aws professional services

Wireshark for Wi-Fi and Big Data

Wireshark, DumpCap, Tshark, MergeCap

Myron Hattig, Sr. IoT Architect, AWS Professional Services, Emerging Technologies and Intelligent Platforms
Gaurav Aggarwal, Software Development Engineer, IoT Device Services

March 27, 2019 V1

Outline

- Wireshark Setup and Navigation
- GUI Packet Capture and Analysis
- Big Data Packet Capture and Manipulation with Python

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Setup Wireshark 2.6.6

Download Wireshark from here:

https://www.wireshark.org/

Clone this github repository:

https://github.com/mhattig/Wireshark

CD to your local clone of the repo, then copy config files from repo into wireshark config directory:

```
> cd ~/Wireshark
➢ ls
Readme.md config python data.zip
➢ cp config/* ~/.config/wireshark
```

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

OSX – Find target Wi-Fi AP’s Channel Number

Go to Airport tool directory.

```
Cd /System/Library/PrivateFrameworks/Apple80211.framework/Resources/
```

Find the AP’s channel number

```
sudo ./airport -s
```

```
          SSID BSSID             RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
       XFINITY 2e:51:a4:1c:97:18 -40  157     Y  US WPA2(802.1x/AES/AES)
       XFINITY 4a:b8:1f:c4:dc:b6 -63  157     Y  US WPA2(802.1x/AES/AES)
  xfinitywifi 0e:51:a4:1c:97:18 -40  157     Y  US NONE
       xfinity 2e:51:a4:1c:97:18 -40  157     Y  US NONE
   BagelBear5G fc:51:a4:1c:97:18 -40  157     Y  US WPA2(PSK/AES/AES)
 HOME-D592-2.XX 18:b8:1f:c4:dc:b6 -63  157     Y  US WPA2(PSK/AES/AES)
     Hotcakes 8 10:05:01:87:32:b0 -74  153     Y  US WPA2(PSK/AES/AES)
       XFINITY 22:05:01:87:32:b0 -74  153     Y  US WPA2(802.1x/AES/AES)
  Eternal Bliss 1c:87:2c:e5:2a:cc -80  149     Y  -- WPA2(PSK/AES/AES)
        gWifi e4:f0:42:ce:9c:ab -41  149     Y  us WPA2(PSK/AES/AES)
       globe11 46:12:65:79:ae:03 -80  149     Y  US WPA2(PSK/AES/AES)
        gWifi e4:f0:42:ce:dd:e5 -56  149     Y  us WPA2(PSK/AES/AES)
        gWifi e4:f0:42:ce:9f:55 -44  149     Y  us WPA2(PSK/AES/AES)
       HPylori bc:64:4b:38:9d:1c -79  48      Y  US WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
TP-LINK_65CC_5G 98:de:d0:e8:65:ce -72  36      Y  -- WPA2(PSK/AES/AES)
  xfinitywifi 2a:b8:1f:c4:dc:b5 -55  11      Y  US NONE
     Hotcakes 2.4 10:05:01:87:32:a8 -63  11      Y  US WPA2(PSK/AES/AES)
   onWifi-guest 4a:07:0b:12:61:d4 -86  11      Y  US WPA2(PSK/AES/AES)
 HOME-D592-2.XX 18:b8:1f:c4:dc:b5 -63  11      Y  US WPA2(PSK/AES/AES)
     Happiness 1c:87:2c:e5:2a:c8 -72  11      Y  -- WPA2(PSK/AES/AES)
  xfinitywifi 1a:05:01:87:32:a8 -68  11      Y  US NONE
 BRCM_TEST_SSID 00:10:18:f1:f2:f3 -59  1       N  -- NONE
   TP-LINK_65CC 98:de:d0:e8:65:cc -69  10      Y  -- WPA2(PSK/AES/AES)
   onWifi-guest c6:e9:84:f4:8d:00 -76  6       Y  us WPA2(PSK/AES/AES)
        onWifi c4:e9:84:f4:8d:01 -77  6       Y  us WPA2(PSK/AES/AES)
      omshanti 24:f5:a2:06:b6:89 -81  5       Y  US WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
        gWifi e4:f0:42:ce:9f:59 -56  6       Y  us WPA2(PSK/AES/AES)
  xfinitywifi 0e:51:a4:1c:97:17 -35  6       Y  US NONE
     BagelBear fc:51:a4:1c:97:17 -28  6       Y  US WPA2(PSK/AES/AES)
FellnyWifiLovoher 10:c3:7b:e0:a8:80 -84  5       Y  -- WPA2(PSK/AES/AES)
       Linksys 60:38:e0:08:dc:98 -80  4       Y  -- WPA2(PSK/AES/AES)
       Andras 88:b4:a6:f7:bc:39 -76  1       Y  -- WPA2(PSK/AES/AES)
       HPylori bc:64:4b:38:9d:1b -63  2,+1    Y  US WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
  xfinitywifi a6:15:88:7a:47:70 -66  1       Y  US NONE
        gWifi e4:f0:42:ce:dd:e9 -52  1       Y  us WPA2(PSK/AES/AES)
  xfinitywifi ce:64:4b:38:9d:1b -72  2,+1    Y  US NONE
   TP-LINK_MPH c0:25:e9:03:89:ae -39  1       Y  -- WPA2(PSK/AES/AES)
        gWifi e4:f0:42:ce:9c:af -32  1       Y  us WPA2(PSK/AES/AES)
```

```
          SSID BSSID             RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
```

AP’s Channel is 1

```
   TP-LINK_MPH c0:25:e9:03:89:ae -39  1       Y  -- WPA2(PSK/AES/AES)
```

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

OSX – Wi-Fi Monitor Mode & Listen

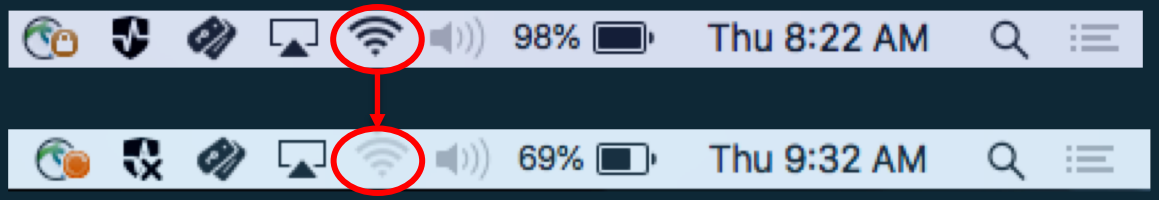
Go to Airport tool directory.

```
Cd /System/Library/PrivateFrameworks/Apple80211.framework/Resources/
```

Put Wi-Fi in Monitor Mode.

```
sudo ./airport -z
```

Wi-Fi icon on toolbar changes to Wi-Fi monitor



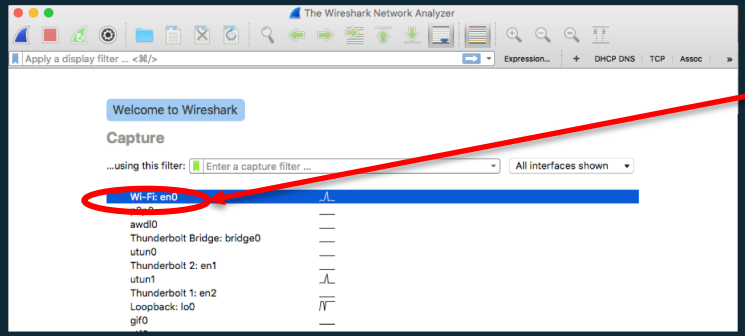
Listen on channel 1:

```
sudo ./airport –c1
```

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

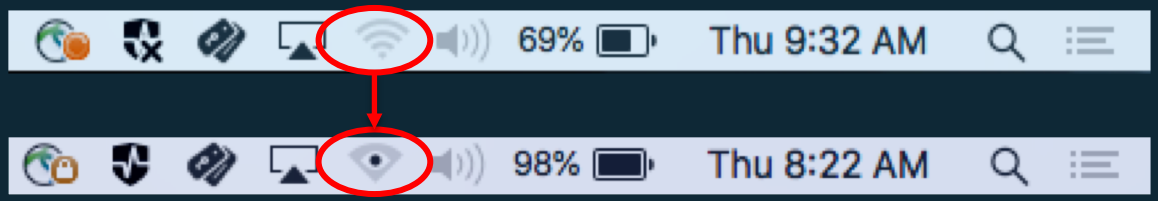
aws professional services

Start Wireshark



Select Wi-Fi interface

Wi-Fi icon on toolbar changes to the "all-seeing-eye" when capture is active



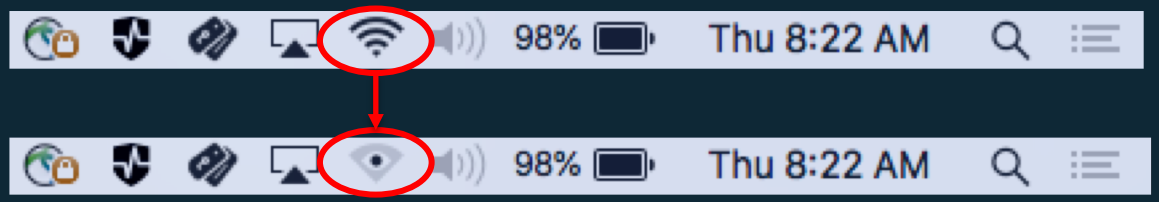
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Start Wireshark From Wi-Fi “on” Warning 1

If laptop is connected to the target AP, then it is possible to just start Wireshark, but beware …

Wi-Fi icon transitions from “on” to “all-seeing-eye”



Capture is happening on the AP channel to which the laptop is connected.

Here is the beware … Google and EERO APs do not allow for different SSIDs for 2.4GHz and 5GHz Wi-Fi. You want to capture on channel 1, but the laptop may be on channel 149

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Start Wireshark From Wi-Fi “on” Warning 1

A scan of an environment with three Google Mesh Wi-Fi AP shows this:

```
 SSID BSSID             RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
gWifi e4:f0:42:ce:9f:55 -59  149     Y  us WPA2(PSK/AES/AES)
gWifi e4:f0:42:ce:dd:e5 -52  153     Y  us WPA2(PSK/AES/AES)
gWifi e4:f0:42:ce:9c:ab -39  157     Y  us WPA2(PSK/AES/AES)
gWifi e4:f0:42:ce:dd:e9 -57  11      Y  us WPA2(PSK/AES/AES)
gWifi e4:f0:42:ce:9c:af -41  6       Y  us WPA2(PSK/AES/AES)
gWifi e4:f0:42:ce:9c:af -31  1       Y  us WPA2(PSK/AES/AES)
```

Laptop may be connected to 2.4GHz channels 1, 6, 11 or 5GHz channels 149, 153, or 157

Best practice is to always:

- Definitely know the correct target channel
- Verify capture is happening on the correct channel

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Start Wireshark From Wi-Fi “on” Warning 2

Another common issue when starting from Wi-Fi “on” is that the wireless interface is not really in monitor mode

Verify the packet capture has packets with MAC addresses that are not Broadcast and not the laptop’s

Otherwise the packet capture only includes packets to/from the laptop

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Start and Stop Capture

After interface is selected on startup, the capture becomes active as indicated by the green shark-fin

Captured packets are scrolling up the screen when shark-fin is green

Click red-square to stop when shark-fin is green
Click shark-fin to start captures when shark-fin is blue

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Preference File

~/.config/wireshark/preference file sets layout

Wi-Fi: en0

Apply a display filter ... <⌘/> | Expression... | + | DHCP DNS | TCP | Assoc | STA MAC | AP MAC | »

No.	Time	Trans	Recv	Data rate	Protocol	Length	Sequence number	Info
7517	28.341522			24	802.11	57		802.11 Block Ack, Flags=.....C
7518	28.364970	e4:f0:42:ce:dd:e9	ff:ff:ff:ff:ff:ff	1	802.11	267	3624	Beacon frame, SN=3624, FN=0, Flags=.....C, BI
7519	28.392860	e4:70:b8:5d:b3:6c	ff:ff:ff:ff:ff:ff	1	802.11	104	3644	Fragmented IEEE 802.11 frame
7520	28.392913	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6	802.11	53	156	Null function (No data), SN=156, FN=0, Flags=...
7521	28.392973			6	802.11	39		Acknowledgement, Flags=.....C
7522	28.395856	e4:f0:42:ce:9c:af	e4:70:b8:5d:b3:6c	1	802.11	261	37	Probe Response, SN=37, FN=0, Flags=.....C, BI
7523	28.396313			1	802.11	39		Acknowledgement, Flags=.....C
7524	28.409046	e4:f0:42:ce:dd:e9	e4:70:b8:5d:b3:6c	1	802.11	261	3774	Probe Response, SN=3774, FN=0, Flags=.....C,
7525	28.409131			1	802.11	39		Acknowledgement, Flags=.....C
7526	28.411995	a4:15:88:7a:47:70	ff:ff:ff:ff:ff:ff	1	802.11	331	2996	Beacon frame, SN=2996, FN=0, Flags=.....C, BI
7527	28.414154	c0:25:e9:03:89:ae	ff:ff:ff:ff:ff:ff	1	802.11	267	493	Beacon frame, SN=493, FN=0, Flags=.....C, BI=
7528	28.414746	80:ce:62:f6:41:7b	ff:ff:ff:ff:ff:ff	6	802.11	441	1783	Beacon frame, SN=1783, FN=0, Flags=.....C, BI
7529	28.443676	e4:f0:42:ce:9c:af	ff:ff:ff:ff:ff:ff	1	802.11	267	1374	Beacon frame, SN=1374, FN=0, Flags=.....C, BI
7530	28.459436	e4:70:b8:5d:b3:6c	ff:ff:ff:ff:ff:ff	1	802.11	104	3778	Probe Request, SN=3778, FN=0, Flags=.....C, S
7531	28.462304	e4:f0:42:ce:9c:af	e4:70:b8:5d:b3:6c	1	802.11	261	38	Probe Response, SN=38, FN=0, Flags=.....C, BI
7532	28.464643	e4:f0:42:ce:9c:af	e4:70:b8:5d:b3:6c	1	802.11	261	38	Probe Response, SN=38, FN=0, Flags=....R...C, BI
7533	28.466852	e4:f0:42:ce:9c:af	e4:70:b8:5d:b3:6c	1	802.11	261	38	Probe Response, SN=38, FN=0, Flags=....R...C, BI
7534	28.469171	e4:f0:42:ce:dd:e9	ff:ff:ff:ff:ff:ff	1	802.11	267	3626	Beacon frame, SN=3626, FN=0, Flags=.....C, BI

```
    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: Google_ce:dd:e9 (e4:f0:42:ce:dd:e9)
    Source address: Google_ce:dd:e9 (e4:f0:42:ce:dd:e9)
    BSS Id: Google_ce:dd:e9 (e4:f0:42:ce:dd:e9)
```

```
0000  00 00 19 00 6f 08 00 00  12 c1 27 16 00 00 00 00   ····o··· ··'·····
0010  10 02 6c 09 80 04 cf 9b  00 80 00 00 00 ff ff ff   ··l····· ********
0020  ff ff ff e4 f0 42 ce dd  e9 e4 f0 42 ce dd e9 a0   *····B·· ···B····
0030  cf 01 50 33 b9 13 00 00  00 64 00 31 14 00 05 67   ··P3···· ·d·1···g
0040  57 69 66 69 01 08 82 84  8b 96 0c 12 18 24 03 01   Wifi···· ·····$··
```

wireshark_en0_20190321083416_c4iM0i.pcapng | Packets: 7621 · Displayed: 7621 (100.0%) | Profile: Default

Display-filtered captured packets

Protocol Dissection

Raw bytes

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Preference File

~/.config/wireshark/preference file configures columns to any desired protocol field

Packet Number

Capture Time

Transmitter MAC

Receiver MAC

Wi-Fi DataRate

Highest-Layer Protocol

Length Preamble-CRC

Wi-Fi Sequence Number

Summary Info depends on Highest-Layer Protocol

Wi-Fi: en0

Apply a display filter ... <⌘/>

Expression... + DHCP DNS TCP Assoc STA MAC AP MAC »

No.	Time	Trans	Recv	Data rate	Protocol	Length	Sequence number	Info
1	0.000000			24	802.11	39		Disassociate[Malformed Packet]
2	0.002404			24	802.11	57		Clear-to-send, Flags=o...RMFTC
3	0.006720	a4:56:cc:45:0c:8d	ff:ff:ff:ff:ff:ff	6	802.11	319	1521	Beacon frame, SN=1521, FN=0, Flags=.....C, BI
4	0.014548	50:f2:32:3f:5f:81	e6:92:0d:f5:6f:2b	48	802.11	719	2092	Fragmented IEEE 802.11 frame
5	0.022940	a4:56:cc:45:0c:8e	ff:ff:ff:ff:ff:ff	6	802.11	265	1514	Beacon frame, SN=1514, FN=0, Flags=.....C, BI
6	0.023306	a4:56:cc:45:0c:92	ff:ff:ff:ff:ff:ff	6	802.11	289	1512	Beacon frame, SN=1512, FN=0, Flags=.....C, BI
7	0.041427	a4:56:cc:45:0c:8f	ff:ff:ff:ff:ff:ff	6	802.11	254	1512	Beacon frame, SN=1512, FN=0, Flags=.....C, BI
8	0.042226			24	802.11	39		Association Request[Malformed Packet]
9	0.046390	a4:15:88:7a:47:70	ff:ff:ff:ff:ff:ff	1	802.11	331	3596	Beacon frame, SN=3596, FN=0, Flags=.....C, BI
10	0.048164	a6:15:88:7a:47:70	ff:ff:ff:ff:ff:ff	1	802.11	228	3597	Beacon frame, SN=3597, FN=0, Flags=.....C, BI
11	0.056592	dc:7f:a4:2e:93:4f	ff:ff:ff:ff:ff:ff	1	LLC	181	987	U, func=DISC; DSAP 0x96 Individual, SSAP IBM Net

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Color Filters File

~/.config/wireshark/colorfilters file sets the color filters based on any protocol field

Wi-Fi Connection

Arp

DHCP
DNS

Grat. Arp

TCP
SYN, ACK

trace2.pcapng

itent_type == 23)) && !(wlan.fc.type_subtype == 0x0018)) && !(frame.len == 1595)) && !(wlan.fc.type_subtype == 0x0019)

Expression… + DHCP DNS TCP Assoc STA MAC AP MAC »

No.	Time	Trans	Recv	Data rate	Protocol	Length	Sequence number	Info
346…	152.467930	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	1	802.11	59	256	Authentication, SN=256, FN=0, Flags=.....C
346…	152.470674	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	1	802.11	145	1992	Association Request, SN=1992, FN=0, Flags=.....
346…	152.472973	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	1	802.11	163	257	Association Response, SN=257, FN=0, Flags=.....
346…	152.474643	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	1	EAPOL	162	0	Key (Message 1 of 4)
346…	152.478389	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	1	EAPOL	182	1993	Key (Message 2 of 4)
346…	152.481450	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	1	EAPOL	218	1	Key (Message 3 of 4)
346…	152.488523	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	1	EAPOL	160	1994	Key (Message 4 of 4)
346…	152.973497	c0:25:e9:03:89:ae	ff:ff:ff:ff:ff:ff	11	ARP	105	474	Who has 192.168.0.103? Tell 192.168.0.1
347…	153.700394	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	52	DHCP	678	0	DHCP Offer - Transaction ID 0x5851f42d
347…	153.705313	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	2	DHCP	379	1	DHCP Request - Transaction ID 0x5851f42d
347…	153.706617	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	58.5	DHCP	678	1	DHCP ACK - Transaction ID 0x5851f42d
347…	153.710790	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	2	ARP	107	2	Gratuitous ARP for 192.168.0.103 (Request)
347…	153.713685	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	TCP	119	0	13609 → secure-mqtt(8883) [RST, ACK] Seq=6703
347…	153.720691	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	DNS	167	1	Standard query 0x2df4 A a27xdhuepxh1ys.iot.us-
347…	153.756633	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	65	DNS	360	3	Standard query response 0x2df4 A a27xdhuepxh1y
347…	153.768167	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	TCP	131	2	[TCP Port numbers reused] 64070 → secure-mqtt(8
347…	153.794417	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	370	488	DHCP Discover - Transaction ID 0x5851f42d
347…	153.794944	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	377	489	DHCP Request - Transaction ID 0x5851f42d
347…	153.795367	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	ARP	105	490	Gratuitous ARP for 192.168.0.103 (Request)
347…	153.896127	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	TCP	154	4	secure-mqtt(8883) → 64070 [SYN, ACK] Seq=0 Ack=1
348…	154.196395	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	TLSv1…	362	4	Client Hello
348…	154.408444	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	TCP	842	7	[TCP Window Full] secure-mqtt(8883) → 64070 [P
348…	154.511822	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	TLSv1…	708	9	Server Hello, Certificate, Server Key Exchange,

```
Type/Subtype: QoS Data (0x0028)
▼ Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)

0010  16 04 6c 09 80 04 ef a6  00 88 41 a2 00 c0 25 e9   ··l····· ··A···%·
0020  03 89 ae cc 50 e3 88 18  6c c0 25 e9 03 89 ae 30   ····P··· l·%····0
```

Frame (362 bytes) | Decrypted CCMP data (291 bytes)

Four sequences of Wi-Fi-DHCP-DNS-TCP

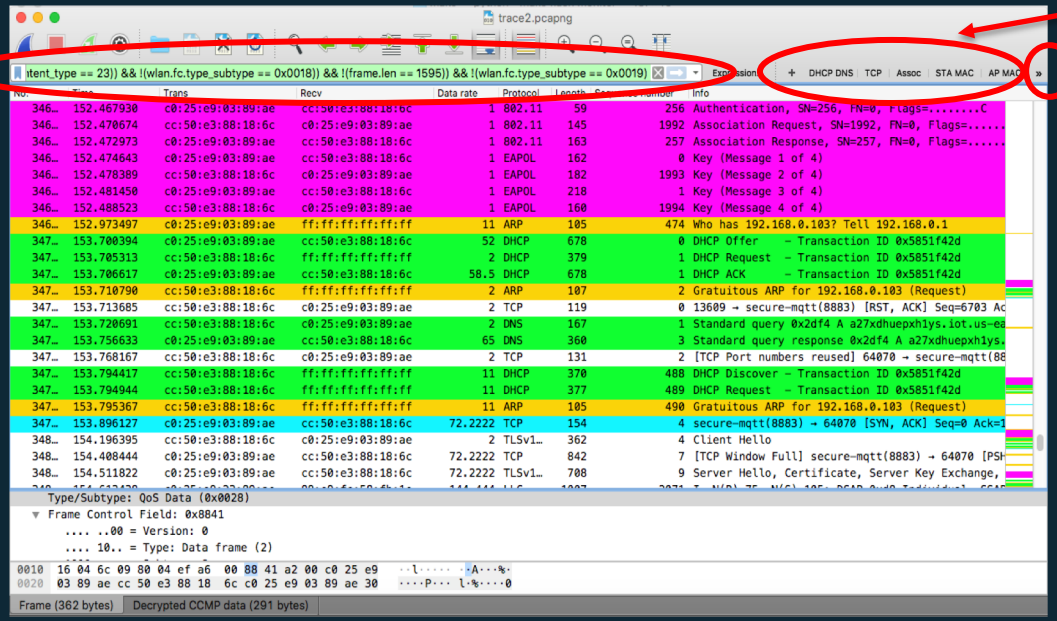
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Display Filters File

~/.config/wireshark/ dfilter_buttons file provides pre-set display filters

Active Display Filter



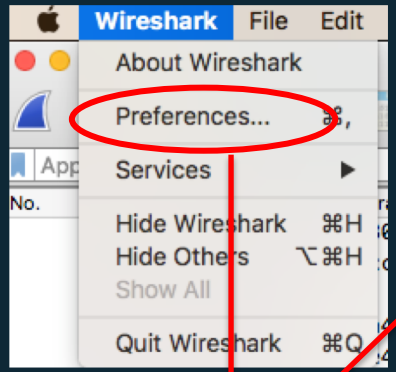
Display Filter Buttons

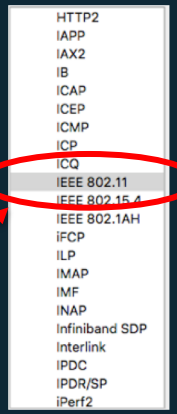
More Display Filter Buttons

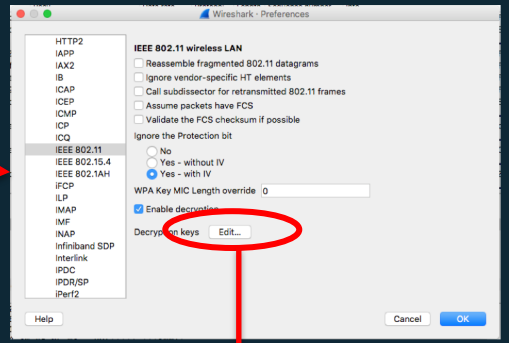
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

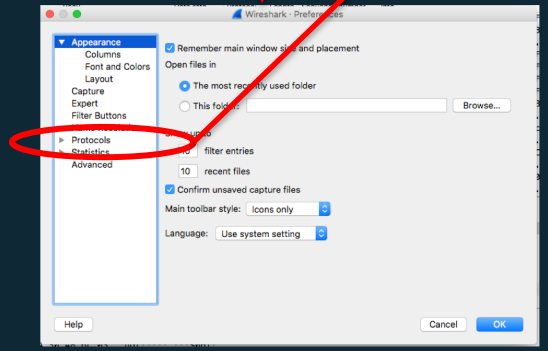
aws professional services

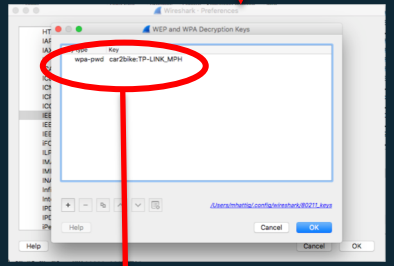
80211_keys File











~/.config/80211_keys

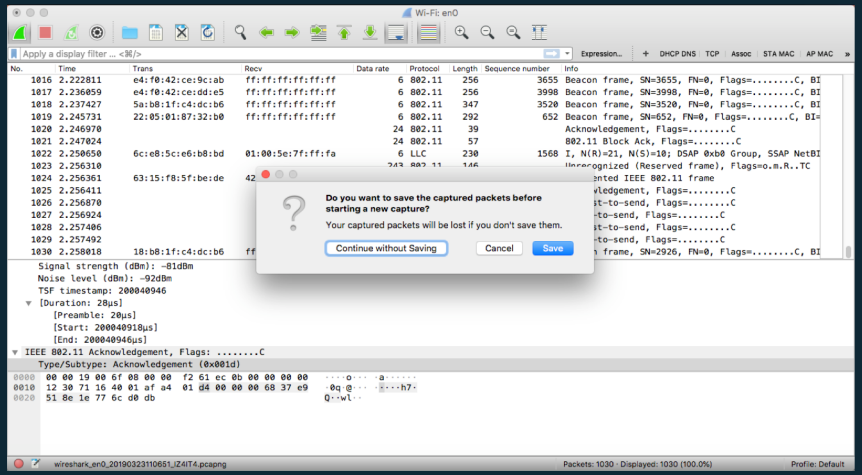
Key type	Key
wpa-pwd	car2bike:TP-LINK_MPH

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

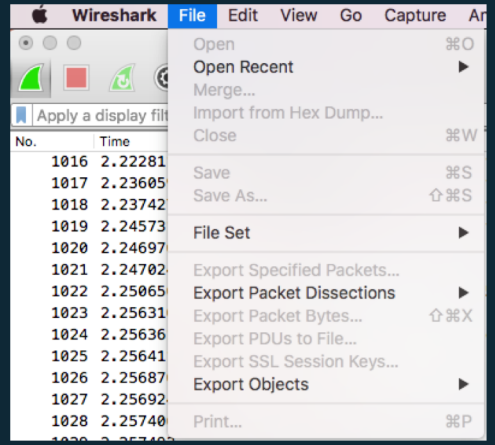
aws professional services

Packet Capture Files use .pcapng Extension

When starting a packet capture, GUI prompts so save the current capture as a file



Packet captures files can be loaded from the tool bar



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Packet Capture and Analysis Sequence

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Setup, Start Wireshark Recap

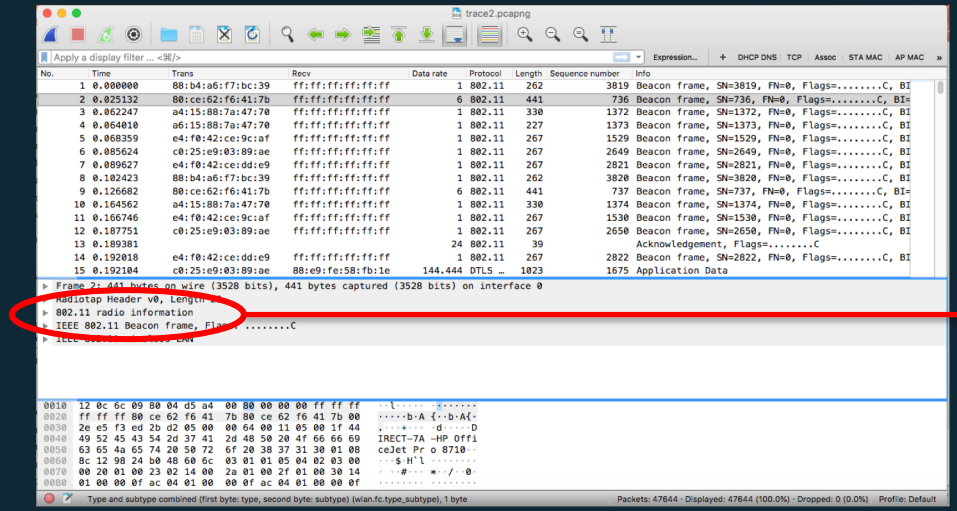
- Copy files from GitHub repo clone ~/Wireshark/config to ~/.config/wireshark:
  - preferences
  - colorfilters
  - dfilter_buttons
  - 80211_keys
- Navigate GUI to set network name (SSID) and password for target AP
- Determine the target AP's Wi-Fi channel
- Put PC Wi-Fi in monitor mode on target channel with ./airport
- Start Wireshark
- Start/Stop captures

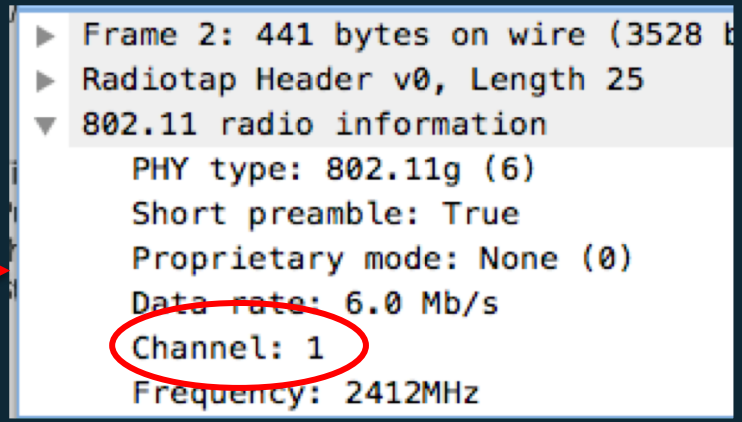
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Channel Verification

- Do a quick start/stop capture of 5 or 10 seconds
- Verify capture is happening on the right channel by expanding “802.11 radio information”, check “Channel:”





© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Monitor Mode Verification

- Do a quick start/stop capture of 5 or 10 seconds
- Verify the packet capture has packets with MAC addresses that are not Broadcast and not the laptop's
- Alternatively look for a packet with IOT device MAC address and no Broadcast
- Steps:
    - High light a packet that does not have ffffffff as Recv
    - In packet dissection pane click on IEEE 802.11
    - Look at all four addresses: Receiver, Destination, Transmitter, Source

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Monitor Mode Verification with IOT Device MAC

trace2.pcapng

Apply a display filter ... <⌘/>

No.	Time	Trans	Recv	Data rate	Protocol	Length	Sequence number	Info
18952	52.902885	e4:f0:42:ce:9c:af	ff:ff:ff:ff:ff:ff	1	802.11	267	2109	Beacon frame, SN=2109, FN=0, Flags=.....C
18953	52.924631	c0:25:e9:03:89:ae	ff:ff:ff:ff:ff:ff	1	802.11	267	3231	Beacon frame, SN=3231, FN=0, Flags=.....C
18954	52.928160	e4:f0:42:ce:dd:e9	ff:ff:ff:ff:ff:ff	1	802.11	267	3404	Beacon frame, SN=3404, FN=0, Flags=.....C
18955	52.937516	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6	802.11	53	614	Null function (No data), SN=614, FN=0, Flags=
18956	52.937566			6	802.11	39		Acknowledgement, Flags=.....C
18957	52.966976	80:ce:62:f6:41:7b	ff:ff:ff:ff:ff:ff	6	802.11	441	1267	Beacon frame, SN=1267, FN=0, Flags=.....C
18958	52.969737			24	802.11	39		Acknowledgement, Flags=.....C
18959	52.970135			24	802.11	39		Clear-to-send, Flags=.....C
18960	52.970182			24	802.11	57		802.11 Block Ack, Flags=.....C
18961	52.982637	c0:25:e9:03:89:ae	88:e9:fe:58:fb:1e	144.444	DTLS …	239	1166	Application Data
18962	53.003160	a4:15:88:7a:47:70	ff:ff:ff:ff:ff:ff	1	802.11	330	2404	Beacon frame, SN=2404, FN=0, Flags=.....C
18963	53.006457	a6:15:88:7a:47:70	ff:ff:ff:ff:ff:ff	1	802.11	227	2405	Beacon frame, SN=2405, FN=0, Flags=.....C
18964	53.027027	c0:25:e9:03:89:ae	ff:ff:ff:ff:ff:ff	1	802.11	267	3232	Beacon frame, SN=3232, FN=0, Flags=.....C
18965	53.030550	e4:f0:42:ce:dd:e9	ff:ff:ff:ff:ff:ff	1	802.11	267	3405	Beacon frame, SN=3405, FN=0, Flags=.....C

```
▶ Frame 18955: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Null function (No data), Flags: ...P...TC
    Type/Subtype: Null function (No data) (0x0024)
  ▶ Frame Control Field: 0x4811
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    Transmitter address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
    Destination address: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    Source address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
    BSS Id: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    STA address: Espressi_88:18:6c (cc:50:e3:88:18:6c)

0000  00 00 19 00 6f 08 00 00  eb dc bf 09 00 00 00 00   ····o··· ********
0010  12 0c 6c 09 80 04 ef a3  00 48 11 3c 00 c0 25 e9   ··l····· ·H·<··%·
0020  03 89 ae cc 50 e3 88 18  6c c0 25 e9 03 89 ae 60   ····P··· l·%····`
0030  26 51 40 2f ff                                     &Q@/·
```

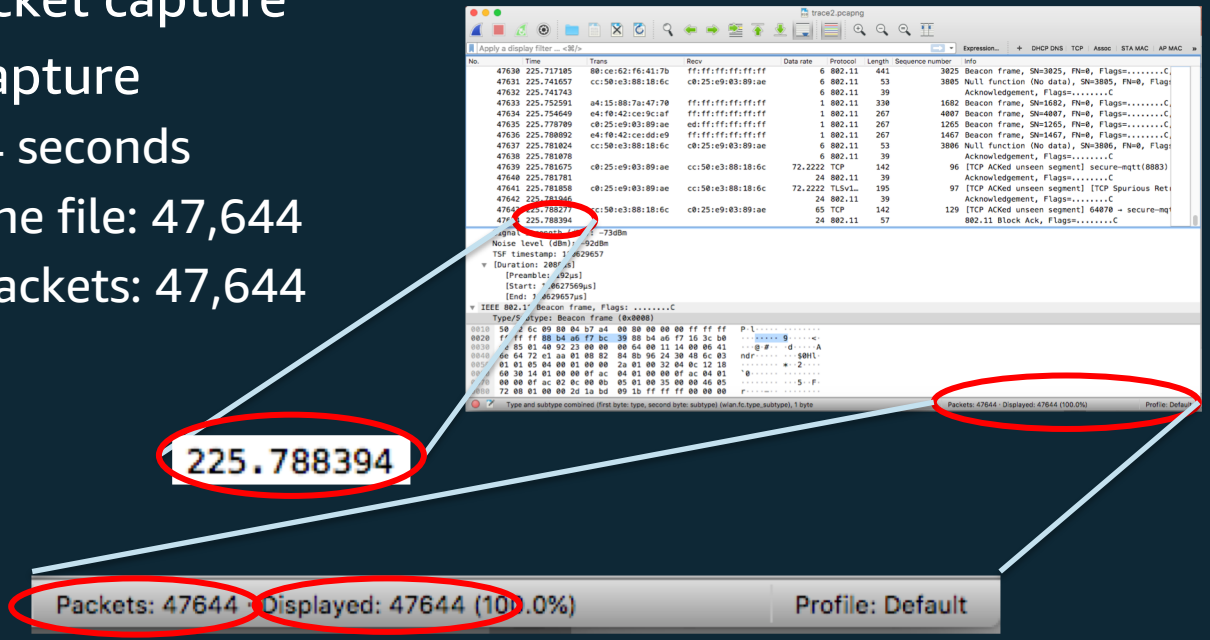
Frame is marked in the GUI (frame.marked) | Packets: 47644 · Displayed: 47644 (100.0%) | Profile: Default

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Remove Noise, Find the Signal

- Step 1:
  - Start/Stop packet capture
  - First look at capture
    - 225.788394 seconds
    - Packets in the file: 47,644
    - Displayed Packets: 47,644



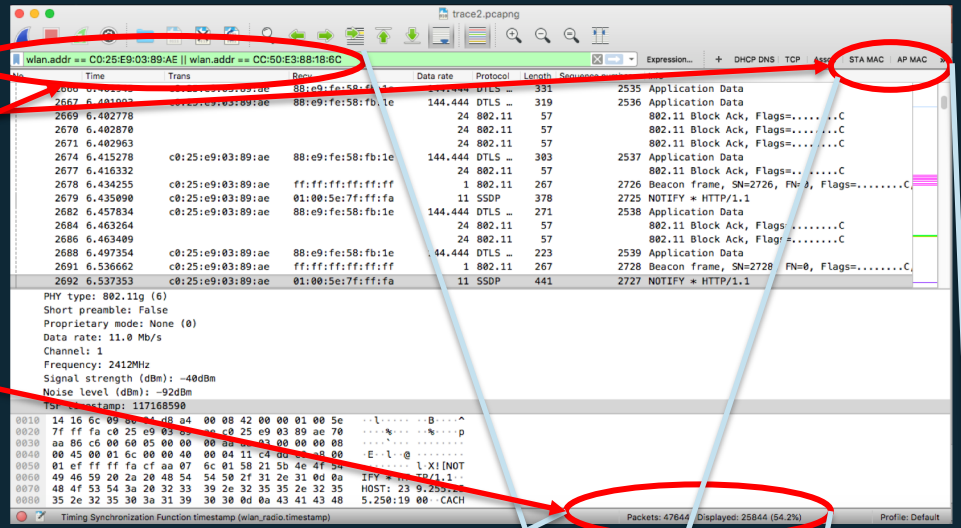
Note:
Keep packet captures to less than 20 minutes and 1 million packets; otherwise, load is slow and may not decode.

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Remove Noise, Find the Signal

- Step 2: STA and AP packets
  - 2.1 Click STA MAC
  - 2.2 Click AP MAC
  - 2.3 Copy past create new display filter
  - 2.4 Look at
    - Packets in the file: 47,644
    - Displayed Packets: 25,844



STA MAC | AP MAC

Packets: 47644 Displayed: 25844 (54.2%)

wlan.addr == C0:25:E9:03:89:AE || wlan.addr == CC:50:E3:88:18:6C

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Remove Noise, Find the Signal

- Step 3: Reduce, Reduce, Reduce
  - 3.1 High-light unwanted packet like BLOCK ACK
  - 3.2 Dissect Packet to find unique field
    - subtype 0x19 is a BLOCK ACK Wi-Fi Packet

```
(wlan.addr == C0:25:E9:03:89:AE || wlan.addr == CC:50:E3:88:18:6C) && !(wlan.fc.type_subtype == 0x0019)
```

  - 3.3 Look at
    - Packets in the file: 47,644
    - Displayed Packets: 20,831

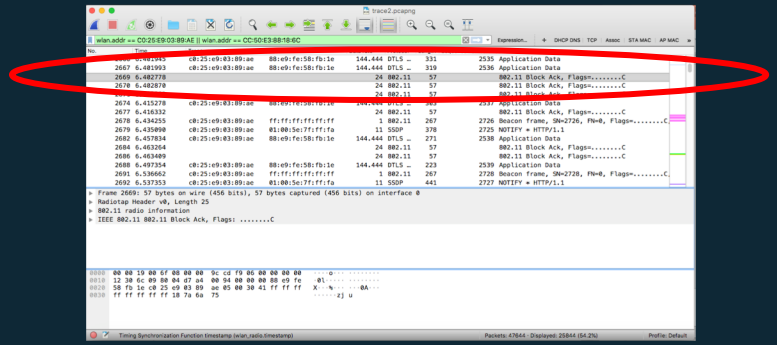
Packets: 47644 · Displayed: 20831 (43.7%)

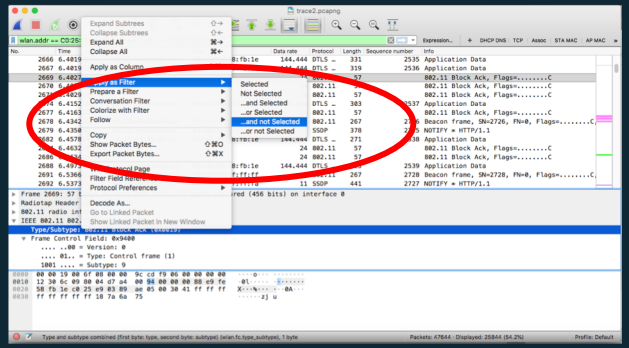
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

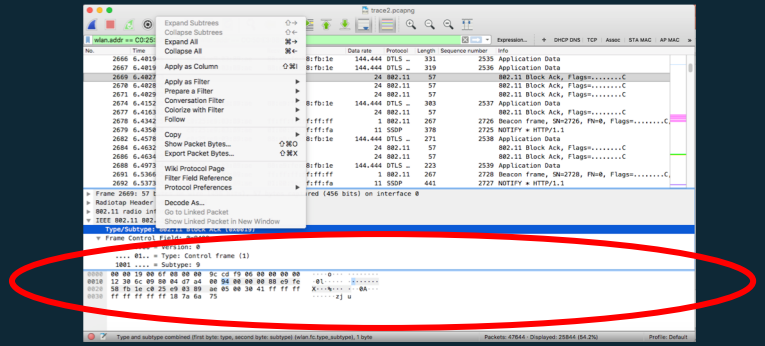
aws professional services

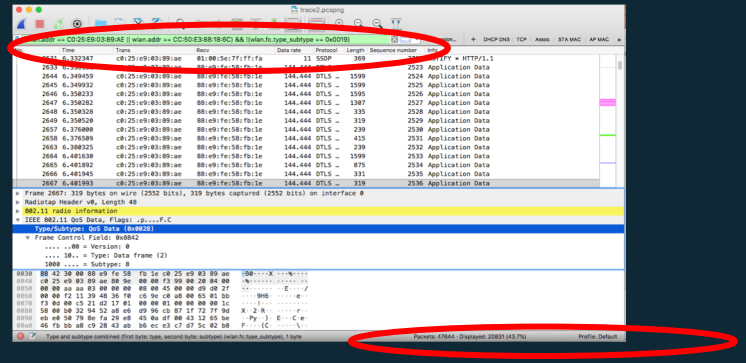
Sequence: Remove Noise, Find the Signal

- Repeat steps 3.1, 3.2, 3.3 with additional unwanted packets







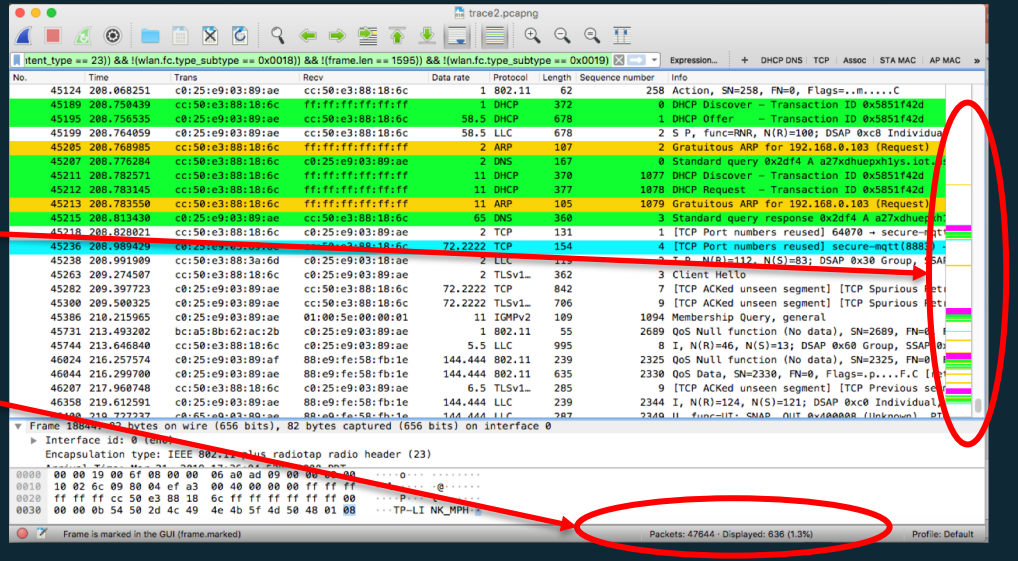


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Remove Noise, Find the Signal

- Step 4: Reduce, Reduce, Reduce
  - Repeat step 3 until to find what want … in this case pattern of re-connects
  - Final packet counts
    - Packets in the file: 47,644
    - Displayed Packets: 636

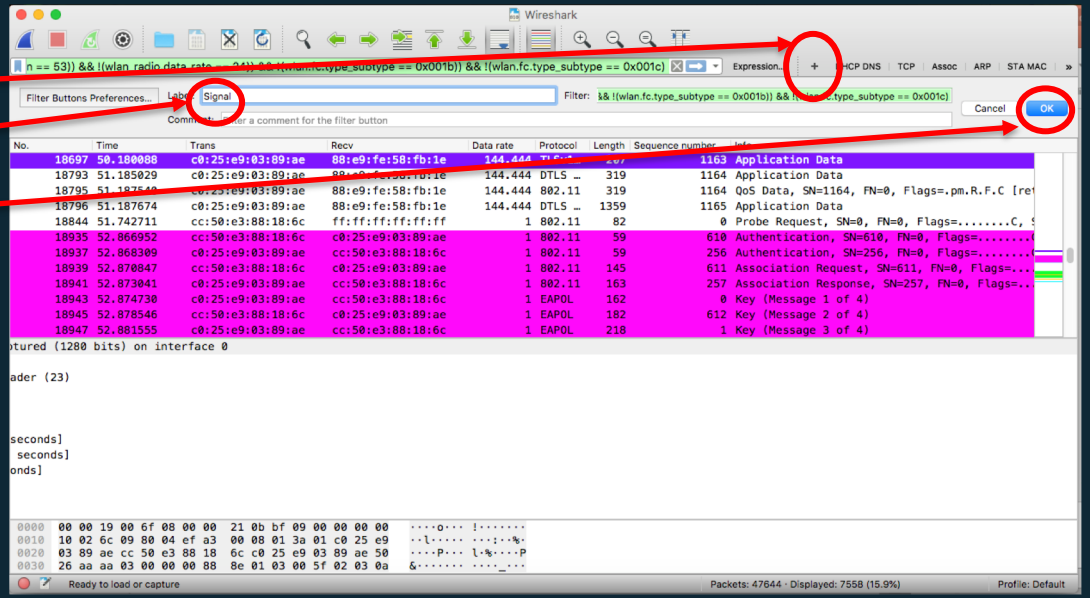


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Remove Noise, Find the Signal

- Step 5: Save display filter
  - Click on "+"
  - Enter name
  - Click OK

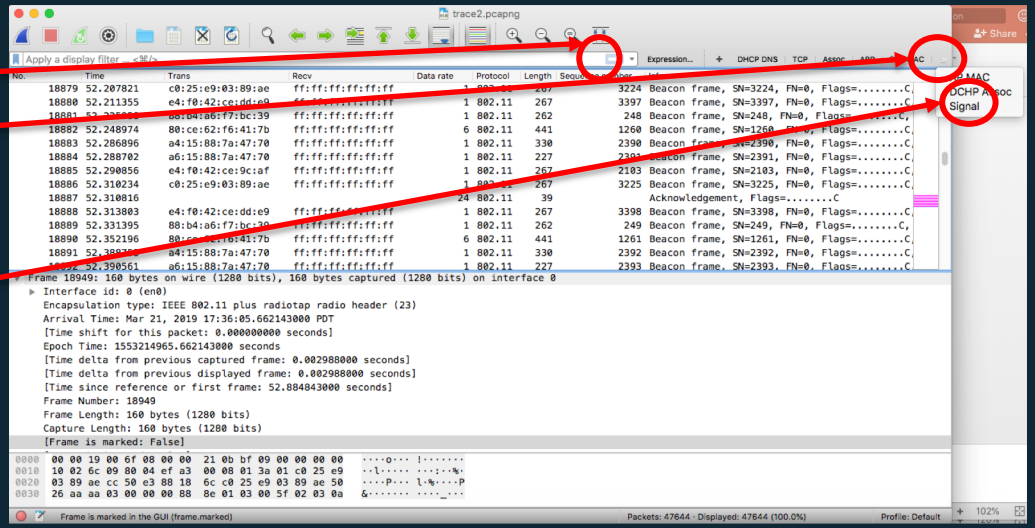


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Remove Noise, Find the Signal

- Step 6: Re-use display filter
  - Click on “x” to clear display filter
  - Click on ”>>” to see more display filters
  - Click on “Signal” to load the display filter

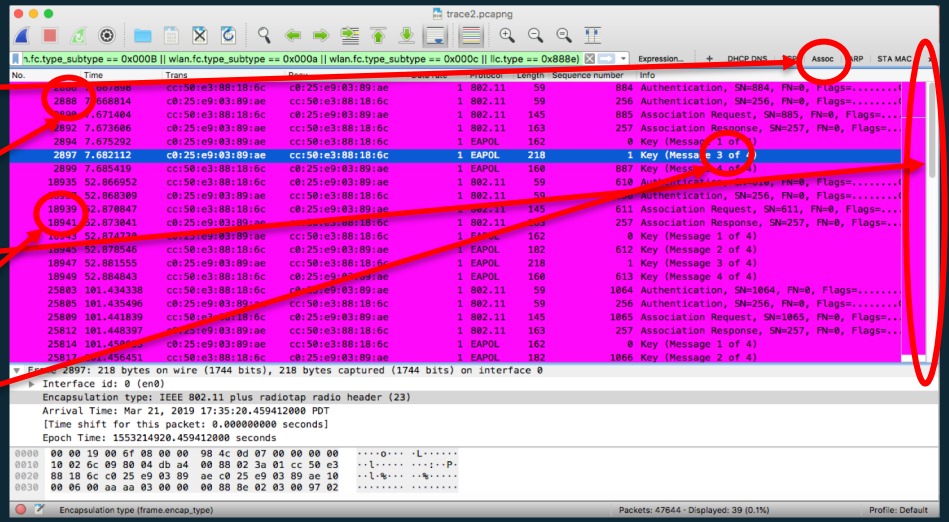


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Wi-Fi 4-Way Handshake Impact

- Step 1: Find bad 4-way handshake
  - Click “Assoc” display filter
  - Scroll up and down to get a sense of the number of Wi-Fi connections
  - Scroll all the way to the top Top packet number 2886
  - Missing Msg 2
  - Second 4-way handshake at packet number 18935 is okay



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: Wi-Fi 4-Way Handshake Impact

- Step 2: See the impact if missing packet
  - Click on display filter “>>” then select ”4-Way All”
  - Scroll through packets 2886-18935
  - Goto packet 8766 – nothing is decoded

8758	26.010757	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	802.11	195	100	QoS Data, SN=100, FN=0, Flags=.p..R.F.C [ret
8766	26.013045	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	65	802.11	195	100	QoS Data, SN=100, FN=0, Flags=.p..R.F.C [ret
8768	26.014891	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	72.2222	LLC	142	134	I P, N(R)=100, N(S)=58; DSAP 0xee Individual
8770	26.034115	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	IPX	227	101	Unknown (0x1ce9)
8773	26.036634	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	72.2222	LLC	142	135	I, N(R)=47, N(S)=15; DSAP 0xee Individual, S
8775	26.040849	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	72.2222	LLC	195	136	I, N(R)=71, N(S)=123; DSAP 0xb2 Individual,
8793	26.294410	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	LLC	142	102	S F, func=RR, N(R)=80; DSAP 0xca Individual,
8795	26.294558	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	72.2222	LLC	195	137	I P, N(R)=121, N(S)=115; DSAP 0x60 Individua
8813	26.354756	c0:25:e9:03:89:ae	88:e9:fe:58:fb:1c	144.444	LLC	239	719	S P, func=RNR, N(R)=20; DSAP 0x9a Group, SSA

  - Scroll through packets after 18935.
  - Goto 20804 to see TLS starting

20764	66.411774	c0:25:e9:03:89:ae	9e:b6:c3:eb:f6:ce	1	802.11	383	3369	Probe Response, SN=3369, FN=0, Flags=.....R...
20765	66.414891	c0:25:e9:03:89:ae	9e:b6:c3:eb:f6:ce	1	802.11	383	3369	Probe Response, SN=3369, FN=0, Flags=.....R...
20766	66.418134	c0:25:e9:03:89:ae	9e:b6:c3:eb:f6:ce	1	802.11	383	3369	Probe Response, SN=3369, FN=0, Flags=.....R...
20804	66.864807	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6.5	TLSv1…	411	10	Certificate Verify
20806	66.865364	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6.5	TLSv1…	148	11	Change Cipher Spec
20809	66.869487	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6.5	TLSv1…	211	12	Encrypted Handshake Message
20822	66.958214	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	TCP	138	13	secure-mqtt(8883) → 64070 [ACK] Seq=2667 Ack=
20823	66.958320	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	TCP	138	14	secure-mqtt(8883) → 64070 [ACK] Seq=2667 Ack=
20824	66.958411	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	72.2222	TLSv1…	217	15	Change Cipher Spec, Encrypted Handshake Messa
20826	66.960999	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6.5	TCP	142	13	64070 → secure-mqtt(8883) [ACK] Seq=1607 Ack=
20830	67.003728	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	6.5	TLSv1…	227	14	Application Data

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: DHCP, DNS

- Step 1: Look at the DHCP sequence
  - Click on display filter “DHCP DNS”
  - Note sequence: Discover->Request->Offer->Ack
  - Note DNS Sequence: Standard Query->Standard Query

trace2.pcapng

(wlan.addr == C0:25:E9:03:89:AE || wlan.addr == CC:50:E3:88:18:6C) && (udp.port == 53 || udp.port == 68 || udp.port == 67)

Expression... + DHCP DNS TCP Assoc ARP STA MAC AP MAC

No.	Time	Trans	Recv	Data rate	Protocol	Length	Sequence number	Info
3042	8.994766	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	370	2763	DHCP Discover - Transaction ID 0x5851f42d
3043	8.996044	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	377	2764	DHCP Request - Transaction ID 0x5851f42d
19055	53.932325	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	1	DHCP	372	0	DHCP Discover - Transaction ID 0x5851f42d
19059	53.933781	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	58.5	DHCP	678	1	DHCP Offer - Transaction ID 0x5851f42d
19061	53.937932	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	2	DHCP	379	1	DHCP Request - Transaction ID 0x5851f42d
19063	53.939390	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	58.5	DHCP	678	2	DHCP ACK - Transaction ID 0x5851f42d
19068	53.949595	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	370	3241	DHCP Discover - Transaction ID 0x5851f42d
19070	53.953055	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	DNS	167	0	Standard query 0x2df4 A a27xdhuepxh1ys.iot.us-east-2.amazona
19074	53.997463	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	65	DNS	360	3	Standard query response 0x2df4 A a27xdhuepxh1ys.iot.us-east-
26247	102.570850	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	1	DHCP	372	0	DHCP Discover - Transaction ID 0x5851f42d
26266	102.586638	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	52	DHCP	678	0	DHCP Offer - Transaction ID 0x5851f42d
26271	102.593824	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	2	DHCP	379	1	DHCP Request - Transaction ID 0x5851f42d
26275	102.595192	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	58.5	DHCP	678	1	DHCP ACK - Transaction ID 0x5851f42d
26282	102.613439	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	DNS	167	0	Standard query 0x2df4 A a27xdhuepxh1ys.iot.us-east-2.amazona
26290	102.692320	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	370	3777	DHCP Discover - Transaction ID 0x5851f42d
26293	102.695134	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	377	3778	DHCP Request - Transaction ID 0x5851f42d
34738	153.700394	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	52	DHCP	678	0	DHCP Offer - Transaction ID 0x5851f42d
34740	153.705313	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	2	DHCP	379	1	DHCP Request - Transaction ID 0x5851f42d
34744	153.706617	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	58.5	DHCP	678	1	DHCP ACK - Transaction ID 0x5851f42d
34752	153.720691	cc:50:e3:88:18:6c	c0:25:e9:03:89:ae	2	DNS	167	1	Standard query 0x2df4 A a27xdhuepxh1ys.iot.us-east-2.amazona
34755	153.756633	c0:25:e9:03:89:ae	cc:50:e3:88:18:6c	65	DNS	360	3	Standard query response 0x2df4 A a27xdhuepxh1ys.iot.us-east-
34765	153.794417	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	370	488	DHCP Discover - Transaction ID 0x5851f42d
34766	153.794944	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	11	DHCP	377	489	DHCP Request - Transaction ID 0x5851f42d
45189	208.750439	cc:50:e3:88:18:6c	ff:ff:ff:ff:ff:ff	1	DHCP	372	0	DHCP Discover - Transaction ID 0x5851f42d

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: DHCP, DNS

- Step 2: Dissect DHCP ACK
  - Highlight a DCHP ACK packet, go the packet dissection

```
▼ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source Port: bootps (67)
    Destination Port: bootpc (68)
    Length: 556
    Checksum: 0x76ca [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
▼ Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x5851f42d
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.103
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (ACK)
  ▶ Option: (54) DHCP Server Identifier
  ▶ Option: (51) IP Address Lease Time
  ▶ Option: (1) Subnet Mask
  ▶ Option: (3) Router
  ▶ Option: (6) Domain Name Server
  ▶ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000...
```

```
▼ Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.0.1
▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
▼ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.0.1
▼ Option: (6) Domain Name Server
    Length: 4
    Domain Name Server: 192.168.0.1
▶ Option: (255) End
```


aws professional services

Sequence: DHCP, DNS

- Step 3: Dissect DNS Response
  - DNS Response packet, go the packet dissection

```
▼ User Datagram Protocol, Src Port: domain (53), Dst Port: 37071 (37071)
    Source Port: domain (53)
    Destination Port: 37071 (37071)
    Length: 238
    Checksum: 0xed29 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
▼ Domain Name System (response)
    Transaction ID: 0x2df4
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
  ▶ Answers
    [Request In: 34752]
    [Time: 0.035942000 seconds]
```

```
▼ Queries
  ▶ a27xdhuepxh1ys.iot.us-east-2.amazonaws.com: type A, class IN
▼ Answers
  ▶ a27xdhuepxh1ys.iot.us-east-2.amazonaws.com: type CNAME, class IN, cname iotmoonraker.us-east-2.prod.iot.us-east-2.amazonaws.com
  ▶ iotmoonraker.us-east-2.prod.iot.us-east-2.amazonaws.com: type CNAME, class IN, cname dualstack.iotmoonraker-u-elb-k8fezfu9j02v-799874780.us-east-2.elb.amazonaws.com
  ▶ dualstack.iotmoonraker-u-elb-k8fezfu9j02v-799874780.us-east-2.elb.amazonaws.com: type A, class IN, addr 13.59.2.98
  ▶ dualstack.iotmoonraker-u-elb-k8fezfu9j02v-799874780.us-east-2.elb.amazonaws.com: type A, class IN, addr 18.217.238.169
  ▶ dualstack.iotmoonraker-u-elb-k8fezfu9j02v-799874780.us-east-2.elb.amazonaws.com: type A, class IN, addr 18.221.142.15
```

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: DHCP, DNS

- Step 4: Dissect DNS Response
  - Type CNAME DNS Record

```
▼ a27xdhuepxh1ys.iot.us-east-2.amazonaws.com: type CNAME, class IN, cname iotmoonraker.us-east-2.prod.iot.us-east-2.amazonaws.com
    Name: a27xdhuepxh1ys.iot.us-east-2.amazonaws.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 154
    Data length: 30
    CNAME: iotmoonraker.us-east-2.prod.iot.us-east-2.amazonaws.com
```

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: DHCP, DNS

- Step 4: Dissect DNS Response
  - Type A DNS Record

```
▼ dualstack.iotmoonraker-u-elb-k8fezfu9j02v-799874780.us-east-2.elb.amazonaws.com: type A, class IN, addr 13.59.2.98
    Name: dualstack.iotmoonraker-u-elb-k8fezfu9j02v-799874780.us-east-2.elb.amazonaws.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 46
    Data length: 4
    Address: 13.59.2.98
```

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Sequence: DHCP Discover is Wi-Fi Broadcast

- Wi-Fi Broadcast is two steps:
  - STA sends to AP, AP sends to all other STAs
- STA to AP: Packet number 19055
  - Recv: AP MAC: C0:50:E9:03:89:AE
  - Trans: STA MAC: CC:50:E3:88:18:6C
  - Dst: Broadcast MAC: FF:FF:FF:FF:FF:FF
  - Src: STA MAC: CC:50:E3:88:18:6C
- AP to all: Packet number 19068
  - Recv: Broadcast MAC: FF:FF:FF:FF:FF:FF
  - Trans: AP MAC: C0:50:E9:03:89:AE
  - Dst: Broadcast MAC: FF:FF:FF:FF:FF:FF
  - Src: STA MAC: CC:50:E3:88:18:6C

```
▶ Frame 19055: 372 bytes on wire (2976 bits), 372 bytes captured
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p.....TC
    Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8841
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    Transmitter address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
    BSS Id: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    STA address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
                 0000 = Fragment number: 0
```

```
▶ Frame 19068: 370 bytes on wire (2960 bits), 370 bytes captured (2
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Data, Flags: .pm...F.C
    Type/Subtype: Data (0x0020)
  ▶ Frame Control Field: 0x0862
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Espressi_88:18:6c (cc:50:e3:88:18:6c)
    BSS Id: Tp-LinkT_03:89:ae (c0:25:e9:03:89:ae)
    STA address: Broadcast (ff:ff:ff:ff:ff:ff)
```

Source & Transmitter are the same STA

Destination is Broadcast

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Big Data Packet Capture and Manipulation with Python

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Wireshark Tools Summary

- Wireshark:
  - GUI based tool to capture, filter, dissect, analyze, and visualize packets & packet traces
  - Manually export all or display-filtered-set of packets to .pcapng, .csv, text, JSON, XML
  - Difficult to automate and scale
- CLI Tools for automation:
  - Dumpcap: packet capture
  - Mergecap: combine multiple packet capture files into a single file
  - Tshark: filter and transform packet captures
  - TCPDump: overlapping features with tshark and dumpcap

Note: Individual packets can be synchronized with unrelated workflows (e.g. serial debug output, cloud logs) using the UTC timestamps on each packet

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

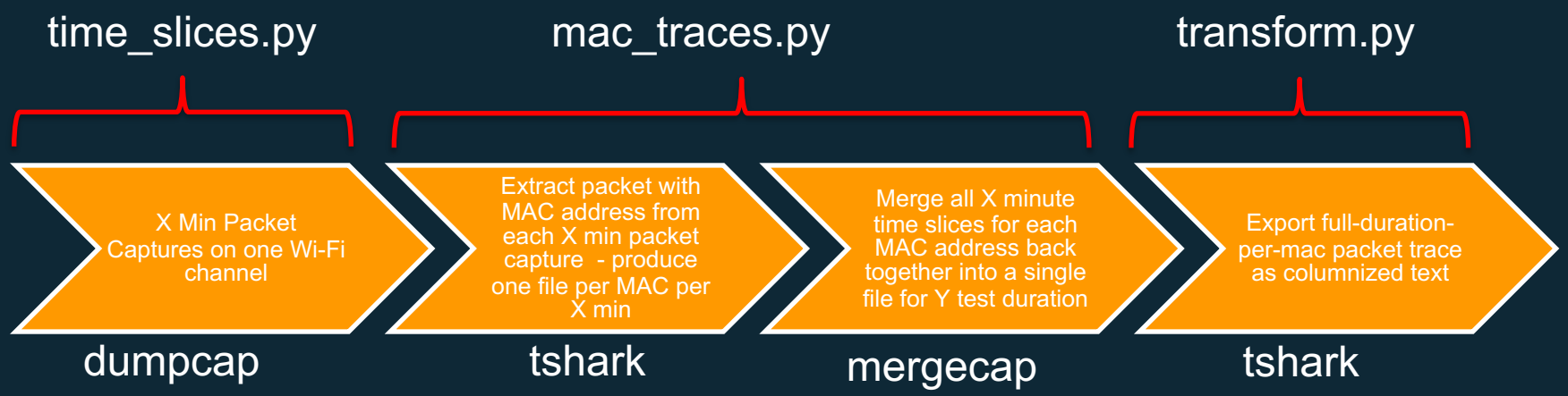
Capture Filter vs Display Filter

- Capture filters and display filters utilize incompatible filter syntaxes
- Purpose of capture filters is to limit packets on ingress
- Purpose of display filter is to limit packets on egress
- Best practice is to not use capture filter on initial capture to insure all packets enter the data pipeline then limit packets is subsequent steps
- Display filters used by Wireshark, Tshark
- Capture filters used by Wireshark, Dumpcap, Tshark, TCPDump

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Data Pipeline



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Steps

- Copy 80211_keys file from GitHub repo clone to ~/.config/wireshark
- Determine the target AP's Wi-Fi channel with ./airport
- Put Laptop Wi-Fi in monitor mode on target channel with ./airport
- Get MAC address of AP and any STA devices of interest
- Configure then run time_slices.py
  - test_duration = 10*60
  - time_slice = 2*60
- Configure then run mac_traces.py:
  - AP_mac = "AA:BB:CC:DD:EE:FF"
  - STA_ macs = ["01:02:03:04:05:06", "07:08:09:10:11:12"]
- Configure then run transform.py:

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Python Programs

1. time_slices.py
    - Listens on a channel for intervals of time (e.g. 20 minutes) until the test duration (e.g. 18 hours) is complete
    - Files go into a directory marked with a date_time value based on when the time_slices.py program was executed
    - Utilizes dumpcap
2. mac_traces.py
    - Uses files from the packet capture directory produced by time_slices.py as input
    - Output is one file for each target MAC address that spans the entire test duration (e.g. 18 hours)
    - Output directory has same date_time value as input
    - Utilizes tshark, mergecap
3. transform.py
    - Uses files from the mac address capture directory produced by mac_traces.p as input
    - Transforms the *.pcapng files to text files with columns for particular protocol fields
    - Display filters determine the protocol fields exported to the text files
    - Utilizes tshark

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Exercise steps

1. Examine sample output
2. Use Wireshark to look for addition packets to remove from text output
3. Modify transform.py with new display filter
4. Re-run transform.py

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services

Thank You!

References:

tshark: https://www.wireshark.org/docs/man-pages/tshark.html
dumpcap: https://www.wireshark.org/docs/man-pages/dumpcap.html
mergecap: https://www.wireshark.org/docs/man-pages/mergecap.html
capture filters: https://wiki.wireshark.org/CaptureFilters, http://www.tcpdump.org/manpages/pcap-filter.7.html
display filters: https://www.wireshark.org/docs/man-pages/wireshark-filter.html

Useful AP: https://www.tp-link.com/us/products/details/cat-9_TL-WR802N.html

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws professional services