1. Alyssa Vallejo (918606017)
2. Isabel Vong (919912852)
3. Part 1B source code: https://github.com/AV-CompSci-Mage/152AProject1.git
    a. dkpt_analyze_alyssavallejo_918606017_isabelvong_919912852.py
    b. dkpt_analyze_chatgpt_alyssavallejo_918606017_isabelvong_919912852.py
    c. icmp_analyze_alyssavallejo_918606017_isabelvong_919912852.py
    d. icmp_analyze_chatgpt_alyssavallejo_918606017_isabelvong_919912852.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\nCo
ntent-Length: 20\r\n\r\n{"secret":"secret3"}'
```

Screenshot of results from running DKPT analysis code 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

```
C:\Users\Isabel\Desktop\EEC 173A>icmp_analyze.py ass1_2.pcap


C:\Users\Isabel\Desktop\EEC 173A\icmp_analyze.py:37: DeprecationWarning: datetime.datetime.utcfromtimestamp() is de
precated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: d
atetime.datetime.fromtimestamp(timestamp, datetime.UTC).
  print('Timestamp: ', str(datetime.datetime.utcfromtimestamp(timestamp)))
Timestamp:  2023-10-21 07:25:06.577492
IP: 192.168.80.223 -> 192.168.80.84
Type: 11
Code: 0
Checksum: 15369
Data: TimeExceed(data=IP(len=52, id=34693, ttl=1, p=17, sum=60252, src=b'\xc0\xa8PT', dst=b']\xb8\xd8"', opts=b'',
data=UDP(sport=34692, dport=33435, ulen=32, sum=44726, data=b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'')))


Timestamp:  2023-10-21 07:25:06.582013
IP: 192.168.80.223 -> 192.168.80.84
Type: 11
Code: 0
Checksum: 15369
Data: TimeExceed(data=IP(len=52, id=34694, ttl=1, p=17, sum=60251, src=b'\xc0\xa8PT', dst=b']\xb8\xd8"', opts=b'',
data=UDP(sport=34692, dport=33436, ulen=32, sum=44725, data=b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'')))


Timestamp:  2023-10-21 07:25:06.590334
IP: 192.168.80.223 -> 192.168.80.84
Type: 11
Code: 0
Checksum: 15369
Data: TimeExceed(data=IP(len=52, id=34695, ttl=1, p=17, sum=60250, src=b'\xc0\xa8PT', dst=b']\xb8\xd8"', opts=b'',
data=UDP(sport=34692, dport=33437, ulen=32, sum=44724, data=b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'')))
```

Screenshot of some results from running ICMP analysis code on ass1_2.pcap

```
C:\Users\Isabel\Desktop\EEC 173A\icmp_analyze.py:37: DeprecationWarning: datetime.datetime.utcfromtimestamp() is de
precated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: d
atetime.datetime.fromtimestamp(timestamp, datetime.UTC).
  print('Timestamp: ', str(datetime.datetime.utcfromtimestamp(timestamp)))
Timestamp:  2023-10-21 07:26:27.484760
IP: 10.0.0.1 -> 10.0.0.252
Type: 11
Code: 0
Checksum: 13832
Data: TimeExceed(data=IP(len=52, id=34758, ttl=1, p=17, sum=61724, src=b'\n\x00\x00\xfc', dst=b']\xb8\xd8"', opts=b
'', data=UDP(sport=34757, dport=33435, ulen=32, sum=46198, data=b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'')))


Timestamp:  2023-10-21 07:26:27.490726
IP: 10.0.0.1 -> 10.0.0.252
Type: 11
Code: 0
Checksum: 13832
Data: TimeExceed(data=IP(len=52, id=34759, ttl=1, p=17, sum=61723, src=b'\n\x00\x00\xfc', dst=b']\xb8\xd8"', opts=b
'', data=UDP(sport=34757, dport=33436, ulen=32, sum=46197, data=b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'')))


Timestamp:  2023-10-21 07:26:27.496899
IP: 10.0.0.1 -> 10.0.0.252
Type: 11
Code: 0
Checksum: 13832
Data: TimeExceed(data=IP(len=52, id=34760, ttl=1, p=17, sum=61722, src=b'\n\x00\x00\xfc', dst=b']\xb8\xd8"', opts=b
'', data=UDP(sport=34757, dport=33437, ulen=32, sum=46196, data=b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'')))
```

Screenshot of some results from running ICMP analysis code 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/672dab08-ad14-8000-aa08-d52b0e5bba0a