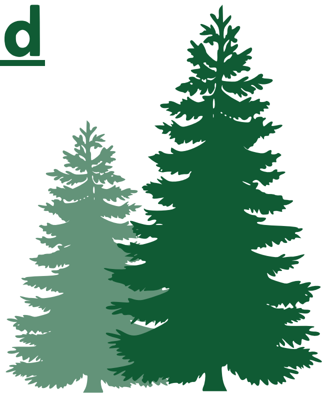
Additional Materials - Networking and Wireshark

The challenges under the "WPA2" category require a basic understanding of networking and wireshark.

First, if you never heard of or worked with packets and network traffic at all, don't worry! You can absolutely still participate in and enjoy the CTF. We are glad that we can be the ones to introduce you to this great topic :) Before you continue, you should read an introduction to networking and packets here.

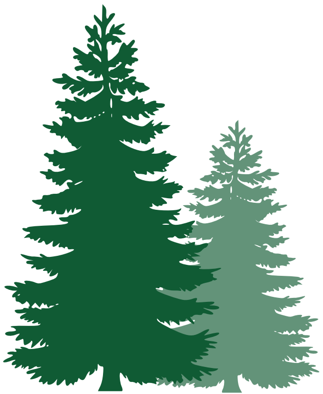


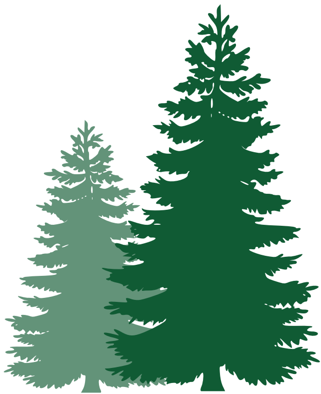
Additional Materials - Networking and Wireshark

Below, we provide you with only the necessary information about wireshark to be able complete our CTF.

As networking is a really interesting and important topic, we strongly encourage you to use this opportunity to study it further!

You can find a more detailed wireshark here.





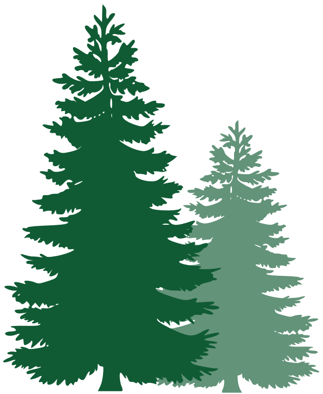
Wireshark Introduction

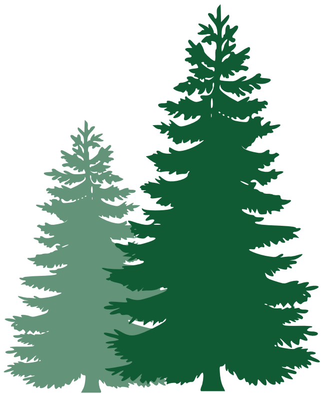
In our challenges, we provide you with .pcap files.

Pcap is a file format used to store network traffic data captured from a network interface. These files contain a detailed record of packets that have traversed the network, including their headers and payloads.

In our case, we provide you with captures of a connection to a wifi network, that used the WPA2 protocol, and ask you to analyze it.

Don’t worry! For the beginner level, we provided ONLY the 5 necessary packets to complete our challenges.



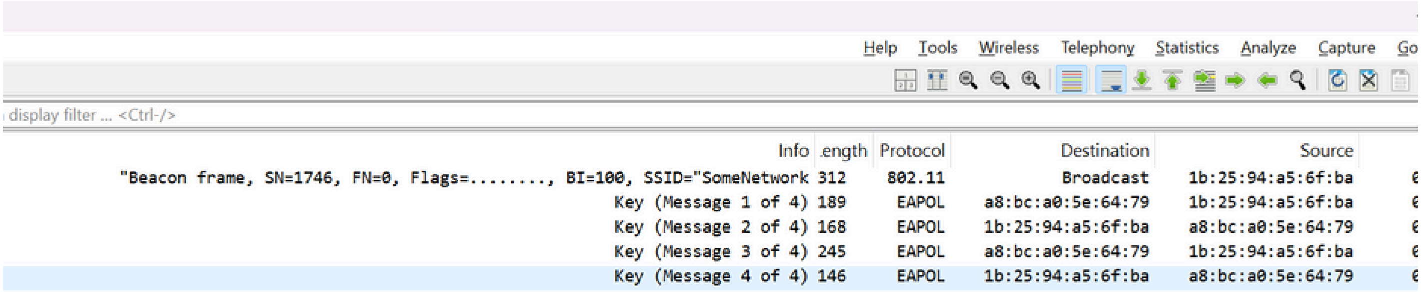


Downloading and Using Wireshark

First, download wireshark here.

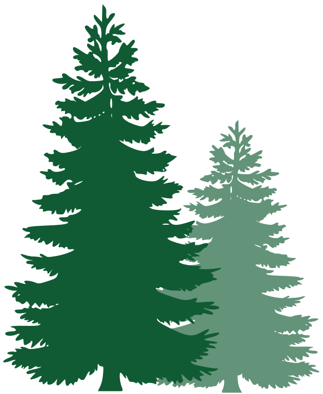
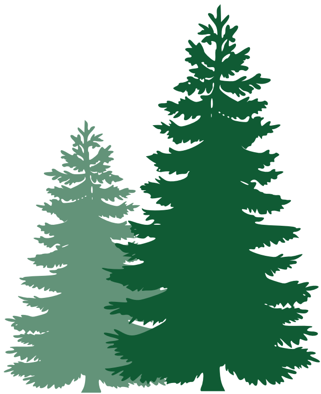
When you open the app, select File at the top corner, then Open, and choose the .pcap file in your challenge directory (each of the WPA2 category challenges should have a .pcap file).

Your screen should now look like this:



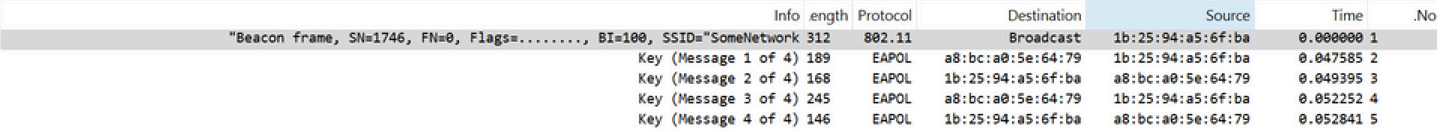
Info	ength	Protocol	Destination	Source	
"Beacon frame, SN=1746, FN=0, Flags=........, BI=100, SSID="SomeNetwork	312	802.11	Broadcast	1b:25:94:a5:6f:ba	6
Key (Message 1 of 4)	189	EAPOL	a8:bc:a0:5e:64:79	1b:25:94:a5:6f:ba	6
Key (Message 2 of 4)	168	EAPOL	1b:25:94:a5:6f:ba	a8:bc:a0:5e:64:79	6
Key (Message 3 of 4)	245	EAPOL	a8:bc:a0:5e:64:79	1b:25:94:a5:6f:ba	6
Key (Message 4 of 4)	146	EAPOL	1b:25:94:a5:6f:ba	a8:bc:a0:5e:64:79	6

and you should be able to see the 5 packets that we filtered out for you.

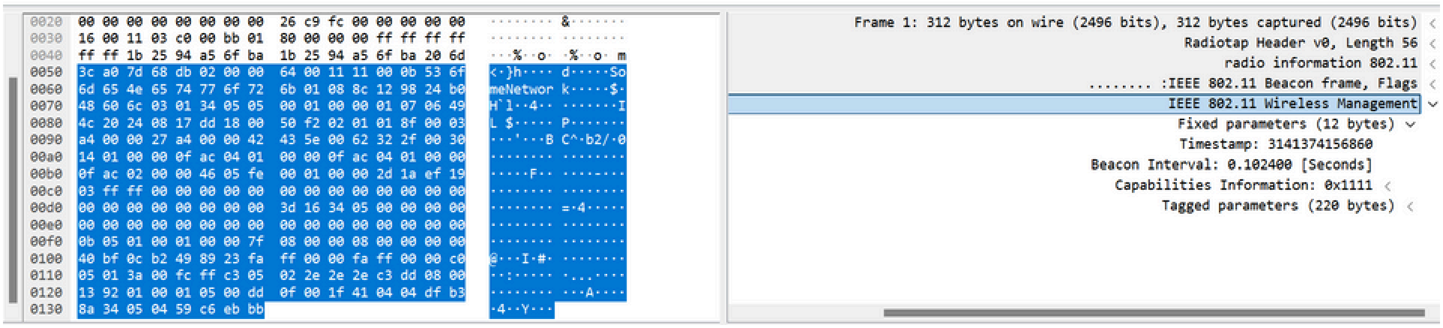



Downloading and Using Wireshark

Each row here is a packet. When you click on a packet, you should be able to see its fields and raw hex bytes below the packet list:

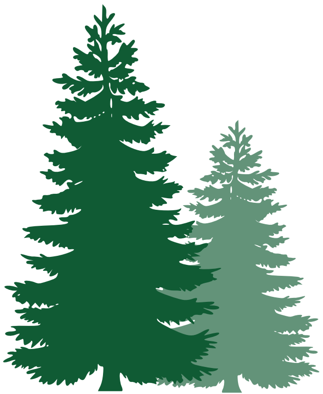


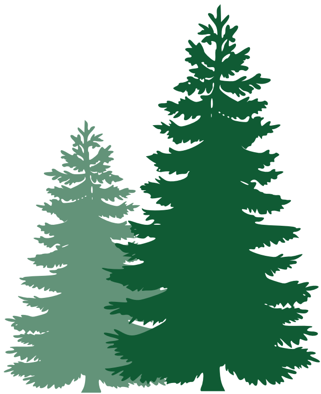
Info	ength	Protocol	Destination	Source	Time	.No
"Beacon frame, SN=1746, FN=0, Flags=........, BI=100, SSID="SomeNetwork	312	802.11	Broadcast	1b:25:94:a5:6f:ba	0.000000	1
Key (Message 1 of 4)	189	EAPOL	a8:bc:a0:5e:64:79	1b:25:94:a5:6f:ba	0.047585	2
Key (Message 2 of 4)	168	EAPOL	1b:25:94:a5:6f:ba	a8:bc:a0:5e:64:79	0.049395	3
Key (Message 3 of 4)	245	EAPOL	a8:bc:a0:5e:64:79	1b:25:94:a5:6f:ba	0.052252	4
Key (Message 4 of 4)	146	EAPOL	1b:25:94:a5:6f:ba	a8:bc:a0:5e:64:79	0.052841	5



```
0020  00 00 00 00 00 00 00 00  26 c9 fc 00 00 00 00 00   ········ &·······
0030  16 00 11 03 c0 00 bb 01  80 00 00 00 ff ff ff ff   ········ ········
0040  ff ff 1b 25 94 a5 6f ba  1b 25 94 a5 6f ba 20 6d   ···%··o· ·%··o· m
0050  3c a0 7d 68 db 02 00 00  64 00 11 11 00 0b 53 6f   <·}h···· d·····So
0060  6d 65 4e 65 74 77 6f 72  6b 01 08 8c 12 98 24 b0   meNetwor k·····$·
0070  48 60 6c 03 01 34 05 05  00 01 00 00 01 07 06 49   H`l··4·· ·······I
0080  4c 20 24 08 17 dd 18 00  50 f2 02 01 01 8f 00 03   L $····· P·······
0090  a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 30   ···'···B C^·b2/·0
00a0  14 01 00 00 0f ac 04 01  00 00 0f ac 04 01 00 00   ········ ········
00b0  0f ac 02 00 00 46 05 fe  00 01 00 00 2d 1a ef 19   ·····F·· ····-···
00c0  03 ff ff 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  3d 16 34 05 00 00 00 00   ········ =·4·····
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  0b 05 01 00 01 00 00 7f  08 00 00 08 00 00 00 00   ········ ········
0100  40 bf 0c b2 49 89 23 fa  ff 00 00 fa ff 00 00 c0   @···I·#· ········
0110  05 01 3a 00 fc ff c3 05  02 2e 2e 2e c3 dd 08 00   ··:····· ·...····
0120  13 92 01 00 01 05 00 dd  0f 00 1f 41 04 04 df b3   ········ ···A····
0130  8a 34 05 04 59 c6 eb bb                            ·4··Y···
```

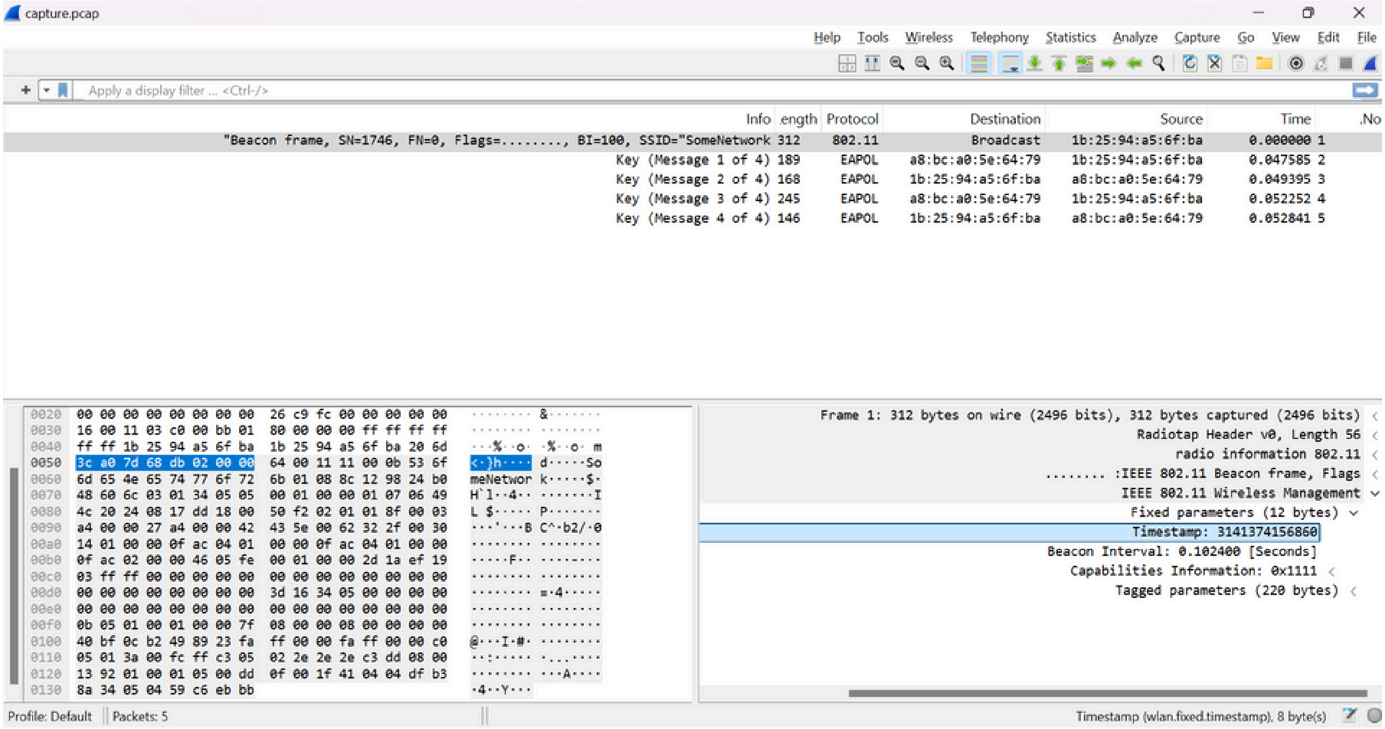
```
Frame 1: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) <
                                        Radiotap Header v0, Length 56 <
                                             radio information 802.11 <
                          ........ :IEEE 802.11 Beacon frame, Flags <
                                 IEEE 802.11 Wireless Management ⌄
                                      Fixed parameters (12 bytes) ⌄
                                      Timestamp: 3141374156860
                             Beacon Interval: 0.102400 [Seconds]
                                Capabilities Information: 0x1111 <
                                      Tagged parameters (220 bytes) <
```





Downloading and Using Wireshark

You can also select a specific field in the packet and see the raw bytes for this field only:


capture.pcap
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
Apply a display filter ... <Ctrl-/>

```
                                                         Info ength Protocol         Destination            Source          Time  .No
     "Beacon frame, SN=1746, FN=0, Flags=........, BI=100, SSID="SomeNetwork 312   802.11          Broadcast  1b:25:94:a5:6f:ba  0.000000 1
                                                       Key (Message 1 of 4) 189    EAPOL  a8:bc:a0:5e:64:79  1b:25:94:a5:6f:ba  0.047585 2
                                                       Key (Message 2 of 4) 168    EAPOL  1b:25:94:a5:6f:ba  a8:bc:a0:5e:64:79  0.049395 3
                                                       Key (Message 3 of 4) 245    EAPOL  a8:bc:a0:5e:64:79  1b:25:94:a5:6f:ba  0.052252 4
                                                       Key (Message 4 of 4) 146    EAPOL  1b:25:94:a5:6f:ba  a8:bc:a0:5e:64:79  0.052841 5
```

```
0020  00 00 00 00 00 00 00 00  26 c9 fc 00 00 00 00 00   ········ &·······
0030  16 00 11 03 c0 00 bb 01  80 00 00 00 ff ff ff ff   ········ ········
0040  ff ff 1b 25 94 a5 6f ba  1b 25 94 a5 6f ba 20 6d   ···%··o· ·%··o· m
0050  3c a0 7d 68 db 02 00 00  64 00 11 11 00 0b 53 6f   <·}h···· d·····So
0060  6d 65 4e 65 74 77 6f 72  6b 01 08 8c 12 98 24 b0   meNetwor k·····$·
0070  48 60 6c 03 01 34 05 05  00 01 00 00 01 07 06 49   H`l··4·· ·······I
0080  4c 20 24 08 17 dd 18 00  50 f2 02 01 01 8f 00 03   L $····· P·······
0090  a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 30   ···'···B C^·b2/·0
00a0  14 01 00 00 0f ac 04 01  00 00 0f ac 04 01 00 00   ········ ········
00b0  0f ac 02 00 00 46 05 fe  00 01 00 00 2d 1a ef 19   ·····F·· ····-···
00c0  03 ff ff 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  3d 16 34 05 00 00 00 00   ········ =·4·····
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  0b 05 01 00 01 00 00 7f  08 00 00 08 00 00 00 00   ········ ········
0100  40 bf 0c b2 49 89 23 fa  ff 00 00 fa ff 00 00 c0   @···I·#· ········
0110  05 01 3a 00 fc ff c3 05  02 2e 2e 2e c3 dd 08 00   ··:····· ·...····
0120  13 92 01 00 01 05 00 dd  0f 00 1f 41 04 04 df b3   ········ ···A····
0130  8a 34 05 04 59 c6 eb bb                            ·4··Y···
```

```
Frame 1: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) <
                                          Radiotap Header v0, Length 56 <
                                              radio information 802.11 <
                                ........ :IEEE 802.11 Beacon frame, Flags <
                                     IEEE 802.11 Wireless Management ⌄
                                          Fixed parameters (12 bytes) ⌄
                                          Timestamp: 3141374156860
                                  Beacon Interval: 0.102400 [Seconds]
                                   Capabilities Information: 0x1111 <
                                          Tagged parameters (220 bytes) <
```

If you right click a certain field, you can use "Copy" and then "as C string" to copy the field to your C code, for example as a constant in your code.

If you face any trouble with wireshark during the challenges, or have any questions, feel free to ask us!