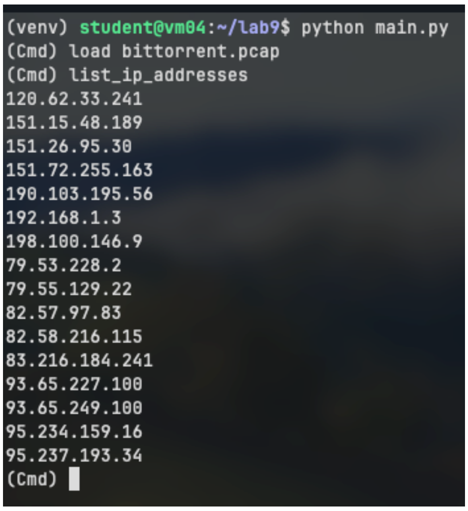
Lab 9

(Vous trouverez plus de justifications dans les commentaires du code, fichier main.py)

Question 1

Adresses IP pour les traces du fichier bittorrent. pcap :

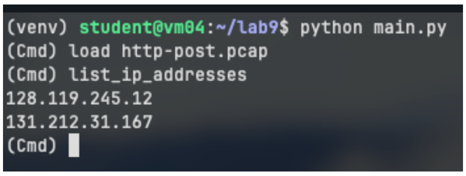
120.62.33.241
151.15.48.189
151.26.95.30
151.72.255.163
190.103.195.56
192.168.1.3
198.100.146.9
79.53.228.2
79.55.129.22
82.57.97.83
82.58.216.115
83.216.184.241
93.65.227.100
93.65.249.100
95.234.159.16
95.237.193.34



```
(venv) student@vm04:~/lab9$ python main.py
(Cmd) load bittorrent.pcap
(Cmd) list_ip_addresses
120.62.33.241
151.15.48.189
151.26.95.30
151.72.255.163
190.103.195.56
192.168.1.3
198.100.146.9
79.53.228.2
79.55.129.22
82.57.97.83
82.58.216.115
83.216.184.241
93.65.227.100
93.65.249.100
95.234.159.16
95.237.193.34
(Cmd) 
```

Adresses IP pour les traces du fichier bittorrent. pcap :

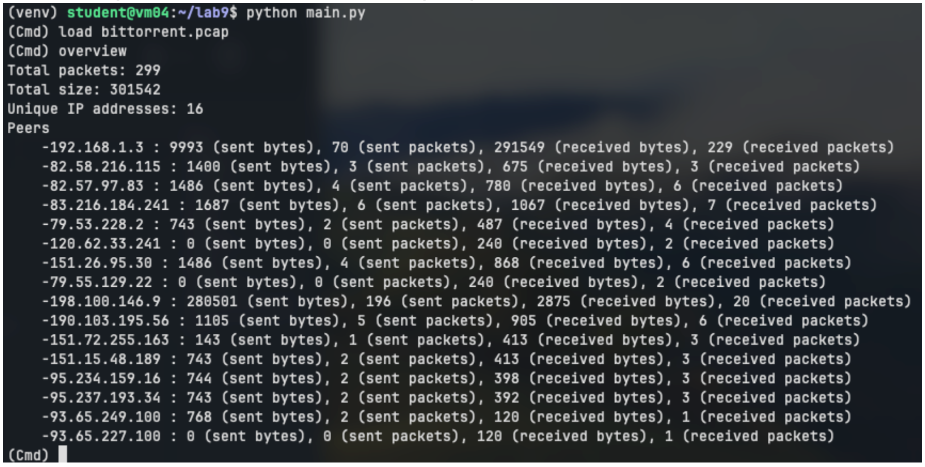
128.119.245.12
131.212.31.167



```
(venv) student@vm04:~/lab9$ python main.py
(Cmd) load http-post.pcap
(Cmd) list_ip_addresses
128.119.245.12
131.212.31.167
(Cmd) 
```

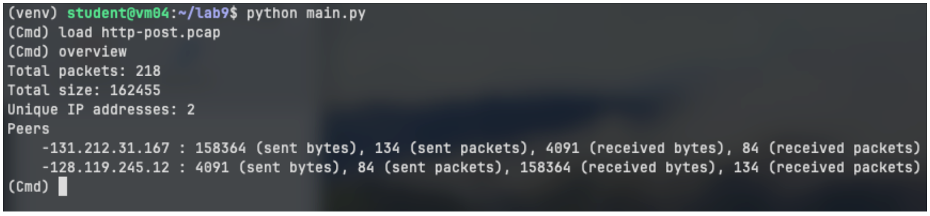
Question 2

Résultat pour le fichier bittorrent.pcap :



```
(venv) student@vm04:~/lab9$ python main.py
(Cmd) load bittorrent.pcap
(Cmd) overview
Total packets: 299
Total size: 301542
Unique IP addresses: 16
Peers
    -192.168.1.3 : 9993 (sent bytes), 70 (sent packets), 291549 (received bytes), 229 (received packets)
    -82.58.216.115 : 1400 (sent bytes), 3 (sent packets), 675 (received bytes), 3 (received packets)
    -82.57.97.83 : 1486 (sent bytes), 4 (sent packets), 780 (received bytes), 6 (received packets)
    -83.216.184.241 : 1687 (sent bytes), 6 (sent packets), 1067 (received bytes), 7 (received packets)
    -79.53.228.2 : 743 (sent bytes), 2 (sent packets), 487 (received bytes), 4 (received packets)
    -120.62.33.241 : 0 (sent bytes), 0 (sent packets), 240 (received bytes), 2 (received packets)
    -151.26.95.30 : 1486 (sent bytes), 4 (sent packets), 868 (received bytes), 6 (received packets)
    -79.55.129.22 : 0 (sent bytes), 0 (sent packets), 240 (received bytes), 2 (received packets)
    -198.100.146.9 : 280501 (sent bytes), 196 (sent packets), 2875 (received bytes), 20 (received packets)
    -190.103.195.56 : 1105 (sent bytes), 5 (sent packets), 905 (received bytes), 6 (received packets)
    -151.72.255.163 : 143 (sent bytes), 1 (sent packets), 413 (received bytes), 3 (received packets)
    -151.15.48.189 : 743 (sent bytes), 2 (sent packets), 413 (received bytes), 3 (received packets)
    -95.234.159.16 : 744 (sent bytes), 2 (sent packets), 398 (received bytes), 3 (received packets)
    -95.237.193.34 : 743 (sent bytes), 2 (sent packets), 392 (received bytes), 3 (received packets)
    -93.65.249.100 : 768 (sent bytes), 2 (sent packets), 120 (received bytes), 1 (received packets)
    -93.65.227.100 : 0 (sent bytes), 0 (sent packets), 120 (received bytes), 1 (received packets)
(Cmd) 
```

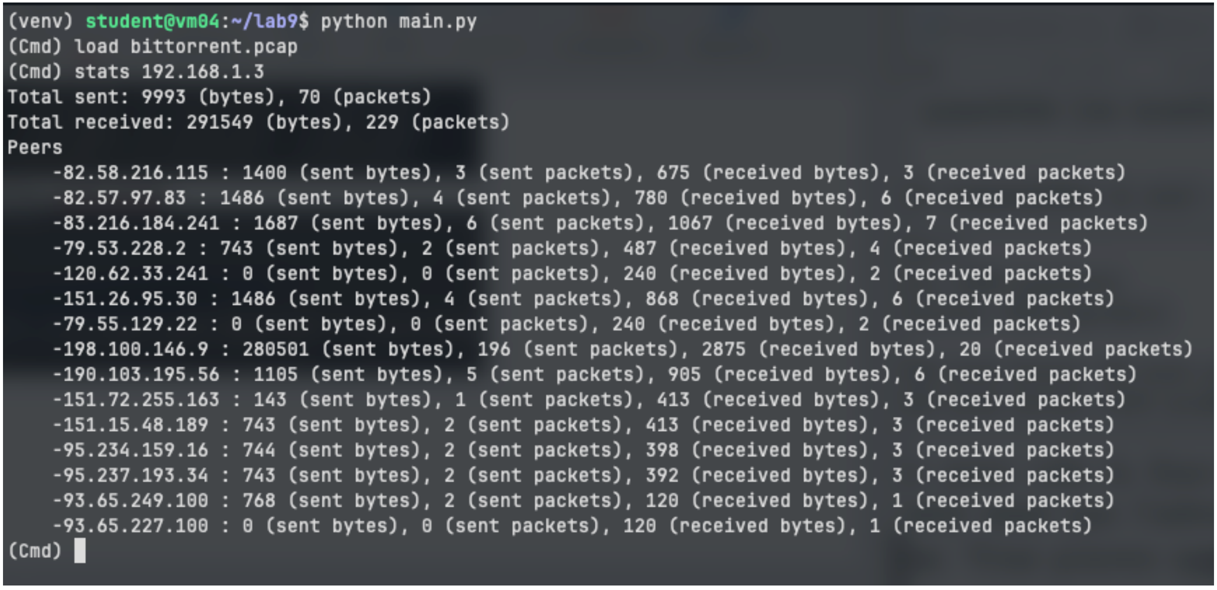
Résultat pour le fichier http-post.pcap :



```
(venv) student@vm04:~/lab9$ python main.py
(Cmd) load http-post.pcap
(Cmd) overview
Total packets: 218
Total size: 162455
Unique IP addresses: 2
Peers
    -131.212.31.167 : 158364 (sent bytes), 134 (sent packets), 4091 (received bytes), 84 (received packets)
    -128.119.245.12 : 4091 (sent bytes), 84 (sent packets), 158364 (received bytes), 134 (received packets)
(Cmd) 
```

Question 3

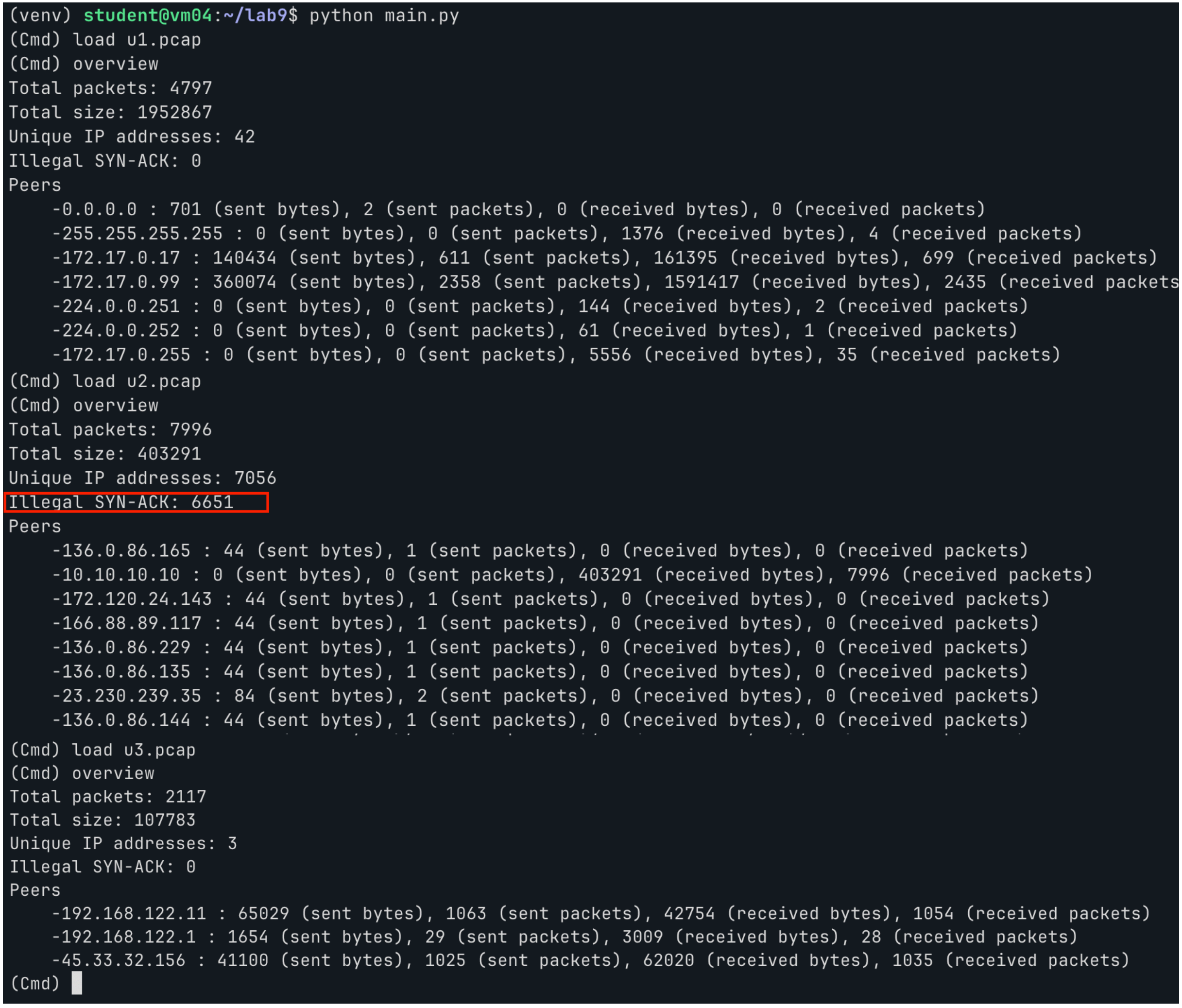
Résultat pour l’hôte 192.168.1.3 de la trace bittorrent.pcap :



```
(venv) student@vm04:~/lab9$ python main.py
(Cmd) load bittorrent.pcap
(Cmd) stats 192.168.1.3
Total sent: 9993 (bytes), 70 (packets)
Total received: 291549 (bytes), 229 (packets)
Peers
    -82.58.216.115 : 1400 (sent bytes), 3 (sent packets), 675 (received bytes), 3 (received packets)
    -82.57.97.83 : 1486 (sent bytes), 4 (sent packets), 780 (received bytes), 6 (received packets)
    -83.216.184.241 : 1687 (sent bytes), 6 (sent packets), 1067 (received bytes), 7 (received packets)
    -79.53.228.2 : 743 (sent bytes), 2 (sent packets), 487 (received bytes), 4 (received packets)
    -120.62.33.241 : 0 (sent bytes), 0 (sent packets), 240 (received bytes), 2 (received packets)
    -151.26.95.30 : 1486 (sent bytes), 4 (sent packets), 868 (received bytes), 6 (received packets)
    -79.55.129.22 : 0 (sent bytes), 0 (sent packets), 240 (received bytes), 2 (received packets)
    -198.100.146.9 : 280501 (sent bytes), 196 (sent packets), 2875 (received bytes), 20 (received packets)
    -190.103.195.56 : 1105 (sent bytes), 5 (sent packets), 905 (received bytes), 6 (received packets)
    -151.72.255.163 : 143 (sent bytes), 1 (sent packets), 413 (received bytes), 3 (received packets)
    -151.15.48.189 : 743 (sent bytes), 2 (sent packets), 413 (received bytes), 3 (received packets)
    -95.234.159.16 : 744 (sent bytes), 2 (sent packets), 398 (received bytes), 3 (received packets)
    -95.237.193.34 : 743 (sent bytes), 2 (sent packets), 392 (received bytes), 3 (received packets)
    -93.65.249.100 : 768 (sent bytes), 2 (sent packets), 120 (received bytes), 1 (received packets)
    -93.65.227.100 : 0 (sent bytes), 0 (sent packets), 120 (received bytes), 1 (received packets)
(Cmd) 
```

Question 4

On observe que le fichier u2.pcap est celui qui contient une attaque de ce style.



```
(venv) student@vm04:~/lab9$ python main.py
(Cmd) load u1.pcap
(Cmd) overview
Total packets: 4797
Total size: 1952867
Unique IP addresses: 42
Illegal SYN-ACK: 0
Peers
    -0.0.0.0 : 701 (sent bytes), 2 (sent packets), 0 (received bytes), 0 (received packets)
    -255.255.255.255 : 0 (sent bytes), 0 (sent packets), 1376 (received bytes), 4 (received packets)
    -172.17.0.17 : 140434 (sent bytes), 611 (sent packets), 161395 (received bytes), 699 (received packets)
    -172.17.0.99 : 360074 (sent bytes), 2358 (sent packets), 1591417 (received bytes), 2435 (received packets
    -224.0.0.251 : 0 (sent bytes), 0 (sent packets), 144 (received bytes), 2 (received packets)
    -224.0.0.252 : 0 (sent bytes), 0 (sent packets), 61 (received bytes), 1 (received packets)
    -172.17.0.255 : 0 (sent bytes), 0 (sent packets), 5556 (received bytes), 35 (received packets)
(Cmd) load u2.pcap
(Cmd) overview
Total packets: 7996
Total size: 403291
Unique IP addresses: 7056
Illegal SYN-ACK: 6651
Peers
    -136.0.86.165 : 44 (sent bytes), 1 (sent packets), 0 (received bytes), 0 (received packets)
    -10.10.10.10 : 0 (sent bytes), 0 (sent packets), 403291 (received bytes), 7996 (received packets)
    -172.120.24.143 : 44 (sent bytes), 1 (sent packets), 0 (received bytes), 0 (received packets)
    -166.88.89.117 : 44 (sent bytes), 1 (sent packets), 0 (received bytes), 0 (received packets)
    -136.0.86.229 : 44 (sent bytes), 1 (sent packets), 0 (received bytes), 0 (received packets)
    -136.0.86.135 : 44 (sent bytes), 1 (sent packets), 0 (received bytes), 0 (received packets)
    -23.230.239.35 : 84 (sent bytes), 2 (sent packets), 0 (received bytes), 0 (received packets)
    -136.0.86.144 : 44 (sent bytes), 1 (sent packets), 0 (received bytes), 0 (received packets)
(Cmd) load u3.pcap
(Cmd) overview
Total packets: 2117
Total size: 107783
Unique IP addresses: 3
Illegal SYN-ACK: 0
Peers
    -192.168.122.11 : 65029 (sent bytes), 1063 (sent packets), 42754 (received bytes), 1054 (received packets)
    -192.168.122.1 : 1654 (sent bytes), 29 (sent packets), 3009 (received bytes), 28 (received packets)
    -45.33.32.156 : 41100 (sent bytes), 1025 (sent packets), 62020 (received bytes), 1035 (received packets)
(Cmd)
```