Mobile Device Forensics

COMPUTER FORENSIC TOOL TESTING

NIST

01000011010001100101010001010100

Rick Ayers

Disclaimer

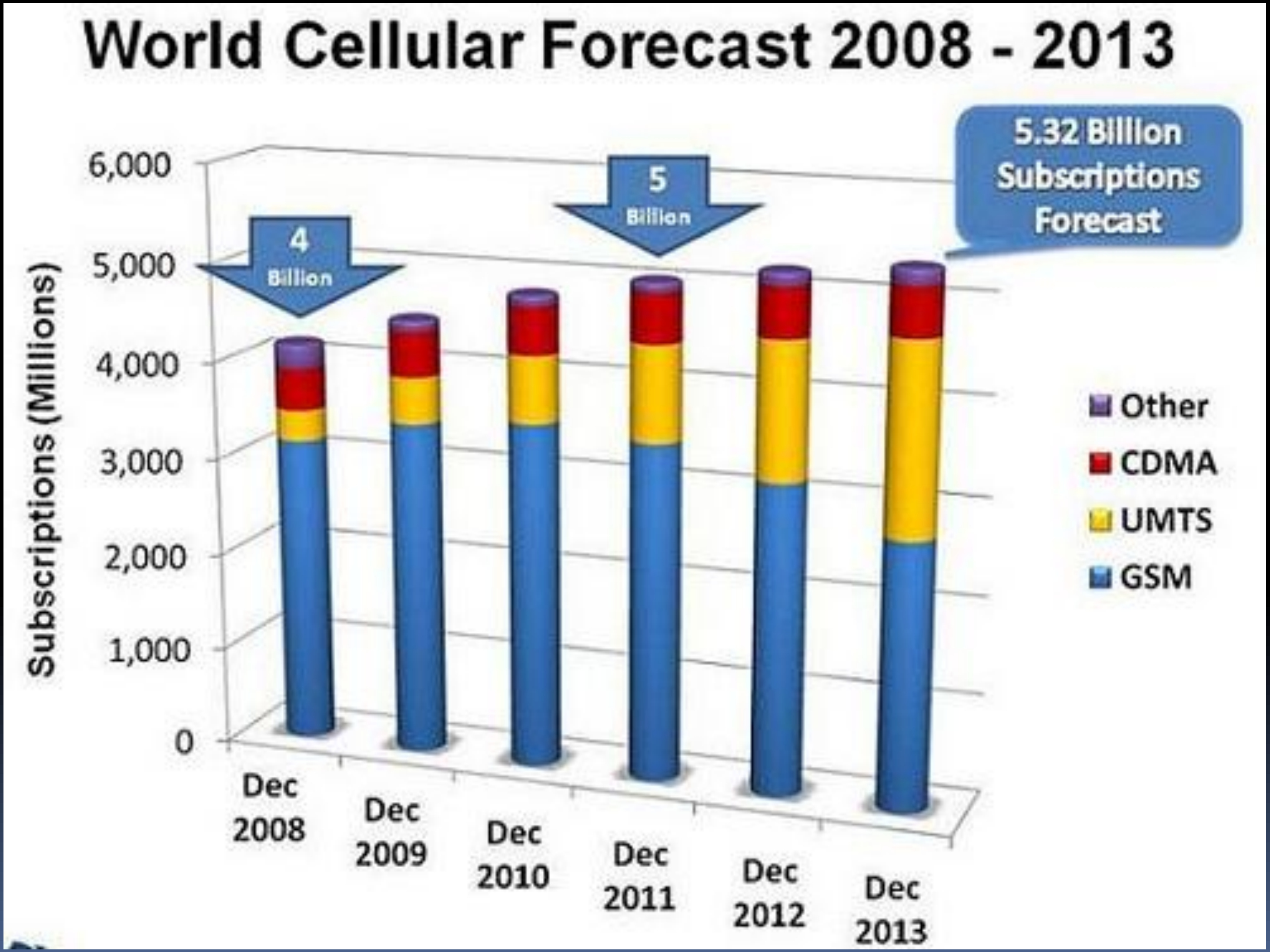
- Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is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

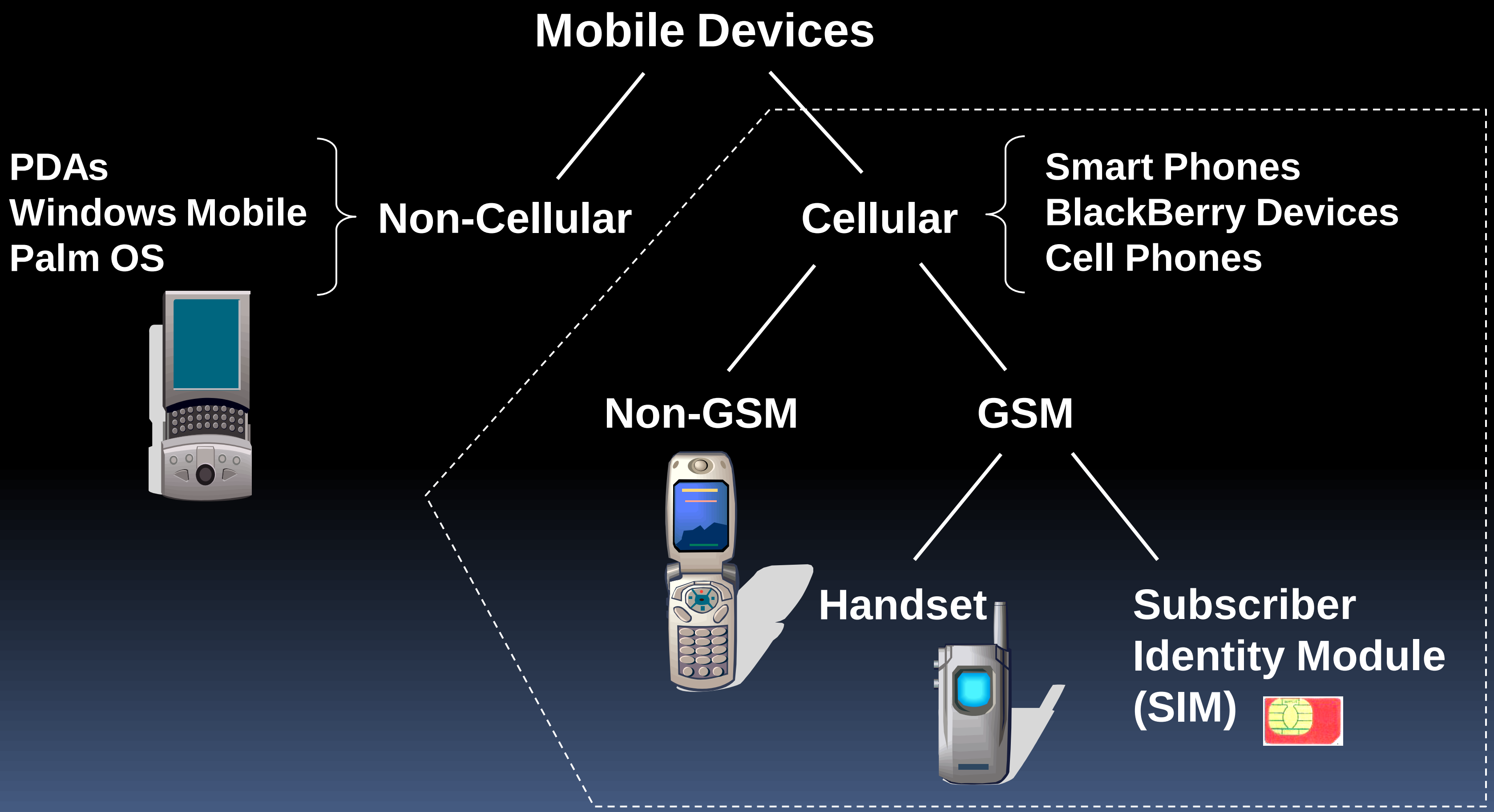
Agenda

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

Motivation


World Cellular Forecast 2008 - 2013
5.32 Billion Subscriptions Forecast
5 Billion
4 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

Mobile Device: Tool Classification



Mobile Devices

PDAs
Windows Mobile
Palm OS

Non-Cellular

Cellular

Smart Phones
BlackBerry Devices
Cell Phones

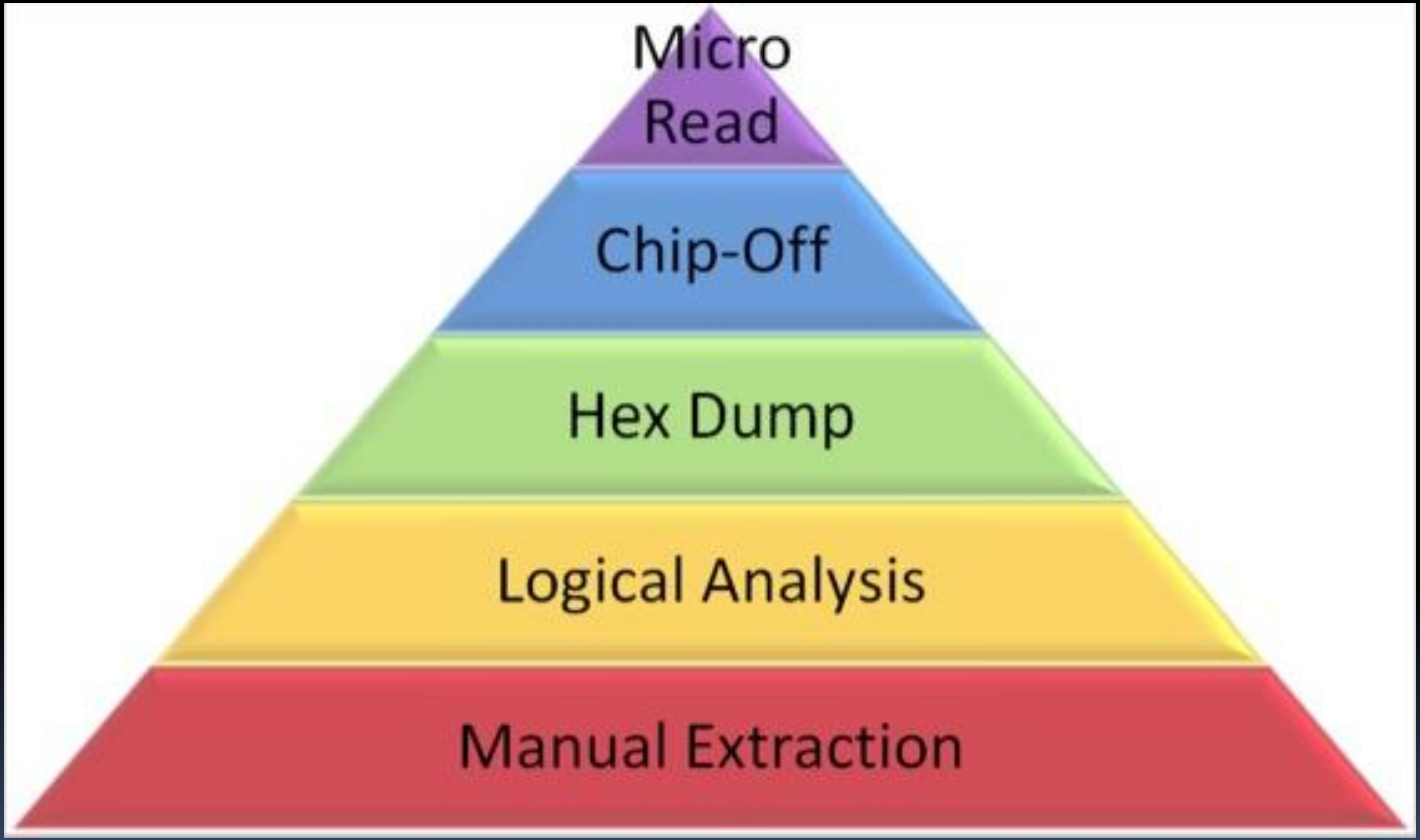
Non-GSM

GSM

Handset

Subscriber Identity Module (SIM)

Acquisition Levels



--Source – Sam Brothers, DHS

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**

Challenges

- Multiple interfaces
- Acquisition support for old and current models
- Quality Control
- Closed mobile device operating systems

CFTT

- **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: NIJ, DHS, OLES, FBI, DoD, Secret Service 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 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.
  - Example: Acquire mobile device internal memory over tool-supported interfaces (e.g., cable, Bluetooth, IrDA)
- Assertions – General statements or conditions checked after a test is executed
  - Example: If a cellular forensic tool provides support for connectivity of the target device then the tool shall successfully recognize the target device via all tool-supported interfaces (e.g., cable, Bluetooth, IrDA).

CFTT Methodology

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

Setup and Test Procedures

- Objective: Provide third parties with information for an independent evaluation or replication of posted test results.

- Example contents:
  - Techniques for populating mobile devices and Subscriber Identity Modules (SIMs) – ADNs, LDNs, SMS, EMS
  - Test Case Execution Procedures

CFTT Methodology

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

Test Report

- Results summary
  - Sufficient for most readers to assess the suitability of the tool for the intended use
- Test case selection
  - Test case run details
- 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-ASCII 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

Thank You!

Contact Information:

Rick Ayers

richard.ayers@nist.gov

susan.ballou@nist.gov

- http://www.cftt.nist.gov
- http://www.cfreds.nist.gov
- http://www.nsrl.nist.gov