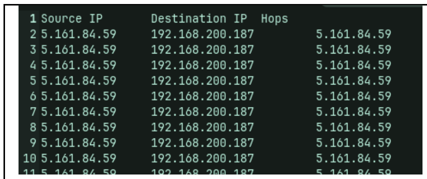
My Contribution in the project

Analysing network packets (pcap files)

Version 1.0: Gathering the list of hops and the details of the communications (Source and Destination IPs, time, packet length, Protocols) and storing them in a file.

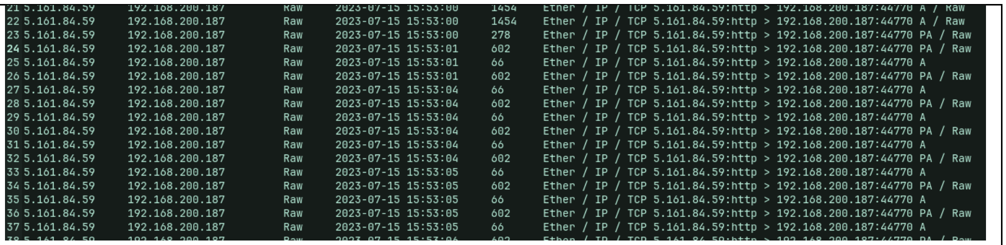
Here, the pcap file provided was analyzed and the list of hops, other details of the communication such as timestamp, packet length, protocol used was captured.

File: pcappostmortem.py



```
Source IP        Destination IP  Hops
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
5.161.84.59      192.168.200.187           5.161.84.59
```

hop_list.txt



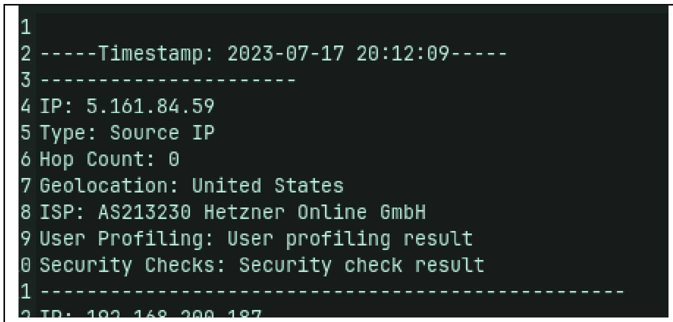
```
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:00     1454    Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:00     1454    Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:00     278     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:01     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:01     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:01     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:04     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:04     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:04     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:04     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:04     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:04     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:05     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:05     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:05     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:05     602     Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 PA / Raw
5.161.84.59     192.168.200.187         Raw     2023-07-15 15:53:05     66      Ether / IP / TCP 5.161.84.59:http > 192.168.200.187:44770 A
```

communication_patterns.txt

Version 2.0: Gathering the list of IPs, The type (Source or Destination), the hop count, Geolocation and ISP

Here, the pcap file provided was analyzed and the list of IPs, the type of IPs (Source or Destnation), the hop count, geolocation and ISP was gathered

File: gatheralldata.py



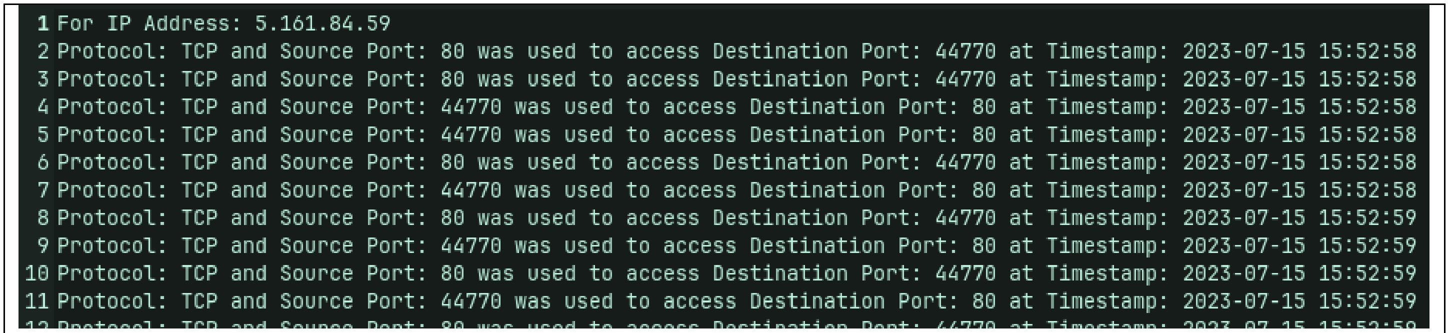
```

-----Timestamp: 2023-07-17 20:12:09-----
----------------------
IP: 5.161.84.59
Type: Source IP
Hop Count: 0
Geolocation: United States
ISP: AS213230 Hetzner Online GmbH
User Profiling: User profiling result
Security Checks: Security check result
--------------------------------------------------
```

GatherAllData.log

Version 2.1: Micro-information: Gathering details on what IP accessed which port to communicate with a certain destination IP.

Here, the pcap file provided was analyzed and a minute detail on what IP accessed which port to communicate with a certain destination IP was gathered.

File: gatheralldata.py



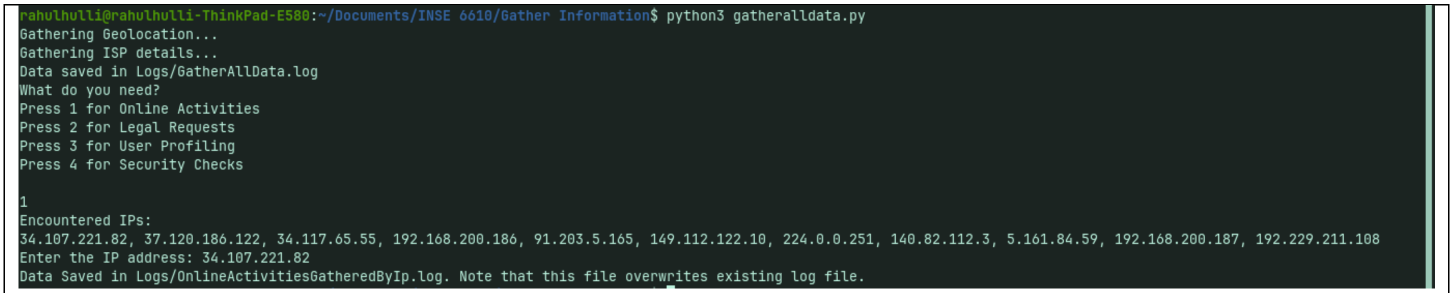
```
For IP Address: 5.161.84.59
Protocol: TCP and Source Port: 80 was used to access Destination Port: 44770 at Timestamp: 2023-07-15 15:52:58
Protocol: TCP and Source Port: 80 was used to access Destination Port: 44770 at Timestamp: 2023-07-15 15:52:58
Protocol: TCP and Source Port: 44770 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:52:58
Protocol: TCP and Source Port: 44770 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:52:58
Protocol: TCP and Source Port: 80 was used to access Destination Port: 44770 at Timestamp: 2023-07-15 15:52:58
Protocol: TCP and Source Port: 44770 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:52:58
Protocol: TCP and Source Port: 80 was used to access Destination Port: 44770 at Timestamp: 2023-07-15 15:52:59
Protocol: TCP and Source Port: 44770 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:52:59
Protocol: TCP and Source Port: 80 was used to access Destination Port: 44770 at Timestamp: 2023-07-15 15:52:59
Protocol: TCP and Source Port: 44770 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:52:59
```

OnlineActivities.log

Version 2.2: Micro-information: Gathering details on what IP accessed which port to communicate with a certain destination IP – You now select the target IP to gather information.

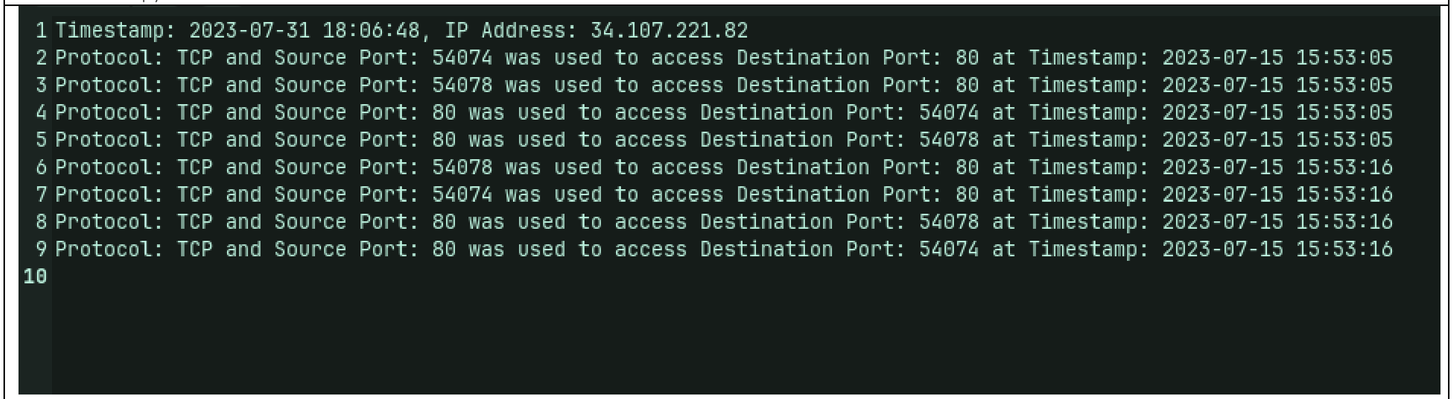
Here, the pcap file provided was analyzed and a minute detail on what IP accessed which port to communicate with a certain destination IP was gathered. Now you select the IP that you need to get details on and the details will be saved in a file.

File: gatheralldata.py



```
rahulhulli@rahulhulli-ThinkPad-E580:~/Documents/INSE 6610/Gather Information$ python3 gatheralldata.py
Gathering Geolocation...
Gathering ISP details...
Data saved in Logs/GatherAllData.log
What do you need?
Press 1 for Online Activities
Press 2 for Legal Requests
Press 3 for User Profiling
Press 4 for Security Checks

1
Encountered IPs:
34.107.221.82, 37.120.186.122, 34.117.65.55, 192.168.200.186, 91.203.5.165, 149.112.122.10, 224.0.0.251, 140.82.112.3, 5.161.84.59, 192.168.200.187, 192.229.211.108
Enter the IP address: 34.107.221.82
Data Saved in Logs/OnlineActivitiesGatheredByIp.log. Note that this file overwrites existing log file.
```

Gatheralldata.py



```
Timestamp: 2023-07-31 18:06:48, IP Address: 34.107.221.82
Protocol: TCP and Source Port: 54074 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:53:05
Protocol: TCP and Source Port: 54078 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:53:05
Protocol: TCP and Source Port: 80 was used to access Destination Port: 54074 at Timestamp: 2023-07-15 15:53:05
Protocol: TCP and Source Port: 80 was used to access Destination Port: 54078 at Timestamp: 2023-07-15 15:53:05
Protocol: TCP and Source Port: 54078 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:53:16
Protocol: TCP and Source Port: 54074 was used to access Destination Port: 80 at Timestamp: 2023-07-15 15:53:16
Protocol: TCP and Source Port: 80 was used to access Destination Port: 54078 at Timestamp: 2023-07-15 15:53:16
Protocol: TCP and Source Port: 80 was used to access Destination Port: 54074 at Timestamp: 2023-07-15 15:53:16
```

OnlineActivitiesGatheredbyIP.txt