C23 Joint Task Action Group (JTAG) Data Extraction and Analysis

Jenise Reyes-Rodriguez, BS, NIST, 100 Bureau Drive, Gaithersburg, MD 20899; and Richard Ayers, MS, 100 Bureau Drive, MS 8970, Gaithersburg, MD 20899-8970*

After attending this presentation, attendees will better understand the importance of JTAG data extraction, analysis research, and testing conducted within the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST).

This presentation will impact the forensic science community by providing awareness of the capabilities and limitations for data extraction and digital forensic tools supporting JTAG binary file analysis.

As mobile device usage and sophistication continues to grow, the need for rigorous research and testing conducted across a variety of forensic tools and techniques is critical.

JTAG, an Institute of Electrical and Electronics Engineers (IEEE) standard, began as a method to verify the design and testing of printed circuit boards after manufacturing. The JTAG interface provides forensic examiners with numerous advantages, such as a non-destructive byte-for-byte memory dump from supported mobile devices whose data contents are typically examined using a traditional digital forensic tool. Additionally, the JTAG interface provides examiners with the ability to bypass mobile devices with disabled USB ports and the ability to extract data from devices that may have been subjected to liquid, thermal, or structural damage.

JTAG research conducted within the CFTT program begins by populating a set of supported mobile phones with a known data set containing active and deleted data. A known data set yields a way for results to be measured across several extraction solutions, techniques (i.e., solder, jig), and tools capable of parsing JTAG binary files. The memory contents are acquired across supporting JTAG extraction tools using a variety of connectivity techniques (e.g., solder, solderless). Data extractions begin with methodically disassembling a supported mobile device and identification of the copper Test Access Ports (TAPs) located on the Printed Circuit Board (PCB). The TAPs across various makes and models of supported mobile devices will vary in location and size. The TAPs are generally about the size of the tip of a thumbtack. Once the TAPs have been identified, various techniques can be utilized to establish connectivity and begin data extraction from the mobile device's internal memory, resulting in a JTAG binary file. After JTAG extraction, the data contents are examined by importing the JTAG binary into supporting analysis tools and comparing the results against known content.

The goal of the research and testing within the CFTT program is intended to provide the forensic community with an understanding of the capabilities and limitations of various JTAG extraction techniques and analysis tools. These results provide insight into any pros and cons across a combination of supported hardware, techniques, and tools capable of performing JTAG data analysis.

This presentation provides a summary of findings and lessons learned during the research and testing process of tools capable of extracting and analyzing memory contents from a mobile device using the JTAG interface.

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

JTAG, Mobile, Forensics