Thomas Bong

HW 5

November 10 2016

CSE 410

1.a)

By extracting the information of each packet’s MAC address, there were 2 Manufacturers: Matsushi Avionics System Coroporation and Apple. And By extracting the information of HTTP packet’s, the companies such as Cloudflare,inc, Kakao Company, Time Warner Cable appeared. From the TCP packets, Facebook, Inc, Google, Inc, Hurricane Electric, inc, Amazon appeared.

Potential devices that were captured in this pcap file may be a laptops or desktops.

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. Also, by looking up some of the IP addresses, UB, Google, Akamai Technologies, Facebook, Skype, Microsoft, Daum, etc appeared.

2.a)

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol | Packet Type | Packet Frequency | Purpose |
| TCP | ACK,PSH,RST,FIN,SYN | 54963(96.1%) | Communication between 2 network devices |
| ARP | ARP | 1621(2.8%) | Convert an IP address into a physical address |
| HTTP | PSH,ACK, | 74(0.1%) | Data is sent from a browser to a website |
| DNS | Type NS, A PTR | 403(0.7%) | Map a domain name with an IP address |
| ICMP | Ping request,3(destination unreachable) | 92(0.2%) | Error report on the network, such as network routes, packet loss. |

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, and the number of lost packets is very small compared to the number of total packets in this file.

3.a)

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

**ARP**:Hardware Type, protocol type, hardware size, protocol size, MAC/IP address of sender/target.

[**HTTP:** Request](http://Request/) Version, Status Code, Response Phrase, Host, Accept-Language, Accept-Encoding, X-Requested-With, Cookie.

**DNS**: UDP, Response Time, Queries, Flags, Answers, Authoritative nameservers.

**ICMP:** Type,Code,Identifier,Sequence number, Checksum.

3.b)

TCP:Source/Destination port, Sequence number, Acknowledgement number, checksum, payload, etc.

IP: Source/Destination Address, Packet length, Time to live, IP protocol version, Transport layer protocol, and fragmentation info.

DNS: Authoritative nameservers.

4.a)

From the payload, we can extract information such as source/destination address and/or port, sequence number, acknowledgement number and other contents of the data.

4.b)

By using a packet sniffer such as Wireshark, you are able to extract information that may be considered as private. You can use a filter for ip address, for example, ip.addr == 172.217.1.70, applying this filter would return all the packets and counts of those including the according ip address as either the source or destination. Another privacy value is using a filter to look up a packet with a url. For example, with a filter such as ‘http contains “google.com”’ or ‘http contains “http://www.google.com”’ would return corresponding packets. These examples show how packet sniffers may capture packets and extract information about the source/destination address, what kind of data is being sent, etc.

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