Thomas Bong

HW 5

November 10 2016

CSE 410

1.a)

1.b)

TCP packets from a variety of sources such as 45.33.49.119, 103.246.57.52, or 104.16.107.204 to 172.19.248.98 was sent from [Source GeoIP: Absecon, NJ, AS6939 Hurricane Electric, Inc., United States, 39.489899, -74.477303], [Source GeoIP: Jeju, 01, AS10158 KAKACO, Korea, Republic of, 33.509701, 126.521896], [Source GeoIP: San Francisco, CA, AS13335 CloudFlare, Inc., United States, 37.769699, -122.393303] and the destination geoIP is unknown.

2.a)

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol | Packet Type | Packet Frequency | Purpose |
| TCP |  | 54963(96.1%) |  |
| ARP |  | 1621(2.8%) |  |
| HTTP |  | 74(0.1%) |  |
| DNS |  | 403(0.7%) |  |
| ICMP |  | 92(0.2%) |  |

TCP takes up about 96% of all the protocols captured.

2.b)

2 corrupt packets from ICMP. 1493 corrupt TCP packets. This pcap file must have been captured over a wired Internet because the link type for each packet is Ethernet.

3.a)

TCP: Source/Destination ports, Stream index, Sequence Number, ACK number.

ARP:Hardware Type, protocol type, hardware size, protocol size, MAC address.

[HTTP: Request](http://Request/) Version, Status Code, Response Phrase.

DNS: UDP, Response Time, Queries,

ICMP: Echo request, Checksum.

3.b) TCP:

IP:

UDP:

4.a) From the payload, we can extract information such as source/destination address or port, sequence number, acknowledgement number, etc.

4.b) The most captured protocol is TCP. TCP is about 96% of all the protocols in the pcap file given.