Periodic Mobile Forensics (PMF)

Rapid differential forensic imaging of mobile devices

DFRWS 2016

Mark Guido – mguido@mitre.org

Justin Grover – jgrover@mitre.org

Jonathan Buttner – jbuttner@mitre.org

Mobile Forensics: Logical vs. Physical

- **Logical Acquisition**
  - Includes “Filesystem” and “Advanced Logical”

- **Physical Acquisition**
  - Reads from block (storage) devices
  - Uncovers deleted files; preserves timestamps

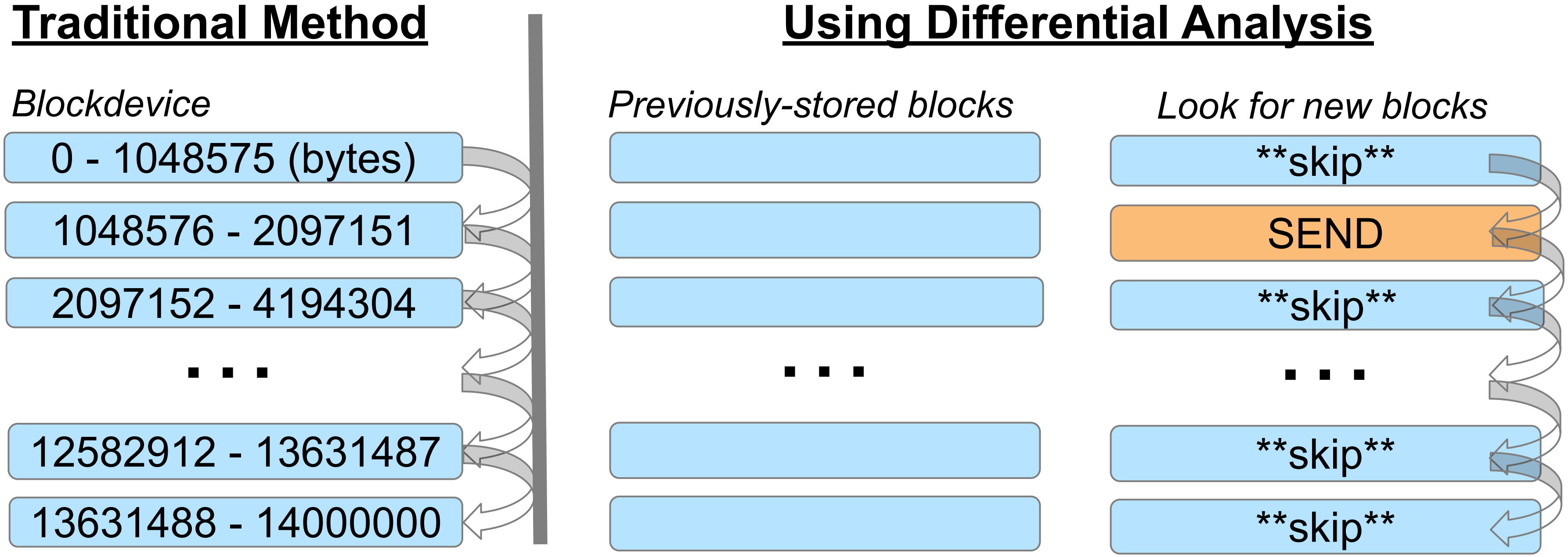
Android: Physical Acquisition Environments

- **Device must be booted in one of these modes to acquire:**

1. Bootloader mode
2. Custom recovery mode
3. Normal mode w/ elevated privileges

* We prefer the bootloader or custom recovery modes because they are more forensically sound.

Physical Acquisition Methods



Garfinkel, Nelson, and Young. "A general strategy for differential forensic analysis." ***Digital Investigation*** **9 (2012): S50-S59.**

Research Question

- **Can we physically acquire never-before-seen mobile devices in 10 minutes or less?**

Answer □ YES!

- **Target use cases:**
  - Crime scene
  - Border crossings
  - Time-sensitive operations

Photo credit: IAEA Imagebank, Flikr.com, Creative Commons

Related Work

- **Periodic Mobile Forensics**
  - Our technique is an extension of this project

Photo credit: Rob Bulmahn, Flikr.com, Creative Commons

☆ **We redesigned the on-device agent to focus on:**

- Speed
- No previous knowledge
- Using the existing PMF backend infrastructure

Related Work

- Teleporter: Physical acquisitions of hard drives in limited bandwidth environments (2009)

Watkins K, McWhorte M, Long J, Hill B. Teleporter: an analytically and forensically sound duplicate transfer system. *Digital Investigation* Sept, 2009;6(Suppl.):S43–47

- Sifting Collectors: Rapid forensic imaging of large disks (2015)

Grier, J. and Richard, G., 2015. Rapid forensic imaging of large disks with sifting collectors. *Digital Investigation*, *14*, pp.S34-S44

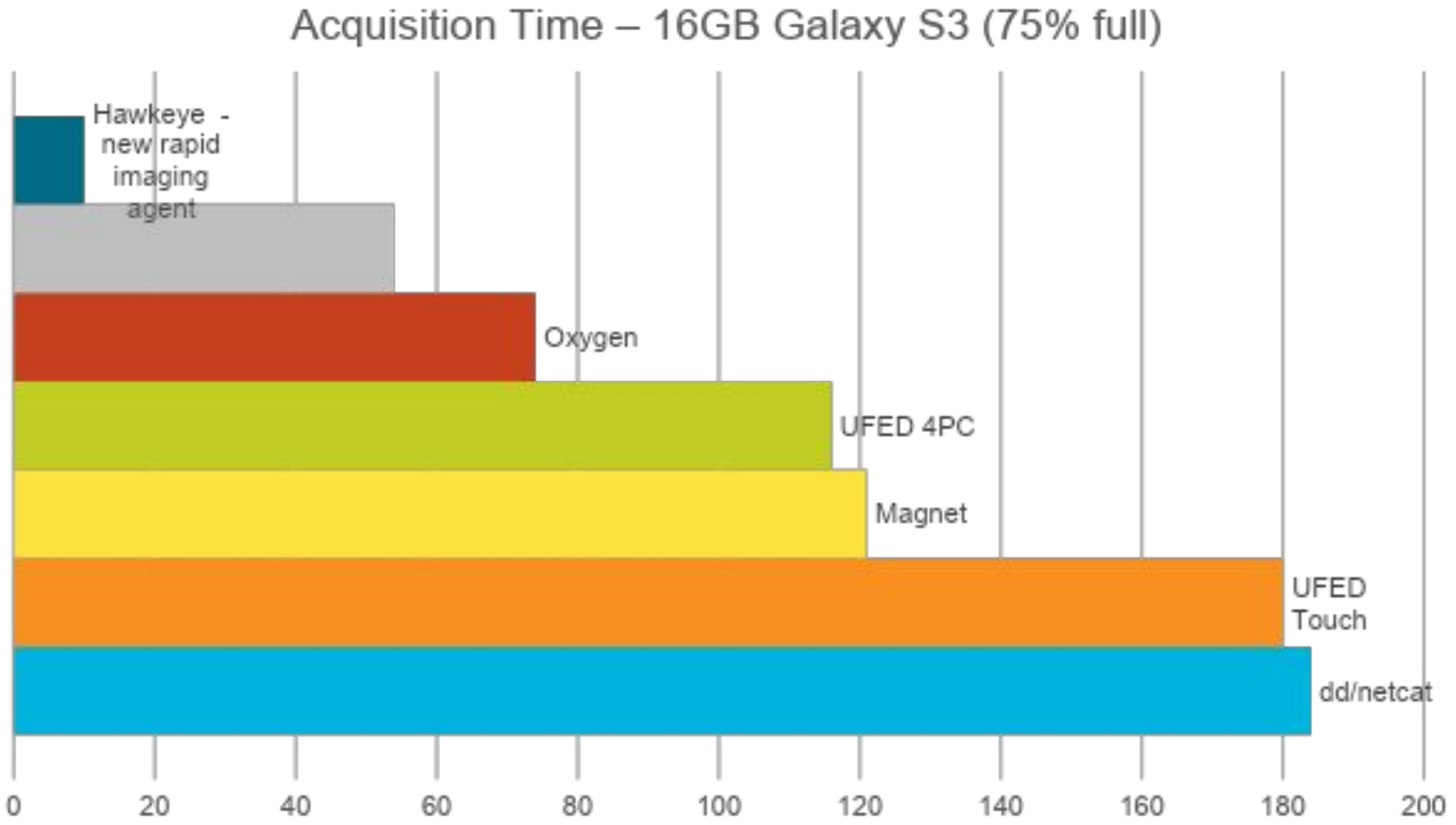
Related Work

- **APD: Android Physical Dump**
  - Bootloader acquisition method for Android™

Yang, S.J., Choi, J.H., Kim, K.B. and Chang, T., 2015. New acquisition method based on firmware update protocols for Android smartphones. *Digital Investigation*, *14*, pp.S68-S76.

- **Acquisitions in 30 minutes for several 32 GB devices:**
  - LG® G3™, Optimus G™, R3, Iron2, Nexus™ 4/5

Comparison to current tools



minutes

What is hawkeye?

- **On-device native multi-threaded C agent**
  - Uses a variety of methods to improve speed
- **Theoretically works on any Android device w/ custom recovery**
  - Tested on 20+ different models
  - Efforts to test on more…
- **Goal: identify and send only the “unknown” storage blocks**
  - USB connection is the bottleneck
- **Manual execution (although this is completely automated) :**

```
./hawkeye  <hashes>  <partitions>  <IP>
```

Improvement #1: Skipping Zeros

- **Many devices are not filled to capacity**
- **Unused blocks contain NULL chars (all-zeros)**
- **We can detect all-zero blocks very quickly**
  - Hashing…too slow
  - Zero-block comparison function…252X faster than MD5!

…00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00…

Improvement #2: Gold Hash List

- **Why transfer data when you already have it?**
  - Remember…USB is the bottleneck
- **Hash list tells hawkeye which blocks to skip**
  - Can include representative portions of files / storage blocks
- **Use of hash maps is well-known in forensics, but not typically found in acquisition tools**
  - NSRL

Improvement #3: 64K “Peek Ahead”

- **Why are you hashing the whole block?**
  - First 64K reveals everything you need to know □ <u>most of the time</u>

- **If first 64K is new, it’s guaranteed you need to send whole block**
  - Full block hash not needed

Improvement #4: Enable Networking

- **Common technique: dd & netcat over adb… too slow**
- **Reverse-tethering is setup between device and laptop**
  - Laptop connection is used by device
- **Allows for asynchronous message queueing with RabbitMQ**
- **Currently testing functionality in Normal mode using “root” exploitation method**

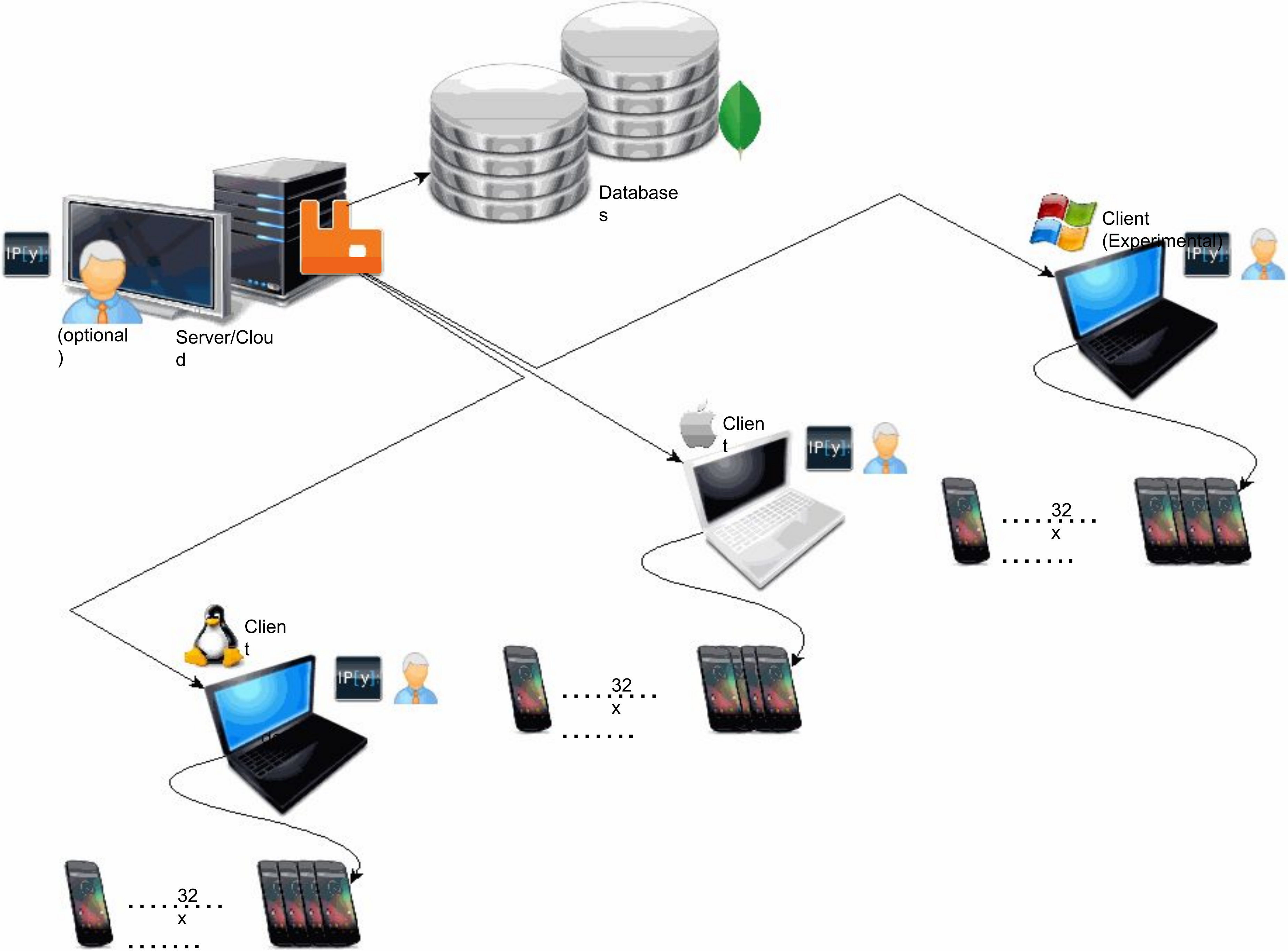
4-step process to using Hawkeye & PMF

1. Identify target mobile device model and verify Hawkeye support

2. Flash a Team Win Recovery Project (TWRP) custom recovery image onto the device and boot the custom recovery kernel

3. Connect the target mobile device to the PMF architecture (e.g., laptop) via USB cable

4. Execute Hawkeye from laptop, which temporarily installs *hawkeye* to the device's volatile memory, sets up communications between client and PMF, and starts the *hawkeye* agent


Databases
IP[y]:
(optional)
Server/Cloud
Client (Experimental)
IP[y]:
Client
IP[y]:
32 x
Client
IP[y]:
32 x
32 x

Best Case / Worst Case

filled from `/dev/zero`

filled from `/dev/urandom`

Device	Capacity	Baseline (secs)	Random-filled (secs)
Nexus 4	8 GB	1 min, 33 sec	6 min, 40 sec
Galaxy S3	16 GB	4 min, 24 sec	14 min, 51 sec

Measuring the Typical Case

We flashed images onto devices from "The Purdue Experiment"

- 34 devices operated by volunteers
- 3 month experiment
- 1000+ physical images taken

Phone ID	Acq. Time
4	5 min 24 sec
15	5 min 33 sec
29	6 min 52 sec
30	8 min 48 sec
33	5 min 02 sec
34	7 min 14 sec

*** Average: 6 min, 29 secs**

Validation

We compared the Hawkeye/PMF output to Cellebrite & XRY…

Hawkeye	Cellebrite	MSAB XRY*
✓	✓	✓

** Raw image file extracted from XRY proprietary format*

Adapting to other platforms

- **We focus on Android, but the technique has broad applicability**
  - iOS devices
    - iPhone 5
      - /dev/disk0s1s1 = system
      - /dev/disk0s1s2 = data

  - Hard drives

  - System-on-chip

Current Efforts

- **Customs & Border Protection (CBP)**
  - Sam Brothers and Ariane Moore using it to image 10,000 devices
- **Champlain College capstone project**
  - Validation of the hawkeye technique
- **Transitioned to 12 U.S. Government groups**
- **Non-commercial license to Netherlands Forensics Institute (NFI)**
- **Commercial license of Hawkeye techniques to a mobile forensics vendor**
  - Will be integrated into product in short timeframe

Thank you!

Mark Guido
mguido@mitre.org

Justin Grover
jgrover@mitre.org

Jonathan Buttner
jbuttner@mitre.org

Photo Credit: Scot Campbell, Wikimedia Commons, Creative Commons