

## ## Challenge 2: Homework Network Analysis

After looking at bad traffic at work all day, you start to wonder what's going on on your home network.

- Run a capture on your homework network on any device. Leave the capture running in the background for 2+ hours. Be sure to use the device some while it is running!
- Stop the capture.
- Identify at least 2 instances of suspicious, interesting, and/or unfamiliar protocols/communication.
- To complete this challenge, you'll submit a document named `Home-Analysis` in your **Challenge-2** folder. It should include:
  - A 2-3 paragraph write-up for each of the communication examples (4-6 paragraphs total).
  - Images and screenshots to communicate how you found the communication, and how you investigated it.
  - An explanation of any unfamiliar protocols and how they work, if relevant.
  - A description of the purpose and outcome of that communication.

capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length
1590...	2019-09-11 12:41:44.601718	173.194.191.106	172.20.20.20	ar_drone	1392
84228	2019-09-11 12:39:38.091274	173.194.191.106	172.20.20.20	ar_drone	1392
1887...	2019-09-11 12:47:14.441005	172.217.8.164	172.20.20.20	UDP	63
1887...	2019-09-11 12:47:14.391131	172.20.20.20	172.217.8.164	UDP	65
1887...	2019-09-11 12:47:13.375726	108.177.112.189	172.20.20.20	UDP	63
1887...	2019-09-11 12:47:13.311562	172.20.20.20	108.177.112.189	UDP	65
1886...	2019-09-11 12:47:08.714133	172.20.20.20	172.217.214.189	UDP	71
1886...	2019-09-11 12:47:08.703658	172.217.214.189	172.20.20.20	UDP	86
1886...	2019-09-11 12:47:08.703658	172.217.214.189	172.20.20.20	UDP	236
1886...	2019-09-11 12:47:08.703565	172.217.214.189	172.20.20.20	UDP	63
1886...	2019-09-11 12:47:08.664980	172.20.20.20	172.217.214.189	UDP	327
1886...	2019-09-11 12:47:08.664084	172.20.20.20	172.217.214.189	UDP	71
1886...	2019-09-11 12:47:08.651715	172.217.214.189	172.20.20.20	UDP	66
1886...	2019-09-11 12:47:08.651154	172.217.214.189	172.20.20.20	UDP	82
1886...	2019-09-11 12:47:02.698052	172.217.5.14	172.20.20.20	UDP	62
1886...	2019-09-11 12:47:02.647417	172.20.20.20	172.217.5.14	UDP	65

> Frame 159085: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface 0  
 > Ethernet II, Src: 00:00:00\_02:02:02 (00:00:00:02:02:02), Dst: fa:28:f6:c5:8b:b3 (fa:28:f6:c5:8b:b3)  
 > Internet Protocol Version 4, Src: 173.194.191.106, Dst: 172.20.20.20  
 > User Datagram Protocol, Src Port: 443, Dst Port: 54676  
 > AR Drone Packet  
 > Command [truncated]: \357\277\275\r\357\277\275\_\023\357\277\275\357\277\275\357\277\275\037\357\277\275\357\277\275  
 > Data (1350 bytes)

This ar\_drone protocol is unfamiliar to me. After doing some research, this protocol is the AR Drone Packet. It's a UDP packet from port 5556. It captures the data that runs over the network between the network and client.

User Datagram Protocol, Src

AR Drone Packet

Command [truncated]: /&\

Data (1350 bytes)

Noticing these commands were truncated, I looked up the bug and it is named "Bugzilla-daemon". Basically, in contrast to other descriptor types, configuration descriptors have varying lengths and may be quite long. This makes them much more prone to truncation by a host that is cautious about reading large descriptors.