Erika Hernandez

CS 3705 – Fall 2021

Professor Paulson

Project Status Update

1. Have you selected your project?

Yes I have, So my project was to capture packets from my smart TV. So in my office, I have my computer. But in the background I have to have a TV playing. The TV is connected to my WiFi and I can stream videos and such.

2. Are you on track to finish the project by the due date?

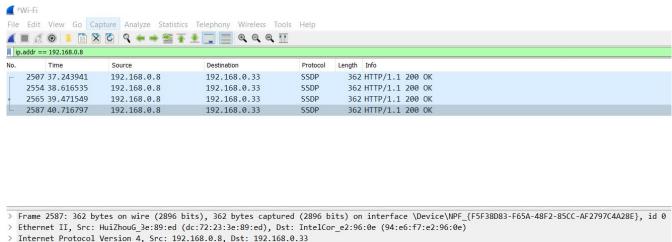
I hope so.

3. Have you run into any obstacles that you need help with?

Yes I have, So I was able to pick my TV IP address with Wireshark. The issue I'm running into is that is saying Protocol SSDP, shouldn't it TCP? Anyways, when I look at the Server it says Roku which is in the TV. But it wont give me much more information than that. So I then I found my Apple TV IP address and I wanted to see if it would do the same thing. It does, I would only see that my Apple TV is getting traffic sent back and fourth. But what its sending? I would get no information at all.

So I doesn't really give me much information about the packages themselves. So what I need to figure out, is how to take of the outer layer and get underneath the packages themselves. I mean is that even a possible? I spend a whole day trying to get this far. So perfect timing how you asked about this.

My next steps are to figure out if its even possible to go further into the packets and see if I can get the actual traffic that my TV Hisense that has Roku as I click on Amazon prime to watch a movie. Basically be the man in the middle of the traffic from the internet and the device its self.



```
Internet Protocol Version 4, Src: 192.168.0.8, Dst: 192.168.0.33
  User Datagram Protocol, Src Port: 1900, Dst Port: 57391
Simple Service Discovery Protocol
  > HTTP/1.1 200 OK\r\n
    Cache-Control: max-age=3600\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r
    Server: Roku/10.0.0 UPnP/1.0 Roku/10.0.0\r\n
    LOCATION: http://192.168.0.8:8060/dial/dd.xml\r\n
    WAKEUP: MAC=dc:72:23:3e:89:ed:Timeout=10\r\n
     [HTTP response 4/4]
    [Prev response in frame: 2565]
00e0 74 3a 20 0d 0a 53 65 72 76 65 72 3a 20 52 6f 6b
00f0 75 2f 31 30 2e 30 2e 30 20 55 50 6e 50 2f 31 2e
                                                      t: -- Ser ver: Rok
                                                      u/10.0.0 UPnP/1.
0100 30 20 52 6f 6b 75 2f 31
                             30 2e 30 2e 30 0d 0a 4c
                                                      0 Roku/1 0.0.0 -- L
0110 4f 43 41 54 49 4f 4e 3a 20 68 74 74 70 3a 2f 2f
                                                      OCATION: http://
0120 31 39 32 2e 31 36 38 2e
                             30 2e 38 3a 38 30 36 30
                                                      192.168. 0.8:8060
0130 2f 64 69 61 6c 2f 64 64 2e 78 6d 6c 0d 0a 57 41
                                                      /dial/dd .xml ·· WA
0140 4b 45 55 50 3a 20 4d 41 43 3d 64 63 3a 37 32 3a
                                                      KEUP: MA C=dc:72:
0150 32 33 3a 33 65 3a 38 39 3a 65 64 3b 54 69 6d 65
                                                      23:3e:89 :ed;Time
HTTP Server (http.server), 42 bytes
                                                                                                                                         Pack
```

Figure 1: WiFi capture of my TV IP address