Mobile Device Forensics

Rick Ayers

Disclaimer

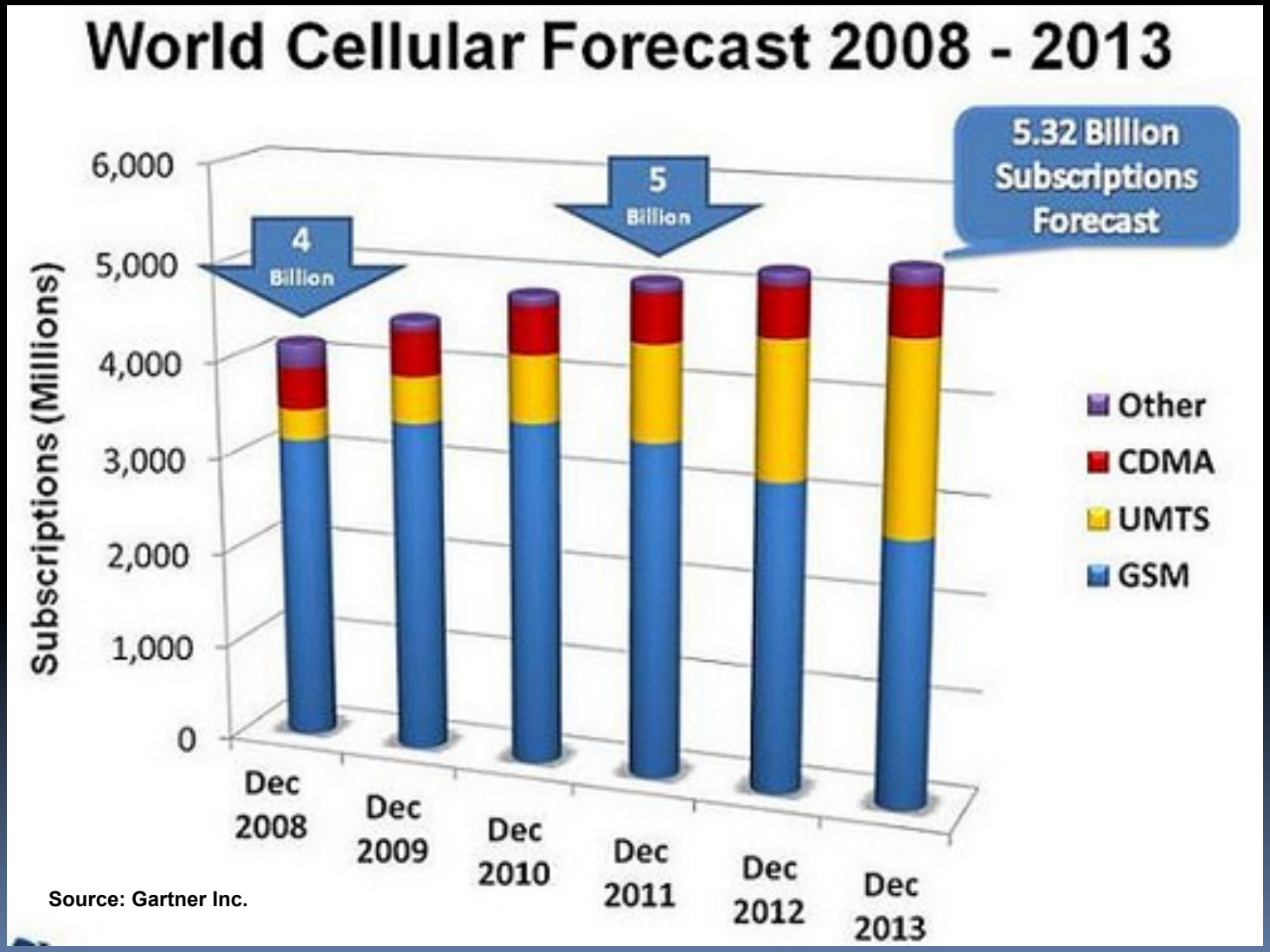
- Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Agenda

- Motivation for Mobile Device Tool Testing
- Evidence Sources
- Acquisition Levels
- Challenges
- CFTT Program
- Tool Validation
- Common Anomalies
- 2014 Mobile Device Testing
- Conclusions

Motivation


World Cellular Forecast 2008 - 2013
5.32 Billion Subscriptions Forecast
4 Billion
5 Billion
Subscriptions (Millions)
6,000
5,000
4,000
3,000
2,000
1,000
0
Dec 2008
Dec 2009
Dec 2010
Dec 2011
Dec 2012
Dec 2013
Other
CDMA
UMTS
GSM
Source: Gartner Inc.

Evidence Sources

- Phonebook
- Calendar
- To do list

- Electronic mail
- Instant messages
- Web information

- Electronic documents
- Photos
- Videos
- Audio

- GPS coordinates
- Social network data

- Subscriber identifiers
- Equipment identifiers
- Service Provider

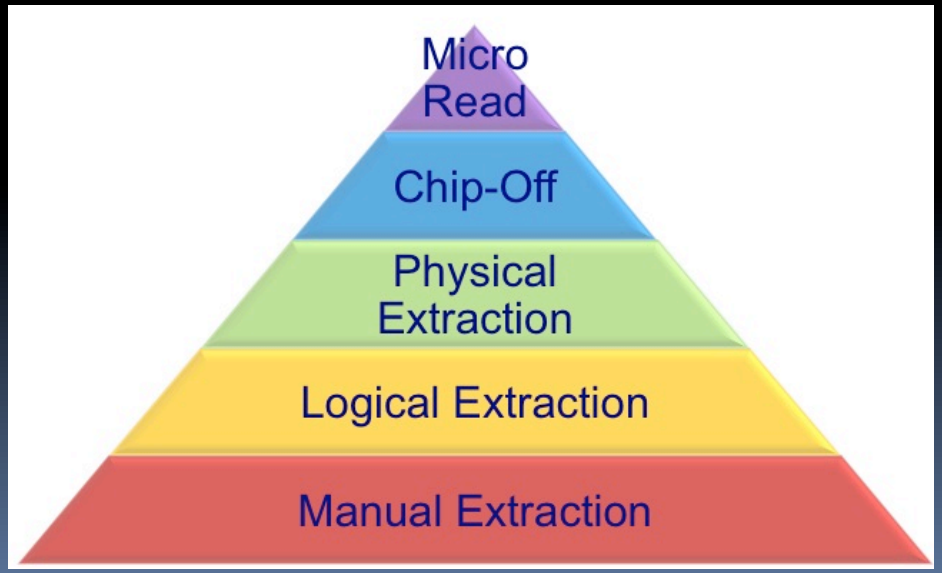
- Last dialed numbers
- Phone number log

- Short text messages
- Enhanced messages
- Multimedia messages

- Last active location (voice and data)
- Other networks encountered

Acquisition Levels

- Micro Read
- Chip-Off
- Physical Extraction
- Logical Extraction
- Manual Extraction



--Source – Sam Brothers, DHS

Challenges

- Multiple interfaces
  - Smart Phones: mini-USB, micro-USB, proprietary
- Acquisition support for old and current models
  - Tool kits containing over a thousand cables
- Quality Control
- Closed mobile device operating systems
  - Reverse engineering the file system

CFTT Overview

- **Computer Forensics Tool Testing Project**

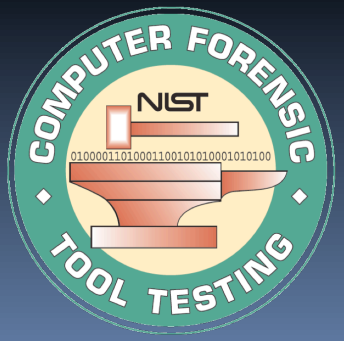
James Lyle, Project Leader

100 Bureau Drive, Stop 8970

Gaithersburg, MD 20899-8970 USA

E-mail cftt@nist.gov

Website: www.cftt.nist.gov



CFTT Overview

- CFTT – Computer Forensics Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.
- Directed by a steering committee composed of representatives of the law enforcement community.
- The steering committee selects tool categories for investigation and testing. A vendor may request testing of a tool, however the steering committee makes the decision about which tools to test.
- CFTT is a joint project of: DHS, OLES, FBI, DoD, Secret Service, NIJ and other agencies.

CFTT Methodology

- **Test Specification – Requirements**
- Test Plan – Test Cases and Assertions
- Setup and Test Procedures
- Final Test Report Generation

Requirements

- Requirements – Statements used to derive test assertions that define expectations of a tool or application.
  - Core Requirements – Requirements that all mobile device acquisition tools shall meet.
  - Optional Requirements – Requirements that all mobile device acquisition tools shall meet on the condition that specified features or options are offered by the tool.

CFTT Methodology

- Test Specification – Requirements
- **Test Plan – Test Cases and Assertions**
- Setup and Test Procedures
- Final Test Report Generation

Test Plan

- Test Cases – Describe the combination of test parameters required to test each assertion.
- Assertions – General statements or conditions that can be checked after a test is executed

CFTT Methodology

- Test Specification – Requirements
- Test Plan – Test Cases and Assertions
- **Setup and Test Procedures**
- Final Test Report Generation

Setup and Test Procedures

- Objective: Documentation on data population of target media and test procedures providing third parties with information for an independent evaluation or replication of posted test results.

- Contents:
  - Techniques used for data population
  - Test Case Execution Procedures

Mobile Device Population

- Manual input (time consuming)
  - SMS/MMS messages
  - Call logs (incoming, outgoing, missed)
- Synchronization over webmail
  - Contacts, calendar entries, memos
  - Email
  - Photos, video, audio files

CFTT Methodology

- Test Specification – Requirements
- Test Plan – Test Cases and Assertions
- Setup and Test Procedures
- **Final Test Report Generation**

Test Report

- Results summary
- Test case selection
- Results by test assertion
  - An overview of the test cases executed, assertions checked and any anomalies found.

Tool Validation

- Tool validation results issued by the CFTT project at NIST provide information necessary for:
  - Toolmakers to improve tools
  - Users to make informed choices about acquiring and using computer forensic tools
  - And for interested parties to understand the tools capabilities

Common Anomalies

- Non-Latin characters
- Truncated entries
- Connectivity issues
- Acquisitions ending in errors
- Subscriber related data not reported (IMEI, MSISDN)
- Unsuccessful recovery of non-overwritten “recoverable” deleted data
- Unsuccessful recovery of Internet and application related data

2014 Mobile Device Testing

- 11 mobile device acquisition tools
- 20 mobile devices
  - CDMA
    - feature phones
    - smart phones
    - tablets
  - GSM
    - feature phones
    - smart phones
    - tablets

Additional 2014 Mobile News

- **SP800-101 Revision1 "Guidelines on Mobile Device Forensics"**
  - ***Mobile device characteristics***
  - ***Forensic tools***
  - ***Preservation***
  - ***Acquisition***
  - ***Examination and analysis***
  - ***Reporting***
- **Mobile Device Specification and Test Plan updated**

Conclusions

- Mobile device subscribers will continue to grow exponentially
- Data storage continues to expand
- Evidence sources
- Acquisition levels
- Challenges
- CFTT testing methodology
- Importance of tool validation
- Common anomalies
- Update on Mobile Testing for 2014

Thank You!

Contact Information:

Rick Ayers
richard.ayers@nist.gov
www.cftt.nist.gov
www.cfreds.nist.gov