
ATTACK
DEFENSE
by PentesterAcademy

Name	Filtering Basics: HTTP
URL	https://www.attackdefense.com/challengedetails?cid=2
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. Command to show only the HTTP traffic from a PCAP file?

Answer: tshark -Y 'http' -r HTTP_traffic.pcap

```
student@attackdefense:~$ tshark -Y 'http' -r HTTP_traffic.pcap
   30   4.166998 192.168.252.128 ? 54.239.32.8  HTTP 904 GET / HTTP/1.1
   38   4.168852 192.168.252.128 ? 54.239.39.114 HTTP 1150 POST /1/batch/1/OE/ HTTP/1.1  (text/plain)
   46   4.472330 54.239.39.114 ? 192.168.252.128 HTTP 431 HTTP/1.1 204 No Content
  146   5.060440 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/412maSA0fuL._AC_SY200_.jpg HTTP/1.1
  150   5.062201 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41wuVnAeedL._AC_SY200_.jpg HTTP/1.1
  158   5.068393 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/412OwlOMxPL._AC_SY200_.jpg HTTP/1.1
  159   5.068453 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/316zh6kkqML._AC_SY200_.jpg HTTP/1.1
  162   5.068562 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41O1oRMP6pL._AC_SY200_.jpg HTTP/1.1
  166   5.069236 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41w3V6ilQPL._AC_SY200_.jpg HTTP/1.1
  189   5.244323 52.84.108.225 ? 192.168.252.128 HTTP 6840 HTTP/1.1 200 OK  (JPEG JFIF image)
  191   5.244536 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41wEkEluHYL._AC_SY200_.jpg HTTP/1.1
  197   5.260023 52.84.108.225 ? 192.168.252.128 HTTP 4061 HTTP/1.1 200 OK  (JPEG JFIF image)
  199   5.260230 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/21RJXZUGwJL._AC_SY200_.jpg HTTP/1.1
  205   5.268244 52.84.108.225 ? 192.168.252.128 HTTP 2615 HTTP/1.1 200 OK  (JPEG JFIF image)
  209   5.268489 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51FKbs7rlkL._AC_SY200_.jpg HTTP/1.1
  213   5.297355 52.84.108.225 ? 192.168.252.128 HTTP 1681 HTTP/1.1 200 OK  (JPEG JFIF image)
  215   5.297530 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51WCISldn8L._AC_SY200_.jpg HTTP/1.1
  223   5.310960 52.84.108.225 ? 192.168.252.128 HTTP 3411 HTTP/1.1 200 OK  (JPEG JFIF image)
```

Q2. Command to show only the IP packets sent from IP address 192.168.252.128 to IP address 52.32.74.91?

Answer: tshark -r HTTP_traffic.pcap -Y "ip.src==192.168.252.128 && ip.dst==52.32.74.91"

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "ip.src==192.168.252.128 && ip.dst==52.32.74.91"
24168 144.928157 192.168.252.128 ? 52.32.74.91  TCP 74 48544 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=837027 TSecr=0 WS=1024
24214 145.179880 192.168.252.128 ? 52.32.74.91  TCP 74 48546 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=837089 TSecr=0 WS=1024
24233 145.236767 192.168.252.128 ? 52.32.74.91  TCP 54 48544 ? 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
24241 145.475893 192.168.252.128 ? 52.32.74.91  TCP 54 48546 ? 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
24276 145.878151 192.168.252.128 ? 52.32.74.91  HTTP 493 GET /420046.gif?partner_uid=o9JecfYE-vSFC1OCbXDJnra2LQPPRlM1ETKuEF9Onaz1rdbviK35w2TZ9S
GQ7pfg HTTP/1.1
24312 146.203489 192.168.252.128 ? 52.32.74.91  TCP 54 48544 ? 80 [ACK] Seq=440 Ack=500 Win=30016 Len=0
24645 147.877429 192.168.252.128 ? 52.32.74.91  HTTP 521 GET /420046.gif?partner_uid=o9JecfYE-vSFC1OCbXDJnra2LQPPRlM1ETKuEF9Onaz1rdbviK35w2TZ9S
GQ7pfg&redirect=1 HTTP/1.1
24772 148.196810 192.168.252.128 ? 52.32.74.91  TCP 54 48546 ? 80 [ACK] Seq=468 Ack=1119 Win=31304 Len=0
26345 156.200222 192.168.252.128 ? 52.32.74.91  TCP 54 [TCP Keep-Alive] 48544 ? 80 [ACK] Seq=439 Ack=500 Win=30016 Len=0
26835 158.196558 192.168.252.128 ? 52.32.74.91  TCP 54 [TCP Keep-Alive] 48546 ? 80 [ACK] Seq=467 Ack=1119 Win=31304 Len=0
29102 166.228525 192.168.252.128 ? 52.32.74.91  TCP 54 [TCP Keep-Alive] 48544 ? 80 [ACK] Seq=439 Ack=500 Win=30016 Len=0
29225 168.211953 192.168.252.128 ? 52.32.74.91  TCP 54 [TCP Keep-Alive] 48546 ? 80 [ACK] Seq=467 Ack=1119 Win=31304 Len=0
29853 173.206316 192.168.252.128 ? 52.32.74.91  TCP 54 48544 ? 80 [FIN, ACK] Seq=440 Ack=500 Win=30016 Len=0
29954 173.228854 192.168.252.128 ? 52.32.74.91  TCP 54 48546 ? 80 [FIN, ACK] Seq=468 Ack=1119 Win=31304 Len=0
30364 173.610539 192.168.252.128 ? 52.32.74.91  TCP 54 48546 ? 80 [ACK] Seq=469 Ack=1120 Win=31304 Len=0
30412 174.324657 192.168.252.128 ? 52.32.74.91  TCP 54 48544 ? 80 [ACK] Seq=441 Ack=501 Win=30016 Len=0
student@attackdefense:~$
```

Q3. Command to print only packets containing GET requests?

Answer: tshark -r HTTP_traffic.pcap -Y "http.request.method==GET"

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "http.request.method==GET"
   30   4.166998 192.168.252.128 ? 54.239.32.8  HTTP 904 GET / HTTP/1.1
  146   5.060440 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/412maSA0fuL._AC_SY200_.jpg HTTP/1.1
  150   5.062201 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41wuVnAeedL._AC_SY200_.jpg HTTP/1.1
  158   5.068393 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/412OwlOMxPL._AC_SY200_.jpg HTTP/1.1
  159   5.068453 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/316zh6kkqML._AC_SY200_.jpg HTTP/1.1
  162   5.068562 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41O1oRMP6pL._AC_SY200_.jpg HTTP/1.1
  166   5.069236 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41w3V6ilQPL._AC_SY200_.jpg HTTP/1.1
  191   5.244536 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41wEkEluHYL._AC_SY200_.jpg HTTP/1.1
  199   5.260230 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/21RJXZUGwJL._AC_SY200_.jpg HTTP/1.1
  209   5.268489 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51FKbs7rlkL._AC_SY200_.jpg HTTP/1.1
  215   5.297530 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51WCISldn8L._AC_SY200_.jpg HTTP/1.1
  227   5.311214 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41VsfYu1RuL._AC_SY200_.jpg HTTP/1.1
  228   5.311295 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/31PoS1o0AbL._AC_SY200_.jpg HTTP/1.1
  236   5.359014 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/414KNwJQbEL._AC_SY200_.jpg HTTP/1.1
  245   5.400521 192.168.252.128 ? 52.84.108.225 HTTP 401 GET /images/I/41eCI%2Bcj1nL._AC_SY200_.jpg HTTP/1.1
  252   5.409441 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51MB9P6MbXL._AC_SY200_.jpg HTTP/1.1
  253   5.409514 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51g0tuo4xtL._AC_SY200_.jpg HTTP/1.1
  260   5.424920 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/31sPuqi12kL._AC_SY200_.jpg HTTP/1.1
  264   5.431390 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/41vStgpPnBL._AC_SY200_.jpg HTTP/1.1
  269   5.442286 192.168.252.128 ? 52.84.108.225 HTTP 399 GET /images/I/51AtpeiusWL._AC_SY200_.jpg HTTP/1.1
  276   5.506322 192.168.252.128 ? 52.84.108.225 HTTP 401 GET /images/I/41%2BthUtP6nL._AC_SY200_.jpg HTTP/1.1
```

Q4. Command to print only packets only source IP and URL for all GET request packets?

Answer: tshark -r HTTP_traffic.pcap -Y "http.request.method==GET" -Tfields -e frame.time -e ip.src -e http.request.full_uri

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "http.request.method==GET" -Tfields -e frame.time -e ip.src -e http.request.full_uri
Jun 20, 2016 07:38:28.678418000 UTC     192.168.252.128 http://www.amazon.in/
Jun 20, 2016 07:38:29.571860000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/412maSA0fuL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.573621000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/41wuVnAeedL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.579813000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/412OwlOMxPL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.579873000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/316zh6kkqML._AC_SY200_.jpg
Jun 20, 2016 07:38:29.579982000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/41O1oRMP6pL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.580656000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/41w3V6ilQPL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.755956000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/41wEkEluHYL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.771650000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/21RJXZUGwJL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.779909000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/51FKbs7rlkL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.808950000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/51WCISldn8L._AC_SY200_.jpg
Jun 20, 2016 07:38:29.822634000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/41VsfYu1RuL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.822715000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/31PoS1o0AbL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.870434000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/414KNwJQbEL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.911941000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/41eCI%2Bcj1nL._AC_SY200_.jpg
Jun 20, 2016 07:38:29.920861000 UTC     192.168.252.128 http://ecx.images-amazon.com/images/I/51MB9P6MbXL._AC_SY200_.jpg
```

Set B:

Q1. How many HTTP packets contain the "password" string?

Answer: 4

Command: tshark -r HTTP_traffic.pcap -Y "http contains password”

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "http contains password"
12866  99.041118 52.84.108.101 ? 192.168.252.128 HTTP 1573 HTTP/1.1 200 OK  (text/javascript)
13089  99.686253 52.84.108.101 ? 192.168.252.128 HTTP 7905 HTTP/1.1 200 OK  (text/css)
13173 100.072333 52.84.108.101 ? 192.168.252.128 HTTP 12836 HTTP/1.1 200 OK  (text/javascript)
13185 100.077752 52.84.108.101 ? 192.168.252.128 HTTP 5527 HTTP/1.1 200 OK  (text/javascript)
student@attackdefense:~$
```

Q2. What is the destination IP address for GET requests sent for New York Times (www.nytimes.com)?

Answer: 170.149.159.130

Command: tshark -r HTTP_traffic.pcap -Y "http.request.method==GET && http.host==www.nytimes.com" -Tfields -e ip.dst

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "http.request.method==GET && http.host==www.nytimes.com" -Tfields -e ip.dst
170.149.159.130
170.149.159.130
170.149.159.130
170.149.159.130
170.149.159.130
student@attackdefense:~$
```

Q3. What is the session ID being used by 192.168.252.128 for Amazon India store (amazon.in)?

Answer: 278-7381968-4337153

Command: tshark -r HTTP_traffic.pcap -Y "ip contains amazon.in && ip.src==192.168.252.128" -Tfields -e ip.src -e http.cookie

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "ip contains amazon.in && ip.src==192.168.252.128" -Tfields -e ip.src -e http.cookie
192.168.252.128 x-wl-uid=1YUrrvyo2aOwaC2tX1u3CL5JwhNCwEZhfsOUf8932b9zxC9BkYOYTKpVuh02IxmGM3Gs2/XgdUCA=; session-id-time=2082758401l; session-id
=278-7381968-4337153; csm-hit=0JAE5VRXPMH77731K1TX+s-0JAE5VRXPMH77731K1TX|1466408308416; visitCount=2; ubid-acbin=280-4213374-9863463; lc-acbin
=en_IN; session-token=4pTTa7bIe2i6bm7hJhGt4Jp7Mr2r5jgqscUc9YZTkXxjaaP+H+ezTpZLgyH8KjFSbiwETGfn0kOVzX5WUyryAQphMTcttvLjvBRVEBmw0UkKdZhVIoiDIT1Ed
QPUzTnfJDAQCKzdVpEGdKxlOlU+rQw+L2ZCE5eMBIZ2ip7xXq3PMsOCq+k2RSZ+4wh50U4EawgJPj7CaidkmVdFLbn0WrJKQw1f9hnd82LtRSDccz8FXsH8ksdKEQ==
192.168.252.128 x-wl-uid=1YUrrvyo2aOwaC2tX1u3CL5JwhNCwEZhfsOUf8932b9zxC9BkYOYTKpVuh02IxmGM3Gs2/XgdUCA=; session-id-time=2082758401l; session-id
=278-7381968-4337153; visitCount=2; ubid-acbin=280-4213374-9863463; lc-acbin=en_IN; session-token=4pTTa7bIe2i6bm7hJhGt4Jp7Mr2r5jgqscUc9YZTkXxja
aP+H+ezTpZLgyH8KjFSbiwETGfn0kOVzX5WUyryAQphMTcttvLjvBRVEBmw0UkKdZhVIoiDIT1EdQPUzTnfJDAQCKzdVpEGdKxlOlU+rQw+L2ZCE5eMBIZ2ip7xXq3PMsOCq+k2RSZ+4wh5
0U4EawgJPj7CaidkmVdFLbn0WrJKQw1f9hnd82LtRSDccz8FXsH8ksdKEQ==
192.168.252.128
192.168.252.128
192.168.252.128
192.168.252.128
192.168.252.128
192.168.252.128
192.168.252.128
```

Q4. What type of OS the machine on IP address 192.168.252.128 is using (i.e. Windows/Linux/MacOS/Solaris/Unix/BSD)?
Bonus: Can you also guess the distribution/flavor?

Answer: Linux (Bonus: Kali)

Command: tshark -r HTTP_traffic.pcap -Y "ip.src==192.168.252.128 && http" -Tfields -e http.user_agent

```
student@attackdefense:~$ tshark -r HTTP_traffic.pcap -Y "ip.src==192.168.252.128 && http" -Tfields -e http.user_agent
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
```

References:

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