C22 Joint Task Action Group (JTAG) Phone Forensics

William Charles Easttom II, MBA, Chuck Easttom Consulting, 5605 Woodspring Drive, Plano, TX 75093*

After attending this presentation, attendees will better understand what it means to use JTAG techniques to access the raw data from a phone. Attendees will also receive an overview of when JTAG is the appropriate approach to phone forensics. This presentation will cover the types of techniques, equipment needed, and skills required to JTAG a phone. This presentation will also cover the limitations of JTAG and help forensic examiners know when this is the appropriate technique and when it is not. The goal of this presentation is to provide attendees with an understanding of JTAG phone forensics techniques.

This presentation will impact the forensic science community by defining how JTAG phone forensics techniques are a very critical topic in the area of mobile forensics.

It is a common occurrence for digital forensic investigators to require data from a phone that is locked or even physically damaged. When one of these situations occurs, common phone forensics tools are not adequate for the task of extracting data from the phone. In many cases, investigators in this situation will determine data cannot be extracted from the phone and will simply stop the investigation; however, there are techniques that allow a forensic examiner to directly access the computer chip on a phone (at least for an Android™ or Windows® phone), then to extract that information in a hexadecimal format.

Many law enforcement agencies lack personnel trained in JTAG techniques. Many forensic examiners assume that JTAG is very complex, exceedingly difficult, and is beyond their skillset. Some even suppose that an electrical engineer is required to JTAG a phone; however, these assumptions are inaccurate. There are a variety of inexpensive kits designed for testing of chips that can be applied to JTAG techniques on a phone.

Forensic investigators need a better understanding of the process, techniques, and procedures in order to begin to leverage JTAG techniques in their phone forensics investigations. This presentation will provide that fundamental knowledge that will allow forensic examiners to take the next step to implementing JTAG in their own investigations.

This topic is very important to digital forensics. As any examiner can attest, it is common to find a phone related to a case but be unable to access the data on that phone. This impedes investigations in all areas. Phone forensics itself impacts not just traditional cyber crime investigations but also violent crimes, drug trafficking, and even terrorism investigations. The ubiquitous nature of smart phones makes phone forensics one of the most critical aspects of digital forensics. Both civilian and law enforcement forensic examiners need to expand their technical skillset in order to provide the possibility of extracting data from a phone, even if that phone is locked or damaged.

JTAG, Mobile Forensics, Phone Forensics