Leveraging Wireshark for Wireless Network Analysis

4/1/2008

Joshua Wright
Senior Security Researcher | Aruba Networks

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

Sample captures at
www.willhackforsushi.com/resources/sharkfest08-samples.zip

Introduction

Introduction

Wireshark and wireless analysis

Leveraging display filters

Customizing the display

Enhancing filters with macros

Searching for anomalies

Extracting data

Decrypting frame contents

Sample captures at
www.willhackforsushi.com/resources/sharkfest08-samples.zip

CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY

Introduction

Wireless networks have become ubiquitious for many organizations

Users bring experiences with home wireless to the enterprise

WPA, PEAP, WMM, QoS, 802.11n, hotspots, TKIP, RFID, WIDS, rogues, DSSS, FMC (it's all complicated)

Wireless troubleshooting can be complex

- Physical layer issues notoriously difficult to characterize

Wireshark is indispensable for WiFi troubleshooting

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

Wireless Sniffing

Wireless capture a universal troubleshooting and analysis mechanism

Requires no authentication or access privileges

- Useful for security auditing, see the network as an adversary does

Wireless cards support multiple operating modes

- Master, Managed, Ad-Hoc, Monitor

Captures in monitor mode disclose 802.11 frame information

Captures in managed mode disclose Ethernet data

Managed Mode vs Monitor Mode

Managed mode capture

```
> tshark -np -i 4
Capturing on Intel(R) PRO/Wireless 2915ABG Network Connection
  0.196409 205.188.9.40 -> 10.240.3.197 Oncoming Buddy: thenickde
  0.307958 10.240.3.197 -> 205.188.9.40 prelude > aol [ACK] Seq=1 Ack=133
Win=65083 Len=0
  2.336869 10.240.3.197 -> 205.188.13.24 AIM SST, Download Buddy Icon Request
  3.850285 00:0b:86:01:87:00 -> ff:ff:ff:ff:ff:ff Who has 10.240.3.27?  Tell
10.240.3.1
```

Monitor mode (RFMON) capture

```
> tshark -n -i 2
Capturing on AirPcap N Wireless Capture Device
  0.001234 00:0b:86:d5:e4:02 -> ff:ff:ff:ff:ff:ff Beacon frame, SN=1297, FN=0,
Flags=........, BI=100, SSID="ethersphere-voip"
  1.077842 00:19:7e:b4:fb:47 -> ff:ff:ff:ff:ff:ff Data, SN=1321, FN=0,
Flags=.p....F.
  6.522158 00:13:ce:55:98:ef -> ff:ff:ff:ff:ff:ff Probe Request, SN=350, FN=0,
Flags=........, SSID=Broadcast[Malformed Packet]
  6.522176                   -> 00:14:bf:0f:03:32 (RA) Acknowledgement, Flags=.......
```

RFMON Implementation

Capture mode driven by drivers

Most Linux wireless drivers support RFMON

- "Yay open source software!"

Windows drivers do not support RFMON

- "What, you want to use it for something other than what we intended?"

Airpcap From CACE Technologies

Listens on one channel at a time

- May collect from other nearby channels

Linux – Setting RFMON Mode (1)

iwconfig - configure wireless parameters

ifconfig - configure an IP address, up/down

Use for Centrino, HostAP, RealTek, RTL, Prism54 and MADWIFI-old drivers

```
wardrive@~:# iwconfig wlan0 mode monitor channel 1
wardrive@~:# iwconfig wlan0 | grep Mode
          Mode:Monitor  Frequency:2.412GHz  Access Point:
00:00:00:00:00:00
wardrive@~:# ifconfig wlan0 | grep HWaddr
wlan0     Link encap:UNSPEC  HWaddr 00-30-F1-0E-51-1F-00-00-00-
00-00-00-00-00-00-00
```

Linux – Setting RFMON Mode (2)

MADWIFI-NG cards use “wlanconfig” to create/destroy

Uses parent/child reference with wifi0 (parent) and arbitrarily named children (often athX)

Monitor mode only allowed when no other interfaces exist

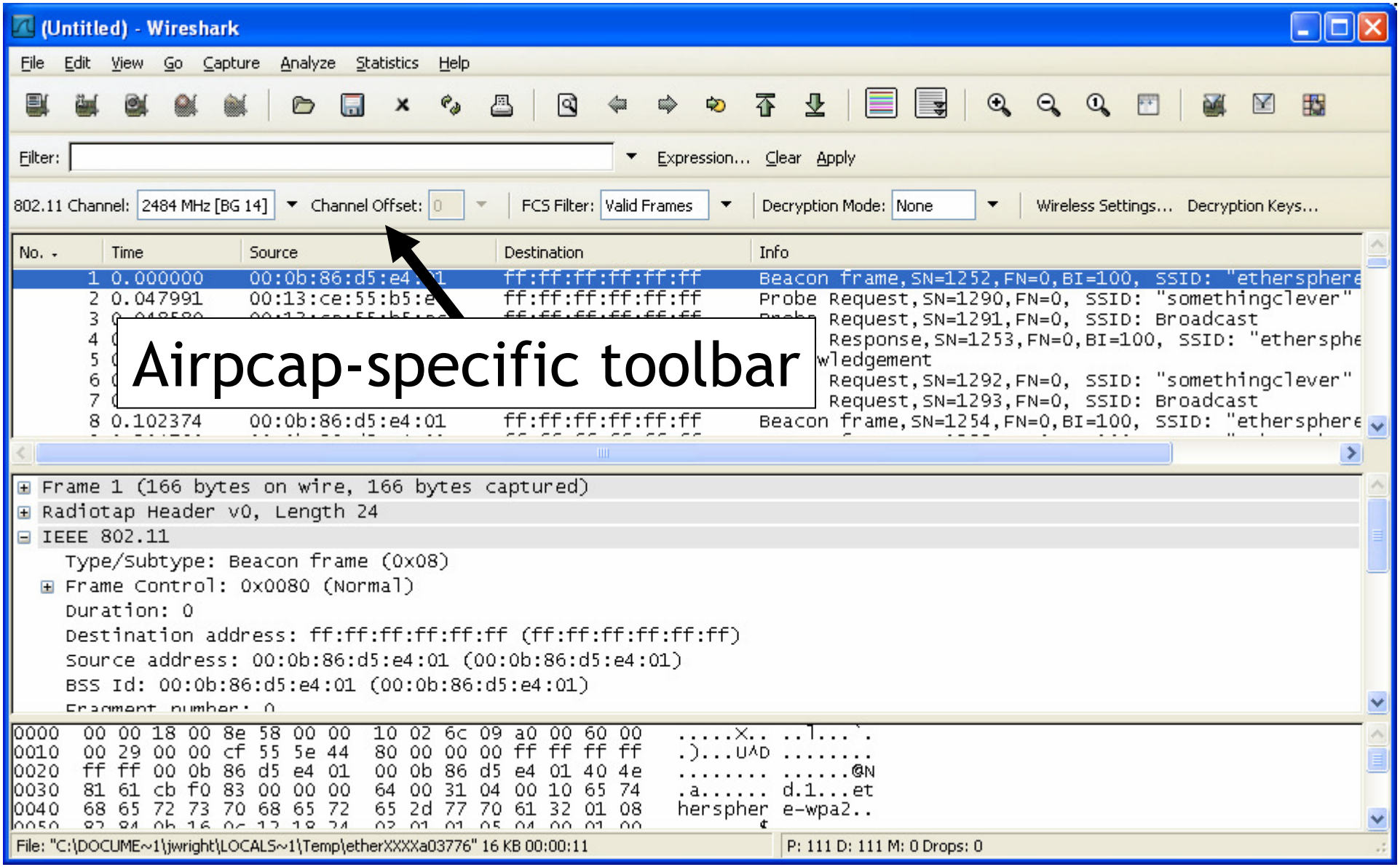
- Must "destroy" all child interfaces first

```
wardrive@~:# wlanconfig ath0 destroy
wardrive@~:# wlanconfig ath0 create wlandev wifi0 wlanmode
monitor
ath0
wardrive@~:# ifconfig ath0 up
wardrive@~:# iwconfig ath0 | grep Mode
        Mode:monitor     Frequency:2.412 GHz     Access Point:
00:00:00:00:00:00
```

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

Airpcap Integration



Leveraging Display Filters

Mastering display filters is the first step in becoming a Wireshark Power User

- Much of the functionality leverages display filters

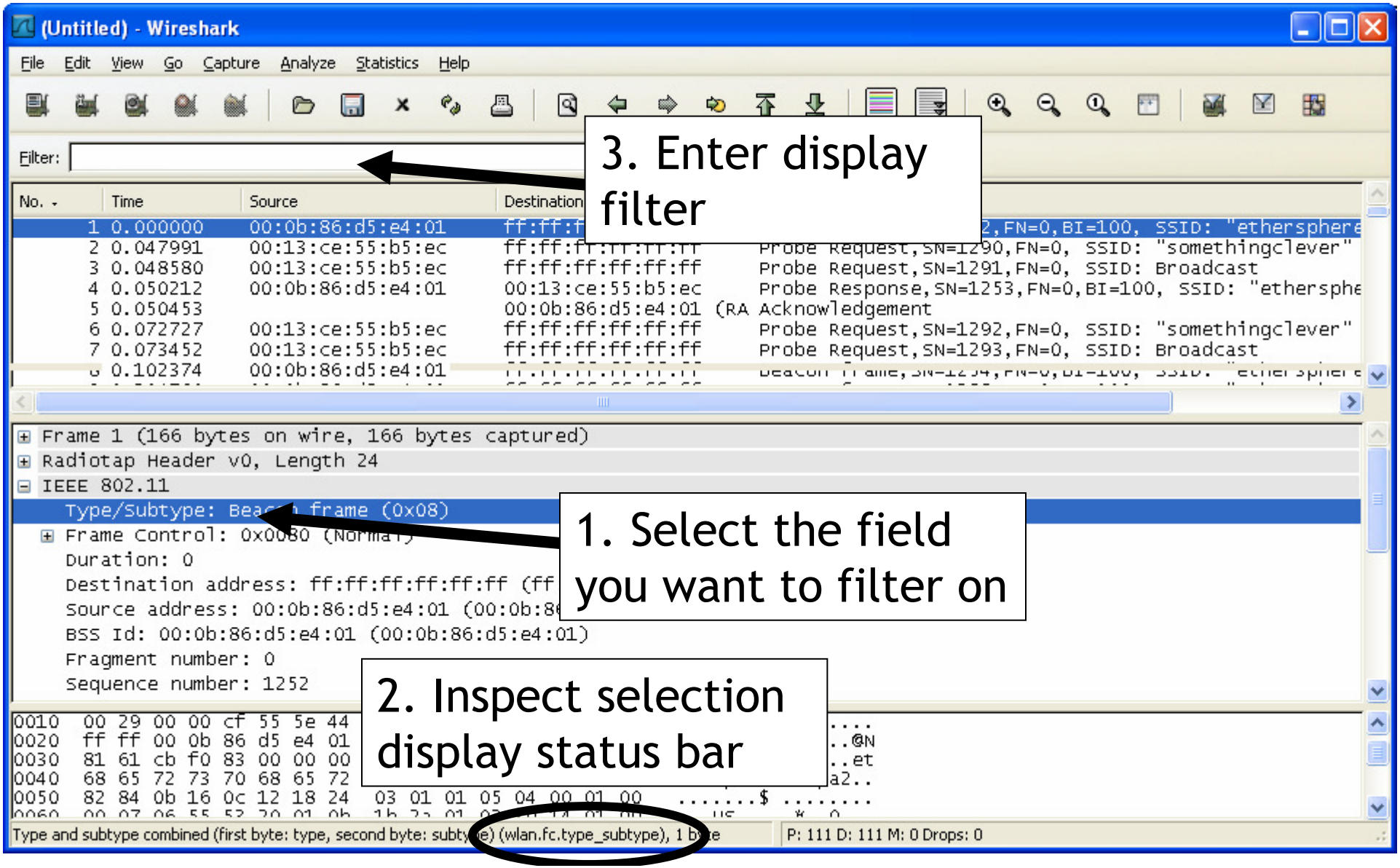
Concept: Use the value of any dissected field to show/hide frames

- Combine field analysis with Boolean operators

Often used to reduce the number of frames listed in the Packet List view

display.field.name operator value

3-Steps for Display Filters



Display Filter Operators

display.field.name *operator* value

- eq, == Equal
- ne, != Not equal
- gt, > Greater than
- lt, < Less Than
- ge, >= Greater than or Equal to
- le, <= Less than or Equal to
- contains, Contains specified data

Combine with and/or, negate with NOT, !

Can use parenthesis to control order for complex filters

Display Filter Example

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: wlan.fc.type_subtype ne 8 and wlan.fc.type ne 1 Expression... Clear Apply

No.	Time	Source	Destination	Info
2	0.047991	00:13:ce:55:b5:ec	ff:ff:ff:ff:ff:ff	Probe Request,SN=1290,FN=0, SSID: "somethingclever"
3	0.048580	00:13:ce:55:b5:ec	ff:ff:ff:ff:ff:ff	Probe Request,SN=1291,FN=0, SSID: Broadcast
4	0.050212	00:0b:86:d5:e4:01	00:13:ce:55:b5:ec	Probe Response,SN=1253,FN=0,BI=100, SSID: "ethersphe
6	0.072727	00:13:ce:55:b5:ec	ff:ff:ff:ff:ff:ff	Probe Request,SN=1292,FN=0, SSID: "somethingclever"
7	0.073452	00:13:ce:55:b5:ec	ff:ff:ff:ff:ff:ff	Probe Request,SN=1293,FN=0, SSID: Broadcast
19	1.144627	00:13:ce:55:b5:ec	ff:ff:ff:ff:ff:ff	Probe Request,SN=1321,FN=0, SSID: Broadcast
20	1.146116	00:0b:86:d5:e4:01	00:13:ce:55:b5:ec	Probe Response,SN=1265,FN=0,BI=100, SSID: "ethersphe
22	1.168243	00:13:ce:55:b5:ec	ff:ff:ff:ff:ff:ff	Probe Request,SN=1322,FN=0, SSID: Broadcast

Don't show me beacons or control frames:
"wlan.fc.type_subtype ne 8 and wlan.fc.type ne 1"

```
⊞ Frame 4 (160
⊞ Radiotap Head
⊟ IEEE 802.11
    Type/Subtype: Probe Response (0x05)
  ⊟ Frame Control: 0x0050 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 5
    ⊞ Flags: 0x0
    Duration: 314
    Destination address: 00:13:ce:55:b5:ec (00:13:ce:55:b5:ec)
```

```
0000  00 00 18 00 8e 58 00 00  10 02 6c 09 a0 00 5c 00   .....X.. ..l...\.
0010  00 29 00 00 fc 47 bb 71  50 00 3a 01 00 13 ce 55   .)...G.q P.:....U
0020  b5 ec 00 0b 86 d5 e4 01  00 0b 86 d5 e4 01 50 4e   ........ ......PN
0030  e3 25 cc f0 83 00 00 00  64 00 31 04 00 10 65 74   .%...... d.1...et
0040  68 65 72 73 70 68 65 72  65 2d 77 70 61 32 01 08   hersphe r e-wpa2..
```

File: "C:\DOCUME~1\jwright\LOCALS~1\Temp\etherXXXXa03776" 16 KB 00:00:11 P: 111 D: 36 M: 0 Drops: 0

Customizing the Display: Columns

Libpcap captures with PrismAVS or Radiotap headers identify RSSI, rate information

AiroPeek NX show RSSI percentage, rate

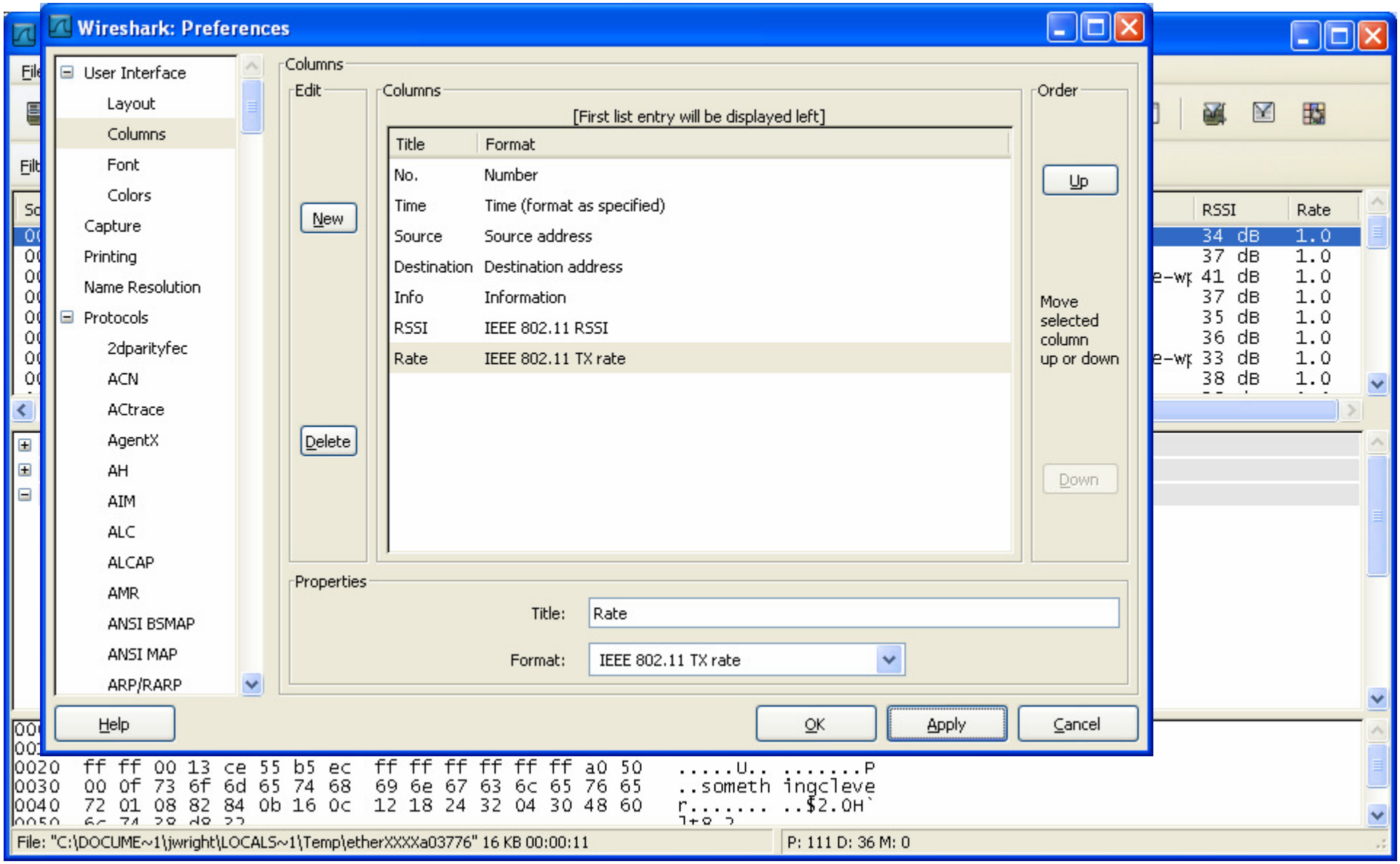
Can add columns to display

Edit → Preferences → Columns

- New, name column, select format "IEEE 802.11 TX Rate"
- Repeat for "IEEE 802.11 RSSI"

Wireshark >=0.99.6, no need to restart for column changes to take effect

Wireshark Column Preferences



Coloring the Display

Can change the packet list display colors depending on frame characteristics

- Identify the characteristics with display filters

A few colored lines can make analysis of a large capture much easier, faster

Click View → Coloring Rules

- Name the view, enter the display filter, select foreground and background colors

Can save custom rules to a file, apply when desired

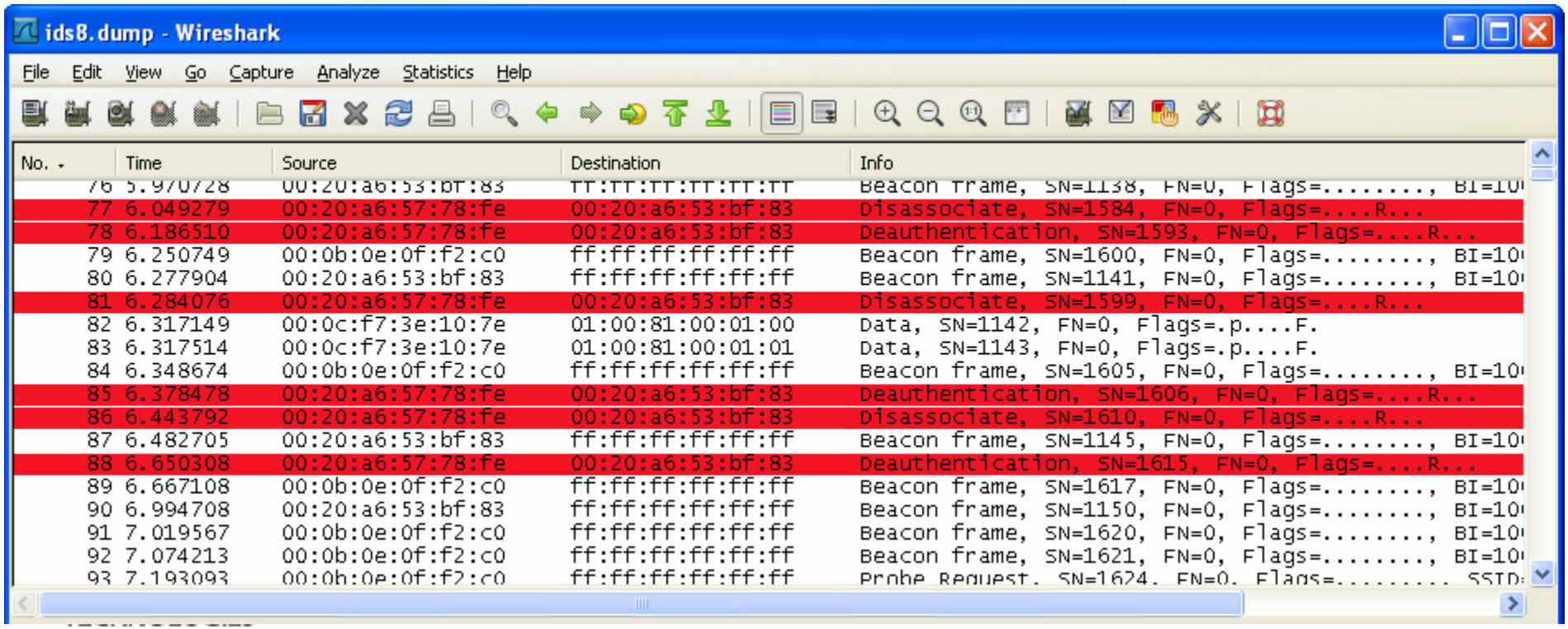
Most-specific frames should be ordered first

Disconnect Frames

"wlan.fc.type_subtype eq 12 or wlan.fc.type_subtype eq 10"

Legitimate part of 802.11, can be used for DoS attacks

Useful identifier for starting analysis

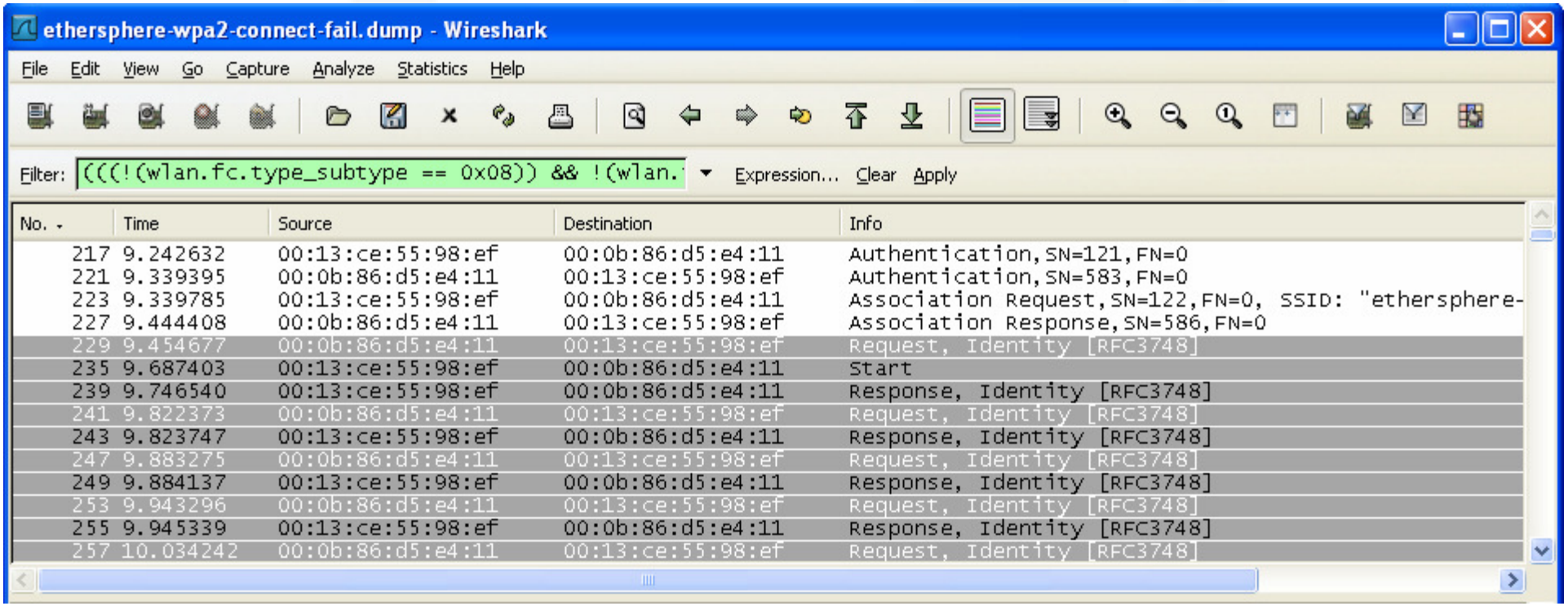


Identifying From DS and To DS traffic

"wlan.fc.fromds eq 1 and wlan.fc.tods eq 0"

"wlan.fc.fromds eq 0 and wlan.fc.tods eq 1"

Useful to identify transmissions from AP or STA
Helpful in identifying transmit power level problems



No.	Time	Source	Destination	Info
217	9.242632	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Authentication, SN=121, FN=0
221	9.339395	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Authentication, SN=583, FN=0
223	9.339785	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Association Request, SN=122, FN=0, SSID: "ethersphere-
227	9.444408	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Association Response, SN=586, FN=0
229	9.454677	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
235	9.687403	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Start
239	9.746540	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
241	9.822373	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
243	9.823747	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
247	9.883275	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
249	9.884137	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
253	9.943296	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
255	9.945339	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
257	10.034242	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]

Other Ideas for Colorizing Packets

Identify traffic from your AP provider (or inverse)

- (wlan.addr[0:3] eq 00:0b:86 or wlan.bssid[0:3] eq 00:0b:86)

Identify packets that are retries

- "wlan.fc.retry eq 1"

Identify packets with weak signal

- Capture-specific, depending on how RSSI is represented
- AiroPeek NX: "wlan.signal_strength < 20"

Identify frames with a bad FCS

- "wlan.fcs_bad eq 1"
- White-on-white makes them easy to ignore, but can view by selecting the frame

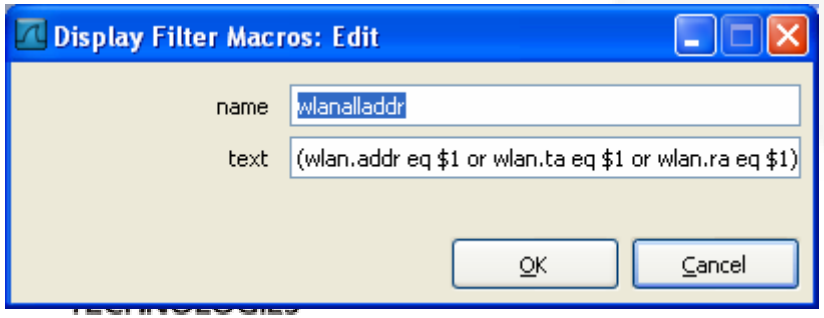
Display Macros for WiFi Addresses

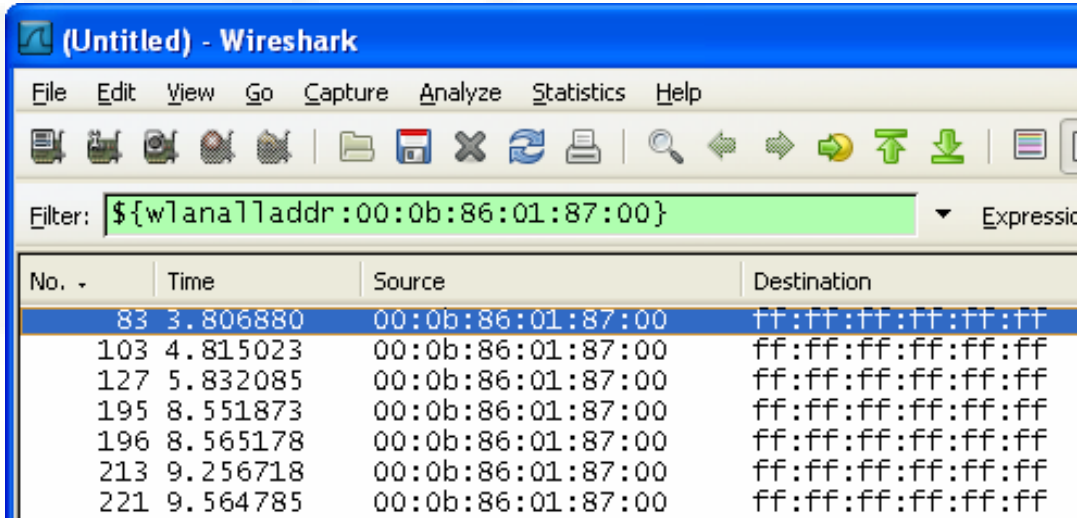
Macros introduced to simplify the use of complex display filters

802.11 uses multiple address fields: Source, Destination, Transmitter, Receiver, BSSID

"wlan.addr" only covers source and destination

Macro: wlanalladdr "(wlan.addr eq $1 or wlan.bssid eq $1 or wlan.ta eq $1 or wlan.ra eq $1)"





Searching for Anomalies

"The wireless network sucks"

- "I can't connect"
- "I get dropped"
- "My performance sucks"

Having a packet capture from the wireless side can be very revealing for troubleshooting

Intermittent problems can be tough to capture

Enter "tshark"

- Monitoring laptop near user with a problem
- When the user experiences the drop, they hit "CTRL+C" to stop a capture

Limiting Capture Size: Dumpcap

Command-line tool included with Wireshark

Does not decode packets, much faster capture

Can capture traffic to multiple files, overwriting older files after a specified capture size or time

- Limits the amount of data an analyst has to look through

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\jwright>dumpcap -i \\.\airpcap00 -b filesize:500 -b du
ration:120 -b files:5 -w troubleshooting
File: troubleshooting_00001_20070824111448
Packets: 1439 File: troubleshooting_00002_20070824111505
Packets: 2849 File: troubleshooting_00003_20070824111521
Packets: 4177 File: troubleshooting_00004_20070824111536
Packets: 5578 File: troubleshooting_00005_20070824111552
Packets: 6938 File: troubleshooting_00006_20070824111607
Packets: 8357 File: troubleshooting_00007_20070824111623
Packets: 9679 File: troubleshooting_00008_20070824111638
Packets: 11014 File: troubleshooting_00009_20070824111654
Packets: 12362 File: troubleshooting_00010_20070824111709
```

Assessing Captures - Unable to Connect

Apply an "exclusive filter"

- Keep adding exclusion criteria to the display filter until you get to a smaller number of frames that can be inspected manually

Skip to deauth frames - often immediately follow suspicious activity

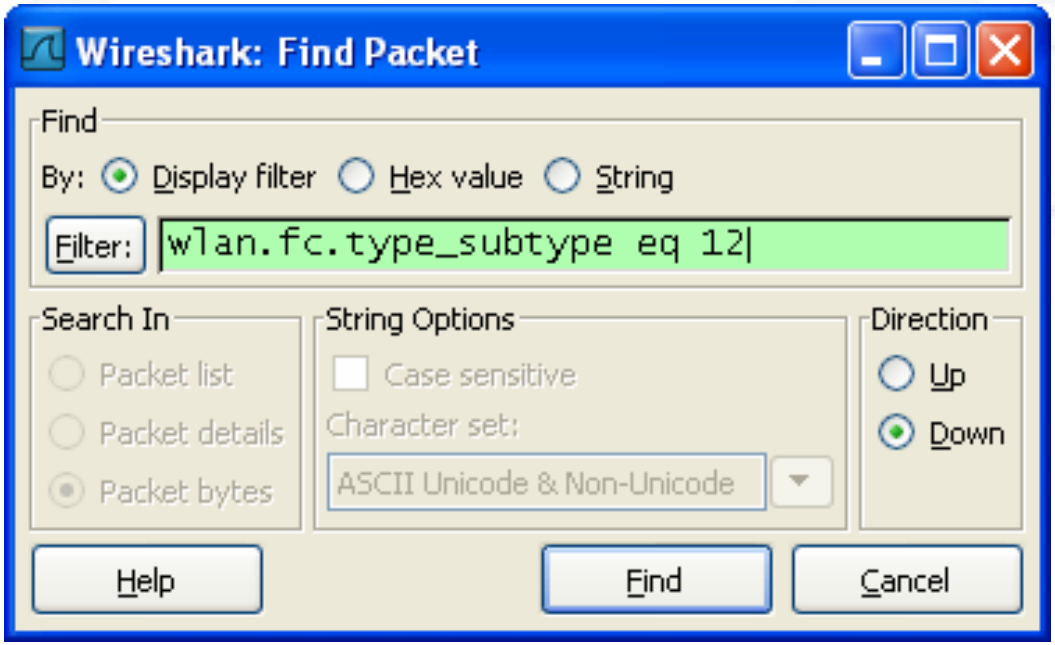
Skip to authenticate request frame - inspect exchange that follows

Finding Packets

Click Edit → Find Packet (or "CTRL+F")

Enter the desired conditions in the filter

- Search for a string or hex value or match a given display filter value
- Can limit search to list, detail or bytes views

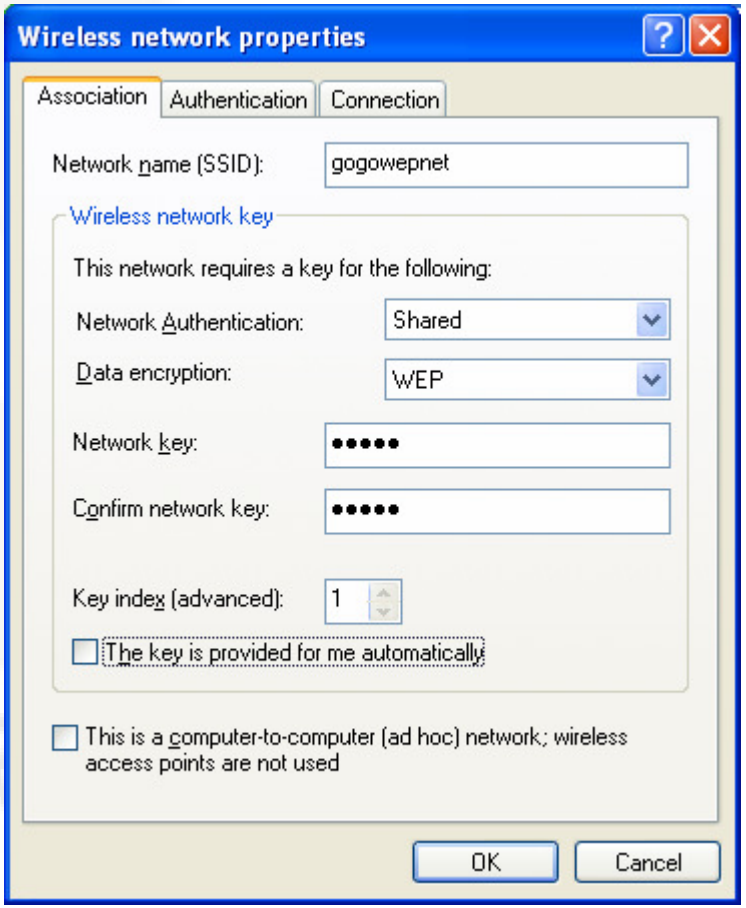


Practical Example - wlan1.pcap

Client is unable to connect to a legacy WEP network

You shouldn't run WEP, but this isn't a wireless security session

Confirmed WEP key entry, WZC wireless stack on XP SP2



CACE TECHNOLOGIES

Analysis steps for wlan1.pcap

1. Reduce frames displayed by filtering out beacons and control frames
   - "wlan.fc.type_subtype ne 8 and wlan.fc.type ne 1"
2. Walk through client connection steps:
   - Probe request, probe response
   - Authentication request, authentication response
   - Association request, association response

Frames 76 and 77 indicate client is not completing the authentication exchange. Status code in authentication response (from AP) supplies additional information.

AP rejects client - Unsupported authentication algorithm

wlan1.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: wlan.fc.type_subtype ne 8 and wlan.fc.type ne 1 | Expression... Clear Apply

No.	Time	Source	Destination	Info
61	5.151268	00:13:ce:55:98:ef	ff:ff:ff:ff:ff:ff	Probe Request, SN=73, FN=0, Flags=....., SSID=Bl
70	5.787219	00:13:ce:55:98:ef	ff:ff:ff:ff:ff:ff	Probe Request, SN=93, FN=0, Flags=....., SSID="(
71	5.788196	00:0b:86:c2:a4:82	00:13:ce:55:98:ef	Probe Response, SN=3117, FN=0, Flags=....., BI=1
74	5.837938	00:13:ce:55:98:ef	00:0b:86:c2:a4:82	Authentication, SN=94, FN=0, Flags=.....
76	5.838939	00:0b:86:c2:a4:82	00:13:ce:55:98:ef	Authentication, SN=3121, FN=0, Flags=.....
77	5.839470	00:0b:86:c2:a4:82	00:13:ce:55:98:ef	Authentication, SN=3121, FN=0, Flags=....R...
79	5.859692	00:13:ce:55:98:ef	ff:ff:ff:ff:ff:ff	Probe Request, SN=95, FN=0, Flags=....., SSID="(
80	5.860633	00:0b:86:c2:a4:82	00:13:ce:55:98:ef	Probe Response, SN=3122, FN=0, Flags=....., BI=1
82	5.910180	00:13:ce:55:98:ef	00:0b:86:c2:a4:82	Authentication, SN=96, FN=0, Flags=.....
84	5.911176	00:0b:86:c2:a4:82	00:13:ce:55:98:ef	Authentication, SN=3123, FN=0, Flags=.....

```
    Duration: 314
    Destination address: 00:13:ce:55:98:ef (00:13:ce:55:98:ef)
    Source address: 00:0b:86:c2:a4:82 (00:0b:86:c2:a4:82)
    BSS Id: 00:0b:86:c2:a4:82 (00:0b:86:c2:a4:82)
    Fragment number: 0
    Sequence number: 3121
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (6 bytes)
      Authentication Algorithm: Shared key (1)
      Authentication SEQ: 0x0002
      Status code: Responding station does not support the specified authentication algorithm (0x000d)
```

```
0070  00 00 04 00 02 00 00 00  44 00 09 00 00 00 04 00   ........ D.......
0080  00 00 00 00 44 00 0a 00  00 00 04 00 92 ff ff ff   ....D... ........
0090  b0 08 3a 01 00 13 ce 55  98 ef 00 0b 86 c2 a4 82   ..:....U ........
00a0  00 0b 86 c2 a4 82 10 c3  01 00 02 00 0d 00         ........ ......
```

Status of requested event (wlan_mgt.fixed.status_code), 2 bytes | Packets: 600 Displayed: 191 Marked: 0

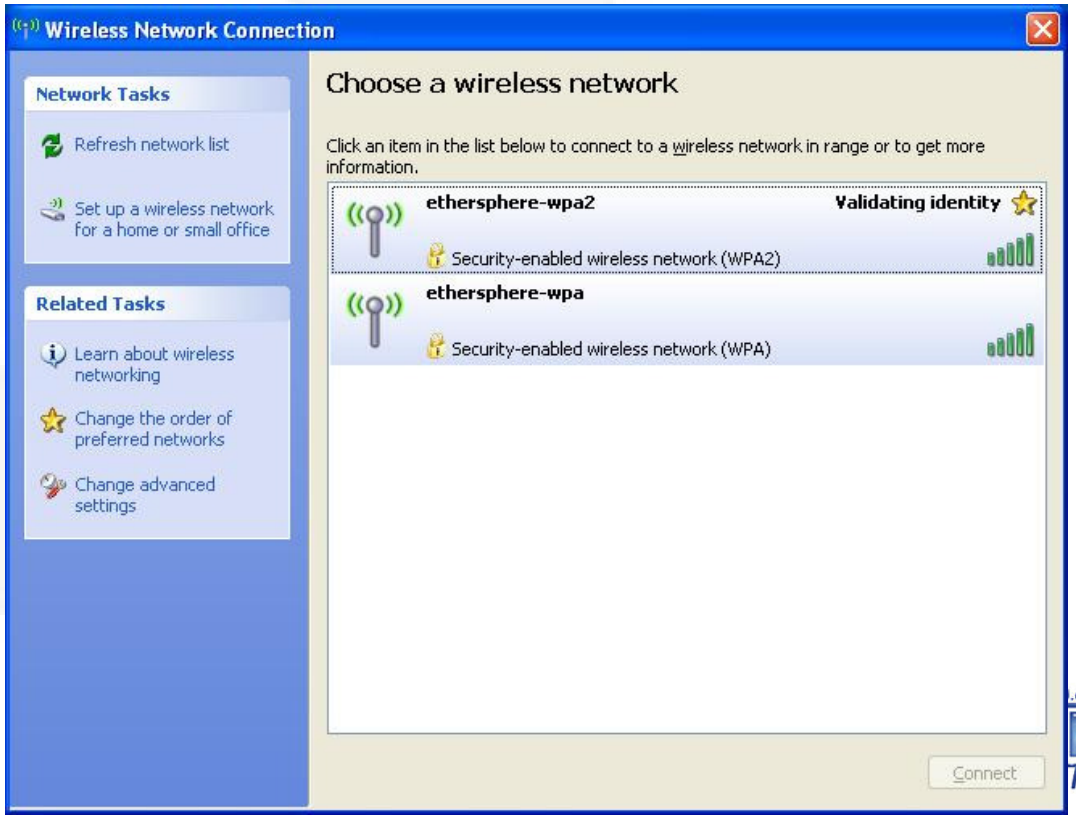
Practical Example - wlan2.pcap

Morning of Friday June 15th 2007 (EDT)

Windows XP SP2 using WZC

"Connecting" logo on the network adapter icon

Further inspection reveals WZC is attempting to validate identity information for my account



Troubleshooting - wlan2.cap

wlan2.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: type_subtype == 0x08)) && !(wlan.fc.type == 1)

Exclusive display filter to remove control frames and beacons from display

No.	Time	Source	Destination	Info
196	8.482758	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Deauthentication, SN=101, FN=0, Flags=.....
212	9.210100	00:13:ce:55:98:ef	ff:ff:ff:ff:ff:ff	Probe Request, SN=120, FN=0, Flags=....., SSID="e
213	9.210614	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Probe Response, SN=578, FN=0, Flags=....., BI=10(
217	9.242632	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Authentication, SN=121, FN=0, Flags=.....
221	9.339395	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Authentication, SN=583, FN=0, Flags=.....
223	9.339785	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Association Request, SN=122, FN=0, Flags=....., S
227	9.444408	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Association Response, SN=586, FN=0, Flags=.....
229	9.454677	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
235	9.687403	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Start
239	9.746540	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
241	9.822373	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
243	9.823747	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
247	9.883275	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
249	9.884137	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
253	9.943296	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
255	9.945339	00:13:ce:55:98:ef	00:0b:86:d5:e4:11	Response, Identity [RFC3748]
257	10.034242	00:0b:86:d5:e4:11	00:13:ce:55:98:ef	Request, Identity [RFC3748]
				Response, Identity [RFC3748]
				Request, Identity [RFC3748]
				Response, Identity [RFC3748]
				Request, Identity [RFC3748]

EAP Request/Response, but no PEAP, indicates no response from RADIUS server

```
0020  55 98 ef 00 0b 86 d5 e4  11 00 0b 86 d5 e4 11 50   U....... .......P
0030  25 00 00 aa aa 03 00 00  00 88 8e 01 00 00 05 01   %....... ........
0040  01 00 05 01 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

File: "C:\Documents and Settings\jwright\Desktop\SHARKFEST 2008\Wireshark Wireless ... Packets: 2692 Displayed: 946 Marked: 0

Practical Example - wlan3.pcap

"Josh, Question for you. I've got a local wireless LAN that's having serious performance problems, and I'm looking at some packet captures in an attempt to diagnose the issue(s)."

Station in question is 00:18:f3:92:30:82

Initial analysis by analyst suggested possible DoS attack

Lots of deauthenticate frames observed

Deauth floods are the port scans of the wired IDS world. They are often misrepresented, and can easily make a smart analyst look silly.

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

Filename: Kismet-May-02-2007-3.dump

Uh, oh: capture was taken with Kismet

Kismet is a great analysis tool, uses channel hopping by default

- Captures with channel hopping enabled can be deceptive re: RSSI, retries, lost frames

Inspect beacons over time to determine if channel hopping was enabled or not

Evaluating Channel Hopping

wlan3.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Show only beacons

Filter: wlan.fc.type_subtype eq 8 Expression... Clear Apply

No.	Time	Source	Destination	Info
16703	247.123536	00:0c:f1:5c:11:8b	ff:ff:ff:ff:ff:ff	Beacon frame, SN=2156, FN=0, Flags=....., BI=100,
16704	247.130102	00:0a:f4:e2:3b:c9	ff:ff:ff:ff:ff:ff	Beacon frame, SN=781, FN=0, Flags=....., BI=100,
16705	247.144175	00:0f:f8:58:6b:26	ff:ff:ff:ff:ff:ff	Beacon frame, SN=1923, FN=0, Flags=....., BI=100,
16706	247.157184	00:16:6f:03:86:36	ff:ff:ff:ff:ff:ff	Beacon frame, SN=60, FN=0, Flags=....., BI=100,
16707	247.200360	00:18:f8:c6:9c:fc	ff:ff:ff:ff:	
16708	247.224985	00:20:a6:56:83:6e	ff:ff:ff:ff:	
16709	247.232553	00:0a:f4:e2:3b:c9	ff:ff:ff:ff:	
16710	247.259837	00:16:6f:03:86:36	ff:ff:ff:ff:	
16711	247.302740	00:18:f8:c6:9c:fc	ff:ff:ff:ff:	

Spot-check several frames over 10 seconds for DS Set value

```
⊞ Frame 16707 (99 bytes on wire, 99 bytes captured)
⊞ IEEE 802.11 Beacon frame, Flags: .....
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (63 bytes)
    ⊞ SSID parameter set: "Moto FE lab Schaumburg"
    ⊞ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 18.0 24.0 36.0 54.0
    ⊞ DS Parameter set: Current Channel: 11
    ⊞ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    ⊞ ERP Information: Non-ERP STAs, do not use protection, long preambles
    ⊞ ERP Information: Non-ERP STAs, do not use protection, long preambles

0000  80 00 00 00 ff ff ff ff  ff ff 00 18 f8 c6 9c fc   ........ ........
0010  00 18 f8 c6 9c fc 90 99  94 01 50 a3 29 01 00 00   ........ ..P.)...
0020  64 00 11 00 00 16 4d 6f  74 6f 20 46 45 20 6c 61   d.....Mo to FE la
0030  62 20 53 63 68 61 75 6d  62 75 72 67 01 08 82 84   b Schaum burg....
0040  8b 96 24 30 48 6c 03 01  0b 05 04 00 01 00 00 2a   ..$0Hl.. .......*
```

Kismet was "locked" during capture, no channel hopping

File: "C:\Documents and Settings\jwright\Desktop\SHARKFEST 2008\Wireshark Wireless ... Packets: 73333 Displayed: 42984 Marked: 0

Client Traffic Analysis

wlan3.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: wlan.addr eq 00:18:f3:92:30:82 or wlan.fc.type Expression... Clear Apply

No.	Time	Source	Destination	Info
14527	216.299904	00:18:f3:92:30:82	ff:ff:ff:ff:ff:ff	Probe Request, SN=69, FN=0, Flags=....., SSID= WA
14528	216.300557	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Probe Response, SN=332, FN=0, Flags=....., BI=10(
14530	216.331542	00:18:f3:92:30:82	00:0a:f4:e2:3b:c9	Authentication, SN=70, FN=0, Flags=.....
14531	216.331680		00:18:f3:92:30:82	(RA Acknowledgement, Flags=.....
14532	216.332775	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Authentication, SN=334, FN=0, Flags=.....
14533	216.334065	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Authentication, SN=334, FN=0, Flags=....R...
14534	216.336426	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Authentication, SN=334, FN=0, Flags=....R...
14536	216.338152	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Authentication, SN=334, FN=0, Flags=....R...
14537	216.338375		00:0a:f4:e2:3b:c9	(RA Acknowledgement, Flags=.....
14539	216.394512	00:18:f3:92:30:82	00:0a:f4:e2:3b:c9	Reassociation Request, SN=71, FN=0, Flags=.....,
14540	216.394635		00:18:f3:92:30:82	(RA Acknowledgement, Flags=.....
14541	216.398772	00:18:f3:92:30:82	00:0a:f4:e2:3b:c9	Reassociation Request, SN=71, FN=0, Flags=....R...,
14542	216.404548	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=.....
14544	216.407245	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14545	216.408449	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14546	216.409829	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14547	216.411454	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14549	216.413267	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14550	216.414642	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14551	216.415885	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14552	216.417591	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14553	216.418844	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14554	216.420543	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14555	216.422015	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14556	216.423659	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14557	216.425316	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14558	216.426549	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14559	216.427880	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Reassociation Response, SN=335, FN=0, Flags=....R...
14560	216.432043	00:0a:f4:e2:3b:c9	00:18:f3:92:30:82	Deauthentication, SN=337, FN=0, Flags=.....

File: "C:\Documents and Settings\jwright\Desktop\SHARKFEST 2008\Wireshark Wireless ... Packets: 73333 Displayed: 13297 Marked: 0

PHY Data Not Available

PHY-layer information is not available in the capture

We can use retry information to detect interference

Manual calculation technique:

- Apply a display filter for retries
- Calculate statistics manually using frame count and display filters
- "wlan.fc.retry eq 0 and wlan.addr eq 00:18:f3:92:30:82", "wlan.fc.retry eq 1 and wlan.addr eq 00:18:f3:92:30:82"

retry eq 0

P: 73333 D: 1983 M: 0

retry eq 1

P: 73333 D: 1586 M: 0

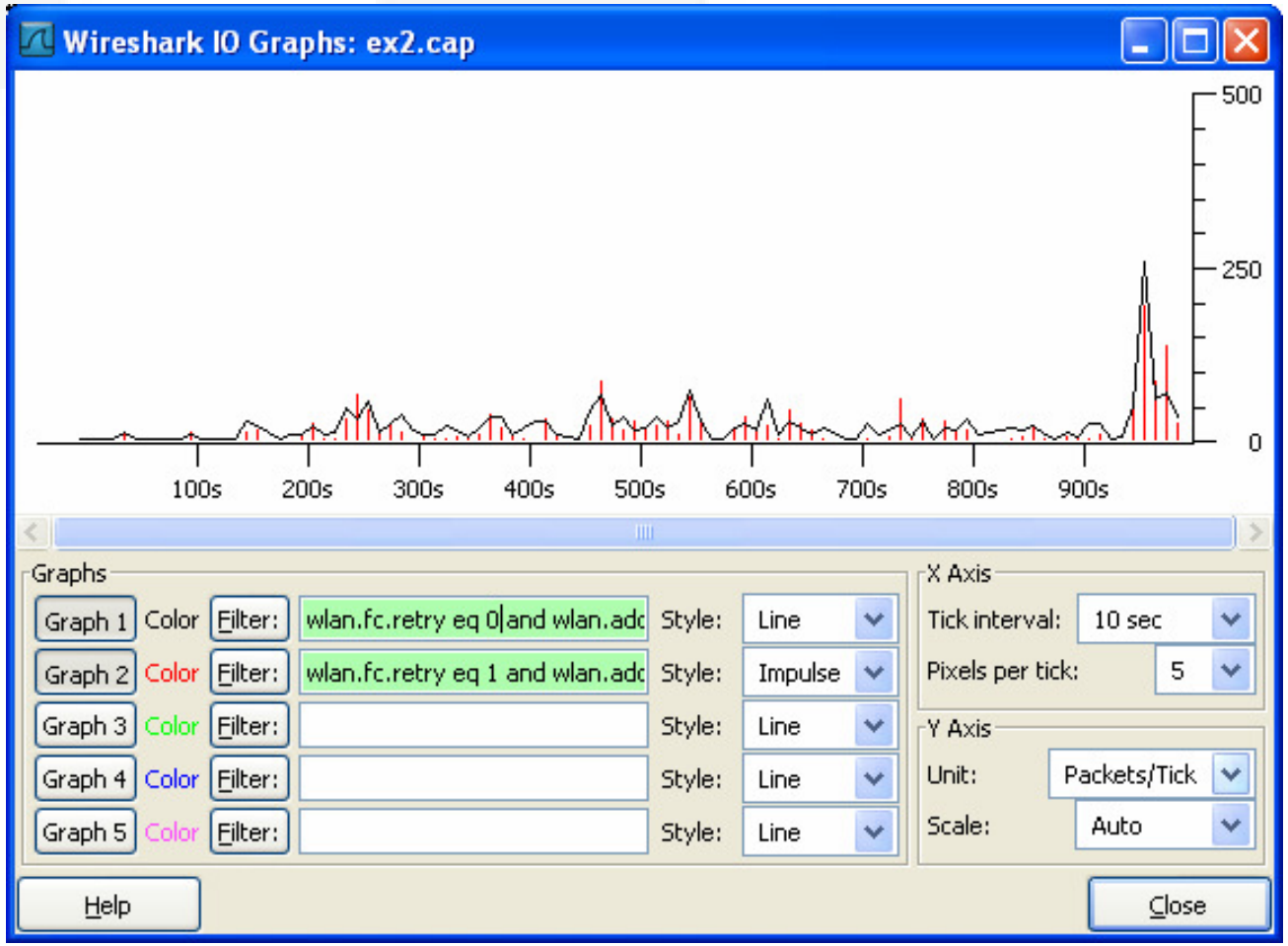
IO Graphing for Retry Statistics

Click Statistics → IO Graphs

Apply one or more display filters

Can change X and Y axis size and scale

Style can be line, impulse, solid



CACE TECHNOLOGIES

Attack Analysis: wlan4.pcap

wlan4.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Info
63	11.053869			Unrecognized (Reserved frame), Flags=.pm..M..
64	11.058502	00:07:0e:b9:74:bb	ff:ff:ff:ff:ff:ff	Beacon frame, SN=221, FN=0, Flags=....., BI=100,
65	11.074068	00:07:0e:b9:74:bb	00:07:0e:b9:74:bb	Data, SN=4039, FN=0, Flags=.pmP...T
66	11.074260		00:07:0e:b9:74:bb (RA	Acknowledgement, Flags=.....
67	11.093401	00:07:0e:b9:74:bb	00:20:a6:4c:d9:4a	Reassociation Request, SN=4040, FN=0, Flags=..mP....
68	11.093617		00:07:0e:b9:74:bb (RA	Acknowledgement, Flags=.....
69	11.113204	00:07:0e:b9:74:bb	00:20:a6:4c:d9:4a	Data, SN=4041, FN=0, Flags=.pm.....
70	11.113397		00:07:0e:b9:74:bb (RA	Acknowledgement, Flags=.....
71	11.135721	00:07:0e:b9:74:bb	00:20:a6:4c:d9:4a	Beacon frame, SN=4042, FN=0, Flags=opmP.M..
72	11.135907		00:07:0e:b9:74:bb (RA	Acknowledgement, Flags=.....
73	11.155358			Unrecognized (Reserved frame), Flags=..m..M..
74	11.160888	00:07:0e:b9:74:bb	ff:ff:ff:ff:ff:ff	Beacon frame, SN=222, FN=0, Flags=....., BI=100,
75	11.175267	00:07:0e:b9:74:bb (BS	00:20:a6	[illegible]
76	11.194623	f5:22:ba:76:0a:99 (TA	00:00:00	[illegible]
77	11.213270		00:20:a6	[illegible]

Quick glance discloses "malformed packets" in the capture

```
⊞ Frame 67 (303 bytes on wire, 303 bytes captured)
⊞ Prism Monitoring Header
⊞ IEEE 802.11 Reassociation Request, Flags: ..mP....
⊞ IEEE 802.11 wireless LAN management frame
  [Malformed Packet: IEEE 802.11]
```

```
0000  44 00 00 00 90 00 00 00  61 74 68 30 00 00 00 00   D....... ath0....
0010  00 00 00 00 00 00 00 00  44 00 01 00 00 00 04 00   ........ D.......
0020  43 b2 39 00 44 00 02 00  00 00 04 00 a8 9f 17 b8   C.9.D... ........
0030  44 00 03 00 00 00 04 00  0b 00 00 00 44 00 04 00   D....... ....D...
0040  00 00 04 00 33 00 00 00  00 00 00 00 00 00 00 00   ....3... ........
0050  00 00 00 00 44 00 06 00  00 00 04 00 d4 ff ff ff   ....D...
```

File: "C:\Documents and Settings\jwright\Desktop\SHARKFEST 2008\Wireshark Wireless ... | Packets: 13744 Displayed: 13744 Marked: 0

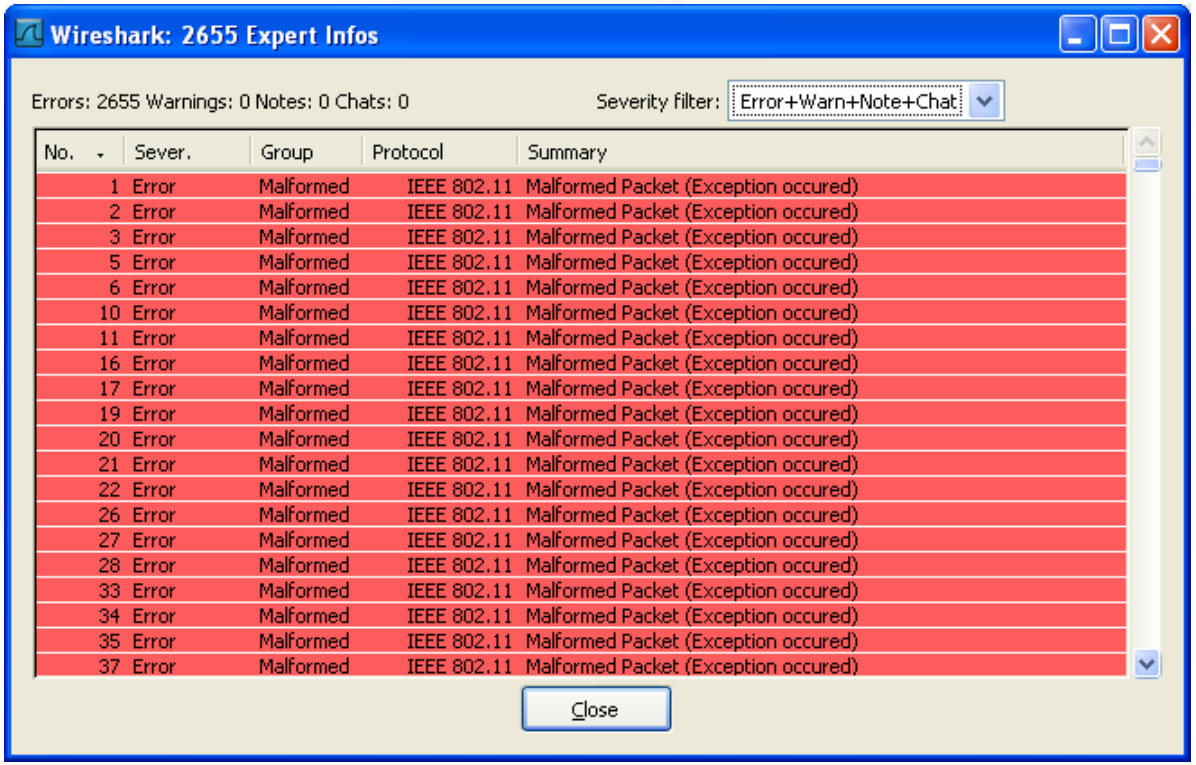
Wireshark Expert Analysis

Wireshark can automatically analyze traffic and identify errors, warnings and other areas of concern

- Analyze → Expert Info

Mike Kershaw is enhancing expert analysis information

Clicking on the warning selects the frame



CACE TECHNOLOGIES

Identifying Conversations

Useful to identify the top-talkers

Statistics → Conversations

Conversations: wlan4.pcap

Ethernet | Fibre Channel | FDDI | IPv4: 3 | IPX: 4 | JXTA | SCTP | TCP | Token Ring | UDP | USB | WLAN: 12 | NCP | RSVP

WLAN Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
00:0f:b5:eb:dc:c0	00:20:a6:4c:d9:4a	1	226	1	226	0	0	45.470898000	0.0000	N/A	N/A
00:14:a4:2a:9e:58	ff:ff:ff:ff:ff:ff	1	198	1	198	0	0	72.682627000	0.0000	N/A	N/A
00:0a:95:f3:2f:ab	ff:ff:ff:ff:ff:ff	3	597	3	597	0	0	38.275889000	50.5179	94.54	N/A
00:07:0e:b9:74:bb	00:14:a4:2a:9e:58	4	1056	4	1056	0	0	73.000259000	126.0679	67.01	N/A
00:20:a6:4c:d9:4a	ff:ff:ff:ff:ff:ff	5	950	5	950	0	0	19.915884000	35.4595	214.33	N/A
00:07:0e:b9:74:bb	00:0d:29:02:44:b8	6	1308	3	792	3	516	56.928882000	126.0545	50.26	32.75
00:0f:b5:eb:dc:c0	ff:ff:ff:ff:ff:ff	13	3016	13	3016	0	0	0.269241000	187.8937	128.41	N/A
00:20:a6:4c:d9:4a	00:40:96:45:91:0c	29	6850	9	2160	20	4690	0.446028000	68.9291	250.69	544.33
00:07:0e:b9:74:bb	ff:ff:ff:ff:ff:ff	153	41310	153	41310	0	0	0.716718000	208.5765	1584.45	N/A
00:0d:29:02:44:b8	00:40:96:45:91:0c	402	96480	202	48480	200	48000	0.733607000	209.9893	1846.95	1828.66
00:07:0e:b9:74:bb	00:07:0e:b9:74:bb	1448	1340668	1448	1340668	0	0	10.835110000	199.7194	53702.06	N/A
00:07:0e:b9:74:bb	00:20:a6:4c:d9:4a	4024	3717327	4020	3716490	4	837	10.799536000	199.9364	148706.90	33.49

☑ Name resolution

Help | Copy | Close

Spoofed Frames?

Casual inspection turned up more anomalies

- Lots of frames with the fragment bit set
- Lots of IE anomalies
- Reserved type and subtype combinations

Beginning to suspect spoofed frames

Can apply sequence number analysis techniques to identify anomalies

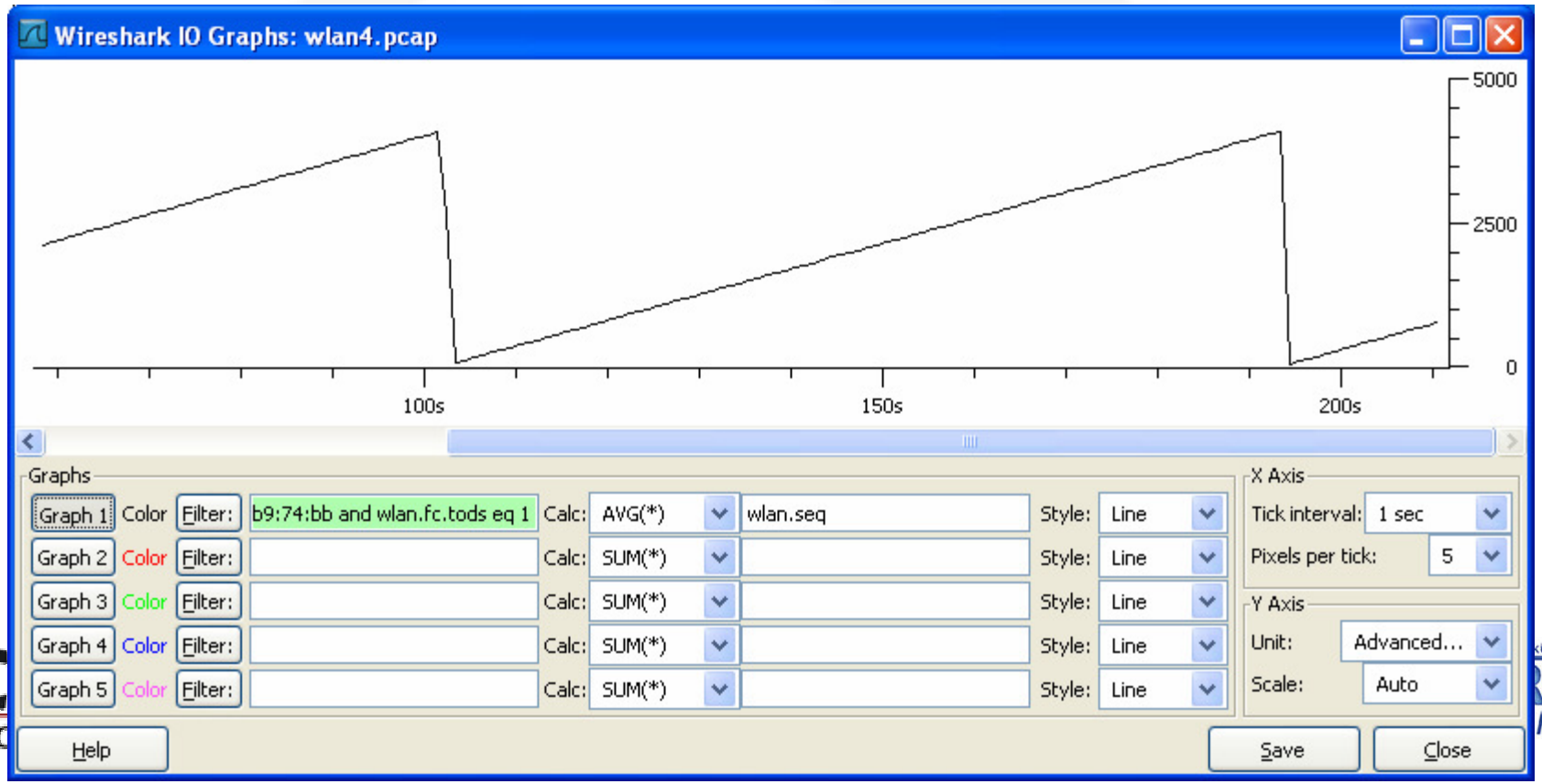
- Using IO Graphs
- When referring to the source address, be sure to differentiate FromDS and ToDS

Normal Sequence Number Graph

Sequence number field is modulo 4096

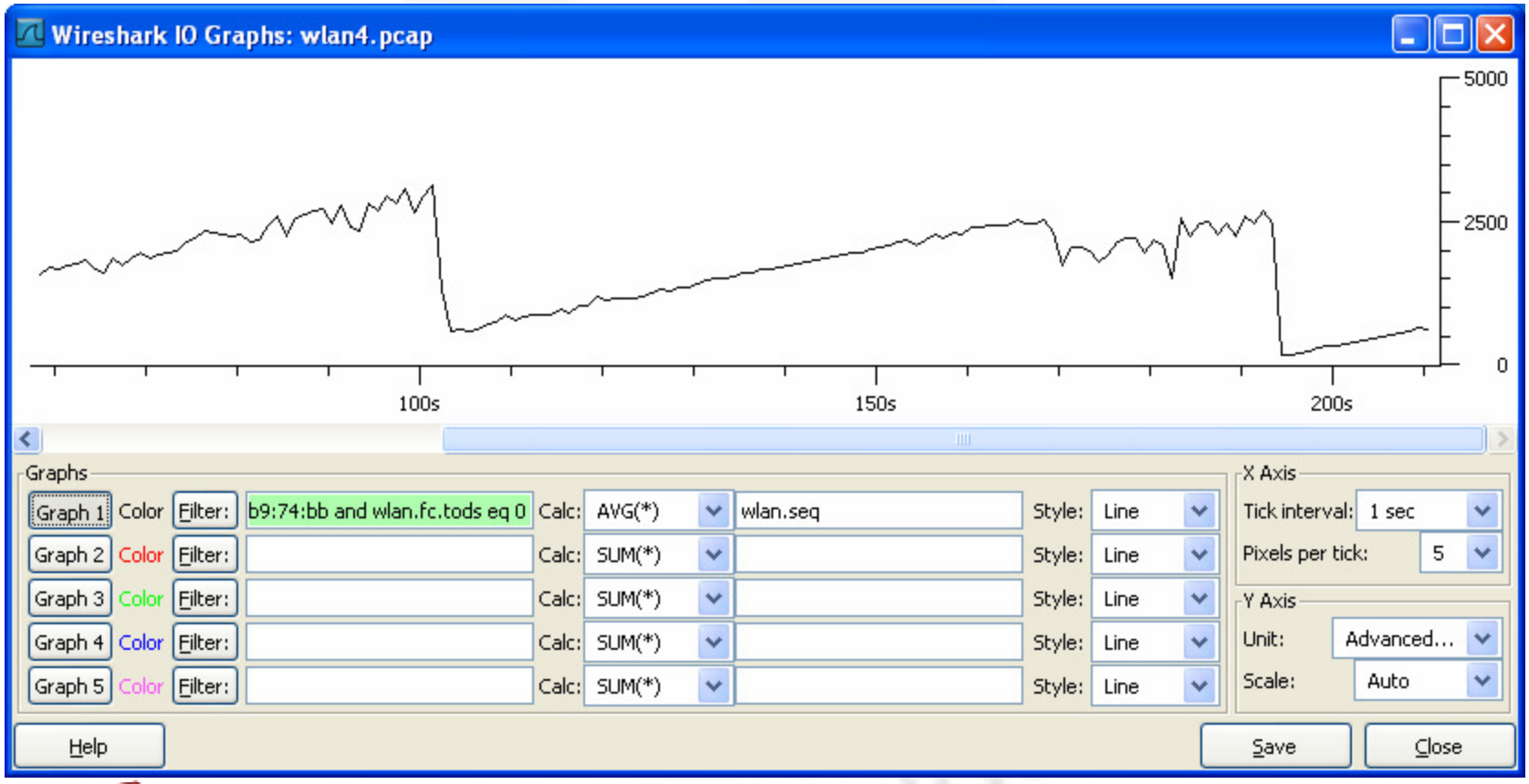
Can graph display filter field values in IO Graphs

- Sum, Count, Max, Min, Avg, Load (time-relative)



Spoofed Frames Sequence Number Graph

Spoofed frames causes average to skew



CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

Extracting Data - wlan5.pcap

Highlighted bytes in the packet bytes view can be saved to a file

Useful for extracting data for additional analysis

- Frame manipulation and retransmission

Select fields to save, File → Export → Selected Packet Bytes

Packet Capture → Certificate DER

wlan5.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: eap

No.	Time	Source	Destination	Info
112	5.681324	00:60:1d:f0:3d:12	00:0f:66:e3:76:3b	Cli
113	5.697017	00:0f:66:e3:76:3b	00:60:1d:f0:3d:12	Ser
115	5.741924	00:60:1d:f0:3d:12	00:0f:66:e3:76:3b	Cli

```
Secure Socket Layer
  TLSv1 Record Layer: Handshake Protocol: Server Hello
  TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 553
    Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 549
      Certificates Length: 546
      Certificates (546 bytes)
        Certificate Length: 543
        Certificate (id-at-organizationName=Internet Widgits
  TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

```
0080  02 29 0b 00 02 25 00 02  22 00 02 1f 30 82 02 1b   .)...%.. "
0090  30 82 01 c5 a0 03 02 01  02 02 01 00 30 0d 06 09   0....... .
00a0  2a 86 48 86 f7 0d 01 01  04 05 00 30 45 31 0b 30   *.H..... .
00b0  09 06 03 55 04 06 13 02  41 55 31 13 30 11 06 03   ...U.... AU
00c0  55 04 08 13 0a 53 6f 6d  65 2d 53 74 61 74 65 31   U....Som e-
```

Certificate (ssl.handshake.certificate), 543 bytes

Packets: 16582 Dis

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	00
Signature algorithm	md5RSA
Issuer	Internet Widgits Pty Ltd, Som...
Valid from	Saturday, February 28, 2004 ...
Valid to	Tuesday, February 27, 2007 6...
Subject	Internet Widgits Pty Ltd, Som...
Public key	RSA (512 Bits)

Edit Properties... | Copy to File...

OK

Modifying Packets

File Edit View Documents Bookmarks Tools Settings Help

```
0000:0000  d4 00 00 00 00 0f 66 e3 76 3b   ô.....fãv;
```

Hex | Find | Backwards | Ign

ack.bin file, exported from capture file

Injected frame that has been modified

```
▷ Frame 1 (10 bytes on wire, 10 bytes captured)
▽ IEEE 802.11
    Type/Subtype: Acknowledgement (29)
  ▽ Frame Control: 0x04D4 (Normal)
      Version: 0
      Type: Control frame (1)
      Subtype: 13
    ▽ Flags: 0x4
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0
        .... .1.. = More Fragments: More fragments follow
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered

0000  d4 04 00 00 00 0f 66 e3  76 3b                .....f. v;
```

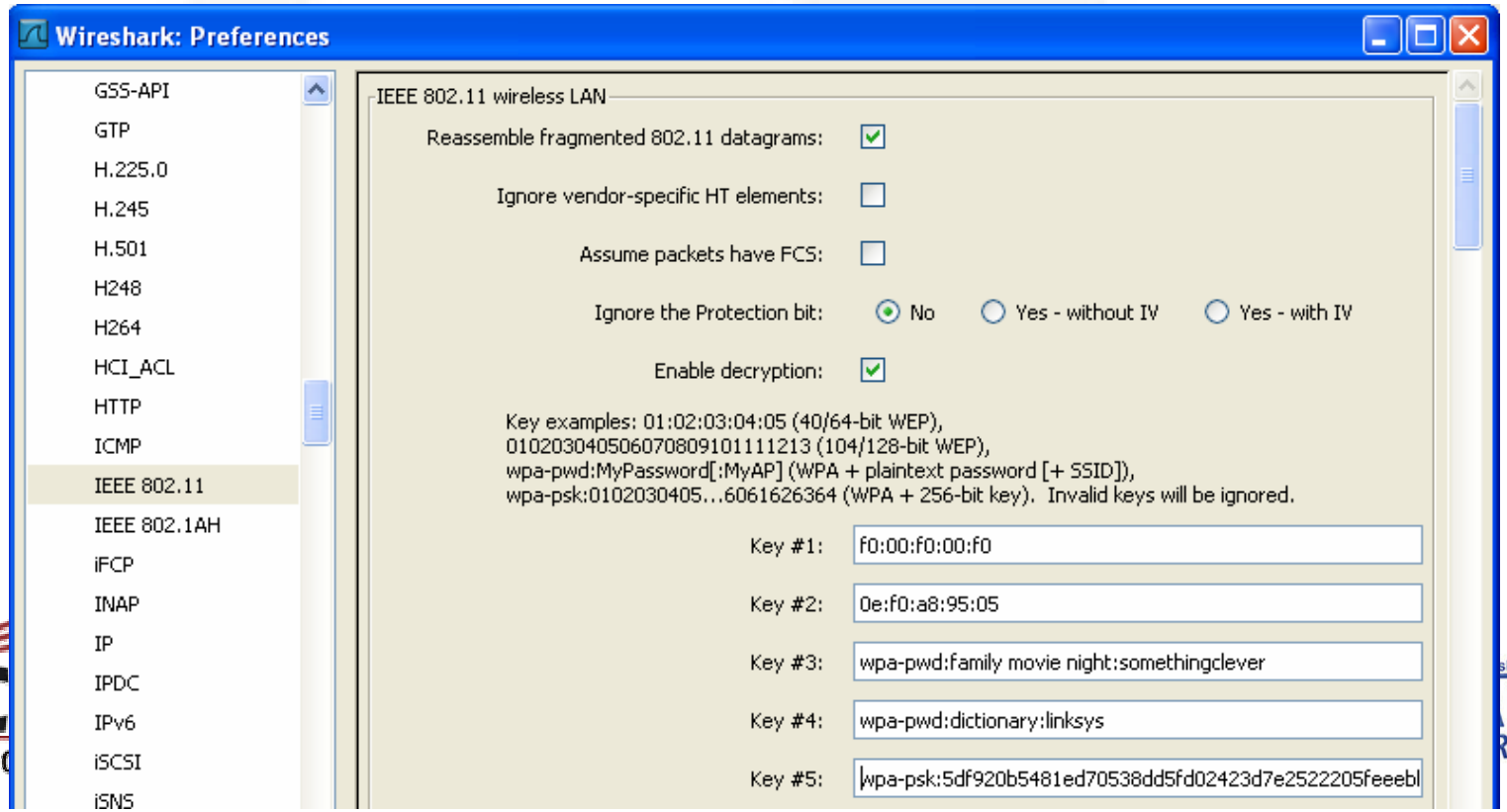
```
# file2air -i wifi0 -f ack.bin -t -r madwifing -n 100
Transmitting packets ...
```

www.wiresharkU.com WIRESHARK UNIVERSITY

Decrypting Frames - wlan6.pcap

Wireshark supports decrypting WEP, WPA/WPA2 traffic

- For WPA/WPA2, only PSK is practical unless your RADIUS server or AP discloses PMK's
- Must include EAPOL Key frames deriving PTK to decrypt



Conclusion

Wireshark is a powerful analysis tool

Monitor-mode functionality on Linux or with Airpcap on Windows

Display filters are applied in many Wireshark features

Familiarity with the tool and specification reduces the time needed to identify the problem!

Questions?

Sample captures at
www.willhackforsushi.com/resources/sharkfest08-samples.zip

CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY