802.11 Protocol Chaos

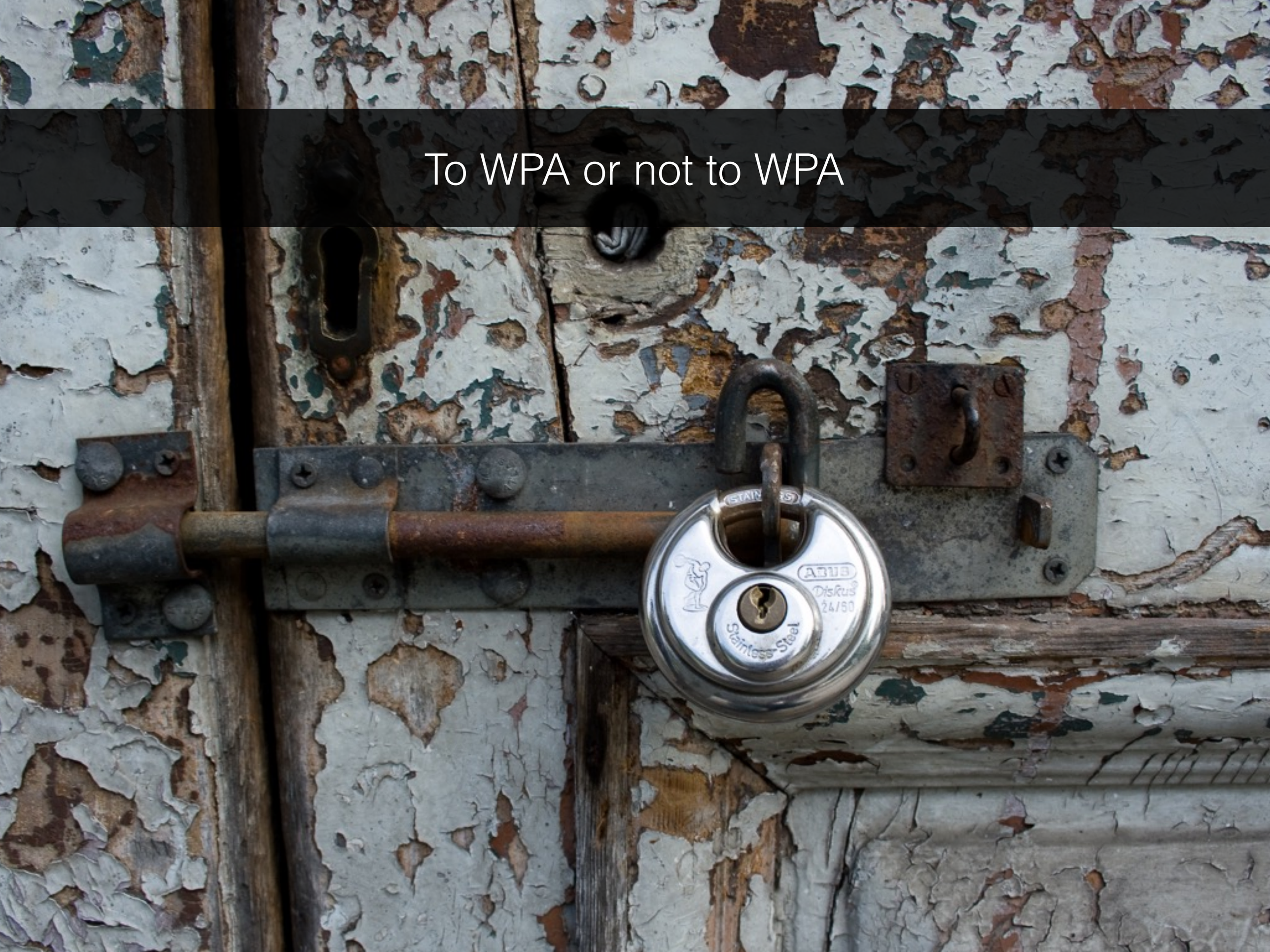
Andrés Blanco

6e726d@gmail.com

@6e726d

INFILTRATE SECURITY CONFERENCE

To WPA or not to WPA



IEEE 802.11 frame types and subtypes

Management

- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Request
- Probe Response
- Beacon
- ATIM
- Disassociation
- Authentication
- Deauthentication
- Action

Control

- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

Data

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll
- QoS data
- QoS data+CF-ACK
- QoS data+CF-Poll
- QoS data+CF-ACK+CF-Poll
- QoS Null
- QoS+CF-Poll
- QoS+CF-ACK

Management frames are used for various link-layer maintenance functions

Management

- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Request
- Probe Response
- Beacon
- ATIM
- Disassociation
- Authentication
- Deauthentication
- Action

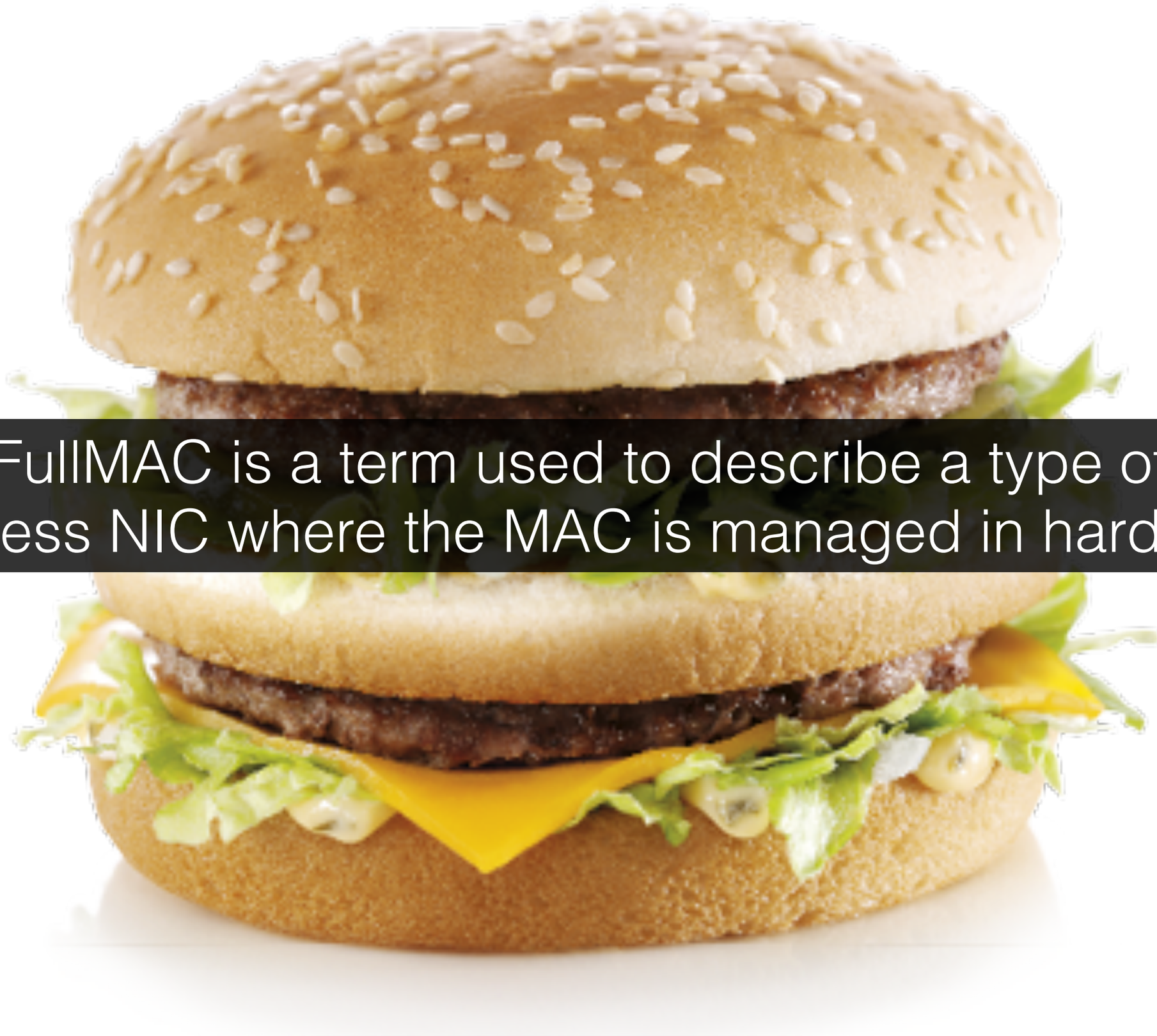
Control

- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK
- CF-End
- CF-End+CF-ACK

Data

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll
- QoS data
- QoS data+CF-ACK
- QoS data+CF-Poll
- QoS data+CF-ACK+CF-Poll
- QoS Null
- QoS+CF-Poll
- QoS+CF-ACK

SoftMAC is a term used to describe a type of Wireless NIC where the MAC is expected to be managed in software



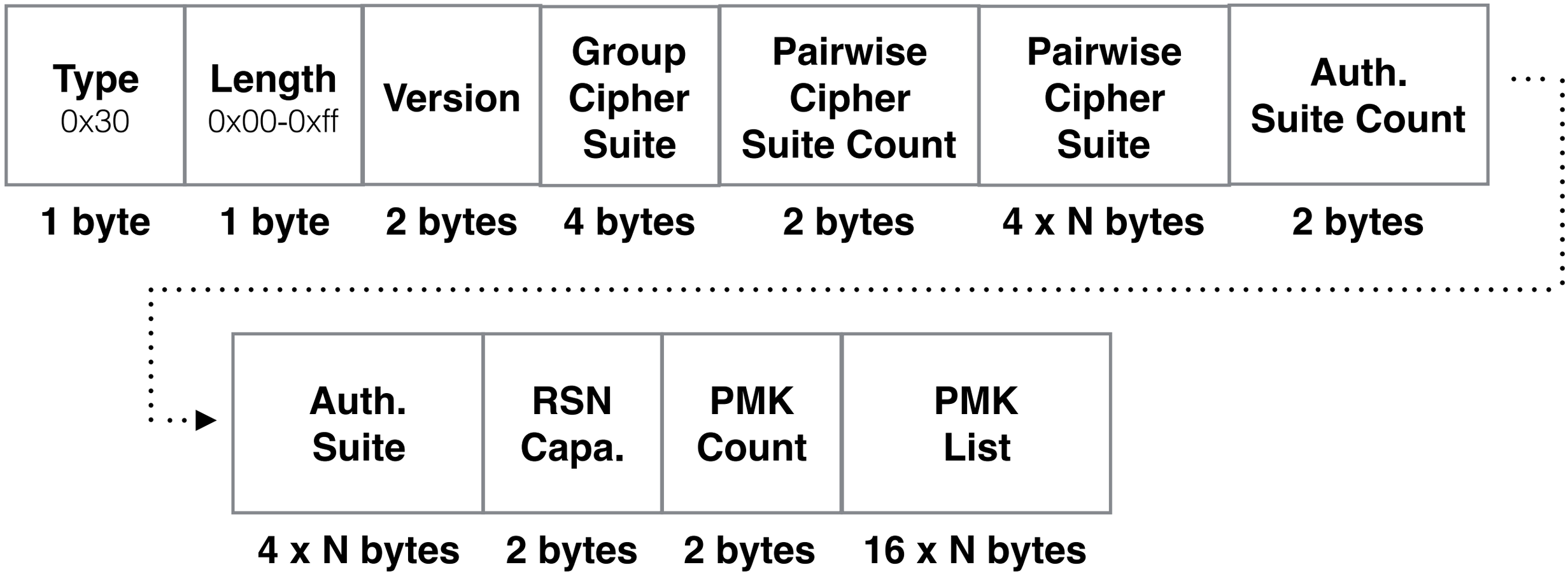
FullMAC is a term used to describe a type of Wireless NIC where the MAC is managed in hardware

Type	Length	Value
1 byte	**1 byte**	**1-255 byte**

Management frames use information elements
structures to communicate information

Type 0x00	**Length** 0x00-0x20	**Value**
1 byte	**1 byte**	**0-32 byte/s**

SSID information element



RSN information element

Wireshark ·

```
▸ Frame 1165: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface 0
▸ Radiotap Header v0, Length 36
▸ 802.11 radio information
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
    Source address: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
    BSS Id: fa:fa:fa:fa:fa:fa (fa:fa:fa:fa:fa:fa)
    .... .... .... 0000 = Fragment number: 0
    0111 0011 1100 .... = Sequence number: 1852
  ▸ Frame check sequence: 0xc201c58e [correct]
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (43 bytes)
    ▸ Tag: SSID parameter set: fafafa
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 6
    ▾ Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 20
        RSN Version: 1
      ▸ Group Cipher Suite: 00-0f-ac AES (CCM)
        Pairwise Cipher Suite Count: 1
      ▸ Pairwise Cipher Suite List 00-0f-ac AES (CCM)
      ▸ Auth Key Management (AKM) Suite Count: 65535
      ▸ Auth Key Management (AKM) List 00-0f-ac PSK
      ▸ RSN Capabilities: 0x0000
```

CVE-2012-2619

No.: 1165 · Time: 16.092353220 · Source: fa:fa:fa:fa:fa:fa · De...acon frame, SN=1852, FN=0, Flags=.....C, BI=100, SSID=fafafa

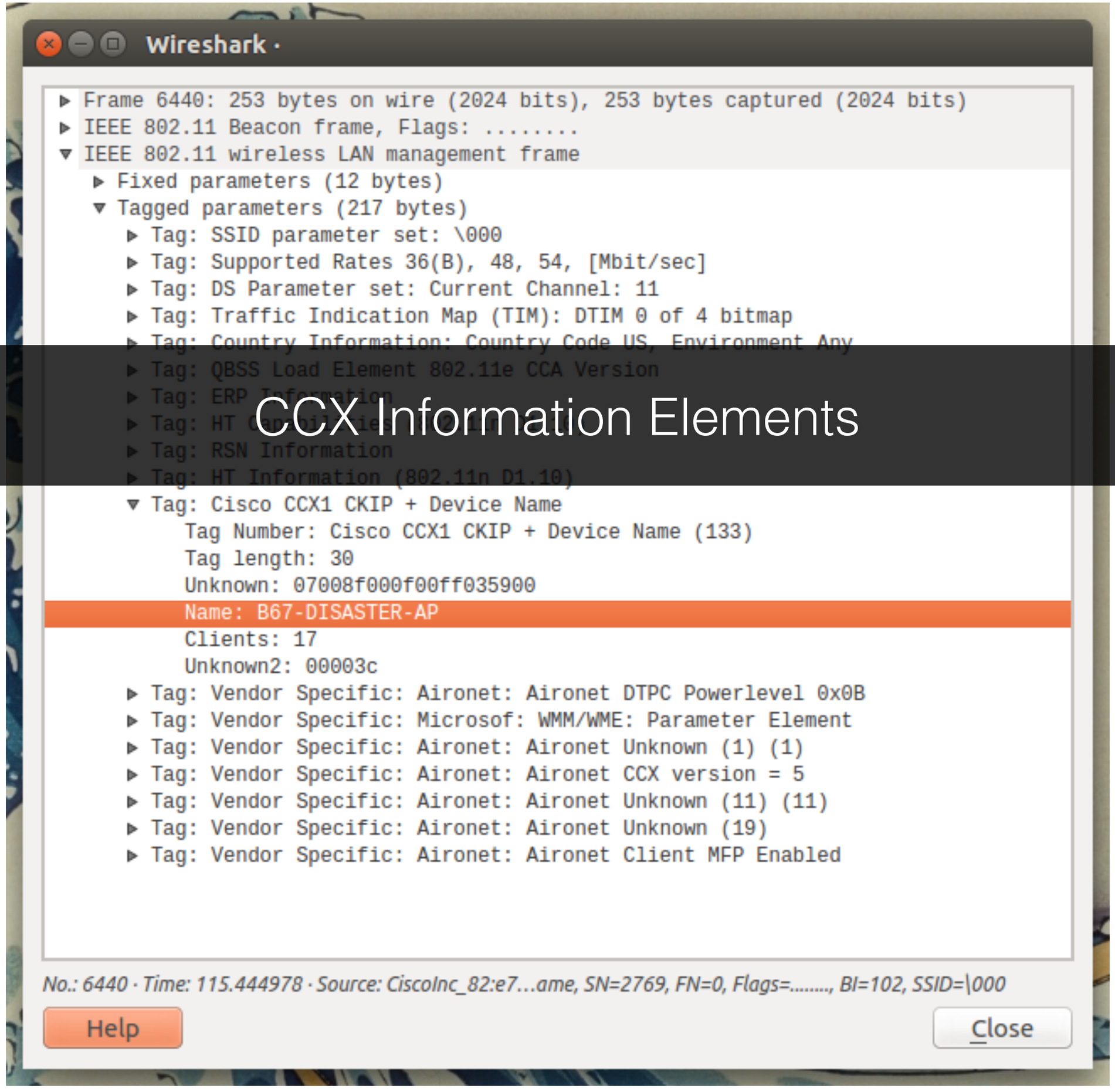
Close Help

Free information

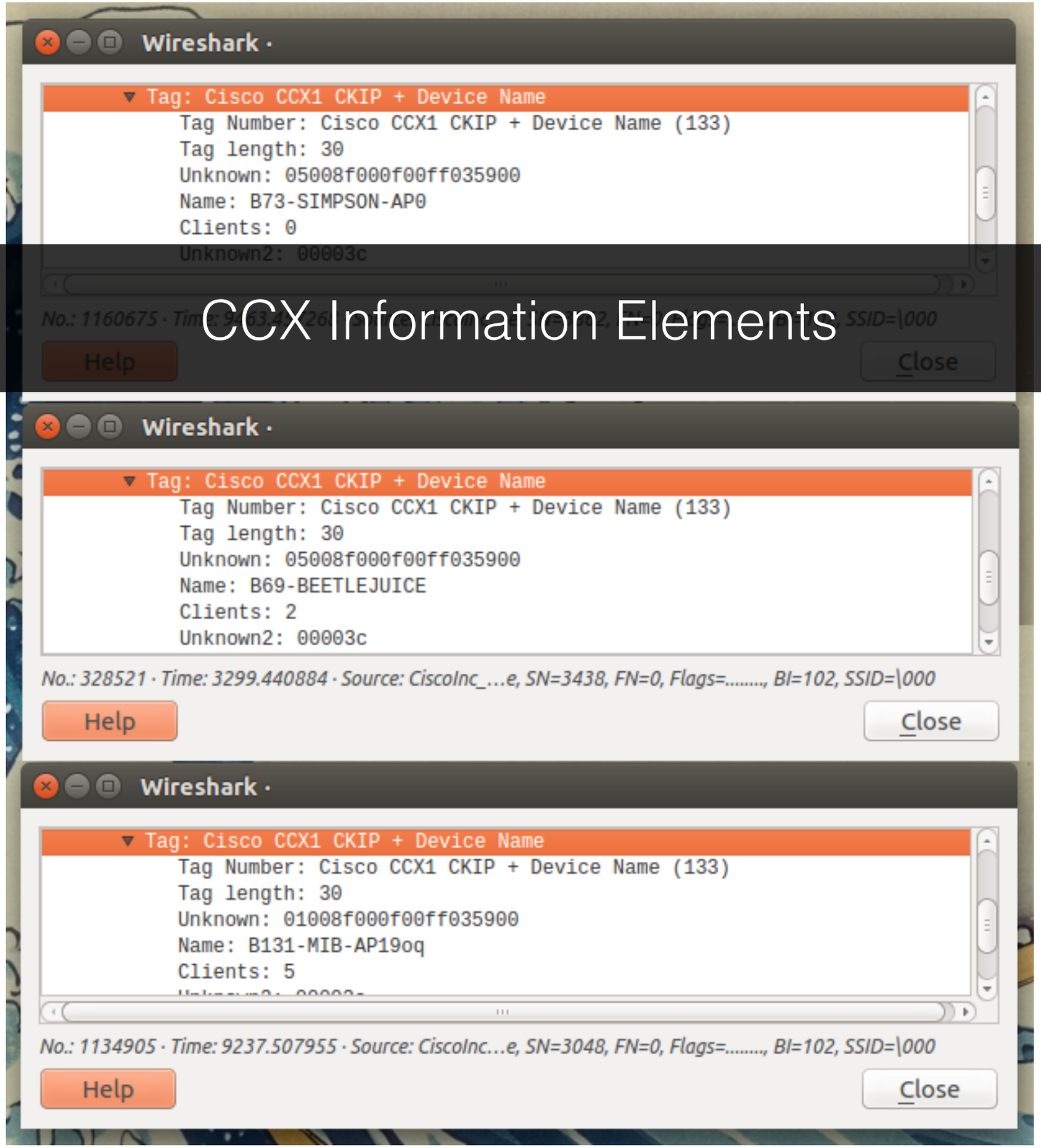
Cisco Client Extensions

If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

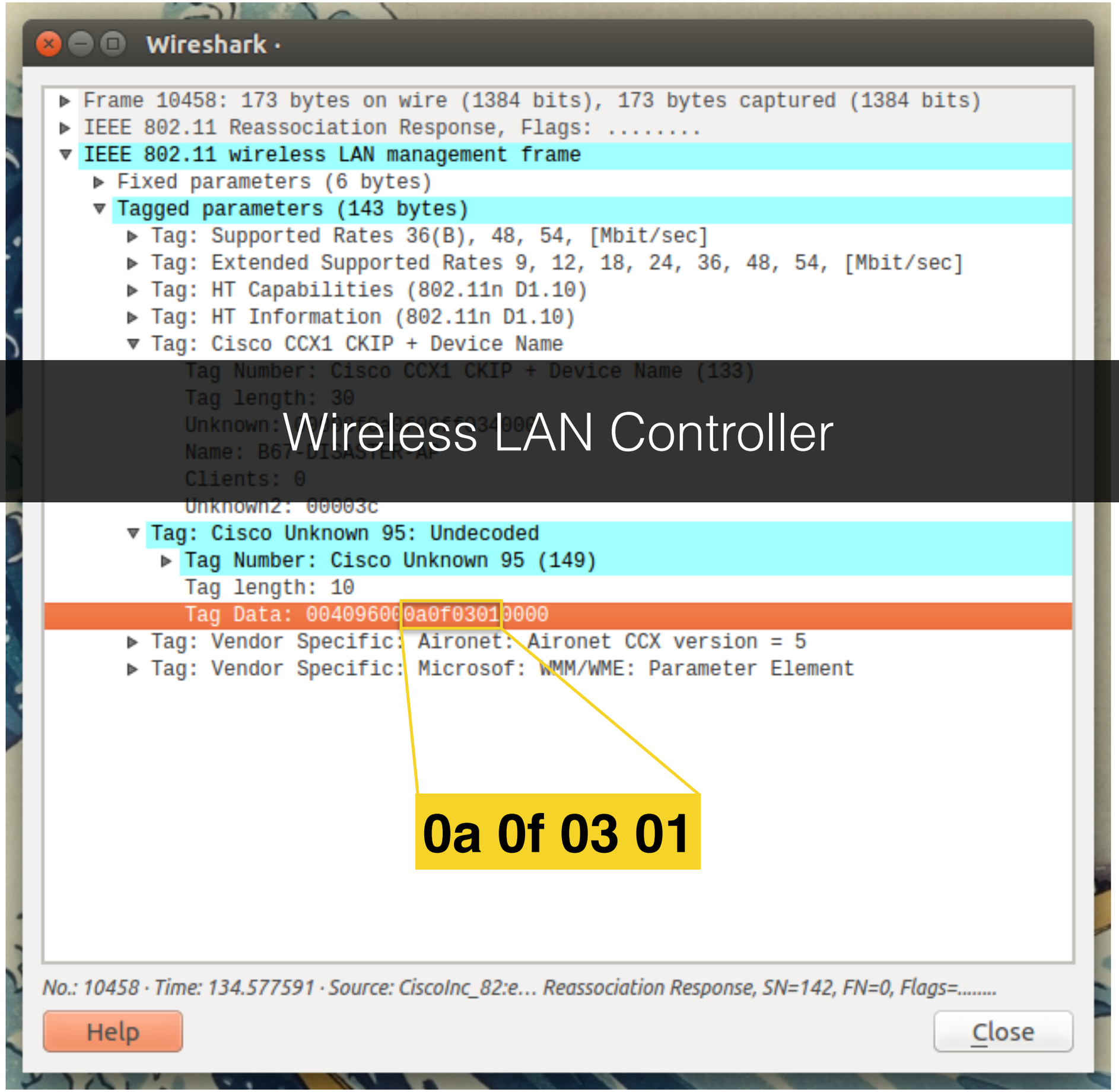
CCX Information Elements



CCX Information Elements



Wireless LAN Controller



Wireshark ·

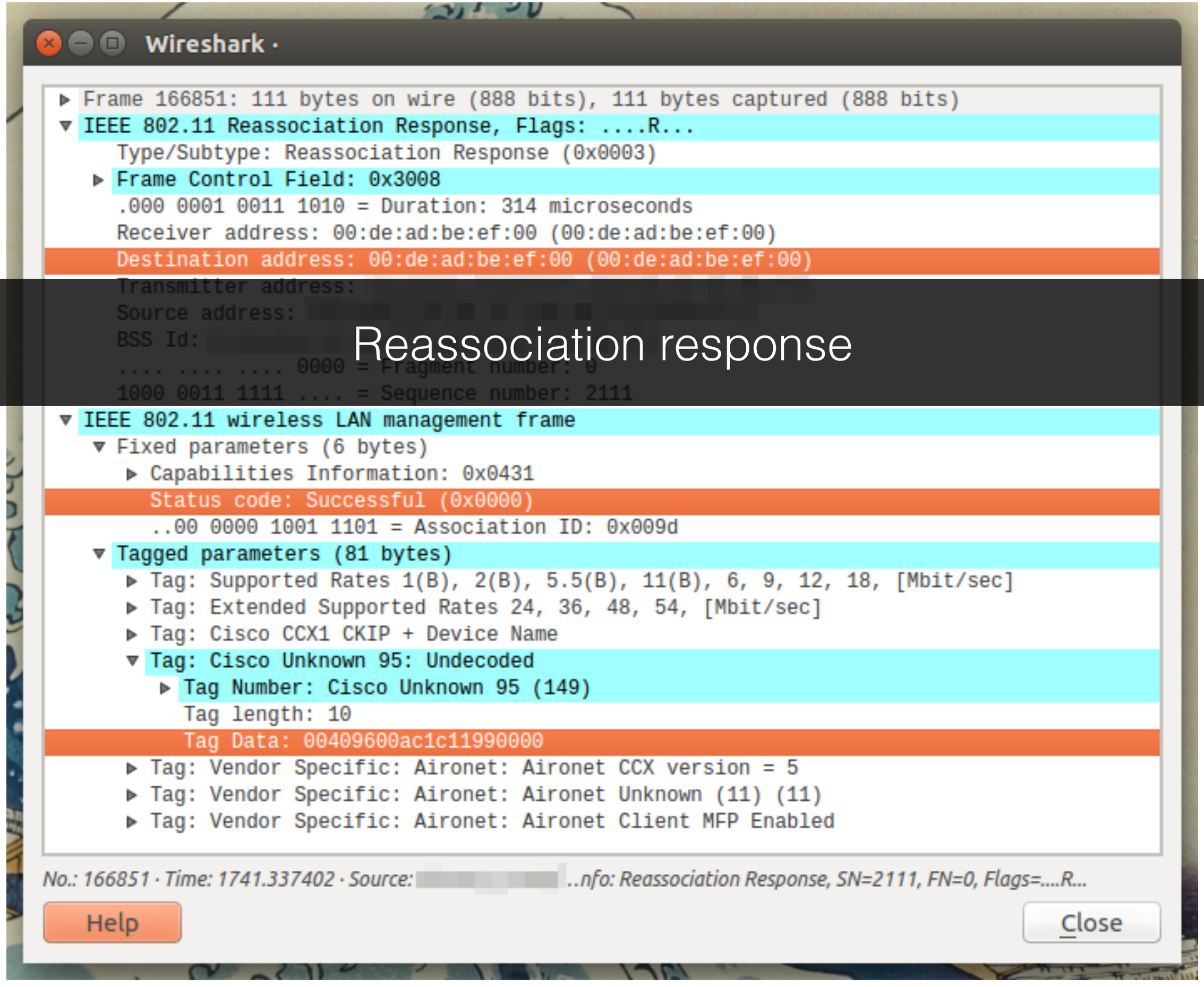
```
▶ Frame 166846: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
▼ IEEE 802.11 Reassociation Request, Flags: ........
    Type/Subtype: Reassociation Request (0x0002)
  ▶ Frame Control Field: 0x2000
    .000 0000 0010 1000 = Duration: 40 microseconds
    Receiver address:
    Destination address:
    Transmitter address: 00:de:ad:be:ef:00 (00:de:ad:be:ef:00)
    Source address: 00:de:ad:be:ef:00 (00:de:ad:be:ef:00)
    BSS Id: CiscoInc_53:85:f7 (68:86:a7:53:85:f7)
    .... .... .... 0000 = Fragment number: 0
    0011 1001 0000 .... = Sequence number: 912
▼ IEEE 802.11 wireless LAN management frame
  ▶ Fixed parameters (10 bytes)
  ▼ Tagged parameters (222 bytes)
    ▶ Tag: SSID parameter set: Usuarios
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 6
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: Country Information: Country Code AR, Environment Any
    ▶ Tag: QBSS Load Element 802.11e CCA Version
    ▶ Tag: ERP Information
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: RSN Information
    ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Cisco CCX1 CKIP + Device Name
    ▶ Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x11
    ▶ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: Aironet: Aironet Unknown (1) (1)
    ▶ Tag: Vendor Specific: Aironet: Aironet CCX version = 5
    ▶ Tag: Vendor Specific: Aironet: Aironet Unknown (11) (11)
```

No.: 166846 · Time: 1741.313941 · Source: 00:de:ad:be:ef:...tion Request, SN=912, FN=0, Flags=........, SSID=Usuarios

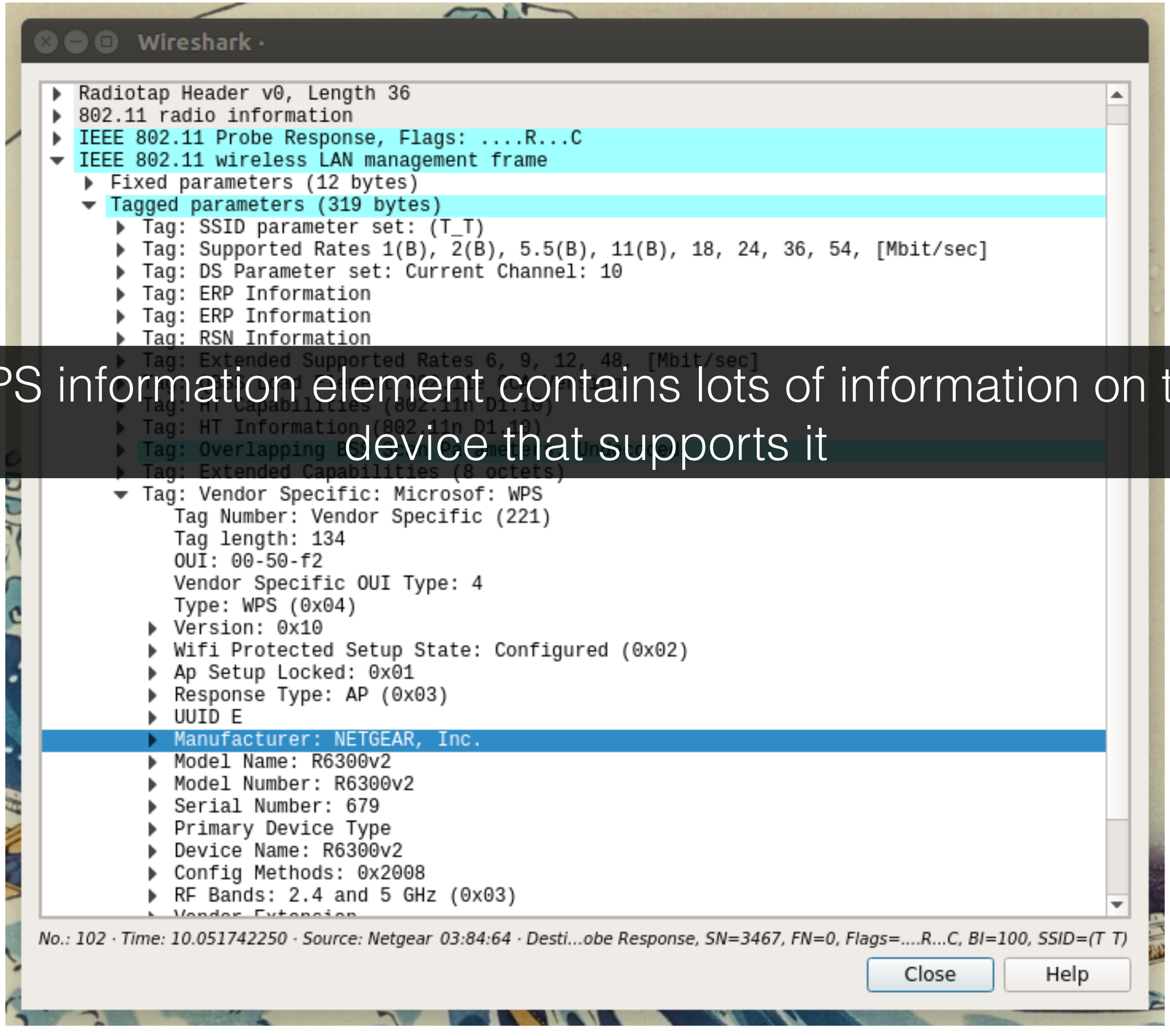
Help Close

Fake reassociation request frame

Reassociation response

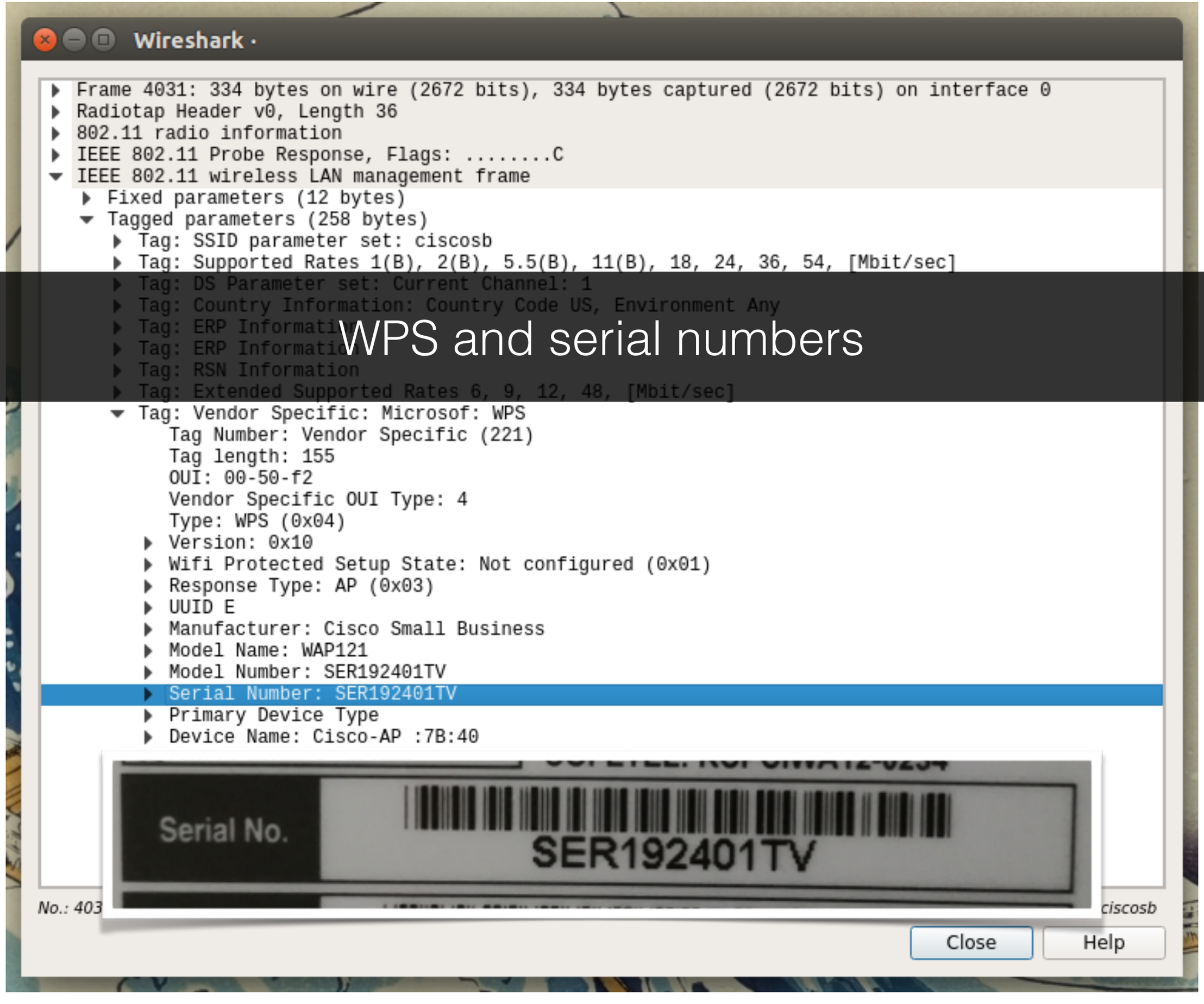


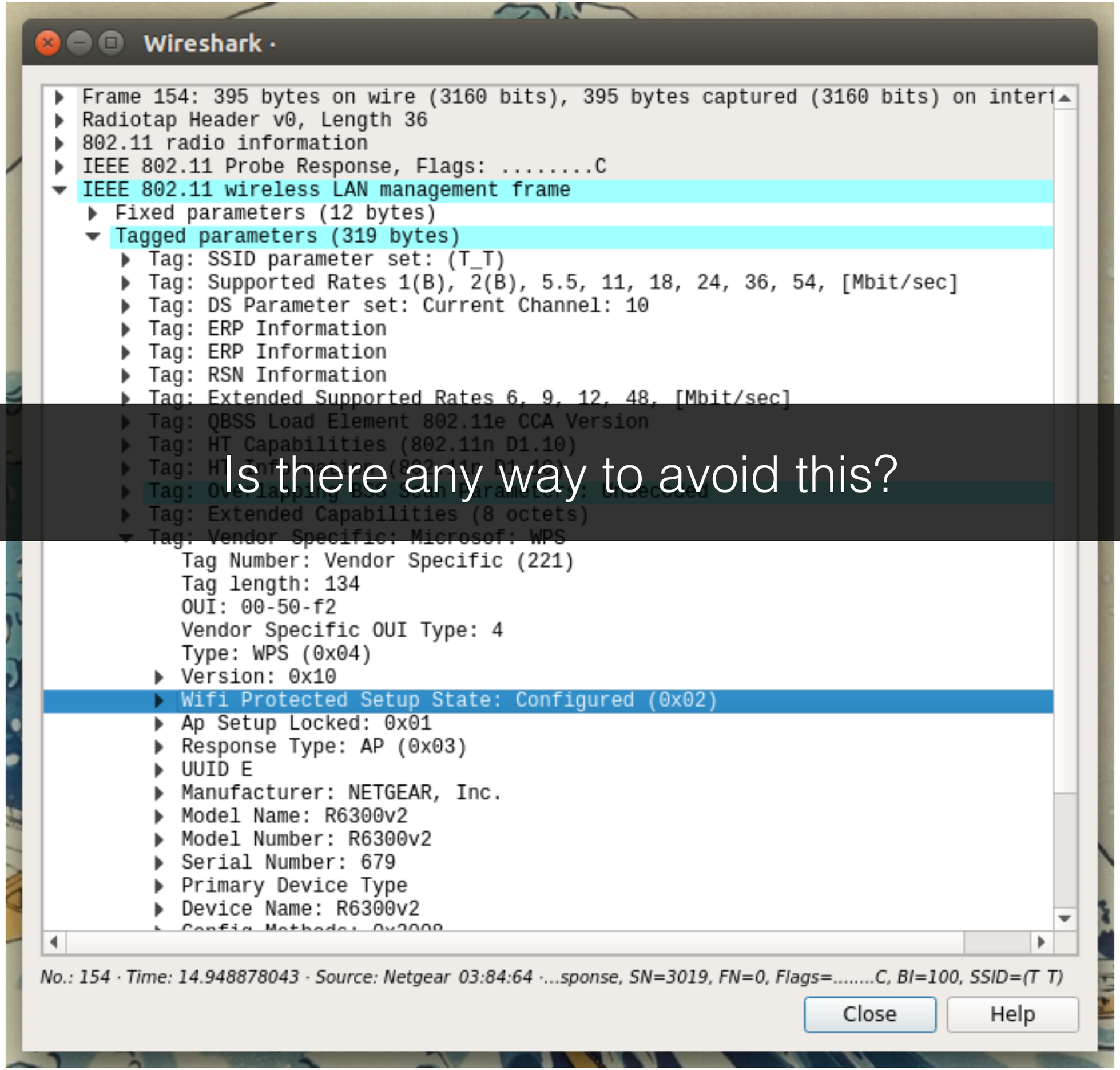
WPS & WiFi-Direct



WPS information element contains lots of information on the device that supports it

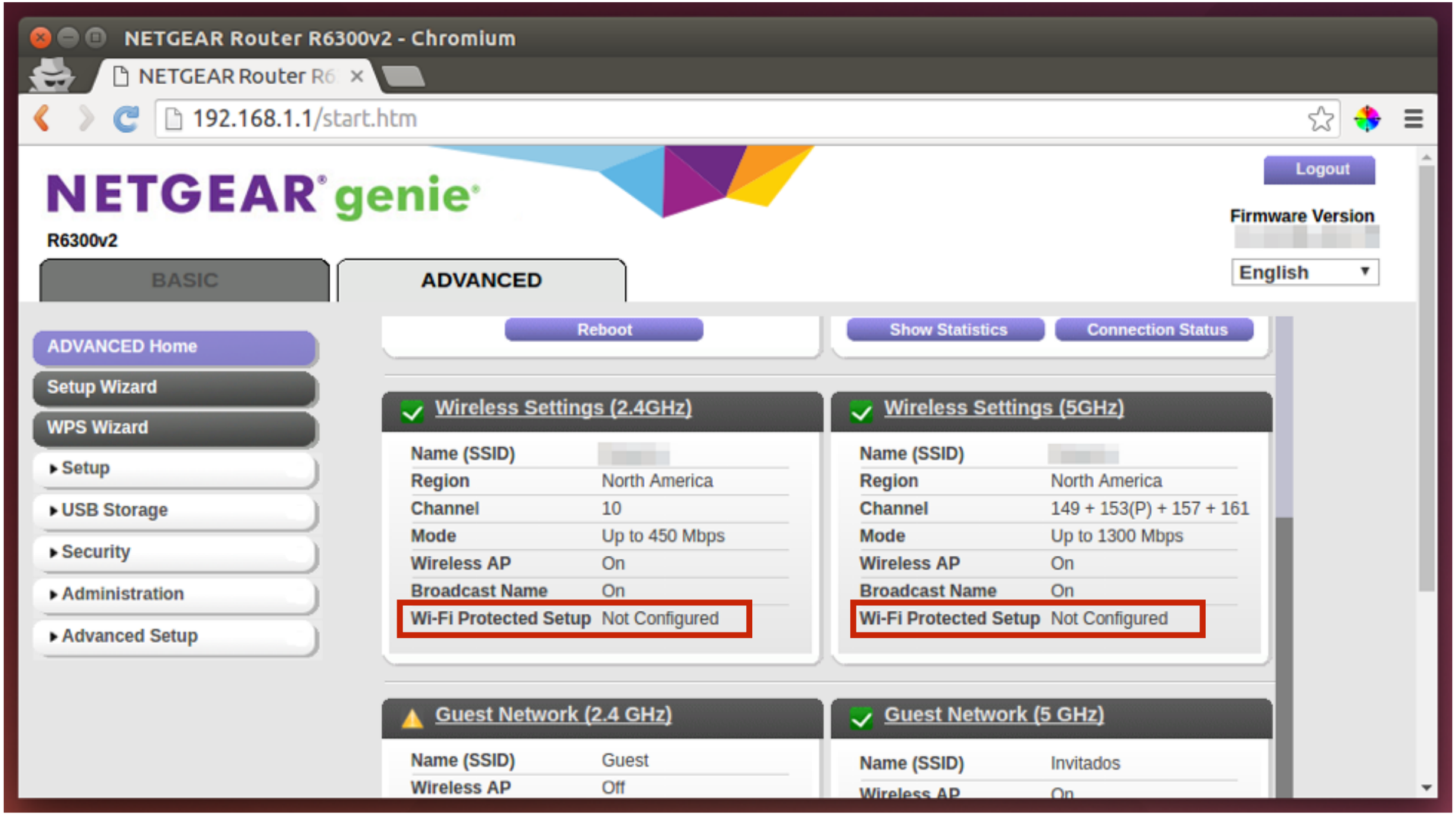
WPS and serial numbers

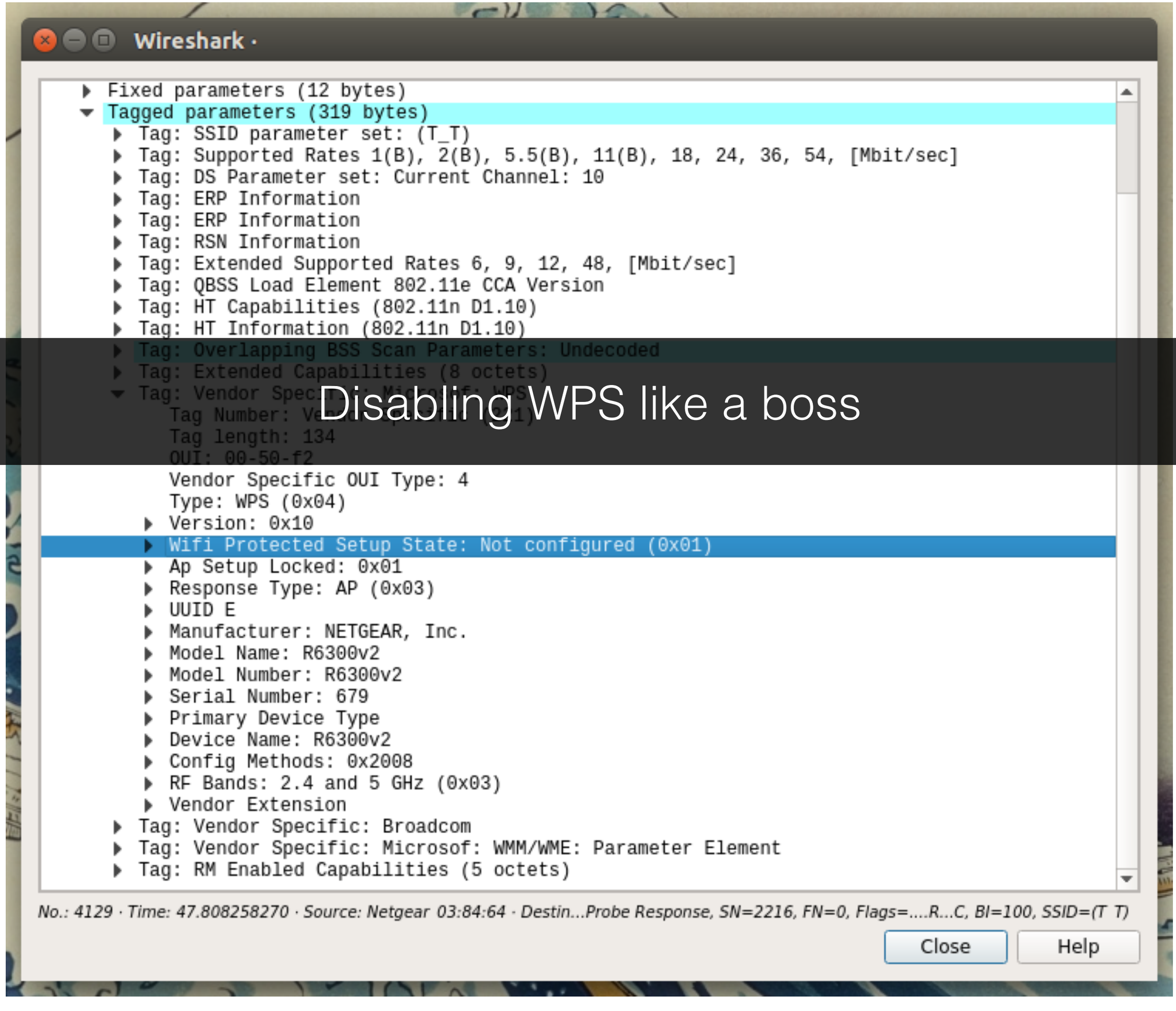




Is there any way to avoid this?

Disabling WPS?





Disabling WPS like a boss

Wireshark ·

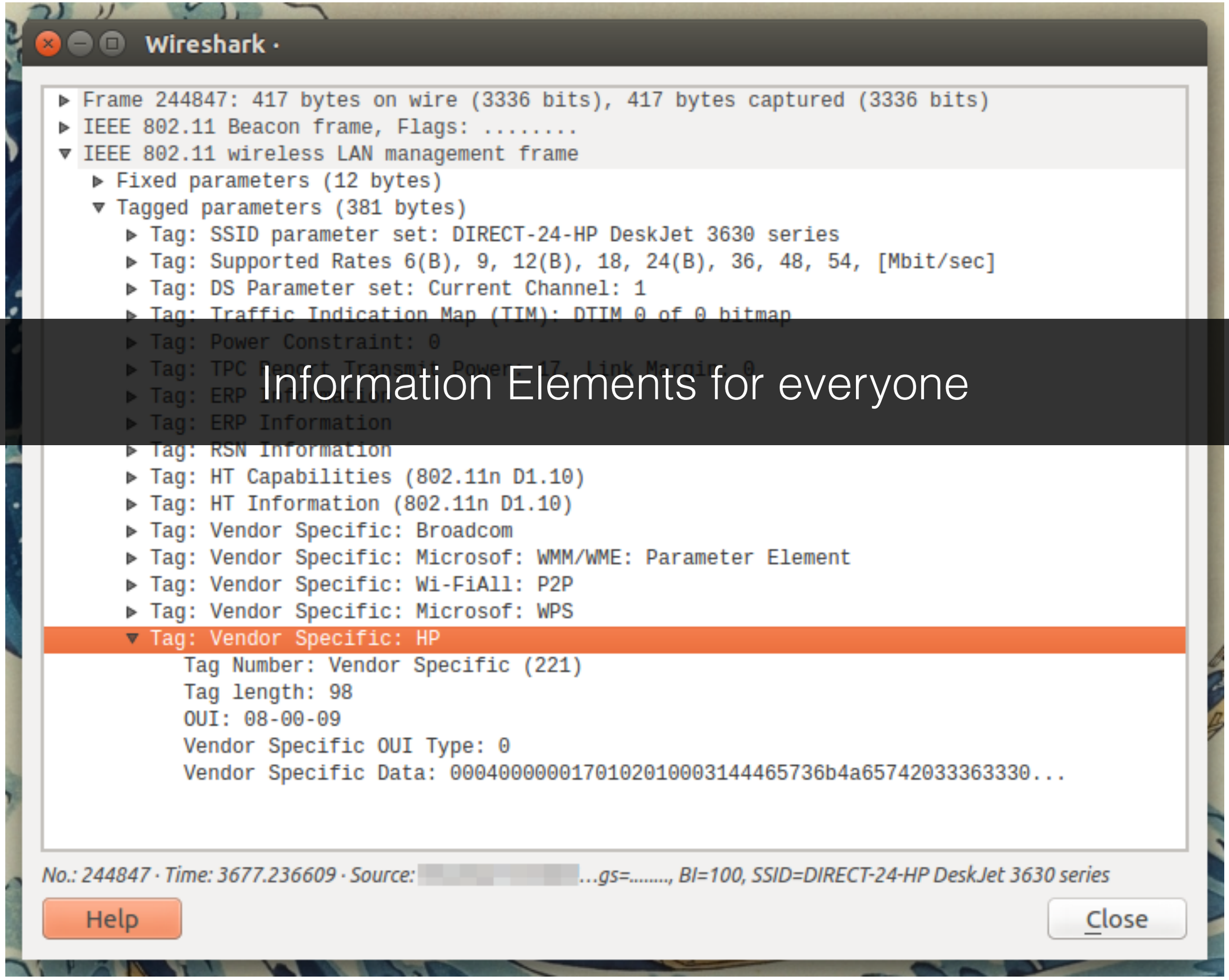
```
▶ Fixed parameters (12 bytes)
▼ Tagged parameters (264 bytes)
   ▶ Tag: SSID parameter set: DIRECT-
   ▶ Tag: Supported Rates 6(B), 9(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
   ▶ Tag: DS Parameter set: Current Channel: 10
   ▼ Tag: Vendor Specific: Microsof: WPS
        Tag Number: Vendor Specific (221)
        Tag length: 163
        OUI: 00-50-f2
        Vendor Specific OUI Type: 4
        Type: WPS (0x04)
      ▶ Version: 0x10
      ▶ Wifi Protected Setup State: Not configured (0x01)
      ▶ Device Password ID: PIN (default) (0x0000)
      ▶ Response Type: Enrollee, Info only (0x00)
      ▶ UUID E
      ▶ Manufacturer: Western Digital Corporation
      ▶ Model Name: WD TV Live
      ▶ Model Number: WDBHG70000NBK
      ▶ Serial Number: WNC441203527
      ▶ Primary Device Type
      ▶ Device Name: WDTVLive
      ▶ Config Methods: 0x2388
      ▶ Vendor Extension
   ▼ Tag: Vendor Specific: Wi-FiAll: P2P
        Tag Number: Vendor Specific (221)
        Tag length: 41
        OUI: 50-6f-9a
        Vendor Specific OUI Type: 9
      ▶ P2P Capability: Device 0x23  Group 0x0
      ▶ P2P Device Info
   ▶ Tag: Vendor Specific: Wi-FiAll: Wi-Fi Display
```

No.: 716 · Time: 17.646745 · Source: 02:90:a9:67:7b:7e · Destin…be Response, SN=667, FN=0, Flags=....., BI=100, SSID=DIRECT-

Help

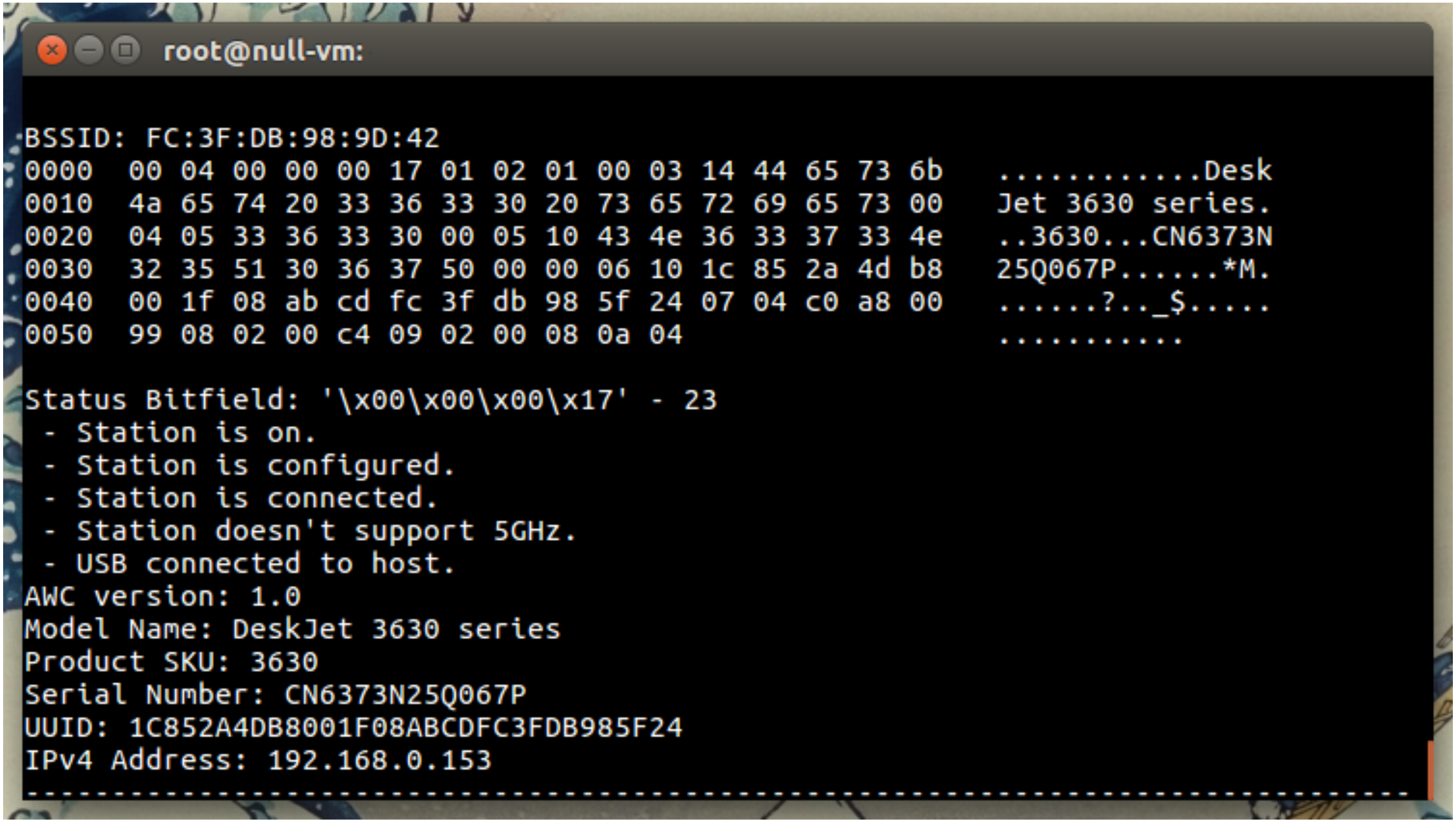
Close

WiFi-Direct



Information Elements for everyone

Information Elements for everyone

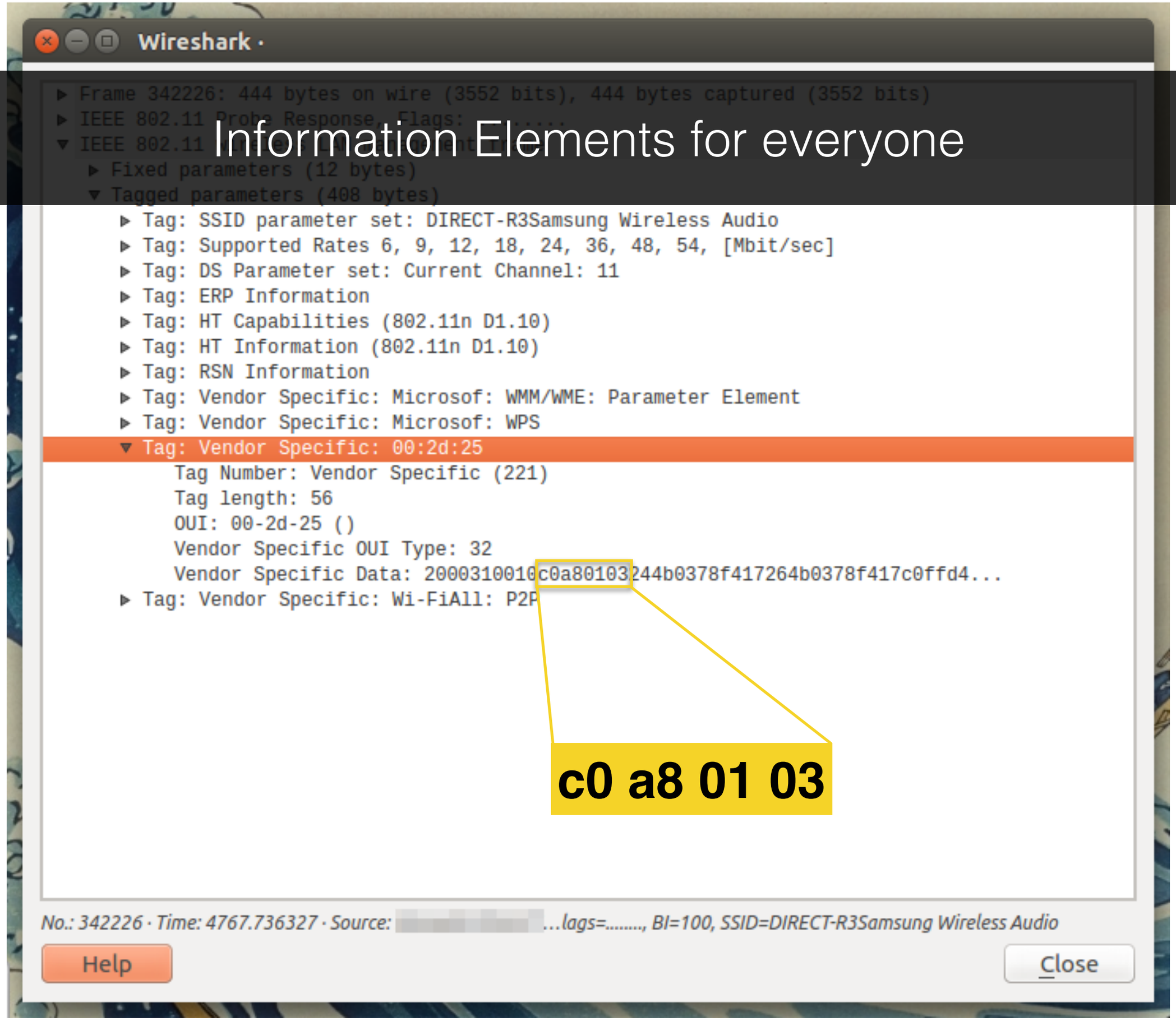


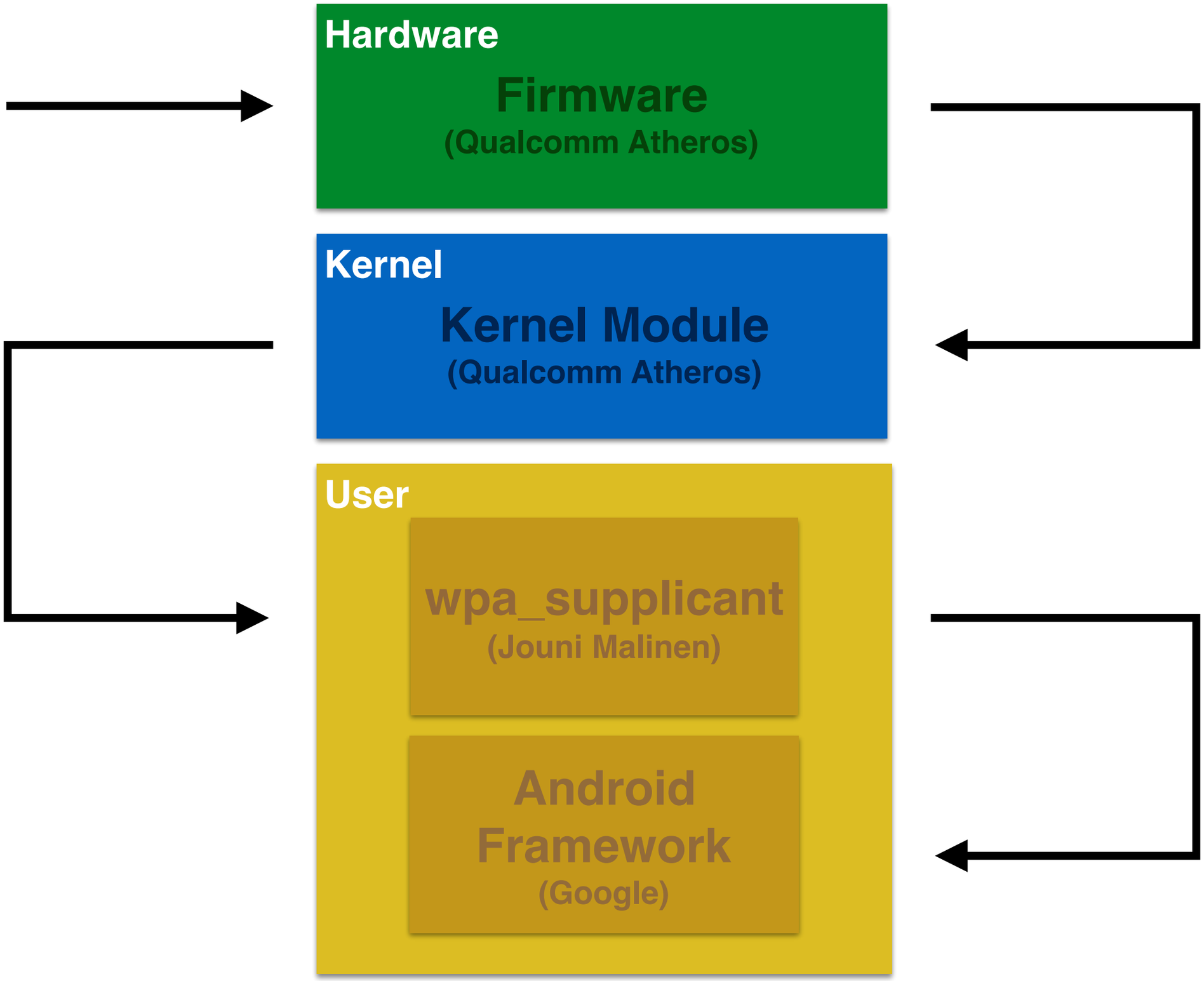
Information Elements for everyone

```
▶ Frame 600: 815 bytes on wire (6520 bits), 815 bytes captured (6520 bits)
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▼ IEEE 802.11 Action, Flags: ....C
    Type/Subtype: Action (0x000d)
  ▶ Frame Control Field: 0xd000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: 9e:ae:17:fd:e4:3b (9e:ae:17:fd:e4:3b)
    Source address: 9e:ae:17:fd:e4:3b (9e:ae:17:fd:e4:3b)
    BSS Id: Apple_ff:94:73 (00:25:00:ff:94:73)
    .... .... .... 0000 = Fragment number: 0
    1100 1001 1001 .... = Sequence number: 3225
  ▶ Frame check sequence: 0xf3580425 [correct]
▶ IEEE 802.11 wireless LAN management frame
▶ [Malformed Packet: IEEE 802.11]
```

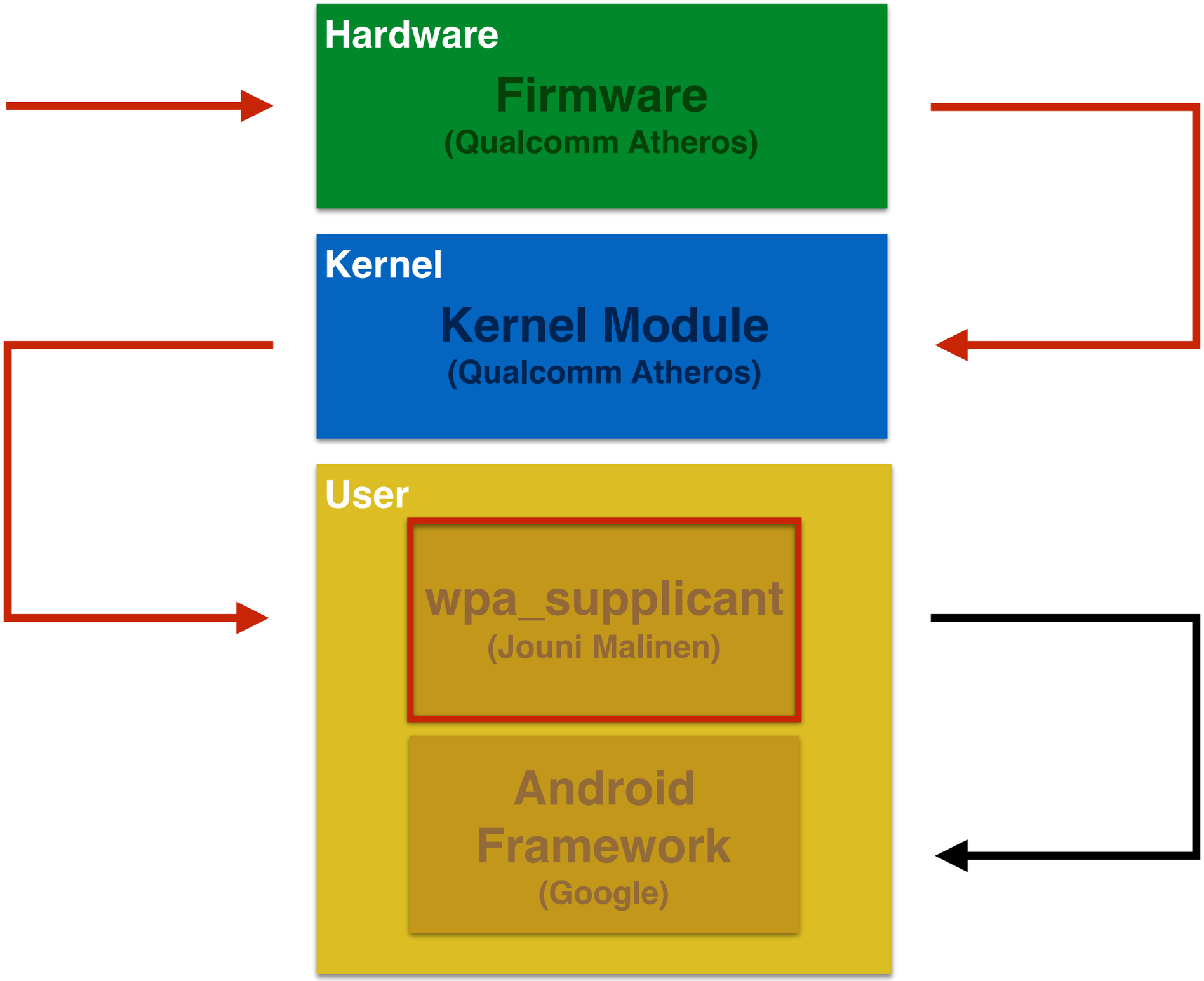
```
01c0  46 46 37 2c 30 78 45 08  6d 64 3d 30 2c 31 2c 32   FF7,0xE. md=0,1,2
01d0  0d 61 6d 3d 41 70 70 6c  65 54 56 33 2c 31 43 70   .am=Appl eTV3,1Cp
01e0  6b 3d 37 62 36 33 33 37  61 38 37 64 62 62 36 30   k=7b6337 a87dbb60
01f0  30 36 66 65 63 66 30 30  37 30 30 34 66 33 62 30   06fecf00 7004f3b0
0200  62 31 34 65 32 38 65 31  66 64 39 31 30 64 36 62   b14e28e1 fd910d6b
0210  63 33 33 39 64 39 31 34  39 30 39 34 65 63 62 61   c339d914 9094ecba
0220  65 64 06 73 66 3d 30 78  34 06 74 70 3d 55 44 50   ed.sf=0x 4.tp=UDP
0230  08 76 6e 3d 36 35 35 33  37 09 76 73 3d 32 32 30   .vn=6553 7.vs=220
0240  2e 36 38 04 76 76 3d 32  02 e0 00 0c 00 08 61 70   .68.vv=2 ......ap
0250  70 6c 65 20 74 76 c0 01  10 ce 00 00 00 1a 64 65   ple tv.. ......de
0260  76 69 63 65 69 64 3d 37  43 3a 44 31 3a 43 33 3a   viceid=7 C:D1:C3:
0270  32 36 3a 35 34 3a 44 31  17 66 65 61 74 75 72 65   26:54:D1 .feature
0280  73 3d 30 78 35 41 37 46  46 46 46 37 2c 30 78 45   s=0x5A7F FFF7,0xE
0290  09 66 6c 61 67 73 3d 30  78 34 10 6d 6f 64 65 6c   .flags=0 x4.model
02a0  3d 41 70 70 6c 65 54 56  33 2c 31 43 70 6b 3d 37   =AppleTV 3,1Cpk=7
02b0  62 36 33 33 37 61 38 37  64 62 62 36 30 30 36 66   b6337a87 dbb6006f
02c0  65 63 66 30 30 37 30 30  34 66 33 62 30 62 31 34   ecf00700 4f3b0b14
```

Information Elements for everyone





802.11 Android architecture



802.11 Android architecture

```
D/TCMD    (  519): Listening for incoming client connection request
I/wpa_supplicant( 3482): P2P-DEVICE-FOUND 70:5a:0f:16:ed:54 p2p_dev_addr=72:5a:0f:16:b4:66 pri_de
 name='DIRECT-66-HP OfficeJet Pro 8710' config_methods=0x5a88 dev_capab=0x4 group_capab=0x1 level
I/wpa_supplicant( 3482): P2P-DEVICE-FOUND 00:de:ad:fa:fa:fa p2p_dev_addr=00:de:ad:fa:fa:fa pri_de
5 name='fafa<FA><FA>' config_methods=0x188 dev_capab=0x21 group_capab=0x0 level=-27
D/MDMCTBK (  267): reply_len: 40 reply is = <3>P2P-DEVICE-FOUND 70:5a:0f:16:ed:54 p2
D/MDMCTBK (  267): Event received = P2P-DEVICE-FOUND 70:5a:0f:16:ed:54 p2
D/MDMCTBK (  267): reply_len: 40 reply is = <3>P2P-DEVICE-FOUND 00:de:ad:fa:fa:fa p2
D/MDMCTBK (  267): Event received = P2P-DEVICE-FOUND 00:de:ad:fa:fa:fa p2
D/WifiP2pService( 1024): InactiveState{ when=-1ms what=147477 obj=Device: DIRECT-66-HP OfficeJet
D/WifiP2pService( 1024):  deviceAddress: 72:5a:0f:16:b4:66
D/WifiP2pService( 1024):  primary type: 3-0050F204-1
D/WifiP2pService( 1024):  secondary type: null
D/WifiP2pService( 1024):  wps: 23176
D/WifiP2pService( 1024):  grpcapab: 1
D/WifiP2pService( 1024):  devcapab: 4
D/WifiP2pService( 1024):  status: 3
D/WifiP2pService( 1024):  wfdInfo: null
D/WifiP2pService( 1024):  level: -49 target=com.android.internal.util.StateMachine$SmHandler }
```

```
D/WifiP2pService( 1024): P2pEnabledState{ when=-1ms what=147477 obj=Device: DIRECT-66-HP OfficeJe
D/WifiP2pService( 1024):  deviceAddress: 72:5a:0f:16:b4:66
D/WifiP2pService( 1024):  primary type: 3-0050F204-1
D/WifiP2pService( 1024):  secondary type: null
D/WifiP2pService( 1024):  wps: 23176
D/WifiP2pService( 1024):  grpcapab: 1
D/WifiP2pService( 1024):  devcapab: 4
D/WifiP2pService( 1024):  status: 3
D/WifiP2pService( 1024):  wfdInfo: null
```

CVE-2014-0997

```
D/WifiP2pService( 1024):  level: -49 target=com.android.internal.util.StateMachine$SmHandler }
W/dalvikvm( 1024): threadid=71: thread exiting with uncaught exception (group=0x4171bd40)
E/AndroidRuntime( 1024): *** FATAL EXCEPTION IN SYSTEM PROCESS: WifiMonitor
E/AndroidRuntime( 1024): java.lang.IllegalArgumentException: Malformed supplicant event
E/AndroidRuntime( 1024):        at android.net.wifi.p2p.WifiP2pDevice.<init>(WifiP2pDevice.java:2
E/AndroidRuntime( 1024):        at android.net.wifi.WifiMonitor$MonitorThread.handleP2pEvents(Wif
E/AndroidRuntime( 1024):        at android.net.wifi.WifiMonitor$MonitorThread.dispatchEvent(WifiM
E/AndroidRuntime( 1024):        at android.net.wifi.WifiMonitor$MonitorThread.run(WifiMonitor.jav
I/Process ( 1024): Sending signal. PID: 1024 SIG: 9
I/ServiceManager(  255): service 'package' died
I/ServiceManager(  255): service 'sensorservice' died
```

WD TV Live

ork Settings

tup

Default?

Network Setup

Check Connection

Auto Detect Wi-Fi Direct Setup On

Wireless Display (Miracast™)

Device Name WDTVLive

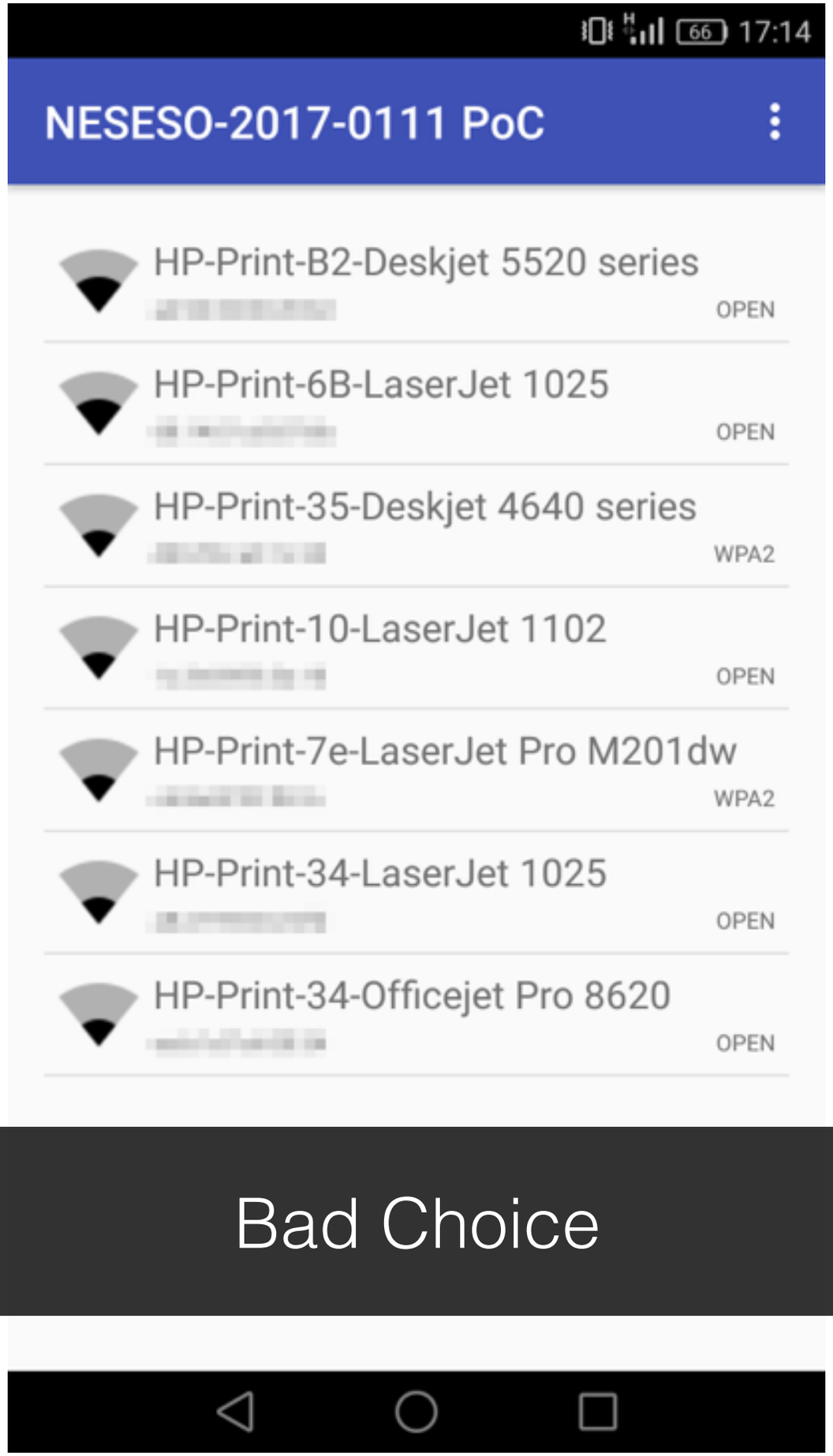
```
Completed SYN Stealth Scan at 22:04, 4.61s elapsed (1000 total ports)
Initiating Service scan at 22:04
Scanning 5 services on 192.168.69.61
Completed Service scan at 22:04, 26.03s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.69.61
Retrying OS detection (try #2) against 192.168.69.61
NSE: Script scanning 192.168.69.61.
Initiating NSE at 22:04
Completed NSE at 22:05, 66.34s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Nmap scan report for 192.168.69.61
Host is up (0.0033s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd (PHP 5.2.17)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp   open  ssl/http    Apache httpd (PHP 5.2.17)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
30000/tcp open  unknown
MAC Address: 02:90:A9:67:7B:7E (Unknown)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -
No OS matches for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   3.34 ms 192.168.69.61

NSE: Script Post-scanning.
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
```

Services

HP WiFi Printers


17:14
NESESO-2017-0111 PoC
HP-Print-B2-Deskjet 5520 series
OPEN
HP-Print-6B-LaserJet 1025
OPEN
HP-Print-35-Deskjet 4640 series
WPA2
HP-Print-10-LaserJet 1102
OPEN
HP-Print-7e-LaserJet Pro M201dw
WPA2
HP-Print-34-LaserJet 1025
OPEN
HP-Print-34-Officejet Pro 8620
OPEN

Bad Choice

HP OfficeJet Pro 8710

Embedded Web Server

Search

Home | Scan | Fax | Web Services | Network | Tools | Settings

NETWORK

+ General

+ Wired (802.3)

+ Wireless (802.11)

– Wi-Fi Direct

Status

+ AirPrint™

+ Google Cloud Print

+ Internet Printing Protocol

+ Advanced Settings

Wi-Fi Direct

Status

Wi-Fi Direct Settings

Change the Wi-Fi Direct settings, and then click Apply.

Status: On

Wi-Fi Direct Name: DIRECT-66-HP OfficeJet Pro 8710

Connection Method: Automatic

Wi-Fi Direct Password: 12345678 Generate

Default credentials for “WiFi-Direct”

Apply Cancel

English

HP Connected | Product Support | Software | HP SureSupply | About HP

HP OfficeJet Pro 8710

Embedded Web Server

Search

Home | Scan | Fax | Web Services | Network | Tools | Settings

NETWORK

- General
  - Network Summary
  - Network Identification
  - Network Protocols
  - Proxy Settings
- + Wired (802.3)
- + Wireless (802.11)
- + Wi-Fi Direct
- + AirPrint™
- + Google Cloud Print
- + Internet Printing Protocol
- + Advanced Settings

General

Network Summary

Wired (802.3)

Status: Not connected

Host Name: HP16B465

IP Address:

Hardware (MAC) Address: 705A0F16B465

Wireless (802.11)

Status: Connected

Host Name: HP16B465

IP Address: 192.168.0.104

Hardware (MAC) Address: 705A0F16B466

SSID: [redacted]

Wi-Fi Direct

Wi-Fi Direct Name: DIRECT-66-HP OfficeJet Pro 8710

Security by default

```
Initiating SYN Stealth Scan at 22:31
Scanning 192.168.223.1 [1000 ports]
Discovered open port 443/tcp on 192.168.223.1
Discovered open port 8080/tcp on 192.168.223.1
Discovered open port 80/tcp on 192.168.223.1
Discovered open port 9220/tcp on 192.168.223.1
Increasing send delay for 192.168.223.1 from 0 to 5 due to 34 out of 113 dropped probe
 increase.
Increasing send delay for 192.168.223.1 from 5 to 10 due to 34 out of 111 dropped prob
t increase.
Discovered open port 515/tcp on 192.168.223.1
Increasing send delay for 192.168.223.1 from 10 to 20 due to 19 out of 61 dropped prob
t increase.
Increasing send delay for 192.168.223.1 from 20 to 40 due to 11 out of 26 dropped prob
t increase.
Increasing send delay for 192.168.223.1 from 40 to 80 due to 11 out of 33 dropped prob
t increase.
```

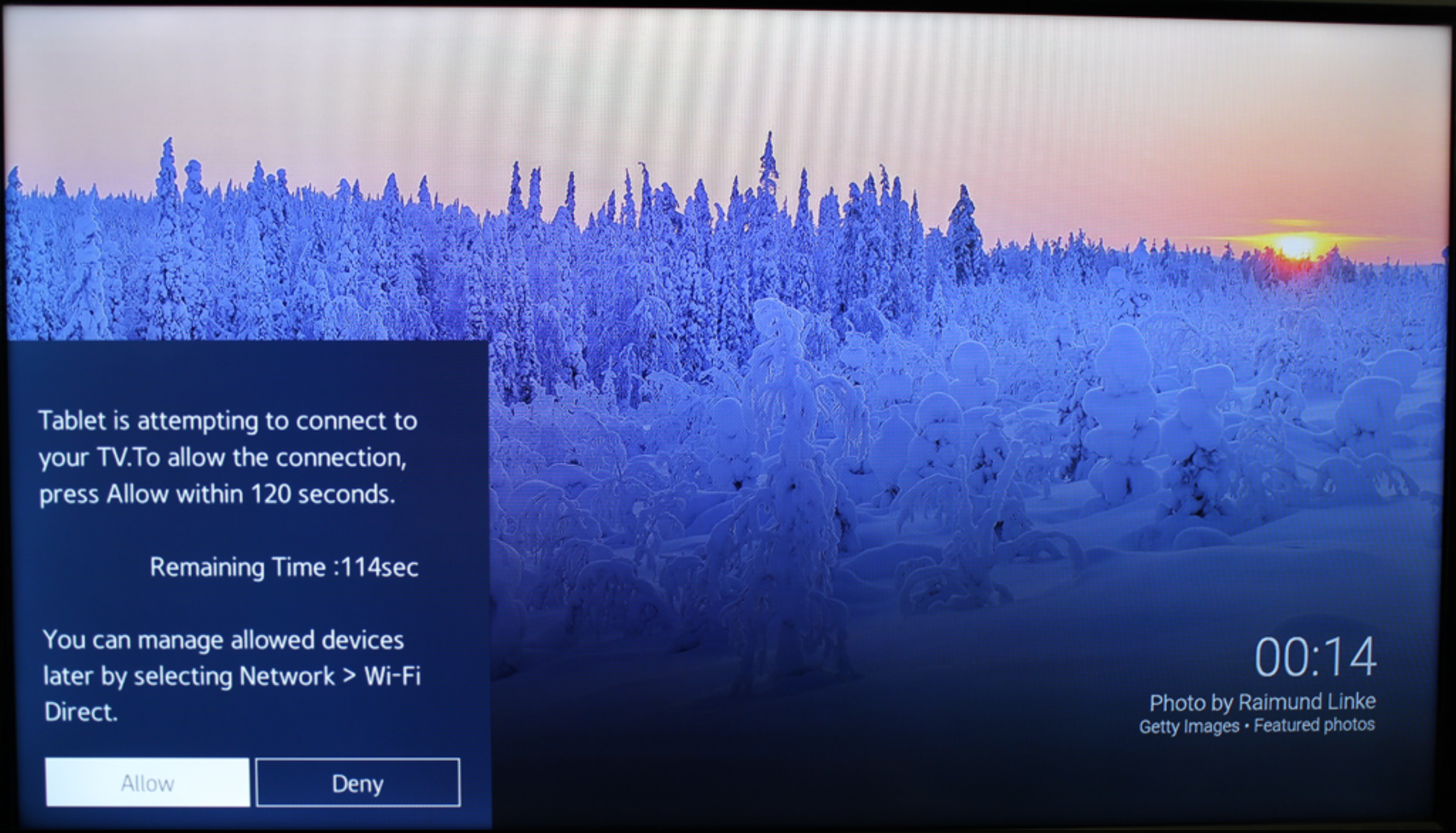
```
Discovered open port 9100/tcp on 192.168.223.1
Discovered open port 631/tcp on 192.168.223.1
Completed SYN Stealth Scan at 22:33, 84.01s elapsed (1000 total ports)
Nmap scan report for 192.168.223.1
Host is up (0.0020s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
8080/tcp open  http-proxy
9100/tcp open  jetdirect
9220/tcp open  unknown
MAC Address: 70:5A:0F:16:ED:54 (Hewlett Packard)

Read data files from: /usr/bin/../share/nmap
```

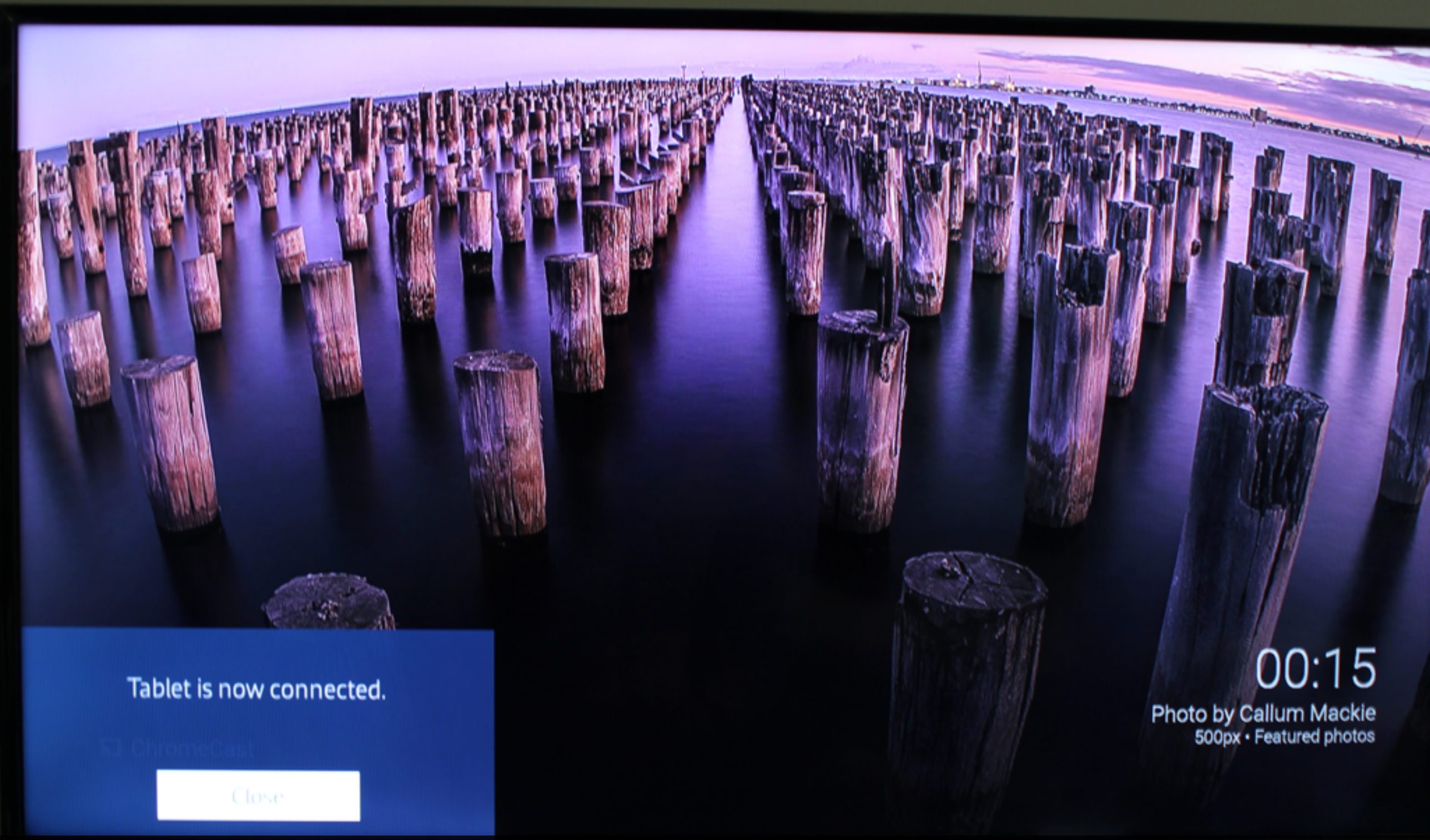
Services


They've got no idea I used my phone

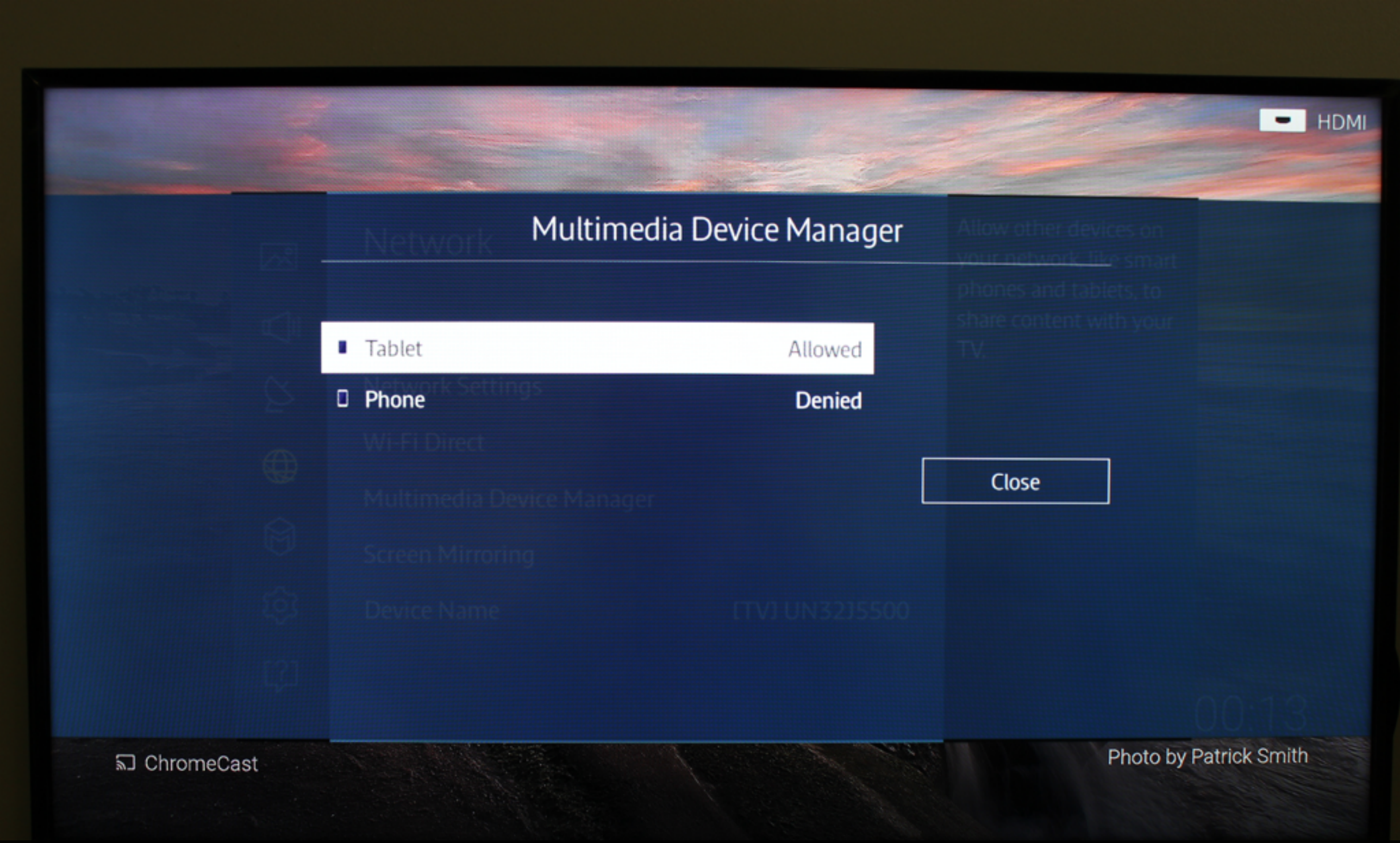
Samsung Smart TVs



Authentication



Notification



Device Manager

```
Initiating SYN Stealth Scan at 22:42
Scanning 192.168.49.1 [1000 ports]
Discovered open port 8080/tcp on 192.168.49.1
Discovered open port 7676/tcp on 192.168.49.1
Discovered open port 8002/tcp on 192.168.49.1
Increasing send delay for 192.168.49.1 from 0 to 5 due to 113 out of 376 dropped probe
 increase.
Increasing send delay for 192.168.49.1 from 5 to 10 due to 145 out of 481 dropped prob
t increase.
Increasing send delay for 192.168.49.1 from 10 to 20 due to 12 out of 39 dropped probe
 increase.
Increasing send delay for 192.168.49.1 from 20 to 40 due to max_successful_tryno incre
Increasing send delay for 192.168.49.1 from 40 to 80 due to 11 out of 34 dropped probe
 increase.
Discovered open port 8001/tcp on 192.168.49.1
Increasing send delay for 192.168.49.1 from 80 to 160 due to 48 out of 159 dropped pro
st increase.
Discovered open port 8000/tcp on 192.168.49.1
Discovered open port 9999/tcp on 192.168.49.1
Completed SYN Stealth Scan at 22:43, 66.01s elapsed (1000 total ports)
Nmap scan report for 192.168.49.1
Host is up (0.062s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
7676/tcp open  imqbrokerd
8000/tcp open  http-alt
8001/tcp open  vcom-tunnel
8002/tcp open  teradataordbms
8080/tcp open  http-proxy
9999/tcp open  abyss
MAC Address: CE:B1:1A:F4:B7:F5 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 79.32 seconds
```

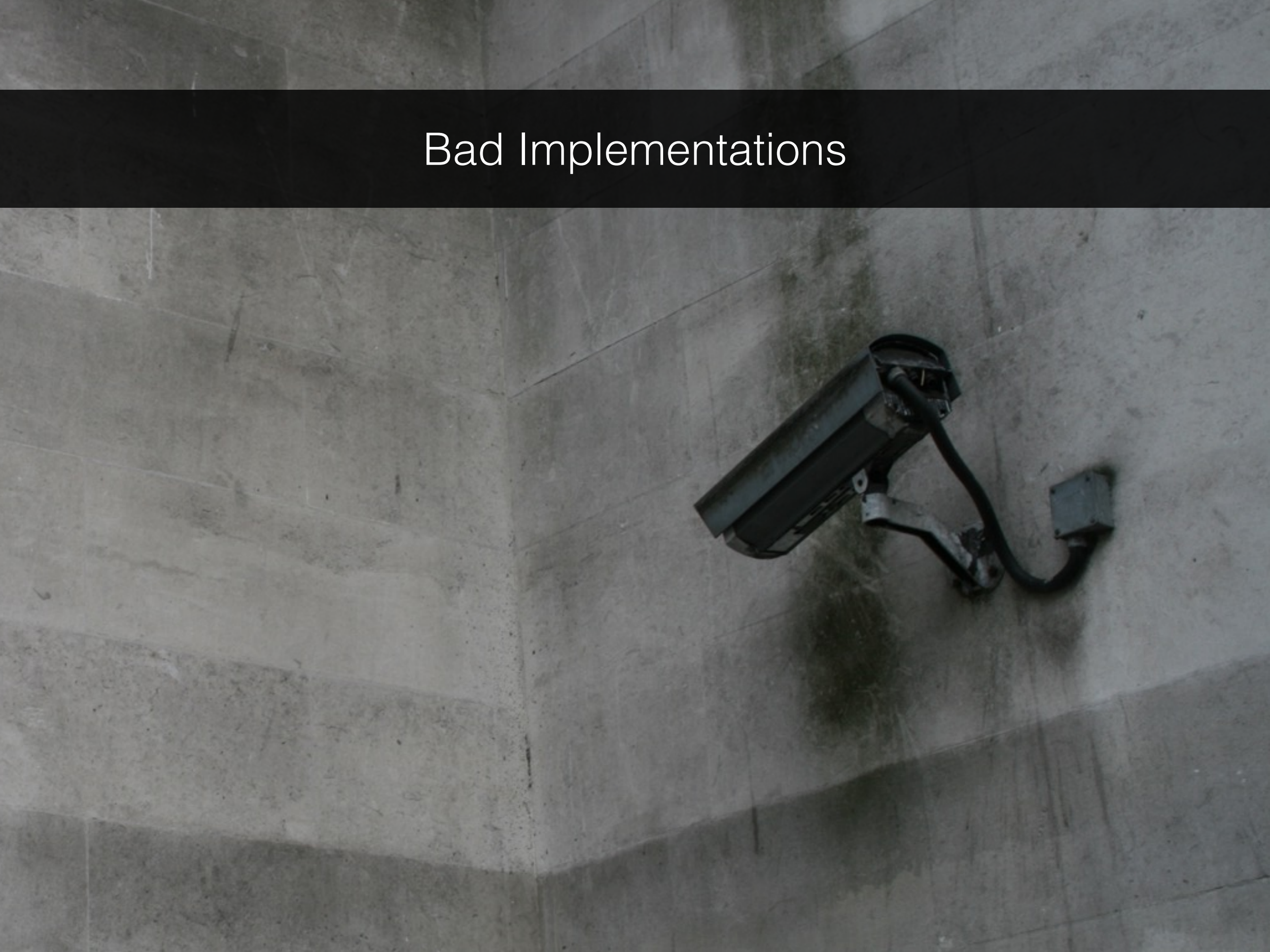
Services

The attack surface it's extending

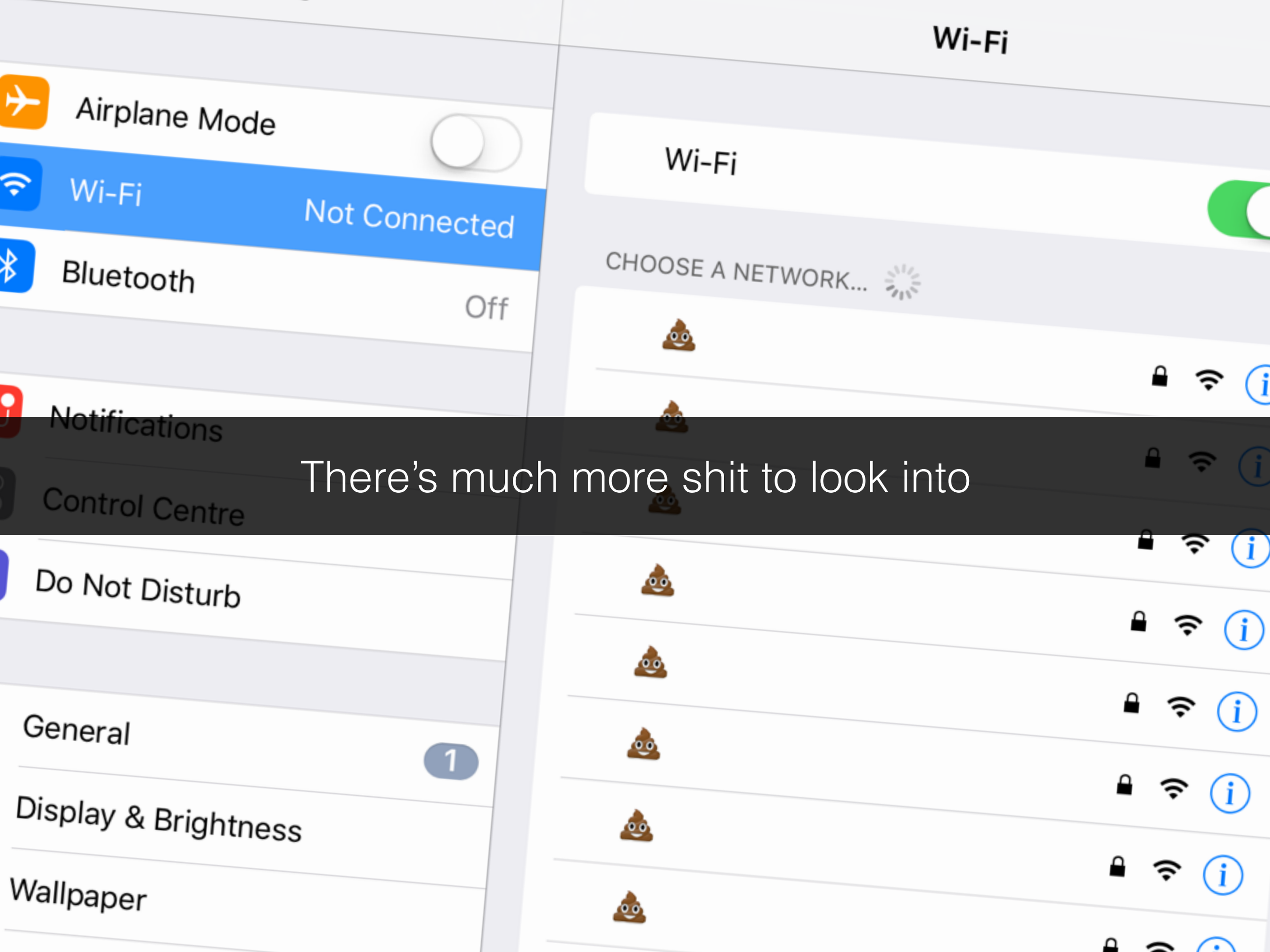
New protocols and specifications could be used for device fingerprinting

Too Many Hands in the Pot

Bad Implementations



Network Access


Airplane Mode
Wi-Fi
Not Connected
Bluetooth
Off
Notifications
Control Centre
Do Not Disturb
General
1
Display & Brightness
Wallpaper
Wi-Fi
Wi-Fi
CHOOSE A NETWORK...
There’s much more shit to look into

Questions

https://github.com/6e726d/WIG

Email: 6e726d@gmail.com **Twitter:** @6e726d