JTAG and Chip-Off
Data Analysis and Testing

NIST
Jenise Reyes-Rodriguez

AAFS – February 20th, 2020
Anaheim, California
DISCLAIMER

Certain company products may be mentioned or identified. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these products are necessarily the best available for the purpose.
CFTT at NIST

• Provides method of assurance that tools used in computer-related crime investigations produce valid results.

• Benefits:
  • Users make informed choices about acquiring/using computer forensic tools
  • Interested parties – understand the tools capabilities
  • Toolmakers – improve their tools
JTAG Overview

- Support admissibility in court
- Test PCBs
- IEE standard
- Bypasses pss/gesture swipes
- Data dumps: Windows & Android
- Damaged devices
- Requirements:
  - Memory
  - Power
  - TAPs
  - Processor
- 2 Methods:
  - Solder
  - Solderless
- It can’t be applied on ALL devices
- Test Access Port:
  - Size
  - Location
  - Shapes
  - Quantity
- Test Support
- Joint Test Action Group

It can’t be applied on ALL devices
Chip-Off Overview

- Physically removing memory chip from PCB
- Support admissibility in court
- Destructive method
- Conducted by Fort Worth Texas Police Dept and VTO labs
- It can’t be applied on ALL devices
- Physically removing memory chip from PCB
## JTAG and Chip-Off side by side

<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>
Data Analysis Flow

- Import Binaries
- Data parsed – analysis tools
- Data compared to known data set
Analysis Tools

- Disk Imaging
- String Search
- Import and Parse JTAG Binaries

Traditional Tools

Mobile Forensics Tools

- Phones
- Tablets
- Import and Parse JTAG Binaries
Data Analysis

• 9 tools used
• 10 devices
### Results – Analysis Tools

**Differences between analysis tools types?**

<table>
<thead>
<tr>
<th>Differences</th>
<th>Traditional Tools</th>
<th>Mobile Forensics Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation of Data</td>
<td>Presents the data in file explorer view format</td>
<td>Presents and categorizes the data better</td>
</tr>
</tbody>
</table>

* User data doesn’t change *
Results – JTAG Technique

- Analysis tools anomalies for JTAG:
  - Social Media data:
    - Facebook, Pinterest, SnapChat were partially or not reported – mostly Facebook/most tools
  - Stand-alone files
    - graphic, video, audio not reported for some devices – an analysis tool
Results – JTAG Technique Cont.

• Analysis tools anomalies for JTAG:
  • GPS:
    • Coordinates or address not reported for some devices – some tools
Results – Chip-Off Technique

- Analysis tools anomalies for Chip-Off:
  - Social Media data:
    - Facebook, Pinterest, Snapchat were partially or not reported – mostly Facebook/most tools
  - Stand-alone files
    - Graphic, video, audio not reported for some devices – most tools
Results – Chip-Off Technique Cont.

• Analysis tools anomalies for Chip-Off:
  • GPS:
    • coordinates or address not reported for some devices – most tools
Conclusions

• JTAG vs Chip-Off
  • both techniques were consistent across the board
• Analysis Tools Types
  • data presentation varies
Contacts

Jenise Reyes-Rodriguez
Jenise.reyes@nist.gov

Richard Ayers
Richard.ayers@nist.gov

Barbara Guttman
Barbara.guttman@nist.gov