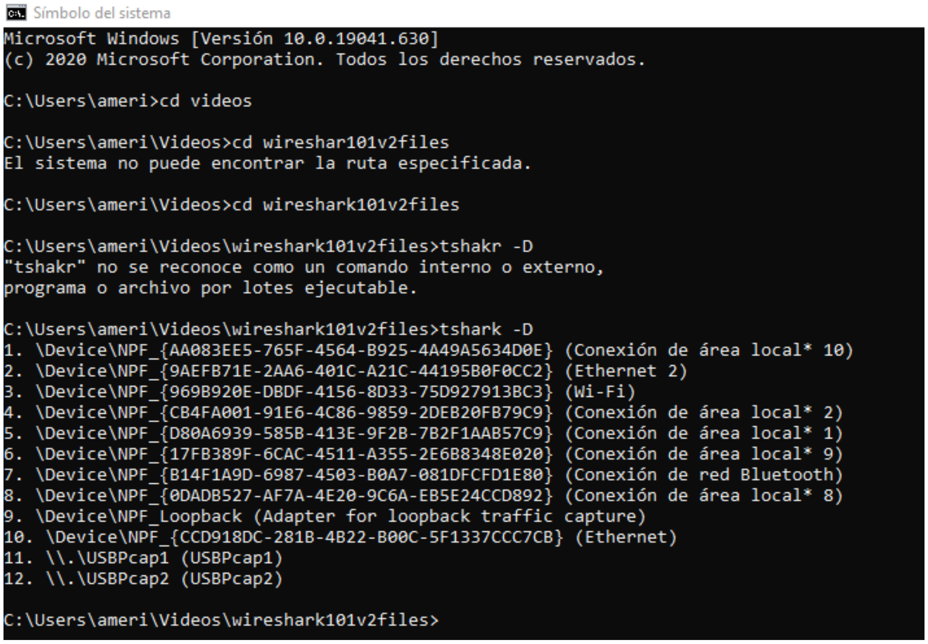
CHALLENGE 8

Open challenge101-8.pcapng and use the techniques covered in this chapter to answer these Challenge questions. The answer key is located inAppendix A.

Question 8-1.
What Tshark parameter should you use to list active interfaces on your Wireshark system?

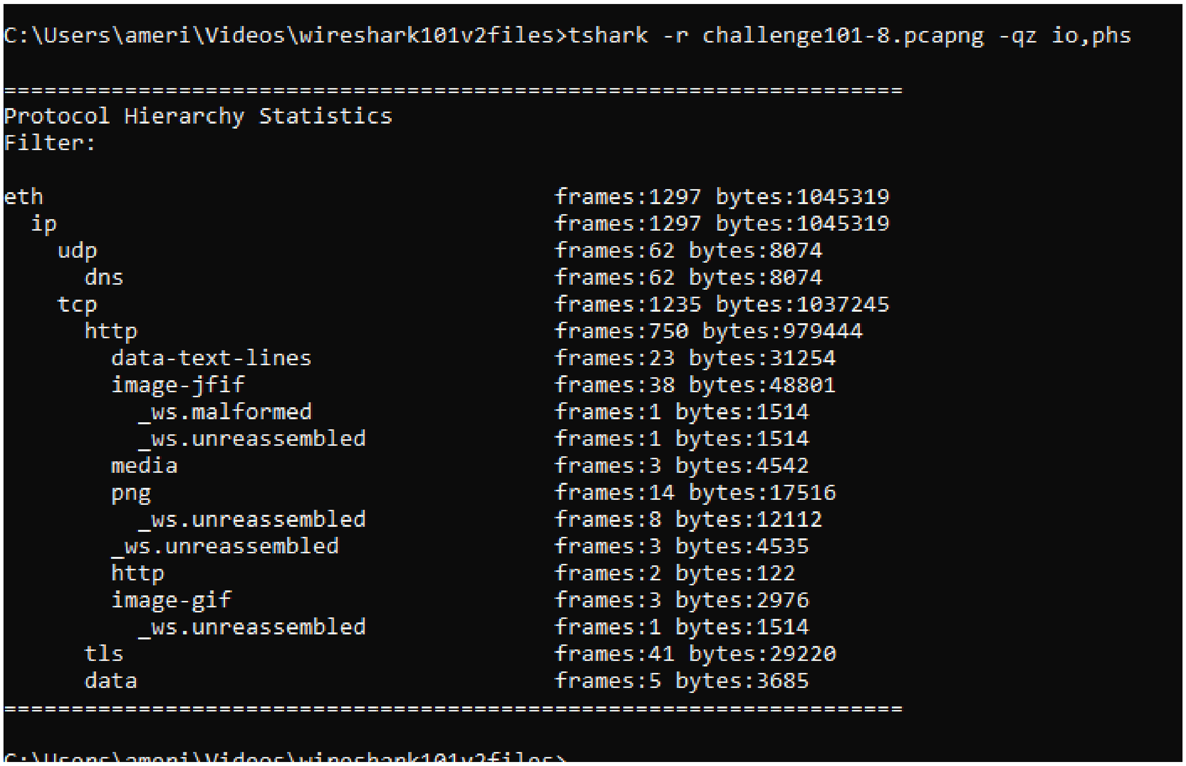
El parámetro –D para enumerar las interfaces activas en su sistema Wireshark



```
Microsoft Windows [Versión 10.0.19041.630]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\ameri>cd videos

C:\Users\ameri\Videos>cd wireshar101v2files
El sistema no puede encontrar la ruta especificada.

C:\Users\ameri\Videos>cd wireshark101v2files

C:\Users\ameri\Videos\wireshark101v2files>tshakr -D
"tshakr" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\ameri\Videos\wireshark101v2files>tshark -D
1. \Device\NPF_{AA083EE5-765F-4564-B925-4A49A5634D0E} (Conexión de área local* 10)
2. \Device\NPF_{9AEFB71E-2AA6-401C-A21C-44195B0F0CC2} (Ethernet 2)
3. \Device\NPF_{969B920E-DBDF-4156-8D33-75D927913BC3} (Wi-Fi)
4. \Device\NPF_{CB4FA001-91E6-4C86-9859-2DEB20FB79C9} (Conexión de área local* 2)
5. \Device\NPF_{D80A6939-585B-413E-9F2B-7B2F1AAB57C9} (Conexión de área local* 1)
6. \Device\NPF_{17FB389F-6CAC-4511-A355-2E6B8348E020} (Conexión de área local* 9)
7. \Device\NPF_{B14F1A9D-6987-4503-B0A7-081DFCFD1E80} (Conexión de red Bluetooth)
8. \Device\NPF_{0DADB527-AF7A-4E20-9C6A-EB5E24CCD892} (Conexión de área local* 8)
9. \Device\NPF_Loopback (Adapter for loopback traffic capture)
10. \Device\NPF_{CCD918DC-281B-4B22-B00C-5F1337CCC7CB} (Ethernet)
11. \\.\USBPcap1 (USBPcap1)
12. \\.\USBPcap2 (USBPcap2)

C:\Users\ameri\Videos\wireshark101v2files>
```

Question 8-2.
Using Tshark to extract protocol hierarchy information, how many UDP frames are in challenge101-8.pcapng?

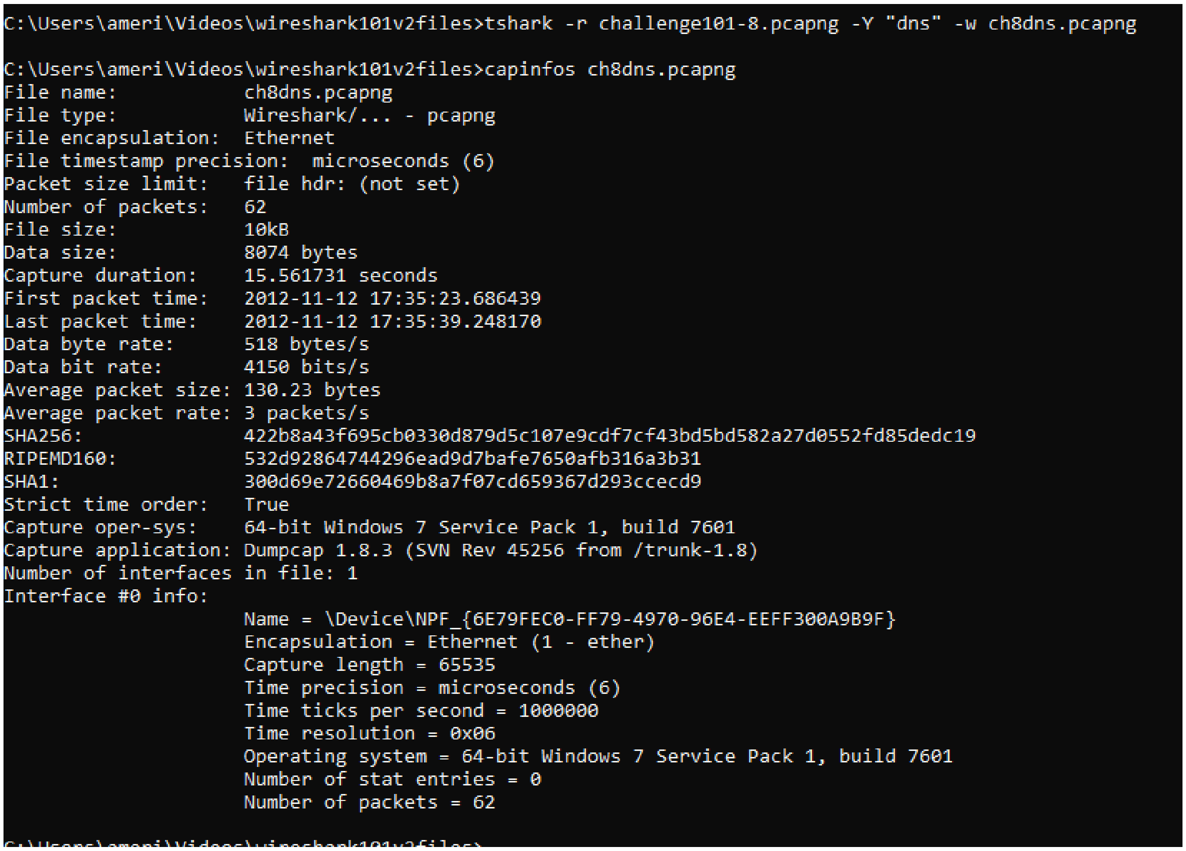
Usando tshark –r challenge101-8.pcapng –qz io, phs, determinamos que hay 62 tramas UDP en challenge101-8.pcapng.



```
C:\Users\ameri\Videos\wireshark101v2files>tshark -r challenge101-8.pcapng -qz io,phs

===================================================================
Protocol Hierarchy Statistics
Filter:

eth                                       frames:1297 bytes:1045319
  ip                                      frames:1297 bytes:1045319
    udp                                   frames:62 bytes:8074
      dns                                 frames:62 bytes:8074
    tcp                                   frames:1235 bytes:1037245
      http                                frames:750 bytes:979444
        data-text-lines                   frames:23 bytes:31254
        image-jfif                        frames:38 bytes:48801
          _ws.malformed                   frames:1 bytes:1514
          _ws.unreassembled               frames:1 bytes:1514
        media                             frames:3 bytes:4542
        png                               frames:14 bytes:17516
          _ws.unreassembled               frames:8 bytes:12112
        _ws.unreassembled                 frames:3 bytes:4535
        http                              frames:2 bytes:122
        image-gif                         frames:3 bytes:2976
          _ws.unreassembled               frames:1 bytes:1514
      tls                                 frames:41 bytes:29220
      data                                frames:5 bytes:3685
===================================================================

C:\Users\ameri\Videos\wireshark101v2files>
```

Question 8-3.
Use Tshark to export all DNS packets from challenge101-8.pcapng to a new trace file called ch8dns.pcapng. How many packets were exported?

Exportamos el tráfico DNS y encontramos que hay 62 paquetes DNS. Aparentemente, todo el tráfico UDP es DNS. Podríamos haber usado capinfos ch8dns.pcapng para obtener el recuento de paquetes también.



```
C:\Users\ameri\Videos\wireshark101v2files>tshark -r challenge101-8.pcapng -Y "dns" -w ch8dns.pcapng

C:\Users\ameri\Videos\wireshark101v2files>capinfos ch8dns.pcapng
File name:           ch8dns.pcapng
File type:           Wireshark/... - pcapng
File encapsulation:  Ethernet
File timestamp precision:  microseconds (6)
Packet size limit:   file hdr: (not set)
Number of packets:   62
File size:           10kB
Data size:           8074 bytes
Capture duration:    15.561731 seconds
First packet time:   2012-11-12 17:35:23.686439
Last packet time:    2012-11-12 17:35:39.248170
Data byte rate:      518 bytes/s
Data bit rate:       4150 bits/s
Average packet size: 130.23 bytes
Average packet rate: 3 packets/s
SHA256:              422b8a43f695cb0330d879d5c107e9cdf7cf43bd5bd582a27d0552fd85dedc19
RIPEMD160:           532d92864744296ead9d7bafe7650afb316a3b31
SHA1:                300d69e72660469b8a7f07cd659367d293ccecd9
Strict time order:   True
Capture oper-sys:    64-bit Windows 7 Service Pack 1, build 7601
Capture application: Dumpcap 1.8.3 (SVN Rev 45256 from /trunk-1.8)
Number of interfaces in file: 1
Interface #0 info:
                     Name = \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}
                     Encapsulation = Ethernet (1 - ether)
                     Capture length = 65535
                     Time precision = microseconds (6)
                     Time ticks per second = 1000000
                     Time resolution = 0x06
                     Operating system = 64-bit Windows 7 Service Pack 1, build 7601
                     Number of stat entries = 0
                     Number of packets = 62

C:\Users\ameri\Videos\wireshark101v2files>
```