OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Digital Forensics

Week 11 – Mobile Forensics

Date: Friday 28th November 2025

Course Code: TU856 TU857 TU858 (Full-Time)

TU Dublin – Grangegorman Campus

School of Computer Science

Seoladh Cláraithe / Registered Address
OT Baile Átha Cliath - Teach na Páirce Ghráinseach Ghormáin
191 An Cuarbhóthar Thuaidh, D07 EWV4, Éire

TU Dublin - Park House Grangegorman
191 North Circular Road, D07 EWV4, Ireland

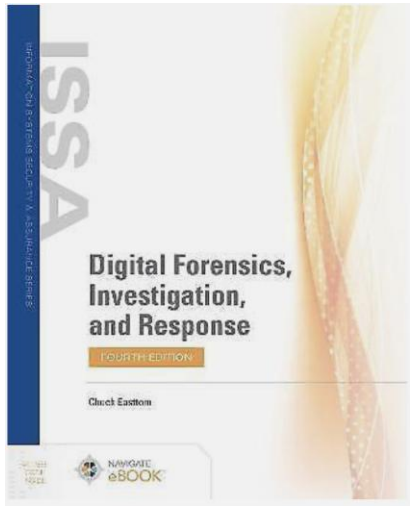
OT Baile Átha Cliath
Gráinseach Ghormáin
D07 H6K8, Éire

TU Dublin
Grangegorman
D07 H6K8, Ireland

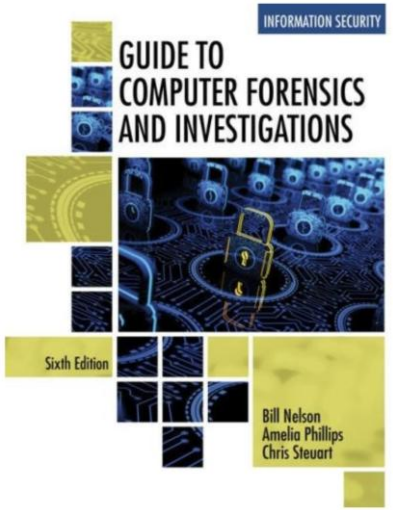
~ +353 1 220500
~ tudublin.ie

Overview

- General Mobile Forensics
- Acquisition Procedures
- SWGDE Guidelines
- NIST Generic States
- Tools Demo



Book reference: Chapter 12



Book reference: Chapter 12

Introduction

- Mobile forensics is focused on recovering, analyzing, and preserving digital evidence from mobile devices.
- It involves using specialized techniques and tools to extract data stored on or transmitted through mobile phones, smartphones, tablets, and other portable devices while ensuring the integrity of the evidence.
- The standard forensics investigative process should be followed.

General Device Information

- Call information
- Messaging
- Instant Messaging logs
- E-mail accounts
- Web pages
- Photos, Videos, Music
- Calendars
- Address books
- Social Media accounts
- GPS data
- Voicemail / voice recordings
- Bank Account details
- Etc…

NIST Guidelines (just for reference)

NIST Special Publication 800-101
Revision 1

Guidelines on Mobile Device Forensics

Rick Ayers
Sam Brothers
Wayne Jansen

"Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics. This guide attempts to bridge the gap by providing an in-depth look into mobile devices and explaining technologies involved and their relationship to forensic procedures. This document covers mobile devices with features beyond simple voice communication and text messaging capabilities. This guide also discusses procedures for the validation, preservation, acquisition, examination, analysis, and reporting of digital information."

Source:
https://www.nist.gov/publications/guidelines-mobile-device-forensics
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Cellular Device Concepts

- To conduct a mobile forensics investigation it is really important to understand the technology of cell phones and other associated devices.
- The field of mobile forensics changes rapidly and poses challenges in retrieving information.
- We will look at some of the essential concepts and technologies used in mobile devices.

Mobile Switching Center (MSC)

- A Mobile Switching Center (MSC) is a critical component in a cellular network responsible for managing mobile communications, routing calls, and ensuring seamless connectivity as users move between different coverage areas. It acts as a central hub for controlling and coordinating various network elements in a mobile communication system.
- If we need access to this data we will need a warrant (criminal case).

Base Transceiver Station (BTS)

- A Base Transceiver Station (BTS) is a critical component of a cellular network that enables wireless communication between mobile devices (such as smartphones) and the network infrastructure. It is essentially the hardware that provides the radio interface for communication with user devices in a specific geographic area, commonly referred to as a cell or cell phone tower.
- A Base Station Controller (BSC) is a combination of hardware and software to manage BTSs and will assign channels by connecting to the mobile switching center.

Mobile Device Characteristics

- “They house a **microprocessor**, read only memory (**ROM**), random access memory (**RAM**), a **radio module**, a digital **signal processor**, a **microphone and speaker**, a variety of hardware keys and interfaces and a liquid crystal display (**LCD**). The **operating system (OS)** of a mobile device may be stored in either NAND or NOR memory while code execution typically occurs in RAM”
- Most have a proprietary OS (Windows Mobile, RIM OS, Android, Google OS, iOS)
- Generally phones store data in electronically erasable programmable read-only memory (EEPROM)
- Mobile phones store their operating system (OS) in non-volatile memory (ROMs), typically in specific types of flash memory chips embedded within the device. These storage locations are designed to retain data even when the device is powered off.

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (page 13)

SIM Cards

- SIM card (Subscriber Identity Module)
- securely store information that identifies and authenticates a subscriber on a cellular network
- Connects the device to the mobile carrier’s network.
- Stores security keys for network authentication.
- Allows users to switch devices while retaining the same subscription.

Acquisition Procedures

- Based on SANS DFIR (Digital Forensics Incident Response)
- 3 scenarios
  - Device is on and unlocked
  - Device is on and locked
  - Device is off

- Source:
  - https://smarterforensics.com/2014/06/getting-the-most-out-of-smartphone-forensic-exams-sans-advanced-smartphone-forensics-poster-release/
- Clearer view of the diagrams:
  - https://bestitdocuments.com/Samples/Smartphone_Forensics_Poster.pdf

Device is on and unlocked

- Isolate the device from the network if possible
  - Disable WiFi and Hotspots
  - Set Airplane mode
  - SIM ID cloning
- Take the necessary steps to ensure physical device access is possible
  - Remove passcode
  - Enable USB debugging
  - Enable “Stay Awake” option
  - Disable timed screen lock features

- Physical Acquisitions
  - Acquire supporting media
  - SIM card(s)
  - Media cards
  - Check associated media for device backups
- Logical Acquisitions
  - Logical/file system acquisitions
  - Device backup

Device is on and locked

- Physical access requires that USB debugging mode is enabled. Forensic tools will use custom bootloaders to bypass the passcode if applicable.
- Acquire supporting media
  - SIM card(s)
  - Media card(s)
- Check associated computers and media for device backups
  - Computer and media cards

Device is off

- Attempt physical acquisition while turned off
- Turn on and try steps for:
  - **Device is on and unlocked or**
  - **Device is on and locked**

Analysis (back in the lab)

- First need to assess what can be retrieved.
- Need to determine whether to perform a physical or logical acquisition
- Physical acquisition
  - involves creating a complete, bit-by-bit copy of the device's entire storage, including unallocated space. This method captures **all data**, whether it is visible, hidden, or deleted.
- Logical acquisition
  - involves extracting specific, accessible data through the device's operating system and APIs (Application Programming Interfaces). It focuses on **active user data** rather than raw storage.

When to Use Each Method

- **Physical Acquisition**:
  - When deleted, hidden, or encrypted data needs to be recovered.
  - For deep forensic investigations requiring raw data.
  - When logical acquisition is insufficient or restricted (e.g., locked devices).
- **Logical Acquisition**:
  - For quick and non-invasive data extraction.
  - When the target data is user-accessible.
  - In cases with legal or technical constraints on deeper access.

Analysis

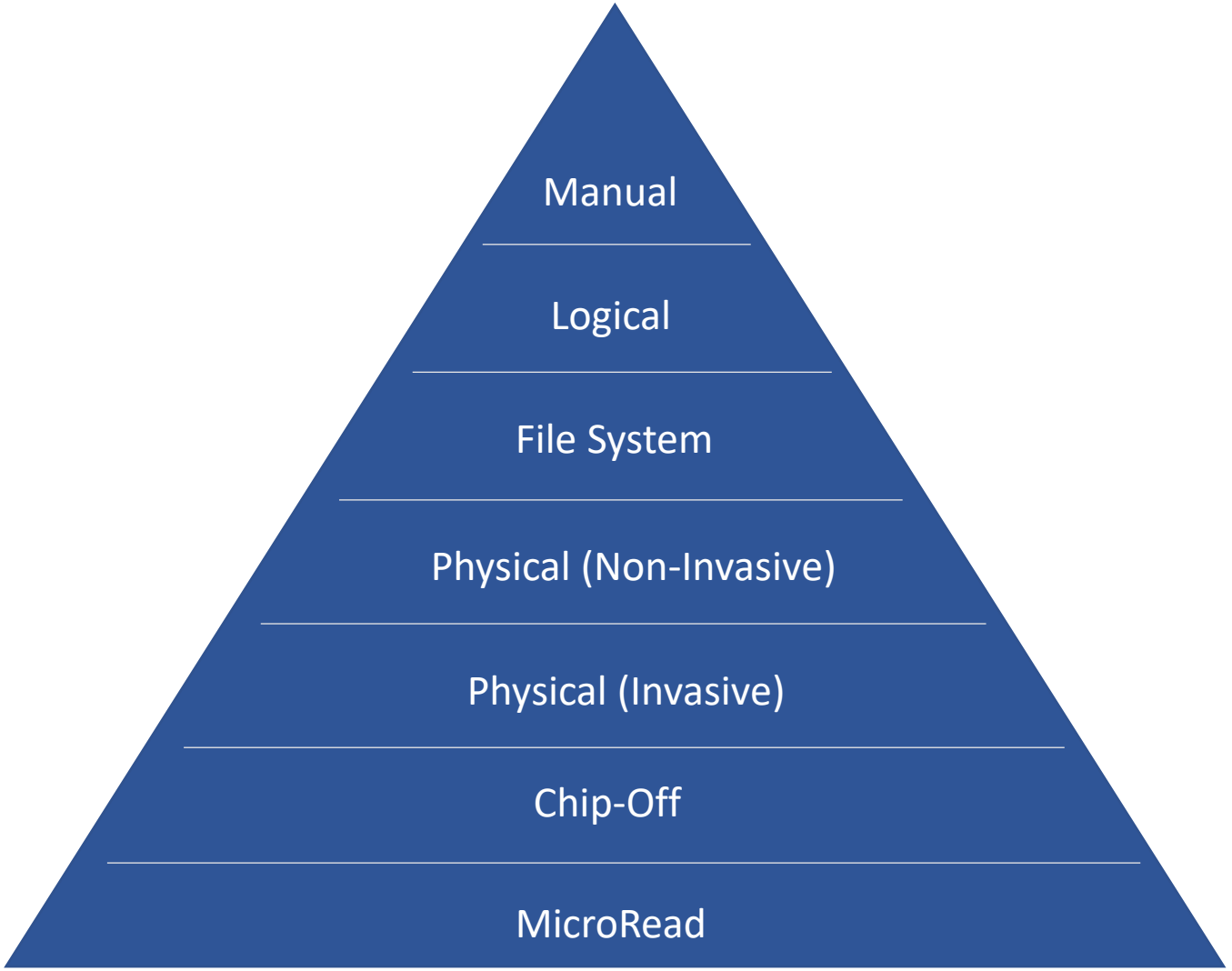
- Check the following locations for information
  - Internal Memory
  - SIM card
  - Removable or external memory cards
  - Network provider

SWGDE Guidelines

- **SWGDE (Scientific Working Group on Digital Evidence)**
- Offers guidelines for mobile forensics provide recommendations and best practices for the forensic examination of mobile devices.
- For Data Acquisition the SWGDE describe the Mobile Forensics Pyramid.
  - The level of extraction and analysis required depends on therequest and the specifics of the investigation. Higher levels require a more comprehensive examination, additional skills and may not be applicable or possible for every phone or situation

Source: https://www.swgde.org/wp-content/uploads/2023/11/2013-02-11-SWGDE-Best-Practices-for-Mobile-Phone-Forensics_V2-0_Final.pdf

Mobile Forensics Pyramid (SWGDE)



Manual Examination (Base Layer)

- **Description:**
  - The simplest form of data access, involving direct interaction with the device's user interface.
- **Methods:**
  - Navigating the device's menus and applications to capture visible data.
  - Taking screenshots or photographs of on-screen information.
- **Challenges:**
  - Time-consuming and prone to human error.
  - Limited to what the examiner can manually see or access without credentials.
  - Data Examples: Contacts, call logs, SMS/MMS messages, photos, app data (if unlocked).

Logical Acquisition

SWGDE Pyramid

- **Description:**
  - Extracting accessible files and data from the device using forensic tools and APIs provided by the device's operating system.
- **Methods:**
  - Tools like Cellebrite, Oxygen Forensics, or Magnet AXIOM are used to access logical partitions of the device.
  - No need for bypassing encryption or deep system access.
- **Challenges:**
  - Limited to unencrypted and non-deleted data.
  - Some apps or operating system restrictions may prevent full access.
  - Data Examples: User data like messages, call logs, app data, photos, and videos stored on the device.

File System Acquisition

SWGDE Pyramid

- **Description:**
  - Provides access to the device's file system, offering deeper visibility into stored data and metadata.
- **Methods:**
  - Accessing files, directories, and the structure of the device’s operating system.
  - Forensic tools that support file system extraction (e.g., rooted Android devices, jailbroken iOS).
- **Challenges:**
  - May require bypassing certain permissions or protections.
  - Requires technical expertise to analyze extracted data.
  - Data Examples: Metadata, app databases, hidden files, and partially deleted data.

Physical Acquisition (Non-Invasive)

SWGDE Pyramid

- **Description:**
  - A process that provides physical acquisition of a phone's data without requiring opening the case of the phone. The most thorough method, involving bit-by-bit copying of the entire physical memory of the device.
- **Methods:**
  - Dumping the memory using chip-off techniques, JTAG, or forensic tools.
  - Accessing flash memory and extracting all stored data, even deleted content.
- **Challenges:**
  - Complex, time-consuming, and may require specialized equipment.
  - Device encryption (e.g., Full Disk Encryption on iOS/Android) can prevent access to usable data.
  - Data Examples: Entire raw memory content, deleted data, unallocated space, and encrypted files.

Physical Acquisition (Invasive)

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TECHNOLOGICAL UNIVERSITY DUBLIN

SWGDE Pyramid

- **Description:**
  - A process that provides physical acquisition of a phone's data requiring disassembly of the phone providing access to the circuit board. (e.g., JTAG). The most thorough method, involving bit-by-bit copying of the entire physical memory of the device.
- **Methods:**
  - JTAG (Joint Test Action Group):
  - Utilizes debugging ports on the device's motherboard to directly access and extract data from memory.
  - A non-destructive invasive method, as the chip is not removed.
  - Requires a thorough understanding of the device's board layout.
- **Challenges:**
  - Device Damage Risk
  - invasive methods involve dismantling and desoldering, which can permanently damage the device.
  - Complex, time-consuming, and may require specialized equipment.

Chip-Off

SWGDE Pyramid

- **Description**
  - Chip-Off forensics involves physically removing the memory chip from the device's motherboard and using specialized equipment to read its raw data.
- **Methods**
  - This method provides direct access to the entire memory, including active data, deleted files, and unallocated space.
- **Challenges**

  Risk of Physical Damage:
  - The desoldering process can damage the memory chip or the motherboard if not handled with precision.
  - Excessive heat or improper handling can corrupt or destroy data.

MicroRead

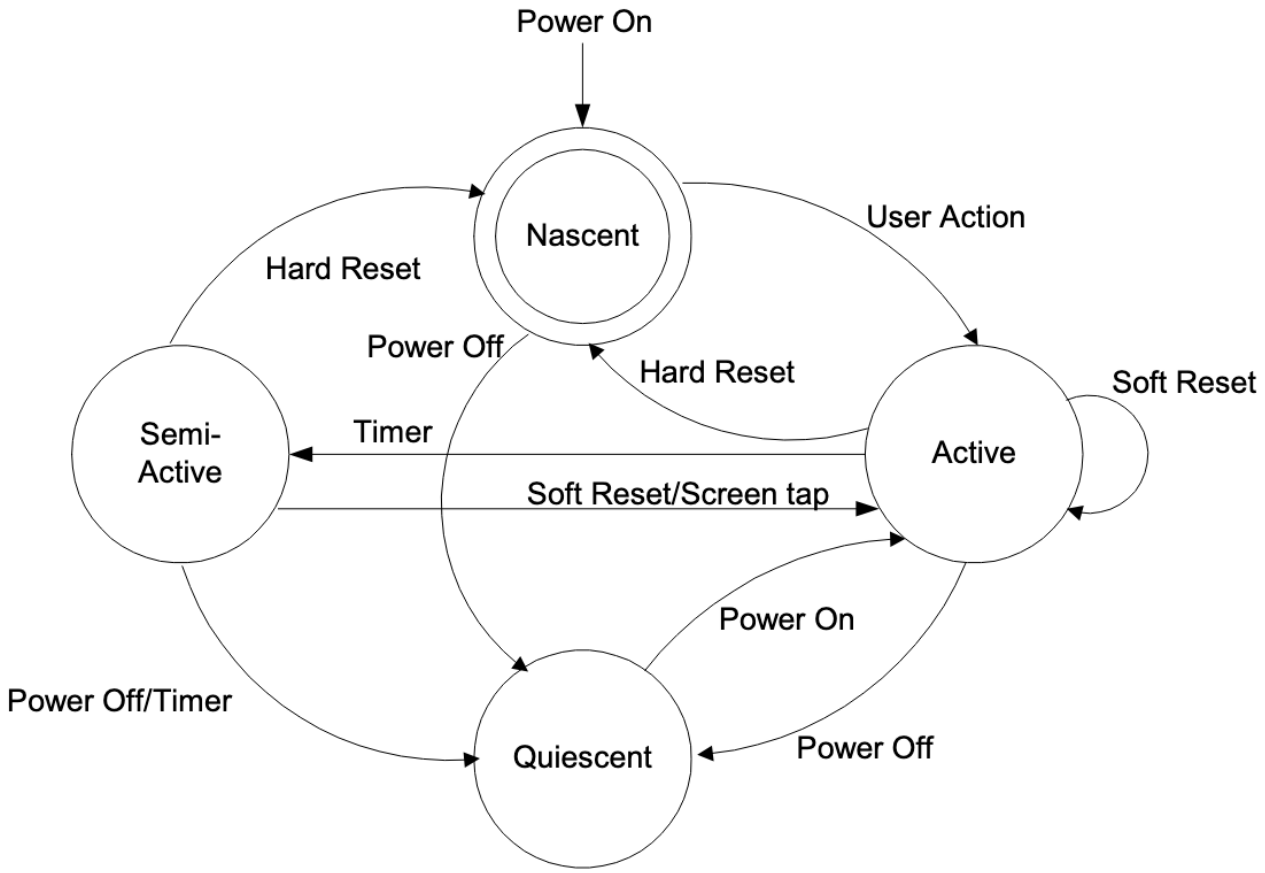
SWGDE Pyramid

- **Description**
  - MicroRead Forensics is a highly advanced and niche forensic technique that involves using a high-powered microscope to physically analyze and interpret the memory cells of a device's storage chip.
- **Methods**
  - A high-powered microscope, such as a scanning electron microscope (SEM) or an optical microscope, is used to capture images of the memory cells.
  - Memory cells in NAND or NOR flash storage represent binary data through physical differences
  - The images of the memory cells are analyzed to identify the state of each cell, translating them into binary (0s and 1s).
- **Challenges**
  - Highly complex with very specialized equipment
  - Last resort option

Generic States

- The **National Institute of Standards and Technology (NIST)** offers **guidelines on four different states a mobile device can be** in when you **extract data.**
- For a standard PC it is either an “on” or “off” state.
- Further amplification is needed, particularly for PDAs, whose behaviour is more complex.
- The following diagram offers a high-level of the various states in which a mobile device can be at any time, along with the transitions that can occur to cause a change of state.

Generic States (Diagram)



Source: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-72.pdf

Nascent State

NIST SP 800-72 – Generic States

- **Description:**
  - Represents the state of the device when it is newly powered on or has been reset to its factory settings.
  - The device contains minimal data (such as the operating system and pre-installed applications) and is not configured with user data or settings.
- **Characteristics:**
  - No user data is present, as the device is in its default condition.
  - Memory usage is limited to system files and applications necessary for basic operation.
  - Forensics in this state focuses on extracting system-level information or validating device integrity.
- **Forensic Implications:**
  - Limited evidence may be available.
  - Useful for understanding the base configuration of the device or confirming the absence of user-specific data.

Source: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-72.pdf

Active State

NIST SP 800-72 – Generic States

- **Description:**
  - This is the fully operational state where the device is powered on, configured, and actively being used by the user.
  - The device has access to all its functionalities, including applications, communication, and data storage.
- **Characteristics:**
  - Contains volatile and non-volatile data such as user files, installed applications, running processes, logs, and cached information.
  - Connections to external networks (e.g., Wi-Fi, cellular, or Bluetooth) may be active.
  - Battery power or external power is required to maintain this state.
- **Forensic Implications:**
  - Maximum data is accessible, including volatile data (e.g., RAM contents, active network connections).
  - Volatile data must be acquired immediately, as powering down the device or changes in usage can lead to data loss.
  - Tools that interact with the operating system can extract logical and file system data efficiently.

Source: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-72.pdf

Quiescent State

NIST SP 800-72 – Generic States

- **Description:**
  - The device is powered on but is not actively being used by the user. It is in a standby or idle mode, conserving power while maintaining a low level of activity.
- **Characteristics:**
  - Volatile data, such as running processes and RAM contents, is still present but may be limited compared to the Active State.
  - Applications may be paused, and network connections may be suspended or restricted to essential services.
  - Non-volatile data remains unchanged and accessible.
- **Forensic Implications:**
  - Volatile data can still be acquired, but it may not reflect active user activity.
  - Data acquisition in this state should prioritize capturing both volatile and non-volatile data before any changes occur (e.g., a power-off event or system sleep).

Source: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-72.pdf

Semi-Active State

NIST SP 800-72 – Generic States

- **Description:**
  - A transitional state where the device is partially powered or experiencing limited activity due to low power or other interruptions. For example, the device may be in a low-power sleep mode or disconnected from external inputs.
- **Characteristics:**
  - Volatile data is at high risk of being lost, as the device may have partially powered down or stopped refreshing memory.
  - Non-volatile data remains intact and can be accessed if proper tools are available.
- **Forensic Implications:**
  - Critical data in volatile memory (e.g., active processes or temporary files) may already be lost or inaccessible.
  - Focus should shift to recovering persistent (non-volatile) data, such as stored files, logs, and system configurations.
  - Special care is needed to preserve device state and avoid further data loss.

Source: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-72.pdf

Android Debugging Bridge

- The **Android Debug Bridge (ADB)** is a versatile command-line tool that allows communication between a computer and an Android device. ADB is part of the Android Software Development Kit (SDK) and is widely used for debugging, development, and forensic purposes. It enables users to execute commands on an Android device from a computer, access files, and obtain system-level data.

Key features of ADB

- Command Execution
- File Transfer
- App Management
- Debugging and Logs
- Root Access (if available)
- Backup and Restore

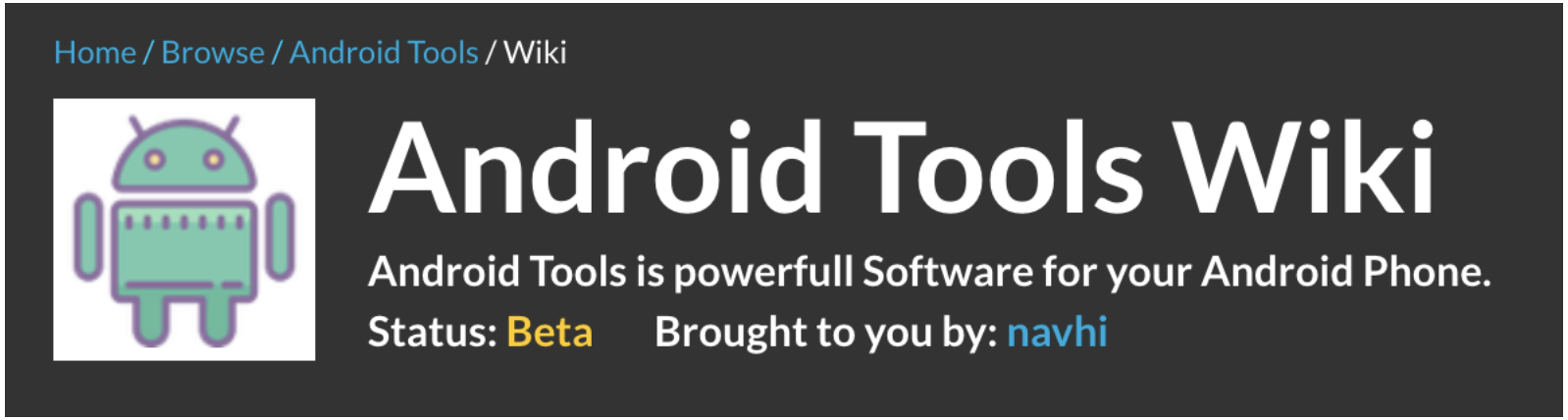
How it works

- **Connection Setup:**
  - ADB requires a USB connection or wireless access over a local network.
  - The device must have Developer Options enabled and USB Debugging activated.
- **Components:**
  - ADB Client: Runs on the host computer (e.g., through a terminal or command prompt).
  - ADB Daemon (adbd): Runs on the Android device, listening for ADB commands.
  - ADB Server: Handles communication between the client and the daemon.
- **Workflow:**
  - Once connected, the host computer sends commands to the ADB daemon running on the Android device.
  - The daemon executes the commands and sends responses back to the computer.

Andriller

- **Andriller** is a forensic software toolkit designed for analyzing Android devices. It focuses on extracting, decoding, and reporting data from Android smartphones and tablets. Andriller is widely used in digital forensic investigations due to its simplicity, effectiveness, and ability to extract critical data from devices. It supports various types of logical acquisition, data decoding, and reporting, making it a valuable tool for forensic analysts.

Android Tools



- https://sourceforge.net/p/android-tools/wiki/Home/

Questions