Smartphone and Network Forensics go Together Like Peas and Carrots

Heather Mahalik | @heathermahalik
Phil Hagen | @philhagen
Background

- No single forensic discipline can give a complete view of an incident

- Leveraging multiple disciplines can give comprehensive visibility

- Incidents are multifaceted…

  …analysis must be as well
The Plan

- Associate both iPhones to wireless access point
- Tap and record all network traffic
- Conduct typical activity on both iPhones
- Filesystem dump from one iPhone
- Network traffic examination from all traffic
The Setup

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
# Evidence Used

## Device-based
- iPhone filesystem dump
  - Logical acquisition
  - Best method for non-jailbroken iOS devices with A5+ chip
  - Doesn’t provide access to all the data…

## Network-based
- NetFlow
  - Statistical traffic abstraction: all metadata – no content
- Full packet capture
  - ALL content of network communications
- PassiveDNS logs
  - ASCII logs detailing all DNS queries and responses
Filesystem Dump

The evidence…

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
Passive DNS

- Broad scoping – protocol-agnostic view of all activity
- 192.168.1.3 (iPhone 5s): 59 total domains
  - 58x google.com, 29x apple.com, 10x amazon.com, 8x twitter.com, 8x facebook.com, 6x icloud.com, 3x pinterest.com, 1x Smarter Forensics.com
- 192.168.1.2 (iPhone 6): 36 total domains
  - 21x instagram.com, 15x pubnub.com, 14x apple.com, 13x facebook.com, 6x icloud.com, 3x nest.com, 2x tripit.com, 1x identityvector.com

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
FaceTime Audio Call on WiFi

- Started 16:33:14, 24 sec
  - +1-703-424-xxxx to +1-703-628-xxxx
- Call is tracked by iOS and stored in CallHistory.storedata
- Status flag reflects WiFi FaceTime audio call
- Forensic tools show expected results
iOS FaceTime Traces
Network FaceTime Artifacts

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Src IP Addr</th>
<th>Dst IP Addr</th>
<th>Packets</th>
<th>Bytes</th>
<th>bps</th>
<th>Bpp</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-07-08 16:33:14.261</td>
<td>0.061</td>
<td>192.168.1.3</td>
<td>192.168.1.1</td>
<td>4</td>
<td>293</td>
<td>38426</td>
<td>73</td>
<td>4</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.277</td>
<td>0.165</td>
<td>192.168.1.1</td>
<td>192.168.1.3</td>
<td>4</td>
<td>573</td>
<td>27781</td>
<td>143</td>
<td>4</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.282</td>
<td>0.036</td>
<td>192.168.1.3</td>
<td>23.207.44.52</td>
<td>7</td>
<td>417</td>
<td>92666</td>
<td>59</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.284</td>
<td>0.031</td>
<td>23.207.44.52</td>
<td>192.168.1.3</td>
<td>5</td>
<td>560</td>
<td>144516</td>
<td>112</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.313</td>
<td>0.120</td>
<td>192.168.1.3</td>
<td>204.0.4.251</td>
<td>2</td>
<td>168</td>
<td>11200</td>
<td>84</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.320</td>
<td>0.120</td>
<td>204.0.4.251</td>
<td>192.168.1.3</td>
<td>2</td>
<td>172</td>
<td>11466</td>
<td>86</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.424</td>
<td>0.173</td>
<td>192.168.1.3</td>
<td>17.178.104.63</td>
<td>5</td>
<td>275</td>
<td>12716</td>
<td>55</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.452</td>
<td>0.825</td>
<td>192.168.1.3</td>
<td>17.154.239.222</td>
<td>9</td>
<td>396</td>
<td>3840</td>
<td>44</td>
<td>2</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.458</td>
<td>0.769</td>
<td>192.168.1.3</td>
<td>17.154.239.223</td>
<td>4</td>
<td>176</td>
<td>1830</td>
<td>44</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.500</td>
<td>0.825</td>
<td>17.154.239.222</td>
<td>192.168.1.3</td>
<td>9</td>
<td>396</td>
<td>3840</td>
<td>44</td>
<td>2</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.502</td>
<td>0.775</td>
<td>192.168.1.3</td>
<td>209.94.244.140</td>
<td>12</td>
<td>528</td>
<td>5450</td>
<td>44</td>
<td>3</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.502</td>
<td>0.267</td>
<td>209.94.244.140</td>
<td>192.168.1.3</td>
<td>6</td>
<td>432</td>
<td>12943</td>
<td>72</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.508</td>
<td>0.767</td>
<td>17.154.239.223</td>
<td>192.168.1.3</td>
<td>4</td>
<td>176</td>
<td>1835</td>
<td>44</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:14.509</td>
<td>0.086</td>
<td>17.178.104.63</td>
<td>192.168.1.3</td>
<td>3</td>
<td>139</td>
<td>12930</td>
<td>46</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:15.762</td>
<td>14.995</td>
<td>192.168.1.3</td>
<td>72.246.45.215</td>
<td>10</td>
<td>1360</td>
<td>725</td>
<td>136</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:15.852</td>
<td>14.933</td>
<td>72.246.45.215</td>
<td>192.168.1.3</td>
<td>7</td>
<td>952</td>
<td>510</td>
<td>136</td>
<td>1</td>
</tr>
<tr>
<td>2015-07-08 16:33:18.641</td>
<td>0.668</td>
<td>192.168.1.3</td>
<td>239.255.255.250</td>
<td>7</td>
<td>1442</td>
<td>1330</td>
<td>206</td>
<td>1</td>
</tr>
</tbody>
</table>

Summary: total flows: 28, total bytes: 10507, total packets: 119, avg bps: 3725, avg pps: 5, avg bpp: 88

Total flows processed: 75, Blocks skipped: 0, Bytes read: 4320
Sys: 0.003s flows/second: 22097.8 Wall: 0.000s flows/second: 250000.0
Network FaceTime Artifacts (2)

- Session Traversal Utilities for NAT (STUN)
  - Traffic present at start of call
  - STUN provides NAT detection, FaceTime Peer location
  - Wireshark parsing does not appear accurate/complete

- Current theory is that STUN allows local network peer discovery for P2P FaceTime call
FaceTime Video Call on LTE

Started 16:41:34, 6sec
+1-703-424-xxxx to +1-703-628-xxxx

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
Network FaceTime Artifacts

- Wireless network died
- Network evidence went bye bye
- Both phones seamlessly transferred to LTE
  - Great for usability
  - Sucks for analysis
Reality of the Smartphone

- Do we really know when we are on WiFi vs. LTE?
- Does it change our user capabilities?
- What happens when we drop off the network?
Device Arrival Detection

- Device makes HTTP request to detect captive portal: http://static.ess.apple.com/connectivity.txt
- Identifies when new device goes online
- http.request.uri == "/connectivity.txt"

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
Application Profiling

- User Agent strings

```
$ tshark -n -r smartphone-network_atnight.pcap -Y 'http.user_agent' -T fields -e ip.src -e http.user_agent | sort | uniq

192.168.1.2  653QP26LZG.com.tripit.tripitmobile.paid
192.168.1.3  AppStore/2.0 iOS/8.4 model/iPhone6,1 build/12H143 (6; dt:89)
...```

- 192.168.1.3 (iPhone 5s)
  itunesstored/1.0 iOS/8.4 model/iPhone6,1 build/12H143 (6; dt:89)
  Mozilla/5.0 (iPhone; CPU iPhone OS 8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) CriOS/43.0.2357.61 Mobile/12H143 Safari/600.1.4
  Mozilla/5.0 (iPhone; CPU iPhone OS 8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12H143
  Mozilla/5.0 (iPhone; CPU iPhone OS 8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12H143 Safari/600.1.4
  Pinterest/5.0.2 CFNetwork/711.4.6 Darwin/14.0.0

- 192.168.1.2 (iPhone 6)
  653QP26LZG.com.tripit.tripitmobile.paid
  TripItPaid/5.3.0.150521670035 CFNetwork/711.4.6 Darwin/14.0.0
  com.revolv.store/2.0.133 CFNetwork/711.4.6 Darwin/14.0.0
  Revolv/2.0.133 (iPhone; iOS 8.4; Scale/2.00)
  Instagram 7.1.0 (iPhone7,2; iPhone OS 8_4; en_US; en) AppleWebKit/420+
  Nest/5.0.1.12 (iOS) os=8.4 platform=iPhone7,2

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
Tracing HTTP Activity

- Opened Safari
- Loaded pages
- What evidence is available and how much can we learn?
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Activity</th>
<th>App</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/8/2015</td>
<td>4:20:37 PM</td>
<td>Has the smartphone finally outsmarted us?</td>
<td>Safari</td>
<td><a href="http://smarterforensics.com/2015/02/has-the-smart">http://smarterforensics.com/2015/02/has-the-smart</a></td>
</tr>
<tr>
<td>7/8/2015</td>
<td>4:25:53 PM</td>
<td>Welcome to Facebook</td>
<td>Safari</td>
<td><a href="https://m.facebook.com/">https://m.facebook.com/</a></td>
</tr>
</tbody>
</table>

**Visited Page**

- **Title:** Practical Mobile Forensics
- **Last Visited:** 7/8/2015 4:22:15 PM (UTC+0)
- **Visits:** 1
- **URL:** [http://www.amazon.com/Practical-Mobile-Forensics-Satish-Bommisetty/dp/1783288310](http://www.amazon.com/Practical-Mobile-Forensics-Satish-Bommisetty/dp/1783288310)
- **Source:** Safari

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC
Un-logged HTTP Artifacts

- User-Agent string is arbitrary and optional, but helpful
- HTTP Referer string indicates “where you came from”
Takeaways (1)

- Smartphone Forensics
  - Tools primarily give insight to human-initiated actions…
    Reality is they miss a lot of data that must be manually recovered
  - Includes artifacts from encrypted communications
  - Provides consistent view as device enters/leaves networks
  - Have to acquire device – not always easy with mobile devices
Takeaways (2)

- Network Forensics
  - Limited by device presence – seamless WiFi/LTE handoffs severely hamper perspective
  - Encryption means functionally opaque communications, but PassiveDNS can give some insight
  - Un/poorly documented protocols hinder analysis
  - Includes all activity including system/background tasks
  - Relatively easy to profile and analyze with most protocols
Comprehensive Analysis!!

- If you rely on only one forensic methodology, you lose perspective!

- No such thing as a single-discipline investigation
  - Don’t let yourself be a single-discipline forensicator

FOR585: Advanced Smartphone Forensics
http://for585.com/course

FOR572: Advanced Network Forensics and Analysis
http://for572.com/course

© 2015 Smarter Forensics, LLC and Lewes Technology Consulting, LLC