

1. Alyssa Vallejo (918606017)
2. Isabel Vong (919912852)
3. Part 1B source code: <https://github.com/AV-CompSci-Mage/152AProject1.git>
 - a. dkpt_analyze.py
 - b. dkpt_analyze_chatgpt.py
 - c. icmp_analyze.py
 - d. icmp_analyze_chatgpt.py

Part 1b: Analyzing Pcap files

```
C:\Users\Isabel\Desktop\EEC 173A>dkpt_analyze.py ass1_1.pcap
Host: example.com
User-agent: curl/7.77.0
Accept: */*
b'GET /?secret=secret1 HTTP/1.1\r\nHost: example.com\r\nUser-Agent: curl/7.77.0\r\nAccept: */*\r\n\r\n'

Host: example.com
User-agent: curl/7.77.0
Accept: */*
Secret: secret2
b'GET / HTTP/1.1\r\nHost: example.com\r\nUser-Agent: curl/7.77.0\r\nAccept: */*\r\nsecret: secret2\r\n\r\n'

Host: example.com
User-agent: curl/7.77.0
Accept: */*
Content-type: application/json
Content-length: 20
b'POST / HTTP/1.1\r\nHost: example.com\r\nUser-Agent: curl/7.77.0\r\nAccept: */*\r\nContent-Type: application/json\r\nContent-Length: 20\r\n\r\n{"secret":"secret3"}'
```

Screenshot of results from running dkpt_analyze.py on ass1_1.pcap

It is seen from the syntax of the request-line (GET /?secret=secret1) that the first secret is a query.

The second secret is a header of the HTTP GET request, and the third secret is data structured in JSON format– {“secret”:”secret3”}. The string secret3 is the value associated with secret.

Link to ChatGPT session: <https://chatgpt.com/share/672da3ae-c450-8000-a8d8-a19e5a4c7196>

[illegible]

Screenshot of some results from running icmp_analyze.py on ass1_3.pcap

Screenshot of some results from running icmp_analyze.py on ass1_3.pcap

The main protocol in the ass1_2.pcap and ass1_3.pcap is ICMP, which is a connectionless protocol and a network layer protocol used by network devices to diagnose network communication issues/send error messages when communicating with another IP address. The activity being performed in these pcap files are traceroutes. The route from host to server is traced through hops to/from routers. The time-to-live exceeded responses are from each hop along the route.

The difference between the two pcap files is that the source and destination are different. There's a noticeable difference in time between packets for each of the pcap files, which could be attributed to a slower/more complex network path (the router may also be already experiencing congestion).

Link to ChatGPT session: <https://chatgpt.com/share/672da447-d424-8000-be2d-bcb68d985097>