C4 Joint Test Action Group (JTAG) Tool Testing

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 be aware of the importance of tool testing and will have better understand the JTAG tool-testing process conducted within the Computer Forensics Tool Testing (CFTT) project.

This presentation will impact the forensic science community by increasing awareness of the impact tool testing has on informing the forensic community of tool capabilities and limitations. Test reports provide a foundation for toolmakers to improve tools, help users make informed choices, and provide interested parties with an overview of any anomalies found. The presentation will provide an overview of tools capabilities for acquiring and analysis of data recovered from the memory of a mobile device using JTAG and various analysis tools capable of parsing JTAG binary images.

The CFTT project has been researching and testing forensic tools capable of acquiring and analyzing JTAG binary images. This presentation discusses all aspects of the testing process that are critical for producing a test report and the information reported by the analysis tools capable of parsing JTAG binary images.

A summary for the test results of the JTAG acquisition and analysis tools examined will be discussed for each JTAG binary image created for the following test cases: (1) acquisition — acquire mobile device internal memory using supported JTAG hardware/software; (2) subscriber/equipment-related data — review acquired subscriber- and equipment-related information (i.e., International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier/Electronic Serial Number (MEID/ESN), Mobile Station International Subscriber Directory Number (MSISDN)); (3) Personal Information Management (PIM) data — review acquired PIM data (i.e., call logs (incoming, outgoing, missed), calendar entries, memos, Short Message Service (SMS), Multimedia Messaging Service (MMS) (audio, graphic, video), stand-alone files (audio, graphic, video), application-related data, social media-related data (Facebook®, LinkedIn®, Twitter®), internet-related data (browsing history, bookmarks); (4) deleted file recovery — review recoverable deleted data elements; and, (5) Global Positioning System (GPS) data — review data containing GSP longitude and latitude coordinates (routes, pictures, video).

Each test report contains an associated table comprised of two subcolumns that define a particular test category and individual subcategories that are verified when acquiring the internal memory for supported mobile devices within each test case. Each individual subcategory row provides results for each mobile device tested. The results are as follows: (1) as expected — the mobile forensic application returned expected test results — the JTAG tool acquired the contents and the analysis tool reported the data from the binary image successfully; (2) partial — the mobile forensic application returned some of the data from the acquired JTAG binary image; (3) not as expected — the mobile forensic application failed to return expected test results — the tool did not acquire or report supported data from the mobile device successfully; and, (4) Not Applicable (NA) — the mobile forensic application does not support reporting for a specific data element.

The presentation gives an overview of the CFTT process as applied to performing a JTAG acquisition and analysis of the acquired JTAG binary image.

The test reports are available from the Department of Homeland Security Cyber FETCH web site: https://www.cyberfetch.org/.

JTAG, Mobile Forensics, Digital

*Presenting Author