Wireless Security – Principles & Tools

Network Startup Resource Center
www.nsrc.org

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Topics Covered

- Network and information security in general
- Wireless security aspects
- Tools for security auditing

General Security: “CIA”

- Preservation of confidentiality, integrity and availability of information.
- Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)

ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

General Security: “CIA”

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)

Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

General Security: “CIA”

Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)

[3] ISACA. (2008). Glossary of terms, 2008.

General Security “CIA”

- Access
  - that you can get to it
- Integrity
  - that information can be trusted to stay unchanged
- Authenticity
  - that it is really what it says it is
  - that it comes from where it says its from
- Availability
  - that information is available

Security Often Means Conflict

Some aspects can be in conflict with one another:

- User Security Problem (Confidentiality)
  - Other people can see & read my traffic
- Network Manager Problem (Availability)
  - I can't see & read my users' traffic

Security Often Means Compromise

- No security is 100%. There are trade-offs.
- Security is connected to usability
- Users will defeat systems that are difficult
  - Complicated passwords get written on post-it notes
  - Frequent password changes lead to weak passwords

More Security Ideas

- Most security problems can not be addressed on network level, but by services and servers.
- According to a 2014 study (source), most attacks come from the inside of networks and organizations.[1]
- Google suggests to no longer make a difference between inner and outer network.[2]

[1] "IBM 2015 Cyber Security Intelligence Index" and the "IBM X-Force Threat Intelligence Quarterly – 2Q 2015."
cited by: https://securityintelligence.com/the-threat-is-coming-from-inside-the-network/
[2] Google BeyondCorp - static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43231.pdf

Security Issues on Campus

- Phishing
- Virus/Malware
  - leading to spam or broadcast storm activity
- Uncontrolled improper use of networks
  - file sharing, videos, torrents
- BYOD
  - uncontrolled quality of network clients
- Operating systems spying

Security Issues on Campus

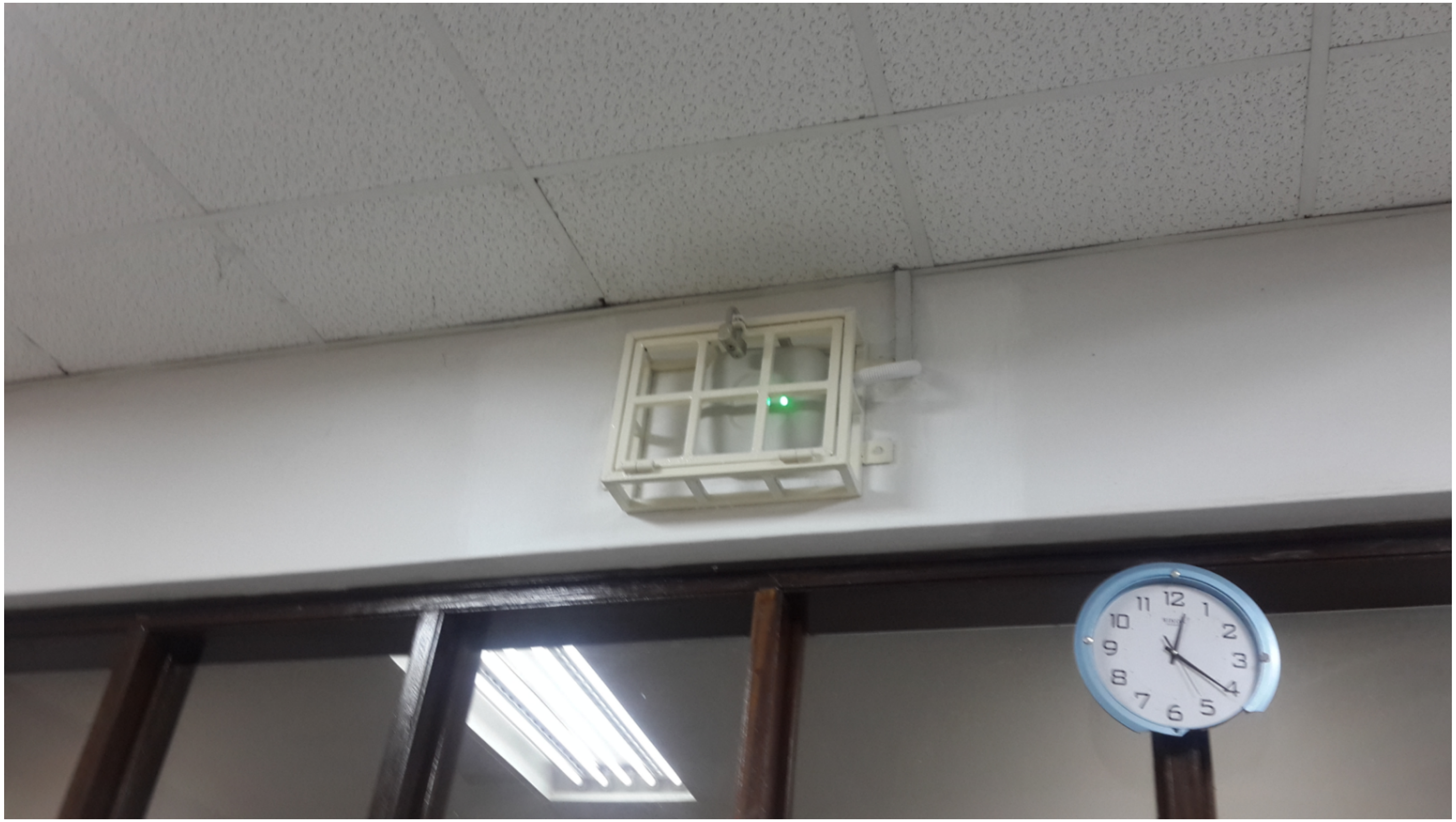
- Non-availability of (wireless) networks
- Physical security – theft and vandalism
- State intrusion / espionage / surveillance
  - as revealed by Snowden and others

Physical security

Don’t forget physical security – for example

- Cables - Hidden and fastened
- Switches, Routers - in locked cabinets
- Power -locked in cabinets
- Water protection - equipment at least 30cm above ground
- Outdoor equipment on secured masts

Physical Security



In this case, physical security interferes with the correct operation of the wireless AP.

Wireless Security

- Main difference between wired and wireless?
  - Wireless is not bound to a physical location
- Securing Ethernet jacks is easy (a lock will do!)
- Authentication is rarely implemented on wired
  - 802.1x does exist for this function
- Securing radio signals is hard (they travel!)

Wireless Security Analogy

- The network is our 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.
- We don’t use passenger cars to transport gold.
  - We use an armored vehicle (“end-to-end security”)
- We try to keep unwanted drivers off the road.
  - We will never have perfect road safety.

Wireless Network Authentication

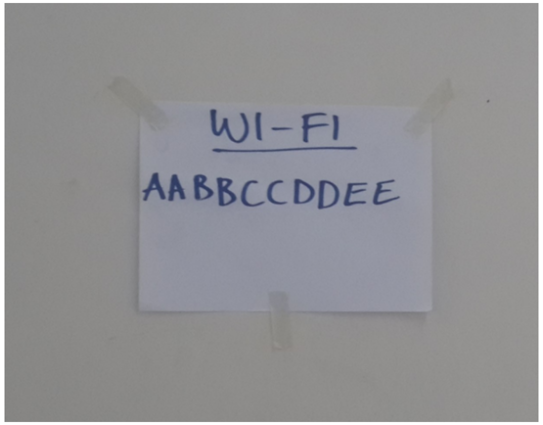
- Authentication can happen in many ways
- MAC Address Restrictions
- Pre-Shared Key based Authentication
  - WPA-PSK – insecure, not scalable
- Captive Portal Authentication
  - Better than a pre-shared key, but not the ideal
- 802.1x based Authentication = Ideal!
  - Performed on centralized servers in the core

MAC Address Restriction

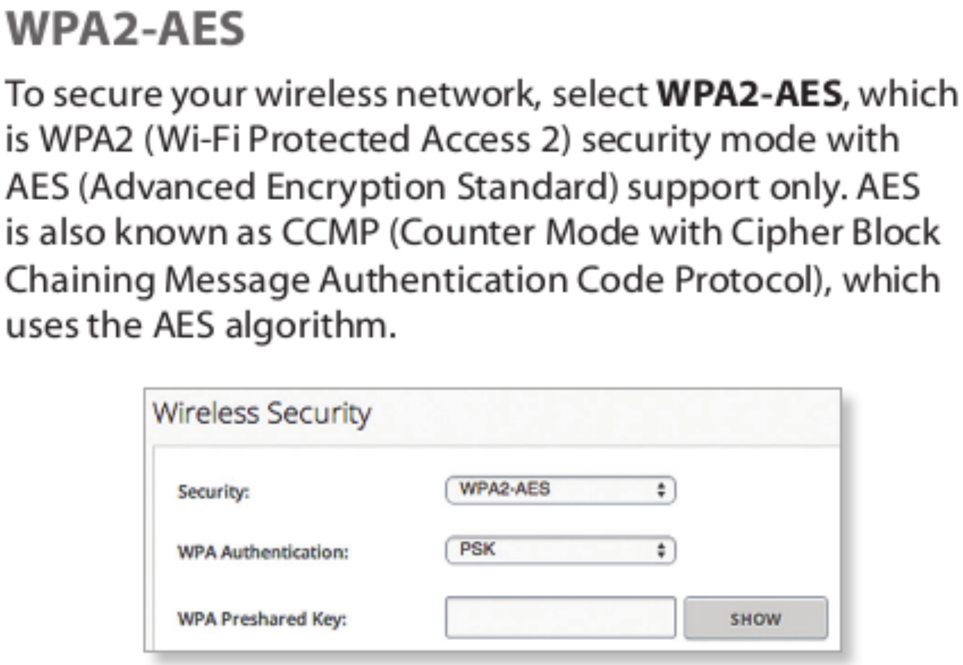
- MAC addresses identify machines, not people
- MAC addresses are easily spoofed
- Adds a lot of work for the helpdesk
    - Move/add/change for end user devices
- MAC restriction ok for infrastructure links & IoT
- Not suitable for user access control

Pre-Shared Keys

- Useful for some tasks
  - Non-critical Sensor devices with no Internet Access
  - Temporary Workshops
- Not recommended for General Use
  - Unless coupled with Portal-based authentication
- Keys will be shared!



802.1x/WPA2 Enterprise Authentication



WPA2-AES

To secure your wireless network, select **WPA2-AES**, which is WPA2 (Wi-Fi Protected Access 2) security mode with AES (Advanced Encryption Standard) support only. AES is also known as CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which uses the AES algorithm.

Wireless Security

Security: WPA2-AES

WPA Authentication: PSK

WPA Preshared Key:

WPA2-AES is the only recommended security mode. WPA1 and WEP are no longer secure.

Source: AirOs7 User Guide / Ubiquiti - http://ubnt.com

802.1x/WPA2 Enterprise Authentication

The important setting is

the address of your **RADIUS server**

We will discuss details of this in the unit on

Authentication

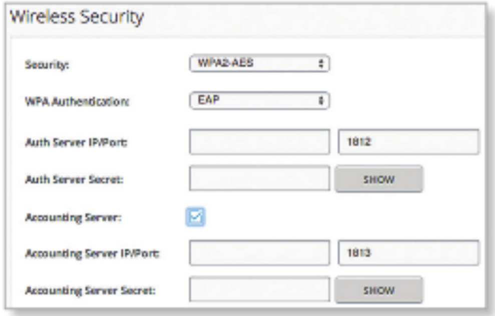
Source: AirOs7 User Guide / Ubiquiti - http://ubnt.com

EAP

Available options depend on the wireless mode, as follows:

EAP - Access Point PTP or Access Point PTMP Mode

The options below apply in *Access Point PTP or Access Point PTMP* mode only.



Wireless Security

Security: WPA2-AES

WPA Authentication: EAP

Auth Server IP/Port: 1812

Auth Server Secret: SHOW

Accounting Server: ☑

Accounting Server IP/Port: 1813

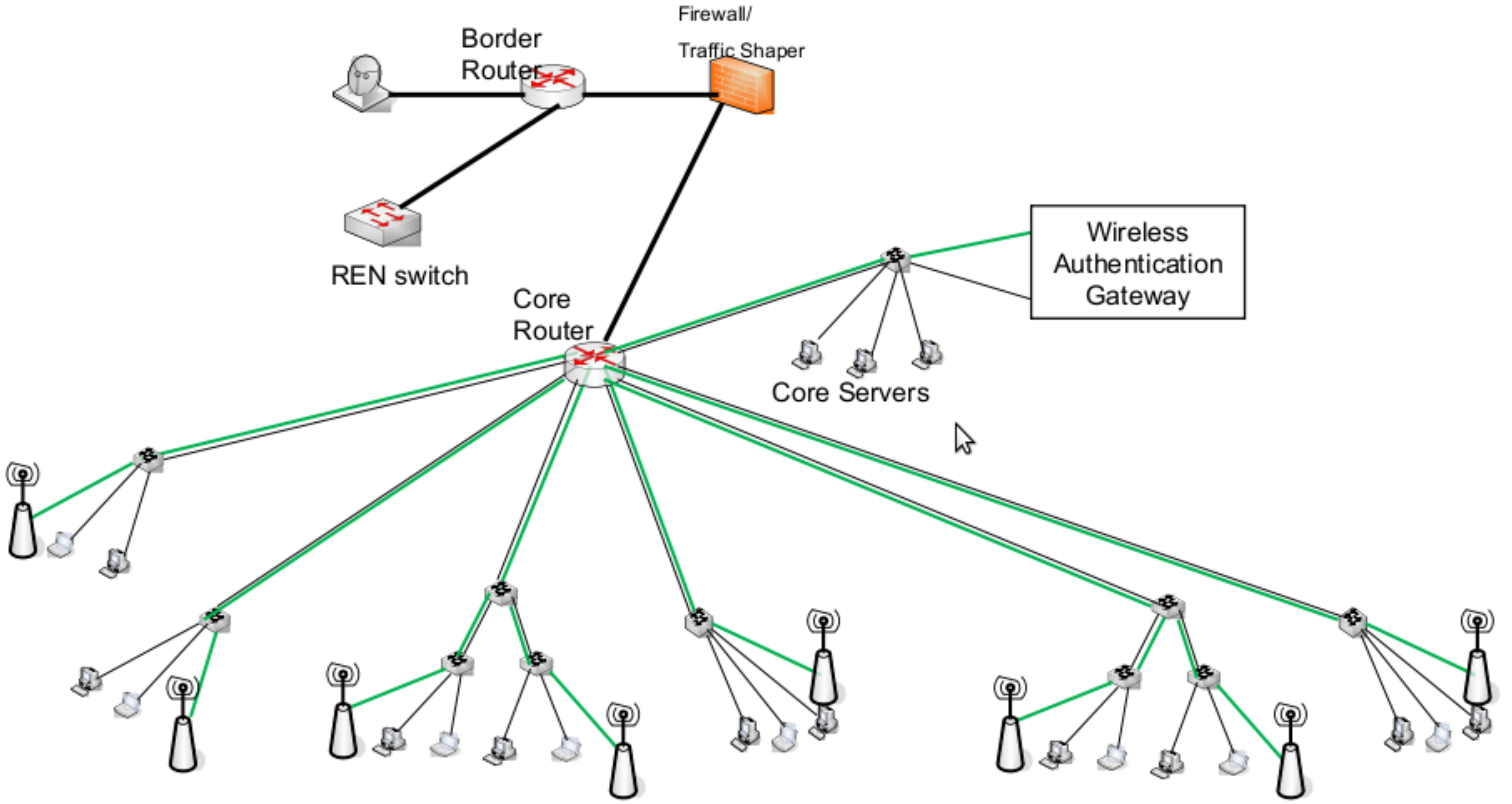
Accounting Server Secret: SHOW

Auth Server IP/Port In the first field, enter the IP address of the RADIUS authentication server. RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service.

In the second field, enter the UDP port of the RADIUS authentication server. The most commonly used port is 1812, but this may vary depending on the RADIUS server you are using.

Auth Server Secret Enter the password. A shared secret is a case-sensitive text string used to validate communication between two RADIUS devices.

Authentication on wireless networks



802.1x Security Problems

- 802.1x or WPA2/EAP is the recommended authentication option, but has security problems
- Outer tunnels rely on TTLS/SSL certificates
  - These are vulnerable to man-in-the-middle attacks – if the client device does not properly check the certificate, then it will give its credentials to ANY AP, e.g. rogue APs
- Inner tunnel authentication is MSCHAP2
  - MSCHAP2 is known to be compromised

802.1x Security Problems

- Client devices that do not check certificates…
  - Will give their credentials to any AP, even a rogue one!
  - Are vulnerable to man-in-the-middle attacks.
- Nothing can protect clients that don’t check…
  - CN (Common Name) or CA (Certificate Authority)
- However we can protect our networks
  - We can enforce the best possible client configuration, for example using the eduroam CAT tool. https://cat.eduroam.org
  - See also security recommendations on https://wiki.geant.org/

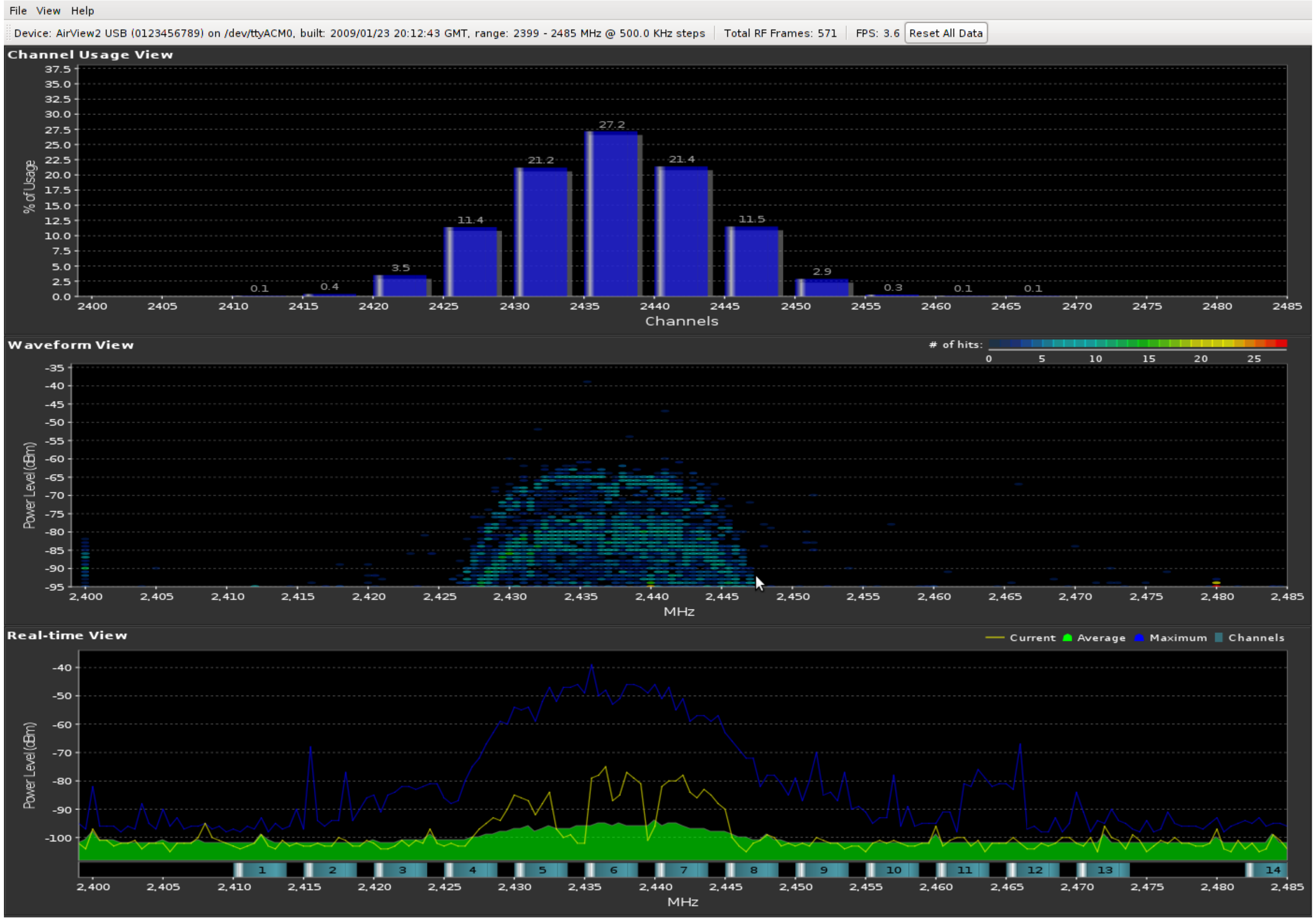
Tools for Wireless Security

- Enterprise Wireless Systems
  - Rogue detection, traffic analysis, logging
- Physical layer:
  - Spectrum analyzers: airview, wispy
  - Wireless Packet sniffers: kismet – Netstumbler (windows)
- General networking tools:
  - etherape, mtr, mrtg, nmap, ntop, rrdtool, wireshark
- Tool collections: backtrack

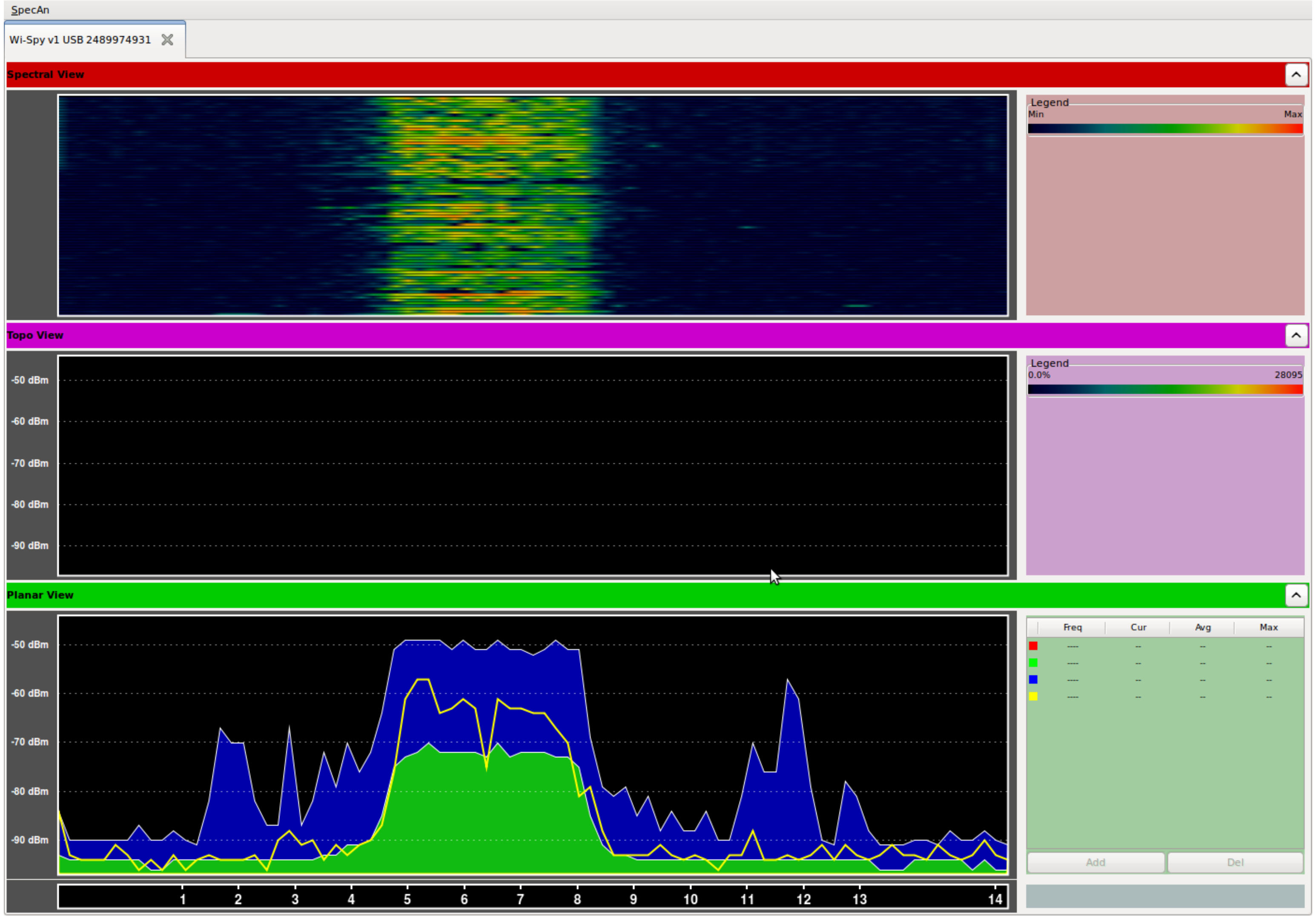
Spectrum Analyzers

- Spectrum Analysers are Layer 1
  - They can represent the physical layer!
  - Can show non-Wi-Fi signals, for example:
  - Microwave ovens, Bluetooth devices, jamming
- Real spectrum analysers are very expensive
- Some equipment includes spectrum analysis
  - For example, Ubiquiti outdoor radios
- USB analysers or RF Explorer can work well
  - e.g. AirView (2.4 GHz), WiSpy (2.4 – 5.8 GHz)

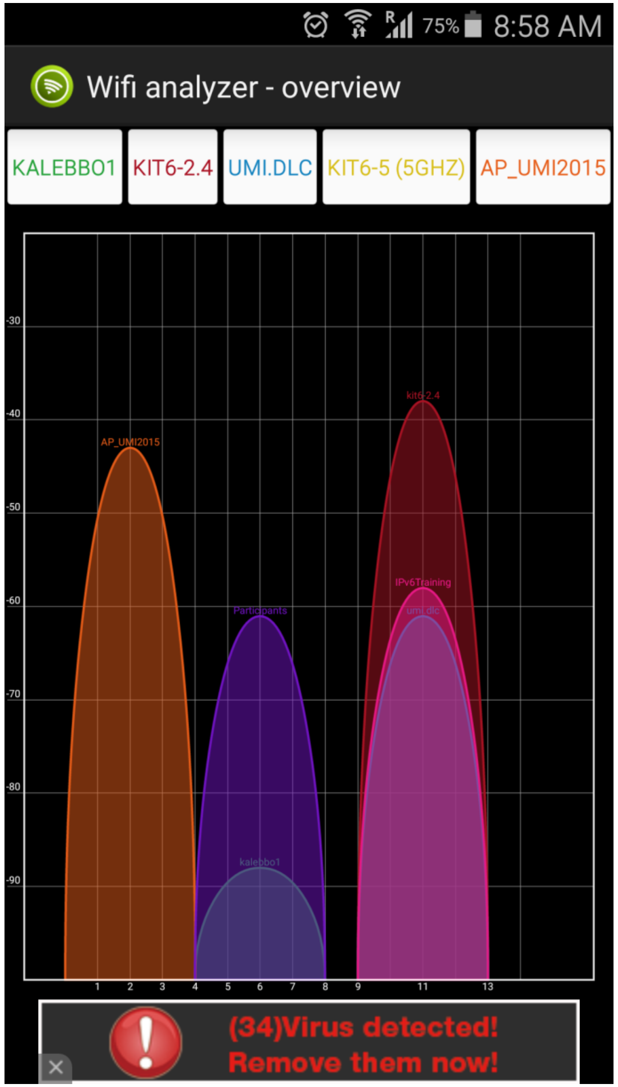
Spectrum analyzers: Airview

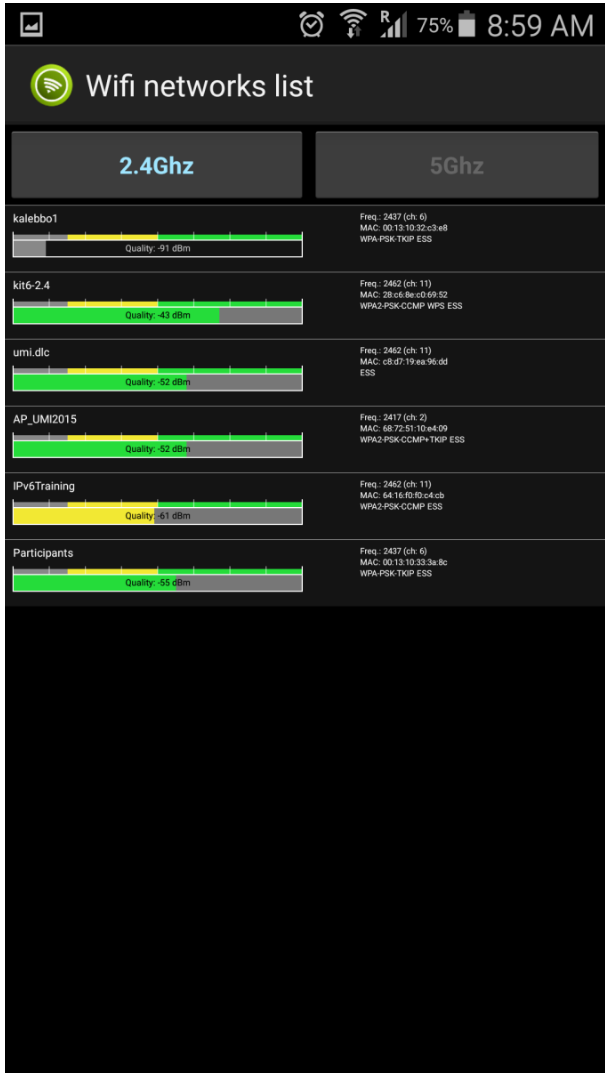


Spectrum analyzers: WiSpy



Android WiFi analyzers





kalebbo1
Quality: -91 dBm
Freq.: 2437 (ch: 6)
MAC: 00:13:10:32:c3:e8
WPA-PSK-TKIP ESS

kit6-2.4
Quality: -43 dBm
Freq.: 2462 (ch: 11)
MAC: 28:c6:8e:c0:69:52
WPA2-PSK-CCMP WPS ESS

umi.dlc
Quality: -52 dBm
Freq.: 2462 (ch: 11)
MAC: c8:d7:19:ea:96:dd
ESS

AP_UMI2015
Quality: -52 dBm
Freq.: 2417 (ch: 2)
MAC: 68:72:51:10:e4:09
WPA2-PSK-CCMP+TKIP ESS

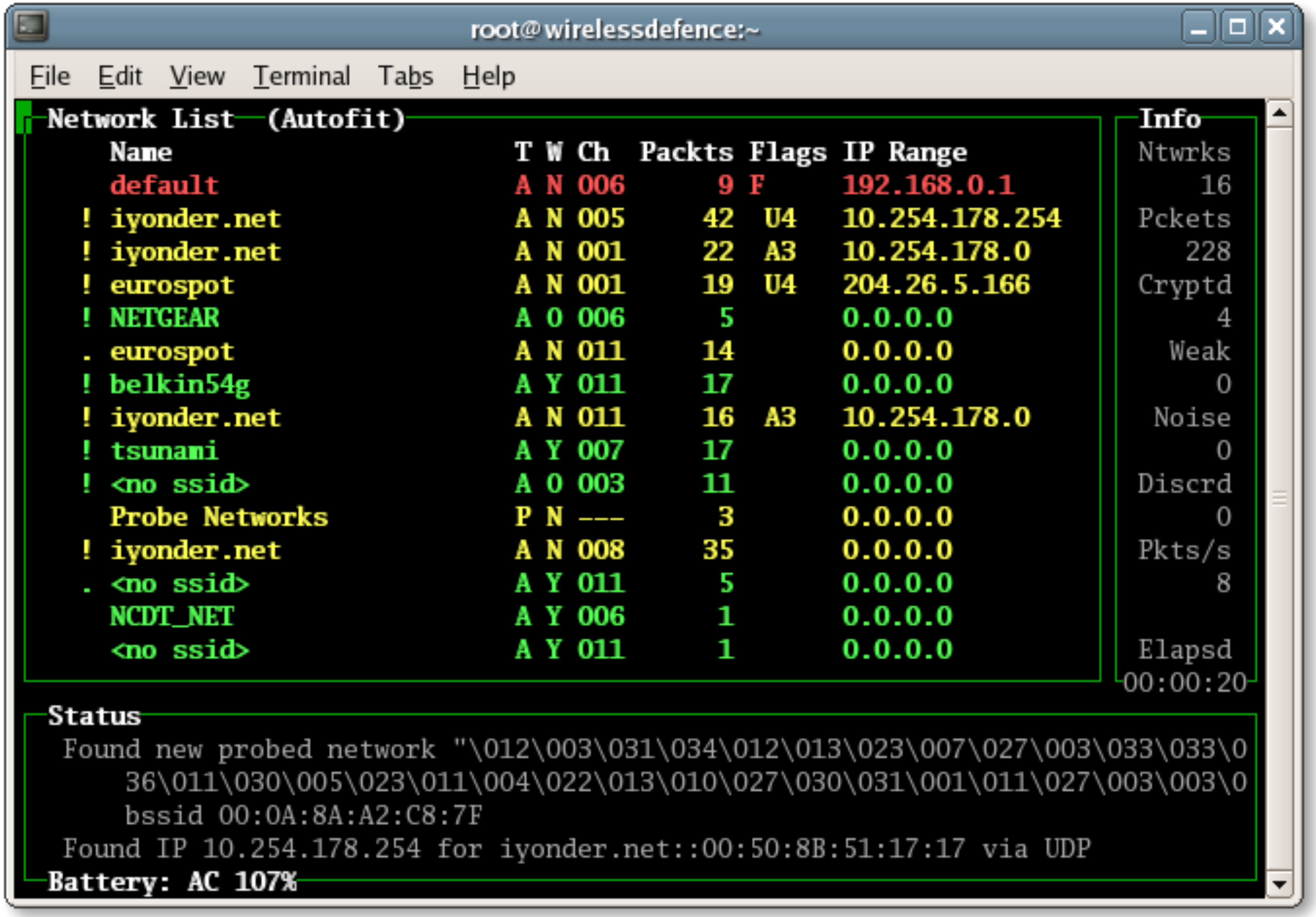
IPv6Training
Quality: -61 dBm
Freq.: 2462 (ch: 11)
MAC: 64:16:f0:f0:c4:cb
WPA2-PSK-CCMP ESS

Participants
Quality: -55 dBm
Freq.: 2437 (ch: 6)
MAC: 00:13:10:33:3a:8c
WPA-PSK-TKIP ESS

Kismet

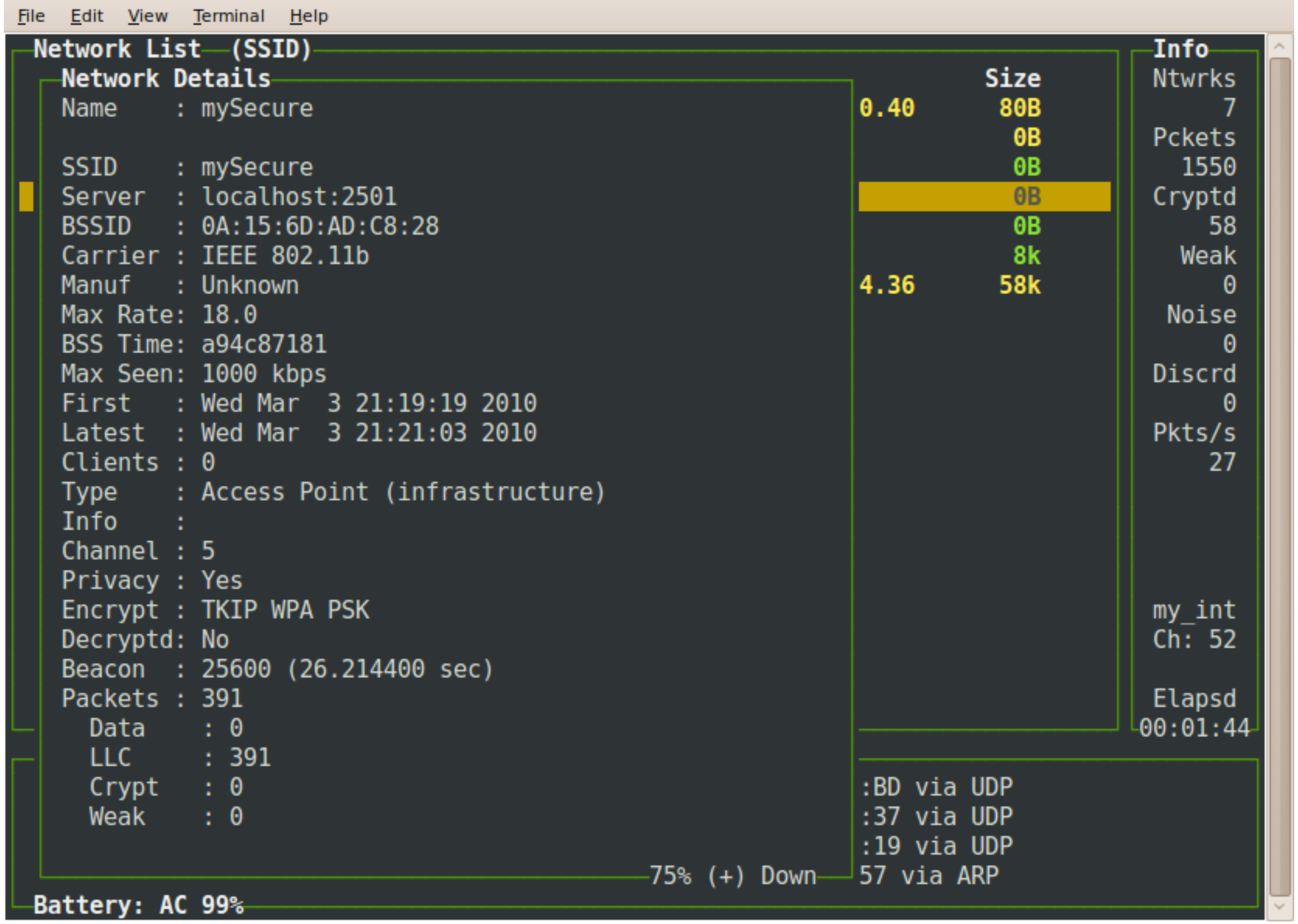
- Wireless network detector, sniffer, and IDS
- Works in raw monitoring (rfmon) mode
- Can sniff 802.11a,b,g,n traffic
- Passively collects packets
- Detects standard named networks
- Detects hidden & non-beaconing networks
- Combine with tools like wireshark, nmap, etc

Kismet



```
Network List—(Autofit)                                         Info
    Name                         T W Ch  Packts Flags IP Range          Ntwrks
    default                      A N 006      9 F     192.168.0.1            16
  ! iyonder.net                  A N 005     42  U4   10.254.178.254    Pckets
  ! iyonder.net                  A N 001     22  A3   10.254.178.0         228
  ! eurospot                     A N 001     19  U4   204.26.5.166      Cryptd
  ! NETGEAR                      A O 006      5       0.0.0.0                4
  . eurospot                     A N 011     14       0.0.0.0             Weak
  ! belkin54g                    A Y 011     17       0.0.0.0                0
  ! iyonder.net                  A N 011     16  A3   10.254.178.0       Noise
  ! tsunami                      A Y 007     17       0.0.0.0                0
  ! <no ssid>                    A O 003     11       0.0.0.0           Discrd
    Probe Networks               P N ---      3       0.0.0.0                0
  ! iyonder.net                  A N 008     35       0.0.0.0           Pkts/s
  . <no ssid>                    A Y 011      5       0.0.0.0                8
    NCDT_NET                     A Y 006      1       0.0.0.0
    <no ssid>                    A Y 011      1       0.0.0.0           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%
```

Kismet

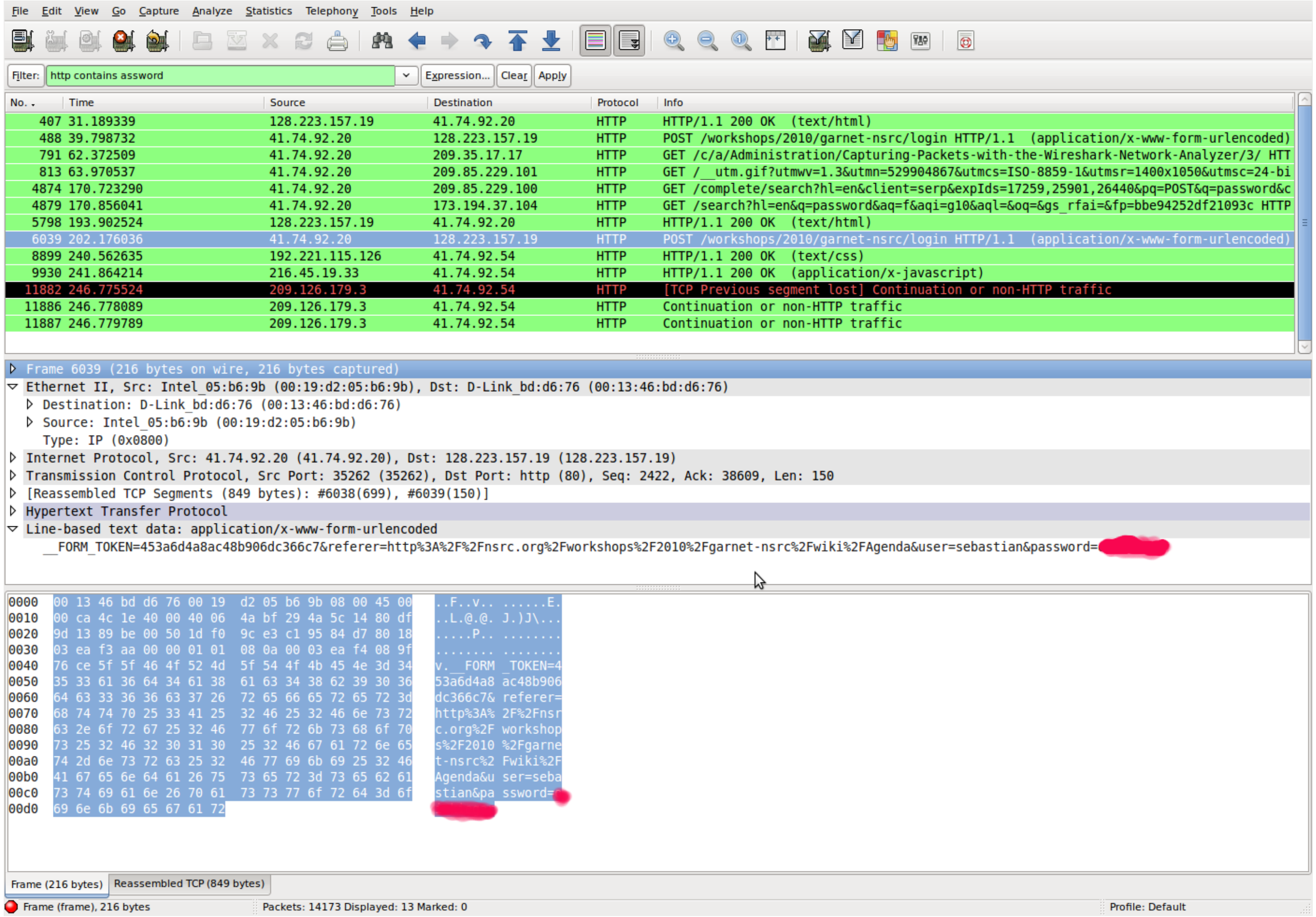


```
Network List─(SSID)─────────────────────────────────────────────────────  Info
  Network Details───────────────────────────────────    Size   Ntwrks
  Name     : mySecure                         0.40        80B        7
                                                           0B   Pckets
  SSID     : mySecure                                      0B     1550
  Server   : localhost:2501                                0B   Cryptd
  BSSID    : 0A:15:6D:AD:C8:28                             0B       58
  Carrier  : IEEE 802.11b                                  8k     Weak
  Manuf    : Unknown                          4.36        58k        0
  Max Rate: 18.0                                                 Noise
  BSS Time: a94c87181                                                0
  Max Seen: 1000 kbps                                           Discrd
  First    : Wed Mar  3 21:19:19 2010                                0
  Latest   : Wed Mar  3 21:21:03 2010                           Pkts/s
  Clients  : 0                                                      27
  Type     : Access Point (infrastructure)
  Info     :
  Channel  : 5
  Privacy  : Yes
  Encrypt  : TKIP WPA PSK                                       my_int
  Decryptd: No                                                  Ch: 52
  Beacon   : 25600 (26.214400 sec)
  Packets  : 391                                                Elapsd
    Data     : 0                                              00:01:44
    LLC      : 391
    Crypt    : 0                      :BD via UDP
    Weak     : 0                      :37 via UDP
                                      :19 via UDP
  ─────────────────────75% (+) Down  57 via ARP
Battery: AC 99%
```

Wireshark

- A free and open-source packet analyzer.
- Used for network troubleshooting, analysis, software and communications protocol development, and education.
- Filter for fast identification of protocols, IP numbers, or keywords

Wireshark


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply
Frame (216 bytes)
Reassembled TCP (849 bytes)

Filter: http contains assword

```
No. .  Time          Source            Destination       Protocol  Info
   407 31.189339     128.223.157.19    41.74.92.20       HTTP      HTTP/1.1 200 OK  (text/html)
   488 39.798732     41.74.92.20       128.223.157.19    HTTP      POST /workshops/2010/garnet-nsrc/login HTTP/1.1  (application/x-www-form-urlencoded)
   791 62.372509     41.74.92.20       209.35.17.17      HTTP      GET /c/a/Administration/Capturing-Packets-with-the-Wireshark-Network-Analyzer/3/ HTT
   813 63.970537     41.74.92.20       209.85.229.101    HTTP      GET /__utm.gif?utmwv=1.3&utmn=529904867&utmcs=ISO-8859-1&utmsr=1400x1050&utmsc=24-bi
  4874 170.723290    41.74.92.20       209.85.229.100    HTTP      GET /complete/search?hl=en&client=serp&expIds=17259,25901,26440&pq=POST&q=password&c
  4879 170.856041    41.74.92.20       173.194.37.104    HTTP      GET /search?hl=en&q=password&aq=f&aqi=g10&aql=&oq=&gs_rfai=&fp=bbe94252df21093c HTTP
  5798 193.902524    128.223.157.19    41.74.92.20       HTTP      HTTP/1.1 200 OK  (text/html)
  6039 202.176036    41.74.92.20       128.223.157.19    HTTP      POST /workshops/2010/garnet-nsrc/login HTTP/1.1  (application/x-www-form-urlencoded)
  8899 240.562635    192.221.115.126   41.74.92.54       HTTP      HTTP/1.1 200 OK  (text/css)
  9930 241.864214    216.45.19.33      41.74.92.54       HTTP      HTTP/1.1 200 OK  (application/x-javascript)
 11882 246.775524    209.126.179.3     41.74.92.54       HTTP      [TCP Previous segment lost] Continuation or non-HTTP traffic
 11886 246.778089    209.126.179.3     41.74.92.54       HTTP      Continuation or non-HTTP traffic
 11887 246.779789    209.126.179.3     41.74.92.54       HTTP      Continuation or non-HTTP traffic
```

```
▷ Frame 6039 (216 bytes on wire, 216 bytes captured)
▽ Ethernet II, Src: Intel_05:b6:9b (00:19:d2:05:b6:9b), Dst: D-Link_bd:d6:76 (00:13:46:bd:d6:76)
  ▷ Destination: D-Link_bd:d6:76 (00:13:46:bd:d6:76)
  ▷ Source: Intel_05:b6:9b (00:19:d2:05:b6:9b)
    Type: IP (0x0800)
▷ Internet Protocol, Src: 41.74.92.20 (41.74.92.20), Dst: 128.223.157.19 (128.223.157.19)
▷ Transmission Control Protocol, Src Port: 35262 (35262), Dst Port: http (80), Seq: 2422, Ack: 38609, Len: 150
▷ [Reassembled TCP Segments (849 bytes): #6038(699), #6039(150)]
▷ Hypertext Transfer Protocol
▽ Line-based text data: application/x-www-form-urlencoded
    __FORM_TOKEN=453a6d4a8ac48b906dc366c7&referer=http%3A%2F%2Fnsrc.org%2Fworkshops%2F2010%2Fgarnet-nsrc%2Fwiki%2FAgenda&user=sebastian&password=[redacted]
```

```
0000  00 13 46 bd d6 76 00 19  d2 05 b6 9b 08 00 45 00   ..F..v.. ......E.
0010  00 ca 4c 1e 40 00 40 06  4a bf 29 4a 5c 14 80 df   ..L.@.@. J.)J\...
0020  9d 13 89 be 00 50 1d f0  9c e3 c1 95 84 d7 80 18   .....P.. ........
0030  03 ea f3 aa 00 00 01 01  08 0a 00 03 ea f4 08 9f   ........ ........
0040  76 ce 5f 5f 46 4f 52 4d  5f 54 4f 4b 45 4e 3d 34   v.__FORM _TOKEN=4
0050  35 33 61 36 64 34 61 38  61 63 34 38 62 39 30 36   53a6d4a8 ac48b906
0060  64 63 33 36 36 63 37 26  72 65 66 65 72 65 72 3d   dc366c7& referer=
0070  68 74 74 70 25 33 41 25  32 46 25 32 46 6e 73 72   http%3A% 2F%2Fnsr
0080  63 2e 6f 72 67 25 32 46  77 6f 72 6b 73 68 6f 70   c.org%2F workshop
0090  73 25 32 46 32 30 31 30  25 32 46 67 61 72 6e 65   s%2F2010 %2Fgarne
00a0  74 2d 6e 73 72 63 25 32  46 77 69 6b 69 25 32 46   t-nsrc%2 Fwiki%2F
00b0  41 67 65 6e 64 61 26 75  73 65 72 3d 73 65 62 61   Agenda&u ser=seba
00c0  73 74 69 61 6e 26 70 61  73 73 77 6f 72 64 3d 6f   stian&pa ssword=[redacted]
00d0  69 6e 6b 69 65 67 61 72                            [redacted]
```

Frame (frame), 216 bytes   Packets: 14173 Displayed: 13 Marked: 0   Profile: Default