NETWORK FORENSICS: UNCOVERING SECRETS OF MOBILE APPLICATIONS

Eric Fulton

BlackHat | Webcasts

Sponsored by: ForeScout

ROADMAP

- Introduction
- Explanation of different mobile fields
- Methods of Interception
- Case Study – Facebook Traffic
- Case Study – Identification of Installed Applications
- NFPC Contest
- Wrap-up

INTRO

- Eric Fulton, Director of Research at LMG Security
  - @Trisk3t
  - LMGSecurity.com
- Other Learning Opportunities
  - Network Forensics, BlackHat USA, July 21-24 2012
  - www.ForensicsContest.com
  - DEFCON Contest (#NFPC)
- Why Network Forensics…

MOBILE DEVICE FIELDS

- Network Forensics
- Hardware Analysis
  - NFC
  - Huawei
- File System Analysis
  - Much like traditional forensics
- Application Analysis
  - Mobile Malware
  - CarrierIQ
- Radio Analysis

MOBILE NETWORK FORENSICS

- Identifying and analyzing data sent via wireless signals
- Relatively easy to intercept
- Often contains sensitive and identifying information
- Plethora of existing tools and learning aids

METHODS OF INTERCEPTION

- GnuRadio
  - Interception GSM and CDMA signals via software defined radio
  - (or get a HAM license, see Chris Paget's talk)
  - Allows for voice, text, and data interception
- Wifi
  - Interception and MiTM of data packets
  - Especially effective with SSLSniff
  - Analysis on a corporate network (BYOD Identification)

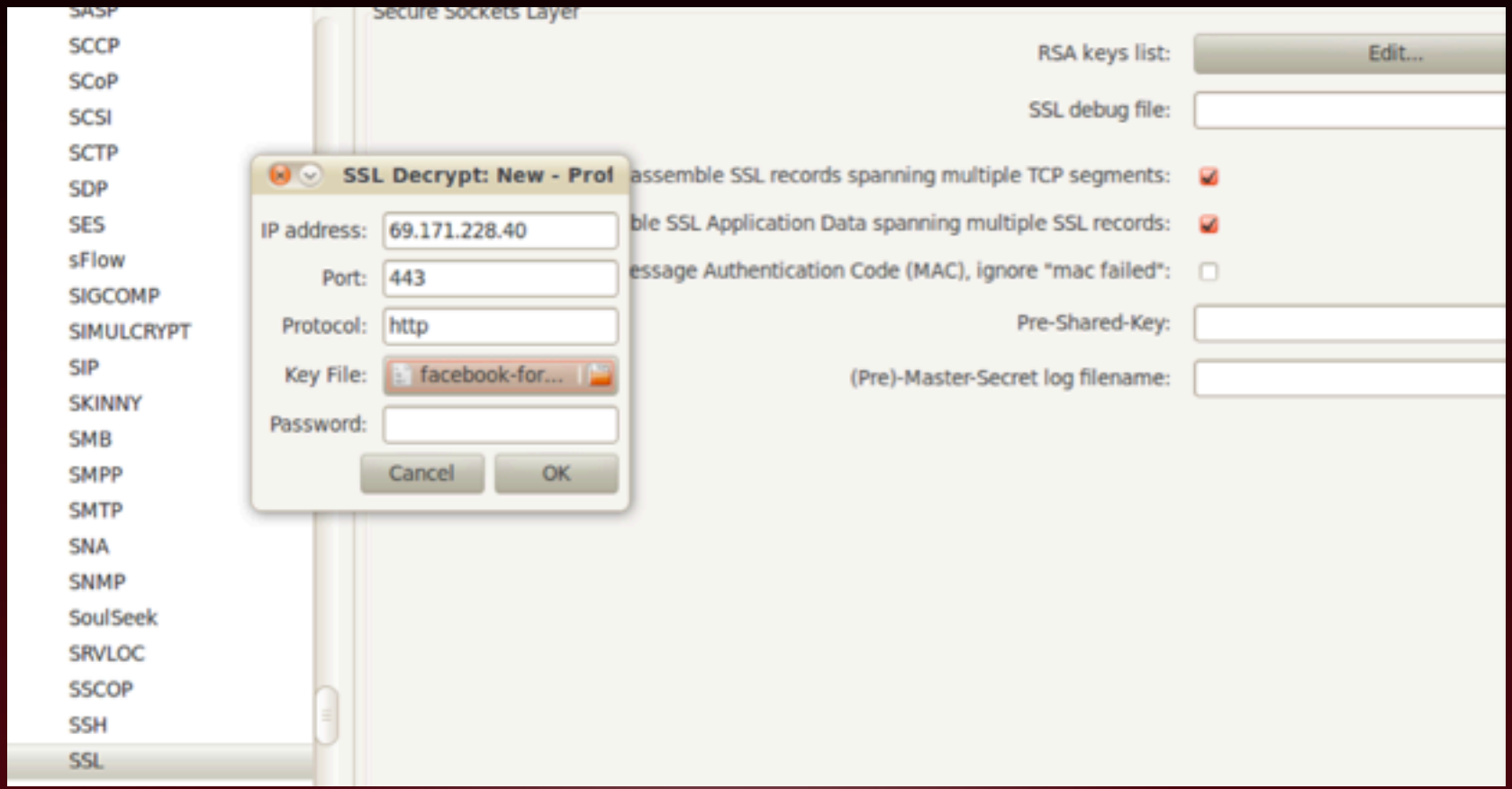
Case Study

ANALYSIS OF FACEBOOK TRAFFIC

MOBILE FACEBOOK TRAFFIC

192.168.1.128	204.2.145.74	TCP	66	43500 > https [FI
204.2.145.74	192.168.1.128	TCP	66	https > 43500 [AC
192.168.1.128	184.25.130.110	TCP	66	55206 > https [FI
184.25.130.110	192.168.1.128	TCP	66	https > 55206 [AC
192.168.1.128	69.171.228.40	TCP	66	58713 > https [FI
69.171.228.40	192.168.1.128	TCP	66	https > 58713 [AC
192.168.1.128	69.171.228.40	TCP	74	58714 > https [SY
69.171.228.40	192.168.1.128	TCP	74	https > 58714 [SY
192.168.1.128	69.171.228.40	TCP	74	58714 > https [AC
192.168.1.128	69.171.228.40	SSLv3	170	Client Hello
69.171.228.40	192.168.1.128	TCP	66	https > 58714 [AC
192.168.1.110	69.171.228.40	TCP	74	57015 > https [SY
69.171.228.40	192.168.1.110	TCP	78	https > 57015 [SY
192.168.1.110	69.171.228.40	TCP	66	57015 > https [AC
192.168.1.110	69.171.228.40	SSLv2	171	Client Hello
69.171.228.40	192.168.1.110	TLSv1	1434	Server Hello
192.168.1.110	69.171.228.40	TCP	66	57015 > https [AC
69.171.228.40	192.168.1.110	TLSv1	683	Certificate, Serv
192.168.1.110	69.171.228.40	TCP	66	57015 > https [AC

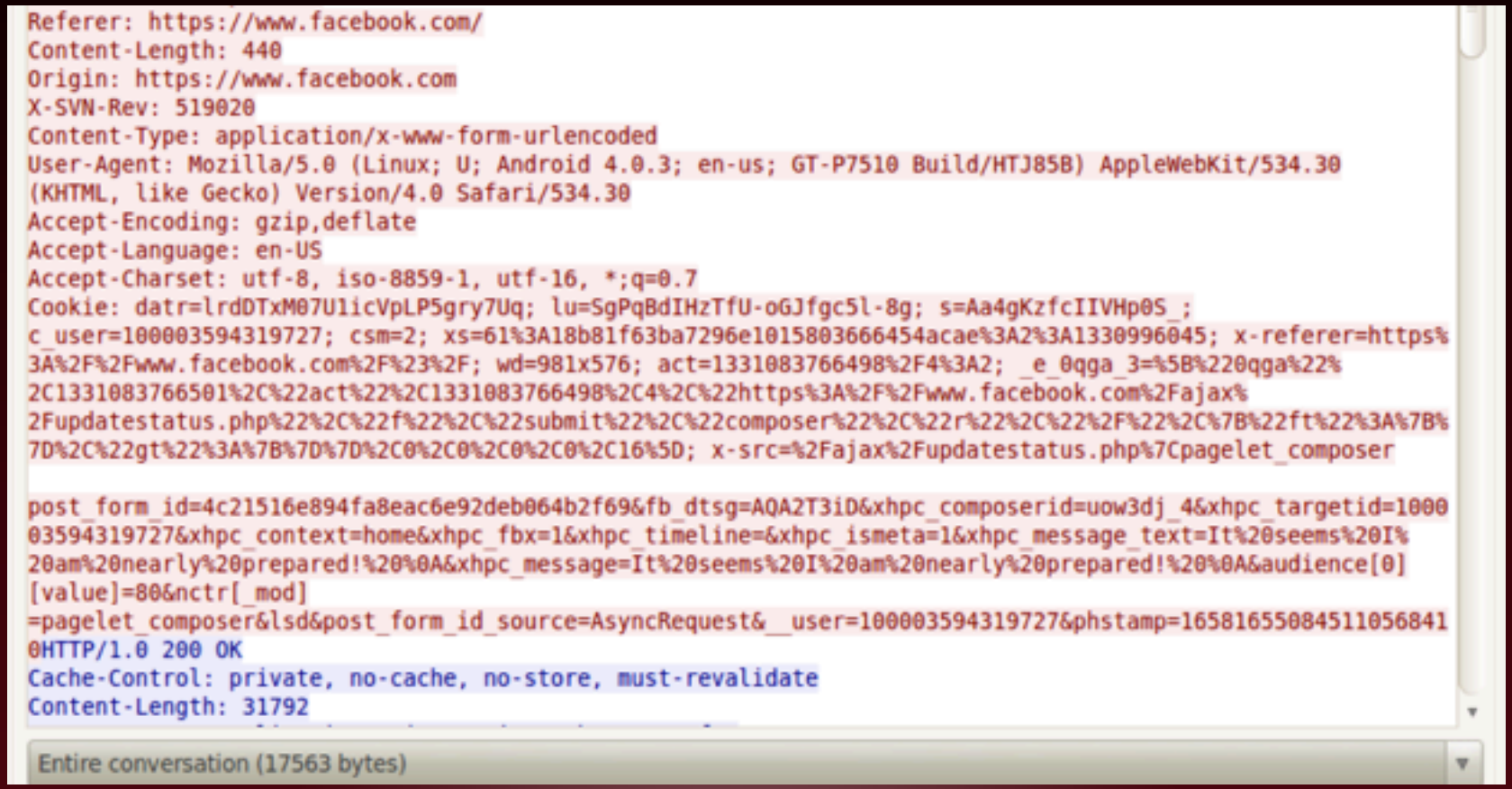
DECRYPTING IN WIRESHARK



FACEBOOK DECRYPTED

Destination	Proto	Length	Info
AsustekC_6d:5a:d8	ARP	60	Who has 192.168.1
Cisco-Li_b3:cc:ee	ARP	42	192.168.1.110 is
AsustekC_6d:5a:d8	ARP	60	Who has 192.168.1
Cisco-Li_b3:cc:ee	ARP	42	192.168.1.110 is
69.171.228.40	HTTP	828	GET / HTTP/1.1
192.168.1.128	HTTP	410	HTTP/1.0 200 OK
69.171.228.40	HTTP	1273	GET /ai.php?aed=A
192.168.1.128	HTTP	396	HTTP/1.0 200 OK
69.171.228.40	HTTP	972	GET /ajax/typeahe
192.168.1.128	HTTP	572	HTTP/1.0 200 OK
69.171.228.40	HTTP	1052	GET /ajax/typeahe
192.168.1.128	HTTP	84	HTTP/1.0 200 OK
69.171.228.40	HTTP	324	GET /ajax/typeahe
192.168.1.128	HTTP	1214	HTTP/1.0 200 OK
69.171.228.40	HTTP	572	POST /ajax/update
192.168.1.128	HTTP	1200	HTTP/1.0 200 OK
192.168.1.128	SSL	1014	[SSL segment of a
192.168.1.128	SSL	618	[SSL segment of a
192.168.1.128	SSL	1340	[SSL segment of a

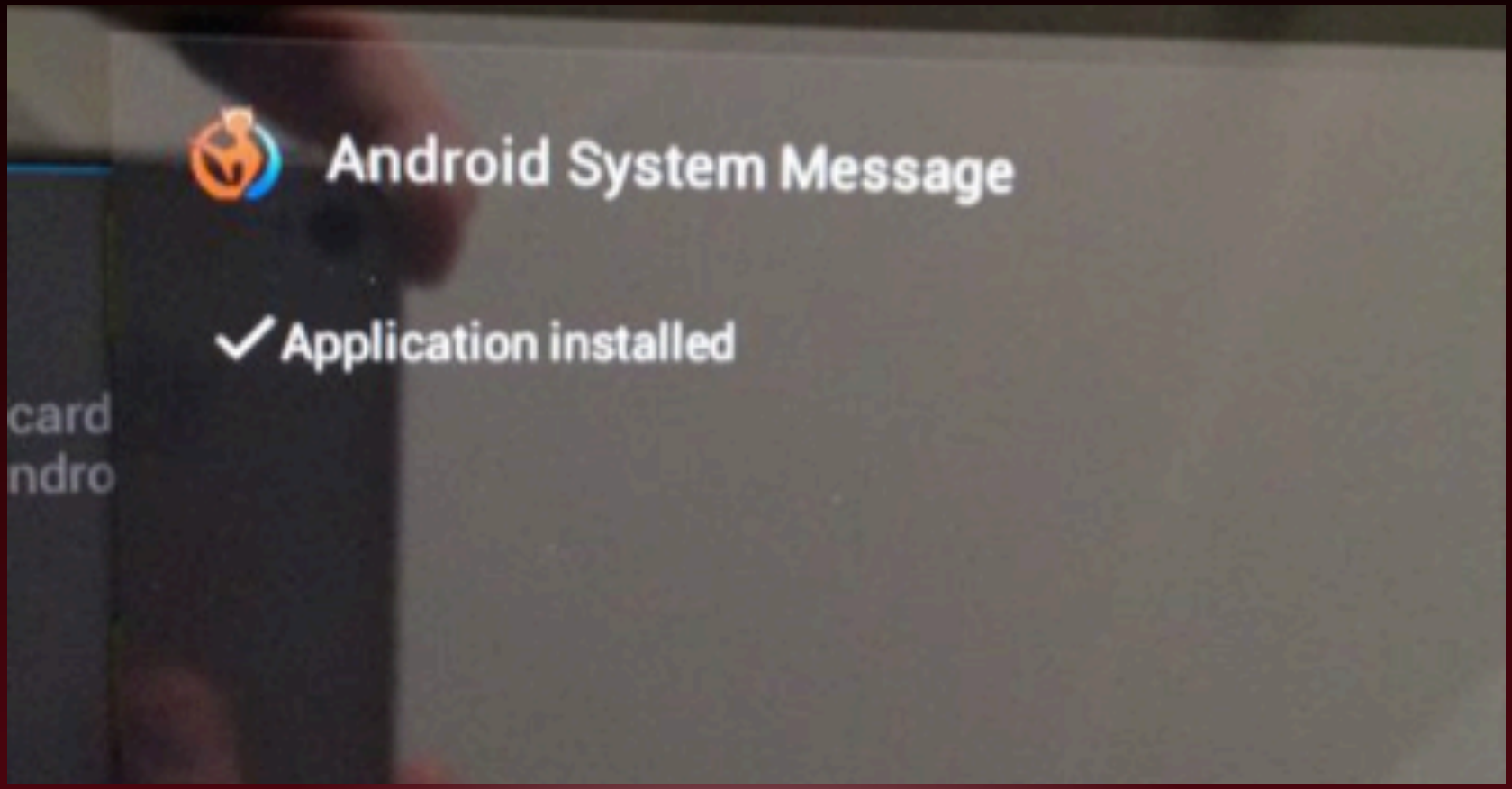
MOBILE APPLICATION STREAM ANALYSIS



Case Study

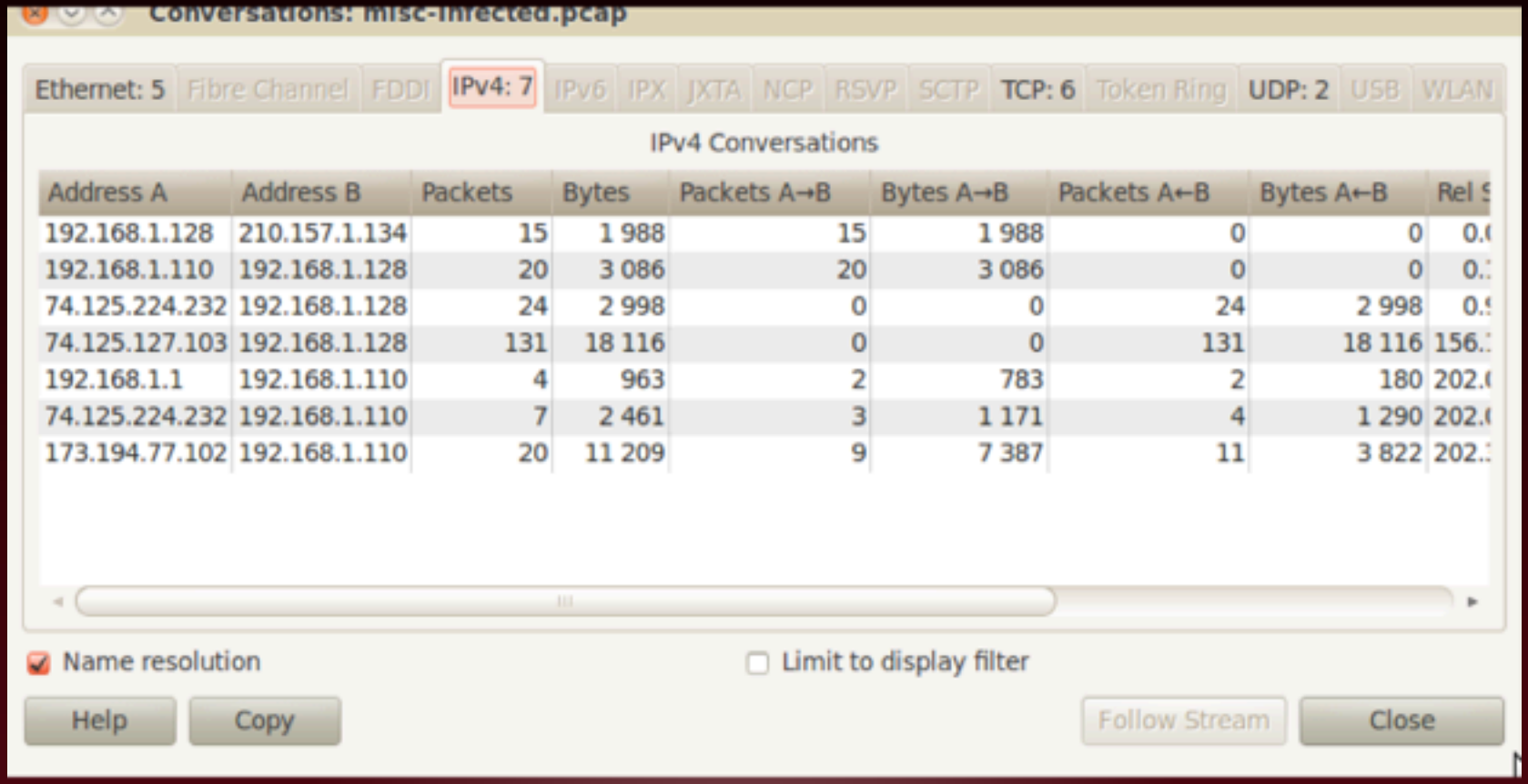
ANALYZING INSTALLED APPLICATIONS

HERE IS AN INSTALLED APPLICATION



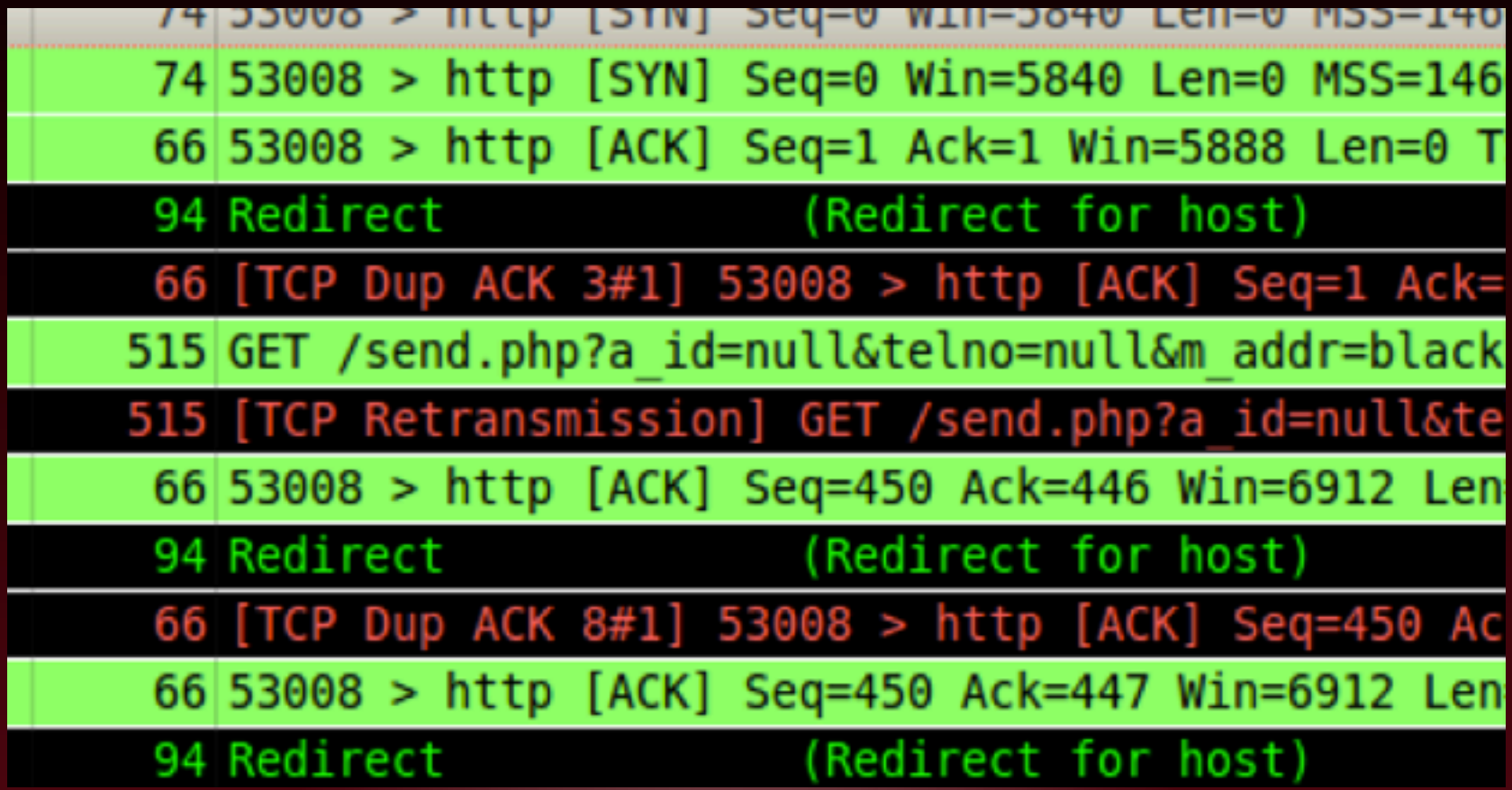
QUESTIONS TO KEEP IN MIND

- How do you identify installed applications when you don't own the device?
- Can you determine the intent of the application via network traffic?
- Are you able to identify sensitive information being exfiltrated by an application?

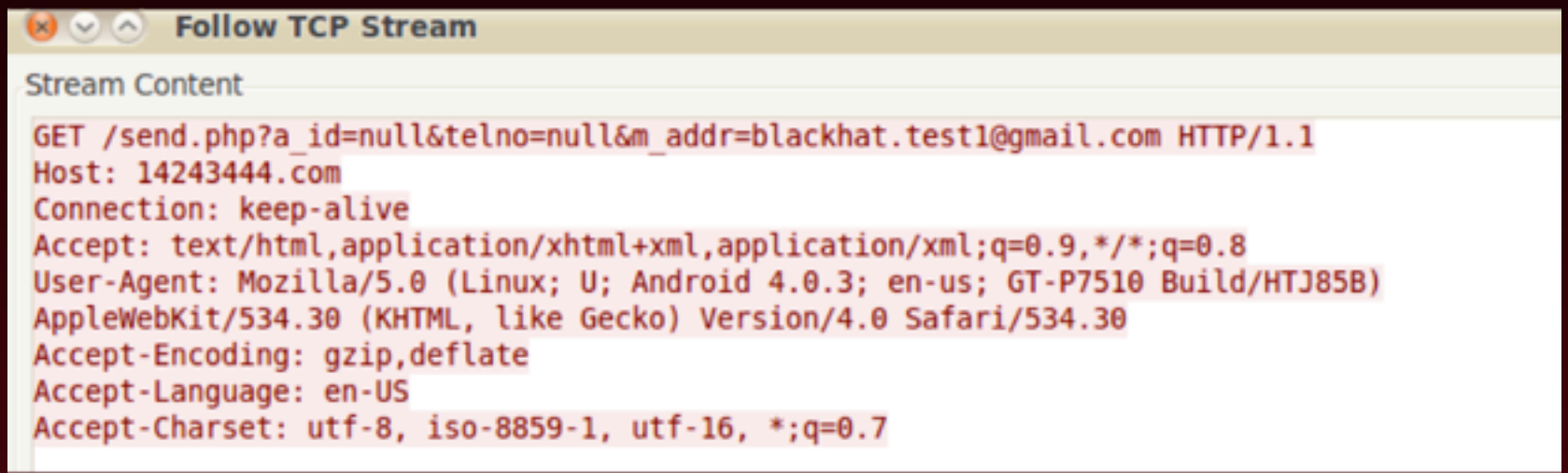

Conversations: misc-infected.pcap
Ethernet: 5
Fibre Channel
FDDI
IPv4: 7
IPv6
IPX
JXTA
NCP
RSVP
SCTP
TCP: 6
Token Ring
UDP: 2
USB
WLAN
IPv4 Conversations
Address A
Address B
Packets
Bytes
Packets A→B
Bytes A→B
Packets A←B
Bytes A←B
192.168.1.128 210.157.1.134 15 1 988 15 1 988 0 0
192.168.1.110 192.168.1.128 20 3 086 20 3 086 0 0
74.125.224.232 192.168.1.128 24 2 998 0 0 24 2 998
74.125.127.103 192.168.1.128 131 18 116 0 0 131 18 116
192.168.1.1 192.168.1.110 4 963 2 783 2 180
74.125.224.232 192.168.1.110 7 2 461 3 1 171 4 1 290
173.194.77.102 192.168.1.110 20 11 209 9 7 387 11 3 822
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Close

```
[ is restricted to network administration purposes. For further information,  ]
[ use 'whois -h whois.nic.ad.jp help'. To only display English output,       ]
[ add '/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.     ]

Network Information:
a. [Network Number]               210.157.0.0/20
b. [Network Name]                 INTERQ
g. [Organization]                 Global Media Online inc.
m. [Administrative Contact]       TW184JP
n. [Technical Contact]            TW184JP
p. [Nameserver]                   dns.interq.or.jp
p. [Nameserver]                   dns1.interq.or.jp
[Assigned Date]                   1997/05/28
[Return Date]
[Last Update]                     2008/07/29 14:05:05(JST)

Less Specific Info.
----------
GMO Internet, Inc.
                    [Allocation]                          210.157.0.0/20
```

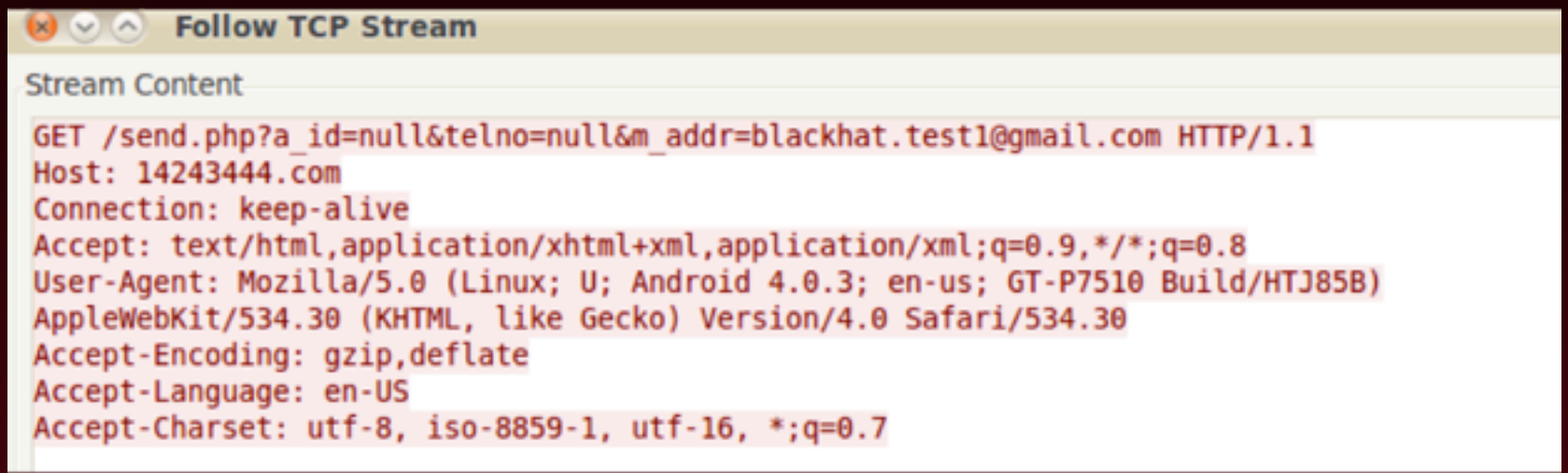
MOBILE APPLICATION TRAFFIC



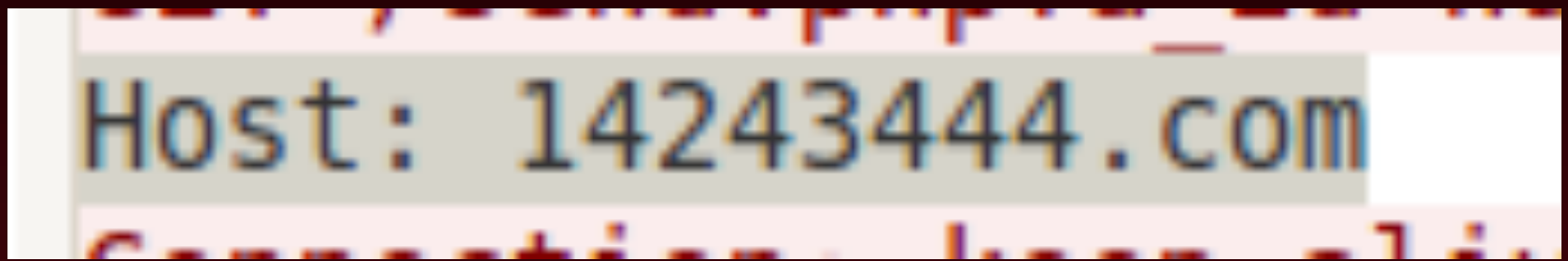
WHAT DO YOU SEE?



TELNUM? M_ADDR?



ZOOM. ENHANCE.



LET US @DIG DEEPER

```
$dig 14243444.com ANY +noall +answer @4.2.2.1

; <<>> DiG 9.7.0-P1 <<>> 14243444.com ANY +noall +answer @4.2.2.1
;; global options: +cmd
14243444.com.           278     IN      A       210.157.1.134
14243444.com.           43177   IN      NS      dns2.onamae.com.
14243444.com.           43177   IN      NS      dns1.onamae.com.
```

WHOIS

```
Last Updated On: 2012-02-23 22:00:34.0
Expiration Date: 2013-01-31 06:41:08.0
Status: ACTIVE
Registrant Name: pixer goudougaisya
Registrant Organization: goudougaisyapikusa-
Registrant Street1: Nakano
Registrant Street2:
Registrant City: Nakano-ku
Registrant State: Tokyo
Registrant Postal Code: 164-0001
Registrant Country: JP
Registrant Phone: 03-5925-4259
```

WHOIS

```
Registrant State: Tokyo
Registrant Postal Code: 164-0001
Registrant Country: JP
Registrant Phone: 03-5925-4259
Registrant Fax:
Registrant Email: pixx55xx@yahoo.co.jp
Admin Name: pixer goudougaisya
Admin Organization: goudougaisyapikusa-
Admin Street1: Nakano
Admin Street2:
Admin City: Nakano-ku
Admin State: Tokyo
Admin Postal Code: 164-0001
```

GOOGLE


OCJP-010 - 0day.jp
unixfreaxjp.blogspot.com/2012/02/ocjp-010.html - Translate this page
... ACTIVE Registrant Name: pixer goudougaisya Registrant Organization:
goudougaisyapikusa- Registrant Street1: Nakano Registrant Street2: Registrant City:
...

Oday.jp

Threats | exploits | Malwares | Zerodays | Vulnerabilities | p a specific security blog

FRIDAY, 10 FEBRUARY 2012

Android malware discovery (206.223.148.230) bananaxxx.maido3.com and 14243444.com: # OCJP-010 [malware warning!

■ The URL below ↓

```
hxxp :/ / www.14243444.com/appli02.php
hxxp :/ / 14243444.com/appli02.php
hxxp :/ / 206.223.148.230 / ~ pj629g01/appli02.php
hxxp :/ / banana8310.maido3.com / ~ pj629g01/appli02.php
hxxp :/ / banana3247.maido3.com / ~ pj629g01/appli02.php
```

DISCUSSION

- How could you identify malware in an enterprise?
- How could you prevent malware in an enterprise?
- What else could you do with the information found?

NETWORK FORENSICS PUZZLE CONTEST

- Puzzle #10: PaulDotCom Goes Off the Air
  - http://forensicscontest.com/2012/05/31/puzzle-10-pauldotcom-goes-off-the-air
  - Winner gets a BlackHat Black Card!
- #NFPC @ Defcon 20
  - Winner gets an iPad!

THANKS!

Questions?