Billy Ouattara (920603707)
Jose Gavidia (921477055)
part1a.py, ping.pcap, example.pcap, httpforever.pcap, ftp.pcap, ssh.pcap

1. To figure out the application layer requests, we first identified wich command or request are associated with which application layer protocol. After doing so, we record their respective port numbers. Below are the port numbers associated with the application layer protocols that was used. http: port 80, https: port 443, ftp: port 20 || 21, lastly ssh: port 22. Below are the list of application layer protocols as well as their count for each respective activities performed:
    a. http: 29, https: 330, icmp: 268, ftp: 0, ssh: 0 (Ping)
    b. http: 0, https: 37, icmp: 0, ftp: 0, ssh: 0 (example.com)
    c. http: 2, https: 62, icmp: 0, ftp: 0, ssh: 0 (httpforever.com)
    d. http: 0, https: 81, icmp: 0, ftp: 3, ssh: 0 (ftp)
    e. http: 0, https: 209, icmp: 0, ftp: 0, ssh: 43 (ssh sdf)
2. Below is the summary of HTTP and HTTPS packets from both activities 2 and 3
    a. Activity 2: 0 HTTP packets and 37 HTTPS packets
    b. Activity 3: 2 HTTP packets and 62 HTTPS packets
3. List of destination IPs and their timestamps
    a. PING.PCAP Report:
        i. Destination IP Address: 142.250.191.78
        ii. Timestamps:
        [1698713944.119941, 1698713945.132646, 1698713946.157904, 1698713947.166129, 1698713948.175875, 1698713949.181564, 1698713950.198401, 1698713951.223787, 1698713952.246073, 1698713953.25955, 1698713954.268858, 1698713955.280212, 1698713956.286935, 1698713956.807297, 1698713956.807544, 1698713956.807807, 1698713956.835183, 1698713956.835251, 1698713956.85168, 1698713956.860848, 1698713956.901046, 1698713956.907147, 1698713957.302634, 1698713958.329246, 1698713958.593002, 1698713958.628671, 1698713958.629004, 1698713958.660097, 1698713959.336699, 1698713960.193949, 1698713960.211415, 1698713960.211481, 1698713960.211557, 1698713960.223075, 1698713960.24468, 1698713960.272223, 1698713960.349016, 1698713961.36186, 1698713962.377658, 1698713963.398176]

    b. EXAMPLE.PCAP Report:
        i. Destination IP Address: 93.184.216.34
        ii. Timestamps:
        [1698701962.654152, 1698701962.904633, 1698701962.904868, 1698701963.006085, 1698701963.032141, 1698701963.03409, 1698701963.034234, 1698701963.084678, 1698701963.136865]
    c. HTTPFOREVER.PCAP Report:

        i. Destination IP Address: 146.190.62.39
        ii. Timestamps: [1698701862.521871, 1698701862.61904]
    d. FTP.PCAP Report:
        i. Destination IP Address: 209.51.188.20
        ii. Timestamps: [1698702141.302639, 1698702141.440621, 1698702141.716018, 1698702141.990116]
    e. SSH.PCAP Report:
        i. Destination IP Address: 205.166.94.9
        ii. Timestamps: [1698703129.54498, 1698703129.585235, 1698703129.585402, 1698703129.671966, 1698703129.671966, 1698703129.738837, 1698703129.744062, 1698703129.893737, 1698703129.947694, 1698703129.998238, 1698703130.114288, 1698703130.216723, 1698703132.733626, 1698703132.861433, 1698703132.965559, 1698703133.032997, 1698703133.153111, 1698703136.892763, 1698703137.206843, 1698703137.470811, 1698703137.470894, 1698703137.470926, 1698703137.481641, 1698703137.633209, 1698703137.633239, 1698703137.633251, 1698703137.633262, 1698703137.633272, 1698703137.633282, 1698703138.053125]
4. For activity 3, we can tell which browser was used using the user agent attribute. However, concerning activity 2, since it is an HTTPS packet, its data is encrypted. Therefore we can analyze its content and determine which browser was used.