Is Mobile Device Forensics Really "Forensics"?

NIST Mobile Forensics Workshop
Gaithersburg, MD
June 2014

Gary C. Kessler
Embry-Riddle Aeronautical University
Overview

- Is digital forensics a forensic science?
- Is mobile device forensics part of digital forensics?
- Is the practice of mobile device analysis good forensics?
Definition of Terms

What is physics?
Defining *forensics*

- "The application of scientific knowledge to legal problems" (Merriam-Webster)
  - Includes forensic medicine, physics, chemistry, dentistry, fingerprints, DNA, firearm analysis, accounting, ....

- Forensic sciences widely tied to Locard's Exchange Principle
  - "Every contact leaves a trace" (Prof. Edmond Locard, c. 1910)
How Does Digital Forensics Fit?

• Does Locard's Principle apply in cyberspace as it does in the real world?
• Does the National Academy of Science report (2009) call *all* forensics processes into question?
• Is *digital forensics* a forensic science?
  – American Academy of Forensic Sciences (AAFS) accepted Digital and Multimedia Science in Feb. 2008
  – *Aren't DOJ and NIST grappling with this question?*
Forensic Process

• The basic process of forensics
  – Identification
  – Preservation
  – Collection
  – Examination
  – Analysis
  – Reporting
But Digital Forensics Is Different...

• Most forensic sciences are comparing a latent sample to a known sample
  – E.g., fingerprints, DNA, blood, bullets, tire prints, tool marks, shoe prints, etc.

• Digital forensics is not a "comparing" science
More Differences

• The *tools* of the physical forensic sciences have changed but the properties of the samples have remained mostly the same
  – DNA and blood haven't changed in millions of years but the science and the tools have improved

• Computers are changing constantly
  – New devices, new architectures, new tools
Where's the Science?

- **Science** is an organized structure for understanding a body of knowledge
  - We are not using digital forensics to seek greater truths
- Digital forensics employs the scientific method to guide our approach to:
  - Find information
  - Apply a context to the information
  - Determine probative value of the information
Mobile Device Forensics

- Does the examination of mobile devices meet this test?
  - Are we imaging mobile devices?
  - Are we changing the state of the device during examination?
Changes in Technology

• It is difficult for laws, investigators, and practitioners to keep up with the increasing acceleration of technological change

• Consider cell phones
  – 1993: We were happy to have dial tone (RAM = 0)
  – 2003: Phone, call history, contact list, SMS, images, videos (RAM = 10-100 MB)
  – 2013: Phone + portable Internet terminal with e-mail, browser history, GPS locations, documents (RAM = 8-64 GB)
Mobile Devices vs. Computers

• Operating systems
  – Computers: 2½ (Windows, Linux/Unix/Mac OS X)
  – Mobile devices: 4+ (Android, Blackberry, iOS, Windows, and more)

• The power of tools such as Cellebrite and XRY have caused some to believe that:
  – The tools are 100% complete
  – If the tools don't report it, it's not there

• There is more probative information on a cell phone per byte examined than on a computer
  (GCK, 2006)
  – But it's not all easy to come by
Is This *Forensics*?

• Many people in our field claim that cell phone analysis is not "forensics"
• Given that *forensics* is the use of science and technology to answer questions in a court of law
  – Mobile device forensics absolutely *is* forensics
  – Yet it *is* different from traditional computer forensics
    • E.g., cell phone power is on, we are not making an "image," the state of the device changes over time, ...
• We do ourselves a disservice to imply that our processes would not pass a Daubert challenge
So....

• Is mobile device forensics actually "forensics"?

• YES!!!!

  “yes....BUT!”

• Unfortunately, we don't practice it that way...
The Relentless Pursuit of The Easy Button
Mobile Device Forensics as Practiced...

• Would any police dept. in the U.S. just hand an EnCase or FTK dongle to a cop and ask them to analyze a computer?
  – So, why do so many police depts. hand a UFED, Touch, or XRY to a cop and ask them to "dump" a smartphone?
• There is so much information on a phone that more and more examiners merely provide the output to the investigator in the form of a several hundred page PDF...
  – We only grab what the tools easily find
  – We are relegating ourselves to the role of technician and not doing any analysis
The Result of This Attitude

• We are not providing sufficient training and education related to
  – Proper seizure procedures for mobile devices
  – Proper transport procedures
  – Proper forensic examinations and analysis
  – The difference between acquisition and parsing
• This is where mobile device forensics suffers as "forensics"
Summary

• Digital forensics is an engineering science
• Mobile device forensics is a digital forensic science
• The profession of digital forensics requires continued education, training, and practice
  – Digital forensics is a computer science
• In U.S. law enforcement, computer forensics is practiced more professionally than mobile device forensics
Author Contact Information

Gary C. Kessler, Ph.D., CCE, CCFP, CISSP
Embry-Riddle Aeronautical University
600 S. Cylde Morris Blvd.
Daytona Beach, FL 32114

mobile: +1 802-238-8913
office: +1 386-226-7947
e-mail: gary.kessler@erau.edu
gck@garykessler.net
Skype: gary.c.kessler

http://www.garykessler.net