AcCCS Hands-on Exercise 1 – EVSE and PEV Communications (Simulation)

Scenario

During this exercise you will use an AcCCS system to simulate and examine the communications between an EVSE and a PEV. The AcCCS system is capable of operating as either or both of these systems, so you will divide your group into two sub-groups (team 1 and team 2). One group will play the role of the EVSE and the other will act as the PEV.

Objective

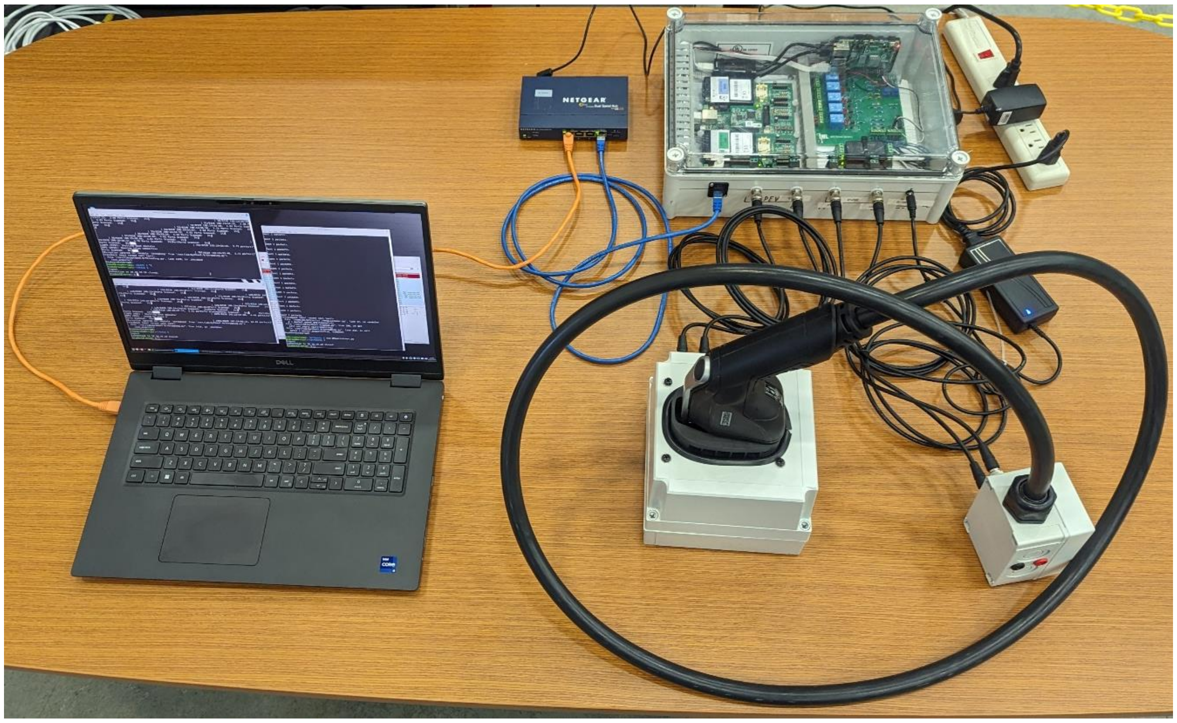
This exercise will allow you to observe the typical behavior of CCS communications and allow you to analyze how this process operates. You will also get some experience using the AcCCS system to further investigate the network connection between the PEV and EVSE.

Preparation

You will need a team of 2-6 people to form two different groups (PEV and EVSE). You will need two laptops, one for each of the teams. Power on the AcCCS system and the small network switch. Connect the laptops to the network switch.

Exercise Steps

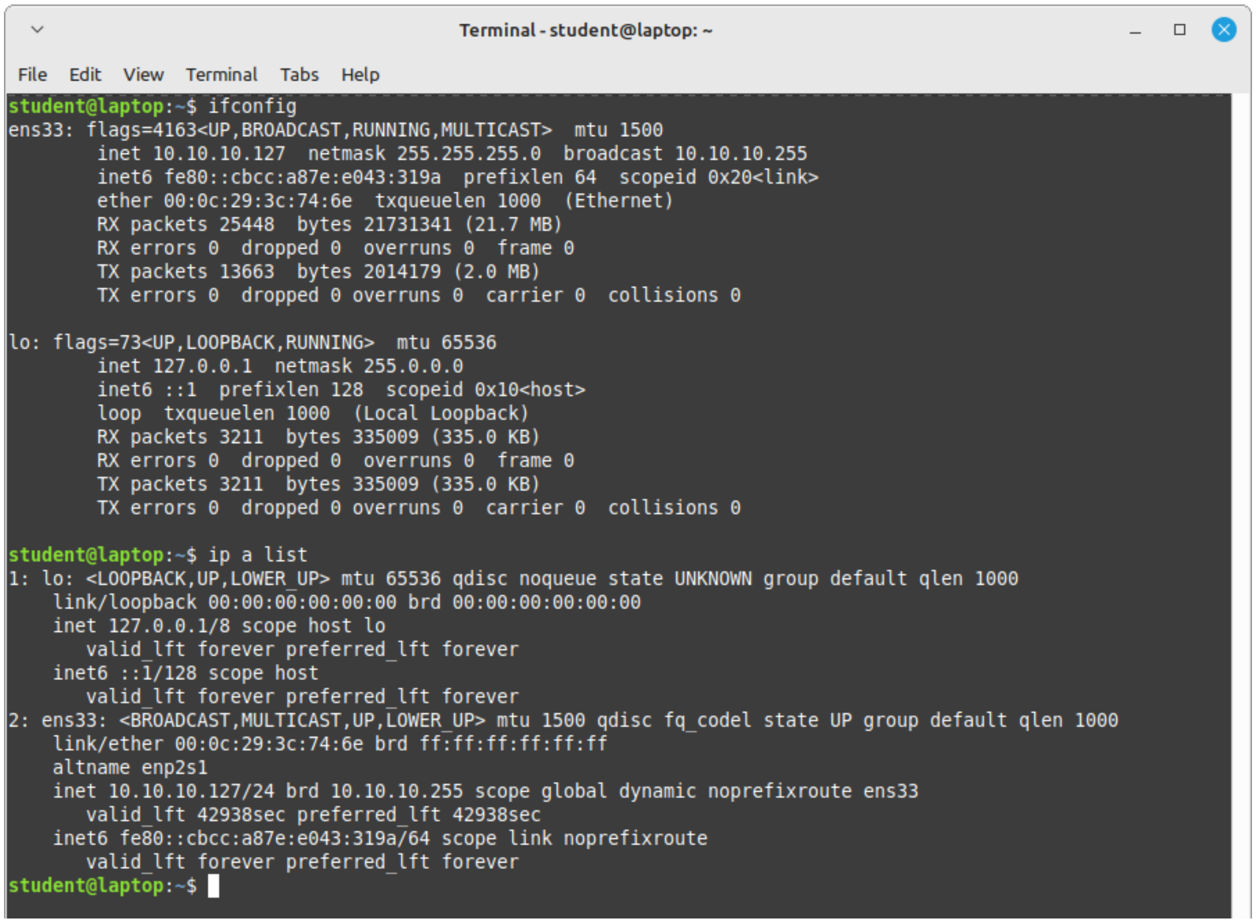
Step 1: Connect the AcCCS box to the provided 12v power supply. Connect the network switch to its power supply and use the short network cable to connect the network switch to the AcCCS box. Connect two laptops to the network switch. Your exercise setup should look something like the following picture.



Note: For this exercise you do not need the inlet port and cordset. You can simply connect the proximity pins and the control pilot ports together with two BNC cables.

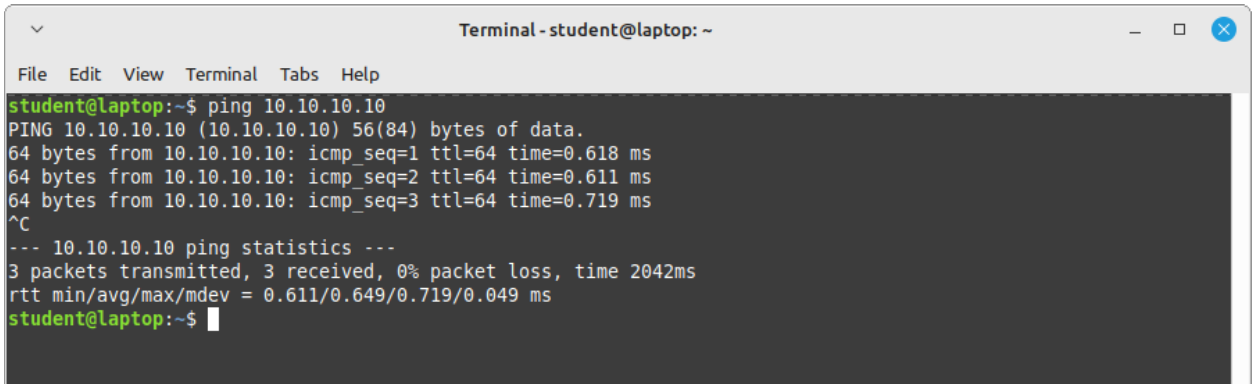
Step 2: Start VMWare Player and power on the provided virtual machine (VM). Log on to the VM using the provided account (user: student, password: password).

Step 3: Verify the VM has received an appropriate IP address from the AcCCS box. The AcCCS box provides IPv4 addresses using DHCP, and your address should reside in the 10.10.10.0/24 address space (e.g. 10.10.10.100, 10.10.10.101, etc.). You can do this by starting a terminal window and using the `ifconfig` command or the `ip` command.


Terminal - student@laptop: ~

```
student@laptop:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.127  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::cbcc:a87e:e043:319a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3c:74:6e  txqueuelen 1000  (Ethernet)
        RX packets 25448  bytes 21731341 (21.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13663  bytes 2014179 (2.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3211  bytes 335009 (335.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3211  bytes 335009 (335.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@laptop:~$ ip a list
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3c:74:6e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.10.10.127/24 brd 10.10.10.255 scope global dynamic noprefixroute ens33
       valid_lft 42938sec preferred_lft 42938sec
    inet6 fe80::cbcc:a87e:e043:319a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
student@laptop:~$
```

Step 4: Ping the Raspberry Pi in the AcCCS box to ensure you have a working network connection.

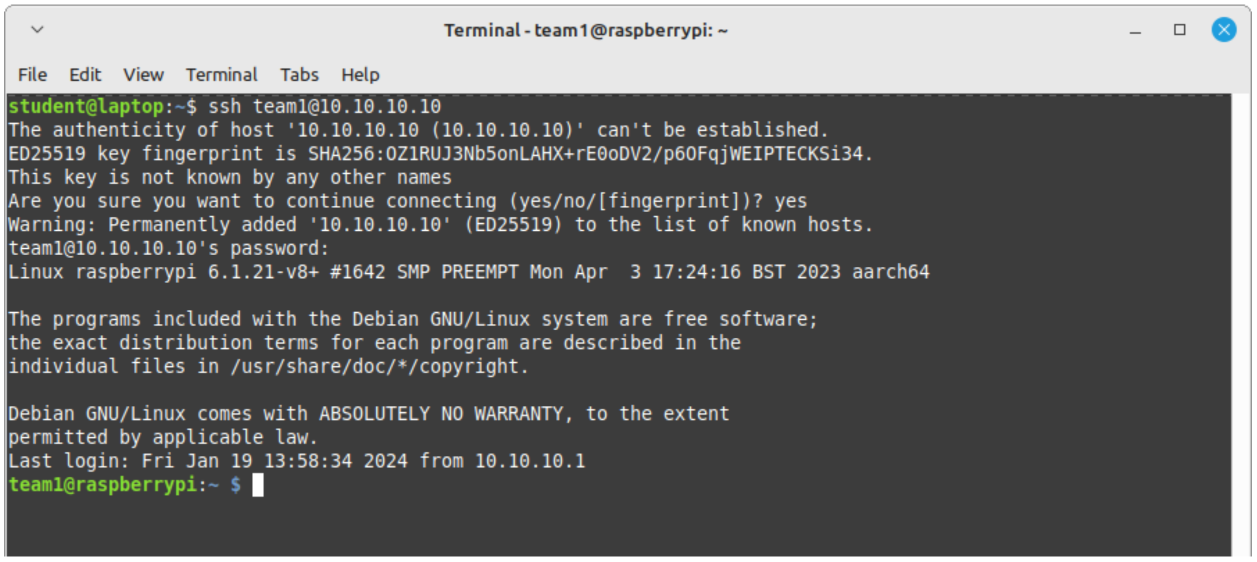

Terminal - student@laptop: ~

```
student@laptop:~$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.618 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.611 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.719 ms
^C
--- 10.10.10.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.611/0.649/0.719/0.049 ms
student@laptop:~$
```

Press Ctrl+C to stop the ping command.

Step 5: Each team will connect to the Raspberry Pi using SSH. The user account for Team 1 is **team1** and for Team 2, **team2** and the password for each team account is “AcCCS”.

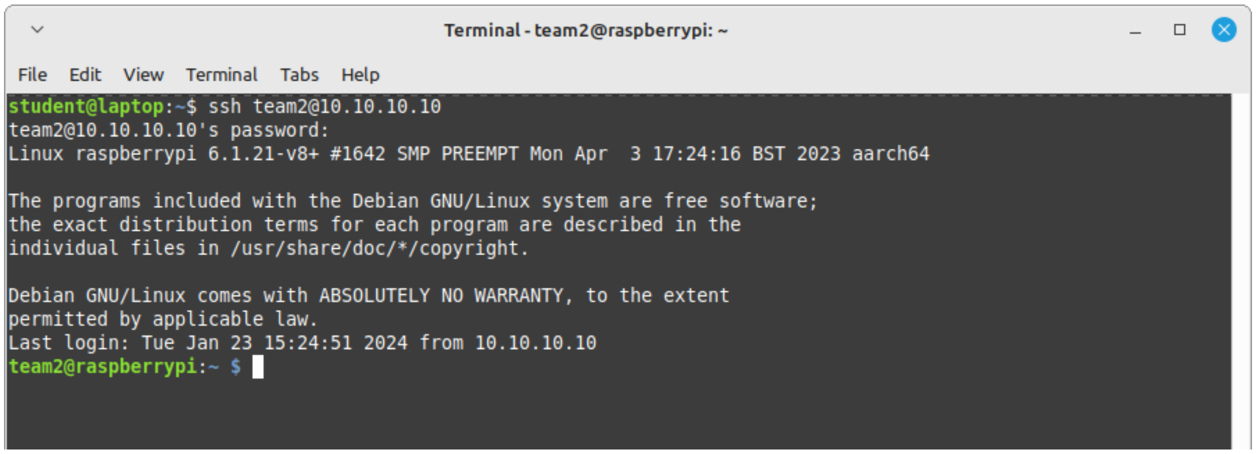
Team 1 (EVSE):


Terminal - team1@raspberrypi: ~
File Edit View Terminal Tabs Help

```
student@laptop:~$ ssh team1@10.10.10.10
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
ED25519 key fingerprint is SHA256:OZ1RUJ3Nb5onLAHX+rE0oDV2/p6OFqjWEIPTECKSi34.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.10' (ED25519) to the list of known hosts.
team1@10.10.10.10's password:
Linux raspberrypi 6.1.21-v8+ #1642 SMP PREEMPT Mon Apr  3 17:24:16 BST 2023 aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 19 13:58:34 2024 from 10.10.10.1
team1@raspberrypi:~ $
```

Note: If you receive a message asking you to confirm the SSH connection based on the SHA256 fingerprint, type ‘yes’ in the terminal to continue.

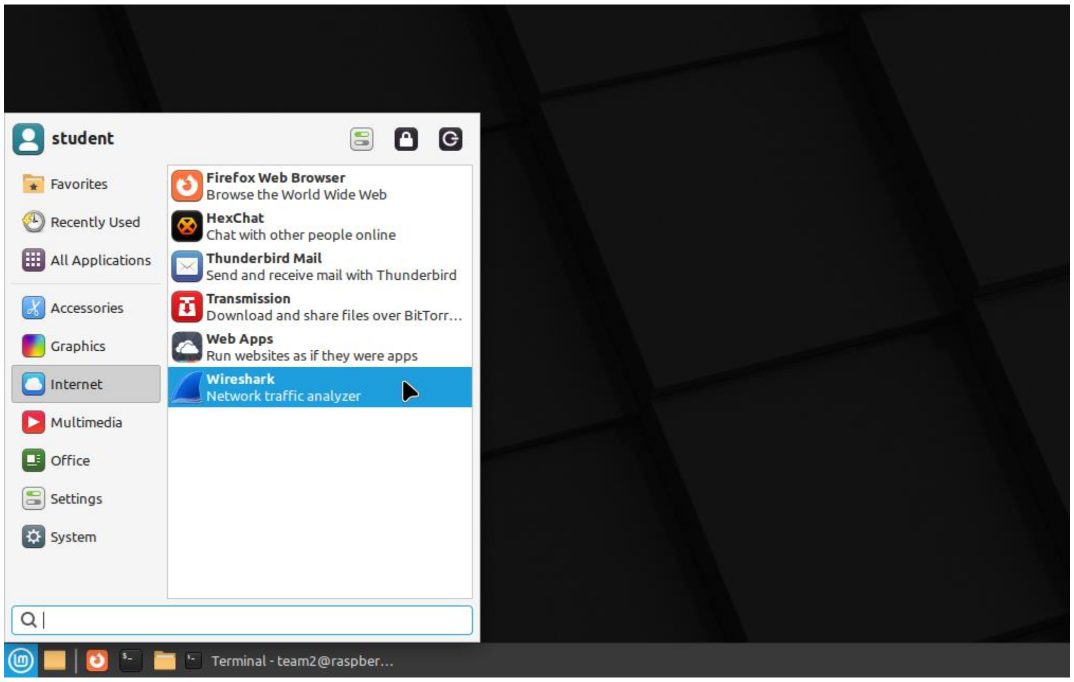
Team 2 (PEV):


Terminal - team2@raspberrypi: ~
File Edit View Terminal Tabs Help

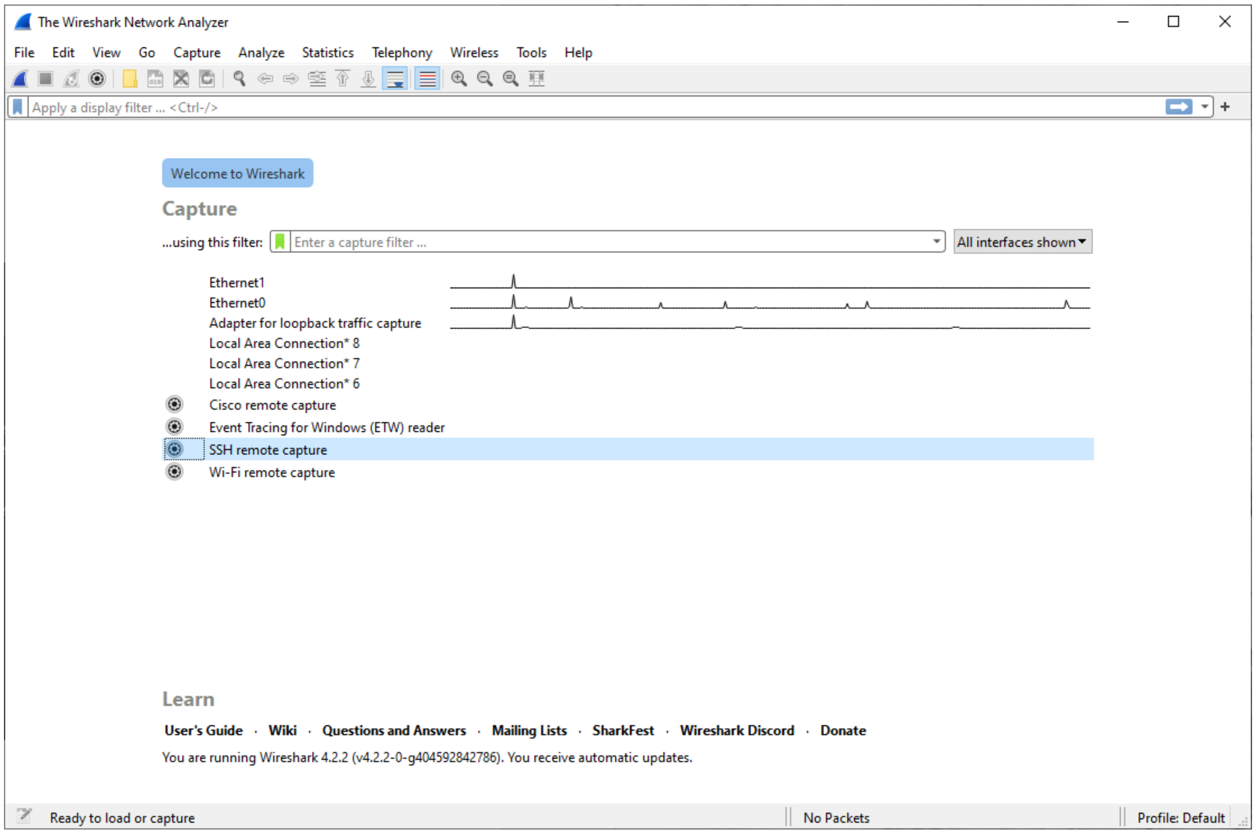
```
student@laptop:~$ ssh team2@10.10.10.10
team2@10.10.10.10's password:
Linux raspberrypi 6.1.21-v8+ #1642 SMP PREEMPT Mon Apr  3 17:24:16 BST 2023 aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan 23 15:24:51 2024 from 10.10.10.10
team2@raspberrypi:~ $
```

Step 6: Start Wireshark in each of the team VMs (team 1 watches one Wireshark and team 2 watches the other). We will use Wireshark to remotely monitor the communications from the Raspberry Pi and monitor the CCS (HomePlug GreenPHY) packets between the EVSE and PEV emulators.

Click on the taskbar menu in the VM, select Internet, and then click on Wireshark.

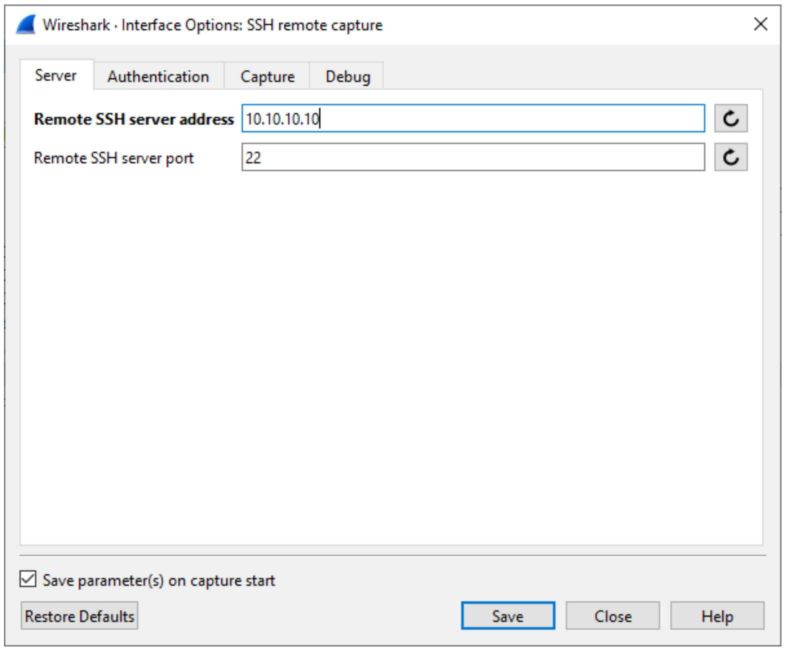


Click the gear (settings) icon next to the "SSH remote capture" interface.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Ethernet1
Ethernet0
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Cisco remote capture
Event Tracing for Windows (ETW) reader
SSH remote capture
Wi-Fi remote capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default

You are running Wireshark 4.2.2 (v4.2.2-0-g404592842786). You receive automatic updates.

On the Server tab, enter "10.10.10.10" for the remote SSH server address.

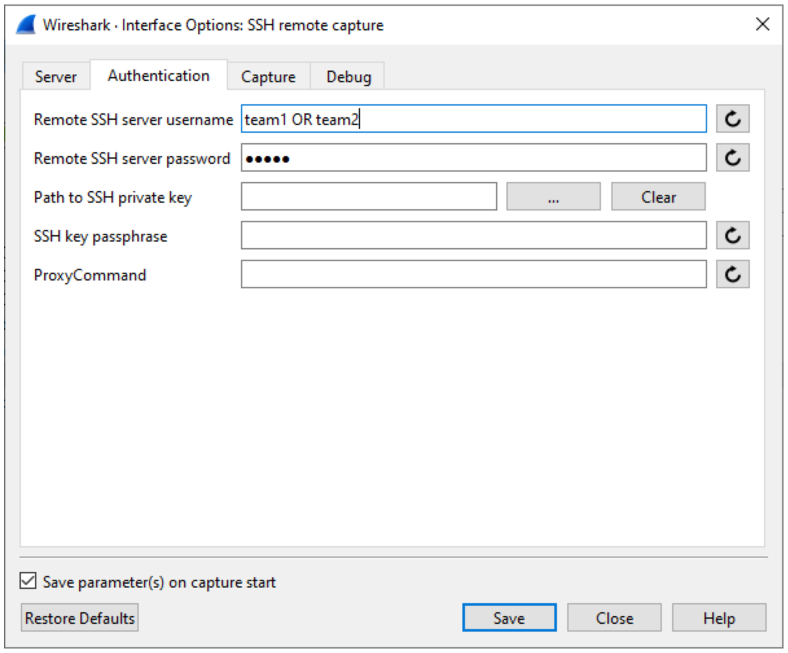


Remote SSH server address 10.10.10.10

Remote SSH server port 22

☑ Save parameter(s) on capture start

On the Authentication tab, enter your team username and password (AcCCS) as appropriate.



Remote SSH server username team1 OR team2

Remote SSH server password •••••

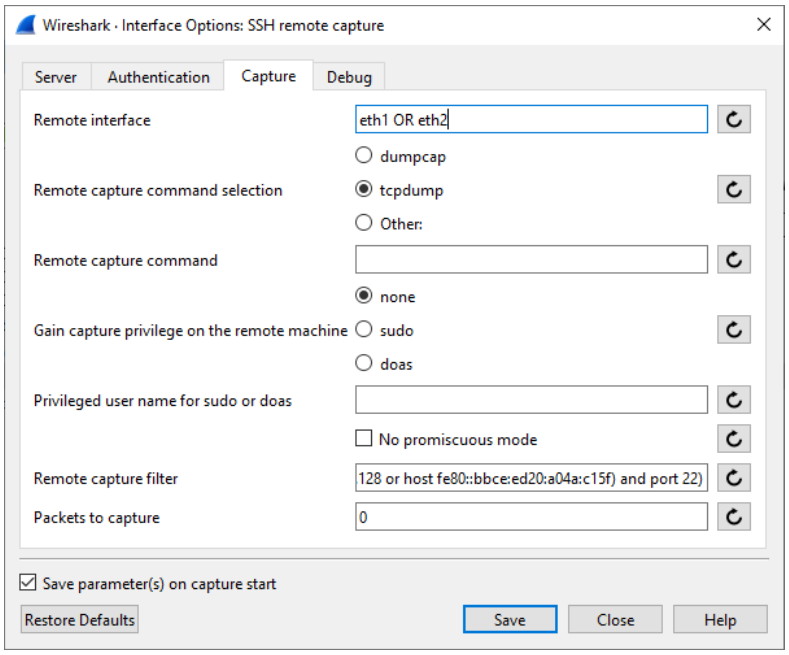
Path to SSH private key

SSH key passphrase

ProxyCommand

☑ Save parameter(s) on capture start

On the Capture tab, enter the appropriate interface name for your team. Team1 will emulate an EVSE and will use network interface **`eth1`** while Team2 will emulate the PEV using **`eth2`**.


Wireshark · Interface Options: SSH remote capture

Server | Authentication | Capture | Debug

Remote interface: eth1 OR eth2

Remote capture command selection: ( ) dumpcap [✓ tcpdump] ( ) Other:

Remote capture command:

Gain capture privilege on the remote machine: [✓ none] ( ) sudo ( ) doas

Privileged user name for sudo or doas:

☐ No promiscuous mode

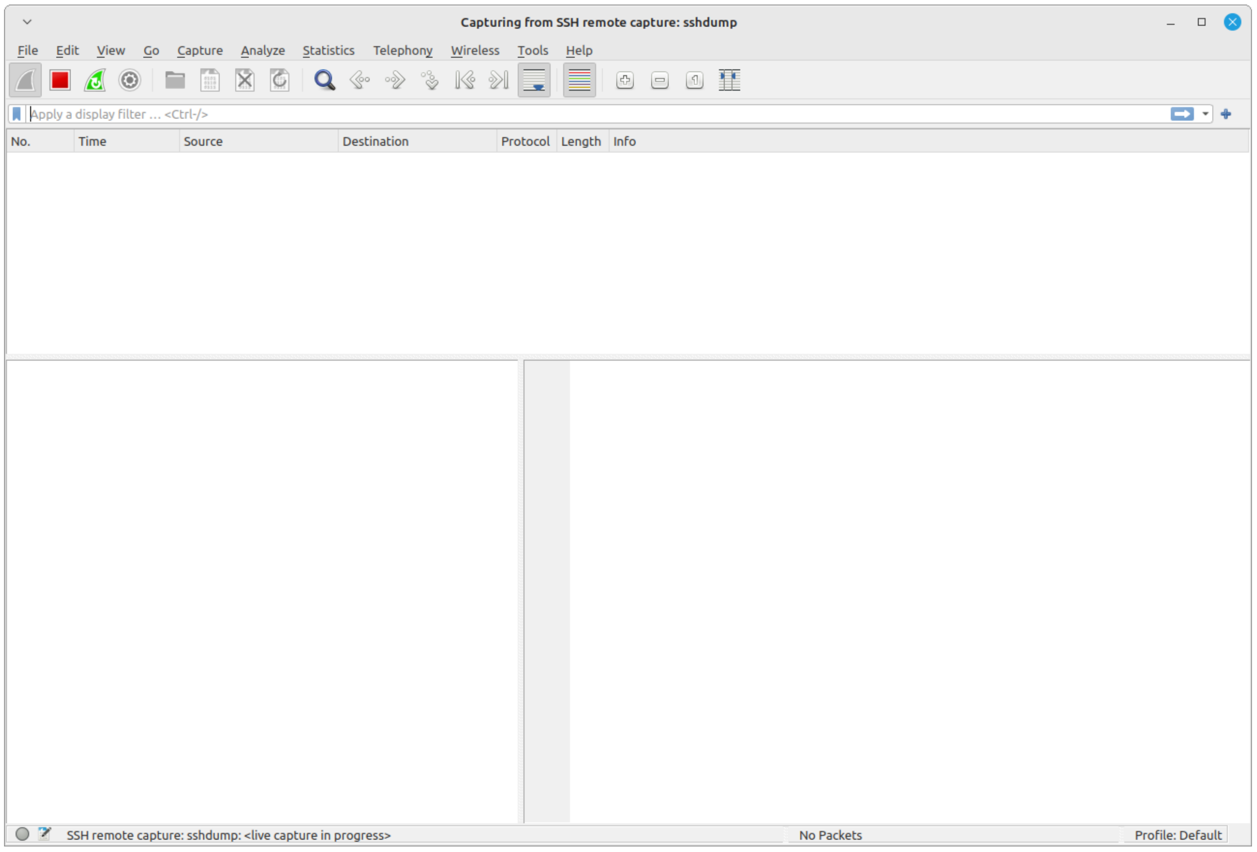
Remote capture filter: 128 or host fe80::bbce:ed20:a04a:c15f) and port 22)

Packets to capture: 0

☑ Save parameter(s) on capture start

Click the save button.

Step 7: Start a Wireshark capture by double-clicking the SSH remote capture interface. If your configuration settings are correct, Wireshark will start with an empty screen.


Capturing from SSH remote capture: sshdump

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info

SSH remote capture: sshdump: <live capture in progress>

No Packets

Profile: Default

Step 8: Start running the EVSE and PEV emulators. Each team has a few steps to execute to properly establish the connection. **Study these steps first** and then execute them at the same time. The two emulators may fail to connect at first, but they will retry the connection periodically.

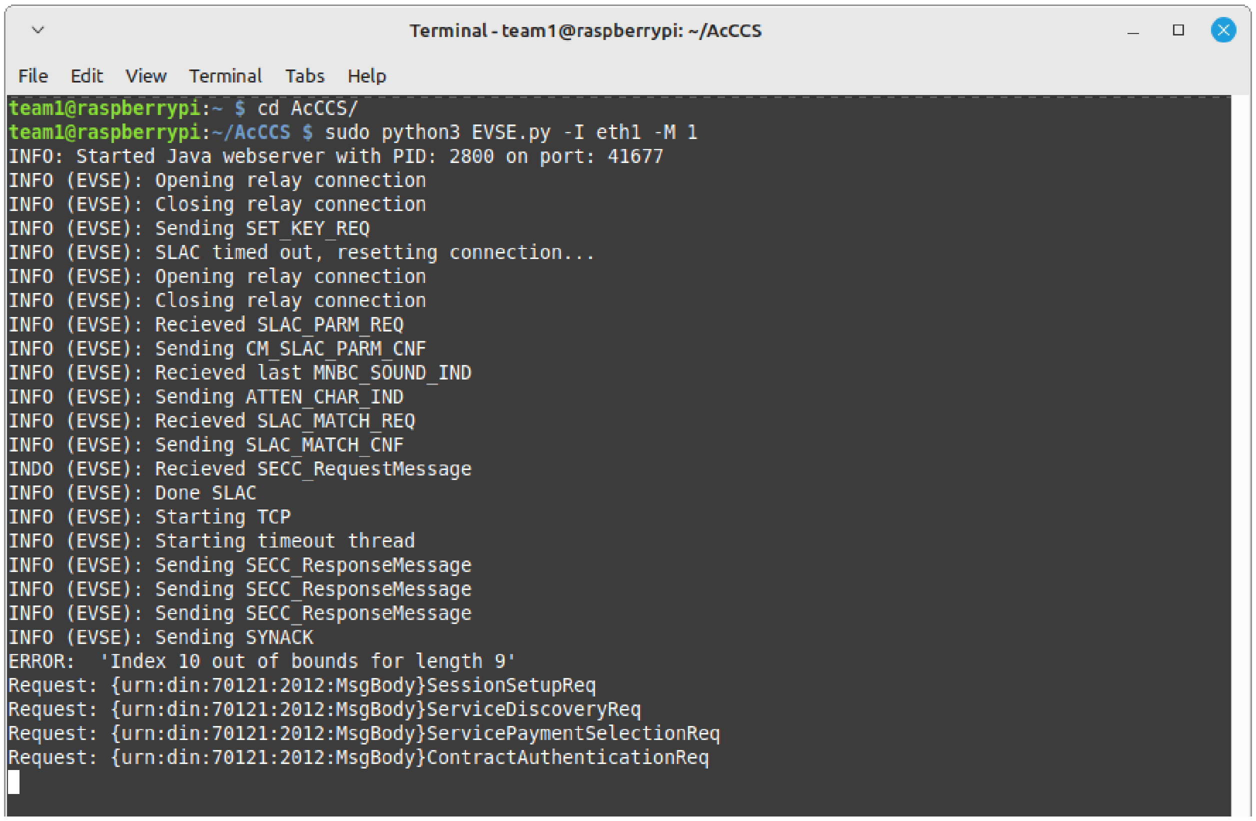
a. Team 1 only:

The EVSE emulator script has several command-line options. Below is a description of each of these options:

```
usage: EVSE.py [-h] [-M MODE] [-I INTERFACE] [--source-mac SOURCE_MAC] [--source-ip SOURCE_IP]
[--source-port SOURCE_PORT] [--NID NID] [--NMK NMK] [-p PROTOCOL] [--nmap-mac NMAP_MAC]
[--nmap-ip NMAP_IP] [--nmap-ports NMAP_PORTS]

EVSE emulator for AcCCS

optional arguments:
  -h, --help            show this help message and exit
  -M MODE, --mode MODE  Mode for emulator to run in: 0 for full conversation, 1 for stalling the
conversation, 2 for portscanning (default: 0)
  -I INTERFACE, --interface INTERFACE Ethernet interface to send/recieve packets on (default: eth1)
  --source-mac SOURCE_MAC Source MAC address of packets (default: 00:1e:c0:f2:6c:a0)
  --source-ip SOURCE_IP Source IP address of packets (default: fe80::21e:c0ff:fef2:72f3)
  --source-port SOURCE_PORT Source port of packets (default: 25565)
  --NID NID Network ID of the HomePlug GreenPHY AVLN (default: \x9c\xb0\xb2\xbb\xf5\x6c\x0e)
  --NMK NMK Network Membership Key of the HomePlug GreenPHY AVLN
    (default: \x48\xfe\x56\x02\xdb\xac\xcd\xe5\x1e\xda\xdc\x3e\x08\x1a\x52\xd1)
  -p PROTOCOL, --protocol PROTOCOL Protocol for EXI encoding/decoding: DIN, ISO-2, ISO-20
    (default: DIN)
  --nmap-mac NMAP_MAC The MAC address of the target device to NMAP scan
    (default: EVCC MAC address)
  --nmap-ip NMAP_IP The IP address of the target device to NMAP scan (default: EVCC IP address)
  --nmap-ports NMAP_PORTS List of ports to scan seperated by commas
    (ex. 1,2,5-10,19,...) (default: Top 8000 common ports)
```

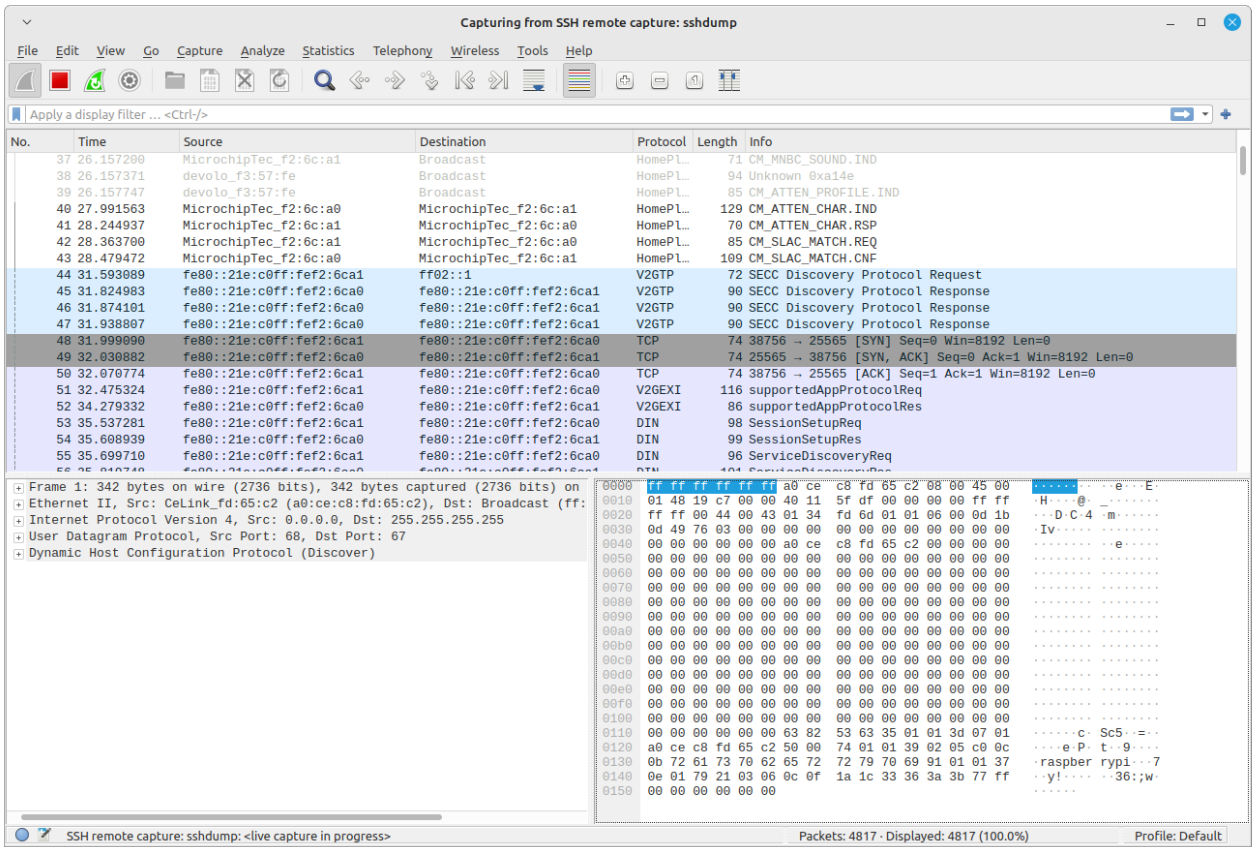
Start the EVSE simulator on the AcCCS Raspberry Pi by running the ***`EVSE.py`*** script with the following options (don't for get to run it with ***`sudo`***):

```
cd AcCCS
sudo python3 EVSE.py -I eth1 -M 1
```


Terminal - team1@raspberrypi: ~/AcCCS
File Edit View Terminal Tabs Help

```
team1@raspberrypi:~ $ cd AcCCS/
team1@raspberrypi:~/AcCCS $ sudo python3 EVSE.py -I eth1 -M 1
INFO: Started Java webserver with PID: 2800 on port: 41677
INFO (EVSE): Opening relay connection
INFO (EVSE): Closing relay connection
INFO (EVSE): Sending SET_KEY_REQ
INFO (EVSE): SLAC timed out, resetting connection...
INFO (EVSE): Opening relay connection
INFO (EVSE): Closing relay connection
INFO (EVSE): Recieved SLAC_PARM_REQ
INFO (EVSE): Sending CM_SLAC_PARM_CNF
INFO (EVSE): Recieved last MNBC_SOUND_IND
INFO (EVSE): Sending ATTEN_CHAR_IND
INFO (EVSE): Recieved SLAC_MATCH_REQ
INFO (EVSE): Sending SLAC_MATCH_CNF
INDO (EVSE): Recieved SECC_RequestMessage
INFO (EVSE): Done SLAC
INFO (EVSE): Starting TCP
INFO (EVSE): Starting timeout thread
INFO (EVSE): Sending SECC_ResponseMessage
INFO (EVSE): Sending SECC_ResponseMessage
INFO (EVSE): Sending SECC_ResponseMessage
INFO (EVSE): Sending SYNACK
ERROR:  'Index 10 out of bounds for length 9'
Request: {urn:din:70121:2012:MsgBody}SessionSetupReq
Request: {urn:din:70121:2012:MsgBody}ServiceDiscoveryReq
Request: {urn:din:70121:2012:MsgBody}ServicePaymentSelectionReq
Request: {urn:din:70121:2012:MsgBody}ContractAuthenticationReq
```

Monitor Wireshark and take notes about what packets are first sent by the EVSE.



Capturing from SSH remote capture: sshdump

```
No. Time      Source                   Destination              Protocol Length Info
 37 26.157200 MicrochipTec_f2:6c:a1    Broadcast                HomePl…    71 CM_MNBC_SOUND.IND
 38 26.157371 devolo_f3:57:fe          Broadcast                HomePl…    94 Unknown 0xa14e
 39 26.157747 devolo_f3:57:fe          Broadcast                HomePl…    85 CM_ATTEN_PROFILE.IND
 40 27.991563 MicrochipTec_f2:6c:a0    MicrochipTec_f2:6c:a1    HomePl…   129 CM_ATTEN_CHAR.IND
 41 28.244937 MicrochipTec_f2:6c:a1    MicrochipTec_f2:6c:a0    HomePl…    70 CM_ATTEN_CHAR.RSP
 42 28.363700 MicrochipTec_f2:6c:a1    MicrochipTec_f2:6c:a0    HomePl…    85 CM_SLAC_MATCH.REQ
 43 28.479472 MicrochipTec_f2:6c:a0    MicrochipTec_f2:6c:a1    HomePl…   109 CM_SLAC_MATCH.CNF
 44 31.593089 fe80::21e:c0ff:fef2:6ca1 ff02::1                  V2GTP      72 SECC Discovery Protocol Request
 45 31.824983 fe80::21e:c0ff:fef2:6ca0 fe80::21e:c0ff:fef2:6ca1 V2GTP      90 SECC Discovery Protocol Response
 46 31.874101 fe80::21e:c0ff:fef2:6ca0 fe80::21e:c0ff:fef2:6ca1 V2GTP      90 SECC Discovery Protocol Response
 47 31.938807 fe80::21e:c0ff:fef2:6ca0 fe80::21e:c0ff:fef2:6ca1 V2GTP      90 SECC Discovery Protocol Response
 48 31.999090 fe80::21e:c0ff:fef2:6ca1 fe80::21e:c0ff:fef2:6ca0 TCP        74 38756 → 25565 [SYN] Seq=0 Win=8192 Len=0
 49 32.030882 fe80::21e:c0ff:fef2:6ca0 fe80::21e:c0ff:fef2:6ca1 TCP        74 25565 → 38756 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
 50 32.070774 fe80::21e:c0ff:fef2:6ca1 fe80::21e:c0ff:fef2:6ca0 TCP        74 38756 → 25565 [ACK] Seq=1 Ack=1 Win=8192 Len=0
 51 32.475324 fe80::21e:c0ff:fef2:6ca1 fe80::21e:c0ff:fef2:6ca0 V2GEXI    116 supportedAppProtocolReq
 52 34.279332 fe80::21e:c0ff:fef2:6ca0 fe80::21e:c0ff:fef2:6ca1 V2GEXI     86 supportedAppProtocolRes
 53 35.537281 fe80::21e:c0ff:fef2:6ca1 fe80::21e:c0ff:fef2:6ca0 DIN        98 SessionSetupReq
 54 35.608939 fe80::21e:c0ff:fef2:6ca0 fe80::21e:c0ff:fef2:6ca1 DIN        99 SessionSetupRes
 55 35.699710 fe80::21e:c0ff:fef2:6ca1 fe80::21e:c0ff:fef2:6ca0 DIN        96 ServiceDiscoveryReq
```

```
+ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on
+ Ethernet II, Src: CeLink_fd:65:c2 (a0:ce:c8:fd:65:c2), Dst: Broadcast (ff:
+ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
+ User Datagram Protocol, Src Port: 68, Dst Port: 67
+ Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff a0 ce  c8 fd 65 c2 08 00 45 00   ········ ··e···E·
0010  01 48 19 c7 00 00 40 11  5f df 00 00 00 00 ff ff   ·H····@· _·······
0020  ff ff 00 44 00 43 01 34  fd 6d 01 01 06 00 0d 1b   ···D·C·4 ·m······
0030  0d 49 76 03 00 00 00 00  00 00 00 00 00 00 00 00   ·Iv····· ········
0040  00 00 00 00 00 00 a0 ce  c8 fd 65 c2 00 00 00 00   ········ ··e·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ······c· Sc5··=··
0120  a0 ce c8 fd 65 c2 50 00  74 01 01 39 02 05 c0 0c   ····e·P· t··9····
0130  0b 72 61 73 70 62 65 72  72 79 70 69 91 01 01 37   ·raspber rypi···7
0140  0e 01 79 21 03 06 0c 0f  1a 1c 33 36 3a 3b 77 ff   ··y!···· ··36:;w·
0150  00 00 00 00 00 00                                  ······
```

SSH remote capture: sshdump: <live capture in progress> Packets: 4817 · Displayed: 4817 (100.0%) Profile: Default

What are some of the most interesting packets? Which packets do you recognize? Which packets have you never seen before? Make note of some of your most interesting discoveries.

____

____

____

____

____

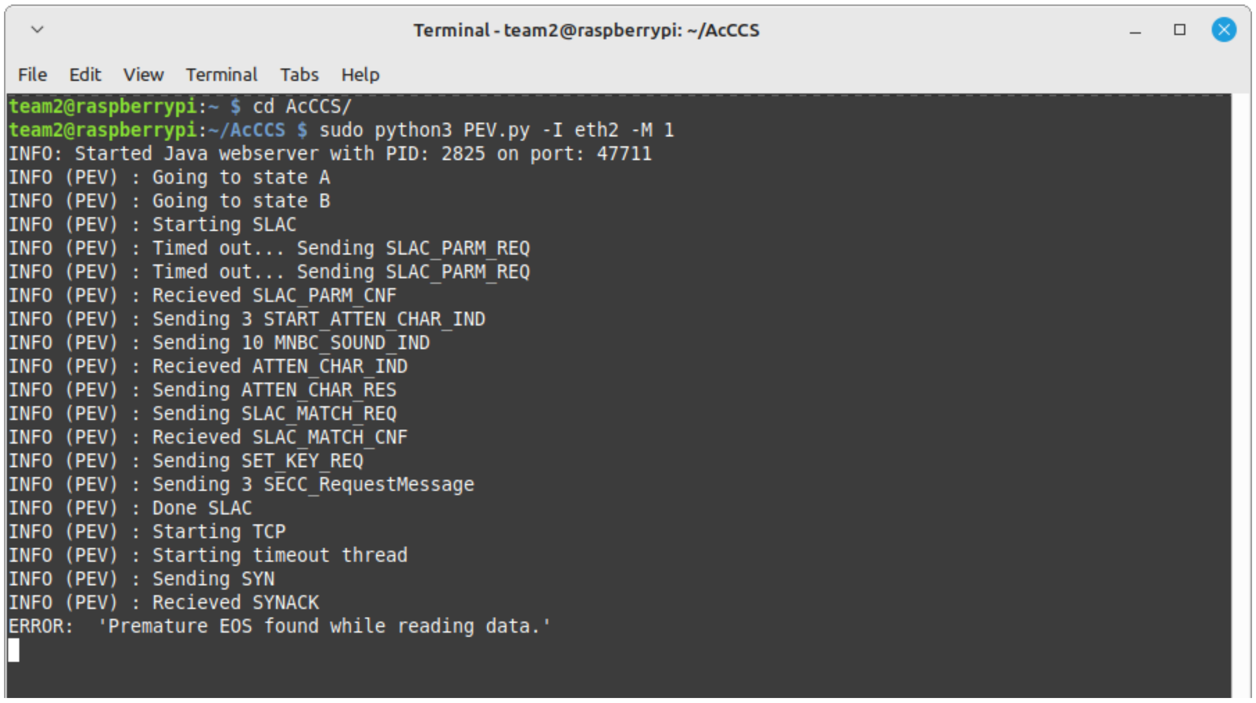
b. Team 2 only:

The PEV emulator script has several command-line options. Below is a description of each of these options:

```
usage: PEV.py [-h] [-M MODE] [-I INTERFACE] [--source-mac SOURCE_MAC] [--source-ip SOURCE_IP]
[--source-port SOURCE_PORT] [-p PROTOCOL] [--nmap-mac NMAP_MAC] [--nmap-ip NMAP_IP]
[--nmap-ports NMAP_PORTS]

PEV emulator for AcCCS

optional arguments:
  -h, --help show this help message and exit
  -M MODE, --mode MODE  Mode for emulator to run in: 0 for full conversation, 1 for stalling the
conversation, 2 for portscanning (default: 0)
  -I INTERFACE, --interface INTERFACE Ethernet interface to send/recieve packets on (default: eth1)
  --source-mac SOURCE_MAC Source MAC address of packets (default: 00:1e:c0:f2:6c:a0)
  --source-ip SOURCE_IP Source IP address of packets (default: fe80::21e:c0ff:fef2:72f3)
  --source-port SOURCE_PORT Source port of packets (default: 25565)
  -p PROTOCOL, --protocol PROTOCOL Protocol for EXI encoding/decoding: DIN, ISO-2, ISO-20
    (default: DIN)
  --nmap-mac NMAP_MAC   The MAC address of the target device to NMAP scan
    (default: SECC MAC address)
  --nmap-ip NMAP_IP     The IP address of the target device to NMAP scan
    (default: SECC IP address)
  --nmap-ports NMAP_PORTS List of ports to scan seperated by commas (ex. 1,2,5-10,19,...)
    (default: Top 8000 common ports)
```

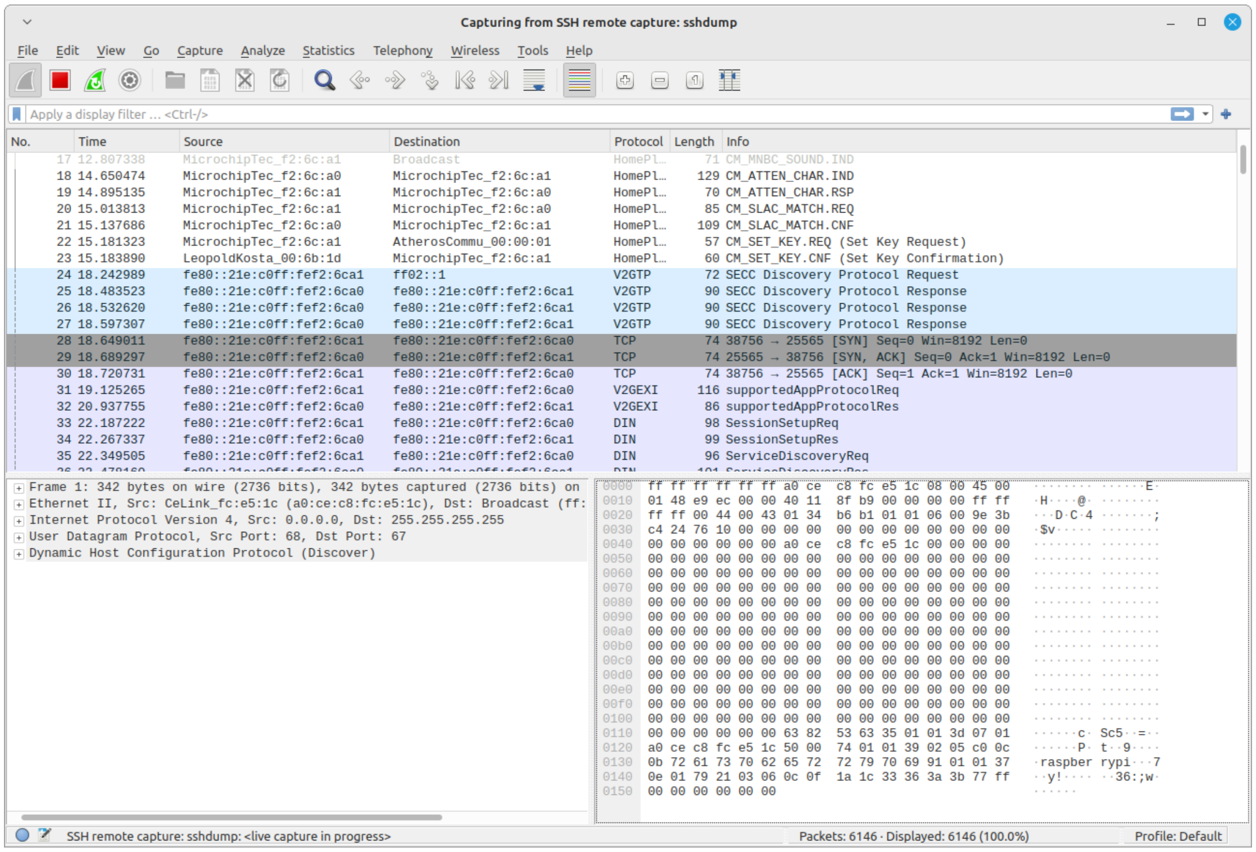
Start the PEV emulator on the AcCCS Raspberry Pi by running the ***PEV.py*** script with the following options (don't for get to run it with ***sudo***):

```
cd AcCCS
sudo python3 PEV.py -I eth2 -M 1
```


Terminal - team2@raspberrypi: ~/AcCCS
File Edit View Terminal Tabs Help

```
team2@raspberrypi:~ $ cd AcCCS/
team2@raspberrypi:~/AcCCS $ sudo python3 PEV.py -I eth2 -M 1
INFO: Started Java webserver with PID: 2825 on port: 47711
INFO (PEV) : Going to state A
INFO (PEV) : Going to state B
INFO (PEV) : Starting SLAC
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Recieved SLAC_PARM_CNF
INFO (PEV) : Sending 3 START_ATTEN_CHAR_IND
INFO (PEV) : Sending 10 MNBC_SOUND_IND
INFO (PEV) : Recieved ATTEN_CHAR_IND
INFO (PEV) : Sending ATTEN_CHAR_RES
INFO (PEV) : Sending SLAC_MATCH_REQ
INFO (PEV) : Recieved SLAC_MATCH_CNF
INFO (PEV) : Sending SET_KEY_REQ
INFO (PEV) : Sending 3 SECC_RequestMessage
INFO (PEV) : Done SLAC
INFO (PEV) : Starting TCP
INFO (PEV) : Starting timeout thread
INFO (PEV) : Sending SYN
INFO (PEV) : Recieved SYNACK
ERROR:  'Premature EOS found while reading data.'
```

Monitor Wireshark and take notes about what packets are first sent by the PEV.


Capturing from SSH remote capture: sshdump

```
No.  Time       Source                     Destination                Protocol  Length Info
  17 12.807338  MicrochipTec_f2:6c:a1      Broadcast                  HomePl…     71 CM_MNBC_SOUND.IND
  18 14.650474  MicrochipTec_f2:6c:a0      MicrochipTec_f2:6c:a1      HomePl…    129 CM_ATTEN_CHAR.IND
  19 14.895135  MicrochipTec_f2:6c:a1      MicrochipTec_f2:6c:a0      HomePl…     70 CM_ATTEN_CHAR.RSP
  20 15.013813  MicrochipTec_f2:6c:a1      MicrochipTec_f2:6c:a0      HomePl…     85 CM_SLAC_MATCH.REQ
  21 15.137686  MicrochipTec_f2:6c:a0      MicrochipTec_f2:6c:a1      HomePl…    109 CM_SLAC_MATCH.CNF
  22 15.181323  MicrochipTec_f2:6c:a1      AtherosCommu_00:00:01      HomePl…     57 CM_SET_KEY.REQ (Set Key Request)
  23 15.183890  LeopoldKosta_00:6b:1d      MicrochipTec_f2:6c:a1      HomePl…     60 CM_SET_KEY.CNF (Set Key Confirmation)
  24 18.242989  fe80::21e:c0ff:fef2:6ca1   ff02::1                    V2GTP       72 SECC Discovery Protocol Request
  25 18.483523  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   V2GTP       90 SECC Discovery Protocol Response
  26 18.532620  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   V2GTP       90 SECC Discovery Protocol Response
  27 18.597307  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   V2GTP       90 SECC Discovery Protocol Response
  28 18.649011  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   TCP         74 38756 → 25565 [SYN] Seq=0 Win=8192 Len=0
  29 18.689297  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   TCP         74 25565 → 38756 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
  30 18.720731  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   TCP         74 38756 → 25565 [ACK] Seq=1 Ack=1 Win=8192 Len=0
  31 19.125265  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   V2GEXI     116 supportedAppProtocolReq
  32 20.937755  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   V2GEXI      86 supportedAppProtocolRes
  33 22.187222  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN         98 SessionSetupReq
  34 22.267337  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN         99 SessionSetupRes
  35 22.349505  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN         96 ServiceDiscoveryReq
```

```
+ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on
+ Ethernet II, Src: CeLink_fc:e5:1c (a0:ce:c8:fc:e5:1c), Dst: Broadcast (ff:
+ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
+ User Datagram Protocol, Src Port: 68, Dst Port: 67
+ Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff a0 ce  c8 fc e5 1c 08 00 45 00   ········ ······E·
0010  01 48 e9 ec 00 00 40 11  8f b9 00 00 00 00 ff ff   ·H····@· ········
0020  ff ff 00 44 00 43 01 34  b6 b1 01 01 06 00 9e 3b   ···D·C·4 ·······;
0030  c4 24 76 10 00 00 00 00  00 00 00 00 00 00 00 00   ·$v····· ········
0040  00 00 00 00 00 00 a0 ce  c8 fc e5 1c 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ······c· Sc5··=··
0120  a0 ce c8 fc e5 1c 50 00  74 01 01 39 02 05 c0 0c   ······P· t··9····
0130  0b 72 61 73 70 62 65 72  72 79 70 69 91 01 01 37   ·raspber rypi···7
0140  0e 01 79 21 03 06 0c 0f  1a 1c 33 36 3a 3b 77 ff   ··y!···· ··36:;w·
0150  00 00 00 00 00 00                                  ······
```

SSH remote capture: sshdump: <live capture in progress> Packets: 6146 · Displayed: 6146 (100.0%) Profile: Default

What are some of the most interesting packets? Which packets do you recognize? Which packets have you never seen before? Make note of some of your most interesting discoveries.

____

____

____

____

____

Step 9: Both teams: review your captured network traffic from Step 8 and answer the following questions:

What is the Network Membership Key (NMK) used to negotiate and set up the HomePlug Green PHY network? Do you know what this key is used for?

____

____

____

____

____

What interesting fields are found in the SECC Discovery Protocol Request and Response?

____
____
____
____
____

What protocol(s) are available for EVSE to PEV communications?

____
____
____
____
____

What message(s) are used to stall the conversation and keep the PEV and EVSE in a waiting state?

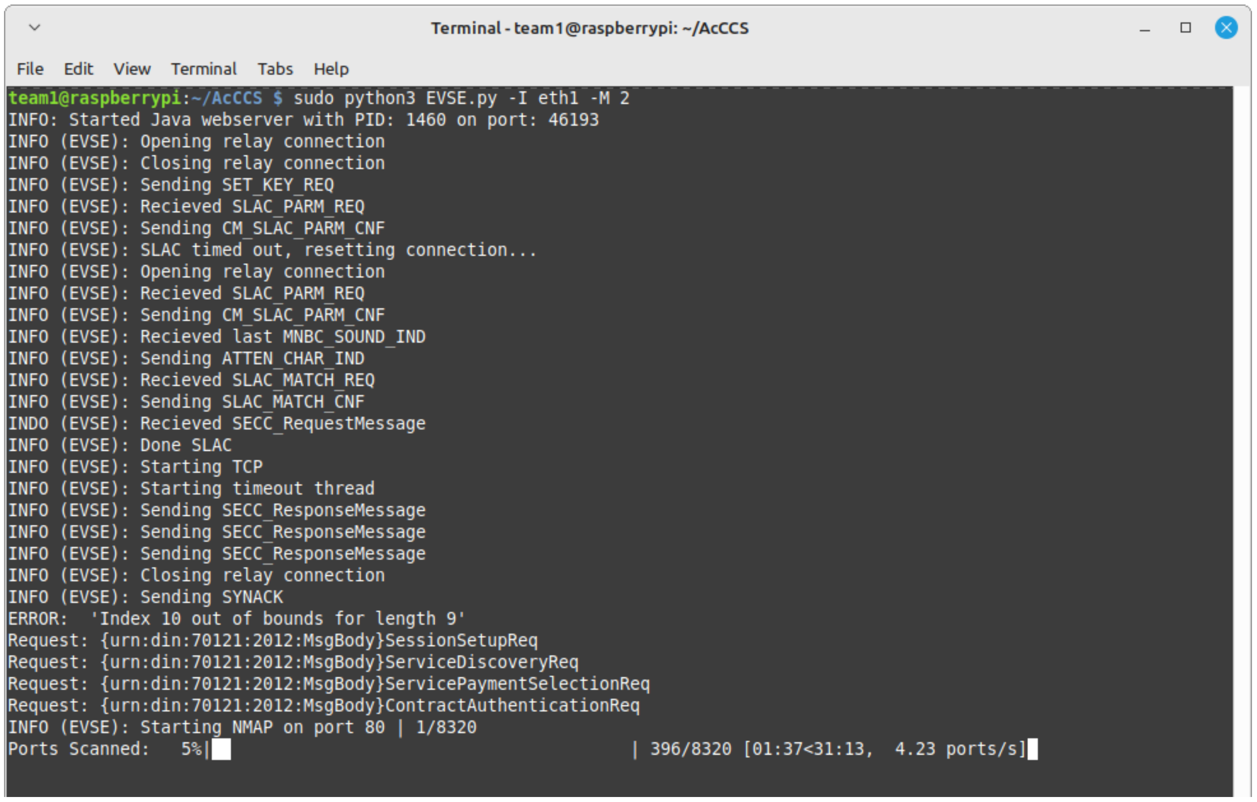
____
____
____
____
____

Step 10: Stop the EVSE and PEV emulator scripts by pressing Ctrl+C. This will interrupt the script and terminate after a few seconds.

We will now re-run the emulators and change the mode to include some basic network port scanning. The port scanning available in AcCCS is a traditional TCP SYN scan of approximately 500 known ports (i.e. the NMap top 500 TCP ports).

Team 1: Start the EVSE emulator in your terminal window with the following command. **Note**: the **–M** option has changed to include port scanning.

```
sudo python3 EVSE.py –I eth1 –M 2
```

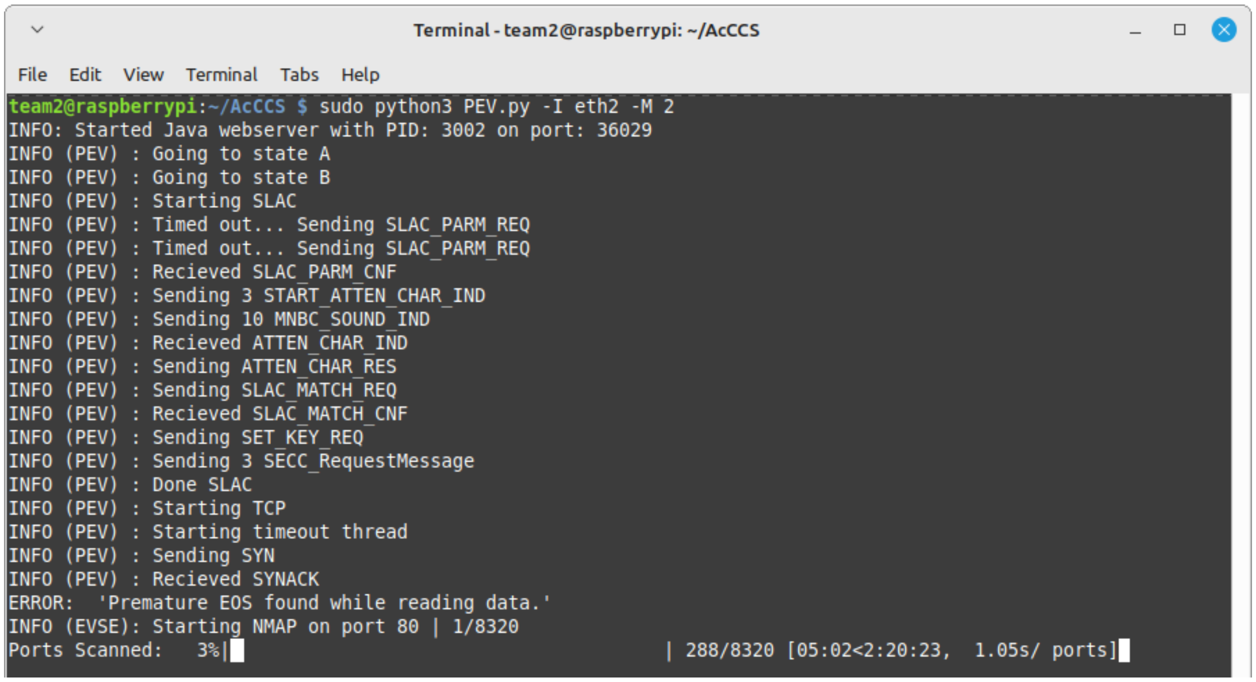

Terminal - team1@raspberrypi: ~/AcCCS
File Edit View Terminal Tabs Help

```
team1@raspberrypi:~/AcCCS $ sudo python3 EVSE.py -I eth1 -M 2
INFO: Started Java webserver with PID: 1460 on port: 46193
INFO (EVSE): Opening relay connection
INFO (EVSE): Closing relay connection
INFO (EVSE): Sending SET_KEY_REQ
INFO (EVSE): Recieved SLAC_PARM_REQ
INFO (EVSE): Sending CM_SLAC_PARM_CNF
INFO (EVSE): SLAC timed out, resetting connection...
INFO (EVSE): Opening relay connection
INFO (EVSE): Recieved SLAC_PARM_REQ
INFO (EVSE): Sending CM_SLAC_PARM_CNF
INFO (EVSE): Recieved last MNBC_SOUND_IND
INFO (EVSE): Sending ATTEN_CHAR_IND
INFO (EVSE): Recieved SLAC_MATCH_REQ
INFO (EVSE): Sending SLAC_MATCH_CNF
INDO (EVSE): Recieved SECC_RequestMessage
INFO (EVSE): Done SLAC
INFO (EVSE): Starting TCP
INFO (EVSE): Starting timeout thread
INFO (EVSE): Sending SECC_ResponseMessage
INFO (EVSE): Sending SECC_ResponseMessage
INFO (EVSE): Sending SECC_ResponseMessage
INFO (EVSE): Closing relay connection
INFO (EVSE): Sending SYNACK
ERROR:  'Index 10 out of bounds for length 9'
Request: {urn:din:70121:2012:MsgBody}SessionSetupReq
Request: {urn:din:70121:2012:MsgBody}ServiceDiscoveryReq
Request: {urn:din:70121:2012:MsgBody}ServicePaymentSelectionReq
Request: {urn:din:70121:2012:MsgBody}ContractAuthenticationReq
INFO (EVSE): Starting NMAP on port 80 | 1/8320
Ports Scanned:   5%|█                                        | 396/8320 [01:37<31:13,  4.23 ports/s]
```

Team 2: Start the PEV emulator in your terminal window with the following command. **Note**: the **–M** option has changed to include port scanning.

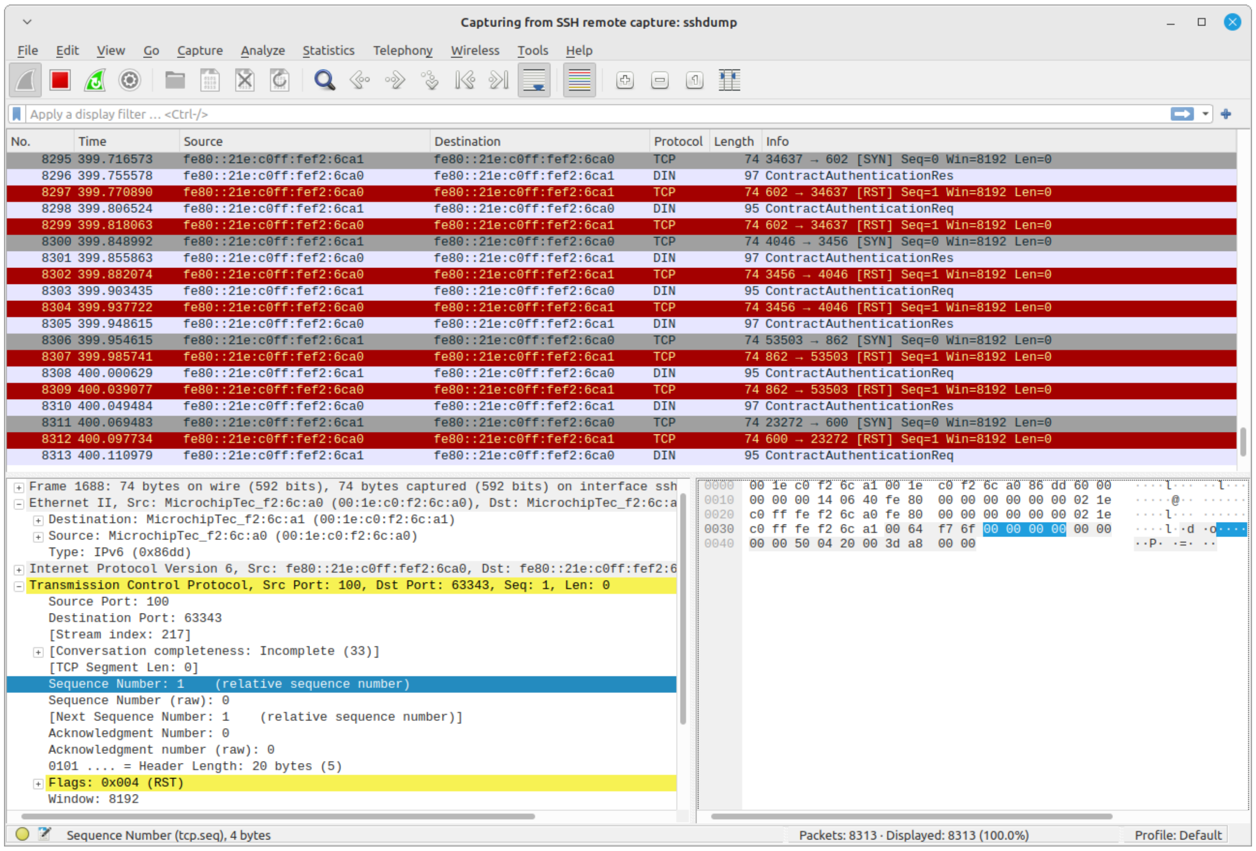
```
sudo python3 PEV.py –I eth2 –M 2
```

The network scan will take several minutes to complete, but you should now have a progress bar in your terminal window indicating how long the scan has remaining.


Terminal - team2@raspberrypi: ~/AcCCS
File Edit View Terminal Tabs Help

```
team2@raspberrypi:~/AcCCS $ sudo python3 PEV.py -I eth2 -M 2
INFO: Started Java webserver with PID: 3002 on port: 36029
INFO (PEV) : Going to state A
INFO (PEV) : Going to state B
INFO (PEV) : Starting SLAC
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Recieved SLAC_PARM_CNF
INFO (PEV) : Sending 3 START_ATTEN_CHAR_IND
INFO (PEV) : Sending 10 MNBC_SOUND_IND
INFO (PEV) : Recieved ATTEN_CHAR_IND
INFO (PEV) : Sending ATTEN_CHAR_RES
INFO (PEV) : Sending SLAC_MATCH_REQ
INFO (PEV) : Recieved SLAC_MATCH_CNF
INFO (PEV) : Sending SET_KEY_REQ
INFO (PEV) : Sending 3 SECC_RequestMessage
INFO (PEV) : Done SLAC
INFO (PEV) : Starting TCP
INFO (PEV) : Starting timeout thread
INFO (PEV) : Sending SYN
INFO (PEV) : Recieved SYNACK
ERROR:  'Premature EOS found while reading data.'
INFO (EVSE): Starting NMAP on port 80 | 1/8320
Ports Scanned:   3%|█                                        | 288/8320 [05:02<2:20:23,  1.05s/ ports]█
```

Monitor the network scan activity in Wireshark.


Capturing from SSH remote capture: sshdump
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time       Source                    Destination               Protocol Length Info
8295 399.716573 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  TCP      74 34637 → 602 [SYN] Seq=0 Win=8192 Len=0
8296 399.755578 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  DIN      97 ContractAuthenticationRes
8297 399.770890 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 602 → 34637 [RST] Seq=1 Win=8192 Len=0
8298 399.806524 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  DIN      95 ContractAuthenticationReq
8299 399.818063 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 602 → 34637 [RST] Seq=1 Win=8192 Len=0
8300 399.848992 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  TCP      74 4046 → 3456 [SYN] Seq=0 Win=8192 Len=0
8301 399.855863 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  DIN      97 ContractAuthenticationRes
8302 399.882074 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 3456 → 4046 [RST] Seq=1 Win=8192 Len=0
8303 399.903435 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  DIN      95 ContractAuthenticationReq
8304 399.937722 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 3456 → 4046 [RST] Seq=1 Win=8192 Len=0
8305 399.948615 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  DIN      97 ContractAuthenticationRes
8306 399.954615 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  TCP      74 53503 → 862 [SYN] Seq=0 Win=8192 Len=0
8307 399.985741 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 862 → 53503 [RST] Seq=1 Win=8192 Len=0
8308 400.000629 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  DIN      95 ContractAuthenticationReq
8309 400.039077 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 862 → 53503 [RST] Seq=1 Win=8192 Len=0
8310 400.049484 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  DIN      97 ContractAuthenticationRes
8311 400.069483 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  TCP      74 23272 → 600 [SYN] Seq=0 Win=8192 Len=0
8312 400.097734 fe80::21e:c0ff:fef2:6ca0  fe80::21e:c0ff:fef2:6ca1  TCP      74 600 → 23272 [RST] Seq=1 Win=8192 Len=0
8313 400.110979 fe80::21e:c0ff:fef2:6ca1  fe80::21e:c0ff:fef2:6ca0  DIN      95 ContractAuthenticationReq
```

```
+ Frame 1688: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ssh
- Ethernet II, Src: MicrochipTec_f2:6c:a0 (00:1e:c0:f2:6c:a0), Dst: MicrochipTec_f2:6c:a
  + Destination: MicrochipTec_f2:6c:a1 (00:1e:c0:f2:6c:a1)
  + Source: MicrochipTec_f2:6c:a0 (00:1e:c0:f2:6c:a0)
    Type: IPv6 (0x86dd)
+ Internet Protocol Version 6, Src: fe80::21e:c0ff:fef2:6ca0, Dst: fe80::21e:c0ff:fef2:6
- Transmission Control Protocol, Src Port: 100, Dst Port: 63343, Seq: 1, Len: 0
    Source Port: 100
    Destination Port: 63343
    [Stream index: 217]
  + [Conversation completeness: Incomplete (33)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  + Flags: 0x004 (RST)
    Window: 8192
```

```
0000  00 1e c0 f2 6c a1 00 1e  c0 f2 6c a0 86 dd 60 00   ····l··· ··l···
0010  00 00 00 14 06 40 fe 80  00 00 00 00 00 00 02 1e   ·····@·· ······
0020  c0 ff fe f2 6c a0 fe 80  00 00 00 00 00 00 02 1e   ····l··· ······
0030  c0 ff fe f2 6c a1 00 64  f7 6f 00 00 00 00 00 00   ····l··d ·o····
0040  00 00 50 04 20 00 3d a8  00 00                     ··P· ·=· ··
```

Sequence Number (tcp.seq), 4 bytes   Packets: 8313 · Displayed: 8313 (100.0%)   Profile: Default

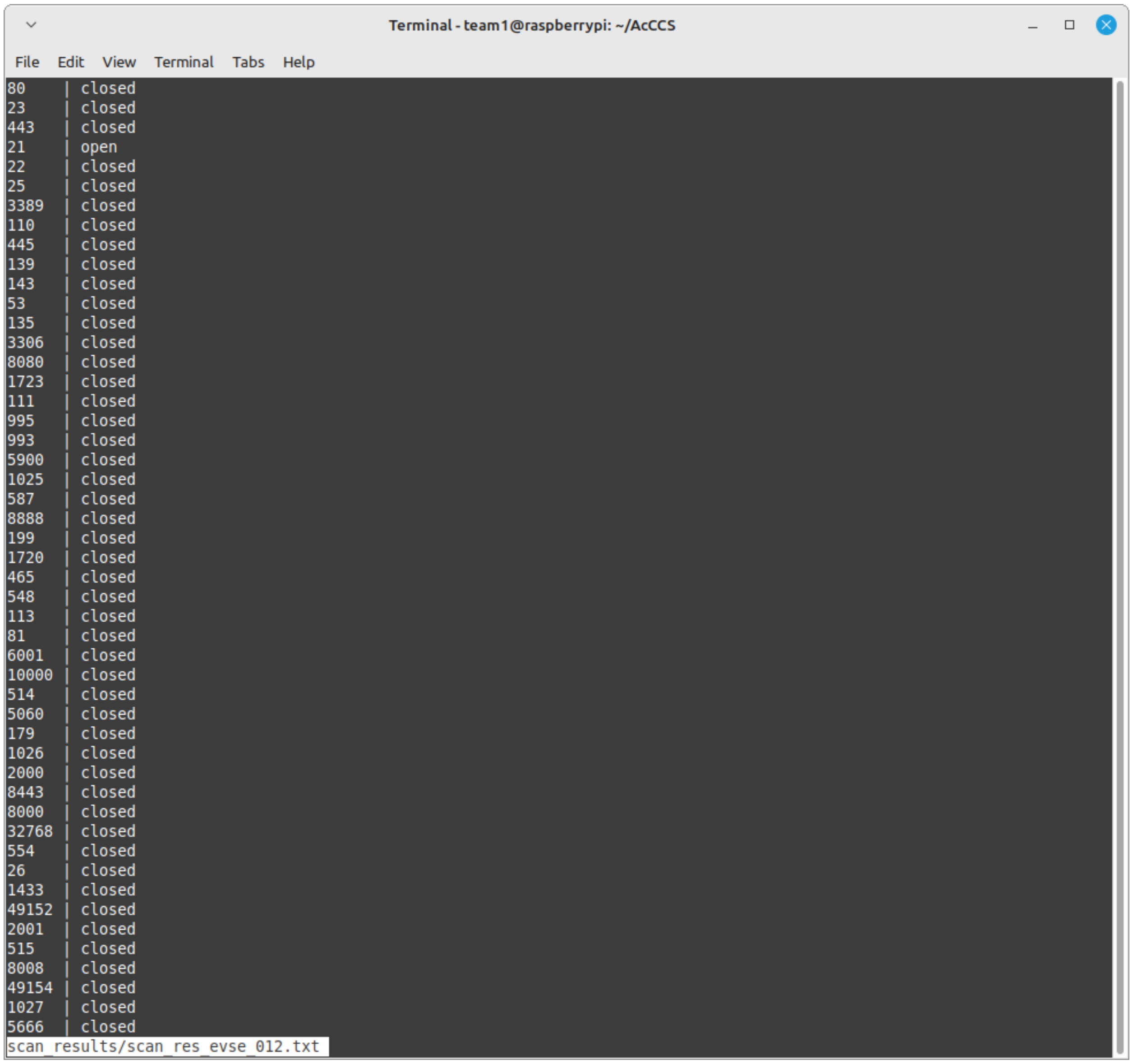
What new packets do you see in your Wireshark capture? What do these packets indicate is happening?

____
____
____
____
____

When the scans are finished, the emulator scripts will save a summary of the port scan in the ***scan_results*** folder. Terminate the emulator scripts by pressing Ctrl+C.

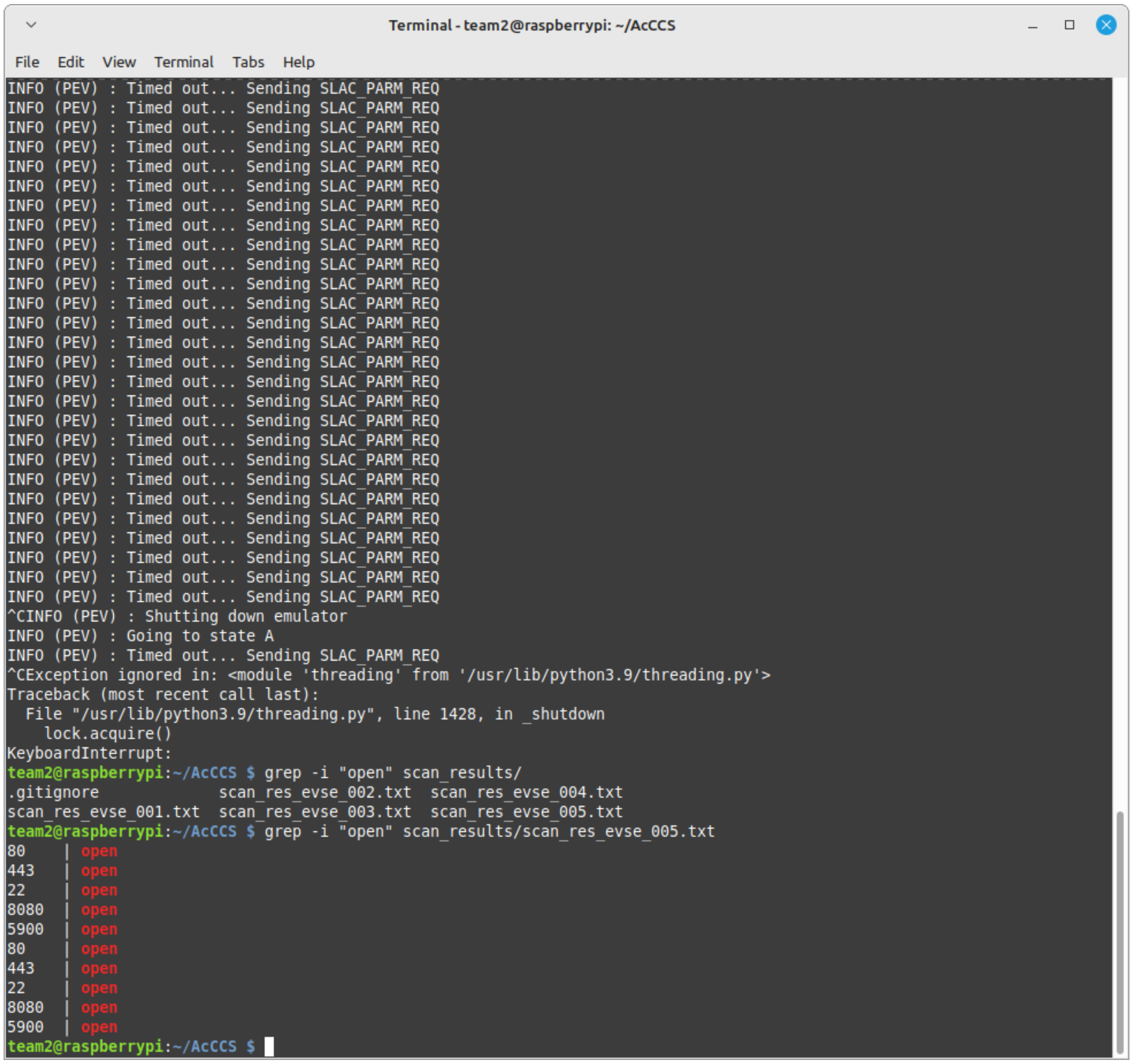
Step 11: Review the port scan results using Linux commands like **`less`**, **`more`**, and **`grep`**. List the open ports you identified. What can you determine from these scan results?

```
less scan_results/scan_res_evse_001.txt
```


Terminal - team1@raspberrypi: ~/AcCCS
File Edit View Terminal Tabs Help

```
80    | closed
23    | closed
443   | closed
21    | open
22    | closed
25    | closed
3389  | closed
110   | closed
445   | closed
139   | closed
143   | closed
53    | closed
135   | closed
3306  | closed
8080  | closed
1723  | closed
111   | closed
995   | closed
993   | closed
5900  | closed
1025  | closed
587   | closed
8888  | closed
199   | closed
1720  | closed
465   | closed
548   | closed
113   | closed
81    | closed
6001  | closed
10000 | closed
514   | closed
5060  | closed
179   | closed
1026  | closed
2000  | closed
8443  | closed
8000  | closed
32768 | closed
554   | closed
26    | closed
1433  | closed
49152 | closed
2001  | closed
515   | closed
8008  | closed
49154 | closed
1027  | closed
5666  | closed
scan_results/scan_res_evse_012.txt
```

```
grep -i “open” scan_results/scan_res_evse_001.txt
```


Terminal - team2@raspberrypi: ~/AcCCS
File Edit View Terminal Tabs Help

```
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
^CINFO (PEV) : Shutting down emulator
INFO (PEV) : Going to state A
INFO (PEV) : Timed out... Sending SLAC_PARM_REQ
^CException ignored in: <module 'threading' from '/usr/lib/python3.9/threading.py'>
Traceback (most recent call last):
  File "/usr/lib/python3.9/threading.py", line 1428, in _shutdown
    lock.acquire()
KeyboardInterrupt:
team2@raspberrypi:~/AcCCS $ grep -i "open" scan_results/
.gitignore             scan_res_evse_002.txt  scan_res_evse_004.txt
scan_res_evse_001.txt  scan_res_evse_003.txt  scan_res_evse_005.txt
team2@raspberrypi:~/AcCCS $ grep -i "open" scan_results/scan_res_evse_005.txt
80    | open
443   | open
22    | open
8080  | open
5900  | open
80    | open
443   | open
22    | open
8080  | open
5900  | open
team2@raspberrypi:~/AcCCS $ 
```

List the ports you found open. What might this mean? How would you investigate further?

____

____

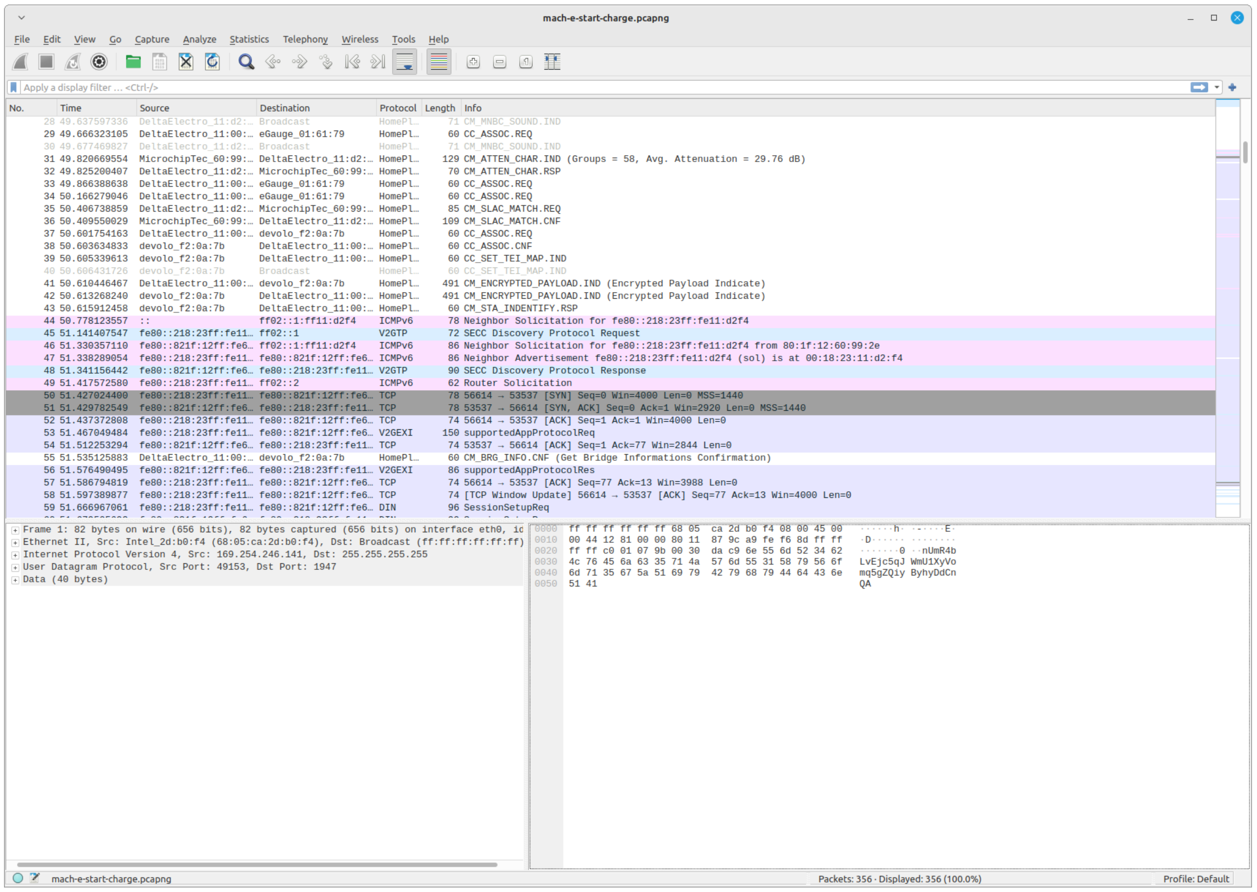
____

____

____

Step 12: Compare the network traffic you collected while running the emulator scripts with known good communications with actual vehicles and EVSE. We provided a couple of saved PCAP files on the desktop. You can open these files by double-clicking on either one to open it in Wireshark.

This will open a new Wireshark window with the contents of your saved network capture.


mach-e-start-charge.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source               Destination          Protocol Length Info
  28 49.637597336  DeltaElectro_11:d2:… Broadcast            HomePl…     71 CM_MNBC_SOUND.IND
  29 49.666323105  DeltaElectro_11:00:… eGauge_01:61:79      HomePl…     60 CC_ASSOC.REQ
  30 49.677469827  DeltaElectro_11:d2:… Broadcast            HomePl…     71 CM_MNBC_SOUND.IND
  31 49.820669554  MicrochipTec_60:99:… DeltaElectro_11:d2:… HomePl…    129 CM_ATTEN_CHAR.IND (Groups = 58, Avg. Attenuation = 29.76 dB)
  32 49.825200407  DeltaElectro_11:d2:… MicrochipTec_60:99:… HomePl…     70 CM_ATTEN_CHAR.RSP
  33 49.866388638  DeltaElectro_11:00:… eGauge_01:61:79      HomePl…     60 CC_ASSOC.REQ
  34 50.166279046  DeltaElectro_11:00:… eGauge_01:61:79      HomePl…     60 CC_ASSOC.REQ
  35 50.406738859  DeltaElectro_11:d2:… MicrochipTec_60:99:… HomePl…     85 CM_SLAC_MATCH.REQ
  36 50.409550029  MicrochipTec_60:99:… DeltaElectro_11:d2:… HomePl…    109 CM_SLAC_MATCH.CNF
  37 50.601754163  DeltaElectro_11:00:… devolo_f2:0a:7b      HomePl…     60 CC_ASSOC.REQ
  38 50.603634833  devolo_f2:0a:7b      DeltaElectro_11:00:… HomePl…     60 CC_ASSOC.CNF
  39 50.605339613  devolo_f2:0a:7b      DeltaElectro_11:00:… HomePl…     60 CC_SET_TEI_MAP.IND
  40 50.606431726  devolo_f2:0a:7b      Broadcast            HomePl…     60 CC_SET_TEI_MAP.IND
  41 50.610446467  DeltaElectro_11:00:… devolo_f2:0a:7b      HomePl…    491 CM_ENCRYPTED_PAYLOAD.IND (Encrypted Payload Indicate)
  42 50.613268240  devolo_f2:0a:7b      DeltaElectro_11:00:… HomePl…    491 CM_ENCRYPTED_PAYLOAD.IND (Encrypted Payload Indicate)
  43 50.615912458  devolo_f2:0a:7b      DeltaElectro_11:00:… HomePl…     60 CM_STA_INDENTIFY.RSP
  44 50.778123557  ::                   ff02::1:ff11:d2f4    ICMPv6      78 Neighbor Solicitation for fe80::218:23ff:fe11:d2f4
  45 51.141407547  fe80::218:23ff:fe11… ff02::1              V2GTP       72 SECC Discovery Protocol Request
  46 51.330357110  fe80::821f:12ff:fe6… ff02::1:ff11:d2f4    ICMPv6      86 Neighbor Solicitation for fe80::218:23ff:fe11:d2f4 from 80:1f:12:60:99:2e
  47 51.338289054  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… ICMPv6      86 Neighbor Advertisement fe80::218:23ff:fe11:d2f4 (sol) is at 00:18:23:11:d2:f4
  48 51.341156442  fe80::821f:12ff:fe6… fe80::218:23ff:fe11… V2GTP       90 SECC Discovery Protocol Response
  49 51.417572580  fe80::218:23ff:fe11… ff02::2              ICMPv6      62 Router Solicitation
  50 51.427024400  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… TCP         78 56614 → 53537 [SYN] Seq=0 Win=4000 Len=0 MSS=1440
  51 51.429782549  fe80::821f:12ff:fe6… fe80::218:23ff:fe11… TCP         78 53537 → 56614 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0 MSS=1440
  52 51.437372808  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… TCP         74 56614 → 53537 [ACK] Seq=1 Ack=1 Win=4000 Len=0
  53 51.467049484  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… V2GEXI     150 supportedAppProtocolReq
  54 51.512253294  fe80::821f:12ff:fe6… fe80::218:23ff:fe11… TCP         74 53537 → 56614 [ACK] Seq=1 Ack=77 Win=2844 Len=0
  55 51.535125883  DeltaElectro_11:00:… devolo_f2:0a:7b      HomePl…     60 CM_BRG_INFO.CNF (Get Bridge Informations Confirmation)
  56 51.576490495  fe80::821f:12ff:fe6… fe80::218:23ff:fe11… V2GEXI      86 supportedAppProtocolRes
  57 51.586794819  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… TCP         74 56614 → 53537 [ACK] Seq=77 Ack=13 Win=3988 Len=0
  58 51.597389877  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… TCP         74 [TCP Window Update] 56614 → 53537 [ACK] Seq=77 Ack=13 Win=4000 Len=0
  59 51.666967061  fe80::218:23ff:fe11… fe80::821f:12ff:fe6… DIN         96 SessionSetupReq
```

```
+ Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface eth0, id
+ Ethernet II, Src: Intel_2d:b0:f4 (68:05:ca:2d:b0:f4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
+ Internet Protocol Version 4, Src: 169.254.246.141, Dst: 255.255.255.255
+ User Datagram Protocol, Src Port: 49153, Dst Port: 1947
+ Data (40 bytes)
```

```
0000  ff ff ff ff ff ff 68 05  ca 2d b0 f4 08 00 45 00   ······h· ·-····E·
0010  00 44 12 81 00 00 80 11  87 9c a9 fe f6 8d ff ff   ·D······ ········
0020  ff ff c0 01 07 9b 00 30  da c9 6e 55 6d 52 34 62   ·······0 ··nUmR4b
0030  4c 76 45 6a 63 35 71 4a  57 6d 55 31 58 79 56 6f   LvEjc5qJ WmU1XyVo
0040  6d 71 35 67 5a 51 69 79  42 79 68 79 44 64 43 6e   mq5gZQiy ByhyDdCn
0050  51 41                                              QA
```

```
mach-e-start-charge.pcapng          Packets: 356 · Displayed: 356 (100.0%)          Profile: Default
```

Examine the conversation between the BMW i3 or the Mach-E and take notes of the differences between this network traffic and the network traffic you generated using AcCCS.

What are some of the differences? What are some of the similarities?

____
____
____
____
____

Congratulations! You are now ready to use an AcCCS system with an actual PEV or EVSE. You can move onto the next hands-on exercise and try these skills with the vehicle or EVSE.

Optional Steps

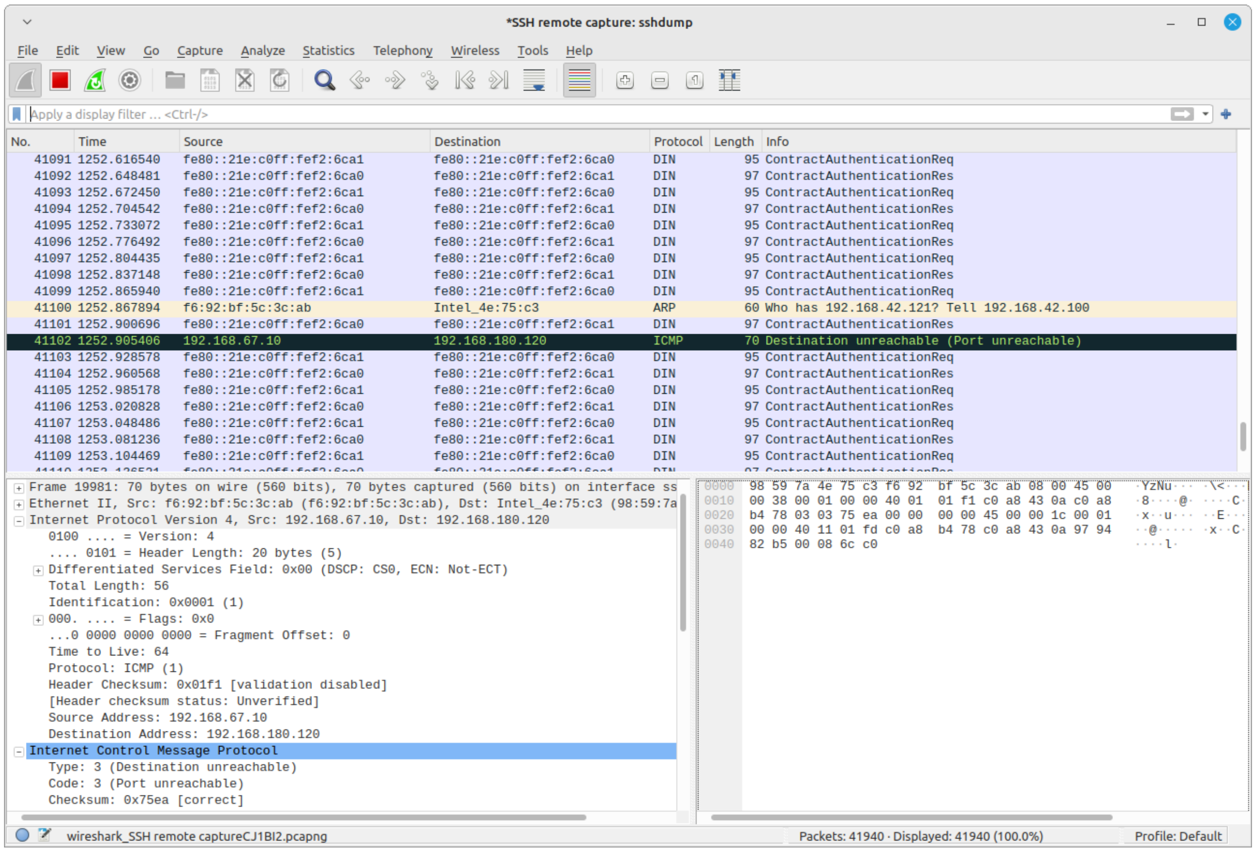
Step 13: We are going to dig a little deeper with Wireshark and investigate the communications between the PEV and EVSE emulators. Follow Steps 7 – 9 to restart each of the emulators in mode 1 (**`-M 1`** option). The communications should again start and continue running indefinitely.

Step 14: Watch Wireshark closely and see if you can visually spot any packets that do not appear to be a part of the normal conversation. The connection between a vehicle and EVSE is a dedicated connection and not used for other network traffic. Make notes of your findings below.

____
____
____
____
____

Step 15: Why do you think these additional packets are visible in Wireshark? If this is a dedicated connection between the PEV and EVSE, what assumptions can you make about these additional broadcast packets?

____
____
____
____
____


*SSH remote capture: sshdump
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source                     Destination                Protocol Length Info
41091 1252.616540  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41092 1252.648481  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41093 1252.672450  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41094 1252.704542  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41095 1252.733072  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41096 1252.776492  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41097 1252.804435  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41098 1252.837148  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41099 1252.865940  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41100 1252.867894  f6:92:bf:5c:3c:ab          Intel_4e:75:c3             ARP      60 Who has 192.168.42.121? Tell 192.168.42.100
41101 1252.900696  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41102 1252.905406  192.168.67.10              192.168.180.120            ICMP     70 Destination unreachable (Port unreachable)
41103 1252.928578  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41104 1252.960568  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41105 1252.985178  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41106 1253.020828  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41107 1253.048486  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
41108 1253.081236  fe80::21e:c0ff:fef2:6ca0   fe80::21e:c0ff:fef2:6ca1   DIN      97 ContractAuthenticationRes
41109 1253.104469  fe80::21e:c0ff:fef2:6ca1   fe80::21e:c0ff:fef2:6ca0   DIN      95 ContractAuthenticationReq
```

```
+ Frame 19981: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface ss
+ Ethernet II, Src: f6:92:bf:5c:3c:ab (f6:92:bf:5c:3c:ab), Dst: Intel_4e:75:c3 (98:59:7a
- Internet Protocol Version 4, Src: 192.168.67.10, Dst: 192.168.180.120
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  + Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0001 (1)
  + 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x01f1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.67.10
    Destination Address: 192.168.180.120
- Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x75ea [correct]
```

```
0000  98 59 7a 4e 75 c3 f6 92  bf 5c 3c ab 08 00 45 00   ·YzNu···  ·\<···E·
0010  00 38 00 01 00 00 40 01  01 f1 c0 a8 43 0a c0 a8   ·8····@·  ····C···
0020  b4 78 03 03 75 ea 00 00  00 00 45 00 00 1c 00 01   ·x··u···  ··E·····
0030  00 00 40 11 01 fd c0 a8  b4 78 c0 a8 43 0a 97 94   ··@·····  ·x··C···
0040  82 b5 00 08 6c c0                                  ····l·
```

wireshark_SSH remote captureCJ1BI2.pcapng   Packets: 41940 · Displayed: 41940 (100.0%)   Profile: Default

Step 16: Use Wireshark display filters to limit the number of shown packets to only include those you find interesting. Dig into those interesting packets and make some assumptions about their purpose and origin. What devices are sending those packets? What potential impacts might this have?

____

____

____

____

____