Going deeper and deeper into Cell Phones

Jenise Reyes-Rodriguez
Software and Systems Division, ITL
NIST November 13, 2019
Computer Forensic Tool Testing

- Provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.
- Established around year 2000
- Develop a specification for analyzing mobile device memory/binary dumps and to support the admissibility of forensic data in court by providing the law enforcement community testing information.
Evolution of Cell phones

Some time ago...

Contacts
Call Logs
Text Messages/SMS
More current cell phones

Up to this day...

Contacts
- Calendar entries
- MMS
- Emails
- Browser history

Call Logs
- Apps
  - Instagram
  - Facebook
  - Snapchat
  - LinkedIn
  - Pinterest
  - Twitter
  - WhatsApp
- Deleted data

Text Messages/SMS
- Notes/Memos
- Media files (audio, pictures, video)
- Damaged devices

GPS

Onboarding 11/13/2019
Damaged Devices

- Structural
- Liquid
- Heat
Data Extraction

- **Level 1**
  - Manual Extraction

- **Level 2 – 3**
  - Logical Extraction
  - Physical Extraction

- **Level 4-5**
  - JTAG
  - Chip-Off
JTAG

- **Joint Test Action Group**

- Electronics industry association formed in 1985 for developing a **method of verifying designs and testing printed circuit boards** after manufacture.

- In 1990 the Institute of Electrical and Electronics Engineers codified the results of the effort in **IEEE Standard 1149.1-1990**, entitled Standard Test Access Port and Boundary-Scan Architecture.
JTAG Requirements

• Power
• Memory
• TAPs (Test Access Ports)
• Processor
JTAG Cycle
JTAG Method 2 – Solderless
Chip-Off

• Advanced digital data extraction and analysis technique which involves physically removing flash memory chip(s) from a subject device and then acquiring the raw data using specialized equipment

• Conducted by Fort Worth, Texas Police Dept.
Chip-Off Process - Material Removal

1. cutting/removing

2. cleaning/grinding

3. reading chip

4. Binary Dump
# JTAG & Chip-Off in forensic investigations

<table>
<thead>
<tr>
<th>Some Advantages</th>
<th>JTAG</th>
<th>Chip-Off</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Byte-for-byte memory extraction</em></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Destructive process</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Require specific data cables for each make/model</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Recover PIN-codes, pass-phrases, gesture swipes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bypass phones with locked/disabled USB data ports</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data recovery from damaged mobile devices (liquid, thermal, structural)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*It depends

**NOTE:** applies only to Android and Windows devices
Data Analysis - Analysis Tools

• Import binary files
• Review data parsed by analysis tools and compare with the known data set
Analysis Tool Types

<table>
<thead>
<tr>
<th>General Purpose</th>
<th>Mobile devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>• disk imaging</td>
<td>• phones</td>
</tr>
<tr>
<td>• string search</td>
<td>• Tablets</td>
</tr>
<tr>
<td>• <strong>import and parse JTAG binary dump</strong></td>
<td>• <strong>import and parse JTAG binary dump</strong></td>
</tr>
</tbody>
</table>

Difference among the tools?
Research Impacts

• Identify capabilities/limitations
• Differences/similarities across a variety of digital forensic tools capable of parsing a mobile device JTAG binary file
• Informs the forensic community and LE of tools capabilities and limitations
• Provides vendors and tool makers with the opportunity to address any anomalous behavior found
Findings

• Our research included 8 different Android devices ranging from Android 2.3 Gingerbread to Android 5.1 Lollipop.
• Of the 8 devices 4 of the devices had both JTAG and Chip-Off data extractions performed and the remaining 4 were Chip-Off.
• Overall the user data analyzed from JTAG and Chip-Off acquires has shown to be mostly consistent.
• There This differences were some minor differences but this was based on issues with a particular tool’s ability to parse and report the data.
• Overall the tools ability to report the user data populated onto each device was as expected. Some problem areas include specific versions of social media applications e.g., facebook, linkedin, twitter, Instagram, pinterest, snapchat, whatsapp, etc.
Contact Information

Jenise Reyes-Rodriguez
jenise.reyes@nist.gov

*** www.cftt.nist.gov ***

James Lyle
James.lyle@nist.gov

Rick Ayers
Richard.ayers@nist.gov