B16 TracHac: Non-Smartphone First Responder Forensic Tool

Marcus Rogers, PhD, Purdue University, Cyber Forensic Lab, 401 North Grant Street, West Lafayette, IN 47907; and Robert Winkworth, MSc, 656 Oval Drive, West Lafayette, IN 47907*

After attending this presentation, attendees will become familiar with the current state of mobile forensics of non-smart phones and will be briefed on a custom hardware/firmware tool developed by the Purdue Cyber Forensic Lab for use with this class of mobile phones.

This presentation will impact the forensic scientific community by detailing the ability to acquire and analyze the data contained within mobile/cellphones. By presenting details regarding the development of a tool to deal with the most commonly used disposable cellphones, the area of mobile phone forensics will be further matured.

The use of disposable cellphones by various criminals and terrorist groups is becoming increasingly more common. This should not be surprising, as this technology has outpaced any other class of technology including personal computers. Criminals and terrorists are very aware that law enforcement considers cellphones to be an important source of evidence and intelligence. As such, the use of low cost, non-contract, disposable cellphones are becoming increasingly common. It is assumed that these devices will be very difficult for law enforcement to connect to the criminal or terrorist and they will contain either a minimum of evidence or be impervious to the current automated cellphone forensic tools. As a result, government and law enforcement are struggling to develop low cost tools and procedures to deal with disposable cellphones. This task is further complicated by the need for these tools to be used in the field to close the gap between the discovery of actionable intelligence or evidence, and the interview of the suspect(s) involved.

This presentation is an overview of a research project conducted at Purdue University that was designed to investigate the feasibility of developing a tool that focused on low cost disposable cellphones (aka, TracFones®). The functional limitations of the tool were determined by the sponsoring agency. The tool was limited to being used with non-smart phones, being non-invasive and automated enough to be used by first responders with only a limited amount of digital forensic training.

These low cost disposable phones often have the limited functionality and as such they fall under the radar of most of the industry standard automated mobile forensic tools. The current project surveyed law enforcement in the southwest region of the USA regarding the most commonly seized disposable mobile phones. The results where then used to purchase a sample of these phones that ranged in price from $20 - $50. These phones were populated with known data and then tested against industry standard automated tools.

The results indicate that the automated tools could not process most of the phones as they did not appear in the tools list of supported phones. A proof of concept first responder hardware/firmware prototype for dealing with these phones was fabricated and tested. This presentation will discuss the specific results and procedures for testing the TracFones® against common industry mobile forensic tools as well as details of the fabrication and development of the Purdue Cyber Forensic TracHac tool itself.

Mobile Phones, Disposable Cellphones, TracFone®

 ** Presenting Author*