C10 Joint Task Action Group (JTAG) and Chip-Off Data Analysis and Testing

Jenise Reyes-Rodriguez, BS, National Institute of Standards and Technology, Gaithersburg, MD 20899; Richard Ayers, MS, Gaithersburg, MD 20899-8970*

Learning Overview: After attending this presentation, attendees will better understand the capabilities and limitations of a variety of digital forensic tools that provide support for the analysis of JTAG and Chip-Off binaries from mobile devices operating over the Android™ operating system. The Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) has performed testing across classic digital forensic tools, as well as tools tailored specifically for the data extraction and analysis from mobile devices.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing an overview on analysis across multiple JTAG and Chip-Off binaries imported within a variety of digital forensic tools.

As mobile device usage and sophistication continue to grow, the need for rigorous research and testing conducted across a variety of forensic tools and techniques is critical. JTAG and Chip-Off data extraction provide forensic examiners with the ability to often recover additional data in comparison to a logical or file system data extraction. JTAG is a non-destructive method that returns a byte-for-byte memory dump of accessible data from supported mobile devices. Chip-Off is a destructive technique that entails removing the flash memory chip from the Printed Circuit Board (PCB). Removing the flash memory entails cutting and grinding the PCB, allowing the chip contacts to be exposed. Once the chip has been prepared, the memory registers of the chip are read utilizing the correct adapter and by running a programmer application.

The JTAG and Chip-Off research and testing conducted within the CFTT lab includes JTAG and Chip-off binaries from a variety of mobile devices. Each mobile device was populated with a defined dataset, including active and deleted data across numerous types of data elements. In addition to binaries collected using either the JTAG or Chip-Off data extraction technique, data for supported devices were extracted using both JTAG and Chip-Off. Analysis across multiple devices and techniques provides insight into advantages of one technique versus another. Additionally, performing both data extractions on supported devices illustrates any differences between JTAG and Chip-Off extractions for a unique mobile device.

The goal of this research and testing within the CFTT program is aimed at providing the forensic community with an understanding of the capabilities and limitations of various digital forensic tools that support analysis of JTAG and Chip-Off binary files. These results provide insight into any pros and cons across a combination of supported techniques and tools.

The presentation gives a summary of findings and lessons learned during the research and testing process of tools capable of extracting and analyzing memory contents from numerous JTAG and Chip-Off binaries.

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the author or the author's employer, nor does it imply that the products are necessarily the best available for the purpose.

Mobile Forensics, JTAG, Chip-Off

*Presenting Author