DEUSOP09 – Using JTAG for Mobile Device Examinations

Table of Contents

1. Scope

1.1. This standard operating procedure is utilized for the acquisition of mobile phone memory using Joint Test Action Group (JTAG).

2. Background

2.1. To establish the practices for documenting the examination of evidence to conform to the requirements of the Department of Forensic Sciences (DFS) Digital Evidence Unit *Quality Assurance Manual*, the accreditation standards under ISO/IEC 17025:2017, and any supplemental standards.

3. Safety

3.1. If necessary due to condition of evidence received (e.g. hazardous and/or biological substances), wear appropriate personal protective equipment (e.g., lab coat, gloves, mask, eye protection), when carrying out standard operating procedures.

3.2. For proper handling of digital evidence see the DEUSOP01 – Handling Digital Evidence.

4. Materials Required

4.1. Forensic workstation with Internet access; JTAG box; JTAG software; JTAG jigs; JTAG cables/connectors; storage device; toolkit; mobile phone cable kit.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. Identify the make and model of the mobile device and determine if the device has support from your JTAG tool (i.e. Test Access Ports (TAPs)/Pinouts available, specific instructions for device, illustration or photograph of the circuit board of the phone available).

7.2. Research the phone's technical characteristics (i.e. microprocessor, operating system version, photos or videos of the phone's circuit board) to determine possible TAP locations and JTAG procedures.

7.3. Determine the connection type required (i.e. soldering the TAPS, non-soldering, flex cable, special jig, eMMC connection).

7.4. Collect instructions for safe disassembly.

Note: Obtain an identical model of a mobile device to use for practice if the procedure seems the least bit difficult or you are unsure of the procedure and its likely success.

7.5. In a story board fashion (allowing for easy reassembly), use the appropriate steps to safely secure all parts, screws, etc. Disassemble the mobile device to the point where the Test Access Ports (TAPs) are exposed.

7.6. Document/record each stage of the disassembly process. Documentation can be done via photography or using DEUF02 – Mobile Device Acquisition or both.

7.7. Perform the JTAG extraction.

7.7.1 Using the JTAG software, determine the pinout interface of the mobile phone device.

7.7.2 Attach the mobile phone device to the JTAG box (e.g., RIFF Box, RIFF Box 2, Octoplus Box) using the Jig specific for mobile phone device.

7.7.3 If a Jig is not available, solder the wires of the Universal JTAG cable to the mobile phone device.

7.7.4 Connect the JTAG box to the forensic workstation and start the JTAG software.

7.8. Verify the acquisition and produce verification hash values, and the total bytes that were acquired.

7.9. Create two copies of the original evidence: a best evidence and a working copy. Create a best evidence copy on appropriate storage media. Enter the item into LIMS and mark with appropriate DFS number for storage in DEU evidence. Create working copy and store the image on DEUNet. The image should be saved in the correct case folder. Within the case folder, the image should be saved in the “Evidence” folder, inside a folder that has the same name as evidence identification (e.g., Item 0006/Item 0006.E01).

7.10. Using the working copy, utilize forensic tools and/or scripts to analyze the JTAG extraction per the scope of the warrant or requesting agent.

8. Sampling

8.1. Not applicable.

9. Calculations

9.1. Not applicable.

10. Uncertainty of Measurement

10.1. Not applicable.

11. Limitations

11.1. Due to damage or other factors, some or all of the above examinations might not be possible. It is at the discretion of the analyst as to what examinations are necessary and if they should be conducted.

12. Documentation

12.1. DEUSOP01 – Handling Digital Evidence

12.2. DEUF01 – Mobile Device Examination

13. References

13.1. Digital Evidence Unit Quality Assurance Manual (Current Version).

13.2. DFS Departmental Operations Manuals (Current Versions).

13.3. Forensic Science Laboratory (FSL) Laboratory Operations Manuals (Current Versions).

13.4. Digital Evidence Unit Laboratory Operations Manuals (Current Versions).

13.5. DEUSOP01 – Handling of Digital Evidence (Current Versions).

13.6. H-11 Digital Forensics Phone Repair and Advanced JTAG Forensics Course Manual (v1.8 Oct 29, 2015).

13.7. SWGDE Standards and Controls Position Paper (v1.0 Jan 30, 2008).

13.8. SWGDE Best Practices for Examining Mobile Phones Using JTAG (v1.0 September 29, 2015).