**Wireshark Assignment**

**Group Members:** Nina Onwuachi (10190678)

                    Sarah Kaunain Syeda (30220873)

                                 Abigail Brown (30214975)

**Exercise 1:**

1. Source Port: 49344

2. Destination IP: 142.251.45.42

3. firebaseinstallations.googleapis.com:  addr 142.251.45.42

4. 104.18.226.52 and 104.18.225.52 was used

    104.18.225.52 was later used to communicate.

A screenshot of a computer

Description automatically generated

5. DNS

6.10.212.163.81

A screenshot of a computer

Description automatically generated

7. Google

A screenshot of a computer

Description automatically generated

8. 33

9. a). 0.0273secs

    b).m.quantcount.com: type CNAME, class IN, cname global.px.quantserve.com

     addr 192.184.69.141

     addr 192.184.69.139

     addr 192.184.69.149

     addr 192.184.69.146

     addr 192.184.69.231

     addr 192.184.69.152

     addr 192.184.69.143

10. >1400 = 20

      >1450 = 1

      >1500 = 0

11. Yes. ARP, DNS, HTTP. TLSv1.2, TLSv1.3, HTTP/JSON

12. 36

13. 27

14. a) 80

      b) 48408

      c)<http://m.quantcount.com/policy.json?v=1_2_3&t=ANDROID&c=us&a=17q11li05fgn48qm-sqv8zrfvy5ttz6s3>

       d) HTTP/1.1 200 OK

       e) 108

       f)  m.quantcount.com

       g)  0.029683 sec

**Exercise 2: Advanced Features**

1. 12
2. 4

A screenshot of a computer

Description automatically generated

1. Filter frame contains "6252dc85-958d-446d-9fab-1d2571a29023"

            Follow"" > ""TCP Stream.""

Inspect the content of the stream to make sure that the Advertising ID appears as expected and is not split into a different packet. Looking at the packets containing all the AAID, none is split over.

A screenshot of a computer

Description automatically generated

1. “gadid”

A screenshot of a computer

Description automatically generated

1. frame.number == 871

Then find ID number from package.

advshield.goforandroid.com

Yes, advertising ID is sent to it

A screenshot of a computer

Description automatically generated

1. Yes

frame contains "android\_id"

A screenshot of a computer

Description automatically generated

      7)  No. they all only the AAID, no UUIDs are sent

Filter by frame matches "([0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA- F]{4}-[0-9a-fA-F]{12})" to examine if any package contains a different UUID, none was found.

      8) There is a % sign in front of all 22 which indicates a quote “sign in URL for processing”. It means they is a specific encoding of the AAID. It will allow advertisers and app developers to track and target users for advertising purposes as well as for analytics.

A screenshot of a computer

Description automatically generated

      9)  Filter frame matches "[A-Za-z]{30}"

Long base sequence = eyJsYW5nIjoiZW4iLCJjb3VudHJ5IjoiVVMiLCJjaGFubmVsIjoyMDAsImN2ZXJzaW9uX25hbWUiOiIyLjkuMTIiLCJjdmVyc2lvbl9udW1iZXIiOjM5fQ

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

To decode the sequence, we used Retool, and it produced {"lang":"en","country":"US","channel":200,"cversion\_name":"2.9.12","cversion\_number":39}

Format is JSON object.

10. Filter frame matches “eyJ”

Using package, no 307, we follow TCP to find another base64 sequence.

eyJhaWQiOiIzYzZiMzNmNWE2NzZjNTllIiwibGFuZyI6ImVuIiwiY291bnRyeSI6IlVTIiwiY2hhbm5lbCI6IjIwMCIsInZlcnNpb25fbnVtYmVyIjozOSwibmV0X3R5cGUiOiJXSUZJIiwicGhvbmVfbW9kZWwiOiJBT1NQIG9uIHNhcmdvIiwic3lzdGVtX3ZlcnNpb25fbmFtZSI6IjEyIn0

A screenshot of a computer

Description automatically generated

{"aid":"3c6b33f5a676c59e","lang":"en","country":"US","channel":"200","version\_number":39,"net\_type":"WIFI","phone\_model":"AOSP on sargo","system\_version\_name":"12"}

aid":"3c6b33f5a676c59e” the advertising id being sent.

lang":"en" is the setting of the language which is set to English.

country":"US","is the setting of the system which is set to US.

channel":"200" is 200 which identifies the specific channel within the system.

version\_number":39is the version of the software system

net\_type":"WIFI shows that the system is connected to a Wifi network.

phone\_model":"AOSP on sargo shows the phone model is AOSP on sargo.

system\_version\_name":"12 is the operating system version name is 12.

It is used for finger printing purpose.