Wireshark: Network analysis and interception

UC Davis Cybersecurity Club
Nate Buttke

February 24, 2022

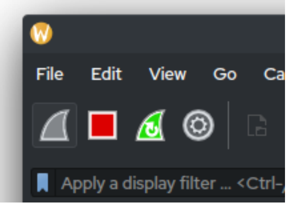
What is Wireshark?

- Free (GPLv2) network analysis software. Implementation of `libpcap`, which is also used by nmap.
- "Promiscuous mode" allows Wireshark to work on insecure routers, like most consumer routers.[1] An interface in this mode *asks* the router for all of the network's traffic.
- In more sophisticated man-in-the-middle attacks, a device running Wireshark can pretend to be the router.

[1] like the one I bought for today

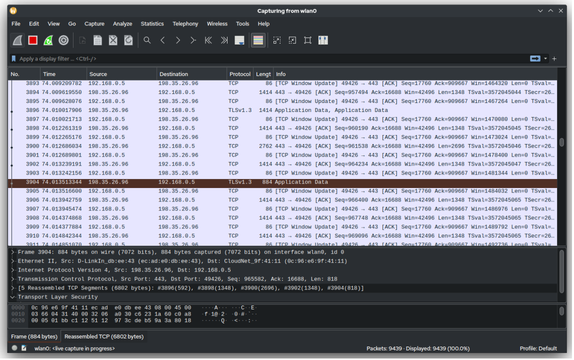
Wireshark setup

- In Kali Linux, Wireshark should be ready for use.
- In general, select the interface that has the most traffic, or the one that you know is connected to the network of interest.
- Control packet capture using these buttons:



Apply a display filter ... <Ctrl-/

Wireshark tour



No.	Time	Source	Destination	Protocol	Lengt	Info
3893	74.009209782	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1464320 Len=0 TSval=…
3894	74.009619550	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=957494 Ack=16688 Win=42496 Len=1348 TSval=3572045044 TSecr=26…
3895	74.009628076	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1467264 Len=0 TSval=…
3896	74.010017906	198.35.26.96	192.168.0.5	TLSv1.3	1414	Application Data, Application Data
3897	74.010021713	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1470080 Len=0 TSval=…
3898	74.012261319	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=960190 Ack=16688 Win=42496 Len=1348 TSval=3572045045 TSecr=26…
3899	74.012265176	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1473024 Len=0 TSval=…
3900	74.012686034	198.35.26.96	192.168.0.5	TCP	2762	443 → 49426 [ACK] Seq=961538 Ack=16688 Win=42496 Len=2696 TSval=3572045046 TSecr=26…
3901	74.012689801	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1478400 Len=0 TSval=…
3902	74.013239191	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=964234 Ack=16688 Win=42496 Len=1348 TSval=3572045047 TSecr=26…
3903	74.013242156	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1481344 Len=0 TSval=…
3904	74.013513344	198.35.26.96	192.168.0.5	TLSv1.3	884	Application Data
3905	74.013516600	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1484032 Len=0 TSval=…
3906	74.013942759	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=966400 Ack=16688 Win=42496 Len=1348 TSval=3572045065 TSecr=26…
3907	74.013945474	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1486976 Len=0 TSval=…
3908	74.014374868	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=967748 Ack=16688 Win=42496 Len=1348 TSval=3572045065 TSecr=26…
3909	74.014377884	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1489792 Len=0 TSval=…
3910	74.014842344	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=969096 Ack=16688 Win=42496 Len=1348 TSval=3572045065 TSecr=26…
3911	74.014851070	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1492736 Len=0 TSval=…

```
> Frame 3904: 884 bytes on wire (7072 bits), 884 bytes captured (7072 bits) on interface wlan0, id 0
> Ethernet II, Src: D-LinkIn_db:ee:43 (ec:ad:e0:db:ee:43), Dst: CloudNet_9f:41:11 (0c:96:e6:9f:41:11)
> Internet Protocol Version 4, Src: 198.35.26.96, Dst: 192.168.0.5
> Transmission Control Protocol, Src Port: 443, Dst Port: 49426, Seq: 965582, Ack: 16688, Len: 818
> [5 Reassembled TCP Segments (6802 bytes): #3896(592), #3898(1348), #3900(2696), #3902(1348), #3904(818)]
v Transport Layer Security
```

```
0000  0c 96 e6 9f 41 11 ec ad  e0 db ee 43 08 00 45 00   ····A··· ···C··E·
0010  03 66 04 31 40 00 32 06  a0 30 c6 23 1a 60 c0 a8   ·f·1@·2· ·0·#·`··
0020  00 05 01 bb c1 12 51 12  97 3c de b5 9a 3a 80 18   ······Q· ·<···:··
```

Frame (884 bytes)
Reassembled TCP (6802 bytes)
wlan0: <live capture in progress>
Packets: 9439 · Displayed: 9439 (100.0%)
Profile: Default

- The middle table shows all captured packets and can be sorted and filtered. Click column titles to sort by ascending or descending
- Filters auto-fill with suggestions. Protocols like DHCP have filters.
- Below the table, information is shown about the current packet.
- Hover over protocol-specific info to see corresponding bytes.

Warm-up: which device is the router?

Can you use the protocols and destinations of the captured packets to discern which device is the router?

Warm-up: who is the programmer pinging?

You are in the offices of a technology company, and have caught word that one of their programmers is working on a new webserver. You know the programmer's ip address is `192.168.1.131`.
The same programmer uses ssh to compile software on another machine. Can you tell which machine?

What is the password?

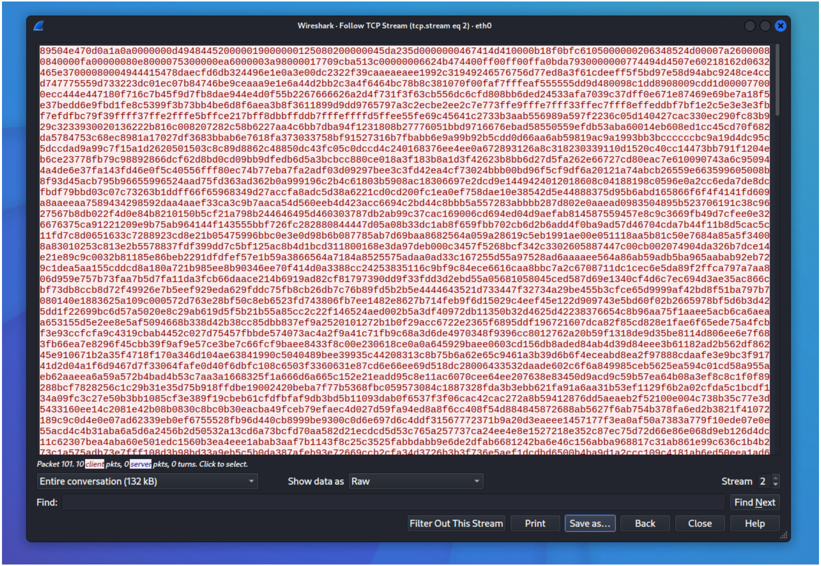
In another department, a team of programmers is devoloping a controversial new social media platform. It's password-protected, but you may be able to discern the password because SSL is not being used.

1. Can you intercept the HTML without the password?
2. What is the password? Now log in.

Steal files

An organization claims to have a proof of Poincare's Conjecture, a Millennium Prize Problem, on its **ftp** server. It could be worth one million dollars. Who is the author of the alleged proof?

Steal files (how to solve it)



Wireshark · Follow TCP Stream (tcp.stream eq 2) · eth0

```
89504e470d0a1a0a0000000d494844520000019000000125080200000045da235d0000000467414d410000b18f0bfc61050000002063 48524d00007a2600008
0840000fa00000080e8000075300000ea6000003a98000017709cba513c00000006624b474400ff00ff00ffa0bda7930000000774494d4507e60218162d0632
465e37000080004944415478daecfd6db324496e1e0a3e00dc2322f39caaeaeaee1992c31949246576756d77ed8a3f61cdeeff5f5bd97e58d94abc9248ce4cc
d747775559d733223dc01ec07b84746be9ceaaa9e1e6a44d2bb2c3a4f6464bc78b8c381070f00faf7fffeaf555555dd9d480098c1dd8908009cdd1d00007700
0ecc444e447180f716c7b45f9d7fb8dae944e4d0f55b2267666626a2d4f731f3f63cb556dc6cfd808bb6ded24533afa7039c37dff0e671e87469e69be7a18f5
e37bedd6e9fbd1fe8c5399f3b73bb4be6d8f6aea3b8f3611899d9dd9765797a3c2ecbe2ee2c7e773ffe9fffe7fff33ffec7fff8effeddbf7bf1e2c5e3e3e3fb
f7efdfbc79f39ffff37ffe2fffe5bffce217bff8dbbffddb7fffeffffd5ffee55fe69c45641c2733b3aab556989a597f2236c05d140427cac330ec290fc83b9
29c3233930020136222b816c008207282c58b6227aa4c6bb7dba94f1231808b27776051bbd9716676ebad58550559efdb53aba60014eb608ed1cc45cd70f682
da5784753c68ec8981a17027df3683bbab6e7618fa373033758bf91527316b7fbabb6e9a99b92b5cdd0d66aa6ab59819ac9a1993bb3bccccccbc9a19d4dc95c
5dccdad9a99c7f15a1d2620501503c8c89d8862c48850dc43fc05c0dccd4c240168376ee4ee0a672893126a8c318230339110d1520c40cc14473bb791f1204e
b6ce23778fb79c98892866dcf62d8bd0cd09bb9dfedb6d5a3bcbcc880ce018a3f183b8a1d3f42623b8bb6d27d5fa262e66727cd80eac7e610090743a6c95094
4a4de6e37fa143fd46e0f5c40556fff80ec74b77eba7fa2adf03d09297bee3c3fd42ea4cf73024bbb00bd96f5cf9df6a20121a74abcb26559e663599605008b
8f93d45acb795b96655996524aad75fd363ad362b0a999196c2b4c61803b5908ac18306697e2dcd9e1449424012018608c04188198c0596e0a2cc6eda7de8dc
fbdf79bbd03c07c73263b1ddff66f65968349d27accfa8adc5d38a6221cd0cd200fc1ea0ef758dae10e38542d5e44888375d95b6abd165866f6f4f4141fd609
a8aaeeaa7589434298592daa4aaef33ca3c9b7aaca54d560eeb4d423acc6694c2bd44c8bbb5a557283abbbb287d802e0aaead0983504895b523706191c38c96
27567b8db022f4d0e84b8210150b5cf21a798b244646495d460303787db2ab99c37cac169006cd694ed04d9aefab814587559457e8c9c3669fb49d7cfee0e32
6676375ca91221209e9b75ab964144f143555bbf726fc282880844447d05a08b33dc1ab8f659fbb702cb6d2b6add4f0ba9ad57d46704cda7b44f11b8d5cac5c
11fd7c8d0651633c7288923cd8e21b05475996bbc0e3e0d98b6b087785ab7d69baa8682564a059a28619c5eb1991ae00e051118aa5b81c50e7684a85a5f3400
8a83010253c813e2b5578837fdf399dd7c5bf125ac8b4d1bcd311800168e3da97deb000c3457f5268bcf342c3302605887447c00cb002074904da326b7dce14
e21e89c9c0032b81185e86beb2291dfdfef57e1b59a3866564a7184a8525575adaa0ad33c167255d55a97528ad6aaaaee564a86ab59adb5ba965aabab92eb72
9c1dea5aa155cddcd8a180a721b985ee8b90346ee70f414d0a3388cc24253835116c9bf9c84ece6616caa8bbc7a2c6708711dc1cec6e5da89f2ffca797a7aa8
06d959e757b73faa7b5d7fa11da3fcb66daace214b6919ad82cf81797390dd9f33fdd3d2ebd55a05681058045ced587d69e1340cf4d6c7ec694d3ae35ac866c
bf73db8ccb8d72f49926e7b5eef929eda629fddc75fb8cb26db7c76b89fd5b2b5e4444643521d733447f32734a29be455b3cfce65d9999af42bd8f51ba797b7
080140e1883625a109c000572d763e28bf50c8eb6523fd743806fb7ee1482e8627b714feb9f6d15029c4eef45e122d909743e5bd60f02b2665978bf5d6b3d42
5dd1f22699bc6d57a5020e8c29ab619d5f5b21b55a85cc2c22f146524aed002b5a3df40972db11350b32d4625d42238376654c8b96aa75f1aaee5acb6ca6aea
a653155d5e2ee8e5af5094668b338d42b38cc85dbb837ef9a2520101272b1b0f29acc6722e2365f6895ddf196721607dca82f85cd828e1fae6f65ede75a4fcb
f3e93ccfcfa9c4319cbab4452c027d75457fbbde574073ac4a2f9a41c71fb9c68a3d6de4970348f9396cc8012762a20b59f1318de9d35be8114d806ee6e7f68
3fb66ea7e8296f45cbb39f9af9e57ce3be7c66fcf9baee8433f8c00e230618ce0a0a645929baee0603cd156db8aded84ab4d39d84eee3b61182ad2b562df862
45e910671b2a35f4718f170a346d104ae63841990c5040489bee39935c44208313c8b75b6a62e65c9461a3b39d6b6f4eceabd8ea2f97888cdaafe3e9bc3f917
41d2d04a1f6d9467d7f33064fafe0d40f6dbfc108c6503f3360631e87cd6e66ee69d518dc28006433532daade602c6f6a849985ceb5625ea594c01cd58a955a
eb62aaeea6a59a572b4bad4b53c7aa3a1668325f1a666d6a665c152e21eadd95c8e11ac6070cee64ee207638e83450d9acd9c59b57ea64b08a3ef8c8c1f0f89
288bcf7828256c1c29b31e35d75b918ffdbe19002420beba7f77b5368fbc059573084c1887328fda3b3ebb621fa91a6aa31b53ef1129f6b2a02cfda5c1bcdf1
34a09fc3c27e50b3bb1085cf3e389f19cbeb61cfdfbfaf9db3bd5b11093dab0f6537f3f06cac42cac272a8b59412876dd5aeaeb2f52100e004c738b35c77e3d
5433160ee14c2081e42b08b0830c8bc0b30eacba49fceb79efaec4d027d59fa94ed8a8f6cc408f54d884845872688ab5627f6ab754b378fa6ed2b3821f41072
189c9c0d4e0e07ad62339eb0ef6755528fb96d440cb8999be9300c0d6e697d6c4ddf31567772371b9a20d3eaeee1457177f3ea0af50a7383a779f10ede07e0e
55acd4c4b31aba6a5d6a2456b2d50532a13cd6a73bcfd70aa582d21ecdcd5d53c765a257737ca24ee4e8e1527218e352c87ec75d72d66e86e068d9eb126d4dc
11c62307bea4aba60e501edc1560b3ea4eee1abab3aaf7b1143f8c25c3525fabbdabb9e6de2dfab6681242ba6e46c156abba968817c31ab861e99c636c1b4b2
73c1a575adb73e7fff108d3b98bd33a9eb5c5b0da387afeb93e72669ccb2cfa34d3726b3b3f736e5aef1dcdbd6500b4ba9d1a2ccc109c4181ab6ed50eea1ad6
```

Packet 101. 10 client pkts, 0 server pkts, 0 turns. Click to select.

Entire conversation (132 kB)

Show data as Raw

Stream 2

Find:

Bonus: find the Tor user

Some students at your university are abusing Tor. If you can find that only one student was using Tor at the time of a crime, you may have evidence of against them.

- Can you tell that someone is using Tor?
- If so, does a bridge look different?