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”, dont 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 dont 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 databetween 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

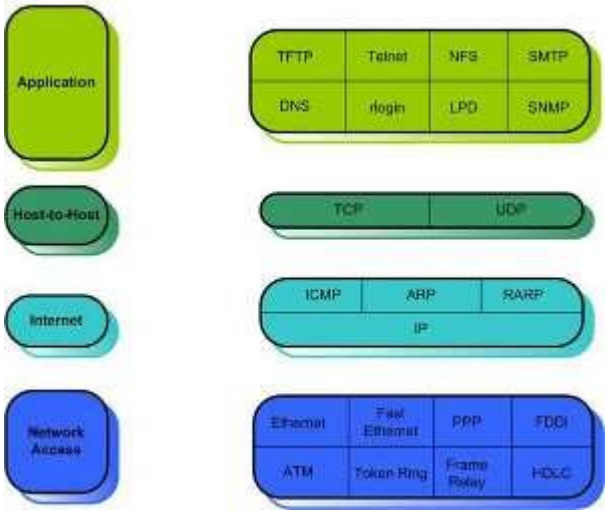
General Security / Methods for Wireless

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?

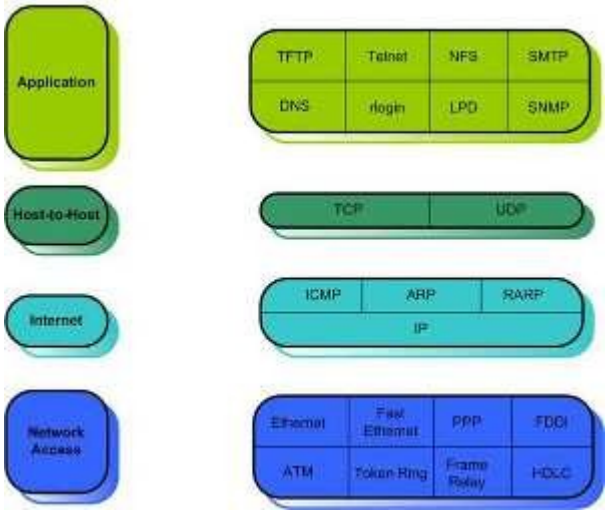
Is your wifi secure?

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)

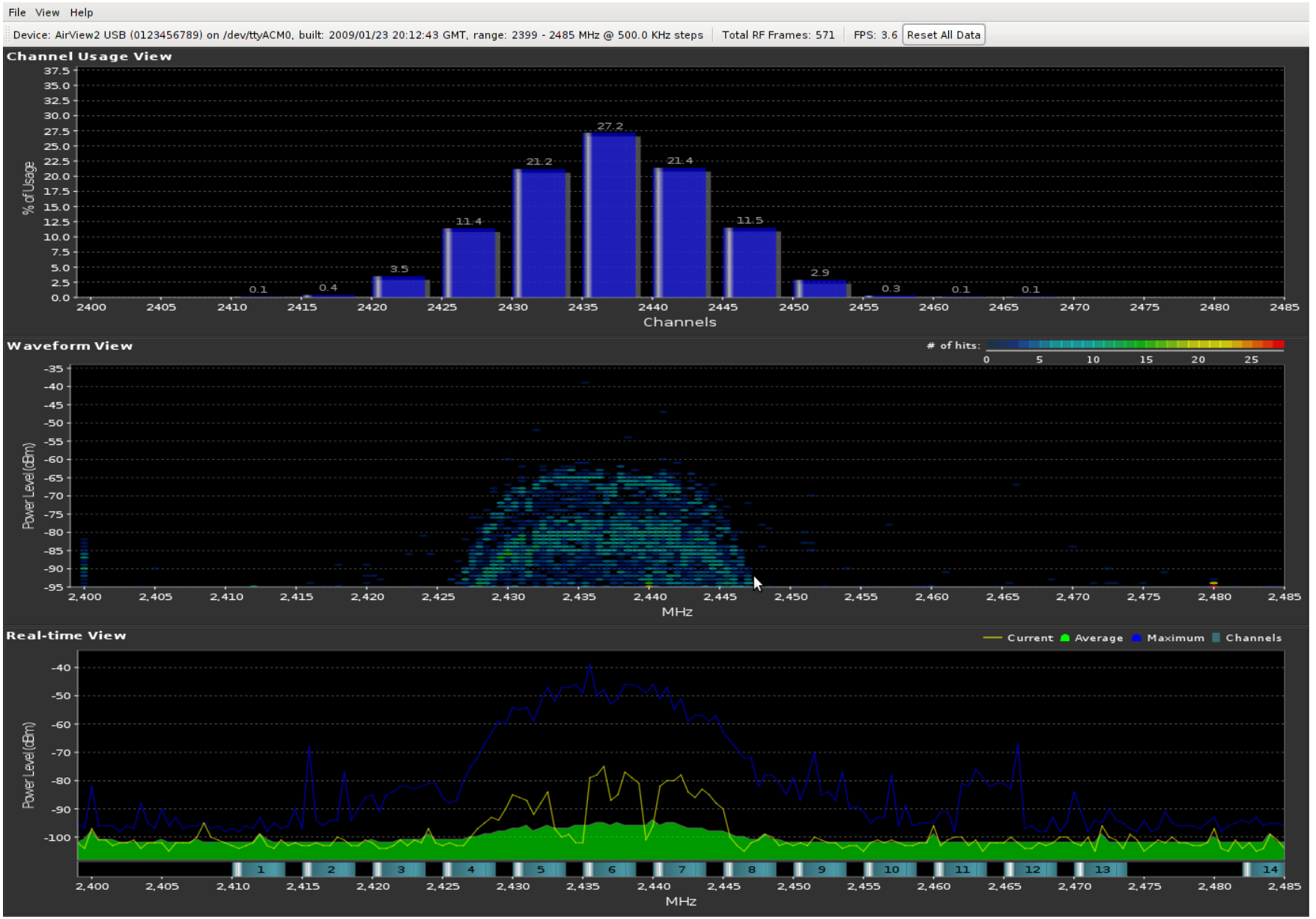
Network layer:

- 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**

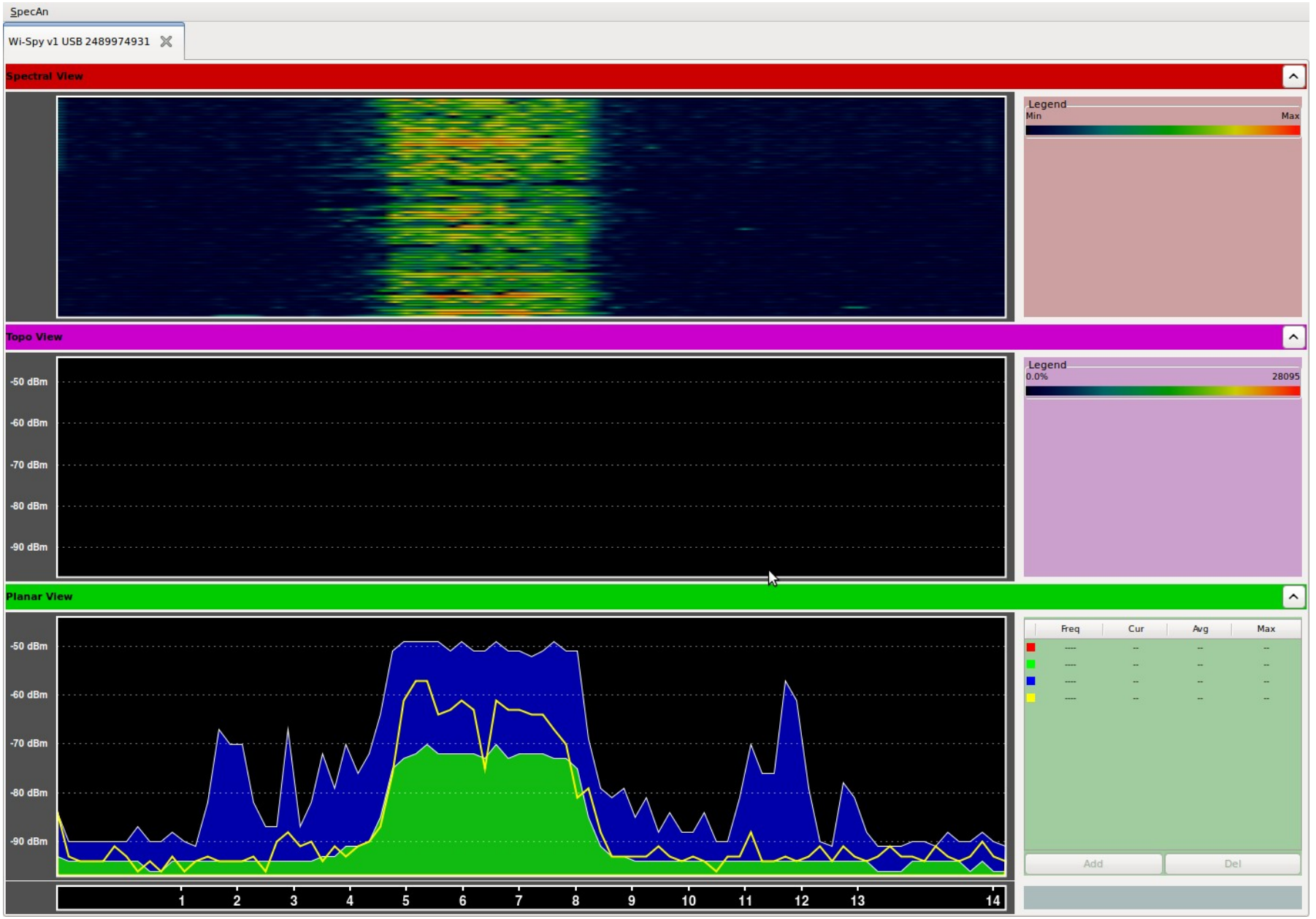
Spectrum Analyzers

- 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

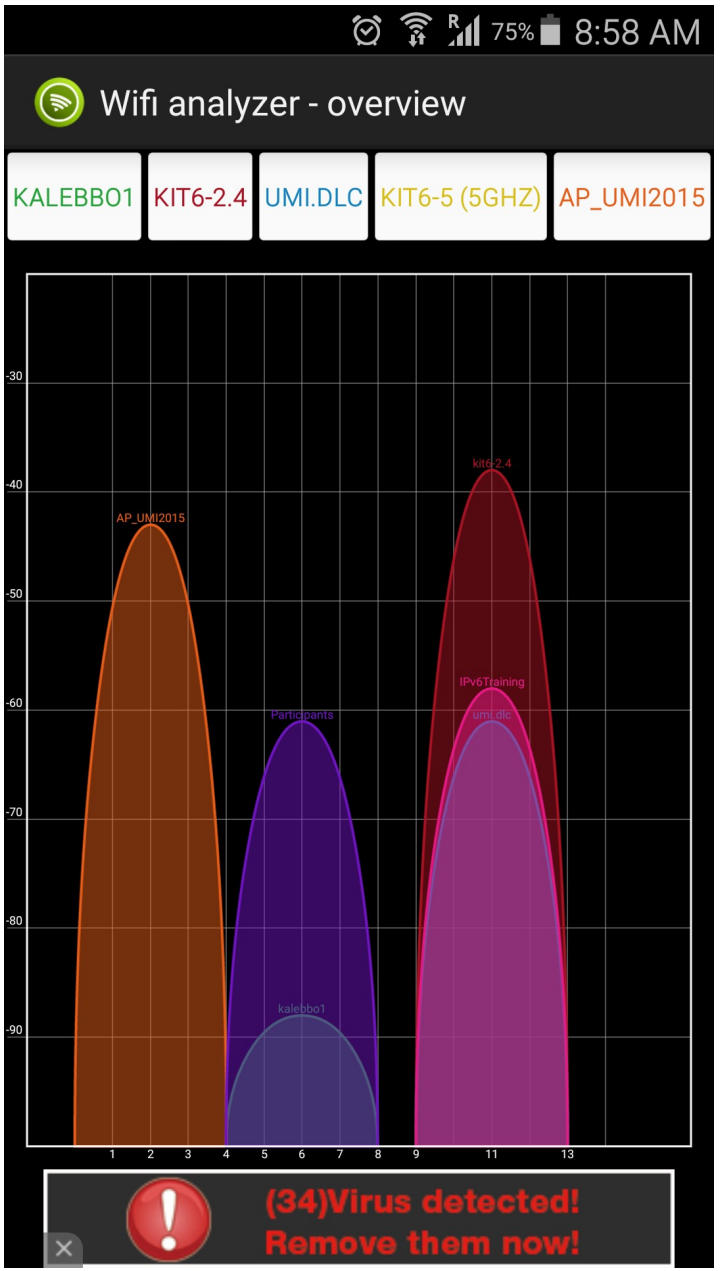
Spectrum Analyzers: Airview

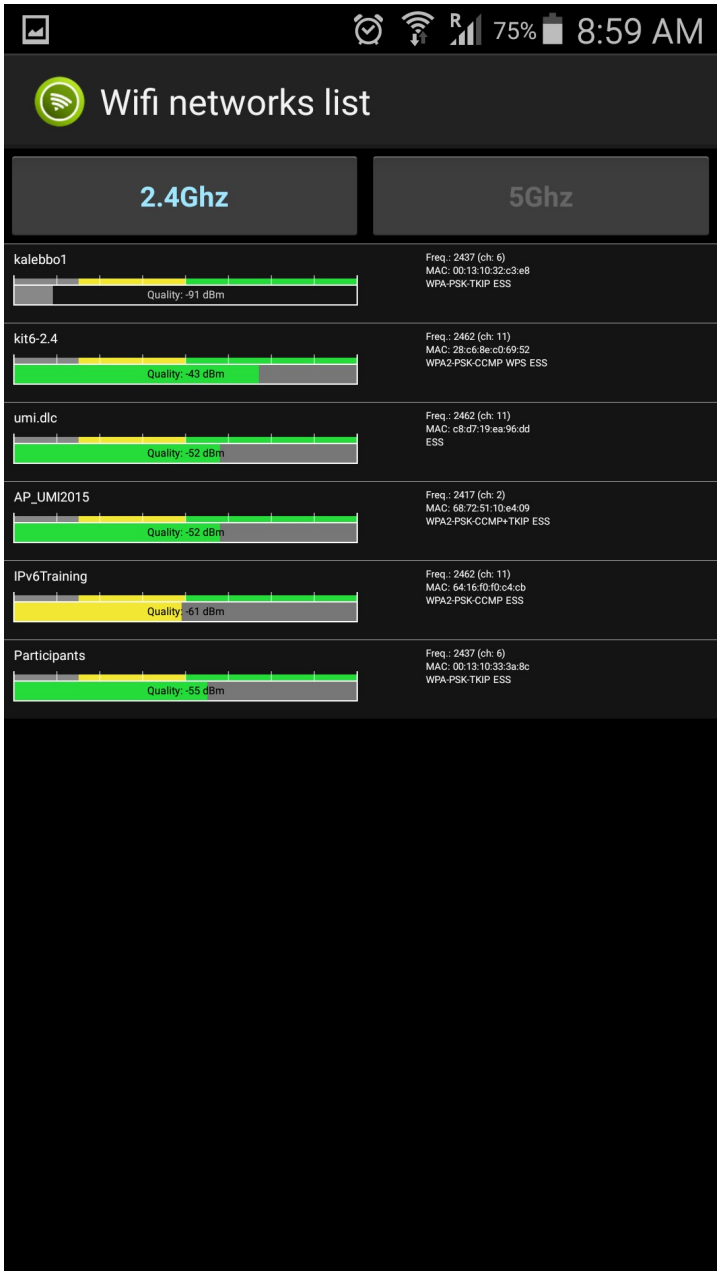


Spectrum Analyzers: WiSpy



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 /ect/kismet.conf`

  ncsource=interface:options

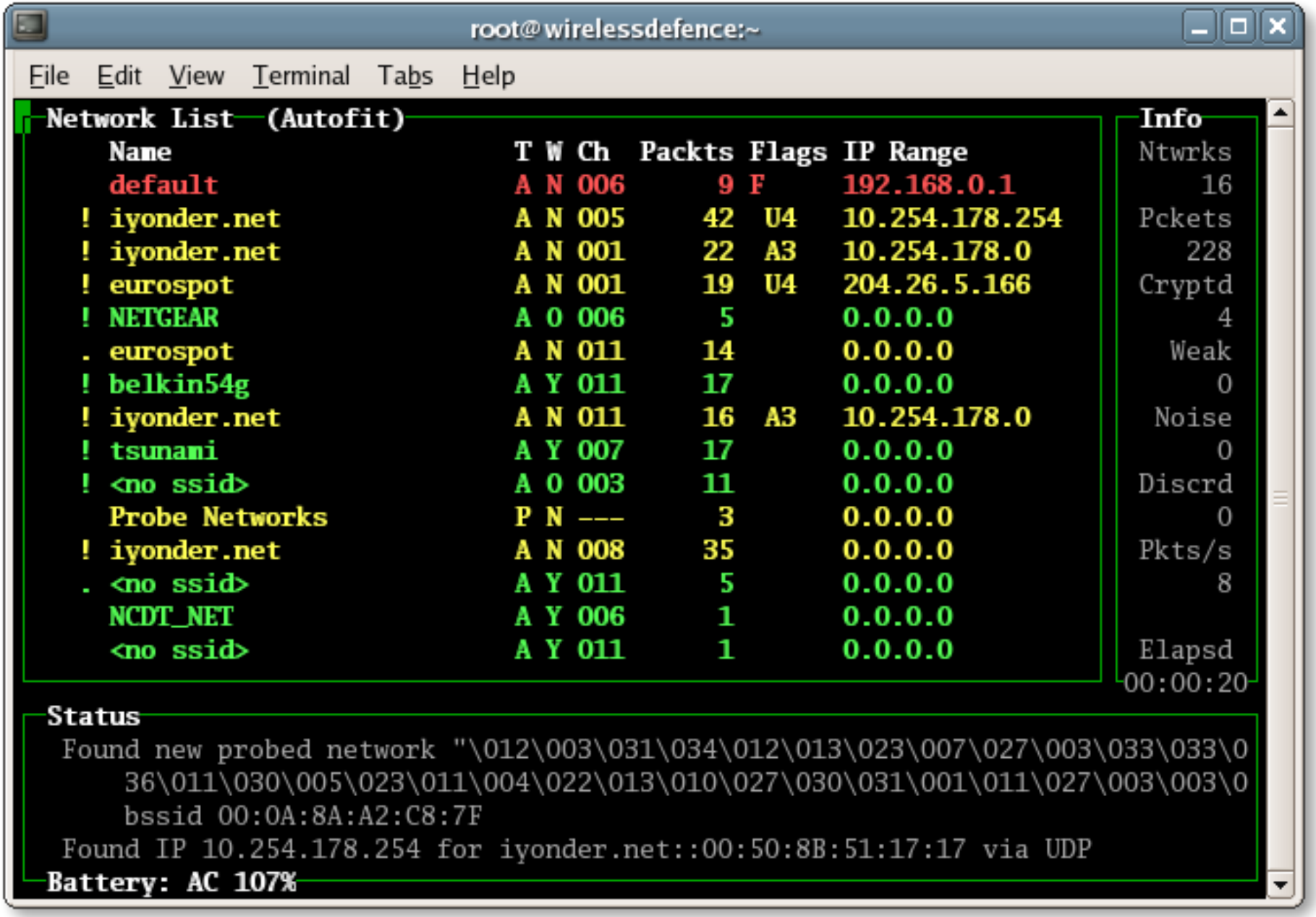
  e.g.

  ncsource=wlo1:type=atheros

- start kismet

  `$ kismet`

Start screen



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

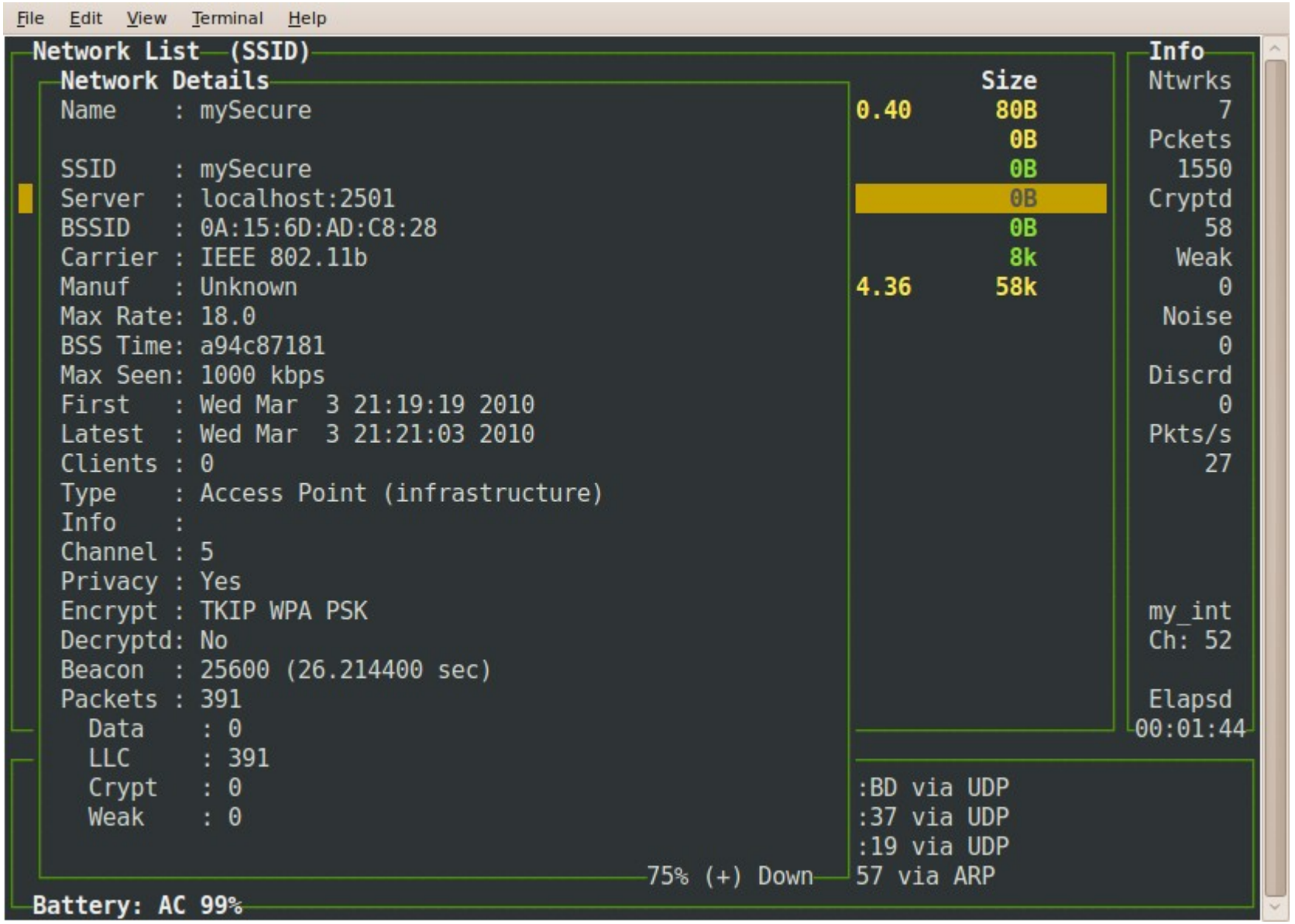
  r Packet rate graph

  a Statistics

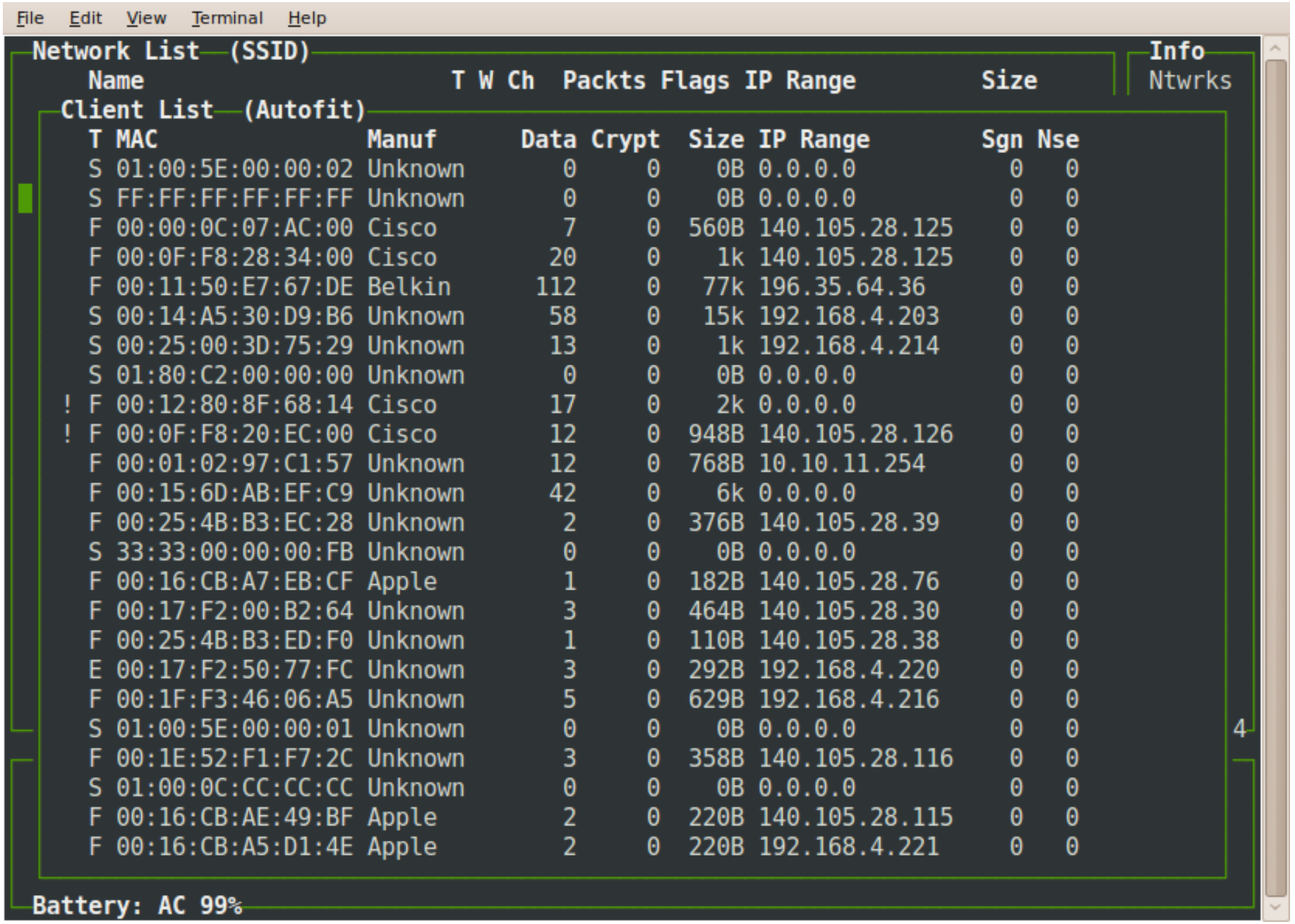
  p Dump packet type

  Q Quit

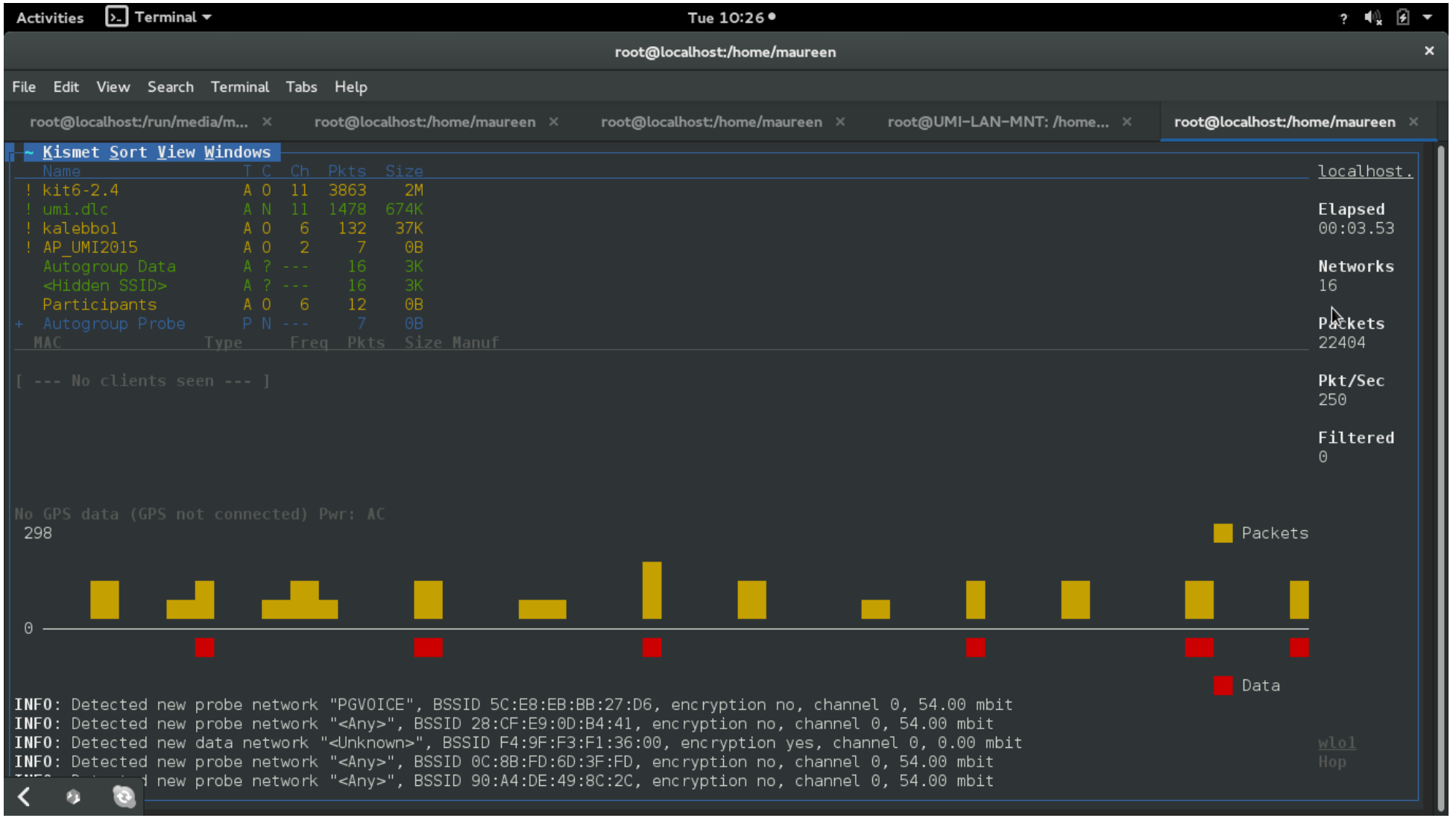
kismet - Network info



Client info


File Edit View Terminal Help
Network List (SSID)
Name T W Ch 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
4
Battery: AC 99%

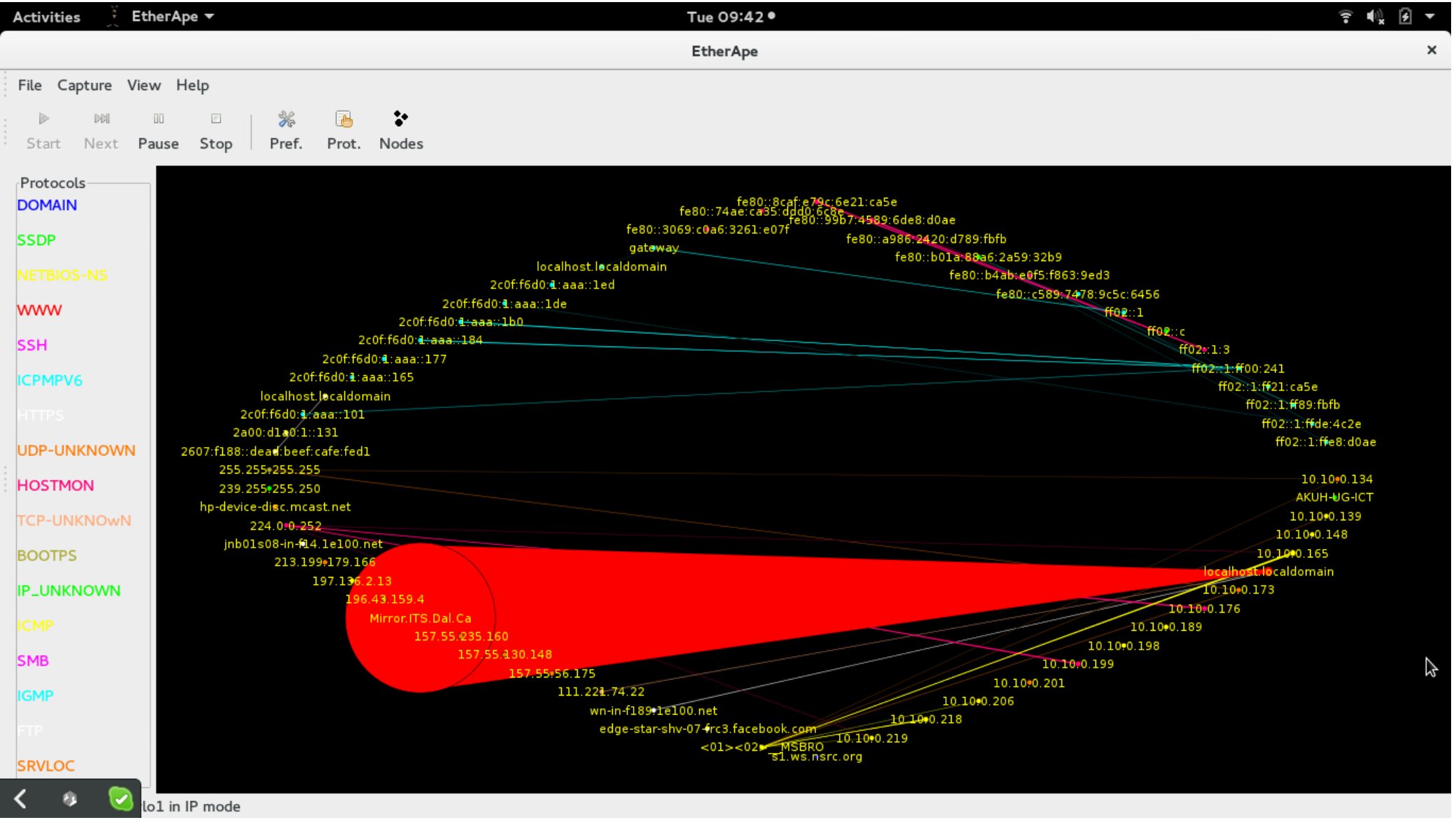
Kismet scan UMI



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.

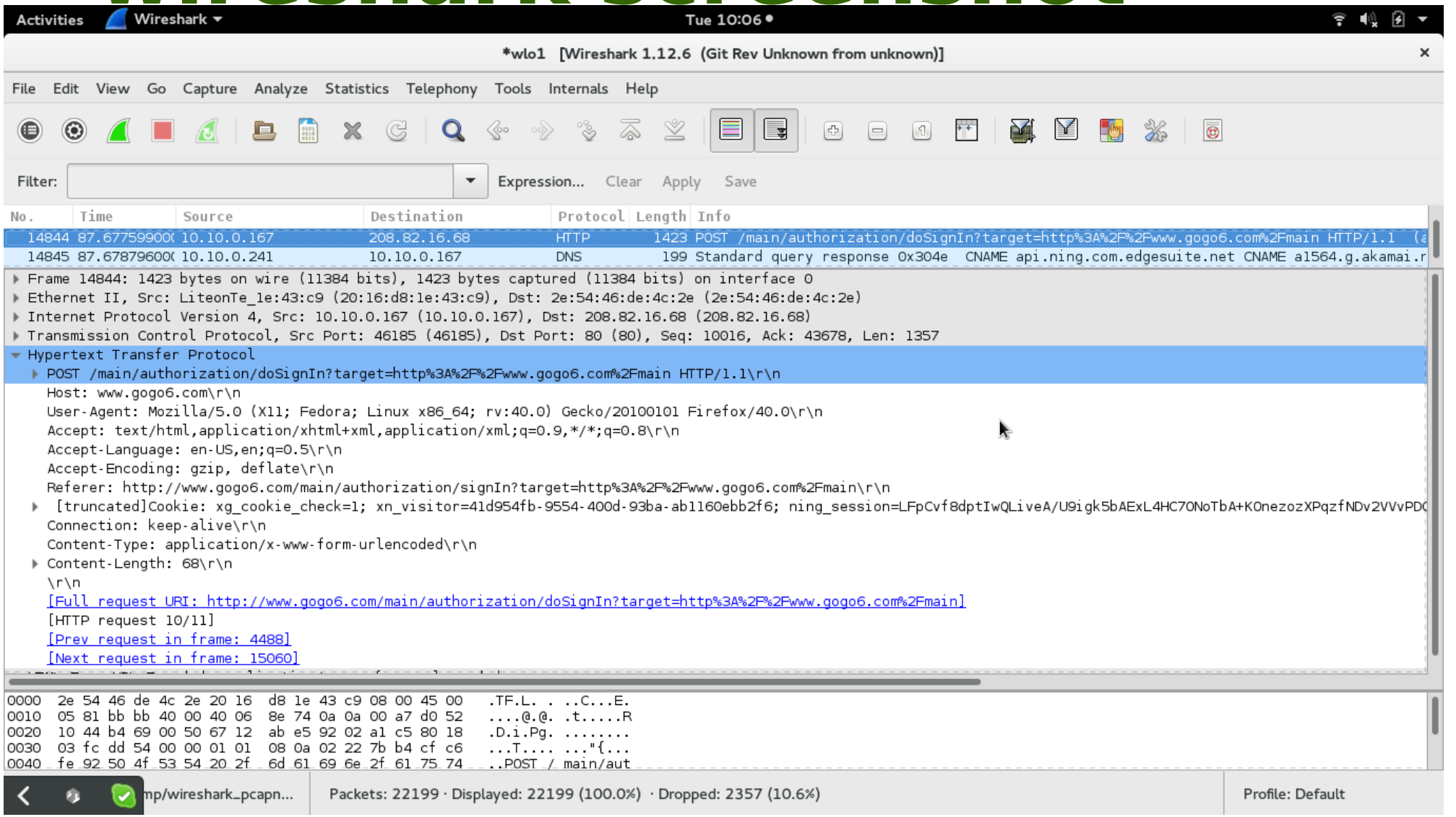
etherape screenshot



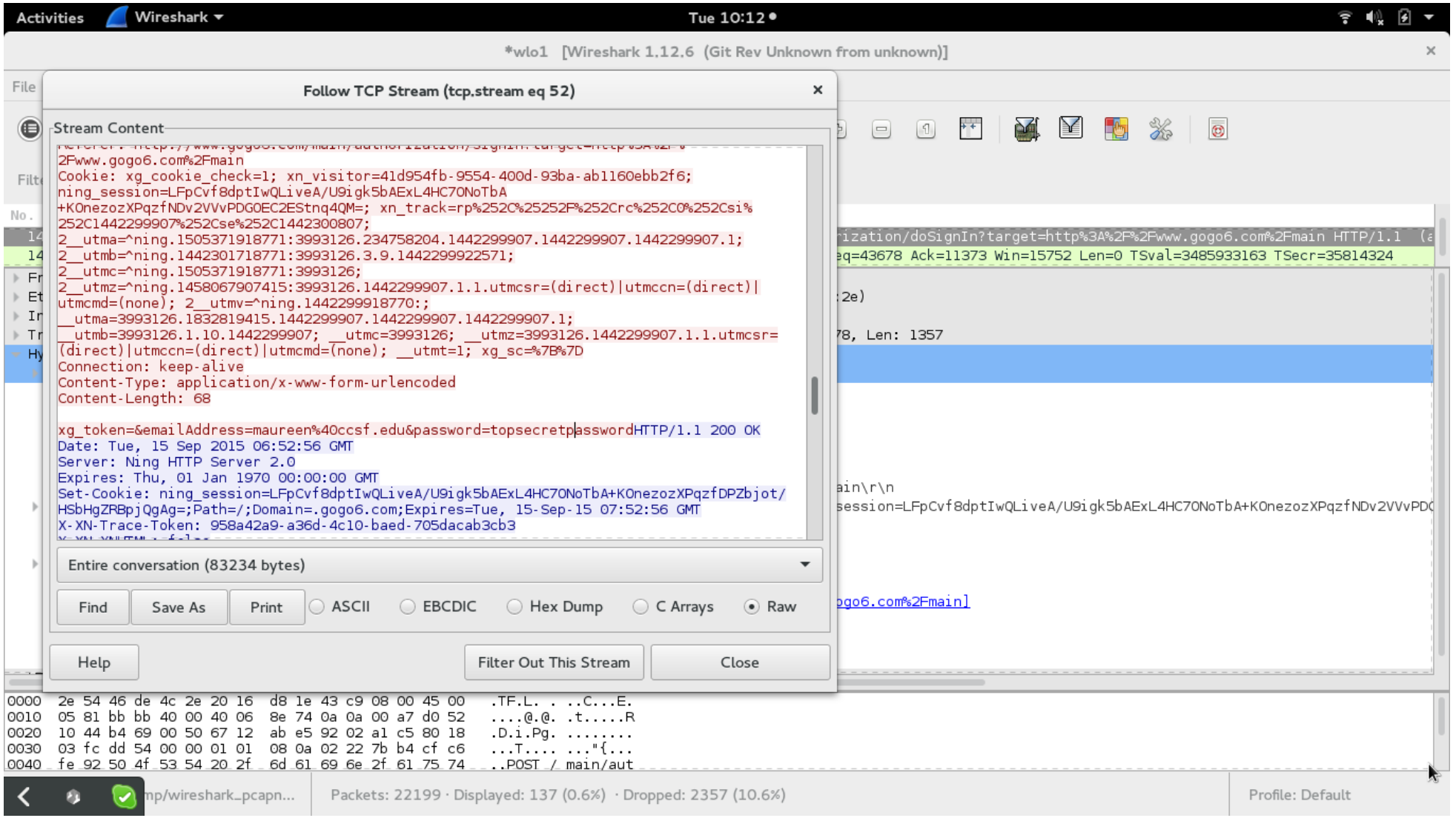
What is wireshark?

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

wireshark screenshot



Wireshark:is that my password?



That was it ...

Thank you!

http://nsrc.org

NSRC