


[illegible]



Name	Getting Started: Tshark
URL	https://www.attackdefense.com/challengedetails?cid=1
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. Which version of Tshark is installed in the lab?

Answer: tshark -v

```
student@attackdefense:~$ tshark -v
TShark (Wireshark) 2.6.1 (Git v2.6.1 packaged as 2.6.1-0ubuntu2~16.04.0)

Copyright 1998-2018 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <http://www.gnu.org/licenses/old-licenses/gpl-2.0.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with libpcap, with POSIX capabilities (Linux), with libnl 3,
with GLib 2.48.2, with zlib 1.2.8, with SMI 0.4.8, with c-ares 1.10.0, with Lua
5.2.4, with GnuTLS 3.4.10, with Gcrypt 1.6.5, with MIT Kerberos, with MaxMind DB
resolver, with nghttp2 1.7.1, with LZ4, with Snappy, with libxml2 2.9.3.

Running on Linux 4.15.0-38-generic, with Intel(R) Xeon(R) Gold 6148 CPU @
2.40GHz (with SSE4.2), with 96677 MB of physical memory, with locale C, with
libpcap version 1.7.4, with GnuTLS 3.4.10, with Gcrypt 1.6.5, with zlib 1.2.8,
binary plugins supported (13 loaded).
```

Q2. Find all Tshark supported network interfaces for monitoring

Answer: tshark -D

```
student@attackdefense:~$ tshark -D
1. eth0
2. any
3. lo (Loopback)
4. nflog
5. nfqueue
6. ciscodump (Cisco remote capture)
7. randpkt (Random packet generator)
8. sshdump (SSH remote capture)
9. udpdump (UDP Listener remote capture)
student@attackdefense:~$
```

Q3. What is the Tshark command to sniff on eth0? Why did this command fail?

Answer: tshark -i eth0

```
student@attackdefense:~$ tshark -i eth0
Capturing on 'eth0'
tshark: The capture session could not be initiated on interface 'eth0' (You don't have permission to capture on that device).
Please check to make sure you have sufficient permissions, and that you have the proper interface or pipe specified.
0 packets captured
student@attackdefense:~$
```

Set B:

Q1. Tshark supports PCAP files. The lab environment has a sample file: HTTP_traffic.pcap. How can you read this file in Tshark and display the packet list on the console?

Answer: tshark -r HTTP_traffic.pcap

```

student@attackdefense:~$ tshark -r HTTP_traffic.pcap
 1  0.000000 192.168.252.128 ? 192.168.252.2 DNS 83 Standard query 0x55cd A g-ecx.images-amazon.com
 2  0.000096 192.168.252.128 ? 192.168.252.2 DNS 83 Standard query 0x989e AAAA g-ecx.images-amazon.com
 3  0.001097 192.168.252.128 ? 192.168.252.2 DNS 83 Standard query 0xffff A g-ecx.images-amazon.com
 4  0.035787 192.168.252.2 ? 192.168.252.128 DNS 210 Standard query response 0x989e AAAA g-ecx.images-amazon.com CNAME d1ge0kk1l5kms0.cloudfront.net SOA ns-1553.awsdns-02.co.uk
 5  0.106961 192.168.252.2 ? 192.168.252.128 DNS 254 Standard query response 0x55cd A g-ecx.images-amazon.com CNAME d1ge0kk1l5kms0.cloudfront.net A 52.84.108.157 A 52.84.108.185 A 52.84.108.225 A 52.84.108.136 A 52.84.108.11 A 52.84.108.71 A 52.84.108.210 A 52.84.108.100
 6  0.132846 192.168.252.2 ? 192.168.252.128 DNS 254 Standard query response 0xffff A g-ecx.images-amazon.com CNAME d1ge0kk1l5kms0.cloudfront.net A 52.84.108.210 A 52.84.108.225 A 52.84.108.71 A 52.84.108.11 A 52.84.108.136 A 52.84.108.157 A 52.84.108.100 A 52.84.108.185
 7  0.133240 192.168.252.128 ? 52.84.108.210 TCP 74 39977 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800828 TSecr=0 WS=1024
 8  0.384492 192.168.252.128 ? 52.84.108.210 TCP 74 39978 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800891 TSecr=0 WS=1024
 9  1.132866 192.168.252.128 ? 52.84.108.210 TCP 74 [TCP Retransmission] 39977 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=801078 TSecr=0 WS=1024
10  1.384243 192.168.252.128 ? 52.84.108.210 TCP 74 [TCP Retransmission] 39978 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=801141 TSecr=0 WS=1024

```

Q2. How can you find the total number of packets in HTTP_traffic.pcap?

Read the pcap file with Tshark and pipe the output to wc (word count) tools.

Answer: tshark -r HTTP_traffic.pcap | wc -l

```

student@attackdefense:~$ tshark -r HTTP_traffic.pcap | wc -l
30418
student@attackdefense:~$

```

Q3. Tshark command to read the first 100 packets only from HTTP_traffic.pcap?

Answer: tshark -r HTTP_traffic.pcap -c 100


```

student@attackdefense:~$ tshark -r HTTP_traffic.pcap -c 100
 1  0.000000 192.168.252.128 ? 192.168.252.2 DNS 83 Standard query 0x55cd A g-ecx.images-amazon.com
 2  0.000096 192.168.252.128 ? 192.168.252.2 DNS 83 Standard query 0x989e AAAA g-ecx.images-amazon.com
 3  0.001097 192.168.252.128 ? 192.168.252.2 DNS 83 Standard query 0xffffd A g-ecx.images-amazon.com
 4  0.035787 192.168.252.2 ? 192.168.252.128 DNS 210 Standard query response 0x989e AAAA g-ecx.images-amazon.com CNAME d1ge0kk1l5kms0.cloudfront.net SOA ns-1553.awsdns-02.co.uk
 5  0.106961 192.168.252.2 ? 192.168.252.128 DNS 254 Standard query response 0x55cd A g-ecx.images-amazon.com CNAME d1ge0kk1l5kms0.cloudfront.net A 52.84.108.157 A 52.84.108.185 A 52.84.108.225 A 52.84.108.136 A 52.84.108.11 A 52.84.108.71 A 52.84.108.210 A 52.84.108.100
 6  0.132846 192.168.252.2 ? 192.168.252.128 DNS 254 Standard query response 0xffffd A g-ecx.images-amazon.com CNAME d1ge0kk1l5kms0.cloudfront.net A 52.84.108.210 A 52.84.108.225 A 52.84.108.71 A 52.84.108.11 A 52.84.108.136 A 52.84.108.157 A 52.84.108.100 A 52.84.108.185
 7  0.133240 192.168.252.128 ? 52.84.108.210 TCP 74 39977 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800828 TSecr=0 WS=102
 8  0.384492 192.168.252.128 ? 52.84.108.210 TCP 74 39978 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800891 TSecr=0 WS=102
 9  1.132866 192.168.252.128 ? 52.84.108.210 TCP 74 [TCP Retransmission] 39977 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=801078 TSecr=0 WS=1024
10  1.384243 192.168.252.128 ? 52.84.108.210 TCP 74 [TCP Retransmission] 39978 ? 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=801141 TSecr=0 WS=1024

```

Q4. Print the list of protocols in HTTP_traffic.pcap

Answer: tshark -r HTTP_traffic.pcap -z io,phs -q

```

student@attackdefense:~$ tshark -r HTTP_traffic.pcap -z io,phs -q

=====
Protocol Hierarchy Statistics
Filter:

eth                                frames:30418 bytes:24643014
  ip                               frames:30413 bytes:24642732
    udp                           frames:1882 bytes:228368
      dns                         frames:1882 bytes:228368
        tcp                       frames:28531 bytes:24414364
          http                    frames:1455 bytes:1705881
            data-text-lines       frames:189 bytes:362230
              tcp.segments        frames:102 bytes:259949
            image-jfif            frames:165 bytes:444708
              tcp.segments        frames:145 bytes:343160
            image-gif            frames:75 bytes:44670
              tcp.segments        frames:6 bytes:7911
            oosp                  frames:73 bytes:62621
              tcp.segments        frames:5 bytes:2451
            media                 frames:120 bytes:217932
              tcp.segments        frames:79 bytes:158145
            png                   frames:61 bytes:113354
              tcp.segments        frames:30 bytes:62520
            json                  frames:29 bytes:35164
              tcp.segments        frames:5 bytes:7115
            data-text-lines       frames:3 bytes:1744

```

References:

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