

NEW & IMPROVED!
Version 2.0!

Smartphone and Network Forensics go Together Like Peas and Carrots

Phil Hagen | @philhagen
Heather Mahalik | @heathermahalik



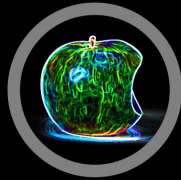
SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

FOR408
Windows Forensics



FOR518
Mac Forensics



FOR526
Memory Forensics
In-Depth



FOR585
Advanced Smartphone
Forensics



OPERATING
SYSTEM &
DEVICE
IN-DEPTH

INCIDENT
RESPONSE &
ADVERSARY
HUNTING



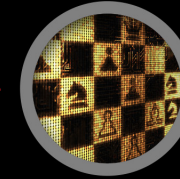
FOR508
Advanced Incident Response



FOR572
Advanced Network Forensics
and Analysis



FOR578
Cyber Threat Intelligence



FOR610
REM: Malware Analysis



SEC504
Hacker Tools, Techniques,
Exploits, and Incident Handling



MGT535
Incident Response
Team Management



@sansforensics



sansforensics



dfir.to/DFIRLinkedInCommunity



dfir.to/gplus-sansforensics



dfir.to/MAIL-LIST

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
- Version 2 designed to dive deeper into interesting findings and address great questions raised from previous talk

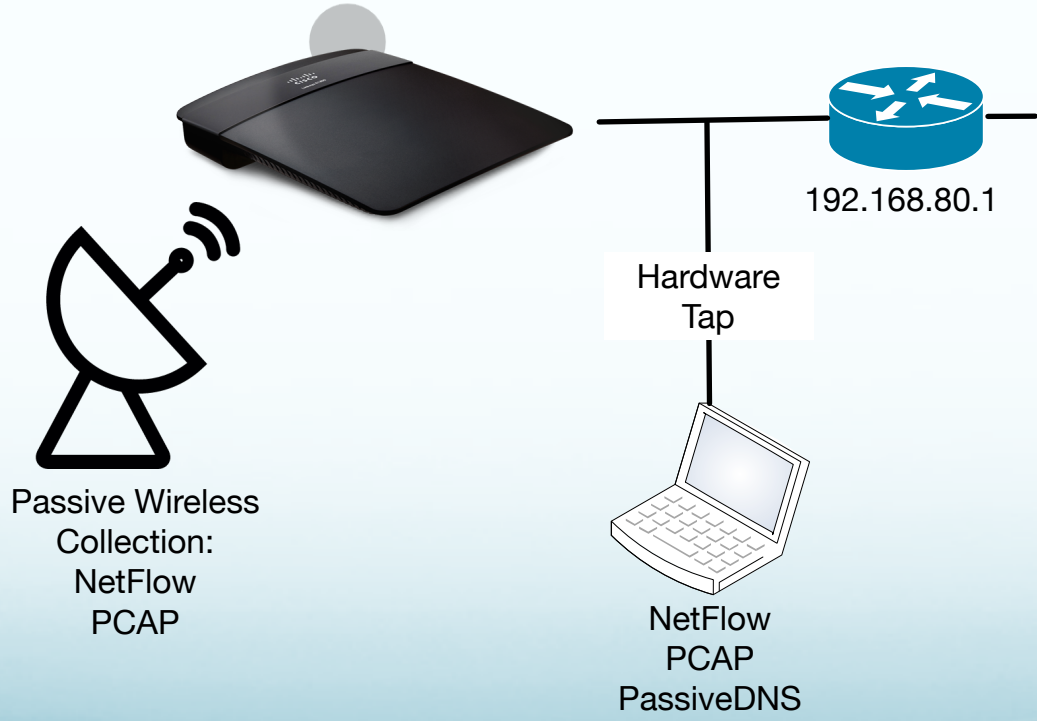
The Plan

- Associate all devices to wireless access point
- Capture all network traffic via tap inside gateway
- Capture wireless traffic
- Conduct typical activity on smartphone devices
- Acquisition on two iPhones and Android
- Network traffic examination from all traffic

Assumptions

- Smartphones
 - Passcodes are known or “crackable”
 - User did not wipe or delete the data
- Network
 - Legal permission to capture wired and wireless
 - Passphrase to WPA2 wireless network

The Setup





Evidence Used

Device-based

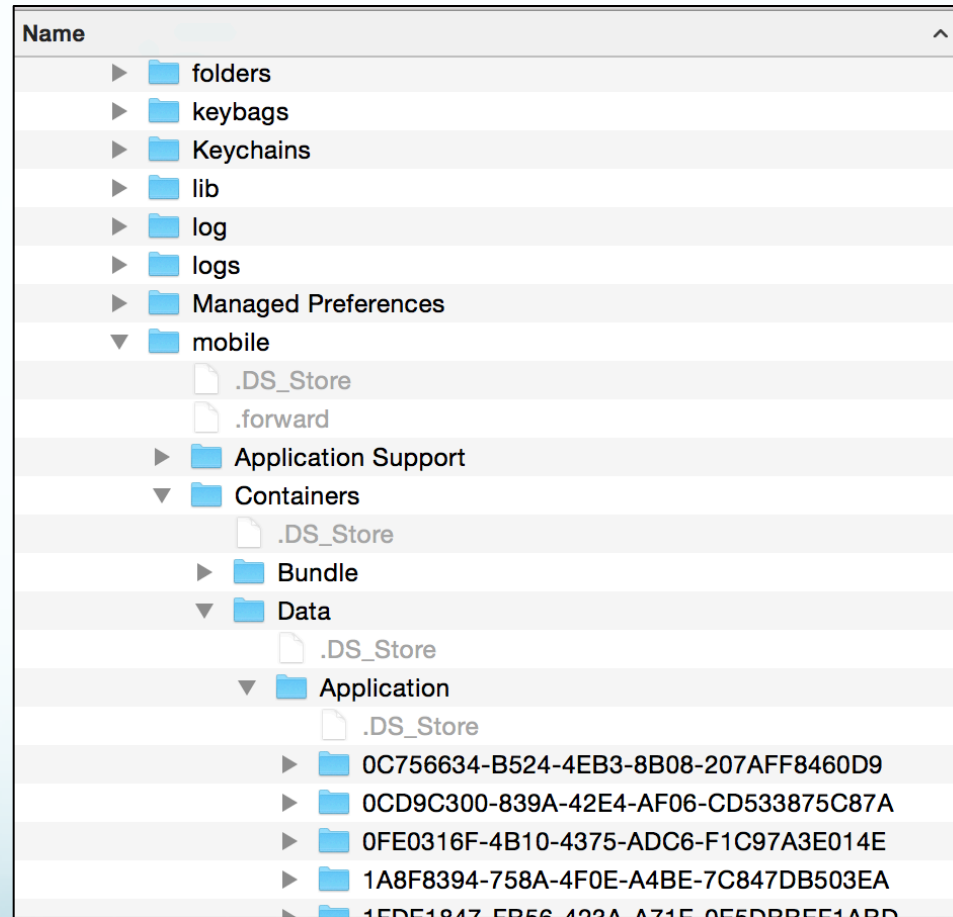
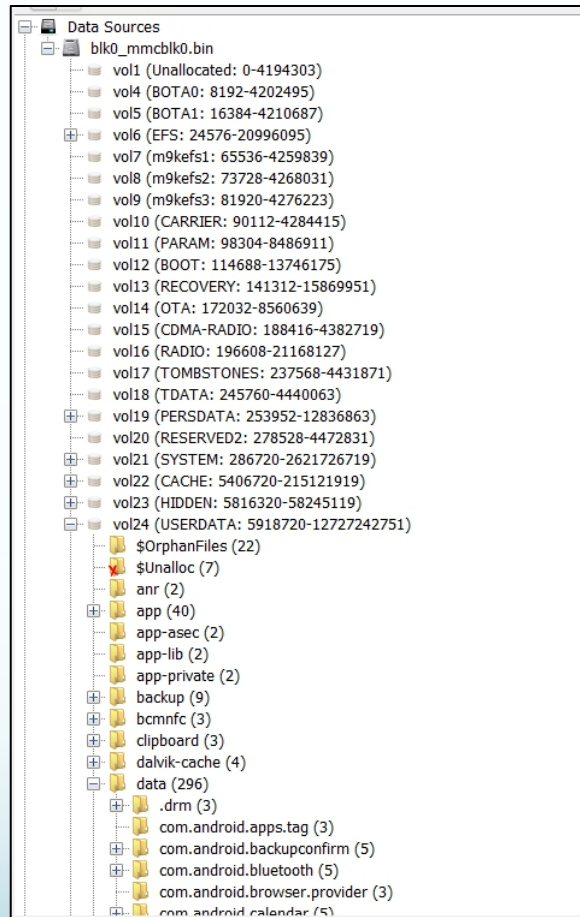
- Jailbroken iPhone 6
 - Advanced logical acquisition
 - Easiest acquisition for jailbroken iOS devices with A7+ chip
- Rooted Samsung Galaxy S5
 - Physical dump
 - Best option when available (assuming the device isn't encrypted)
- Commercial and Open Source tools

Network-based

- NetFlow
 - Statistical traffic abstraction: all metadata – no content
 - From tap and wireless
- Full packet capture
 - ALL content of network communications
 - From tap and wireless
- PassiveDNS logs
 - ASCII logs detailing all DNS queries and responses



Filesystem Dump





Device Arrival

```

6E 74 65 72 6E 65 74 5F 63 68 65 63 6B 3D 30 0A 7D 0A 0A 6E 65 74
77 6F 72 6B 3D 7B 0A 09 73 73 69 64 3D 22 70 65 61 73 2D 63 61 72
72 6F 74 73 22 0A 09 70 73 6B 3D 30 65 39 61 32 36 63 37 35 37 35
65 36 34 39 63 37 34 37 62 32 62 33 31 36 30 31 64 38 37 33 30 0A
09 6B 65 79 5F 6D 67 6D 74 3D 57 50 41 2D 50 53 4B 0A 09 70 72 69
6F 72 69 74 79 3D 33 0A 09 66 72 65 71 75 65 6E 63 79 3D 32 34 33
32 0A 09 61 75 74 6F 6A 6F 69 6E 3D 31 0A 09 75 73 61 62 6C 65 5F
69 6E 74 65 72 6E 65 74 3D 31 0A 09 73 6B 69 70 5F 69 6E 74 65 72
6E 65 74 5F 63 68 65 63 6B 3D 30 0A 7D 0A

```

```

internet_check=0.}.net
work={..ssid="peas-car
rots"..psk=0e9a26c7575
e649c747b2b31601d8730.
.key_mgmt=WPA-PSK..pri
ority=3..frequency=243
2..autojoin=1..usable_
internet=1..skip_inter
net_check=0.}.

```

CHANNEL_CLASS	integer	10
CHANNEL_WIDTH	integer	20
FT_ENABLED	boolean	true
IE	data	...
NOISE	integer	0
ORIG_AGE	integer	41
PHY_MODE	integer	
RATES	array	
RSN_IE	dict	
RSSI	integer	
SCAN_RESULT_FRO	boolean	
SNR	integer	
SSID	data	
SSID_STR	string	
ScaledRSSI	real	
ScaledRate	real	
SecurityMode	string	
Strength	real	
WEPKeyLen	integer	
WiFiManagerKnow	integer	
authMode	integer	
isValid	boolean	
isWPA	integer	
lastAutoJoined	date	
lastJoined	date	

Follow TCP Stream (tcp.stream eq 808) · peascarrots_v2_tap_all-ip

Wireshark · Follow TCP Stream (tcp.stream eq 7) · peascarrots_v2_tap_all-ip

```

GET /lp7w1KxUs/OTMfc2vg0/Mr1RVpHRf/YPMYriReZ/xgsGb3T79.html HTTP/1.0
Host: captive.apple.com
Connection: close
User-Agent: CaptiveNetworkSupport-306.20.1 wispr

HTTP/1.0 200 OK
Content-Type: text/html
Content-Length: 68
Date: Sat, 06 Feb 2016 21:26:40 GMT
Connection: close

<HTML><HEAD><TITLE>Success</TITLE></HEAD><BODY>Success</BODY></HTML>

```



FaceTime Audio, Video Device-Device Calls

<input checked="" type="checkbox"/>	8	★			To: +1703[redacted]
<input checked="" type="checkbox"/>	7	★			From: phil-apple@[redacted]
<input checked="" type="checkbox"/>	6	★		📹	To: nevie@i[redacted]
<input checked="" type="checkbox"/>	5	★		📹	To: +1703[redacted]
<input checked="" type="checkbox"/>	4	★			To: +1703[redacted]
<input checked="" type="checkbox"/>	3	★		📹	To: +1703[redacted]
<input type="checkbox"/>	2			📹	From: (571) [redacted] To: [redacted]

1 = Cellular
 8 = FT Video
 16 = FT Audio

Icon = FT Video **only via WiFi!**

```
SELECT ZCALLRECORD.ZCALLTYPE,
ZCALLRECORD.ZDATE,
ZCALLRECORD.ZDURATION,
ZCALLRECORD.ZADDRESS,
ZCALLRECORD.ZNAME
FROM ZCALLRECORD
```

Results, Rows = 19

ZCALLTYPE	ZDATE	ZDURATION	ZADDRESS
1	2016/02/06 21:29:17	69	+1703[redacted]
16	2016/02/06 21:31:20	75	phil-apple@[redacted]
8	2016/02/06 21:33:34	77	nevie@i[redacted]
8	2016/02/06 21:35:55	0	+1703[redacted]
1	2016/02/06 21:36:06	24	+1703[redacted]
8	2016/02/06 21:36:29	61	+1703[redacted]
1	2015/08/11 11:15:04	0	571[redacted]
1	2015/08/11 18:50:15	0	703[redacted]
8	2015/08/12 11:21:26	0	+15712[redacted]
1	2015/08/12 16:11:36	0	610[redacted]

FaceTime Audio, Video Device-Device Calls

Tap

```
pc@sift:$ nfdump -R 2016/ -t '2016/02/06.21:31-2016/02/06.21:38' 'proto tcp and (host 192.168.80.12 or host 192.168.80.6) and not (port 80 or port 443)'
Date first seen      Duration Proto      Src IP Addr:Port      Dst IP Addr:Port      Packets  Bytes Flows
2016-02-06 21:31:16.154  139.278 TCP        192.168.80.12:49337 -> 17.172.239.61:5223     57      26886   1
2016-02-06 21:31:16.000  139.507 TCP        17.172.239.61:5223 -> 192.168.80.12:49337     56      14630   1
2016-02-06 21:35:53.928   72.191 TCP        192.168.80.12:49337 -> 17.172.239.61:5223     58      27408   1
2016-02-06 21:35:53.958   72.189 TCP        17.172.239.61:5223 -> 192.168.80.12:49337     54      13296   1
Summary: total flows: 4, total bytes: 82220, total packets: 225, avg bps: 1878, avg pps: 0, avg bpp: 365
```

Tap

```
192.168.80.6      192.168.80.12      STUN      198 Binding Success Response user: '@, [MAPPED-ADDRESS: 192.168.80.12:16402
192.168.80.6      192.168.80.12      STUN      198 Binding Success Response user: '@, [MAPPED-ADDRESS: 192.168.80.12:16402
192.168.80.6      192.168.80.12      STUN      186 Binding Request user: '@, [
192.168.80.6      192.168.80.12      STUN      198 Binding Success Response user: '@, [MAPPED-ADDRESS: 192.168.80.12:16402
192.168.80.12    192.168.80.6      STUN      194 Binding Success Response user: [ MAPPED-ADDRESS: 192.168.80.6:16402
192.168.80.6      192.168.80.12      STUN      378 Binding Request user: '@, [
192.168.80.12    192.168.80.6      STUN      298 Binding Success Response user: [ MAPPED-ADDRESS: 192.168.80.6:16402
192.168.80.6      192.168.80.12      SIP/SDP   801 Request: INVITE sip:user@192.168.80.12:16402 |
192.168.80.12    192.168.80.6      SIP       387 Status: 100 Trying |
192.168.80.12    192.168.80.6      SIP       438 Status: 180 Ringing |
192.168.80.12    192.168.80.6      SIP/SDP   740 Status: 200 OK |
192.168.80.6      192.168.80.12      SIP       433 Request: ACK sip:192.168.80.12:16402 |
192.168.80.6      192.168.80.12      UDP       197 16402 -> 16402 Len=87
192.168.80.6      192.168.80.12      UDP       197 16402 -> 16402 Len=87
```

WiFi

```
pc@sift:$ nfdump -R 2016/ 'host 192.168.80.12 and host 192.168.80.6'
Date first seen      Duration Proto      Src IP Addr:Port      Dst IP Addr:Port      Packets  Bytes Flows
2016-02-06 21:31:19.637   75.417 UDP        192.168.80.12:16402 -> 192.168.80.6:16402     3673    452444   1
2016-02-06 21:31:19.937   75.146 UDP        192.168.80.6:16402 -> 192.168.80.12:16402     3580    548290   1
2016-02-06 21:36:29.432   61.156 UDP        192.168.80.12:16402 -> 192.168.80.6:16402    12440   12.1 M   1
2016-02-06 21:36:29.000   61.646 UDP        192.168.80.6:16402 -> 192.168.80.12:16402     9373    3.4 M   1
Summary: total flows: 4, total bytes: 16582386, total packets: 29066, avg bps: 357562, avg pps: 78, avg bpp: 570
Time window: 2016-02-06 21:26:35 - 2016-02-06 22:54:02
Total flows processed: 10743, Blocks skipped: 0, Bytes read: 517272
Sys: 0.016s flows/second: 671437.5 Wall: 0.005s flows/second: 1828595.7
```



Web Activity

IEF Report Viewer v6.7.3.0370 - Examiner Mode - Case: Not entered

Licensing Help

Go To #: Search:

Count	#	Search Term	URL	Date/Time - (UTC) (..)	Web Page Title	Original Search Query
83	45	mupoets	https://www.google.com/search?q=mupoets&rlz=1CD...	02/06/2016 09:42:49 ..		mupoets
	19	mupoets	https://www.google.com/search?q=mupoets&rlz=1CD...	02/06/2016 09:42:48 ..	mupoets - Google Search	mupoets
	39	mupoets	https://www.google.com/search?q=mupoets&rlz=1CD...	02/06/2016 09:42:48 ..	mupoets - Google Search	mupoets
	22	practical mobile forensi...	https://www.google.com/search?q=practical+mobile+f...	02/06/2016 09:41:47 ..	practical mobile forensics - Google Search	practical mob
	38	practical mobile forensi...	https://www.google.com/search?q=practical+mobile+f...	02/06/2016 09:41:47 ..	practical mobile forensics - Google Search	practical mob
	46	practical mobile forensi...	https://www.google.com/search?q=practical+mobile+f...	02/06/2016 09:41:47 ..	practical mobile forensics - Google Search	practical mob
	20	practical mobile forensi...	https://www.google.com/search?q=practical+mobile+f...	02/06/2016 09:41:26 ..	practical mobile forensics - Google Search	practical mob
	37	practical mobile forensi...	https://www.google.com/search?q=practical+mobile+f...	02/06/2016 09:41:26 ..	practical mobile forensics - Google Search	practical mob
	36	mupoets	https://www.google.com/search?q=mupoets&rlz=1CD...	02/06/2016 09:41:10 ..	mupoets - Google Search	mupoets
	35	mupoets	https://www.google.com/search?q=mupoets&rlz=1CD...	02/06/2016 09:41:09 ..	mupoets - Google Search	mupoets

Restore
 Move
 Size
 Minimize
 Maximize
 Close Alt+F4

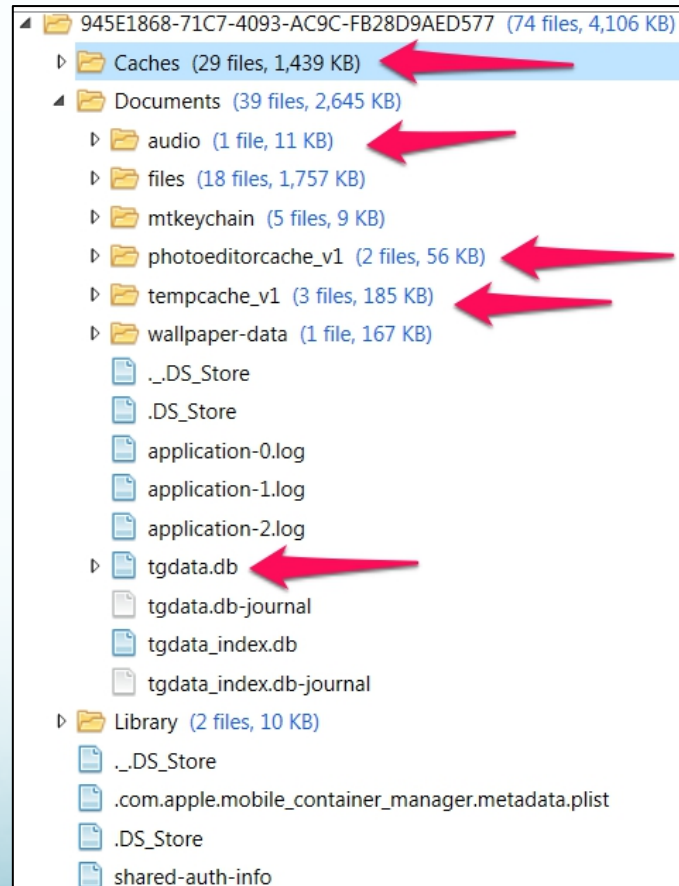
- Classified URLs
- Facebook URLs
- Google Analytics First Visit Cookies
- Google Analytics Referral Cookies
- Google Analytics Session Cookies
- Google Analytics URLs
- Google Searches
- Identifiers
- Parsed Search Queries

```

GET /Practical-Mobile-Forensics-Satish-Bommisetty/dp/1783288310 HTTP/1.1
Host: www.amazon.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,image/webp
Referer: https://www.google.com/
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) GSA/12.0.68608 Mobile/12F70 Safari/600.1.4
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en
  
```

Telegram Chats

- Messaging application, including private secure chat





Telegram Chats

```
pc@sift:~$ grep telegram passivedns.log
pc@sift:~$ grep tele passivedns.log
pc@sift:~$
```

No.	Time	Source
30813	2016-02-06 21:46:07.358113	192.168.80.1
30814	2016-02-06 21:46:07.400140	149.154.175.50
30815	2016-02-06 21:46:07.402850	192.168.80.1
30816	2016-02-06 21:46:07.419599	192.168.80.1
30817	2016-02-06 21:46:07.460977	149.154.175.50
30818	2016-02-06 21:46:07.463306	192.168.80.1
30819	2016-02-06 21:46:07.486474	192.168.80.1
30820	2016-02-06 21:46:07.527643	149.154.175.50
30821	2016-02-06 21:46:07.536492	192.168.80.1
30822	2016-02-06 21:46:07.536537	192.168.80.1
30823	2016-02-06 21:46:07.587619	149.154.175.50
30824	2016-02-06 21:46:07.589790	192.168.80.1
30825	2016-02-06 21:46:07.595249	149.154.175.50
30826	2016-02-06 21:46:07.596359	149.154.175.50

```
phil@mbp:~ phil$ whois 149.154.175.50
inetnum:        149.154.172.0 - 149.154.175.255
netname:        Telegram_Messenger_Network
descr:          Telegram Messenger Network
country:        gb
admin-c:        ND2624-RIPE
tech-c:         ND2624-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-TELEGRAM
created:        2014-09-19T22:27:16Z
last-modified: 2014-09-19T22:27:16Z
source:         RIPE

person:         Nikolai Durov
address:        P.O. Box 146, Road Town, Tortola, British Virgin Islands
phone:          +357 96 287319
nic-hdl:        ND2624-RIPE
mnt-by:         MNT-TELEGRAM
created:        2014-03-07T19:25:00Z
last-modified: 2014-03-08T03:31:36Z
source:         RIPE

% Information related to '149.154.172.0/22AS59930'

route:          149.154.172.0/22
descr:          Telegram Messenger Network
origin:         AS59930
mnt-by:         MNT-TELEGRAM
created:        2014-10-15T14:23:11Z
last-modified: 2014-10-15T14:23:11Z
source:         RIPE
```

Wireshark - Follow TCP Stream (tcp.stream eq 587) - peascarrots_v2_tap_all-ip

```
...5... t]
...s...}.a..4.)]c*..#.p%.:a..1..7...!P, .y.v..}
...OU.i.z.:
!S...h...!.$..#}...&.h...x.*.?....@^..aD...e6.T`
!0.}j...w...9...Xi..]...AQP.UT.....E.
.T.v.M8v...5Mb..1..a..y.>..{K..x...y...e.
.../<'R...k..._I.P..?uD.}...c...I\...V.C.P.y...9..r.

./..4...7.v..Y. [.I.W~(T..xw.r...)]Q...yBG.....<..h...
b..0.....Wm..i...=0..2...K.9.T.....a.~+.$...C5....
dZ.S...Z....."..h...w~..Y...!L..e ^V.J...5.....

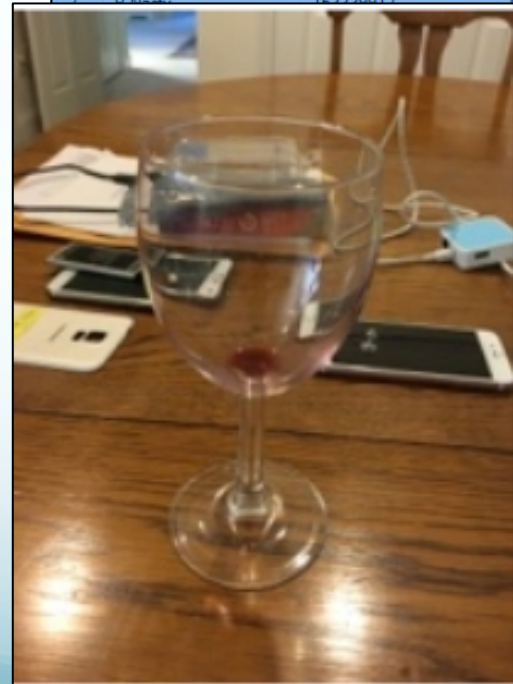
s.)*/..ri8.....:h.....=JX.%+.o.o.J..o.x.L.
...c).....@...!...p.}.t....
...n...w...7..].X.....+U....I..
R*.....nIV.a..KXB.....h...P0.H...W.+K.
...A...N...Fr.....+..L..u...4BP?...$F...<=..~..
e/<!.|.FaA...-".|...l.....h.....(....^Q..(.B.%...
A.....<
...ah..|g.9...-C.d..3..u.uj.;...h.....g...#..Ll...|
]wk...Z...S]9..... A
V...p.f...?....[.U.O. ....<....r{ST...4.m.c.....
|.p*M>.Y...}....O.'K...GPb.|...dy.f...G...x.B..a.
...~7~...X+Z.c..DPE.....A...h.....[.jW!..b.K.2...
.)y.$...6.<.dA"...=Z0^...: &.r..P..Y...E48..6....f.
...&.D=<.M..
|.v~.4r.5.d.q.Bf...h.....#.$...8...M...C...o
5..c...0.\...n...%...o.<.05..7,...36%..Z.....W}.H.

A.QYG0Dc...:../.7D.....+?8..0...qzf%:.....M
..I..=H(( ..T<'....[';.]I.0...p.>.i...
)!qeC.>pg.....(S.J.....n..h.....
..o? .8.Vt?.t%....,0..m*.|X..). ...._".Y....&...5,w.
Zoa..
..@..wr.....?.....N.....H.AD.....:~.y...D...thK.
```



Telegram Chats

46		777000	Martha Vines	162132182	New in version 3.4:...	02/06/2016 09:46:07 ...
38	Martha Vines	162132182	P Nasty	153339917		02/06/2016 09:46:54 ... <click to v
39	Martha Vines	162132182	P Nasty	153339917	I'm drinking your beer!	02/06/2016 09:47:01 ...
40	P Nasty	153339917	Martha Vines	162132182	Oh shit	02/06/2016 09:47:06 ...
41	P Nasty	153339917	Martha Vines	162132182	It's on	02/06/2016 09:47:09 ...
6	P Nasty	153339917	Martha Vines	162132182		02/06/2016 09:48:38 ... <click to v
7	P Nasty	153339917	Martha Vines	162132182	I drank your wine	02/06/2016 09:48:44 ...
				-2147483650	Oh no!!!!	02/06/2016 09:49:03 ...
				-2147483650	Must chug the beer	02/06/2016 09:49:10 ...



3786aa57bbfca7d97	2/6/2016 4:48 PM	File
d0df941604d2d0b40	2/6/2016 4:46 PM	File





Samsung Call Join

Close Case + Add Data Source Generate Report

com.sec.android.p
cache (2)
databases (4)
com.sec.android.p
com.sec.android.p
com.sec.android.R
com.sec.android.s
com.sec.android.s
com.sec.android.s
com.sec.android.s
com.sec.android.s
com.sec.android.v
com.sec.android.v
com.sec.android.v
com.sec.android.v

```
SELECT logs_id,  
logs.number,  
logs.address,  
logs.date,  
logs.duration,  
logs.type,  
logs.new,  
logs.geocoded_location
```

Results, Rows = 8

_id	number	address	date	duration	type	new	geocoded_location
2	703-		2016/01/25 16:20:17	67	2	0	Virginia
1	111-		2016/01/25 16:20:35	0	1	0	
3	703-		2016/01/25 16:21:57	0	2	0	Virginia
4	+11		2016/01/25 16:22:38	0	1	0	
6	703-		2016/02/06 22:11:18	81	2	1	Virginia
7	703-		2016/02/06 22:12:08	33	2	1	Virginia
8	703-		2016/02/06 22:13:31	10	2	1	Virginia
5	703-		2016/02/06 21:16:33	0	2	0	Virginia

roid.provider.logsprovider/databases

Change Time	Access T
2015-09-02 04:03:27 UTC	2015-09-0
2015-09-02 04:03:27 UTC	2015-09-0
2016-02-08 14:46:55 UTC	2015-09-0
2016-02-06 22:13:48 UTC	2015-09-0



Samsung Call Join





Twitter Activity

```
pc@sift:$ grep twitter passivedns.log |grep 192.168.80.13
1454796908.905159|192.168.80.13|192.168.80.1|IN|platform.twitter.com.||CNAME||cs472.wac.edgecastcdn.net.||11||1
1454797069.091571|192.168.80.13|192.168.80.1|IN|twitter.com.||A||199.16.156.6||27||1
1454797069.092616|192.168.80.13|192.168.80.1|IN|mobile.twitter.com.||A||199.16.156.107||2||1
1454797069.092616|192.168.80.13|192.168.80.1|IN|mobile.twitter.com.||A||199.16.156.43||2||1
1454798548.352627|192.168.80.13|192.168.80.1|IN|twitter.com.||A||199.16.156.6||28||6
1454798548.352627|192.168.80.13|192.168.80.1|IN|twitter.com.||A||199.16.156.102||29||8
1454798548.352627|192.168.80.13|192.168.80.1|IN|twitter.com.||A||199.16.156.230||29||10
```

ID	Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
1454	2016-02-06 22:15:11.510	47.060	TCP	192.168.80.13:54000 ->	199.16.156.200:443	20	1944	1
1454	2016-02-06 22:15:11.510	47.060	TCP	192.168.80.13:42126 ->	199.16.156.75:443	14	1678	1
1454	2016-02-06 22:15:11.541	46.998	TCP	199.16.156.75:443 ->	192.168.80.13:42126	15	5011	1
1454	2016-02-06 22:15:11.542	46.997	TCP	199.16.156.200:443 ->	192.168.80.13:54000	16	4830	1
1454	2016-02-06 22:17:49.138	0.610	TCP	192.168.80.13:52613 ->	199.16.156.70:443	11	1918	1
1454	2016-02-06 22:17:49.138	0.640	TCP	192.168.80.13:45793 ->	199.16.156.107:443	12	1582	1
1454	2016-02-06 22:17:49.138	0.790	TCP	192.168.80.13:59808 ->	199.16.156.104:443	16	3212	1
1454	2016-02-06 22:17:49.169	0.704	TCP	199.16.156.104:443 ->	192.168.80.13:59808	14	10397	1
1454	2016-02-06 22:17:49.169	0.525	TCP	199.16.156.70:443 ->	192.168.80.13:52613	8	4507	1
1454	2016-02-06 22:17:49.171	0.562	TCP	199.16.156.107:443 ->	192.168.80.13:45793	11	6119	1
1454	2016-02-06 22:17:49.828	0.240	TCP	192.168.80.13:56516 ->	199.16.156.104:443	7	1815	1
1454	2016-02-06 22:17:49.828	0.265	TCP	192.168.80.13:36250 ->	199.16.156.104:443	7	1551	1
1454	2016-02-06 22:17:49.859	0.204	TCP	199.16.156.104:443 ->	192.168.80.13:56516	7	1353	1
1454	2016-02-06 22:17:49.859	0.209	TCP	199.16.156.104:443 ->	192.168.80.13:36250	7	1494	1
	2016-02-06 22:17:59.381	120.422	TCP	192.168.80.13:35499 ->	199.16.156.72:443	445	30875	1
	2016-02-06 22:17:59.410	120.384	TCP	199.16.156.72:443 ->	192.168.80.13:35499	684	648401	1
	2016-02-06 22:18:32.535	8.593	TCP	192.168.80.13:51956 ->	199.16.156.230:443	15	3596	1
	2016-02-06 22:18:32.565	8.264	TCP	199.16.156.230:443 ->	192.168.80.13:51956	14	4787	1
	2016-02-06 22:18:37.487	21.304	TCP	192.168.80.13:57021 ->	199.16.156.199:443	12	2042	1
	2016-02-06 22:18:37.519	21.245	TCP	199.16.156.199:443 ->	192.168.80.13:57021	12	4888	1
	2016-02-06 22:18:57.050	52.711	TCP	192.168.80.13:45734 ->	199.16.156.38:443	17	7352	1
	2016-02-06 22:18:57.082	52.639	TCP	199.16.156.38:443 ->	192.168.80.13:45734	12	1856	1
	2016-02-06 22:19:58.263	0.570	TCP	192.168.80.13:42409 ->	199.16.156.102:443	13	6024	1
	2016-02-06 22:19:58.295	0.526	TCP	199.16.156.102:443 ->	192.168.80.13:42409	9	1154	1



Twitter Activity

The screenshot displays a forensic analysis tool interface. At the top, there is a header for an "Installed Application" named "Twitter". Below this, a file explorer window shows a directory listing for the path `/img_blk0_mmcbk0.bin/vol_vol24/data/com.twitter.android/databases`. A red arrow points to this directory listing. The listing shows a table with columns for Name, Modified Time, and Change Time. Below the directory listing, a message log is visible, showing a message from "HeatherMahalik" to "Phil Hagen" with the text "Hello my name is hank. I like ...". A "Details" pane at the bottom provides more information about the selected message, including the direction (Outgoing message), remote party (Phil Hagen), text, and time stamp.

Name	Modified Time	Change Time
[current folder]	2016-02-06 22:20:31 UTC	2016-02-06 22:20:31 UTC

Direction	Remote party	Text	Time stamp (Device time)
➡	Phil Hagen	Sweet	2/6/2016 10:27:52 PM
➡	Phil Hagen	☐	2/6/2016 10:27:22 PM
➡	Phil Hagen	Hello my name is hank. I like ...	2/6/2016 10:26:30 PM

Details

Direction: ➡ (Outgoing message)
Remote party: Phil Hagen
Text: Hello my name is hank. I like whiskey
Time stamp (Device time): 2/6/2016 10:26:30 PM (+00:00 UTC)



Profiling: iOS

- User Agent strings
 - 192.168.1.6 (iPhone 6S)

```
102 Mozilla/5.0 (iPhone; CPU iPhone OS 9_2_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13D15 Safari/601.1
45 News/351 CFNetwork/758.2.8 Darwin/15.0.0
14 Mozilla/5.0 (iPhone; CPU iPhone OS 9_2_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Mobile/13D15 [FBAN/FBIO;FBAV/48.0.0
;FBSV/9.2.1;FBSS/2: FBCR/AT&T;FBID/phone:FBLC/en US:FBOP/5]
13 Mozilla/5.0 (iPhone; CPU iPhone OS 9_2_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Mobile/13D15
3 securityd (unknown version) CFNetwork/758.2.8 Darwin/15.0.0
3
2 T84QZS65DQ.com.facebook.Facebook
2 server-bag [watch OS,9.2.1,135661,watch1,2]
2 server-bag [iPhone OS,9.2.1,13D15,iPhone8,1]
2 Search%20Framework/1.0 CFNetwork/758.2.8 Darwin/15.0.0
2 com.apple.invitation-registration [iPhone OS,9.2.1,13D15,iPhone8,1]
1 MobileAsset/1.1
1 iPhone8,1/9.2.1 (13D15)
```

- 192.168.1.12 (Jailbroken iPhone 6)

```
233 Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) CriOS/47.0.2526.107 Mobile/12F70 Safari/600.1.4
177 Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) GSA/12.0.68608 Mobile/12F70 Safari/600.1.4
131 AppStore/2.0 iOS/8.3 model/iPhone7,2 build/12F70 (6; dt:106)
36 Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12F70 Safari/600.1.4
27
6 CommCenter (unknown version) CFNetwork/711.3.18 Darwin/14.0.0
5 securityd (unknown version) CFNetwork/711.3.18 Darwin/14.0.0
3 server-bag [iPhone OS,8.3,12F70,iPhone7,2]
3 com.apple.invitation-registration [iPhone OS,8.3,12F70,iPhone7,2]
2 MobileAsset/1.1
2 iPhone7,2/8.3 (12F70)
2 CaptiveNetworkSupport-306.20.1 wispr
1 gamed/4.10.18.4.6.15.5.3.2 (iPhone7,2; 8.3; 12F70; GameKit-194.29)
1 assetsd (unknown version) CFNetwork/711.3.18 Darwin/14.0.0
```



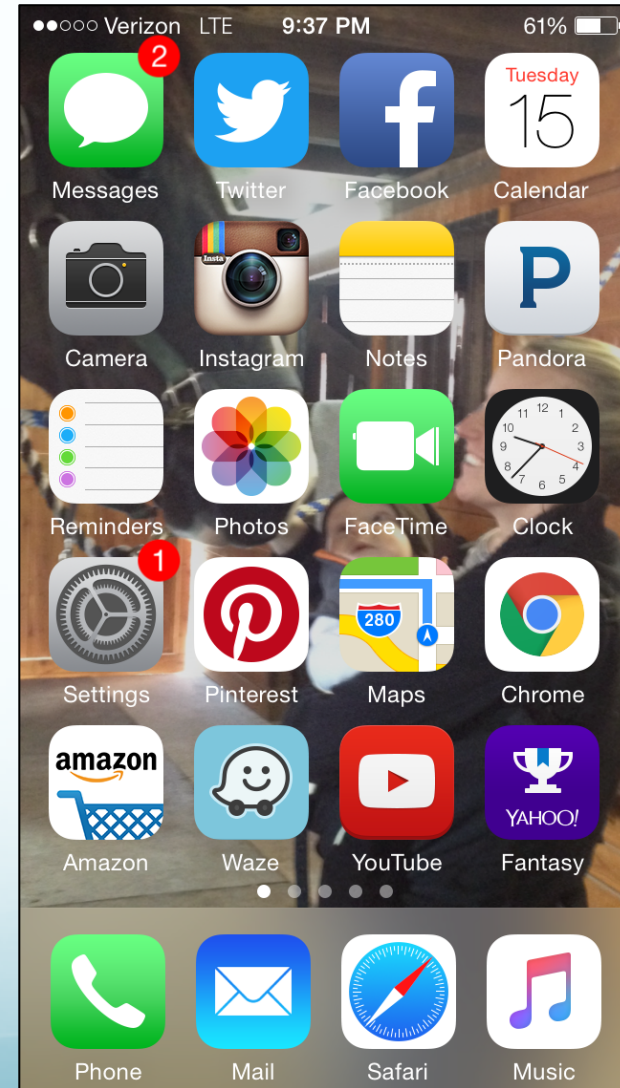
Profiling: Android

- Samsung Galaxy S5

```
510 Mozilla/5.0 (Linux; Android 5.0; SM-G900H Build/LRX21T) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.95 Mobile Safari
106 okhttp/2.3.0
79 Mozilla/5.0 (Linux; Android 5.0; SM-G900H Build/LRX21T; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/47.0.2526
66 Dalvik/1.6.0 (Linux; U; Android 4.3; SM-G900H Build/JSS15J)
12 okhttp/2.1.0
10
9 Dalvik/2.1.0 (Linux; U; Android 5.0; SM-G900H Build/LRX21T)
6 unused/0 (k3g; LRX21T); gzip
4 TwitterAndroid/5.94.0 (5110031-r-844) SM-G900H/5.0 (samsung;SM-G900H;samsung;k3gxx;0;;1)
3 Mozilla/5.0 (Linux; Android 5.0; SAMSUNG SM-G900H Build/LRX21T) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/2.1 Chrom
2 SAMSUNG-Android
2 Pinterest for Android/5.8.2 (k3g; 5.0)
2 Mozilla/5.0 (Linux; Android 5.0; SM-G900H Build/LRX21T; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/47.0.2526
1 Android
```

Reality of the Smartphone

- How secure are our chats?
- One tool can't do it all
- 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?





Takeaways

- 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
 - Not when the device fails to connect
 - Have to acquire device – not always easy with mobile devices



Takeaways (2)

- Network Forensics
 - Scoping and profiling activity relatively easy for plaintext protocols
 - 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 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: GASF

<http://for585.com/course>

FOR572: Advanced Network Forensics

and Analysis: GNFA

<http://for572.com/course>

