Alex Tran #919196458

Muhammad Reza # 919508305

Pcap files:

google.pcap, example.pcap, httpforever.pcap, ftp.pcap, ssh.pcap

Python files:

google.py, example.com.py, httpforever.py, ftp.py, ssh.pcap

1.

For pinging google in the first activity, the application layer protocol was ICMP and we received in total, 40 of them with one for making the ping request from the client and one for the reply from the server. We were about to figure this out because of the pattern of Echo ping request/reply on a section of Wireshark. For example.com, there were in total 5 application layer protocols with the TCP 3 way handshake and a HTTP GET request and the corresponding response containing the HTML text from the server. We figured out these numbers through filtering based on TCP and HTTP requests in Wireshark and through the assigned port for HTTP which was port 80. For httpforever.com, there are also 5 application layer protocols, with the TCP 3 way handshake and the HTTPS GET request and the corresponding response. We used the same method as example.com. The FTP request had 15 application layer protocols of type FTP and we obtained this using the FTP filter in Wireshark. For SSH with SDF Public Access UNIX System, we obtained a total of 117 SSHv2 protocols and we figured this out through the assigned port of SSH which is port 22.

2.

For activities 2 and 3, I got 2 HTTPS requests with example.com and 2 HTTP requests with httpforever.com.

3.

Google.com pinging

```
Protocol: ICMP, Timestamp: 1697949286.995907, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949287.015038, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949288.001158, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949288.022679, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949289.004936, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949289.028942, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949290.012601, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949290.034014, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949291.017045, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949291.037634, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949292.021827, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949292.044732, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949293.025577, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949293.046743, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949294.02636, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949294.045932, Dest IP Address: 10.0.0.161
Protocol: ICMP, Timestamp: 1697949295.031663, Dest IP Address: 172.217.12.110
Protocol: ICMP, Timestamp: 1697949295.056638, Dest IP Address: 10.0.0.161
```

```
Protocol: ICMP, Timestamp: 1697949296.036217, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949296.061909, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949297.037629, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949297.062457, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949298.040806, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949298.063201, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949299.042198, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949299.05936, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949300.046566, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949300.06646, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949301.052014, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949301.080051, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949302.05711, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949302.086767, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949303.06178, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949303.080274, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949304.066388, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949304.213416, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949305.071758, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949305.087441, Dest IP Address: 10.0.0.161

Protocol: ICMP, Timestamp: 1697949306.074971, Dest IP Address: 172.217.12.110

Protocol: ICMP, Timestamp: 1697949306.096051, Dest IP Address: 10.0.0.161
```

```
example.com:
Protocol: HTTP, Timestamp: 1698005056.944875, Dest IP Address: 93.184.216.34
Protocol: HTTP, Timestamp: 1698005056.96296, Dest IP Address: 168.150.113.10

httpforever.com:
Protocol: HTTP, Timestamp: 1698006221.774743, Dest IP Address: 146.190.62.39

ftp:
Protocol: FTP, Timestamp: 1698007650.284424, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007654.471157, Dest IP: 209.51.188.20
Protocol: FTP, Timestamp: 1698007655.049258, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050816, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050817, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050818, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050819, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050819, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.05082, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.05082, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050821, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.050821, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007655.224199, Dest IP: 168.150.113.10
Protocol: FTP, Timestamp: 1698007658.799334, Dest IP: 209.51.188.20
Protocol: FTP, Timestamp: 1698007658.901312, Dest IP: 168.150.113.10
```

SSH:

```
Protocol: SSHv2, Timestamp: 1698625842.747725, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625842.822189, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625842.823911, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625842.865639, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625843.068212, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625843.147656, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625843.147659, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625843.189495, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625843.466765, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625843.510993, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625843.511591, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625843.623425, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625843.624189, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625843.69337, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625843.694742, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625843.753504, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625844.802178, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625844.903794, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625844.90512, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625844.947615, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625844.994423, Dest IP Address: 10.0.0.161
```

```
Protocol: SSHv2, Timestamp: 1698625844.995202, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625845.0524, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625845.125666, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625845.1267, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625845.1267, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625846.300849, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625846.569076, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625847.051143, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051146, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051146, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051147, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051148, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051148, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051247, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051247, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.051248, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.055038, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.057839, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.061896, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.065282, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.069803, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.072789, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.075891, Dest IP Address: 10.0.0.161
```

```
Protocol: SSHv2, Timestamp: 1698625847.080157, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.083891, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.090567, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.090712, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.094711, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.097432, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.101133, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.107562, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.10896, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.110791, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.114915, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.119981, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.128932, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.133215, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.136837, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.141679, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625847.14174, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.307447, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625848.351908, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.360317, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.360365, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.360366, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362238, Dest IP Address: 10.0.0.161
```

```
Protocol: SSHv2, Timestamp: 1698625848.362239, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.36224, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362241, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362242, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362242, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362243, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362244, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362244, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362245, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362245, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362246, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362247, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362247, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362248, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362248, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362249, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.36225, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362251, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362251, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362252, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625848.362252, Dest IP Address: 10.0.0.161

Protocol: SSHv2, Timestamp: 1698625850.199738, Dest IP Address: 205.166.94.4

Protocol: SSHv2, Timestamp: 1698625850.248935, Dest IP Address: 10.0.0.161
```

```
Protocol: SSHv2, Timestamp: 1698625850.277635, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.277638, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.277639, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.27764, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.277641, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.294602, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.294605, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.294605, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.294606, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.294606, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.32084, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.322146, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.322457, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625850.348971, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625852.219451, Dest IP Address: 205.166.94.4
Protocol: SSHv2, Timestamp: 1698625852.264722, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625852.442263, Dest IP Address: 205.166.94.4
Protocol: SSHv2, Timestamp: 1698625852.482126, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625852.585, Dest IP Address: 205.166.94.4
Protocol: SSHv2, Timestamp: 1698625852.624518, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625852.783755, Dest IP Address: 205.166.94.4
Protocol: SSHv2, Timestamp: 1698625852.830148, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625853.15902, Dest IP Address: 205.166.94.4
```

```
Protocol: SSHv2, Timestamp: 1698625853.199975, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625853.223843, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625853.224311, Dest IP Address: 10.0.0.161
Protocol: SSHv2, Timestamp: 1698625853.224312, Dest IP Address: 10.0.0.161
```

4.

Yes you can. If you take a look at the payload in the application layer of the HTTP request sent from the client to server, there is a user agent field which specifies the web browser being used.