Smartphone and Network Forensics go Together Like Peas and Carrots

Heather Mahalik | @heathermahalik
Phil Hagen | @philhagen

Background

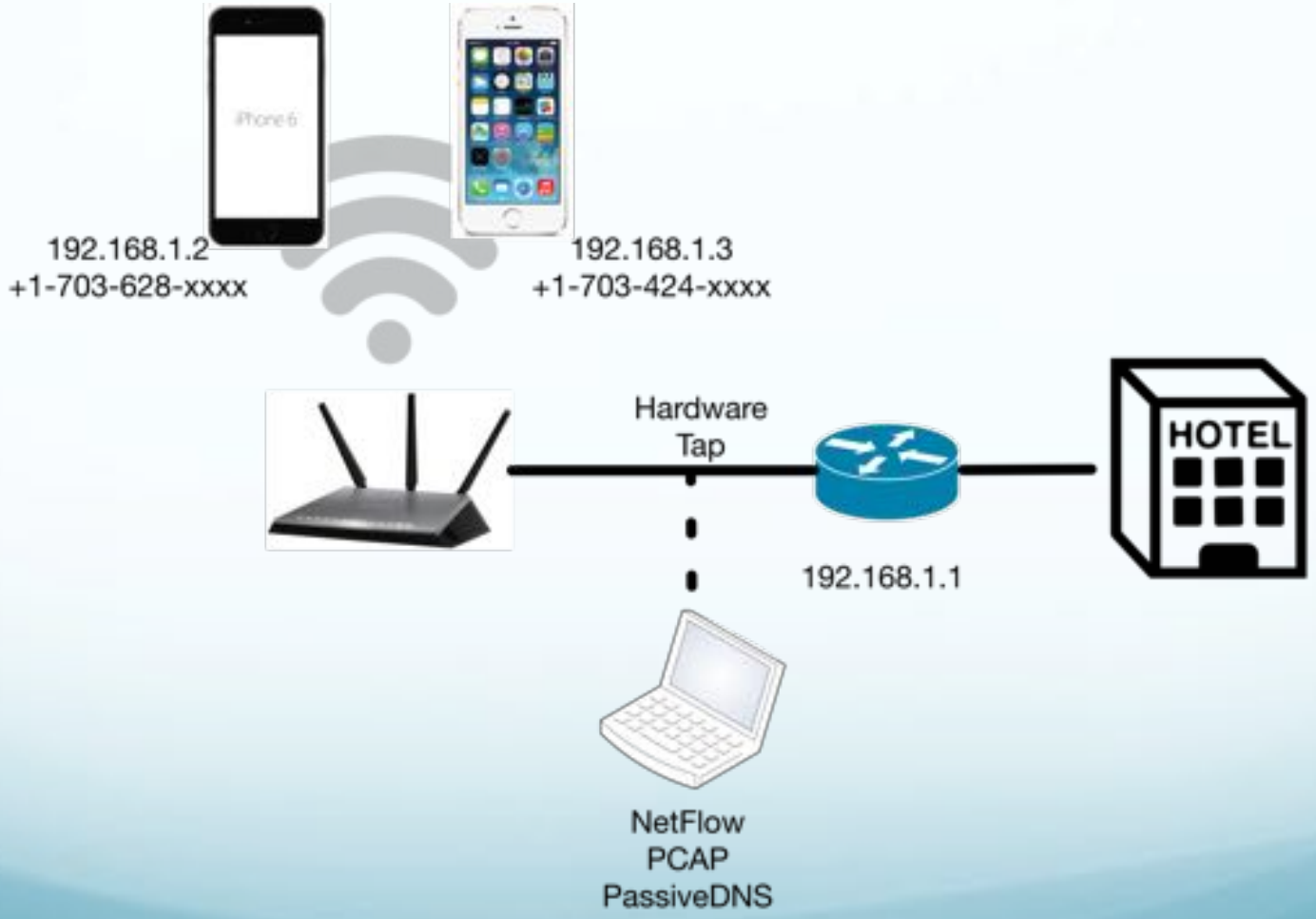
- No single forensic discipline can give a complete view of an incident
- Leveraging multiple disciplines can give comprehensive visibility
- Incidents are multifaceted…

…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



Evidence Used

Device-based

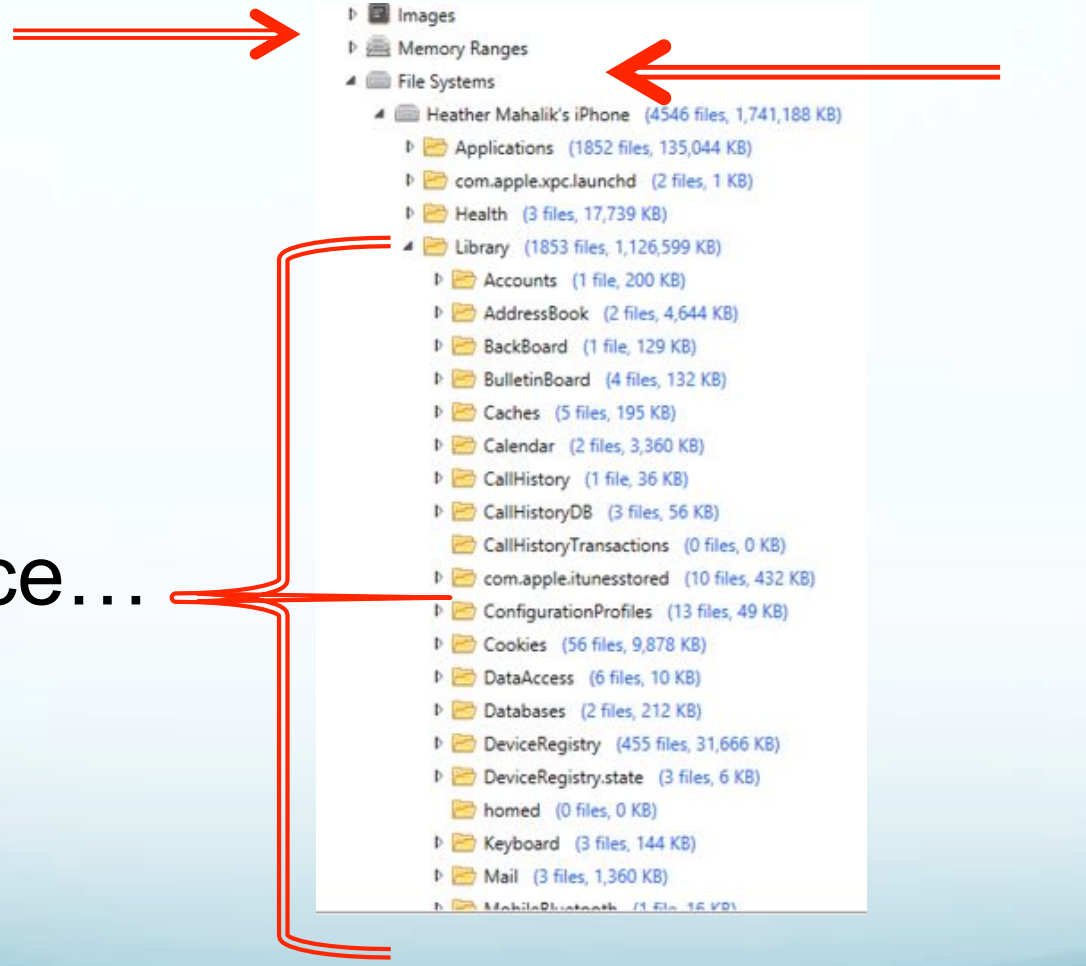
- iPhone filesystem dump
  - Logical acquisition
  - Best method for non-jailbroken iOS devices with A5+ chip
  - Doesn't provide access to all the data…

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…



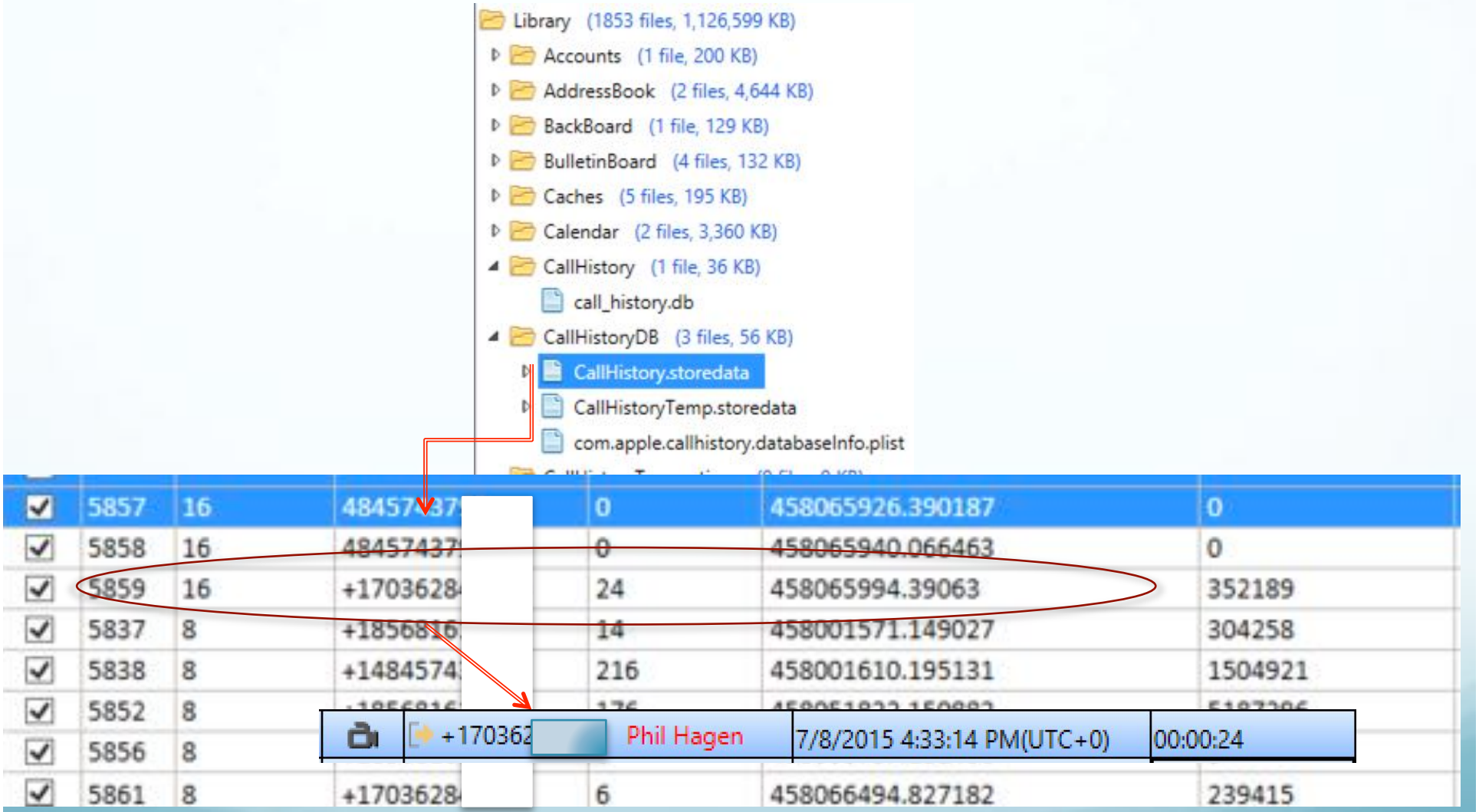
Passive DNS

- Broad scoping – protocol-agnostic view of all activity
  - `1436372003.802274||192.168.1.2||192.168.1.1||IN||apple.com.||A||17.178.96.59||1998||1`
- 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

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

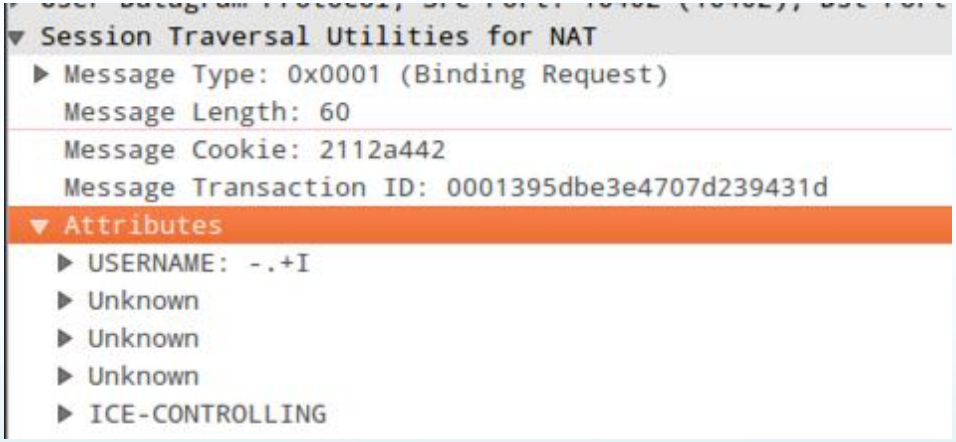


Network FaceTime Artifacts (1)

```
$ nfdump -R . -t '2015/07/08.16:33:10-2015/07/08.16:33:45' -O tstart -A srcip,dstip
Date first seen          Duration      Src IP Addr      Dst IP Addr   Packets     Bytes      bps     Bpp Flows
2015-07-08 16:33:14.261     0.061     192.168.1.3      192.168.1.1         4       293    38426      73     4
2015-07-08 16:33:14.277     0.165     192.168.1.1      192.168.1.3         4       573    27781     143     4
2015-07-08 16:33:14.282     0.036     192.168.1.3     23.207.44.52         7       417    92666      59     1
2015-07-08 16:33:14.284     0.031    23.207.44.52      192.168.1.3         5       560   144516     112     1
2015-07-08 16:33:14.313     0.120     192.168.1.3      204.0.4.251         2       168    11200      84     1
2015-07-08 16:33:14.320     0.120      204.0.4.251      192.168.1.3         2       172    11466      86     1
2015-07-08 16:33:14.350    22.471     192.168.1.3     10.13.141.87        19      2052      730     108     1
2015-07-08 16:33:14.424     0.173     192.168.1.3    17.178.104.63         5       275    12716      55     1
2015-07-08 16:33:14.452     0.825     192.168.1.3   17.154.239.222         9       396     3840      44     2
2015-07-08 16:33:14.458     0.769     192.168.1.3   17.154.239.223         4       176     1830      44     1
2015-07-08 16:33:14.500     0.825    17.154.239.222      192.168.1.3         9       396     3840      44     2
2015-07-08 16:33:14.502     0.775     192.168.1.3   209.94.244.140        12       528     5450      44     3
2015-07-08 16:33:14.502     0.267    209.94.244.140      192.168.1.3         6       432    12943      72     1
2015-07-08 16:33:14.508     0.767    17.154.239.223      192.168.1.3         4       176     1835      44     1
2015-07-08 16:33:14.509     0.086     17.178.104.63      192.168.1.3         3       139    12930      46     1
2015-07-08 16:33:15.762    14.995     192.168.1.3     72.246.45.215        10      1360      725     136     1
2015-07-08 16:33:15.852    14.933     72.246.45.215      192.168.1.3         7       952      510     136     1
2015-07-08 16:33:18.641     8.668     192.168.1.3  239.255.255.250         7      1442     1330     206     1
Summary: total flows: 28, total bytes: 10507, total packets: 119, avg bps: 3725, avg pps: 5, avg bpp: 88
Time window: 2015-07-08 09:26:55 - 2015-07-08 16:33:36
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

☑	5857	16	4845743	0	458065926.390187	0
☑	5858	16	4845743	0	458065940.066463	0
☑	5859	16	+170362	24	458065994.39063	352189
☑	5837	8	+185681	14	458001571.149027	304258
☑	5838	8	+148457	216	458001610.195131	1504921
☑	5852	8	+185681	176	458051822.150882	5187296
☑	5856	8	+185681	0	458065737.131456	0
☑	5861	8	+170362	6	458066494.827182	239415

	Parties	Timestamp	Duration
	+1703628 Phil Hagen	7/8/2015 4:41:34 PM(UTC+0)	00:00:06
	61059492	7/8/2015 4:35:04 PM(UTC+0)	00:02:15
📹	+1703628 Phil Hagen	7/8/2015 4:33:14 PM(UTC+0)	00:00:24
📹	48457437 Shannon Church	7/8/2015 4:32:20 PM(UTC+0)	00:00:00
📹	48457437 Shannon Church	7/8/2015 4:32:06 PM(UTC+0)	00:00:00
	+185681 Joanne	7/8/2015 4:28:57 PM(UTC+0)	00:00:00

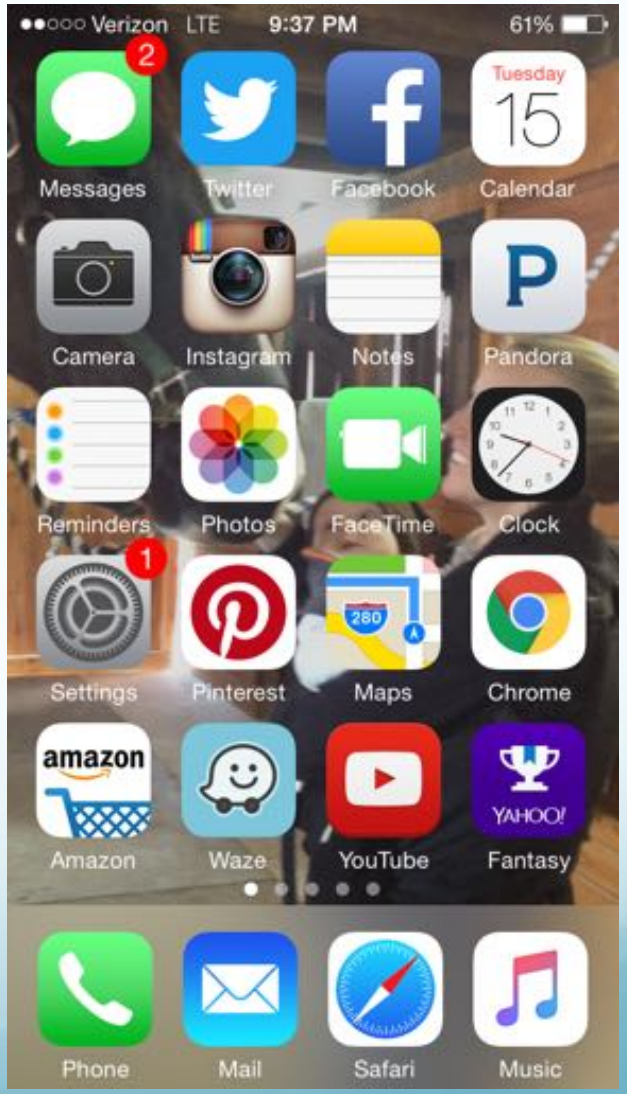
Network FaceTime Artifacts

```
$ nfdump -R . -t '2015/07/08.09:41:30-2015/07/08.09:41:45' -O tstart -A srcip,dstip
Date first seen                 Src IP Addr   Dst IP Addr   Packets    Bytes      bps    Bpp Flows
Summary: total flows: 0, total bytes: 0, total packets: 0, avg bps: 0, avg pps: 0, avg bpp: 0
Time window: 2015-07-08 09:38:58 - 2015-07-08 09:43:31
Total flows processed: 615, Blocks skipped: 0, Bytes read: 34560
Sys: 0.008s flows/second: 75349.2    Wall: 0.002s flows/second: 237635.2
```

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

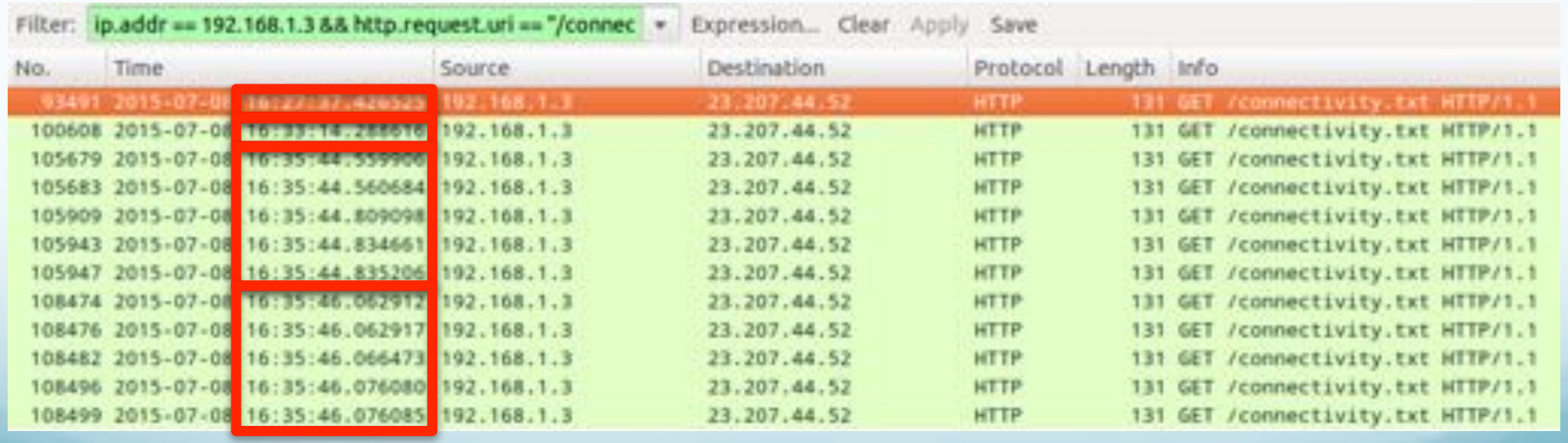
Reality of the Smartphone

- 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"`



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
```

Chrome

Mobile Safari

Pinterest App

- 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
```

TripIt Travel Planning App

Revolv Home Automation App

Instagram App

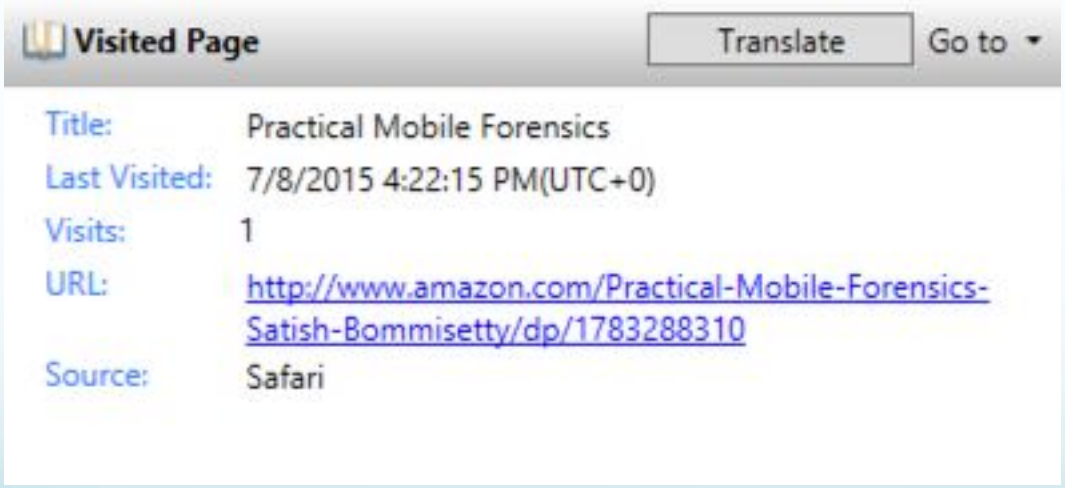
Nest Thermostat App

Tracing HTTP Activity

- Opened Safari
- Loaded pages
- What evidence is available and how much can we learn?

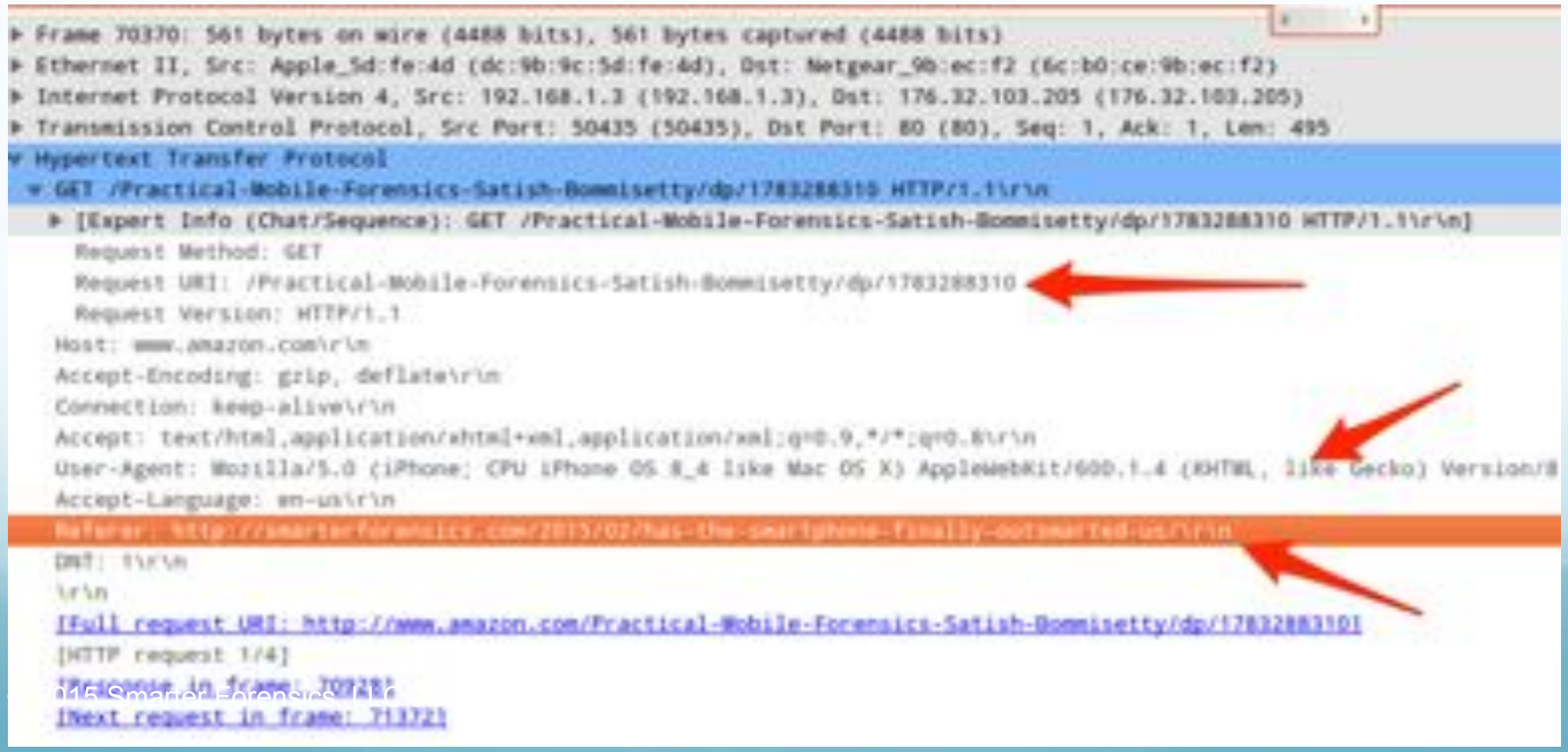
Smartphone Evidence

7/8/2015 4:20:37 PM...	Has the smartphone finally outsmarted us? |...	Safari	http://smarterforensics.com/2015/02/has-the-smartp
7/8/2015 4:22:15 PM...	Practical Mobile Forensics	Safari	http://www.amazon.com/Practical-Mobile-Forensics-
7/8/2015 4:25:50 PM...	facebook - Google Search	Safari	https://www.google.com/search?...
7/8/2015 4:25:53 PM...	Welcome to Facebook	Safari	https://m.facebook.com/



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