NIST Mobile Forensics Workshop and Webcast
Mobile Device Forensics: A – Z

Disclaimer:

Certain commercial entities, equipment, or materials may be identified in this presentation. Such identification is not intended to imply recommendation nor endorsement by myself nor my employer, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

I have NO financial nor commercial interest in any of the products I will be discussing today!
Mobile Forensic Tool Classification

- Micro Read
- Chip-Off
- Hex Dumping/JTAG
- Logical Extraction
- Manual Extraction

How Mobile Forensic Tools Actually Work…

1. The broken tool story…

2. Proposed Changes…

3. Tool Leveling System
But first, the broken tool story…

The broken tool story…

- Purchased tool “X” from company Y.
- 8PM on Saturday evening… I hit the “get data button” and then…
Windows

A fatal exception OE has occurred at 0020:0001E36 in VXD UMM(01) + 0001E36. The current application will be terminated.

- Press any key to terminate the current application.
- Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue _

Options:

A. Email encrypted debug logs to company Y support for analysis

B. Try different combinations till it works

C. Try another tool

D. Quit and become a pro card counter

E. Figure out why the tool is broken myself!
And I…

- I took the road less traveled…

A methodical approach:

- Wearing my “Malware Analysis” hat…
- I read* that running PortMon for Windows would allow a “diagnostic view” of the data.
- Voila!
NOTE:

- This idea came from:
  - NIST Special Publication: 800-101 “Guidelines on Cell Phone Forensics”
  - Serial Sniffing:
    - PortMon (Now called: “Process Monitor”)
  - USB Sniffing:
    - USB Monitor
    - (http://www.hhdsoftware.com)

Tweaking portmon’s settings:

- Select ONLY the port you want to capture
  - Capture | Ports | <Your Port>
- Change Max Output Bytes to 2048
  - Edit | Max Output Bytes | 2048 | Apply
Things that make you go hmm.....

- You can use this to:
  - Compare different tools
  - How protocols work.
  - Application error checking.
  - See what data is NOT reported to you by the tool.
  - Observe the tool communication in real time.

Lots of options...
Think about it…

- Many tools still use a Serial Port, you may use this method to log all I/O during data collection:
  1. Tool validation
  2. Error Checking
  3. Legal Proceedings
  4. Tool Comparison
  5. Free
  6. Other tools work nearly the same for direct USB communication (USBSnoop)

What was next…

- In communicating this concept to fellow peers, it occurred to me…
Mobile Forensic Tool Classification

- A common method/framework to describe HOW data is extracted from digital devices (e.g., Phones and GPS)
- Provides a common ground for all Mobile Examiners
- Vendors could classify tools

Mobile Forensic Tool Classification System…
5- Levels of Mobile Forensic Tool Classification:

1. Manual Extraction
2. Logical Extraction
3. Physical Analysis (Hex/JTAG)
4. Physical Analysis (Chip-Off)
5. Physical Analysis (Micro Read)

Tool Classification Pyramid

- Micro Read
- Chip-Off
- Hex Dumping/JTAG
- Logical Extraction
- Manual Extraction
Tool Classification Pyramid – Going Up

- More technical
- Longer analysis times
- More training required
- More invasive

*Products may exist at more than one level

Tool Classification Pyramid – Going Down

- Less technical
- Shorter analysis times
- Less training required
- Less invasive

*Cost is not proportional


Level 1: Manual Extraction

- **Manual Extraction:**
  - **Process:**
    - Review phone documentation, and browse the using device buttons to view and record data by hand.
  - **Pros:**
    - Fast
    - Will work on nearly every device
    - No cables required
    - Easy to use
  - **Cons:**
    - Will not get to ALL data
    - Prone to errors
    - Foreign language barrier
    - Booby traps
    - Broken buttons/device
    - No Deleted Files
    - Time consuming
  - **Tools available:**
    - Ramsey’s STE3000FAV
    - Eclipse
    - ZRT
    - Project-A-Phone
  - **Notes:**
    - Popular with local PD
    - Hand Jamming
    - NOT fun!

Level 2: Logical Extraction

- **Logical Extraction:**
  - **Process:**
    - Connect data cable to the handset. Extract data using AT, BREW, etc. commands in client/server architecture.
  - **Pros:**
    - Fast
    - Easy to use
    - Lots of research
    - Lots of info available
    - Foreign Language support
    - Standard report format
    - Repeatable
  - **Cons:**
    - May change data (e.g., Unread SMS)
    - Log file access (minimal)
    - End user understanding
    - Lots-o- Cables
    - Deleted files
  - **Tools available:**
    - Paraben’s Device Seizure
    - Susteen’s Data Pilot
  - **Notes:**
    - Many cell phone tools fit in this category.
    - Some GPS tools exist at this level
Level 3: Physical Extraction

- **Hex Dumping/JTAG**
  - **Pros:**
    - Deleted Data
    - Extract data hidden from device menus
    - Password Bypass - YMMV!
  - **Cons:**
    - Requires data conversion
    - Inconsistent report formats
    - Some tools came out of hacker community
    - Difficult to operate
    - Custom Cables
    - Source code not available
    - Limited to specific manufacturers
  - **Process:**
    - Push Boot Loader into phone and dump memory.
    - Includes using JTAG for data extraction
  - **Tools available:**
    - CelleBrite’s UFED Touch Ultimate
    - MSAB’s XRY Complete
    - RIFF Box
  - **Notes:**
    - Fastest growing segment in the marketplace.
    - Thanks to: Mike Harrington’s Hex Dumping Primer I and II

Level 4: Physical Extraction

- **Chip-Off**
  - **Pros:**
    - Able to extract ALL data from device memory
    - Better picture of what is going on holistically in the device
    - *Training now available!*
  - **Cons:**
    - Data is not contiguous!
    - No single report format
    - Difficult to use
    - May damage chip on extraction.
    - Source code not available
    - Custom cable harnesses needed
    - *JTAG may a better option!*
  - **Process:**
    - Remove memory from the device and read in either second device or EEprom reader.
  - **Tools available:**
    - UP-828
    - SD Flash Doctor
    - Custom Tools/Scripts
      - CheekyMonkeyForensics
  - **Notes:**
    - This includes de-soldering
    - More tools now available to reverse wear-leveling!
Level 5: Physical Extraction

- **Micro Read**
  - **Process:**
    - Use a high-power microscope to view state of memory.
  - **Tools available:**
    - High-Power Microscope
  - **Notes:**
    - This method would be reserved for high value devices or damaged memory chips.
  - **Pros:**
    - Able to extract and verify all data from device memory
    - Best picture of what is going on holistically in the device
  - **Cons:**
    - Most time consuming
    - Hard to interpret/convert
    - No report format
    - VERY Expensive
    - Highly technical

Leveling System Examples:

- **ZRT2** – **Level 1**
- **Data Pilot** – **Level 2**
- **UFED Touch Ultimate** – **Level 3**
- **UP-828** – **Level 4**
- **Hitachi S-450 SEM** – **Level 5**
Standard, Mini, Micro & Nano…

CSIM’s/RUIM’s
C-SIM = CDMA Subscriber Identity Module

✓ For **CDMA** handsets to extend a **GSM SIM** card for **CDMA** phones and networks.

✓ UICC may have: C-SIM, GSM **and** U-SIM partitions/application!

✓ Only commercial tool I know of right now is: SIMIS (3g Forensics – Lester Wilson)
Level 1 Tools:

Level 2 Tools:
(Basic)
Level 2/3 Tools:
(Basic)

Level 3 Tools:
(Advanced)
Level 4 Tools: (Chip Off)

Pieces and Parts...

1. Remove Chip
   A. IRSA IR 550 Plus
      • ~$20,000
   B. Heat Gun
      • ~$75
   C. Soldering Iron
      • ~$200

2. Read Chip
   A. FlashPak III
      • ~$10,000
   B. NAND Socket Module
      • ~$1,500

Cost: $32,000 USD
Pieces and Parts…

3. Reassembling data (e.g. 512K chunks)
   a) DDF (Free)
   b) SalvationData ($1500)

4. Translating the data…
   a) DDF (Free)
   b) SalvationData ($1500)

Level 4 Analysis Tool Examples:

- UFED’s Physical Analyzer
- AccesData’s MPE+
- MicroSystemation’s XRY Complete
- SQLite’s SQLite3 and SQLiteAnalyzer
- NaviCAT’s Navicat for SQLite (Good for visual joins of multiple tables)!
- Custom Scripts (e.g. CheekyMonkeyForensics)
Pieces and Parts…

- **Level 4 Training:**
  

- **Level 4 Research (2010 DFRWS Challenge):**
  

- **NAND Flash Memories and Programming NAND Flash Memories Using EL NEC Device Programmers:**
  
  [http://www.el nec.com/sw/an_el nec_nand_flash.pdf](http://www.el nec.com/sw/an_el nec_nand_flash.pdf)

- **Forensic Data Recovery from Flash Memory:**
  
  [http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf](http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf)

---

**Level 5 Tools:**

*(Micro Read)*

---
High-Power Microscope

1. Use chemical process to remove top layer of chip
2. Use microscope to read gates manually.
3. Translate binary to hex
4. Translate hex to data

Level 5 Tools:
(Micro Read)

- “Design Principles for Tamper-Resistant Smartcard Processors”
- “Physical NAND Flash Security: Preventing Recovery of Deleted Data”
Other Links:

- NIST: Computer Forensics Tool Testing (CFTT) of Mobile Devices:
  - Includes: Smart Phones, GSM and Non-GSM Phones
    - Tool Specifications
    - Test Assertions
    - Test Plans
    - Test Results

Contact Info:

- **Email:**
  - sam.brothers@dhs.gov

- **Phone:**
  - (703) 921-7149