Wireless Network Risks and Controls

Offensive Security Tools, Techniques, and Defenses

13 March 2015 – CactusCon 2015 – Phoenix, AZ

CactusCon

Presented by:
Ruihai Fang
Bishop Fox
www.bishopfox.com

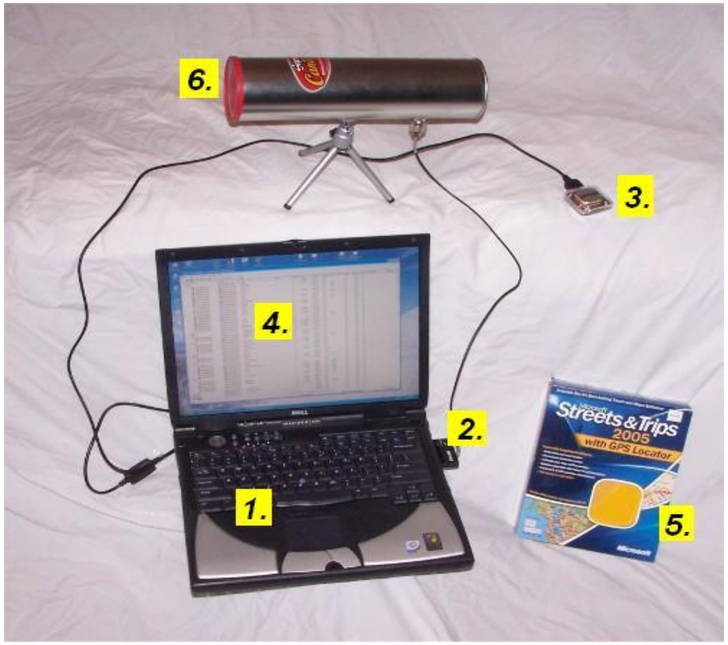
BISHOP FOX

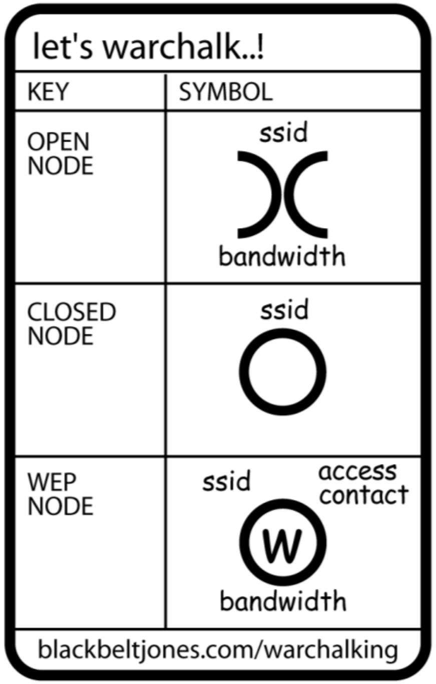
Introduction/Background

GETTING UP TO SPEED

Used to be a Pain

Lots to of heavy things to carry





let's warchalk..!

KEY	SYMBOL
OPEN NODE	ssid)(bandwidth
CLOSED NODE	ssid ○
WEP NODE	ssid access contact Ⓦ bandwidth

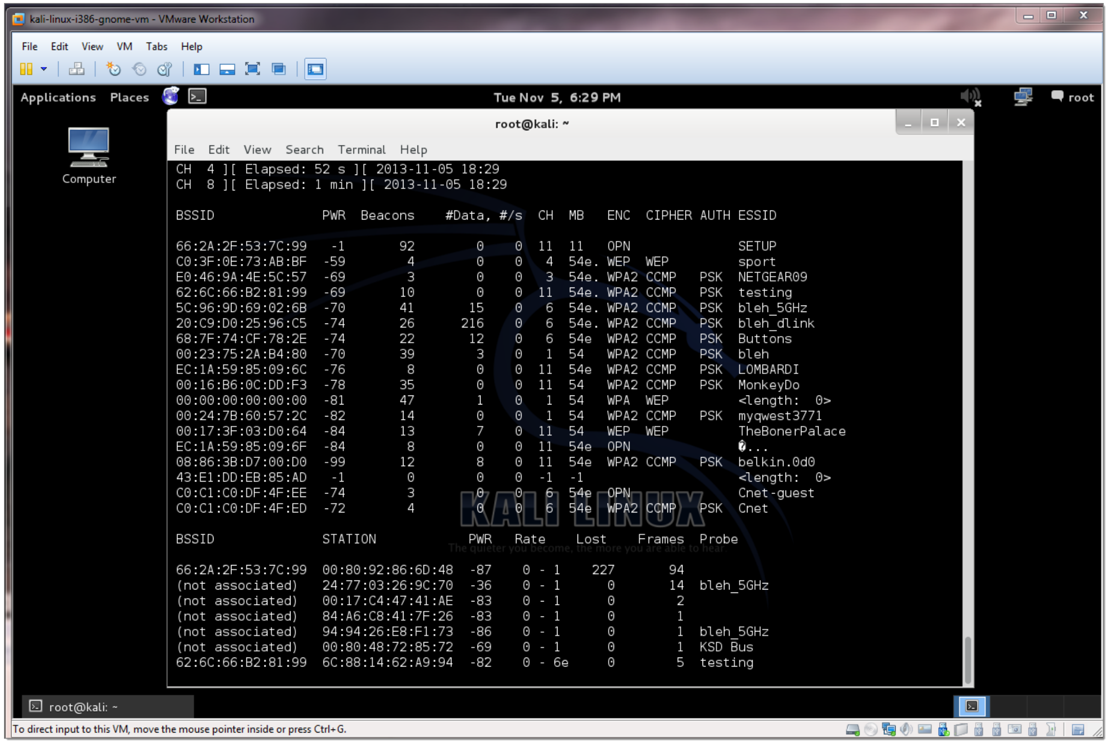
blackbeltjones.com/warchalking

Kali VM and USB Adapter

NOW EASY

- Kali Linux VM + TP-LINK - TL-WN722N (USB)

+


kali-linux-i386-gnome-vm - VMware Workstation
File Edit View VM Tabs Help
Applications Places
Tue Nov 5, 6:29 PM
root
Computer
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.
root@kali: ~

```
CH  4 ][ Elapsed: 52 s ][ 2013-11-05 18:29
CH  8 ][ Elapsed: 1 min ][ 2013-11-05 18:29

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

66:2A:2F:53:7C:99   -1       92        0    0  11  11   OPN              SETUP
C0:3F:0E:73:AB:BF  -59        4        0    0   4  54e. WEP  WEP         sport
E0:46:9A:4E:5C:57  -69        3        0    0   3  54e. WPA2 CCMP   PSK  NETGEAR09
62:6C:66:B2:81:99  -69       10        0    0  11  54e. WPA2 CCMP   PSK  testing
5C:96:9D:69:02:6B  -70       41       15    0   6  54e. WPA2 CCMP   PSK  bleh_5GHz
20:C9:D0:25:96:C5  -74       26      216    0   6  54e. WPA2 CCMP   PSK  bleh_dlink
68:7F:74:CF:78:2E  -74       22       12    0   6  54e  WPA2 CCMP   PSK  Buttons
00:23:75:2A:B4:80  -70       39        3    0   1  54   WPA2 CCMP   PSK  bleh
EC:1A:59:85:09:6C  -76        8        0    0  11  54e  WPA2 CCMP   PSK  LOMBARDI
00:16:B6:0C:DD:F3  -78       35        0    0  11  54   WPA2 CCMP   PSK  MonkeyDo
00:00:00:00:00:00  -81       47        1    0   1  54   WPA  WEP         <length:  0>
00:24:7B:60:57:2C  -82       14        0    0   1  54   WPA2 CCMP   PSK  myqwest3771
00:17:3F:03:D0:64  -84       13        7    0  11  54   WEP  WEP         TheBonerPalace
EC:1A:59:85:09:6F  -84        8        0    0  11  54e  OPN              �...
08:86:3B:D7:00:D0  -99       12        8    0  11  54e  WPA2 CCMP   PSK  belkin.0d0
43:E1:DD:EB:85:AD   -1        0        0    0  -1  -1                    <length:  0>
C0:C1:C0:DF:4F:EE  -74        3        0    0   6  54e  OPN              Cnet-guest
C0:C1:C0:DF:4F:ED  -72        4        0    0   6  54e  WPA2 CCMP   PSK  Cnet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

66:2A:2F:53:7C:99  00:80:92:86:6D:48  -87    0 - 1    227       94
(not associated)   24:77:03:26:9C:70  -36    0 - 1      0       14  bleh_5GHz
(not associated)   00:17:C4:47:41:AE  -83    0 - 1      0        2
(not associated)   84:A6:C8:41:7F:26  -83    0 - 1      0        1
(not associated)   94:94:26:E8:F1:73  -86    0 - 1      0        1  bleh_5GHz
(not associated)   00:80:48:72:85:72  -69    0 - 1      0        1  KSD Bus
62:6C:66:B2:81:99  6C:88:14:62:A9:94  -82    0 - 6e     0        5  testing
```

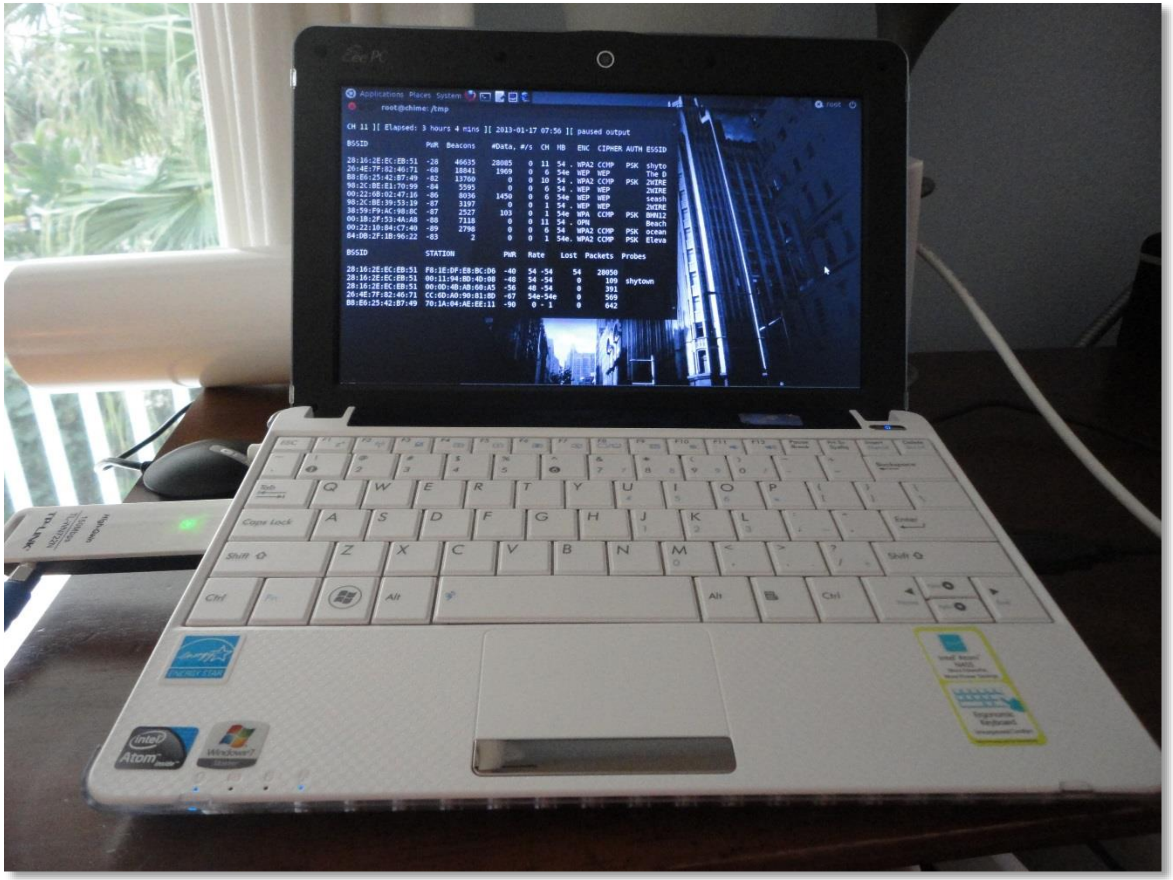
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

BISHOP FOX

Laptops, Netbooks (easier to conceal), and adapters

TP-Link Adapter
Capable of attaching a
YAGI antenna

Asus EEPc



```
root@chime: /tmp

CH 11 ][ Elapsed: 3 hours 4 mins ][ 2013-01-17 07:56 ][ paused output

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:16:2E:EC:EB:51  -28    46635    28085    0  11  54 . WPA2 CCMP   PSK  shyto
26:4E:7F:82:46:71  -68    18841     1969    0   6  54e  WEP  WEP         The D
B8:E6:25:42:B7:49  -82    13760        0    0  10  54 . WPA2 CCMP   PSK  2WIRE
98:2C:BE:E1:70:99  -84     5595        0    0   6  54 . WEP  WEP         2WIRE
00:22:6B:02:47:16  -86     8036     1450    0   6  54e  WEP  WEP         seash
98:2C:BE:39:53:19  -87     3197        0    0   1  54 . WEP  WEP         2WIRE
38:59:F9:AC:98:8C  -87     2527      103    0   1  54e  WPA  CCMP   PSK  BHN12
00:1B:2F:53:4A:A8  -88     7118        0    0  11  54 . OPN              Beach
00:22:10:84:C7:40  -89     2798        0    0   6  54   WPA2 CCMP   PSK  ocean
84:DB:2F:1B:96:22  -83        2        0    0   1  54e. WPA2 CCMP   PSK  Eleva

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

28:16:2E:EC:EB:51  F8:1E:DF:E8:BC:D6  -40   54 -54    54    28050
28:16:2E:EC:EB:51  00:11:94:BD:40:08  -48   54 -54     0      109  shytown
28:16:2E:EC:EB:51  00:0D:4B:AB:60:A5  -56   48 -54     0      391
26:4E:7F:82:46:71  CC:6D:A0:90:81:8D  -67   54e-54e    0      569
B8:E6:25:42:B7:49  70:1A:04:AE:EE:11  -90    0 - 1     0      642
```

YAGI Antennas – Directional

Yagi 2.45GHz 15dBi White, Outdoor
cantenna Y2415BW Made In USA
simpleWiFi

Very good for attacking from a distance, like from the comfort of your hotel room.

Wireless Tools

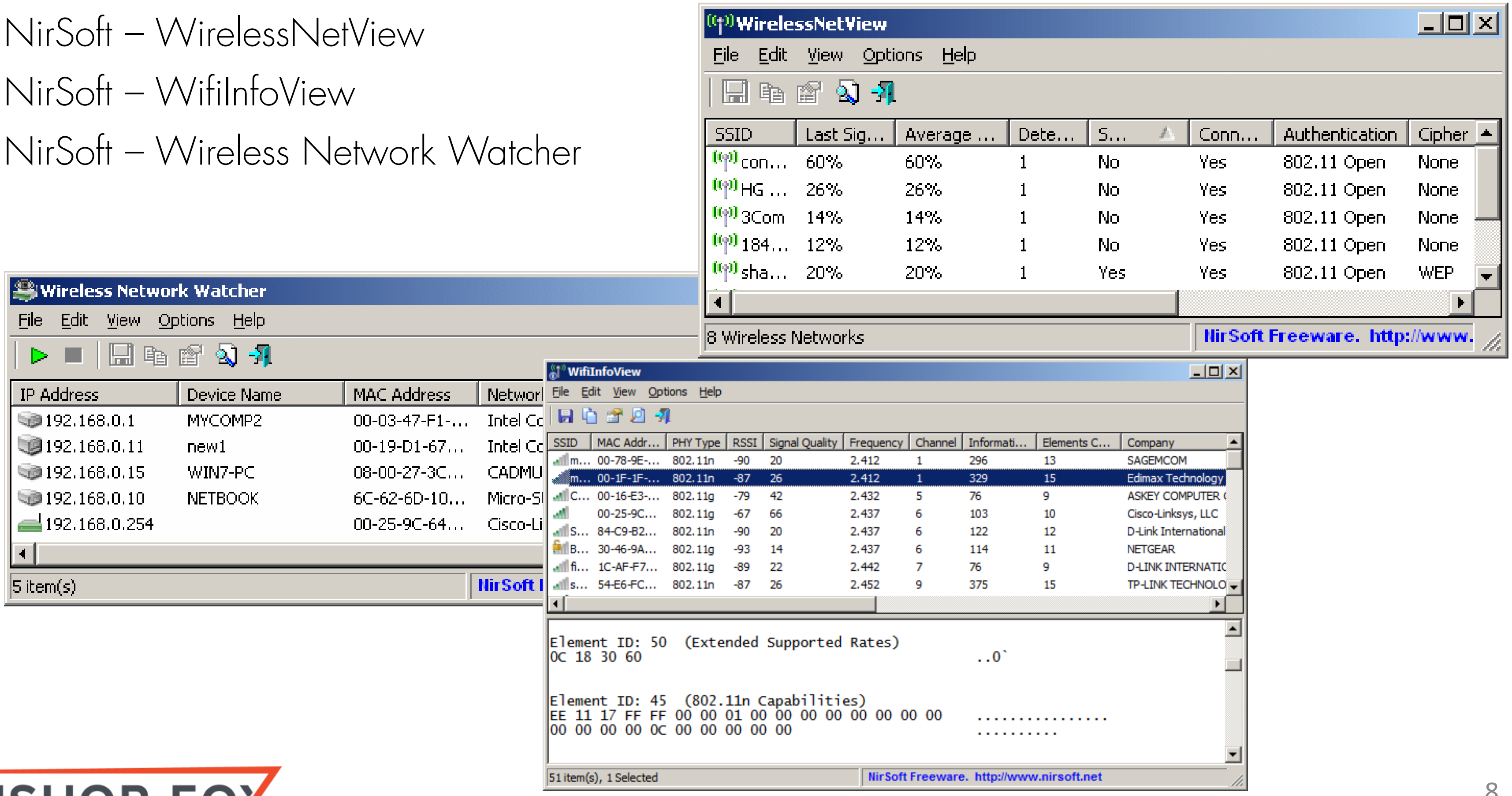
Discovery

- Supported operating systems
- Supported wireless protocols
- Active vs. passive scanning
- Packet capturing and decoding
- Distinguishes between AP, ad hoc, and client devices
- Statistics and reporting capabilities
- User interface
- Price

NirSoft Wireless Tools

WINDOWS HACKING TOOLS

- NirSoft – WirelessNetView
- NirSoft – WifiInfoView
- NirSoft – Wireless Network Watcher


WirelessNetView
File Edit View Options Help
Wireless Network Watcher
File Edit View Options Help
WifiInfoView
File Edit View Options Help

SSID	Last Sig...	Average ...	Dete...	S...	Conn...	Authentication	Cipher
con...	60%	60%	1	No	Yes	802.11 Open	None
HG ...	26%	26%	1	No	Yes	802.11 Open	None
3Com	14%	14%	1	No	Yes	802.11 Open	None
184...	12%	12%	1	No	Yes	802.11 Open	None
sha...	20%	20%	1	Yes	Yes	802.11 Open	WEP

8 Wireless Networks NirSoft Freeware. http://www.

IP Address	Device Name	MAC Address	Networ
192.168.0.1	MYCOMP2	00-03-47-F1-...	Intel Co
192.168.0.11	new1	00-19-D1-67...	Intel Co
192.168.0.15	WIN7-PC	08-00-27-3C...	CADMU
192.168.0.10	NETBOOK	6C-62-6D-10...	Micro-St
192.168.0.254		00-25-9C-64...	Cisco-Li

5 item(s) NirSoft I

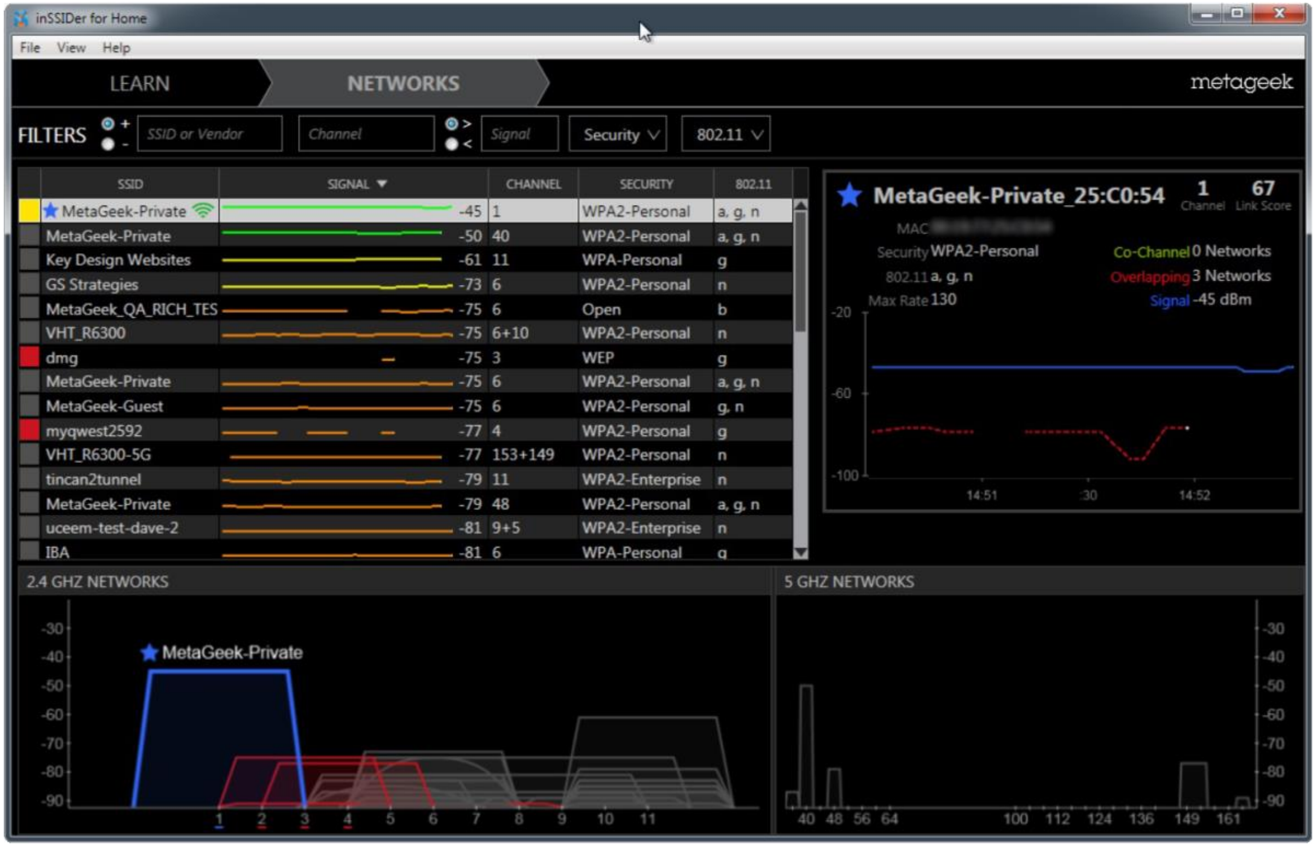
SSID	MAC Addr...	PHY Type	RSSI	Signal Quality	Frequency	Channel	Informati...	Elements C...	Company
m...	00-78-9E-...	802.11n	-90	20	2.412	1	296	13	SAGEMCOM
m...	00-1F-1F-...	802.11n	-87	26	2.412	1	329	15	Edimax Technology
C...	00-16-E3-...	802.11g	-79	42	2.432	5	76	9	ASKEY COMPUTER (
	00-25-9C...	802.11g	-67	66	2.437	6	103	10	Cisco-Linksys, LLC
S...	84-C9-B2...	802.11n	-90	20	2.437	6	122	12	D-Link International
B...	30-46-9A...	802.11g	-93	14	2.437	6	114	11	NETGEAR
fi...	1C-AF-F7...	802.11g	-89	22	2.442	7	76	9	D-LINK INTERNATIC
s...	54-E6-FC...	802.11n	-87	26	2.452	9	375	15	TP-LINK TECHNOLO

```
Element ID: 50  (Extended Supported Rates)
0C 18 30 60                                   ..0`


Element ID: 45  (802.11n Capabilities)
EE 11 17 FF FF 00 00 01 00 00 00 00 00 00 00 00   ................
00 00 00 00 0C 00 00 00 00 00                     ..........
```

51 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

inSSIDer Wi-Fi Scanner

WINDOWS HACKING TOOLS



	SSID	SIGNAL ▼	CHANNEL	SECURITY	802.11
🟨	★ MetaGeek-Private	-45	1	WPA2-Personal	a, g, n
	MetaGeek-Private	-50	40	WPA2-Personal	a, g, n
	Key Design Websites	-61	11	WPA-Personal	g
	GS Strategies	-73	6	WPA2-Personal	n
	MetaGeek_QA_RICH_TES	-75	6	Open	b
	VHT_R6300	-75	6+10	WPA2-Personal	n
🟥	dmg	-75	3	WEP	g
	MetaGeek-Private	-75	6	WPA2-Personal	a, g, n
	MetaGeek-Guest	-75	6	WPA2-Personal	g, n
🟥	myqwest2592	-77	4	WPA2-Personal	g
	VHT_R6300-5G	-77	153+149	WPA2-Personal	n
	tincan2tunnel	-79	11	WPA2-Enterprise	n
	MetaGeek-Private	-79	48	WPA2-Personal	a, g, n
	uceem-test-dave-2	-81	9+5	WPA2-Enterprise	n
	IBA	-81	6	WPA-Personal	g

★ MetaGeek-Private_25:C0:54

1 Channel

67 Link Score

MAC [redacted]

Security WPA2-Personal

802.11 a, g, n

Max Rate 130

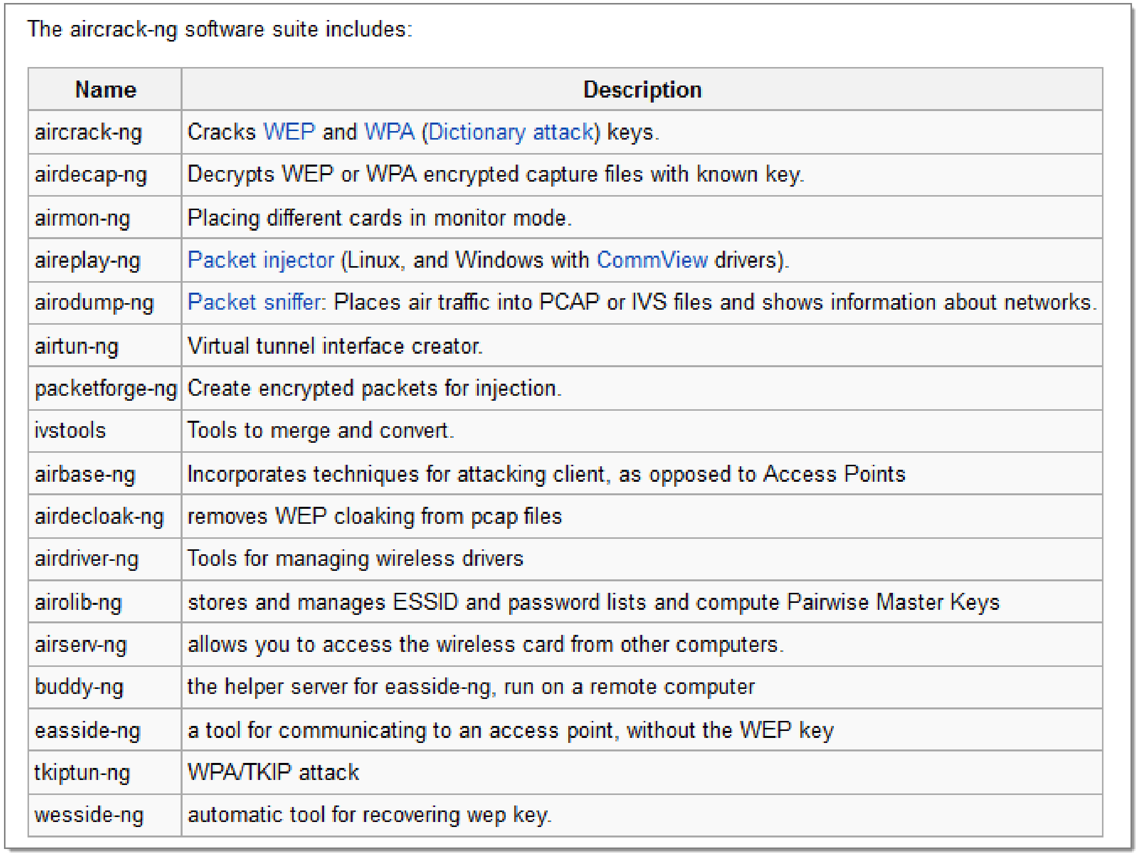
Co-Channel 0 Networks

Overlapping 3 Networks

Signal -45 dBm

Aircrack-ng Suite

LINUX HACKING TOOLS

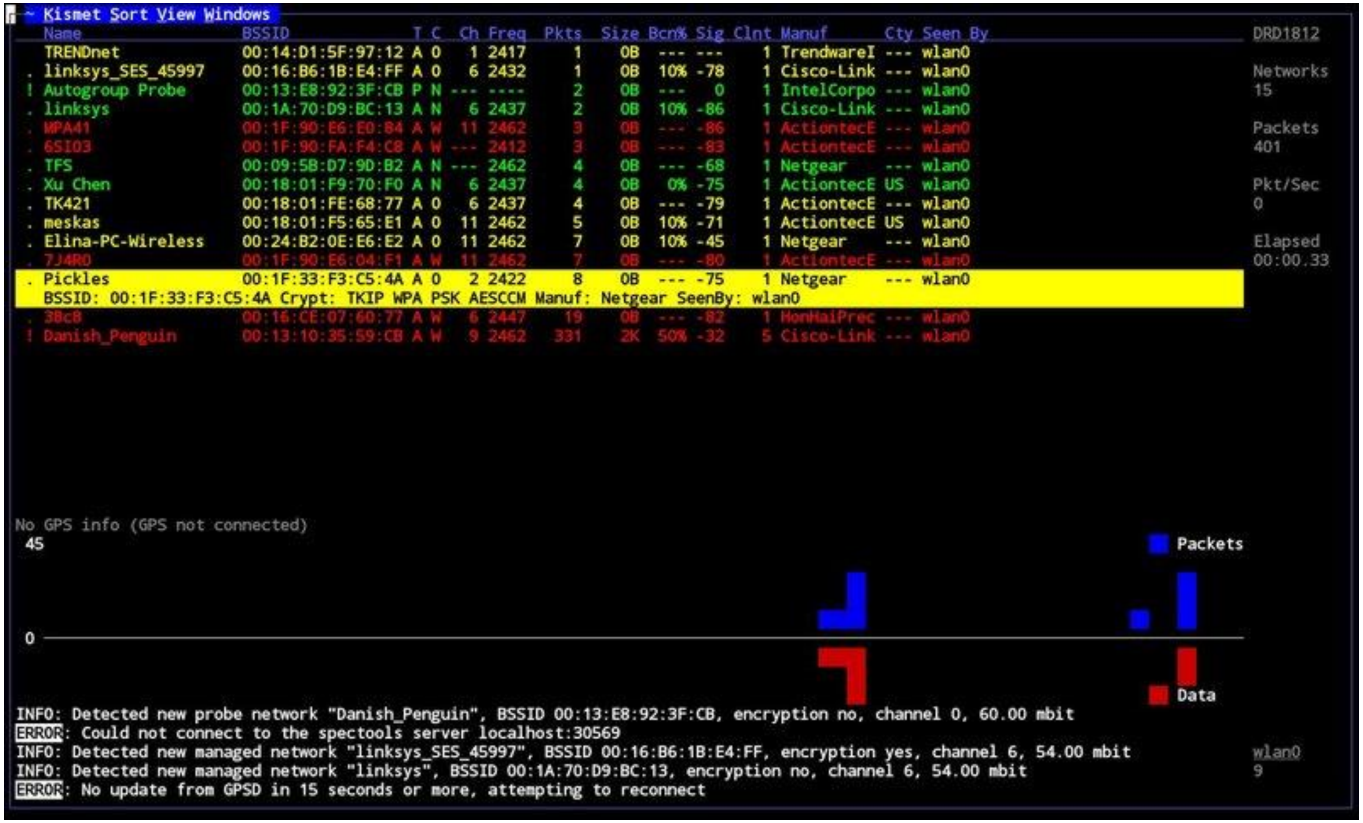


The aircrack-ng software suite includes:

Name	Description
aircrack-ng	Cracks WEP and WPA (Dictionary attack) keys.
airdecap-ng	Decrypts WEP or WPA encrypted capture files with known key.
airmon-ng	Placing different cards in monitor mode.
aireplay-ng	Packet injector (Linux, and Windows with CommView drivers).
airodump-ng	Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks.
airtun-ng	Virtual tunnel interface creator.
packetforge-ng	Create encrypted packets for injection.
ivstools	Tools to merge and convert.
airbase-ng	Incorporates techniques for attacking client, as opposed to Access Points
airdecloak-ng	removes WEP cloaking from pcap files
airdriver-ng	Tools for managing wireless drivers
airolib-ng	stores and manages ESSID and password lists and compute Pairwise Master Keys
airserv-ng	allows you to access the wireless card from other computers.
buddy-ng	the helper server for easside-ng, run on a remote computer
easside-ng	a tool for communicating to an access point, without the WEP key
tkiptun-ng	WPA/TKIP attack
wesside-ng	automatic tool for recovering wep key.

Kismet

LINUX HACKING TOOLS



```
~ Kismet Sort View Windows
  Name                BSSID              T C  Ch Freq  Pkts  Size Bcn% Sig Clnt Manuf      Cty Seen By          DRD1812
  TRENDnet            00:14:D1:5F:97:12 A 0   1 2417     1    0B  --- ---    1 TrendwareI --- wlan0
. linksys_SES_45997   00:16:B6:1B:E4:FF A 0   6 2432     1    0B  10% -78    1 Cisco-Link --- wlan0            Networks
! Autogroup Probe     00:13:E8:92:3F:CB P N --- ----     2    0B  ---   0    1 IntelCorpo --- wlan0            15
. linksys             00:1A:70:D9:BC:13 A N   6 2437     2    0B  10% -86    1 Cisco-Link --- wlan0
. WPA41               00:1F:90:E6:E0:84 A W  11 2462     3    0B  --- -86    1 ActiontecE --- wlan0            Packets
. 6SI03               00:1F:90:FA:F4:C8 A W --- 2412     3    0B  --- -83    1 ActiontecE --- wlan0            401
. TFS                 00:09:5B:D7:9D:B2 A N --- 2462     4    0B  --- -68    1 Netgear    --- wlan0
. Xu Chen             00:18:01:F9:70:F0 A N   6 2437     4    0B   0% -75    1 ActiontecE US  wlan0            Pkt/Sec
. TK421               00:18:01:FE:68:77 A 0   6 2437     4    0B  --- -79    1 ActiontecE --- wlan0            0
. meskas              00:18:01:F5:65:E1 A 0  11 2462     5    0B  10% -71    1 ActiontecE US  wlan0
. Elina-PC-Wireless   00:24:B2:0E:E6:E2 A 0  11 2462     7    0B  10% -45    1 Netgear    --- wlan0            Elapsed
. 7J4R0               00:1F:90:E6:04:F1 A W  11 2462     7    0B  --- -80    1 ActiontecE --- wlan0            00:00.33
. Pickles             00:1F:33:F3:C5:4A A 0   2 2422     8    0B  --- -75    1 Netgear    --- wlan0
  BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
. 3BcB                00:16:CE:07:60:77 A W   6 2447    19    0B  --- -82    1 HonHaiPrec --- wlan0
! Danish_Penguin      00:13:10:35:59:CB A W   9 2462   331    2K  50% -32    5 Cisco-Link --- wlan0

No GPS info (GPS not connected)

INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit    wlan0
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit               9
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
```

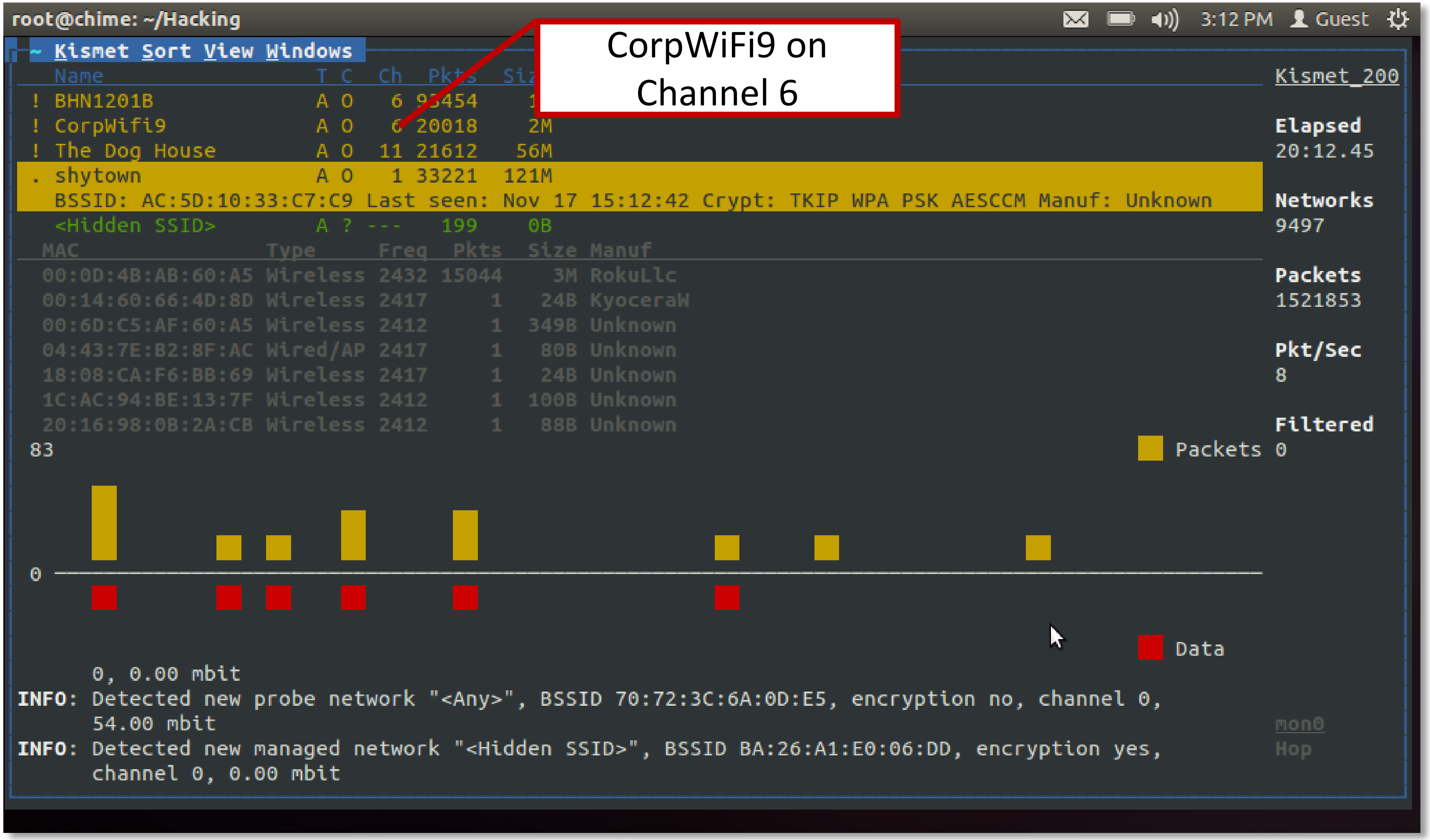
Cracking WPA2-PSK with Pyrit

Pyrit

https://code.google.com/p/pyrit/

Pyrit allows to create massive databases, pre-computing part of the IEEE 802.11 WPA/WPA2-PSK authentication phase in a space-time-tradeoff. Exploiting the computational power of Many-Core- and other platforms through ATI-Stream, Nvidia CUDA and OpenCL, it is currently by far the most powerful attack against one of the world's most used security-protocols.

During Recon Find What Channel Your Target Is On and Capture Only on That Channel to Increase Your Chances of Getting a Valid WPA Handshake

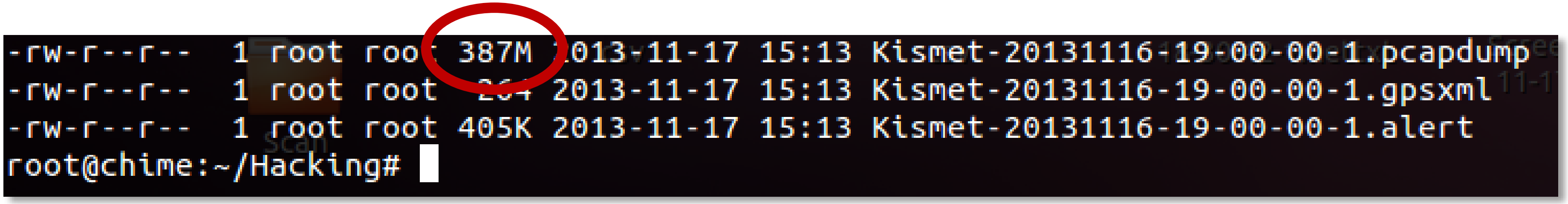


CorpWiFi9 on Channel 6

```
   Name                   T C  Ch  Pkts  Si                                            Kismet_200
 ! BHN1201B               A O   6 93454    1
 ! CorpWifi9              A O   6 20018    2M                                          Elapsed
 ! The Dog House          A O  11 21612   56M                                          20:12.45
 . shytown                A O   1 33221  121M
   BSSID: AC:5D:10:33:C7:C9 Last seen: Nov 17 15:12:42 Crypt: TKIP WPA PSK AESCCM Manuf: Unknown   Networks
   <Hidden SSID>          A ? ---    199    0B                                         9497
  MAC               Type      Freq  Pkts  Size Manuf
  00:0D:4B:AB:60:A5 Wireless 2432 15044    3M RokuLlc                                  Packets
  00:14:60:66:4D:8D Wireless 2417     1   24B KyoceraW                                 1521853
  00:6D:C5:AF:60:A5 Wireless 2412     1  349B Unknown
  04:43:7E:B2:8F:AC Wired/AP 2417     1   80B Unknown                                  Pkt/Sec
  18:08:CA:F6:BB:69 Wireless 2417     1   24B Unknown                                  8
  1C:AC:94:BE:13:7F Wireless 2412     1  100B Unknown
  20:16:98:0B:2A:CB Wireless 2412     1   88B Unknown                                  Filtered
 83                                                                        Packets     0

 0 ----------------------------------------------------------------------------------

                                                                           Data
      0, 0.00 mbit
INFO: Detected new probe network "<Any>", BSSID 70:72:3C:6A:0D:E5, encryption no, channel 0,
      54.00 mbit                                                                       mon0
INFO: Detected new managed network "<Hidden SSID>", BSSID BA:26:A1:E0:06:DD, encryption yes,   Hop
      channel 0, 0.00 mbit
```

Passive Monitoring with Kismet

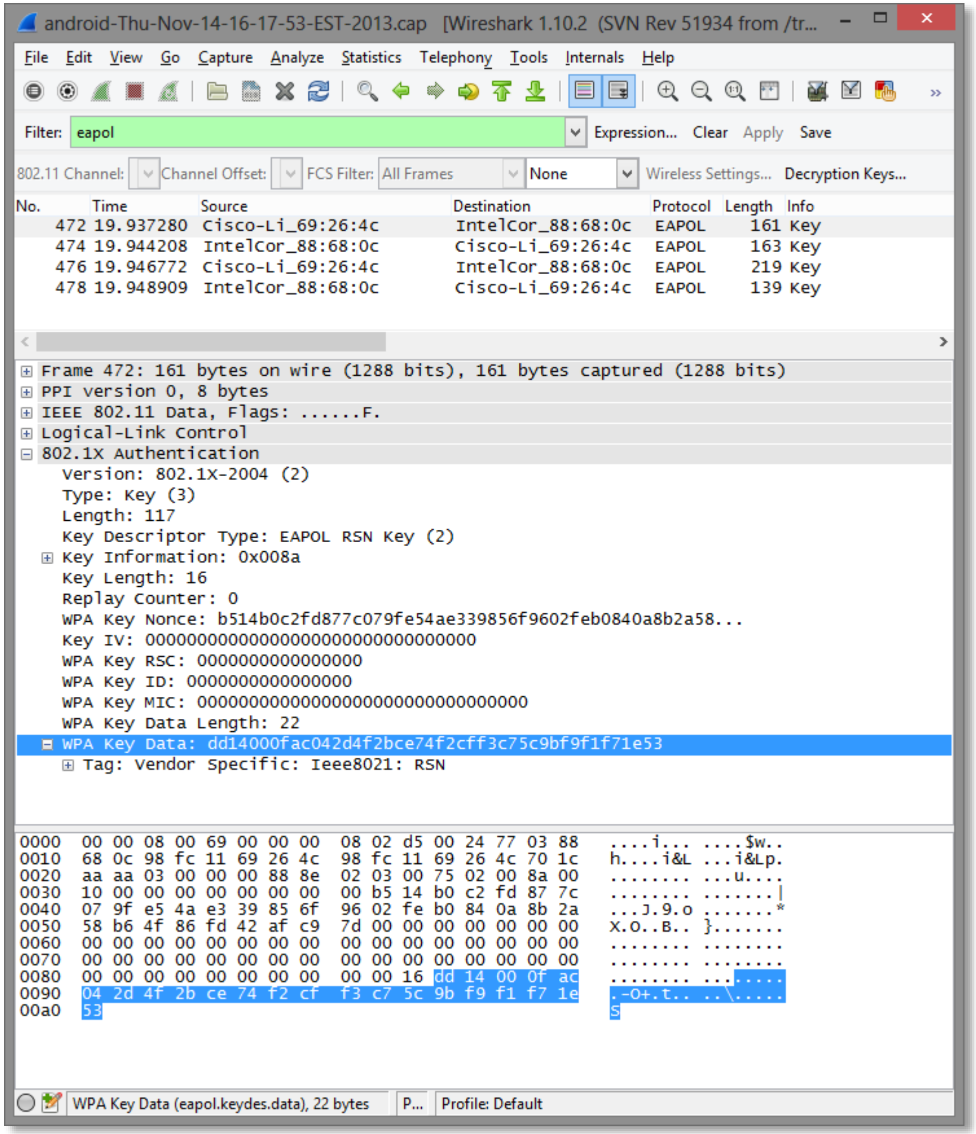
Running Kismet for 12 hours will capture lots of packets and PCAP files can be large.



```
-rw-r--r--  1 root root 387M 2013-11-17 15:13 Kismet-20131116-19-00-00-1.pcapdump
-rw-r--r--  1 root root  264 2013-11-17 15:13 Kismet-20131116-19-00-00-1.gpsxml
-rw-r--r--  1 root root 405K 2013-11-17 15:13 Kismet-20131116-19-00-00-1.alert
root@chime:~/Hacking# 
```

BISHOP FOX

WPA 4-Way Handshake



android-Thu-Nov-14-16-17-53-EST-2013.cap [Wireshark 1.10.2 (SVN Rev 51934 from /tr...

Filter: eapol

802.11 Channel: Channel Offset: FCS Filter: All Frames None

```
No.    Time       Source              Destination         Protocol  Length  Info
   472 19.937280  Cisco-Li_69:26:4c   IntelCor_88:68:0c   EAPOL        161  Key
   474 19.944208  IntelCor_88:68:0c   Cisco-Li_69:26:4c   EAPOL        163  Key
   476 19.946772  Cisco-Li_69:26:4c   IntelCor_88:68:0c   EAPOL        219  Key
   478 19.948909  IntelCor_88:68:0c   Cisco-Li_69:26:4c   EAPOL        139  Key
```

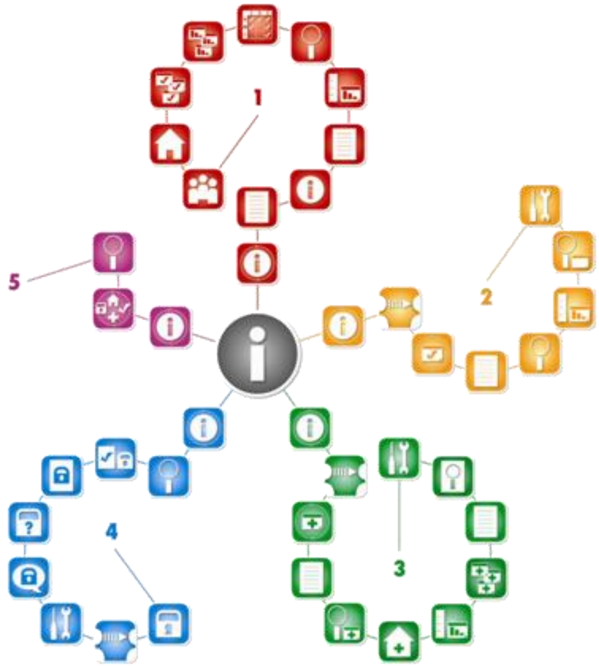
```
⊞ Frame 472: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)
⊞ PPI version 0, 8 bytes
⊞ IEEE 802.11 Data, Flags: ......F.
⊞ Logical-Link Control
⊟ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
  ⊞ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 0
    WPA Key Nonce: b514b0c2fd877c079fe54ae339856f9602feb0840a8b2a58...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  ⊟ WPA Key Data: dd14000fac042d4f2bce74f2cff3c75c9bf9f1f71e53
    ⊞ Tag: Vendor Specific: Ieee8021: RSN
```

```
0000  00 00 08 00 69 00 00 00  08 02 d5 00 24 77 03 88   ....i... ....$w..
0010  68 0c 98 fc 11 69 26 4c  98 fc 11 69 26 4c 70 1c   h....i&L ...i&Lp.
0020  aa aa 03 00 00 00 88 8e  02 03 00 75 02 00 8a 00   ........ ...u....
0030  10 00 00 00 00 00 00 00  00 b5 14 b0 c2 fd 87 7c   ........ .......|
0040  07 9f e5 4a e3 39 85 6f  96 02 fe b0 84 0a 8b 2a   ...J.9.o .......*
0050  58 b6 4f 86 fd 42 af c9  7d 00 00 00 00 00 00 00   X.O..B.. }.......
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 16 dd 14 00 0f ac   ........ ........
0090  04 2d 4f 2b ce 74 f2 cf  f3 c7 5c 9b f9 f1 f7 1e   .-O+.t.. ..\.....
00a0  53                                                 S
```

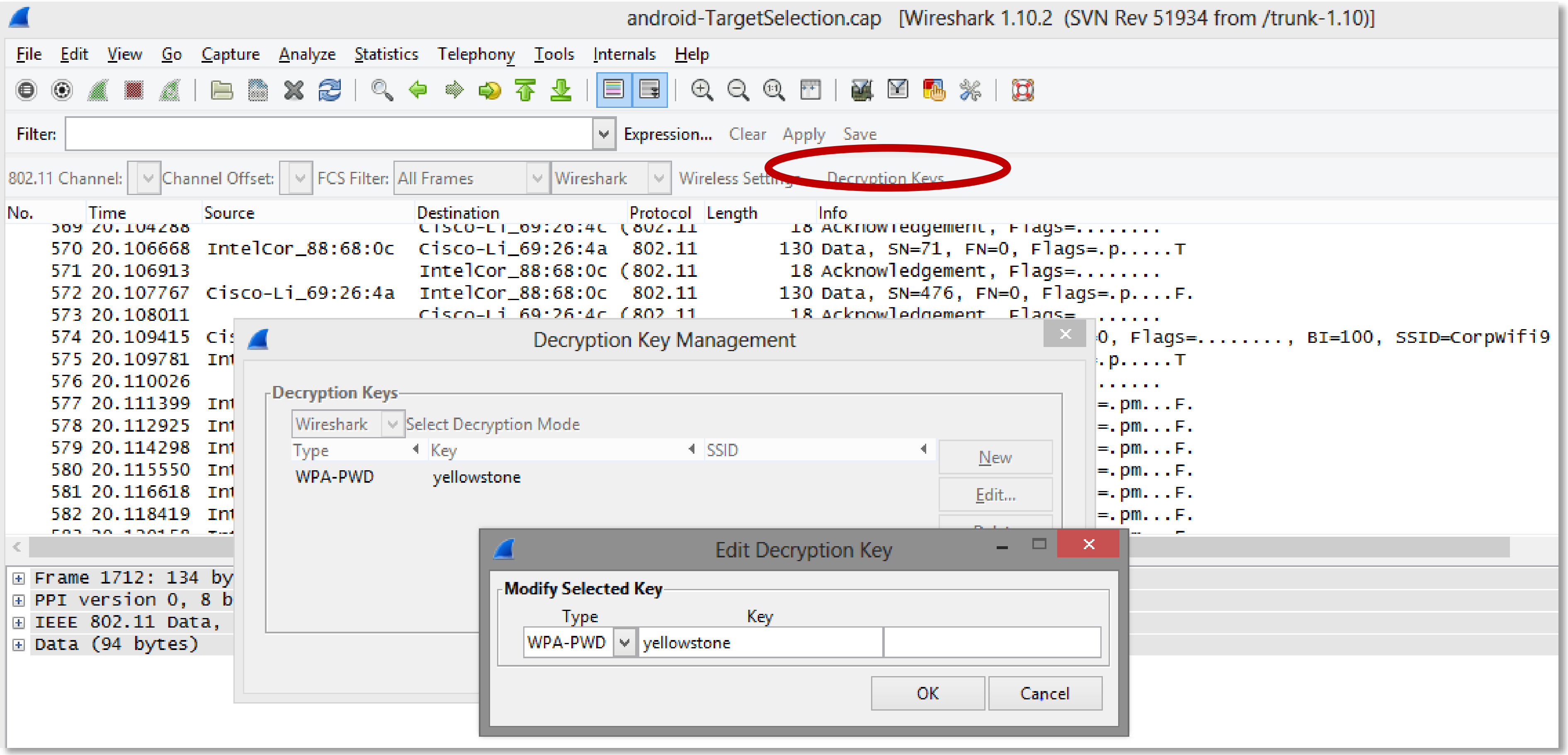
WPA Key Data (eapol.keydes.data), 22 bytes P... Profile: Default

BISHOP FOX

DEMO



Decrypting WPA Packet Captures with Found Key in Wireshark



android-TargetSelection.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames Wireshark Wireless Settings Decryption Keys

```
No.   Time       Source             Destination         Protocol Length Info
  569 20.104288                     Cisco-Li_69:26:4c (802.11     18 Acknowledgement, Flags=........
  570 20.106668 IntelCor_88:68:0c  Cisco-Li_69:26:4a   802.11    130 Data, SN=71, FN=0, Flags=.p.....T
  571 20.106913                     IntelCor_88:68:0c (802.11     18 Acknowledgement, Flags=........
  572 20.107767 Cisco-Li_69:26:4a  IntelCor_88:68:0c   802.11    130 Data, SN=476, FN=0, Flags=.p....F.
  573 20.108011                     Cisco-Li_69:26:4c (802.11     18 Acknowledgement, Flags=........
  574 20.109415 Ci                                                  0, Flags=........, BI=100, SSID=Corpwifi9
  575 20.109781 Int                                                 .p.....T
  576 20.110026                                                     ......
  577 20.111399 Int                                                 =.pm...F.
  578 20.112925 Int                                                 =.pm...F.
  579 20.114298 Int                                                 =.pm...F.
  580 20.115550 Int                                                 =.pm...F.
  581 20.116618 Int                                                 =.pm...F.
  582 20.118419 Int                                                 =.pm...F.
```

```
⊞ Frame 1712: 134 by
⊞ PPI version 0, 8 b
⊞ IEEE 802.11 Data,
⊞ Data (94 bytes)
```

Decryption Key Management

Decryption Keys

Wireshark | Select Decryption Mode

Type	Key	SSID
WPA-PWD	yellowstone	

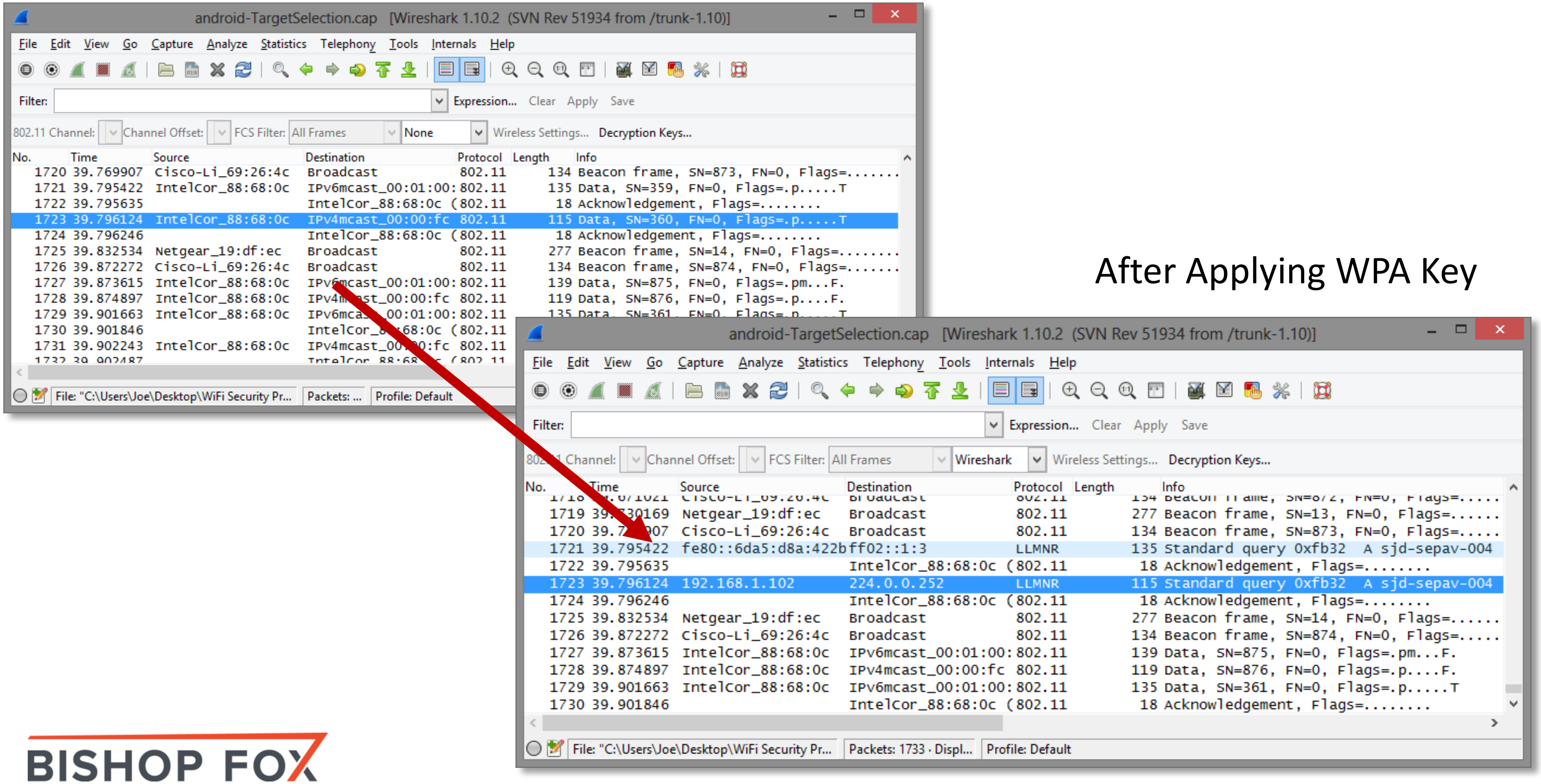
Edit Decryption Key

Modify Selected Key

Type	Key
WPA-PWD	yellowstone

Before and After Decryption in Wireshark

Before Applying WPA Key



android-TargetSelection.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

Filter:

802.11 Channel: Channel Offset: FCS Filter: All Frames None

```
No.   Time      Source             Destination          Protocol Length Info
 1720 39.769907 Cisco-Li_69:26:4c  Broadcast            802.11     134 Beacon frame, SN=873, FN=0, Flags=.......
 1721 39.795422 IntelCor_88:68:0c  IPv6mcast_00:01:00:  802.11     135 Data, SN=359, FN=0, Flags=.p.....T
 1722 39.795635                    IntelCor_88:68:0c (  802.11      18 Acknowledgement, Flags=........
 1723 39.796124 IntelCor_88:68:0c  IPv4mcast_00:00:fc  802.11     115 Data, SN=360, FN=0, Flags=.p.....T
 1724 39.796246                    IntelCor_88:68:0c (  802.11      18 Acknowledgement, Flags=........
 1725 39.832534 Netgear_19:df:ec   Broadcast            802.11     277 Beacon frame, SN=14, FN=0, Flags=........
 1726 39.872272 Cisco-Li_69:26:4c  Broadcast            802.11     134 Beacon frame, SN=874, FN=0, Flags=.......
 1727 39.873615 IntelCor_88:68:0c  IPv6mcast_00:01:00:  802.11     139 Data, SN=875, FN=0, Flags=.pm...F.
 1728 39.874897 IntelCor_88:68:0c  IPv4mcast_00:00:fc  802.11     119 Data, SN=876, FN=0, Flags=.p....F.
 1729 39.901663 IntelCor_88:68:0c  IPv6mcast_00:01:00:  802.11     135 Data, SN=361, FN=0, Flags=.p.....T
 1730 39.901846                    IntelCor_88:68:0c (  802.11
 1731 39.902243 IntelCor_88:68:0c  IPv4mcast_00:00:fc  802.11
 1732 39.902487                    IntelCor_88:68:0c (  802.11
```

File: "C:\Users\Joe\Desktop\WiFi Security Pr... Packets: ... Profile: Default

After Applying WPA Key

android-TargetSelection.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

Filter:

802.11 Channel: Channel Offset: FCS Filter: All Frames Wireshark

```
No.   Time      Source             Destination          Protocol Length Info
 1718 39.671021 Cisco-Li_69:26:4c  Broadcast            802.11     134 Beacon frame, SN=872, FN=0, Flags=.....
 1719 39.730169 Netgear_19:df:ec   Broadcast            802.11     277 Beacon frame, SN=13, FN=0, Flags=......
 1720 39.769907 Cisco-Li_69:26:4c  Broadcast            802.11     134 Beacon frame, SN=873, FN=0, Flags=.....
 1721 39.795422 fe80::6da5:d8a:422bff02::1:3            LLMNR      135 Standard query 0xfb32  A sjd-sepav-004
 1722 39.795635                    IntelCor_88:68:0c (  802.11      18 Acknowledgement, Flags=........
 1723 39.796124 192.168.1.102      224.0.0.252          LLMNR      115 Standard query 0xfb32  A sjd-sepav-004
 1724 39.796246                    IntelCor_88:68:0c (  802.11      18 Acknowledgement, Flags=........
 1725 39.832534 Netgear_19:df:ec   Broadcast            802.11     277 Beacon frame, SN=14, FN=0, Flags=......
 1726 39.872272 Cisco-Li_69:26:4c  Broadcast            802.11     134 Beacon frame, SN=874, FN=0, Flags=.....
 1727 39.873615 IntelCor_88:68:0c  IPv6mcast_00:01:00:  802.11     139 Data, SN=875, FN=0, Flags=.pm...F.
 1728 39.874897 IntelCor_88:68:0c  IPv4mcast_00:00:fc  802.11     119 Data, SN=876, FN=0, Flags=.p....F.
 1729 39.901663 IntelCor_88:68:0c  IPv6mcast_00:01:00:  802.11     135 Data, SN=361, FN=0, Flags=.p.....T
 1730 39.901846                    IntelCor_88:68:0c (  802.11      18 Acknowledgement, Flags=........
```

File: "C:\Users\Joe\Desktop\WiFi Security Pr... Packets: 1733 · Displ... Profile: Default

BISHOP FOX

Wi-Fi Pineapple

WIRELESS PENETRATION TESTING ROUTER

Features

WHAT CAN IT DO?

- Wireless Jamming (De-auth Attack)
- Man-in-the-Middle attack
- DNS Spoof on lure client
- Web base management
- Tether via Mobile Broadband
- Battery power and portable

BISHOP FOX

Methodology

Social Engineering

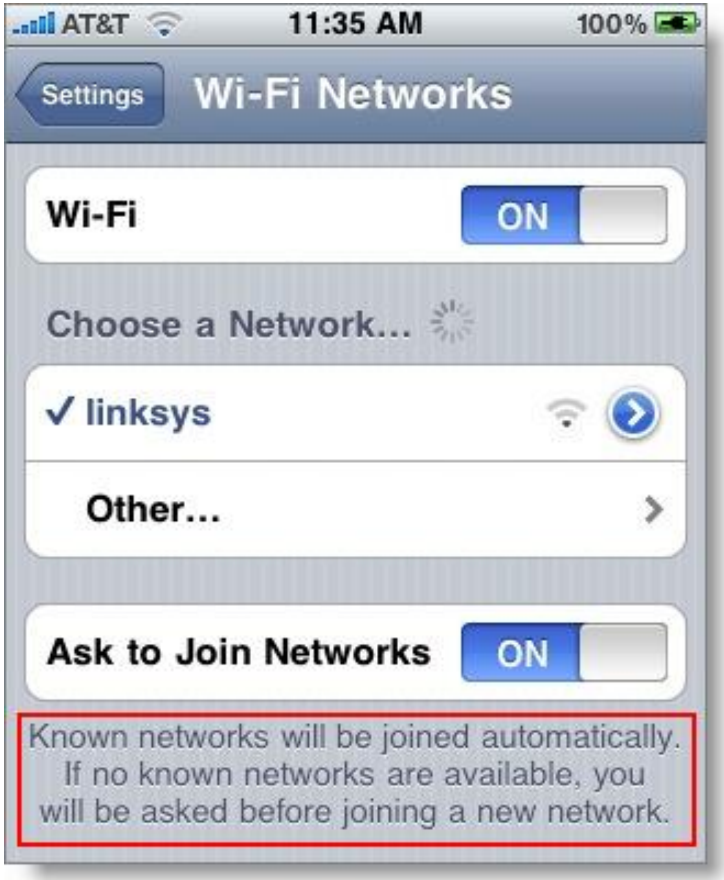
1. Karma (Rogue AP)

2. DNS Spoof & MITM

3. Phishing

Auto-Association

PROBLEM TO EXPLOIT



Wi-Fi Networks

Wi-Fi: ON

Choose a Network...

✓ linksys

Other...

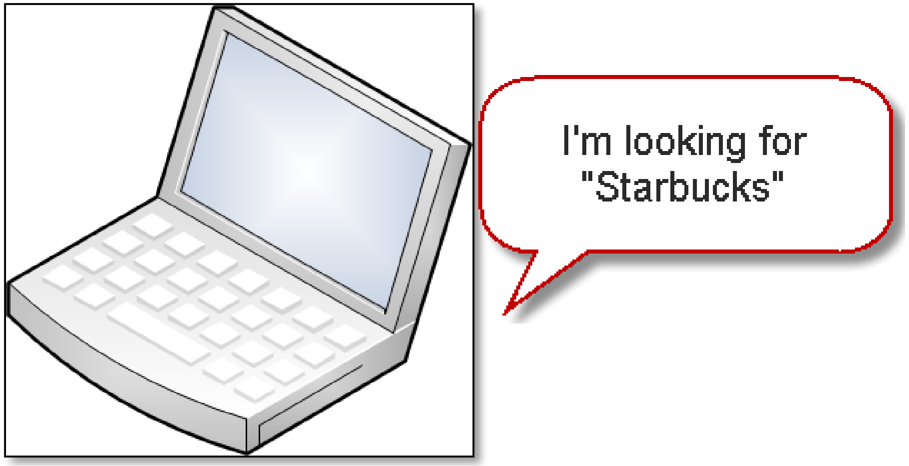
Ask to Join Networks: ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Karma

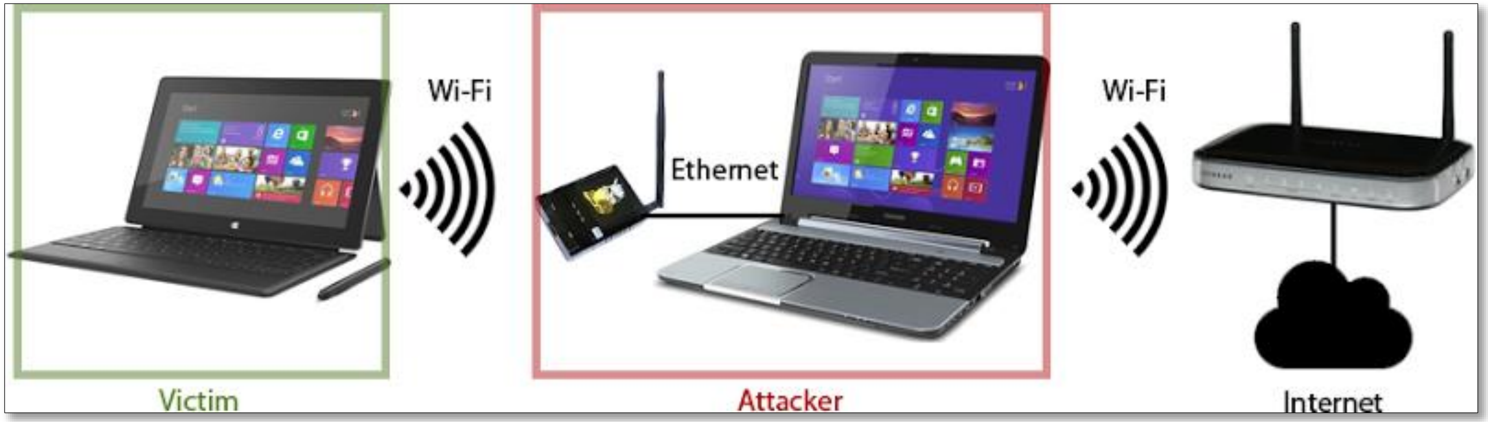
HOW DOES IT WORK?

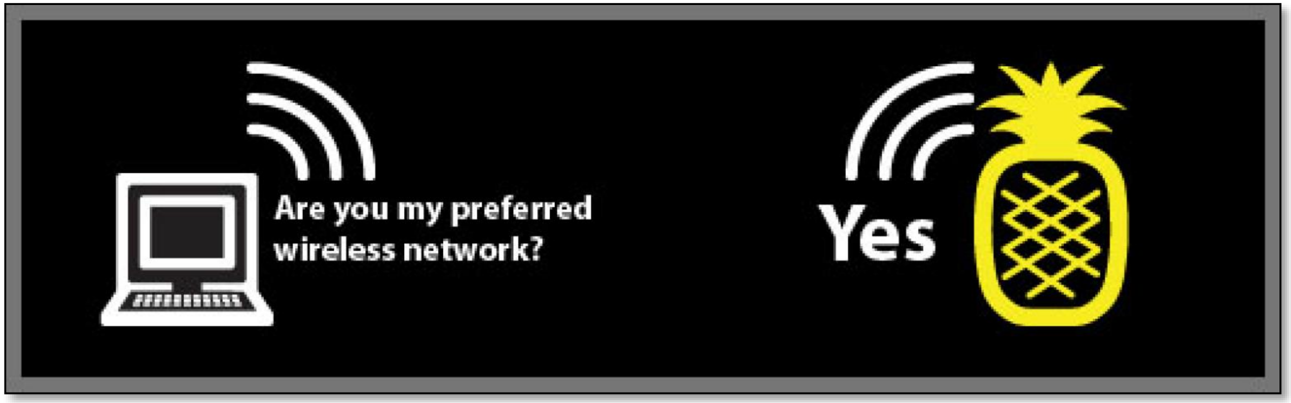
- Listen to wireless probes from nearby wireless devices
- Impersonate as the requested wireless AP



Karma

ROGUE AP

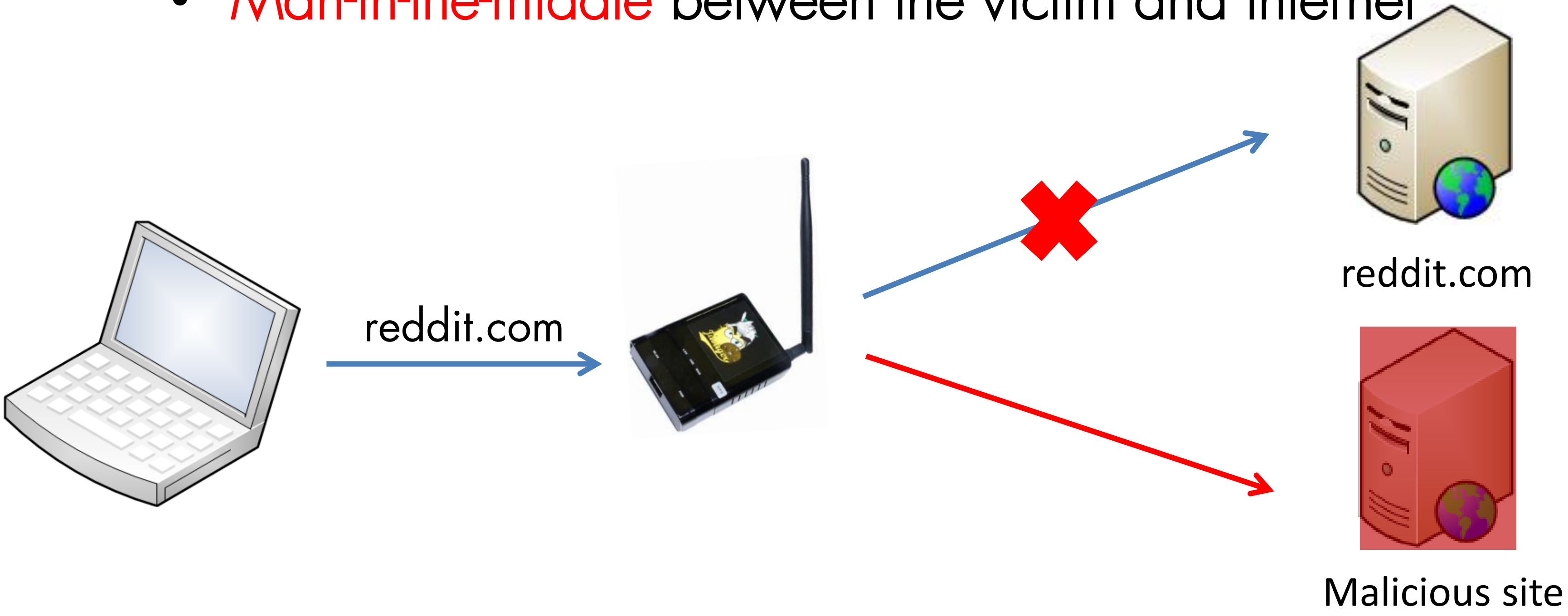




DNS Spoof

POISONING YOUR DNS

- Modify DNS records and point to a malicious site
- Man-in-the-middle between the victim and Internet

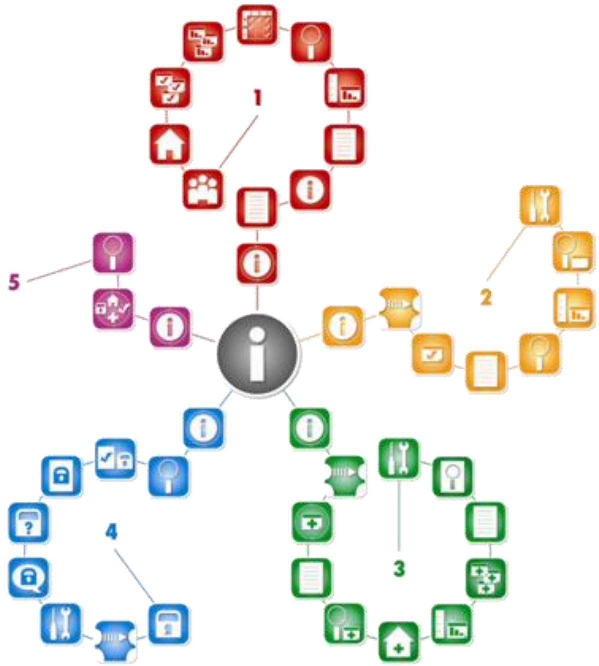


Phishing

PHISHING ATTACK

- Clone the official website (reddit.com)
- Implement key logger
- Deploy malware or backdoor on the forged website
- Compromise the victim

DEMO



Mitigation

Things that you should be doing

1. Disable the "Connect Automatically" setting on all unsecured wireless networks.

2. Use DNS Crypt or Google DNS.

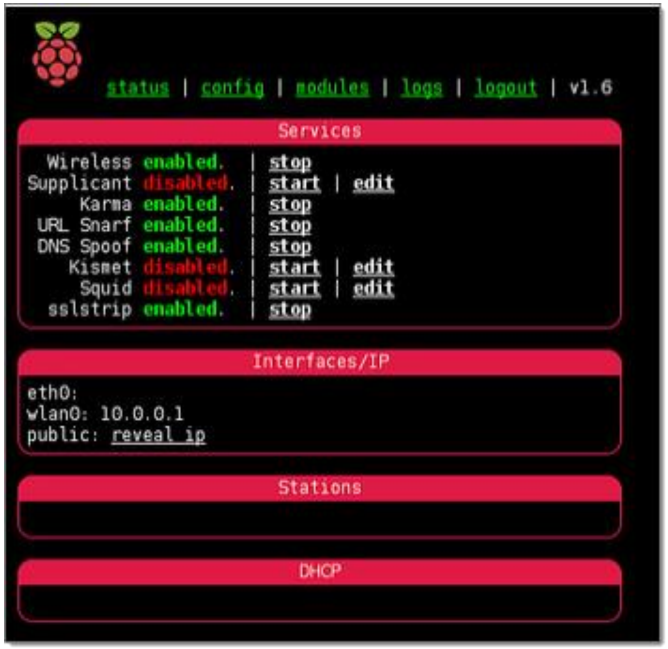
3. Don't connect to any unsecured or unknown wireless network.

4. Use a trusted VPN tunnel to encrypt the traffic on public network.

Raspberry Pi

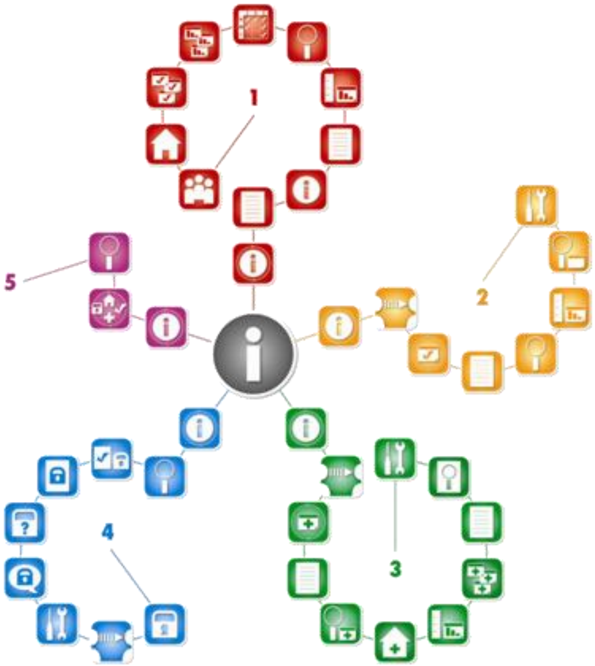
FRUITY WIFI

- Raspberry Pi – cheap alternative (~$35)
  - Fruity WiFi – Raspberry Pi version of the WiFi Pineapple



```
status | config | modules | logs | logout | v1.6

                     Services
   Wireless enabled.  | stop
 Supplicant disabled. | start | edit
      Karma enabled.  | stop
  URL Snarf enabled.  | stop
   DNS Spoof enabled. | stop
     Kismet disabled. | start | edit
      Squid disabled. | start | edit
   sslstrip enabled.  | stop

                   Interfaces/IP
eth0:
wlan0: 10.0.0.1
public: reveal ip

                     Stations

                       DHCP
```

Mobile WiFi Security Tools



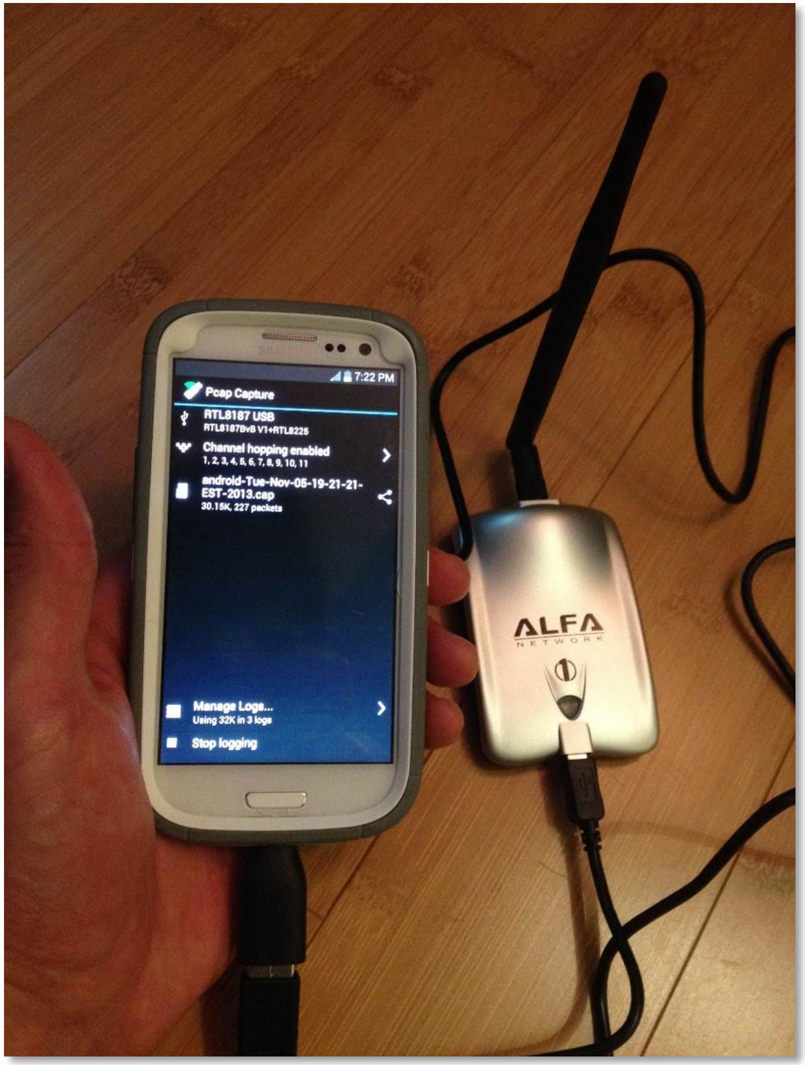
Popular Mobile WiFi Hacking Tools

WiFi Sniffing on Android in Monitor Mode
http://www.kismetwireless.net/android-pcap/

Password Sniffing & Session Hijacking Using dSploit
http://dsploit.net/

iphone-wireless https://code.google.com/p/iphone-wireless/wiki/Stumbler

More Discreet Monitoring Using Alpha 1 802.11b/g



7:22 PM

Pcap Capture

RTL8187 USB
RTL8187BvB V1+RTL8225

Channel hopping enabled
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

android-Tue-Nov-05-19-21-21-EST-2013.cap
30.15K, 227 packets

Manage Logs...
Using 32K in 3 logs

Stop logging

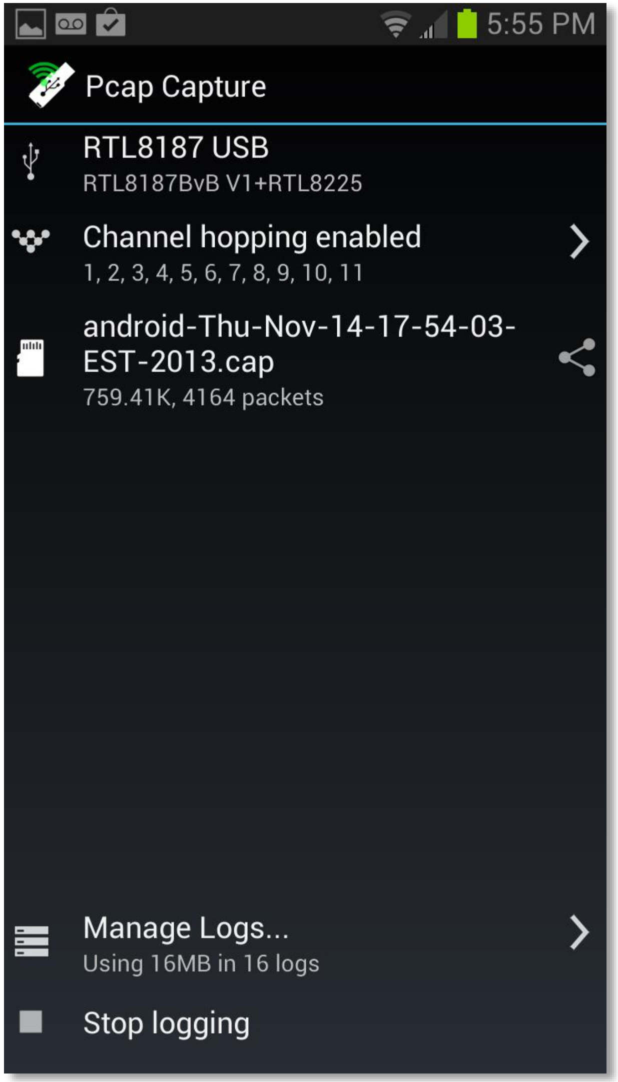
Model Number AWUS036H. This uses the RTL8187 Wireless Chipset.

#wifisecurityselfie

Monitor mode in places laptops can't go! Like someone else's data center, telcos, power substations, or just places you plain should not be.

BISHOP FOX

Android PCAP Monitor Mode on a Galaxy S3



5:55 PM

Pcap Capture

RTL8187 USB
RTL8187BvB V1+RTL8225

Channel hopping enabled
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

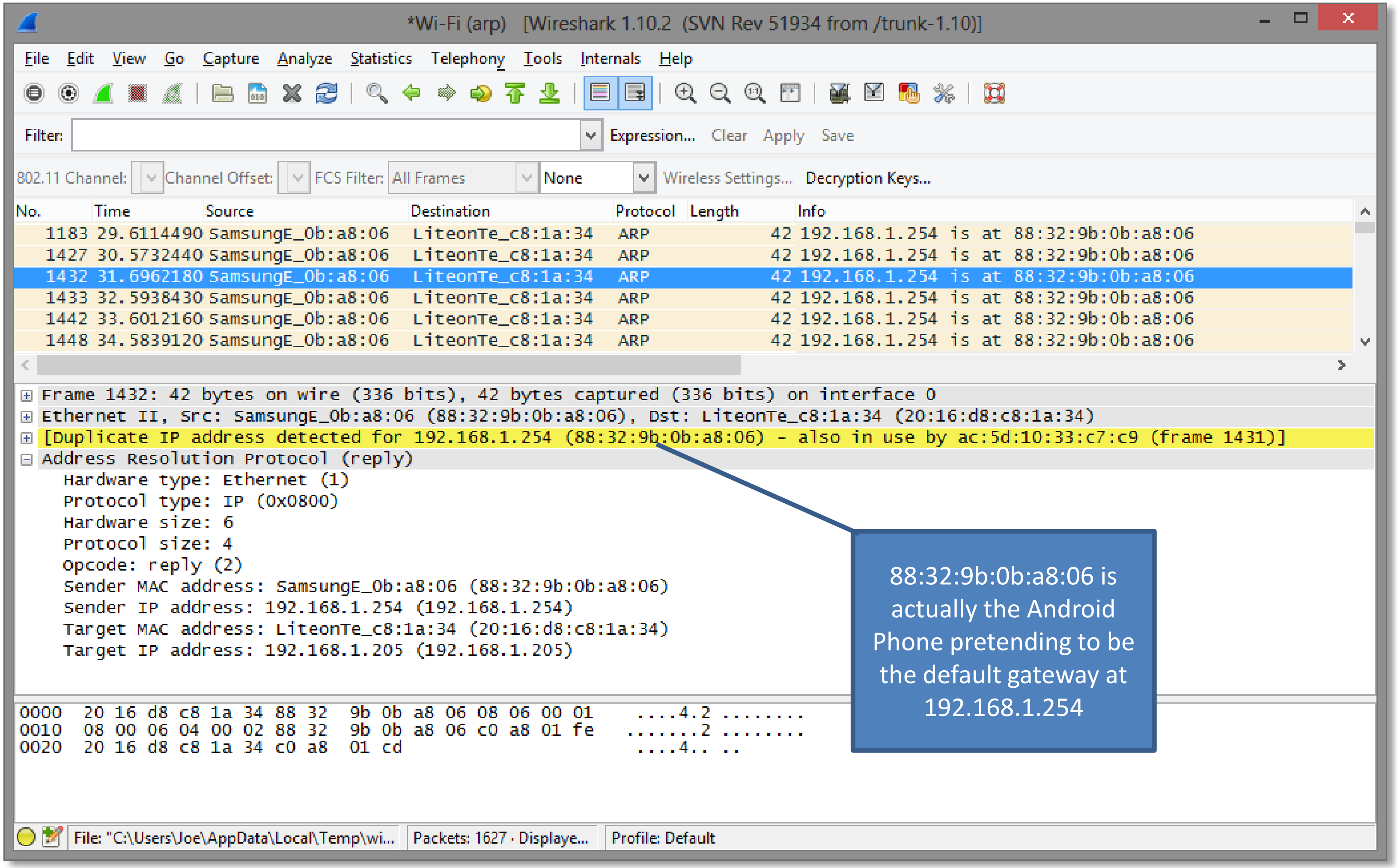
android-Thu-Nov-14-17-54-03-EST-2013.cap
759.41K, 4164 packets

Manage Logs...
Using 16MB in 16 logs

Stop logging

BISHOP FOX

Arp Spoofing & Detection


*Wi-Fi (arp) [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames None
Wireless Settings... Decryption Keys...
File: "C:\Users\Joe\AppData\Local\Temp\wi... Packets: 1627 · Displaye... Profile: Default

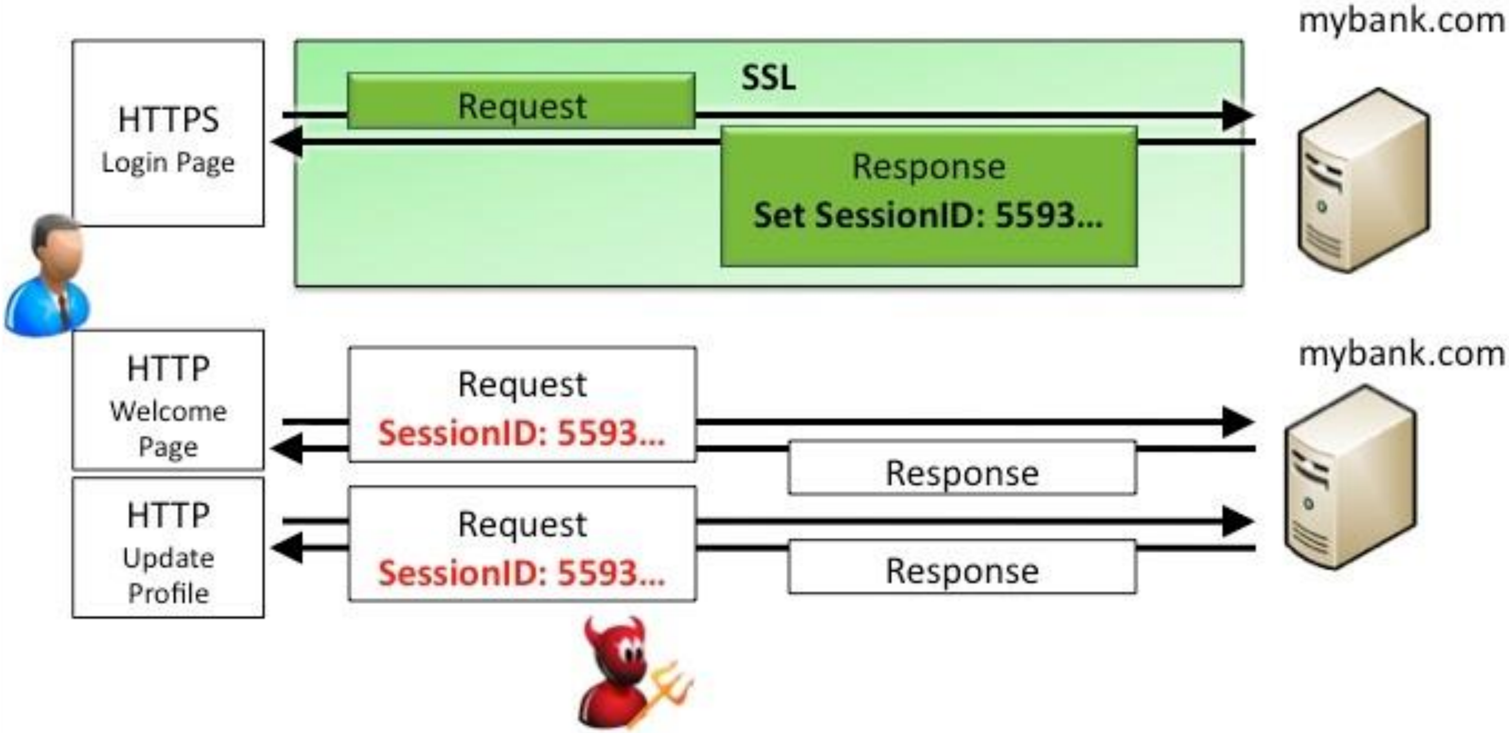
```
No.   Time       Source             Destination        Protocol Length Info
 1183 29.6114490 SamsungE_0b:a8:06  LiteonTe_c8:1a:34  ARP          42 192.168.1.254 is at 88:32:9b:0b:a8:06
 1427 30.5732440 SamsungE_0b:a8:06  LiteonTe_c8:1a:34  ARP          42 192.168.1.254 is at 88:32:9b:0b:a8:06
 1432 31.6962180 SamsungE_0b:a8:06  LiteonTe_c8:1a:34  ARP          42 192.168.1.254 is at 88:32:9b:0b:a8:06
 1433 32.5938430 SamsungE_0b:a8:06  LiteonTe_c8:1a:34  ARP          42 192.168.1.254 is at 88:32:9b:0b:a8:06
 1442 33.6012160 SamsungE_0b:a8:06  LiteonTe_c8:1a:34  ARP          42 192.168.1.254 is at 88:32:9b:0b:a8:06
 1448 34.5839120 SamsungE_0b:a8:06  LiteonTe_c8:1a:34  ARP          42 192.168.1.254 is at 88:32:9b:0b:a8:06
```

```
⊞ Frame 1432: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
⊞ Ethernet II, Src: SamsungE_0b:a8:06 (88:32:9b:0b:a8:06), Dst: LiteonTe_c8:1a:34 (20:16:d8:c8:1a:34)
⊞ [Duplicate IP address detected for 192.168.1.254 (88:32:9b:0b:a8:06) - also in use by ac:5d:10:33:c7:c9 (frame 1431)]
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: SamsungE_0b:a8:06 (88:32:9b:0b:a8:06)
    Sender IP address: 192.168.1.254 (192.168.1.254)
    Target MAC address: LiteonTe_c8:1a:34 (20:16:d8:c8:1a:34)
    Target IP address: 192.168.1.205 (192.168.1.205)
```

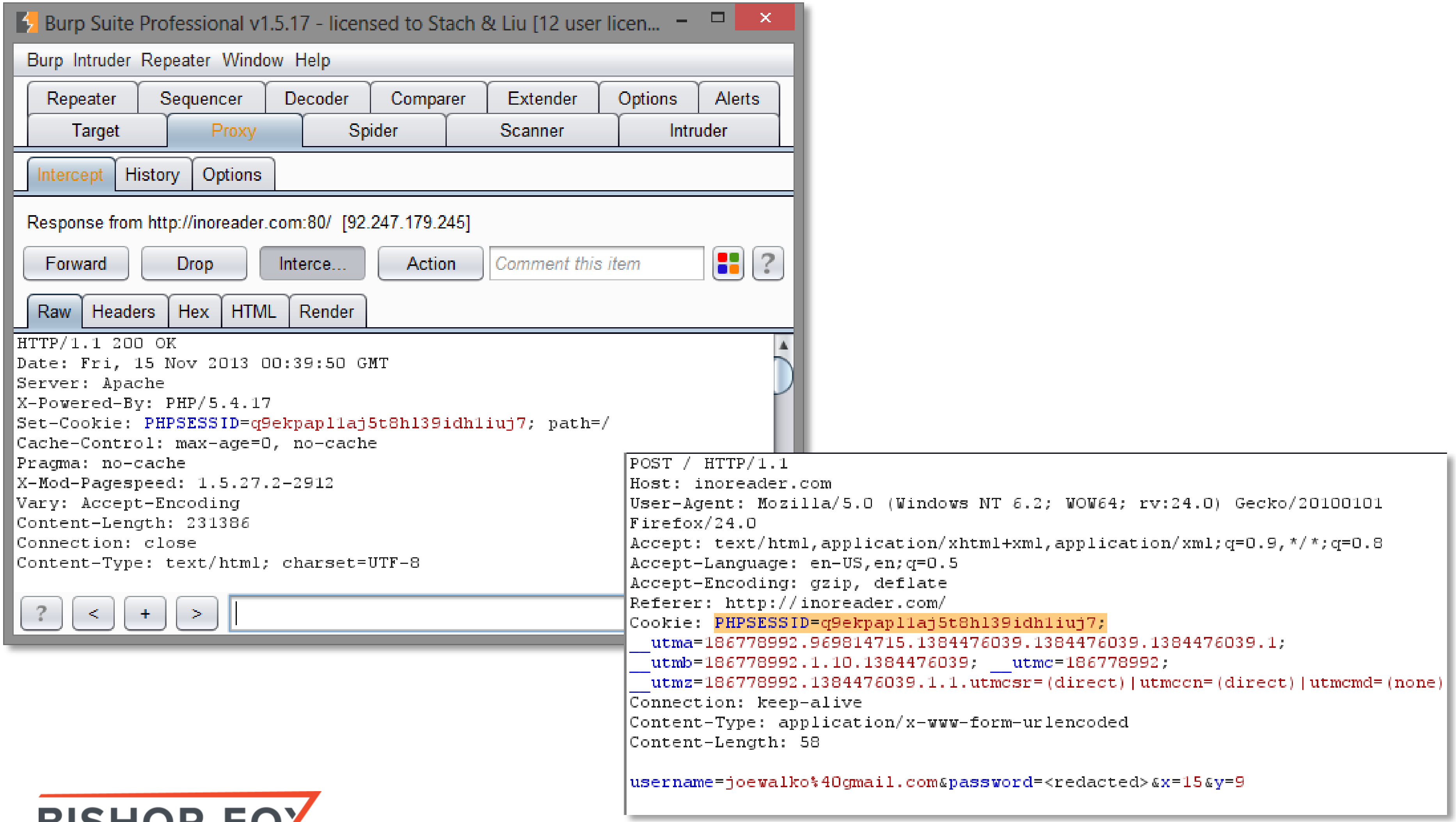
```
0000  20 16 d8 c8 1a 34 88 32  9b 0b a8 06 08 06 00 01    ....4.2 ........
0010  08 00 06 04 00 02 88 32  9b 0b a8 06 c0 a8 01 fe   .......2 ........
0020  20 16 d8 c8 1a 34 c0 a8  01 cd                      ....4.. ..
```

88:32:9b:0b:a8:06 is actually the Android Phone pretending to be the default gateway at 192.168.1.254

Stealing Unencrypted Session IDs



Web Session Hijacking using dSploit



Response from http://inoreader.com:80/ [92.247.179.245]

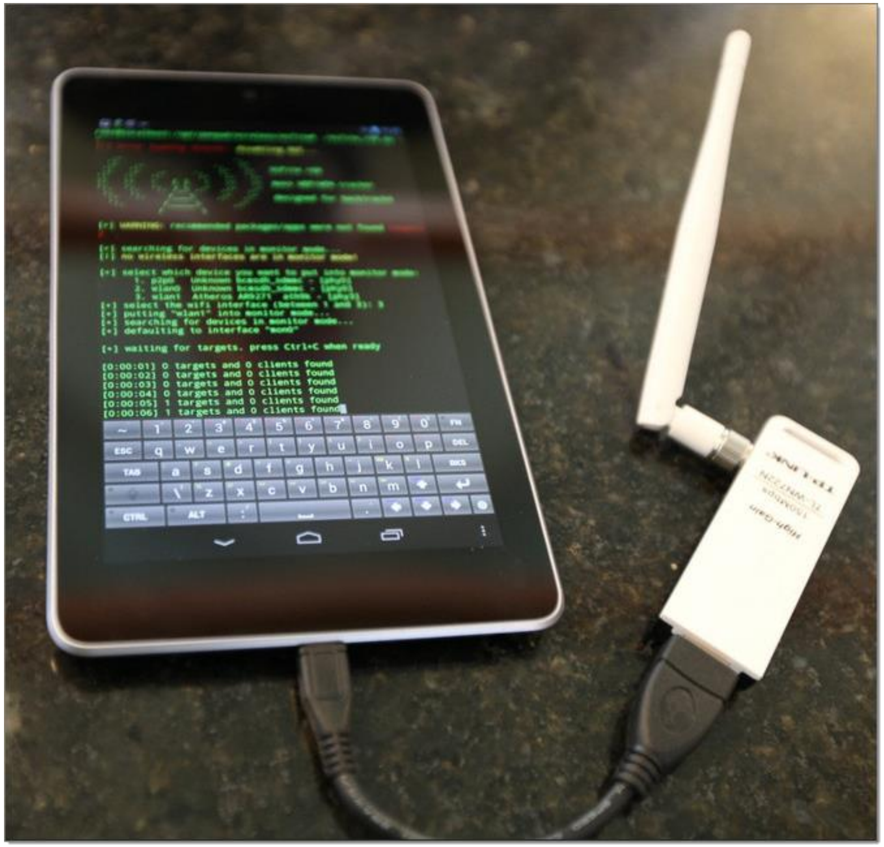
```
HTTP/1.1 200 OK
Date: Fri, 15 Nov 2013 00:39:50 GMT
Server: Apache
X-Powered-By: PHP/5.4.17
Set-Cookie: PHPSESSID=q9ekpapllaj5t8hl39idhliuj7; path=/
Cache-Control: max-age=0, no-cache
Pragma: no-cache
X-Mod-Pagespeed: 1.5.27.2-2912
Vary: Accept-Encoding
Content-Length: 231386
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
POST / HTTP/1.1
Host: inoreader.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:24.0) Gecko/20100101
Firefox/24.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://inoreader.com/
Cookie: PHPSESSID=q9ekpapllaj5t8hl39idhliuj7;
__utma=186778992.969814715.1384476039.1384476039.1384476039.1;
__utmb=186778992.1.10.1384476039; __utmc=186778992;
__utmz=186778992.1384476039.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

username=joewalko%40gmail.com&password=<redacted>&x=15&y=9
```

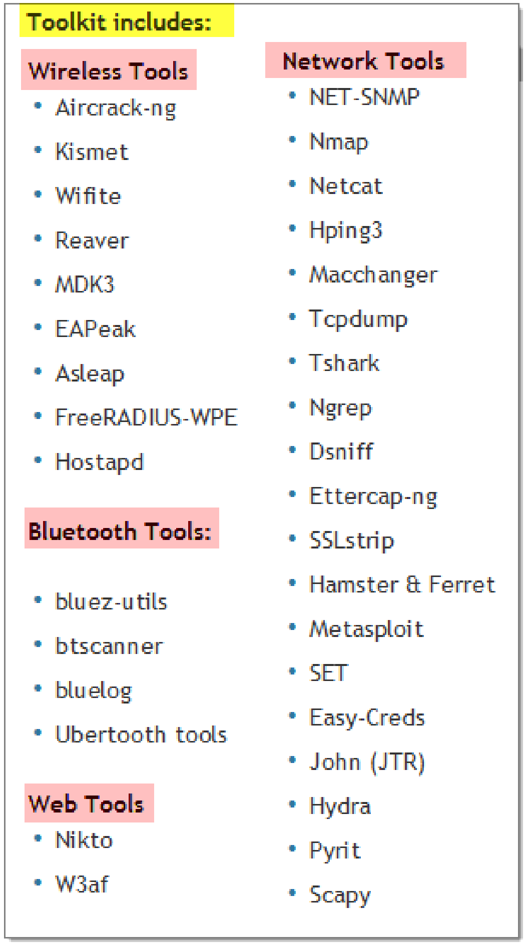
BISHOP FOX

PwnPad

NEXUS 7 PENTEST DEVICE



```
[+] WARNING: recommended packages/apps were not found

[+] searching for devices in monitor mode...
[!] no wireless interfaces are in monitor mode!

[+] select which device you want to put into monitor mode:
     1. p2p0   Unknown bcm4330_sdmmc - [phy0]
     2. wlan0  Unknown bcm4330_sdmmc - [phy0]
     3. wlan1  Atheros AR9271  ath9k - [phy1]
[+] select the wifi interface (between 1 and 3): 3
[+] putting "wlan1" into monitor mode...
[+] searching for devices in monitor mode...
[+] defaulting to interface "mon0"

[+] waiting for targets. press Ctrl+C when ready

[0:00:01] 0 targets and 0 clients found
[0:00:02] 0 targets and 0 clients found
[0:00:03] 0 targets and 0 clients found
[0:00:04] 0 targets and 0 clients found
[0:00:05] 1 targets and 0 clients found
[0:00:06] 1 targets and 0 clients found
```



Toolkit includes:

Wireless Tools

- Aircrack-ng
- Kismet
- Wifite
- Reaver
- MDK3
- EAPeak
- Asleap
- FreeRADIUS-WPE
- Hostapd

Bluetooth Tools:

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools

Web Tools

- Nikto
- W3af

Network Tools

- NET-SNMP
- Nmap
- Netcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng
- SSLstrip
- Hamster & Ferret
- Metasploit
- SET
- Easy-Creds
- John (JTR)
- Hydra
- Pyrit
- Scapy

Defenses

AVOID BEING PROBED

Defenses

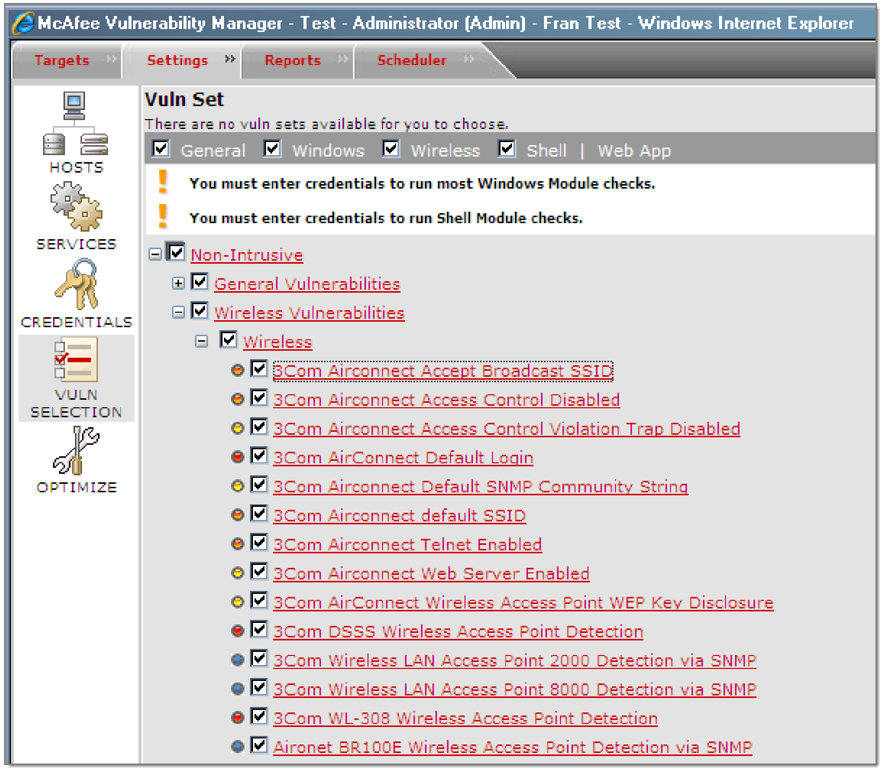
RECOMMENDATIONS

- Conduct regular wireless assessments
- Employ strong encryption and authentication methods
- Employ wireless IDS/IPS
- Secure wireless clients (laptops, phones, …)

Defenses

RECOMMENDATIONS

Use "wireless checks" of network vulnerability scanners



McAfee Vulnerability Manager - Test - Administrator (Admin) - Fran Test - Windows Internet Explorer

Targets | Settings | Reports | Scheduler

HOSTS
SERVICES
CREDENTIALS
VULN SELECTION
OPTIMIZE

Vuln Set

There are no vuln sets available for you to choose.

☑ General ☑ Windows ☑ Wireless ☑ Shell | Web App

! You must enter credentials to run most Windows Module checks.

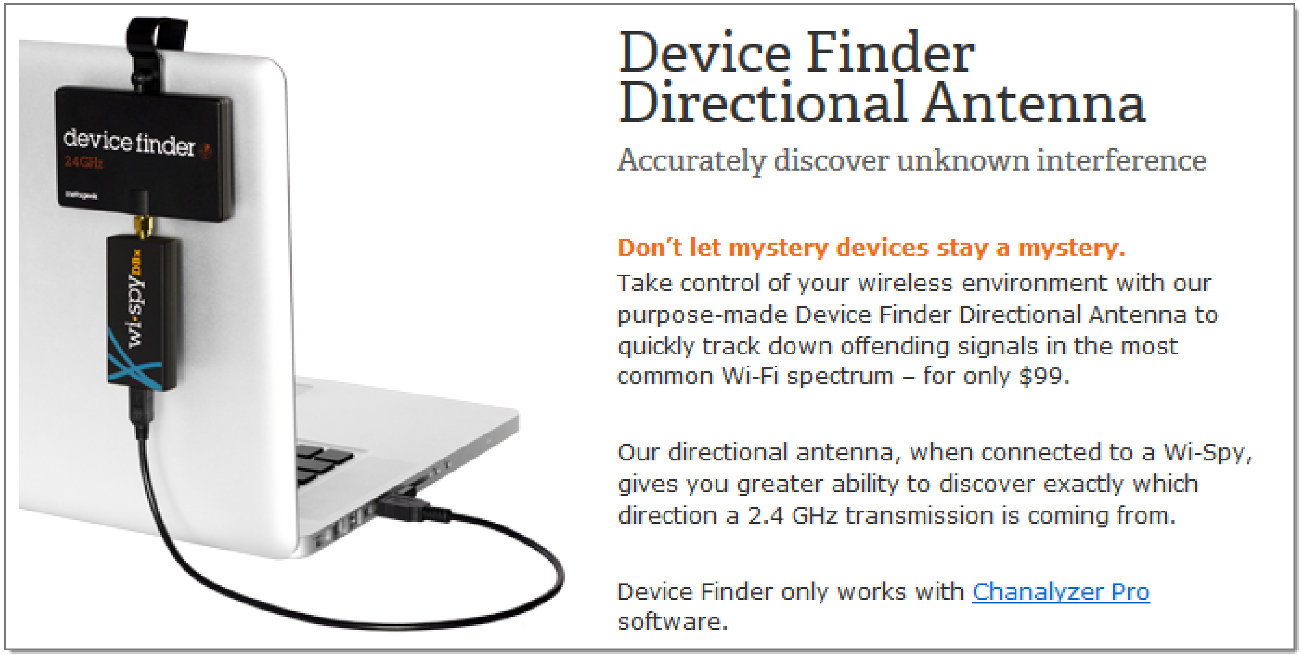
! You must enter credentials to run Shell Module checks.

- ☑ Non-Intrusive
  - ☑ General Vulnerabilities
  - ☑ Wireless Vulnerabilities
    - ☑ Wireless
      - ☑ 3Com Airconnect Accept Broadcast SSID
      - ☑ 3Com Airconnect Access Control Disabled
      - ☑ 3Com Airconnect Access Control Violation Trap Disabled
      - ☑ 3Com AirConnect Default Login
      - ☑ 3Com Airconnect Default SNMP Community String
      - ☑ 3Com Airconnect default SSID
      - ☑ 3Com Airconnect Telnet Enabled
      - ☑ 3Com Airconnect Web Server Enabled
      - ☑ 3Com AirConnect Wireless Access Point WEP Key Disclosure
      - ☑ 3Com DSSS Wireless Access Point Detection
      - ☑ 3Com Wireless LAN Access Point 2000 Detection via SNMP
      - ☑ 3Com Wireless LAN Access Point 8000 Detection via SNMP
      - ☑ 3Com WL-308 Wireless Access Point Detection
      - ☑ Aironet BR100E Wireless Access Point Detection via SNMP

Defenses

RECOMMENDATIONS

Physically track down rogue access points and malicious devices



Device Finder Directional Antenna

Accurately discover unknown interference

Don't let mystery devices stay a mystery.
Take control of your wireless environment with our purpose-made Device Finder Directional Antenna to quickly track down offending signals in the most common Wi-Fi spectrum – for only $99.

Our directional antenna, when connected to a Wi-Spy, gives you greater ability to discover exactly which direction a 2.4 GHz transmission is coming from.

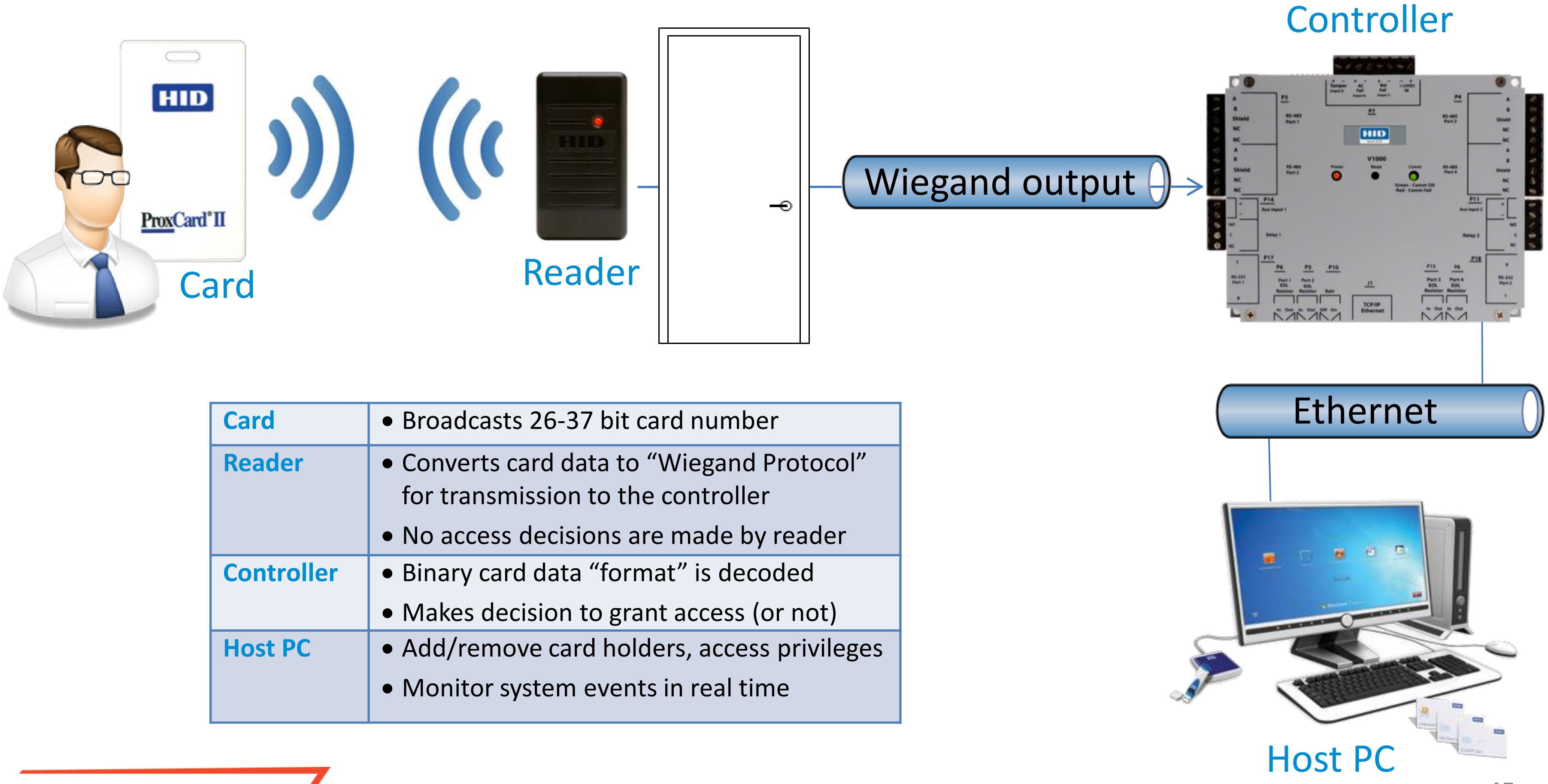
Device Finder only works with Chanalyzer Pro software.

RFID Hacking Tools

PENTEST TOOLKIT

How a Card Is Read

POINTS OF ATTACK



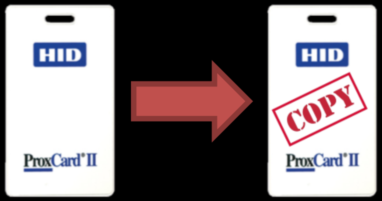
Card	• Broadcasts 26-37 bit card number
Reader	• Converts card data to “Wiegand Protocol” for transmission to the controller • No access decisions are made by reader
Controller	• Binary card data “format” is decoded • Makes decision to grant access (or not)
Host PC	• Add/remove card holders, access privileges • Monitor system events in real time

Methodology

3 STEP APPROACH

1. Silently steal badge info

2. Create card clone

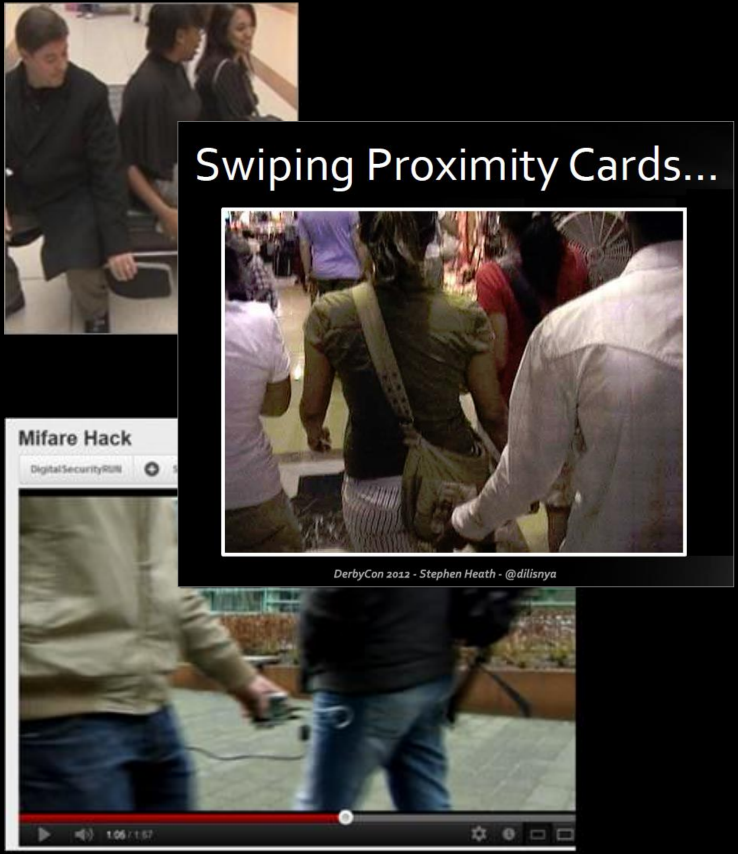


3. Enter and plant backdoor

Distance Limitations

A$$ GRABBING METHOD

Existing RFID hacking tools only work when a few centimeters away from badge

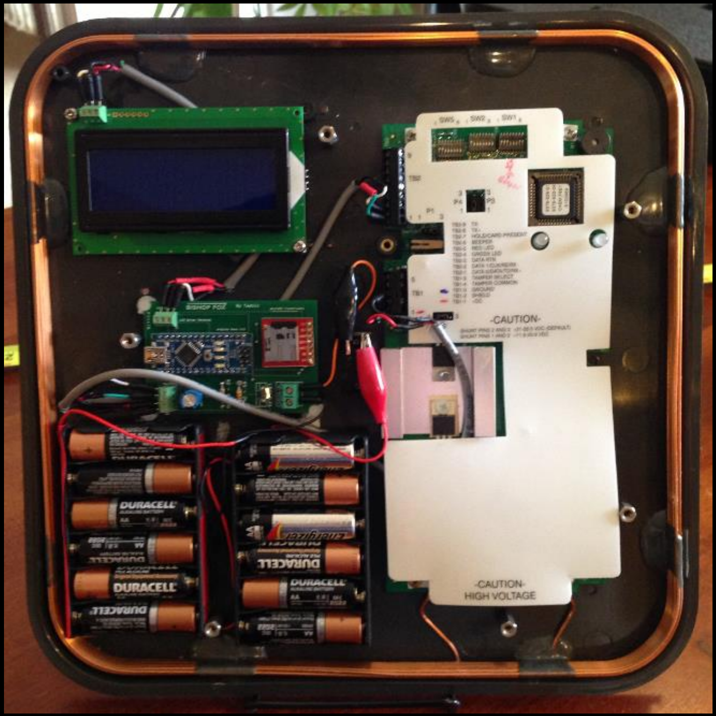

Swiping Proximity Cards...
DerbyCon 2012 - Stephen Heath - @dilisnya
Mifare Hack
DigitalSecurityRUN
1:06 / 1:57

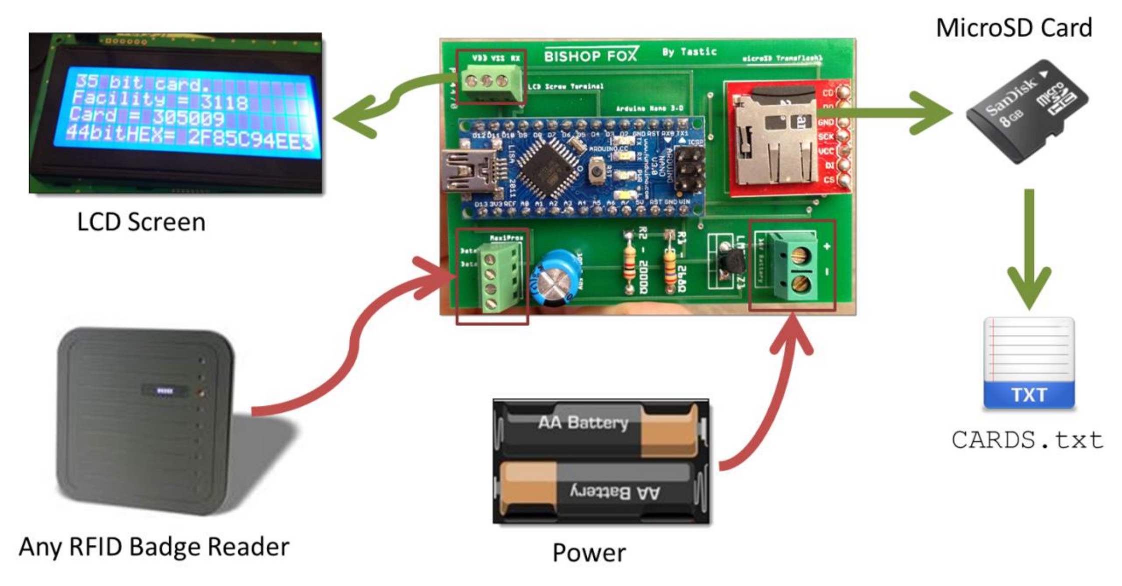
```
hid fskdemod
98139d7c32 (5432)
98139d7c32 (5432)
98139d7c32 (5432)
```

```
proxmark3> lf hid sim 98139d7c32
Emulating tag with ID 98139d7c32
#db# Stopped
```

Custom PCB

TASTIC RFID THIEF





```
35 bit card.
Facility = 3118
Card = 305009
44bitHEX= 2F85C94EE3
```

Programmable Cards

Cloning to T55x7 Card using Proxmark3

- Simulate data *and behavior* of any badge type

- T55x7 Cards
- Q5 cards (T5555)

- HID Prox Cloning – example:

```
lf hid clone <HEX>
lf hid clone 20068d83d5
```

- Indala Prox Cloning – example:

```
lf indalaclone <HEX>
lf indalaclone 4f2b04795
```

Thank You

Bishop Fox – see for more info:
http://www.bishopfox.com/
@bishopfox

BISHOP FOX

We're hiring!