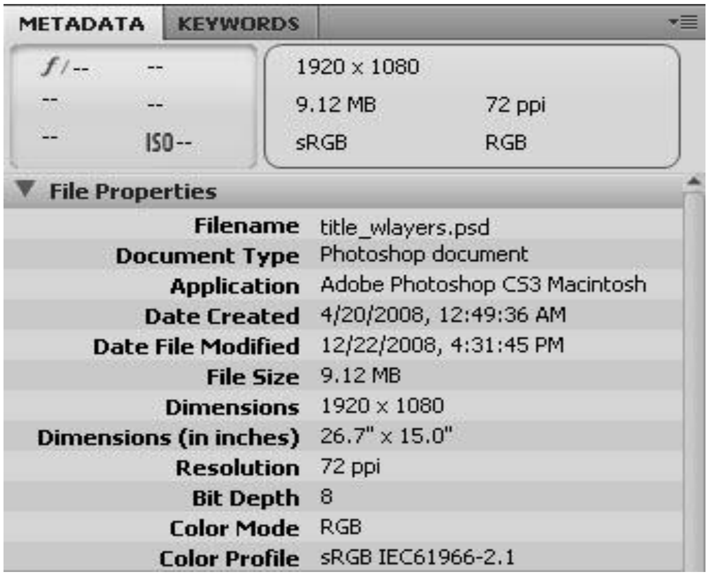
On a solid state drive, the operating system will periodically erase deleted data on its own, making recovery impossible. New data received, such as incoming text messages or e-mails, may also cause old data to be lost. When the device is powered on but idle, the operating system may use the idle time to clean allocation units for reuse and copy database files to purge them of deleted data. The best practices require rapid assessment, proper handling and preservation to prevent the permanent loss of data.

Backed Up Files

A backup of a mobile device can sometimes provide significant information that was on the device. In the event the mobile device such as a cell phone is no longer available, the next option would be to determine if a backup copy exists either on a host computer or on the cloud.

Metadata

Files and programs have unique identifying information such as created date, modified date accessed dates also called metadata. Metadata is the data that describes data.



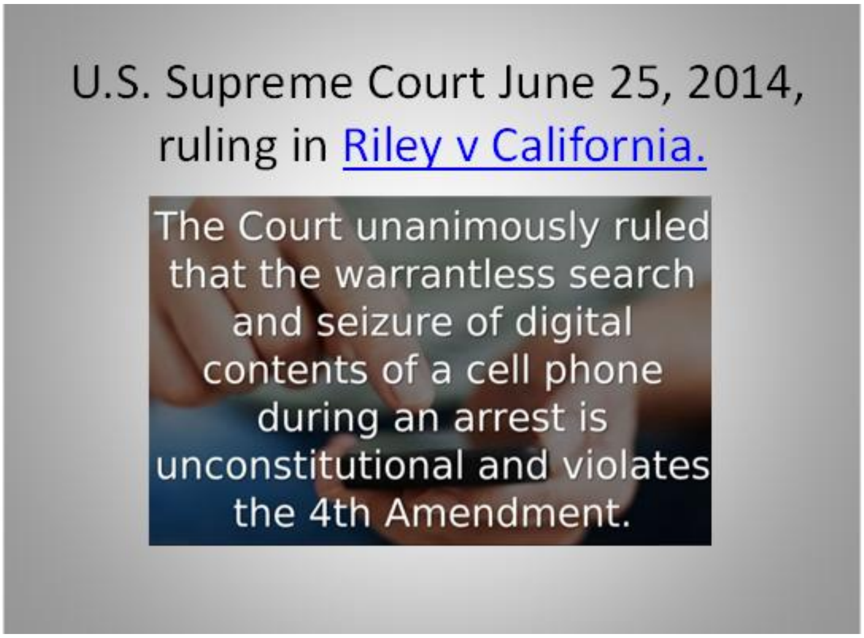
f/-- --
-- --
-- ISO--

1920 x 1080
9.12 MB 72 ppi
sRGB RGB

File Properties

Filename	title_wlayers.psd
Document Type	Photoshop document
Application	Adobe Photoshop CS3 Macintosh
Date Created	4/20/2008, 12:49:36 AM
Date File Modified	12/22/2008, 4:31:45 PM
File Size	9.12 MB
Dimensions	1920 x 1080
Dimensions (in inches)	26.7" x 15.0"
Resolution	72 ppi
Bit Depth	8
Color Mode	RGB
Color Profile	sRGB IEC61966-2.1

Consent to Search



U.S. Supreme Court June 25, 2014, ruling in Riley v California.

The Court unanimously ruled that the warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional and violates the 4th Amendment.

Types of Data from Mobile Devices

- Device users, settings, languages and time zone information
- Contacts
- Multi-media (photos, videos or audio files)
- Location data: GPS and Cell networks
- E-mail

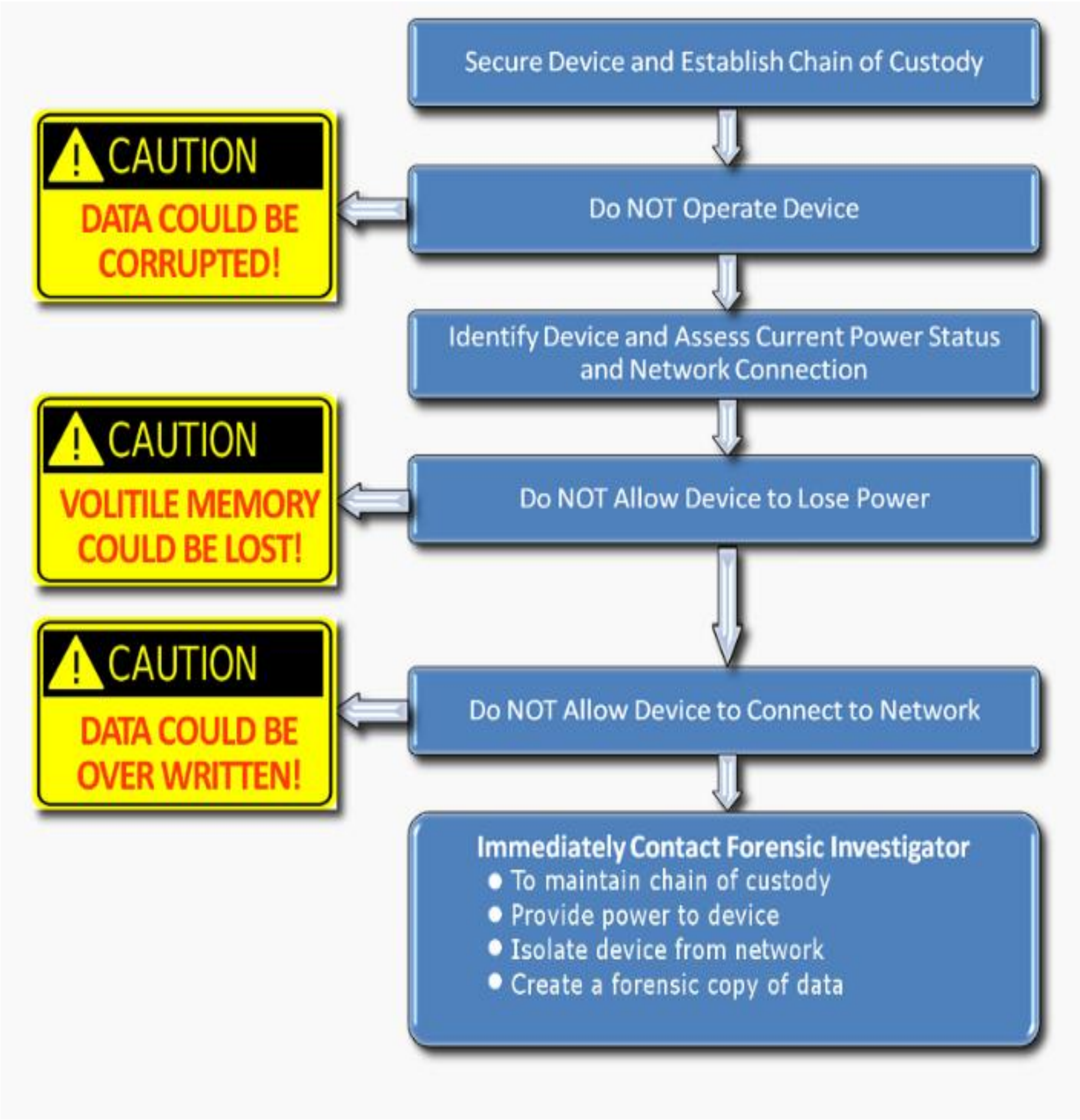
- Calendar
- MMS (Multimedia Message Service) and SMS (Short Message Service) text messages
- Internet browsing history (searches, sites visited, typed addresses)
- Installed Applications and app file system data
- Deleted files and programs
- Encrypted files and folders
- Social networking data
- Mobile device backup information (tethering information)
- Financial records
- File metadata
- Wi-Fi networks
- Connected Bluetooth devices

Evidence Seizure

If a mobile device is on, a person without proper training should not attempt to search the device. The contents displayed on the screen may be photographed and the following information recorded:

- Information from mobile phone user to determine the phone number, service provider, passcodes, pattern locks or PINs.
- Obtain charger/cables and user manual if available.
- If the phone is unable to be processed immediately, turn off the phone, remove the battery if practical and do not turn it back on.
    - The benefits of turning off the phone include:
        - Preserving call logs and last cell site location information (LOCI).
        - Preventing overwriting deleted data.
        - Preventing data destruction signals from reaching the mobile phone.
        - Preventing improper mobile phone handling (i.e., placing calls, sending messages, taking photos or deleting files).
    - The risks of turning off the mobile phone include possibly engaging authentication mechanisms (e.g., passwords, PINs, etc). An urgent need or demand may dictate that the mobile phone remains on for immediate processing. If the mobile phone must be left on, isolate it from its network while maintaining power.
        - Radio Frequency (RF) shielding - Mobile phones communicate with cell sites. Allowing this communication will change data on the phone.
        - Many mobile phones can be placed in "Airplane" mode limiting access to cell sites (e.g., 911 calls still available). This requires user input on the handset.
        - Disable Wi-Fi, Bluetooth, RFID and IrDA communications if practical

Rapid Assessment Guide for Cell Phone Evidence Preservation


Secure Device and Establish Chain of Custody
CAUTION
DATA COULD BE CORRUPTED!
Do NOT Operate Device
Identify Device and Assess Current Power Status and Network Connection
CAUTION
VOLITILE MEMORY COULD BE LOST!
Do NOT Allow Device to Lose Power
CAUTION
DATA COULD BE OVER WRITTEN!
Do NOT Allow Device to Connect to Network
Immediately Contact Forensic Investigator
● To maintain chain of custody
● Provide power to device
● Isolate device from network
● Create a forensic copy of data

Evidence Packaging & Transport

Each piece of evidence should be protected from damage or alteration, labeled and a chain-of-custody maintained as determined by organizational policy. Specific care should be taken with the transportation of digital evidence to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variations of temperature and/or humidity. Plastic bags other than specific anti-static bags should not be used due to static electricity. Paper bags or envelopes can be used and sealed and labeled.

Forensic Data Acquisition

The first step for investigation of digital evidence begins with the preservation of evidence through the forensic acquisition process. The forensic acquisition process is to create a verified forensic copy of the electronic data to be examined. Methods of acquiring evidence should be forensically sound and verifiable; method deviations shall be documented.

Acquisition Types

NIST has defined the mobile device tool classifications system as follows:

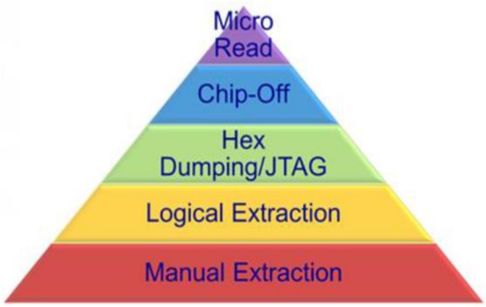


Figure 6: Mobile Device Tool Classification System

- **Micro Read** – Highest level of forensic examination, where the device memory chip is shaved in extremely thin layers and the data is read bit by bit from the source using an electron microscope or other device. It is extremely technical, and would only be used after all other means had been exhausted.
- **Physical or Hex Dump** – The most comprehensive and forensically sound process. A complete copy of the device physical memory is obtained. Not all devices are supported for physical extraction and the strong encryption used by some devices prevents the data from being of value.
- **JTAG** (Joint Test Access Group) – A physical extraction process where data is read by connection made directly to the device memory chip. Used in some cases where the device is damaged, or on some pre-paid "burner" phones that do not have an active data port.
- **File System** – This method obtains the user data and database files from the device and can recover some deleted data.
- **Logical** – This is the simplest forensic extraction which obtains the user data that is available by the device user.
- **Manual** – This involves operating and searching the device by hand and photographing the display. This could result in accidental deletion of data, and would change metadata such as an unread message to read.

Acquisition Documentation should include

- Examiner’s name.
- Acquisition date.
- Acquisition details (e.g., type of acquisition, imaging tool and version number).
- Physical condition of the evidence and unique identifiers (e.g., serial number, description, make and model, phone number).
- Original and verification hash values.
- Photographs and/or sketches.
- Any additional documentation as required by the examiner’s organization.

Examination Documentation

The secondary objective is to conduct forensic examination and searching for evidence. Examination documentation should be case specific and contain sufficient details to allow another forensic examiner, competent in the same area of expertise, to identify what was done and to replicate the findings independently.

Report of Finding

- Information should be presented in a format that may be read and understood by non-technical individuals.
- Examiners should be able to explain all information contained within the report.
- Should include any relevant information contained within the acquisition and/or evidence handling documentation.
- Reports issued by the examiner should address the requestor’s needs.
- Document the scope and/or purpose of the examination.
- Give a detailed description of the media examined (e.g., hard disk, optical media or flash drive).
- Include any supplemental reports related to the examination.
- Provide the examiner’s name and date of exam.
- Be reviewed according to organizational policy.

Language for Motion for Discovery of Mobile Device Evidence

(When dealing with digital evidence from a mobile device that has been preserved and examined by law enforcement, industry standards recommend that a full report and copy of the original; extraction file and proprietary file viewer be requested.)

1. All reports including search warrant or consent, and reports regarding the seizure and the chain of custody of the evidence.
2. Full forensic extraction report in PDF format.
3. A copy of the extraction file in the native (original) format of the forensic device or software used to conduct the extraction.
4. The proprietary file viewer for the specific forensic tool used to create the extraction.
5. The forensic examiners report detailing the tools and all procedures used to examine the mobile device.

Digital Evidence Toolbox

Call detail and Cell-site records are the billing records cellular service providers use to keep track of their customers' calls and cellular data usage. They show the date and time of all calls made or received, the numbers called, the duration of each call, and the cell sites used to begin and end a call. For more information regarding call detail records and mobile device location information, see the Digital Evidence Toolbox sections:

- ***Call Detail/Cell-Site***
- ***Location Data***

References

NIST Guidelines on Mobile Device Forensics 05-2014
SWGDE Best Practices for Collection of Damaged Mobile Devices 020816
SWGDE Best Practices for Examining Magnetic Card Readers 092915
SWGDE Best Practices for Mobile Phone Forensics 021113
SWGDE Best Practices for Portable GPS Device Examinations 091212
SWGDE Core Competencies for Mobile Phone Forensics 021113
SWGDE Best Practices for Vehicle Infotainment and Telematics Systems 062316

For more information on mobile devices, digital forensics and digital evidence, call now and speak with a certified expert. I.R.I.S. LLC is available 24 hours in emergency cases.

WE'RE CERTIFIED.