CERIAS

the center for education and research in information assurance and security

Verifying Case File Integrity in Mobile Phone Forensics

Sean Sobieraj, CERIAS Graduate Student
Professor Rick Mislan, CI&T, Cyber Forensics Lab, CERIAS

There is a trial where evidence found on a mobile device is critical to its outcome. The prosecutors call an expert witness to the stand, who testifies that the evidence acquired from the mobile device is forensically sound, and has not been tampered with or altered. Hashes are provided that the expert witness confirms are correct and were used to verify the integrity of the evidence. The defense then states, through an expert witness of their own, that their acquisition of the mobile device produced different hashes than those provided by the prosecution. Why are they different? Which is correct? Can an investigator be trusted to answer these questions without the support of the forensic tools to back up their statements?

Up until recently, mobile forensic examiners were trusted to maintain the integrity of acquired evidence on there own. The newest versions of forensic software, specifically Paraben's Device Seizure and Susteen's SecureView, have implemented integrity protection mechanisms for protecting acquired data.

- **What is being hashed?**
- **When in the acquisition process are hashes computed?**
- **How are they computed?**
- **Where are the hashes stored?**
- **How are they used to maintain the integrity of the data?**
- **Are they successful?**

ffd93f16876049265fbaef4da268dd0e
d41d8cd98f00b204e9800998ecf8427e
da1e100dc9e7bebb810985e37875de38

paraben forensic tools

susteen

The goal of this paper is to verify the methods implemented by Paraben's Device Seizure and Susteen's SecureView to protect the integrity of data obtained from mobile phones.

ffd93f16876049265fba
ef4da268dd0e
d41d8cd98f00b204e9
800998ecf8427e
da1e100dc9e7bebb81
0985e37875de38

The dynamic nature of mobile phone memory causes hash inconsistencies in subsequent acquisitions of the same phone. Identical hashes from different model phones has also been documented. These erratic hash values are believed to be a result of the proprietary limitations of what can be acquired from a phone, and constantly changing timestamps in phone memory.

The forensics tools are expected to maintain the integrity of collected evidence on a per acquisition basis, however the granularity in which the hashing mechanisms are implemented may need improvement. Each type of data object obtained from the phone provides a unique fingerprint (ie. call logs, address book, text messages), and standard methods of integrity protection may be possible based on the available data from the phone.

PURDUE
UNIVERSITY
COLLEGE OF TECHNOLOGY
CYBER FORENSICS LAB

PURDUE
UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center