

# **Wireless Security: Principles & Tools**

NSRC

# **Reminder: Aspects of IT Security**

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation
- Risk management

# “Wireless Security”

- The term “wireless security” is most often used as synonym for “keeping unwanted users out of your network” & “encrypting traffic”
- This addresses to some extent (!)
  - Confidentiality
  - Integrity
  - Availability
- However, none of these are fully secured by “wireless security”!

# “Wireless Security”

- The idea of “wireless security” seems to be changing:  
in the old days, it meant:  
“How do I keep the outsider out”?
- Maybe, today it means:  
“How do I keep the insider from clogging up my network?”

# “Wireless Security”

- When discussing “wireless security”, don't assume that the wired side is so much more secure!
- Most threats are NOT specifically wireless!
- Biggest threats today probably:
  - Windows computers
  - Virus/bots/trojans
  - Uncontrolled file sharing
  - Systems not prepared for high bandwidth connectivity and many dynamic users
  - ...

# Category of Users who may cause problems on a wireless network

- Unintentional users
- War drivers
- Rogue access points
- Eavesdroppers- tool Kismet

# “Wireless Security”

- A healthy way of looking at security on the network level:
  - The network is the streets and roads
  - Many people and vehicles travel on these roads
  - Streets and roads are open, or mostly open – we don't lock people into their houses
  - If we need to transport money from A to B – we use a protected vehicle (= “end-to-end security”)

# Physical Security





# Physical Security

- Cables- Hidden and fastened
- Switches- in Cabinets (Locked Cabinets)
- Power-locked in cabinets
- Water- Equipment at-least 30cm above ground
- Masts

# General Security / Methods for Wireless

## **Hidden / Closed** networks

- The access point is not broadcasting the SSID
- User types in the SSID so as to join
- May be found by passive sniffers anyway eg Kismet
- Misleading “Security by Obscurity”

# General Security / Methods for Wireless

## **Key based encryption of wireless network (WEP/WPA)**

- WEP(Wired Equivalent Privacy) uses a shared 40-bit key to encrypt data between the access point and client.  
The key must be entered on the Aps as well as on each of the clients.
- WPA takes longer, but is crackable
- If anything, use WPA2 – but even that is vulnerable
- WPA might force you to offer a lot of user support

- WPA (Wi-Fi Protected Access)intended to be a backwards compatible interim solution while the full standard 802.11i (WPA2) was developed
- Uses TKIP (Temporary Key Integrity Protocol) that continuously and automatically changes the keying material between clients and access points.

# General Security / Methods for Wireless

## **MAC (hardware address) based ACL**

- MAC black/whitelisting on AP or gateways
- Might be useful for stable user groups, registered equipment
- Difficult to maintain, easy to spoof

# General Security / Methods for Wireless

## **Summary of key based and ACL methods**

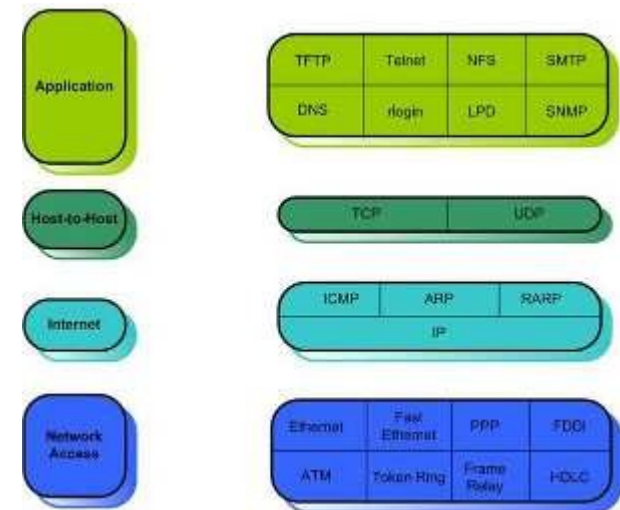
- While none of those offers 100% security, appropriate combinations may give reasonable protection
- All of these are hard to maintain with fast changing, large usergroups
- All of these pose communication challenges – how to hand out keys? How to keep MAC lists up-to-date?

# Is your wifi secure?



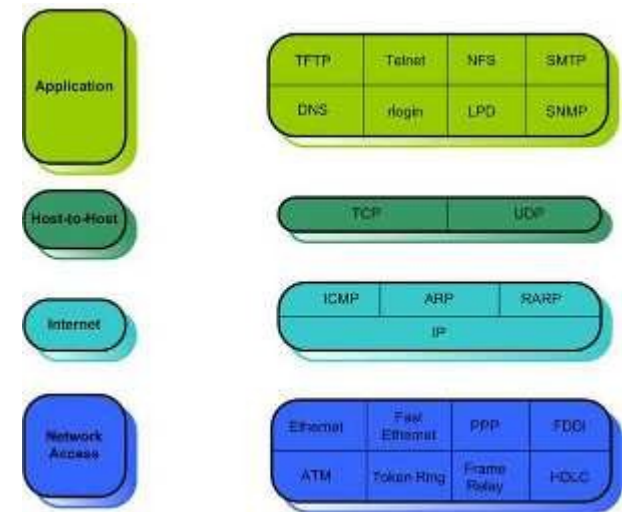
# Essential tools

- **Reminder: think layers!**
- **Working with wireless security to some extent means working with compromising tools**





# Essential tools



## Physical layer:

- Spectrum analyzers: airview, wispy
- **Packet sniffers: kismet** – Netstumbler (windows)

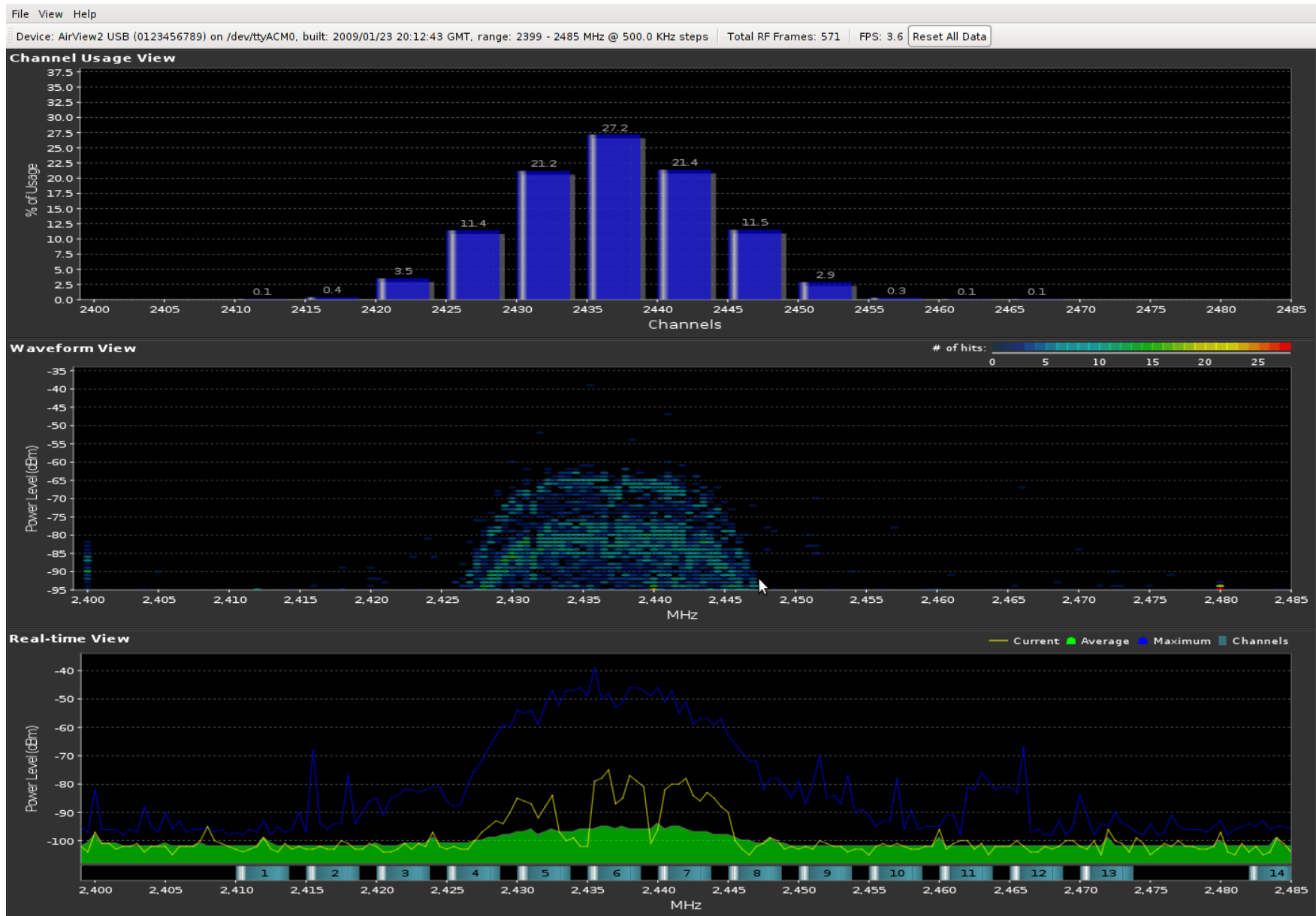
## Network layer:

- etherape (no admin tool – just quick visual overview)
- General networking and management tools: **wireshark**, ntop, mrtg, rrdtool, **nmap**, **mtr**
- WEP/WPA/WPA2 cracking: aircrack etc
- Tool collections: **backtrack**

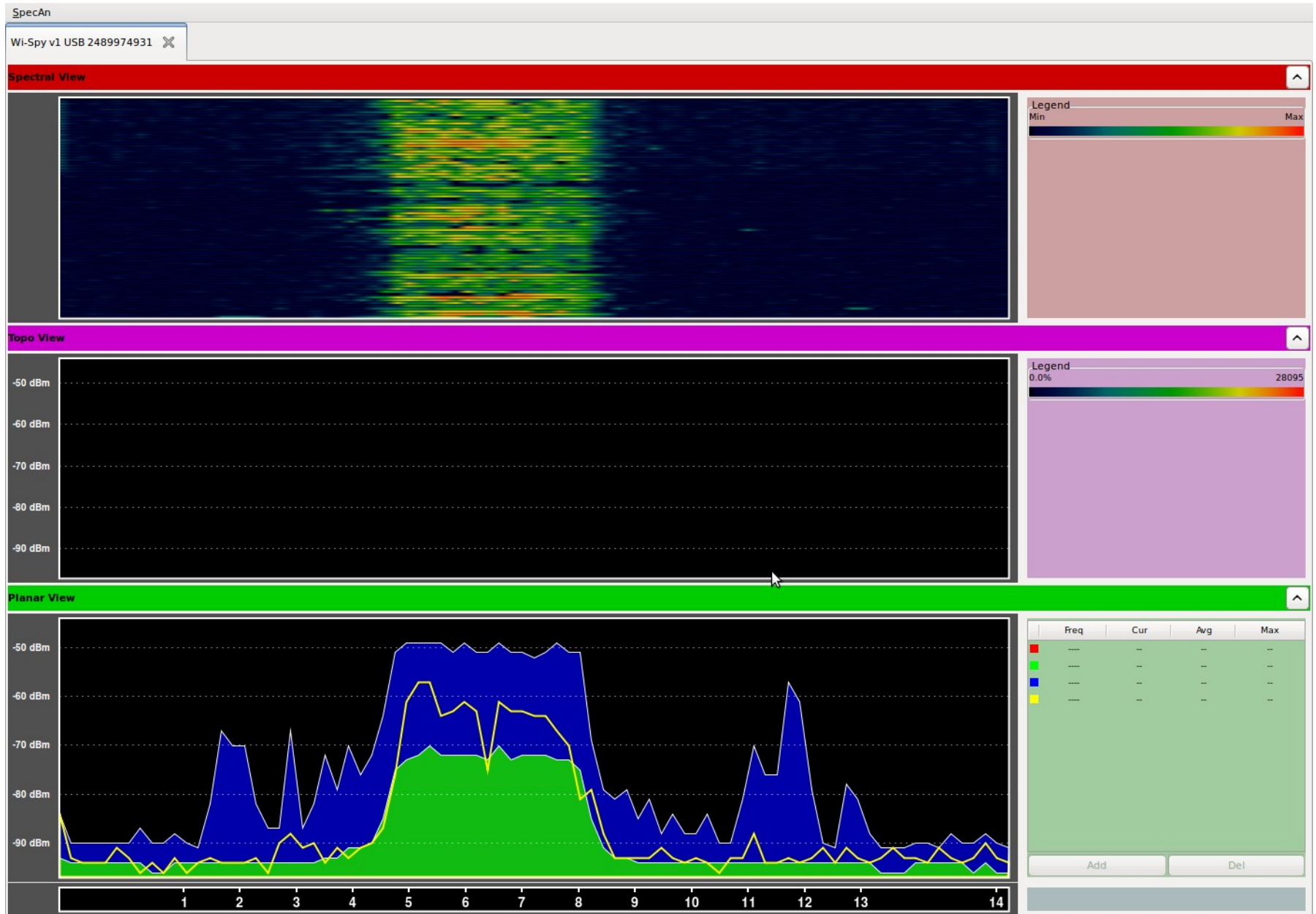
# Spectrum Analyzers

- Real spectrum analyzers very expensive, but USB analyzers are a reasonable compromise
- e.g. AirView (2.4 GHz), WiSpy (2.4 – 5.8 GHz)
- Pure physical layer! They will show you non-WiFi stuff, like microwave ovens, jamming attempts, bluetooth phones, etc

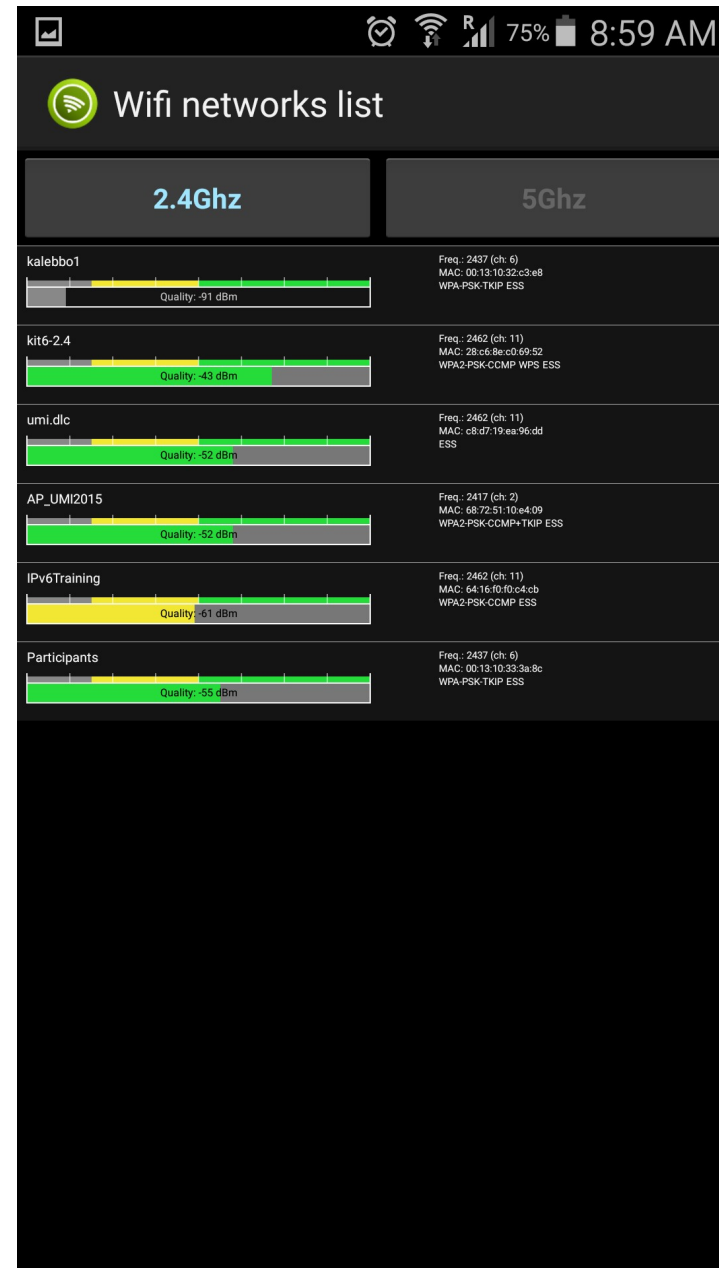
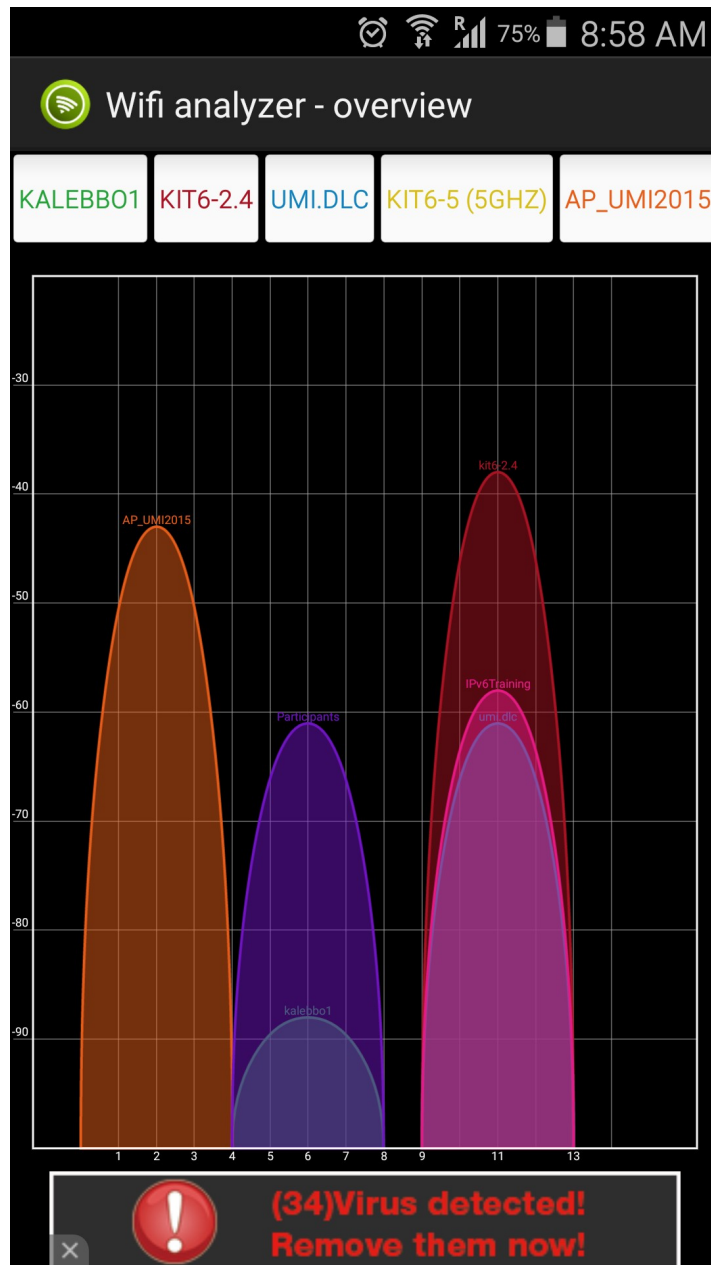
# Spectrum Analyzers: Airview



# Spectrum Analyzers: WiSpy



# Android wifi analyzer



# What is kismet?

- Kismet is an 802.11 **layer2 wireless network detector**, sniffer, and intrusion detection system.
- Works in **raw monitoring** (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic.
- It is **passively collecting packets** and detecting standard named networks, detecting (and given time, decloaking) **hidden networks**, and presence of **nonbeaconing networks** via data traffic.

# kismet - strengths

- Server – Client architecture
- Drones: distributed kismet servers running on remote devices, reporting back to central server, allow for the building of distributed reporting and intrusion detection systems
- Kismet is powerful - especially when combined with other tools like wireshark, nmap

# kismet - Installing I

- The following guide assumes you are on Ubuntu 9.10 / GNU/Linux - but works for other systems accordingly.
- Get kismet via apt-get (or synaptic)  

```
$ apt-get install kismet
```
- edit /etc/kismet.conf -  
Definition of sources is a must. Sources are defined as:  

```
ncsource=interface:options
```

  
For the list of sourcetypes, see the README or online documentation.



# kismet - Installing II

- `$ vi /etc/kismet.conf`  
`ncsource=interface:options`  
  
e.g.  
`ncsource=wlo1:type=atheros`
- start kismet  
`$ kismet`

# Start screen

```
root@wirelessdefence:~  
File Edit View Terminal Tabs Help  
Network List (Autofit)  
Name           T W Ch  Packts  Flags  IP Range  
default        A N 006    9 F    192.168.0.1  
! iyonder.net  A N 005   42 U4    10.254.178.254  
! iyonder.net  A N 001   22 A3    10.254.178.0  
! eurospot    A N 001   19 U4    204.26.5.166  
! NETGEAR      A 0 006    5      0.0.0.0  
. eurospot    A N 011   14      0.0.0.0  
! belkin54g    A Y 011   17      0.0.0.0  
! iyonder.net  A N 011   16 A3    10.254.178.0  
! tsunami     A Y 007   17      0.0.0.0  
! <no ssid>    A 0 003   11      0.0.0.0  
Probe Networks  P N ---    3      0.0.0.0  
! iyonder.net  A N 008   35      0.0.0.0  
. <no ssid>    A Y 011    5      0.0.0.0  
NCDT_NET       A Y 006    1      0.0.0.0  
<no ssid>     A Y 011    1      0.0.0.0  
Info  
Ntwrks        16  
Pckets        228  
Cryptd         4  
Weak           0  
Noise          0  
Discrd         0  
Pkts/s         8  
Elapsd        00:00:20  
Status  
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0  
36\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0  
bssid 00:0A:8A:A2:C8:7F  
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP  
Battery: AC 107%
```

# What does kismet show?

- List of SSIDs

Note: it also shows networks with hidden SSIDs / no beacons - just blank!

If a client associates to those, you will also see the SSID.

# What does kismet show?

- **T = Type**

P Probe request - no associated connection yet

A Access point - standard wireless network

H Ad-hoc - point to point wireless network

T Turbocell - Turbocell aka Karlnet or Lucent Router

G Group - Group of wireless networks

D Data - Data only network with no control packets

# What does kismet show?

- **W = Encryption**
- **Colour = Network/Client Type:**

Yellow      Unencrypted Network

Red          Factory default settings in use!

Green       Secure Networks (WEP, WPA etc..)

Blue        SSID cloaking on / Broadcast SSID disabled

# kismet - options

- **(Some of the) Options:**
  - c Show clients in current network
  - h Help
  - i Detailed info about current network
  - s Sort network list
  - r Packet rate graph
  - a Statistics
  - p Dump packet type
  - Q Quit

# kismet - Network info

File Edit View Terminal Help

### Network List (SSID)

Network Details	Size	Info
Name : mySecure	0.40	80B
		0B
		0B
SSID : mySecure		0B
Server : localhost:2501		0B
BSSID : 0A:15:6D:AD:C8:28		0B
Carrier : IEEE 802.11b		8k
Manuf : Unknown	4.36	58k
Max Rate: 18.0		
BSS Time: a94c87181		
Max Seen: 1000 kbps		
First : Wed Mar 3 21:19:19 2010		
Latest : Wed Mar 3 21:21:03 2010		
Clients : 0		
Type : Access Point (infrastructure)		
Info :		
Channel : 5		
Privacy : Yes		
Encrypt : TKIP WPA PSK		
Decryptd: No		
Beacon : 25600 (26.214400 sec)		
Packets : 391		
Data : 0		
LLC : 391		
Crypt : 0		
Weak : 0		

75% (+) Down

Battery: AC 99%

Info

Ntwrks 7

Pckets 1550

Cryptd 58

Weak 0

Noise 0

Discrd 0

Pkts/s 27

my\_int

Ch: 52

Elapsd 00:01:44

:BD via UDP

:37 via UDP

:19 via UDP

57 via ARP

# Client info

FileEditViewTerminalHelp

Network List (SSID)

Name

TWCh

Packts

Flags

IP Range

Size

Info

Ntwrks

Client List (Autofit)

T

MAC

Manuf

Data

Crypt

Size

IP Range

Sgn

Nse

S

01:00:5E:00:00:02

Unknown

0

0

0B

0.0.0.0

0

0

S

FF:FF:FF:FF:FF:FF

Unknown

0

0

0B

0.0.0.0

0

0

F

00:00:0C:07:AC:00

Cisco

7

0

560B

140.105.28.125

0

0

F

00:0F:F8:28:34:00

Cisco

20

0

1k

140.105.28.125

0

0

F

00:11:50:E7:67:DE

Belkin

112

0

77k

196.35.64.36

0

0

S

00:14:A5:30:D9:B6

Unknown

58

0

15k

192.168.4.203

0

0

S

00:25:00:3D:75:29

Unknown

13

0

1k

192.168.4.214

0

0

S

01:80:C2:00:00:00

Unknown

0

0

0B

0.0.0.0

0

0

!

F

00:12:80:8F:68:14

Cisco

17

0

2k

0.0.0.0

0

0

!

F

00:0F:F8:20:EC:00

Cisco

12

0

948B

140.105.28.126

0

0

F

00:01:02:97:C1:57

Unknown

12

0

768B

10.10.11.254

0

0

F

00:15:6D:AB:EF:C9

Unknown

42

0

6k

0.0.0.0

0

0

F

00:25:4B:B3:EC:28

Unknown

2

0

376B

140.105.28.39

0

0

S

33:33:00:00:00:FB

Unknown

0

0

0B

0.0.0.0

0

0

F

00:16:CB:A7:EB:CF

Apple

1

0

182B

140.105.28.76

0

0

F

00:17:F2:00:B2:64

Unknown

3

0

464B

140.105.28.30

0

0

F

00:25:4B:B3:ED:F0

Unknown

1

0

110B

140.105.28.38

0

0

E

00:17:F2:50:77:FC

Unknown

3

0

292B

192.168.4.220

0

0

F

00:1F:F3:46:06:A5

Unknown

5

0

629B

192.168.4.216

0

0

S

01:00:5E:00:00:01

Unknown

0

0

0B

0.0.0.0

0

0

F

00:1E:52:F1:F7:2C

Unknown

3

0

358B

140.105.28.116

0

0

S

01:00:0C:CC:CC:CC

Unknown

0

0

0B

0.0.0.0

0

0

F

00:16:CB:AE:49:BF

Apple

2

0

220B

140.105.28.115

0

0

F

00:16:CB:A5:D1:4E

Apple

2

0

220B

192.168.4.221

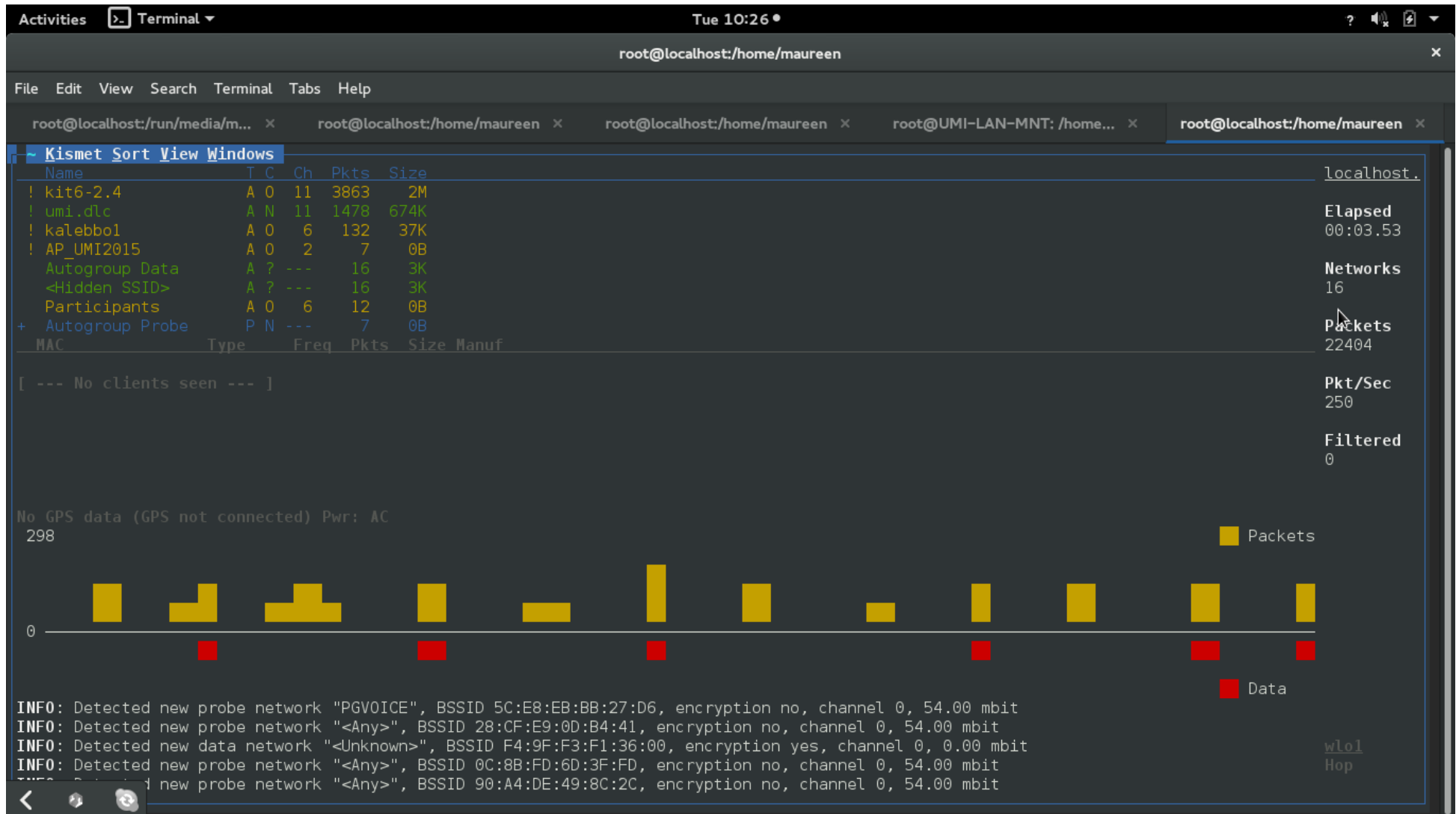
0

0

Battery: AC 99%



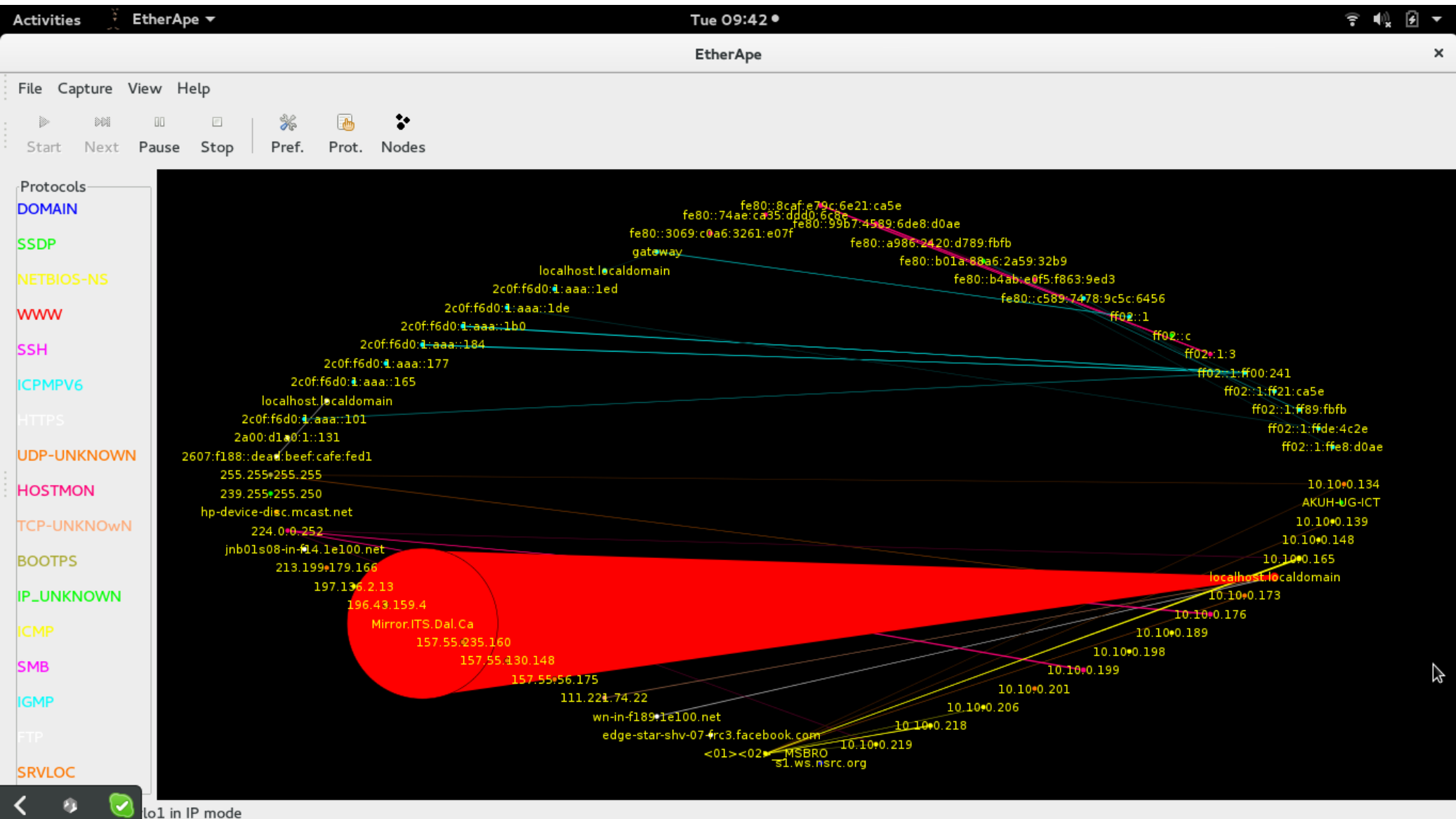
# Kismet scan UMI



# What is etherApe?

- **EtherApe** is not really a security tool, but it gives a **very useful quick first view of traffic** in your network.
- For example, in case you have a spam virus in your network, you will see this immediately.
- It also gives you a good feel for what various applications, such as skype or torrent clients, are doing to your network.

# etherape screenshot



# What is Wireshark?

- Wireshark, formerly known as ethereal, is a powerful packet dumping and analyzing program
- Extremely nice filtering for fast identification of problems, e.g. specific protocols (e.g. ARP), IP numbers, or keywords

# wireshark screenshot

Activities Wireshark Tue 10:06

\*wlo1 [Wireshark 1.12.6 (Git 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
14844	87.67759900	10.10.0.167	208.82.16.68	HTTP	1423	POST /main/authorization/doSignIn?target=http%3A%2F%2Fwww.gogo6.com%2Fmain HTTP/1.1 (a
14845	87.67879600	10.10.0.241	10.10.0.167	DNS	199	Standard query response 0x304e CNAME api.ning.com.edgesuite.net CNAME al564.g.akamai.r

▶ Frame 14844: 1423 bytes on wire (11384 bits), 1423 bytes captured (11384 bits) on interface 0

▶ Ethernet II, Src: LiteonTe\_1e:43:c9 (20:16:d8:1e:43:c9), Dst: 2e:54:46:de:4c:2e (2e:54:46:de:4c:2e)

▶ Internet Protocol Version 4, Src: 10.10.0.167 (10.10.0.167), Dst: 208.82.16.68 (208.82.16.68)

▶ Transmission Control Protocol, Src Port: 46185 (46185), Dst Port: 80 (80), Seq: 10016, Ack: 43678, Len: 1357

▶ Hypertext Transfer Protocol

▶ POST /main/authorization/doSignIn?target=http%3A%2F%2Fwww.gogo6.com%2Fmain HTTP/1.1\r\n

Host: www.gogo6.com\r\n

User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86\_64; rv:40.0) Gecko/20100101 Firefox/40.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://www.gogo6.com/main/authorization/signIn?target=http%3A%2F%2Fwww.gogo6.com%2Fmain\r\n

▶ [truncated]Cookie: xg\_cookie\_check=1; xn\_visitor=41d954fb-9554-400d-93ba-ab1160ebb2f6; ning\_session=LFPcVf8dptIwQLiveA/U9igk5bAExL4HC70NoTbA+K0nezozXPqzfNDv2VVvPDC

Connection: keep-alive\r\n

Content-Type: application/x-www-form-urlencoded\r\n

Content-Length: 68\r\n

\r\n

[Full request URI: <http://www.gogo6.com/main/authorization/doSignIn?target=http%3A%2F%2Fwww.gogo6.com%2Fmain>]

[HTTP request 10/11]

[Prev request in frame: 4488]

[Next request in frame: 15060]

0000 2e 54 46 de 4c 2e 20 16 d8 1e 43 c9 08 00 45 00 .TF.L. . .C...E.

0010 05 81 bb bb 40 00 04 06 8e 74 0a 0a 00 a7 d0 52 ....@.@. .t....R

0020 10 44 b4 69 00 50 67 12 ab e5 92 02 a1 c5 80 18 .D.i.Pg. ....

0030 03 fc dd 54 00 00 01 01 08 0a 02 22 7b b4 cf c6 ...T.... ."{...

0040 fe 92 50 4f 53 54 20 2f 6d 61 69 6e 2f 61 75 74 ..POST / main/aut

mp/wireshark\_pcap... Packets: 22199 · Displayed: 22199 (100.0%) · Dropped: 2357 (10.6%) Profile: Default

# Wireshark: is that my password?

Activities Wireshark Tue 10:12

\*wlo1 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Follow TCP Stream (tcp.stream eq 52)

Stream Content

```
HTTP/1.1 200 OK
Date: Tue, 15 Sep 2015 06:52:56 GMT
Server: Ning HTTP Server 2.0
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: ning_session=LFPcvf8dptIwQLiveA/U9igk5bAExL4HC70NoTbA+K0nezozXPqzfNDv2VVvPDG0EC2ESTnq4QM=; xn_track=rp%252C%25252F%252Crc%252C0%252Csi%252C1442299907%252Cse%252C1442300807; 2__utma=^ning.1505371918771:3993126.234758204.1442299907.1442299907.1; 2__utmb=^ning.1442301718771:3993126.3.9.1442299922571; 2__utmc=^ning.1505371918771:3993126; 2__utmz=^ning.1458067907415:3993126.1442299907.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); 2__utmv=^ning.1442299918770;; __utma=3993126.1832819415.1442299907.1442299907.1442299907.1; __utmb=3993126.1.10.1442299907; __utmc=3993126; __utmz=3993126.1442299907.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmt=1; xg_sc=%7B%7D
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

xg_token=&emailAddress=maureen%40ccsf.edu&password=topsecret&passwordHTTP/1.1 200 OK
Date: Tue, 15 Sep 2015 06:52:56 GMT
Server: Ning HTTP Server 2.0
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: ning_session=LFPcvf8dptIwQLiveA/U9igk5bAExL4HC70NoTbA+K0nezozXPqzfDPZbjot/HSbHgZRBpjQgAg=; Path=/; Domain=.gogo6.com; Expires=Tue, 15-Sep-15 07:52:56 GMT
X-XN-Trace-Token: 958a42a9-a36d-4c10-baed-705dacab3cb3
```

Entire conversation (83234 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

0000 2e 54 46 de 4c 2e 20 16 d8 1e 43 c9 08 00 45 00 .TF.L. . .C...E.  
0010 05 81 bb bb 40 00 40 06 8e 74 0a 0a 00 a7 d0 52 ....@.@. .t....R  
0020 10 44 b4 69 00 50 67 12 ab e5 92 02 a1 c5 80 18 .D.i.Pg. ....  
0030 03 fc dd 54 00 00 01 01 08 0a 02 22 7b b4 cf c6 ..T.... "{...  
0040 fe 92 50 4f 53 54 20 2f 6d 61 69 6e 2f 61 75 74 ..POST / main/aut

mp/wireshark\_pcapn... Packets: 22199 · Displayed: 137 (0.6%) · Dropped: 2357 (10.6%) Profile: Default

# That was it ...

## Thank you!

<http://nsrc.org>

NSRC



<http://creativecommons.org/licenses/by-nc-sa/3.0/>