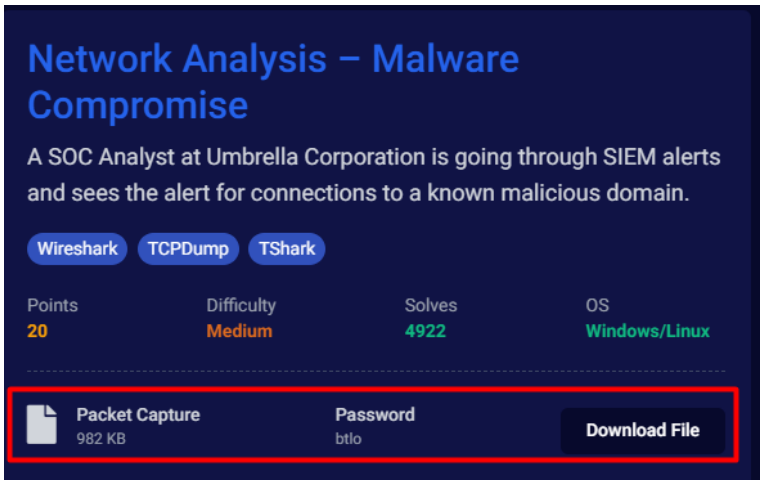
Reference: https://blueteamlabs.online/home/challenge/network-analysis-malware-compromise-e882f32908

Download the PCAP from the above link



In Linux with tcpdump

```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ sudo tcpdump -tt -r traffic-with-dridex-infection.pcap | cut -d " " -f 3
reading from file traffic-with-dridex-infection.pcap, link-type EN10MB (Ethernet), snapshot length 65535
10.11.27.101.65289
10.11.27.1.domain
10.11.27.101.49158
95.181.198.231.http
10.11.27.101.49158
10.11.27.101.49158
95.181.198.231.http
95.181.198.231.http
95.181.198.231.http
95.181.198.231.http
95.181.198.231.http
10.11.27.101.49158
95.181.198.231.http
```

```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Network analysis - Malware Compromise$ sudo tcpdump -tt -r traffic-with-dridex-infection.pcap | cut -d " " -f 3 | sort |
uniq -c |sort -nr
reading from file traffic-with-dridex-infection.pcap, link-type EN10MB (Ethernet), snapshot length 65535
    406 95.181.198.231.http
    333 83-166-247-211.cloudvps.regruhosting.ru.https
    302 176.32.33.108.http
     79 10.11.27.101.49161
     77 10.11.27.101.49181
     77 10.11.27.101.49159
     75 10.11.27.101.49158
     39 172.106.33.46.https
     38 185.158.251.55.https
     38 174.34.253.11.https
     37 185-244-150-230.hostsailor.com.https
     14 10.11.27.101.49192
     13 10.11.27.101.49221
     13 10.11.27.101.49218
     13 10.11.27.101.49217
     13 10.11.27.101.49214
     13 10.11.27.101.49209
     13 10.11.27.101.49208
```

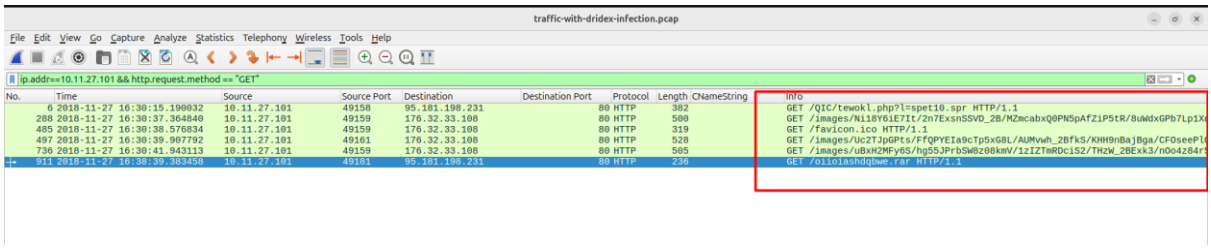
Wireshark Output

Ip addresses used in talking

Ethernet · 1 | IPv4 · 9 | IPv6 | TCP · 51 | UDP · 8

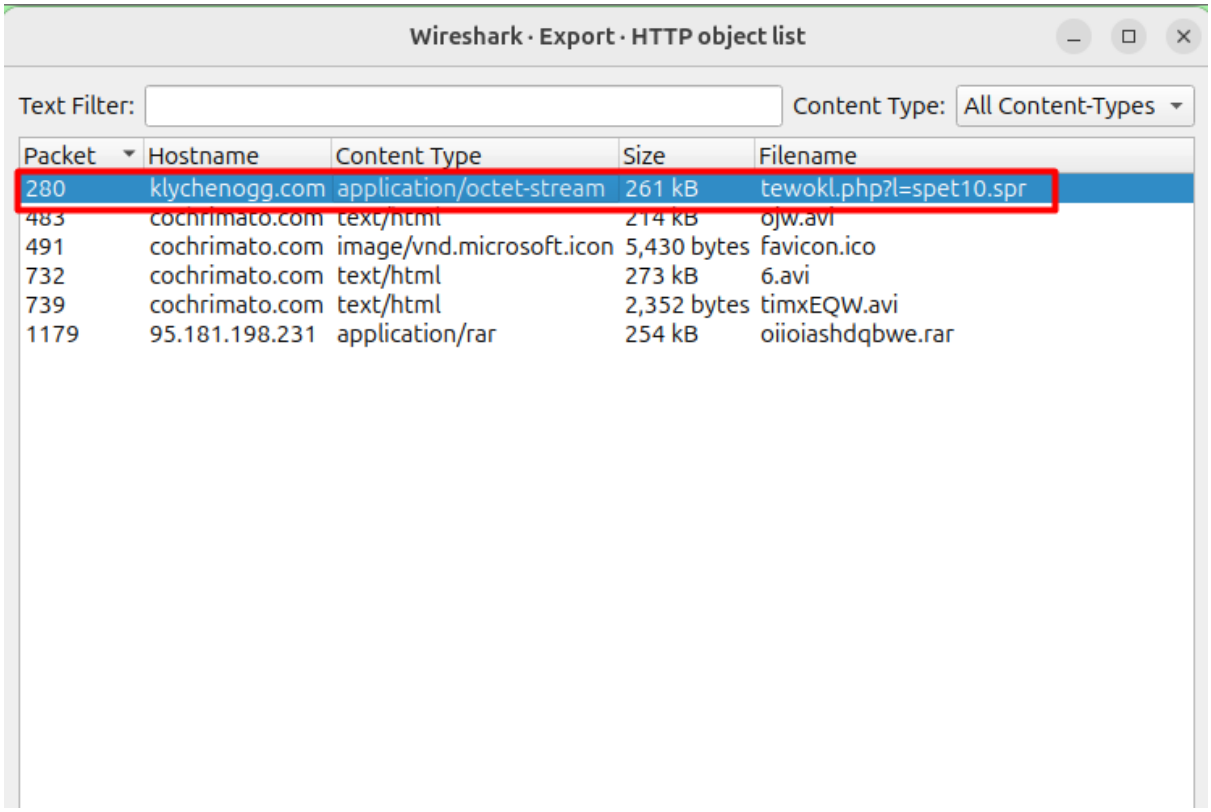
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.11.27.101	83.166.247.211	711	117 kB	378	53 kB	333	64 kB	99.256729	2424.2444
10.11.27.101	176.32.33.108	458	405 kB	156	10 kB	302	395 kB	24.283321	5.8906
10.11.27.101	95.181.198.231	558	546 kB	152	9 kB	406	538 kB	2.123144	537.1739
10.11.27.101	172.106.33.46	79	28 kB	40	21 kB	39	7 kB	698.722003	1457.7267
10.11.27.101	174.34.253.11	77	27 kB	39	20 kB	38	6 kB	990.749952	1447.6811
10.11.27.101	185.244.150.230	76	27 kB	39	21 kB	37	7 kB	524.881874	1466.4519
10.11.27.101	185.158.251.55	77	27 kB	39	21 kB	38	7 kB	838.328764	1464.5101
10.11.27.101	10.11.27.1	11	1 kB	5	377 bytes	6	1 kB	0.000000	2118.5054
10.11.27.101	208.67.222.222	6	575 bytes	3	239 bytes	3	336 bytes	96.715429	0.1224

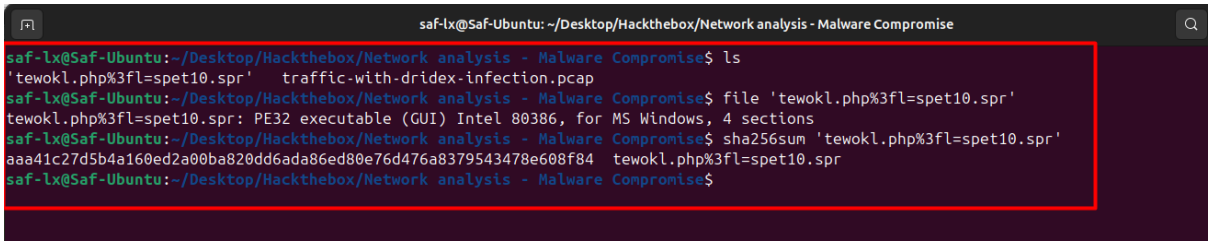
We can investigate in these IP addresses



Follow the http stream

Download the suspicious file and then check its reputation in virustotal





Sha 256 Hash -> **aaa41c27d5b4a160ed2a00ba820dd6ada86ed80e76d476a8379543478e608f84**