ATTACK DEFENSE

by PentesterAcademy

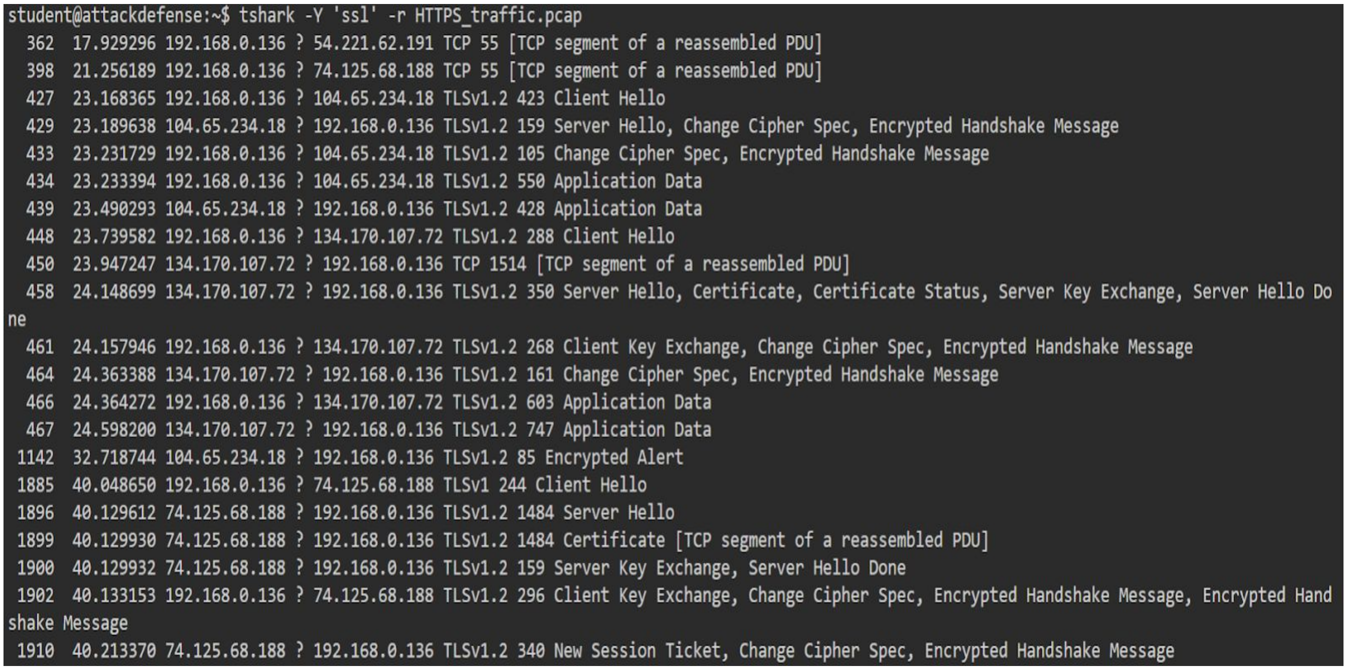
Name	Filtering Advanced: HTTPS
URL	https://www.attackdefense.com/challengedetails?cid=3
Type	Traffic Analysis: Tshark Fu

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Set A:

Q1. What command can be used to only show SSL traffic?

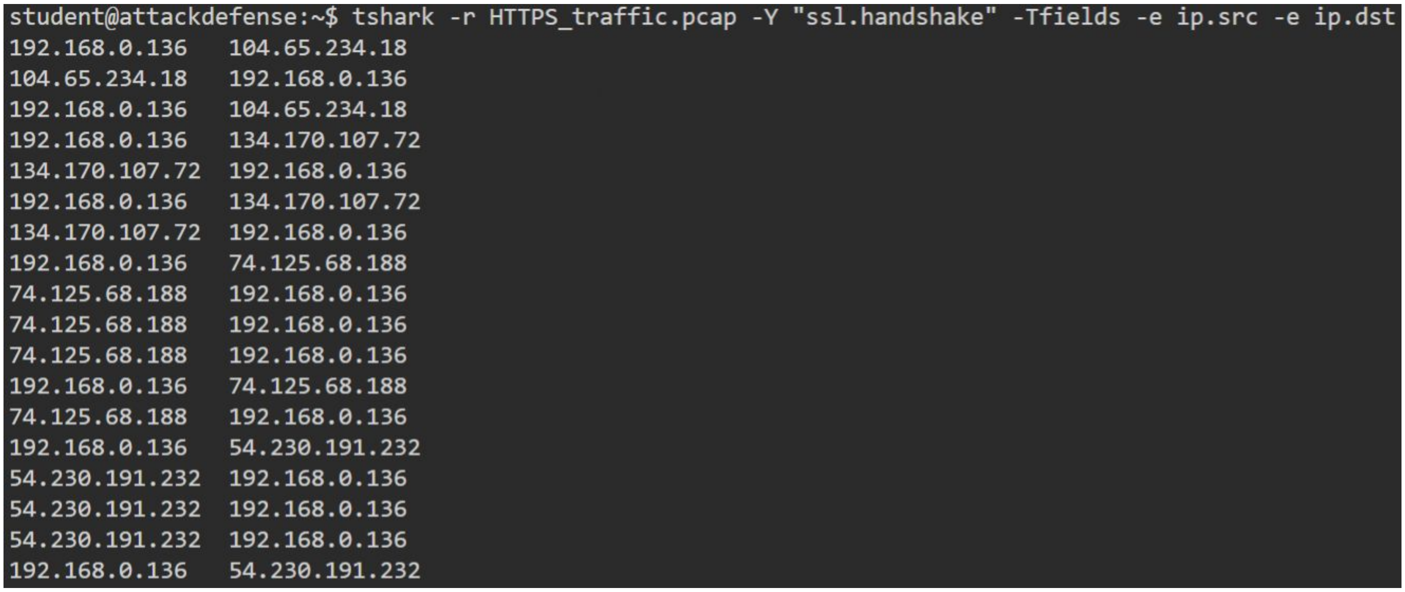
Answer: tshark -Y ‘ssl’ -r HTTPS_traffic.pcap



```
student@attackdefense:~$ tshark -Y 'ssl' -r HTTPS_traffic.pcap
  362  17.929296 192.168.0.136 ? 54.221.62.191 TCP 55 [TCP segment of a reassembled PDU]
  398  21.256189 192.168.0.136 ? 74.125.68.188 TCP 55 [TCP segment of a reassembled PDU]
  427  23.168365 192.168.0.136 ? 104.65.234.18 TLSv1.2 423 Client Hello
  429  23.189638 104.65.234.18 ? 192.168.0.136 TLSv1.2 159 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  433  23.231729 192.168.0.136 ? 104.65.234.18 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
  434  23.233394 192.168.0.136 ? 104.65.234.18 TLSv1.2 550 Application Data
  439  23.490293 104.65.234.18 ? 192.168.0.136 TLSv1.2 428 Application Data
  448  23.739582 192.168.0.136 ? 134.170.107.72 TLSv1.2 288 Client Hello
  450  23.947247 134.170.107.72 ? 192.168.0.136 TCP 1514 [TCP segment of a reassembled PDU]
  458  24.148699 134.170.107.72 ? 192.168.0.136 TLSv1.2 350 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Do
ne
  461  24.157946 192.168.0.136 ? 134.170.107.72 TLSv1.2 268 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  464  24.363388 134.170.107.72 ? 192.168.0.136 TLSv1.2 161 Change Cipher Spec, Encrypted Handshake Message
  466  24.364272 192.168.0.136 ? 134.170.107.72 TLSv1.2 603 Application Data
  467  24.598200 134.170.107.72 ? 192.168.0.136 TLSv1.2 747 Application Data
 1142  32.718744 104.65.234.18 ? 192.168.0.136 TLSv1.2 85 Encrypted Alert
 1885  40.048650 192.168.0.136 ? 74.125.68.188 TLSv1 244 Client Hello
 1896  40.129612 74.125.68.188 ? 192.168.0.136 TLSv1.2 1484 Server Hello
 1899  40.129930 74.125.68.188 ? 192.168.0.136 TLSv1.2 1484 Certificate [TCP segment of a reassembled PDU]
 1900  40.129932 74.125.68.188 ? 192.168.0.136 TLSv1.2 159 Server Key Exchange, Server Hello Done
 1902  40.133153 192.168.0.136 ? 74.125.68.188 TLSv1.2 296 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, Encrypted Hand
shake Message
 1910  40.213370 74.125.68.188 ? 192.168.0.136 TLSv1.2 340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
```

Q2. What command can be used to only print the source IP and destination IP for all SSL handshake packets?

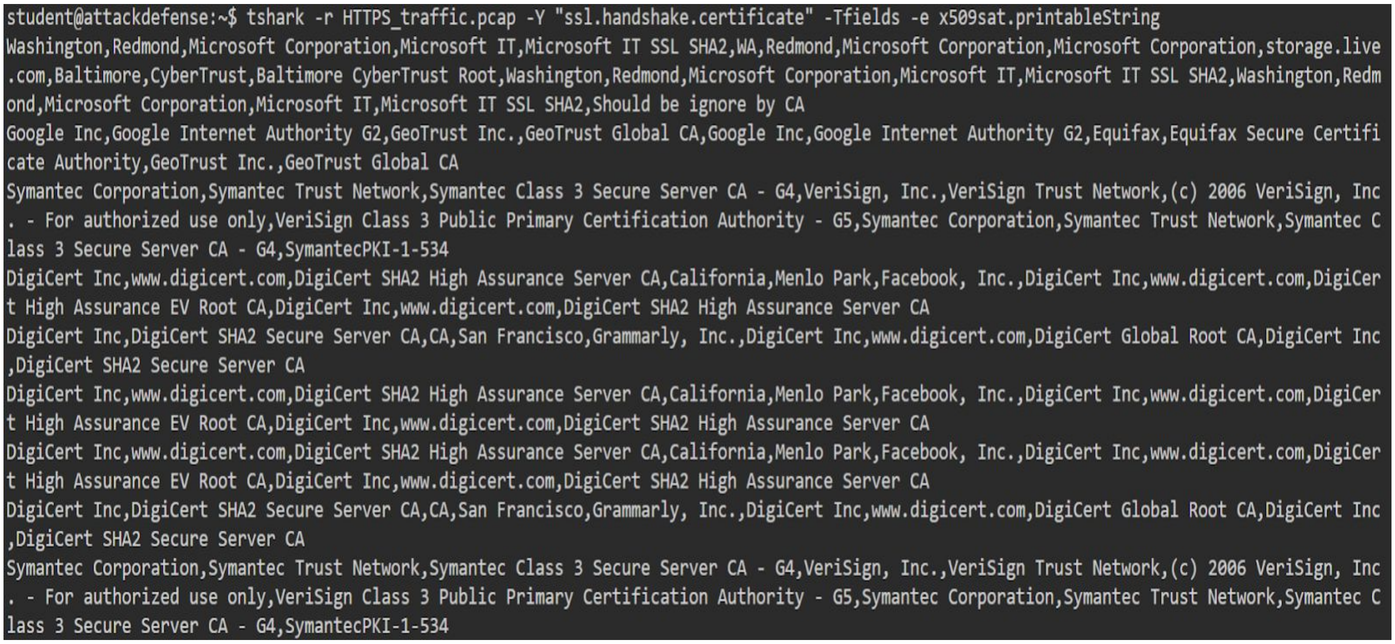
Answer: tshark -r HTTPS_traffic.pcap -Y "ssl.handshake" -Tfields -e ip.src -e ip.dst



```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "ssl.handshake" -Tfields -e ip.src -e ip.dst
192.168.0.136   104.65.234.18
104.65.234.18   192.168.0.136
192.168.0.136   104.65.234.18
192.168.0.136   134.170.107.72
134.170.107.72  192.168.0.136
192.168.0.136   134.170.107.72
134.170.107.72  192.168.0.136
192.168.0.136   74.125.68.188
74.125.68.188   192.168.0.136
74.125.68.188   192.168.0.136
74.125.68.188   192.168.0.136
192.168.0.136   74.125.68.188
74.125.68.188   192.168.0.136
192.168.0.136   54.230.191.232
54.230.191.232  192.168.0.136
54.230.191.232  192.168.0.136
54.230.191.232  192.168.0.136
192.168.0.136   54.230.191.232
```

Q3. What command can be used to list issuer name for all SSL certificates exchanged?

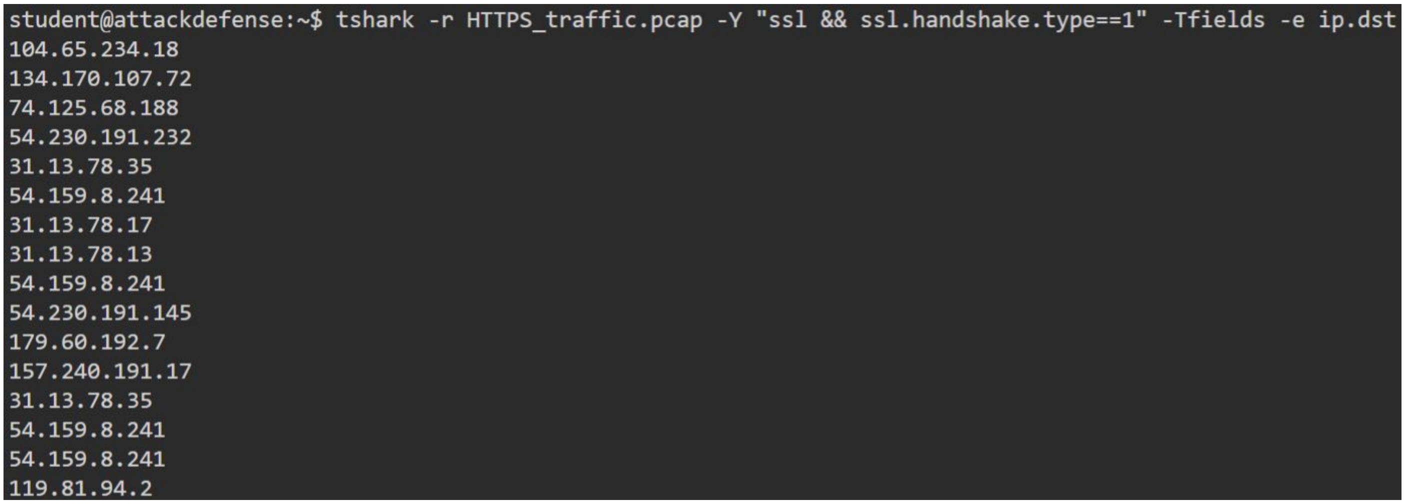
Answer: tshark -r HTTPS_traffic.pcap -Y "ssl.handshake.certificate" -Tfields -e x509sat.printableString



```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "ssl.handshake.certificate" -Tfields -e x509sat.printableString
Washington,Redmond,Microsoft Corporation,Microsoft IT,Microsoft IT SSL SHA2,WA,Redmond,Microsoft Corporation,Microsoft Corporation,storage.live
.com,Baltimore,CyberTrust,Baltimore CyberTrust Root,Washington,Redmond,Microsoft Corporation,Microsoft IT,Microsoft IT SSL SHA2,Washington,Redm
ond,Microsoft Corporation,Microsoft IT,Microsoft IT SSL SHA2,Should be ignore by CA
Google Inc,Google Internet Authority G2,GeoTrust Inc.,GeoTrust Global CA,Google Inc,Google Internet Authority G2,Equifax,Equifax Secure Certifi
cate Authority,GeoTrust Inc.,GeoTrust Global CA
Symantec Corporation,Symantec Trust Network,Symantec Class 3 Secure Server CA - G4,VeriSign, Inc.,VeriSign Trust Network,(c) 2006 VeriSign, Inc
. - For authorized use only,VeriSign Class 3 Public Primary Certification Authority - G5,Symantec Corporation,Symantec Trust Network,Symantec C
lass 3 Secure Server CA - G4,SymantecPKI-1-534
DigiCert Inc,www.digicert.com,DigiCert SHA2 High Assurance Server CA,California,Menlo Park,Facebook, Inc.,DigiCert Inc,www.digicert.com,DigiCer
t High Assurance EV Root CA,DigiCert Inc,www.digicert.com,DigiCert SHA2 High Assurance Server CA
DigiCert Inc,DigiCert SHA2 Secure Server CA,CA,San Francisco,Grammarly, Inc.,DigiCert Inc,www.digicert.com,DigiCert Global Root CA,DigiCert Inc
,DigiCert SHA2 Secure Server CA
DigiCert Inc,www.digicert.com,DigiCert SHA2 High Assurance Server CA,California,Menlo Park,Facebook, Inc.,DigiCert Inc,www.digicert.com,DigiCer
t High Assurance EV Root CA,DigiCert Inc,www.digicert.com,DigiCert SHA2 High Assurance Server CA
DigiCert Inc,www.digicert.com,DigiCert SHA2 High Assurance Server CA,California,Menlo Park,Facebook, Inc.,DigiCert Inc,www.digicert.com,DigiCer
t High Assurance EV Root CA,DigiCert Inc,www.digicert.com,DigiCert SHA2 High Assurance Server CA
DigiCert Inc,DigiCert SHA2 Secure Server CA,CA,San Francisco,Grammarly, Inc.,DigiCert Inc,www.digicert.com,DigiCert Global Root CA,DigiCert Inc
,DigiCert SHA2 Secure Server CA
Symantec Corporation,Symantec Trust Network,Symantec Class 3 Secure Server CA - G4,VeriSign, Inc.,VeriSign Trust Network,(c) 2006 VeriSign, Inc
. - For authorized use only,VeriSign Class 3 Public Primary Certification Authority - G5,Symantec Corporation,Symantec Trust Network,Symantec C
lass 3 Secure Server CA - G4,SymantecPKI-1-534
```

Q4. What command can be used to print the IP addresses of all servers accessed over SSL?

Answer: tshark -r HTTPS_traffic.pcap -Y "ssl && ssl.handshake.type==1" -Tfields -e ip.dst



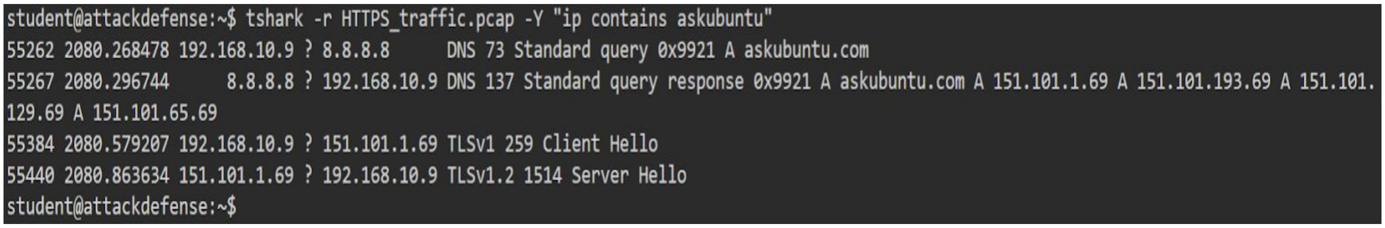
```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "ssl && ssl.handshake.type==1" -Tfields -e ip.dst
104.65.234.18
134.170.107.72
74.125.68.188
54.230.191.232
31.13.78.35
54.159.8.241
31.13.78.17
31.13.78.13
54.159.8.241
54.230.191.145
179.60.192.7
157.240.191.17
31.13.78.35
54.159.8.241
54.159.8.241
119.81.94.2
```

Set B:

Q1. What are the IP addresses associated with Ask Ubuntu servers (askubuntu.com)?

Answer: 151.101.1.69 , 151.101.193.69, 151.101.129.69, 151.101.65.69

Command: tshark -r HTTPS_traffic.pcap -Y "ip contains askubuntu"

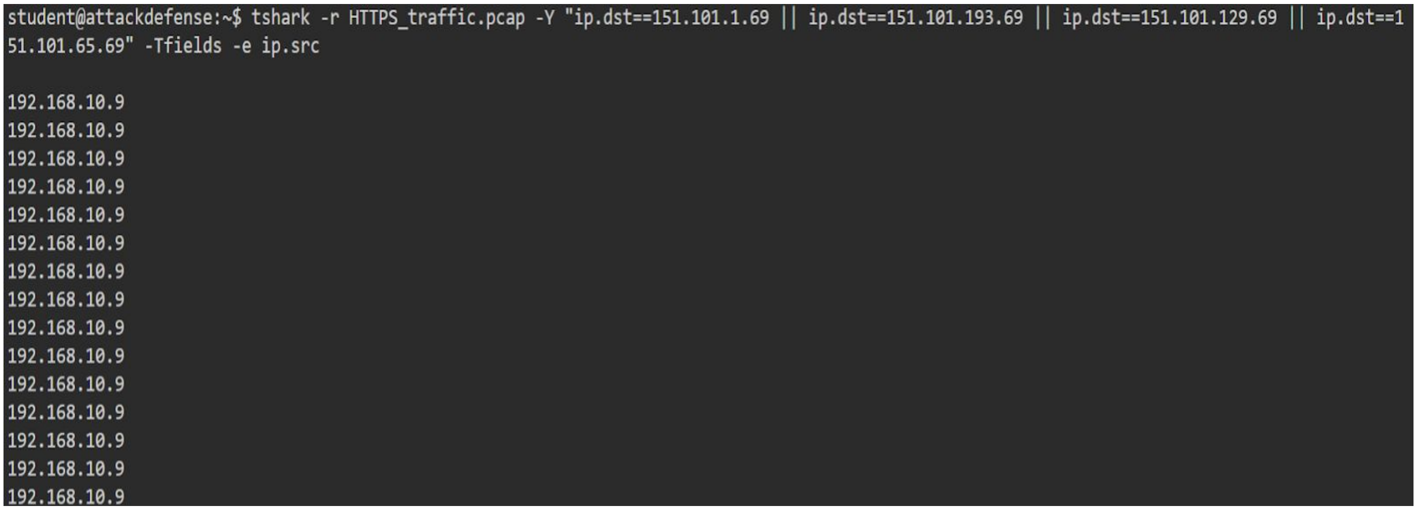


```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "ip contains askubuntu"
55262 2080.268478 192.168.10.9 ? 8.8.8.8      DNS 73 Standard query 0x9921 A askubuntu.com
55267 2080.296744      8.8.8.8 ? 192.168.10.9 DNS 137 Standard query response 0x9921 A askubuntu.com A 151.101.1.69 A 151.101.193.69 A 151.101.
129.69 A 151.101.65.69
55384 2080.579207 192.168.10.9 ? 151.101.1.69 TLSv1 259 Client Hello
55440 2080.863634 151.101.1.69 ? 192.168.10.9 TLSv1.2 1514 Server Hello
student@attackdefense:~$
```

Q2. What is the IP address of the user who interacted with with Ask Ubuntu servers (askubuntu.com)?

Answer: 192.168.10.9

Command: tshark -r HTTPS_traffic.pcap -Y "ip.dst==151.101.1.69 || ip.dst==151.101.193.69 || ip.dst==151.101.129.69 || ip.dst==151.101.65.69" -Tfields -e ip.src



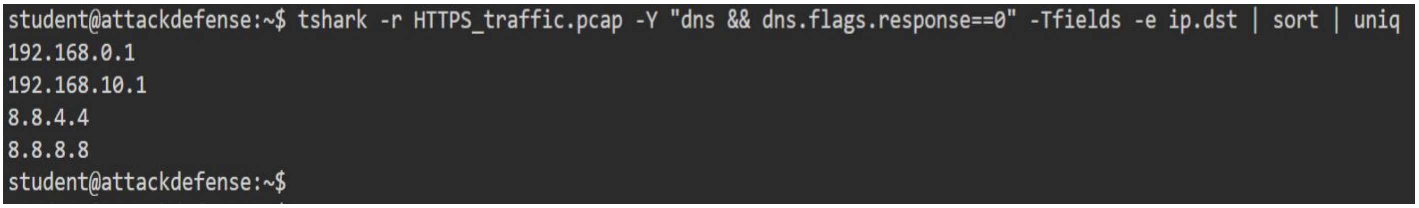
```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "ip.dst==151.101.1.69 || ip.dst==151.101.193.69 || ip.dst==151.101.129.69 || ip.dst==1
51.101.65.69" -Tfields -e ip.src

192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
192.168.10.9
```

Q3. What DNS servers were used by the clients for domain name resolutions?

Answer: 192.168.0.1, 8.8.8.8, 8.8.4.4, 192.168.10.1

Command: tshark -r HTTPS_traffic.pcap -Y "dns && dns.flags.response==0" -Tfields -e ip.dst

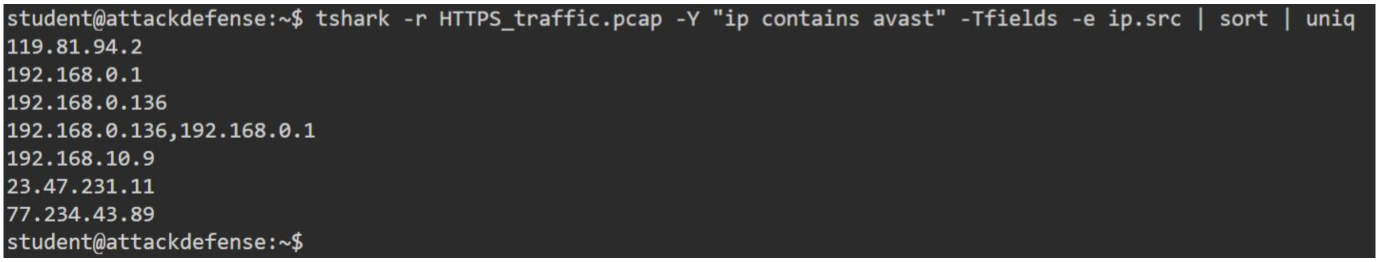


```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "dns && dns.flags.response==0" -Tfields -e ip.dst | sort | uniq
192.168.0.1
192.168.10.1
8.8.4.4
8.8.8.8
student@attackdefense:~$
```

Q4. Some machines have a popular antivirus software running on them. What is the name of the antivirus solution? What are the IP addresses of the machines running this solution?

Answer: Avast antivirus, 192.168.10.9, 192.168.0.1, 192.168.0.136

Command: tshark -r HTTPS_traffic.pcap -Y "ip contains avast" -Tfields -e ip.src



```
student@attackdefense:~$ tshark -r HTTPS_traffic.pcap -Y "ip contains avast" -Tfields -e ip.src | sort | uniq
119.81.94.2
192.168.0.1
192.168.0.136
192.168.0.136,192.168.0.1
192.168.10.9
23.47.231.11
77.234.43.89
student@attackdefense:~$
```

References:

1. Tshark (https://www.wireshark.org/docs/man-pages/tshark.html)
2. Wireshark (https://www.wireshark.org/)