# Packet Analysis with Wireshark

Singhal, Madhur
2015CS10235

Chhajwani, Anant
2015CS50281

August 21, 2017

## 1 Introduction

Wireshark is a free and open source packet analyzer. It provides a Graphical User Interface for viewing packets that are travelling through the computer. Wireshark also decomposes the packet and extracts the fields for each layer the packet has encapsulated in it.

In this Assignment part we first use wireshark to understand different types of packets sent or receieved by our computer. Later we go on to analyze some simple requests and analyze the progression of packets related to them. All these experiments are done on a computer on WiFi running Ubuntu 17.10.

## 2 Background Packets

We captured the background packets for 60 seconds. Below are two pictures showing the different types of Protocols and Destinations that background packets comprise of.

| | | | | | |
|---|---|---|---|---|---|
| 0.000000000 | Cisco_7d:93:3f | Broadcast | ARP | 60 | Who has 10.192.25.121? Tell 10.192.0.1 |
| 0.923094289 | 10.192.2.64 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 0.925798956 | 10.192.13.227 | 239.255.255.250 | SSDP | 318 | NOTIFY * HTTP/1.1 |
| 0.929227310 | Microsof_ad:8f:ca | Broadcast | ARP | 52 | Who has 10.192.13.183? Tell 0.0.0.0 |
| 0.930363495 | Microsof_ad:8f:ca | Broadcast | ARP | 52 | Who has 10.192.0.1? Tell 10.192.13.183 |
| 0.931354185 | Microsof_ad:8f:ca | Broadcast | ARP | 52 | Who has 10.192.0.1? Tell 10.192.13.183 |
| 1.547262536 | 0.0.0.0 | 255.255.255.255 | DHCP | 368 | DHCP Request - Transaction ID 0x94580 |
| 1.741208473 | Cisco_7d:93:3f | Broadcast | ARP | 60 | Who has 10.192.23.123? Tell 10.192.0.1 |
| 1.744132241 | 10.192.31.252 | 10.192.31.255 | UDP | 305 | 54915 → 54915 Len=263 |
| 1.945873958 | AsustekC_1d:6d:5e | Broadcast | ARP | 52 | Who has 10.192.0.1? Tell 10.192.19.105 |
| 2.047799592 | ArubaNet_0e:45:80 | Broadcast | ARP | 56 | Who has 10.192.23.82? Tell 10.192.0.4 |
| 2.048898089 | 10.192.24.226 | 224.0.0.252 | LLMNR | 65 | Standard query 0x7cf1 A https |
| 2.458016897 | 10.192.24.226 | 224.0.0.252 | LLMNR | 65 | Standard query 0x7cf1 A https |
| 2.461306544 | 0.0.0.0 | 255.255.255.255 | DHCP | 346 | DHCP Discover - Transaction ID 0x93f7a |
| 2.462044610 | Cisco_7d:93:3f | Broadcast | ARP | 60 | Who has 10.192.0.239? Tell 10.192.0.1 |
| 2.662650685 | 10.192.1.65 | 224.0.0.251 | MDNS | 112 | Standard query 0x0000 PTR _sleep-proxy |
| 2.773860984 | 10.192.31.252 | 10.192.31.255 | UDP | 305 | 54915 → 54915 Len=263 |
| 3.074190246 | ArubaNet_0e:45:80 | Broadcast | ARP | 56 | Who has 10.192.23.82? Tell 10.192.0.4 |
| 3.379608992 | 10.194.19.206 | 224.0.0.252 | LLMNR | 65 | Standard query 0xf2ed ANY VD-PC |

.

| | | | | | |
|---|---|---|---|---|---|
| 40.144062717 | 10.192.25.225 | 239.255.255.250 | SSDP | 179 | M-SEARCH * HTTP/1.1 |
| 40.245368658 | 10.192.6.178 | 224.0.0.251 | MDNS | 173 | Standard query 0x0000 PTR _ni-rt._tcp. |
| 40.554754921 | 10.192.29.78 | 255.255.255.255 | UDP | 58 | 51108 → 40006 Len=16 |
| 40.556402091 | 10.192.11.6 | 224.0.0.251 | MDNS | 119 | Standard query 0x0003 PTR _C1EB68AE._s |
| 40.588451047 | 128.199.109.89 | 10.192.2.239 | TCP | 66 | 80 → 55272 [FIN, ACK] Seq=1 Ack=2 Win= |
| 40.588527130 | 10.192.2.239 | 128.199.109.89 | TCP | 66 | 55272 → 80 [ACK] Seq=2 Ack=2 Win=241 L |
| 40.656486484 | 10.192.6.178 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 40.660894643 | ArubaNet_0e:45:80 | Broadcast | ARP | 56 | Who has 10.192.25.121? Tell 10.192.0.4 |
| 40.765450786 | 10.192.29.253 | 10.192.31.255 | NBNS | 92 | Name query NB WORKGROUP<1c> |
| 40.863842075 | 10.192.15.109 | 224.0.0.251 | MDNS | 103 | Standard query 0x0003 PTR _D2CA5178._s |
| 41.795064164 | 10.192.31.252 | 10.192.31.255 | UDP | 305 | 54915 → 54915 Len=263 |
| 41.802444637 | 0.0.0.0 | 255.255.255.255 | DHCP | 356 | DHCP Discover - Transaction ID 0x20a5a |
| 41.804587122 | Cisco_7d:93:3f | Broadcast | ARP | 60 | Who has 10.192.10.171? Tell 10.192.0.1 |
| 42.089245098 | 10.192.25.53 | 224.0.0.251 | MDNS | 103 | Standard query 0x0002 PTR _805741C9._s |
| 42.703771471 | 10.192.6.178 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 42.706706100 | 10.192.4.100 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 43.317854279 | 10.192.28.44 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 43.627130892 | 10.192.7.114 | 224.0.0.251 | MDNS | 112 | Standard query 0x0000 PTR _sleep-proxy |
| 43.629097505 | 10.192.6.178 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |

## Applications

1. **ARP Packets** The IP module generates the ARP (Address Resolution Protocol) packets. They are used to resolve local IP addresses into MAC addresses. The Destination address for such packets is "Broadcast" which means they are automatically sent to all receivers on the WiFi Network.

2. **SSDP Packets** The SSDP (Simple Service Discovery Protocol is used to discover services being offered on the local network. The SSDP packets were originating elsewhere so I think the application generating them was in some other computer on the network. Some analysis suggests that windows may be automatically sending those packets to search for services.

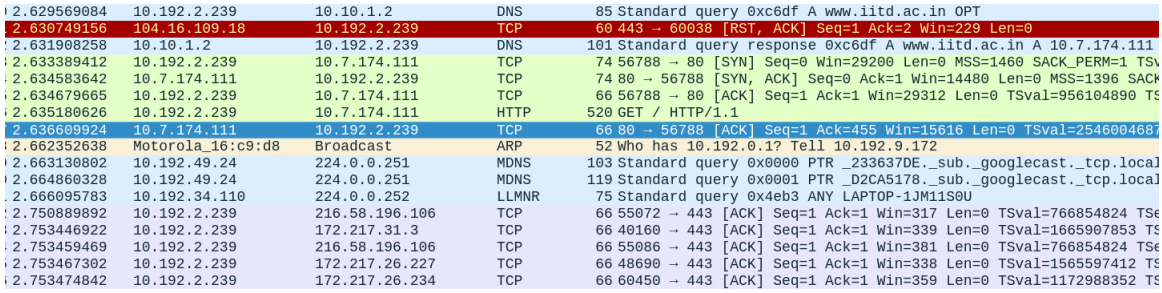
3. **LLMNR Packets** The LLMNR (Link-Local Multicast Name Resolution) is used to resolve addresses to local addresses. It is generated by systemd on Ubuntu.

4. **MDNS Packets** The MDNS ( Multicast Domain Name System) is used in this context for providing wake on ping services. Apple devices provide this service, wherein you can wake up a sleeping device by sending a proper packet to it.

5. **NBNS Packets** The NBNS (Net Bios Name Resolution System) provides name resolution for legacy Net-Bios over IP Services. It is primarily used by Windows to maintain it's sharing features.

6. **Miscellaneous Packets** There are some other TCP and UDP packets with encrypted data so I can't find out what is generating them. Could be vestiges of previous connections to web servers before starting the scan.

# 3 Analysis of Webpage Fetch



| | | | | | |
|---|---|---|---|---|---|
| 2.629569084 | 10.192.2.239 | 10.10.1.2 | DNS | 85 | Standard query 0xc6df A www.iitd.ac.in OPT |
| 2.630749156 | 104.16.109.18 | 10.192.2.239 | TCP | 60 | 443 → 60038 [RST, ACK] Seq=1 Ack=2 Win=229 Len=0 |
| 2.631908258 | 10.10.1.2 | 10.192.2.239 | DNS | 101 | Standard query response 0xc6df A www.iitd.ac.in A 10.7.174.111 |
| 2.633389412 | 10.192.2.239 | 10.7.174.111 | TCP | 74 | 56788 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSv |
| 2.634583642 | 10.7.174.111 | 10.192.2.239 | TCP | 74 | 80 → 56788 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1396 SACK |
| 2.634679665 | 10.192.2.239 | 10.7.174.111 | TCP | 66 | 56788 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=956104890 TS |
| 2.635180626 | 10.192.2.239 | 10.7.174.111 | HTTP | 520 | GET / HTTP/1.1 |
| 2.636609924 | 10.7.174.111 | 10.192.2.239 | TCP | 66 | 80 → 56788 [ACK] Seq=1 Ack=455 Win=15616 Len=0 TSval=2546004687 |
| 2.662352638 | Motorola_16:c9:d8 | Broadcast | ARP | 52 | Who has 10.192.0.1? Tell 10.192.9.172 |
| 2.663130802 | 10.192.49.24 | 224.0.0.251 | MDNS | 103 | Standard query 0x0000 PTR _233637DE._sub._googlecast._tcp.local |
| 2.664860328 | 10.192.49.24 | 224.0.0.251 | MDNS | 119 | Standard query 0x0001 PTR _D2CA5178._sub._googlecast._tcp.local |
| 2.666095783 | 10.192.34.110 | 224.0.0.252 | LLMNR | 75 | Standard query 0x4eb3 ANY LAPTOP-1JM11S0U |
| 2.750889892 | 10.192.2.239 | 216.58.196.106 | TCP | 66 | 55072 → 443 [ACK] Seq=1 Ack=1 Win=317 Len=0 TSval=766854824 TSe |
| 2.753446922 | 10.192.2.239 | 172.217.31.3 | TCP | 66 | 40160 → 443 [ACK] Seq=1 Ack=1 Win=339 Len=0 TSval=1665907853 TS |
| 2.753459469 | 10.192.2.239 | 216.58.196.106 | TCP | 66 | 55086 → 443 [ACK] Seq=1 Ack=1 Win=381 Len=0 TSval=766854824 TSe |
| 2.753467302 | 10.192.2.239 | 172.217.26.227 | TCP | 66 | 48690 → 443 [ACK] Seq=1 Ack=1 Win=338 Len=0 TSval=1565597412 TS |
| 2.753474842 | 10.192.2.239 | 172.217.26.234 | TCP | 66 | 60450 → 443 [ACK] Seq=1 Ack=1 Win=359 Len=0 TSval=1172988352 TS |

1. **Servers for which a DNS query was launched** Only one DNS query for www.iitd.ac.in was launched. The response was 10.7.174.111.

2. **Number of HTTP requests generated** After filtering the packets to http only, I see 162 packets, half of which are requests and the other half are responses. Thus **81 Requests** are generated.

3. **Number of TCP connections opened - Six** TCP connections were opened.

4. **Total time taken for download** The total time taken was **2.7575 seconds.**

5. **Any TCP losses/retransmits noticed** No Losses/Retransmits observed.

## HTTP Request

```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
       [GET / HTTP/1.1\r\n]
       [Severity level: Chat]
       [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
  Host: www.iitd.ac.in\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  DNT: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  Cookie: SESS1f002926bf876664ed5383994cb4c1de=qes0234q558315psi5m0rtda61\r\n
  \r\n
  [Full request URI: http://www.iitd.ac.in/]
  [HTTP request 1/13]
  [Response in frame: 155]
  [Next request in frame: 172]
```

## TCP Header

```
Transmission Control Protocol, Src Port: 56788, Dst Port: 80, Seq: 455, Ack: 10133, Len: 0
  Source Port: 56788
  Destination Port: 80
  [Stream index: 3]
  [TCP Segment Len: 0]
  Sequence number: 455    (relative sequence number)
  Acknowledgment number: 10133    (relative ack number)
  Header Length: 32 bytes
  Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
```

```
0000  50 57 a8 7d 93 3f 58 00  e3 d5 28 af 08 00 45 00   PW.}.?X. ..(...E.
0010  00 34 f8 c6 40 00 40 06  7b d8 0a c0 02 ef 0a 07   .4..@.@. {.......
0020  ae 6f dd d4 00 50 4c ca  11 25 0d b0 be c5 80 10   .o...PL. .%......
0030  01 99 c6 4b 00 00 01 01  08 0a 38 fd 01 5f 97 c0   ...K.... ..8.._..
0040  f3 64                                             .d
```

## IP Header

```
Internet Protocol Version 4, Src: 10.192.2.239, Dst: 10.7.174.111
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0xf8bf (63679)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  Header checksum: 0x7bdf [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.192.2.239
  Destination: 10.7.174.111
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```