U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

Wireshark

📅 October 2023

✉ cyberforcecompetition@anl.gov

Wireshark 101

Introduction

Wireshark is an opensource application with a GUI that is used to capture and analyze network traffic. It can be used to fix network problems, identify security issues, debug applications and more. Wireshark does this by allowing users to open captured packets, capture packets in real time, filter and save packets, create detailed reports and much more. It is important understand that Wireshark only observes network traffic, it cannot change anything on the network.

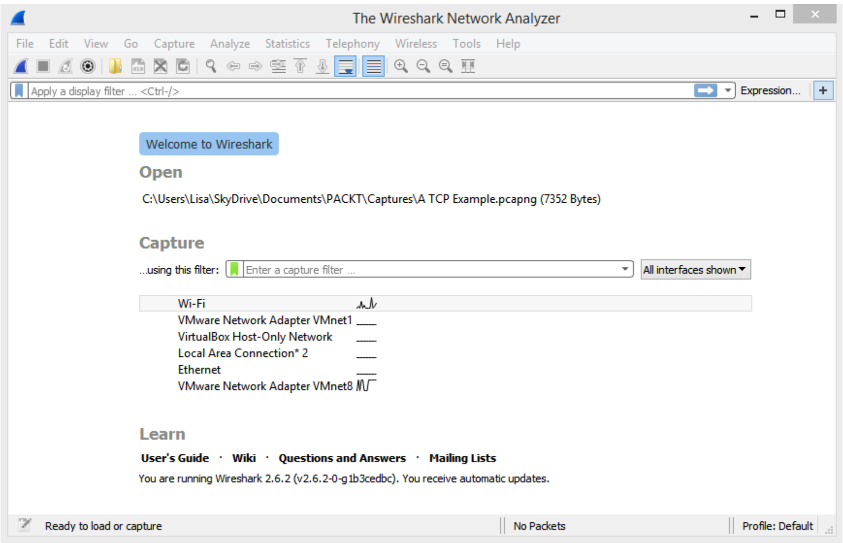
Wireshark Use

Before Wireshark can be used, users should go to the Wireshark website and download the application onto their system. Users can download different versions to match their systems.

To run Wireshark on a system, enter the command:

```
sudo wireshark
```

The Wireshark GUI will then open to its home screen. There will be a text box reading "Welcome to Wireshark" and below it will be a bar for users to type in. That bar is used for entering restrictions on the type of packets Wireshark should capture. If the command entered is valid, the bar will turn green. If it is left empty, the application will capture and record any packets it finds.



Apply a display filter ... <Ctrl-/>

Open

C:\Users\Lisa\SkyDrive\Documents\PACKT\Captures\A TCP Example.pcapng (7352 Bytes)

Capture

...using this filter: Enter a capture filter ...

Wi-Fi
VMware Network Adapter VMnet1
VirtualBox Host-Only Network
Local Area Connection* 2
Ethernet
VMware Network Adapter VMnet8

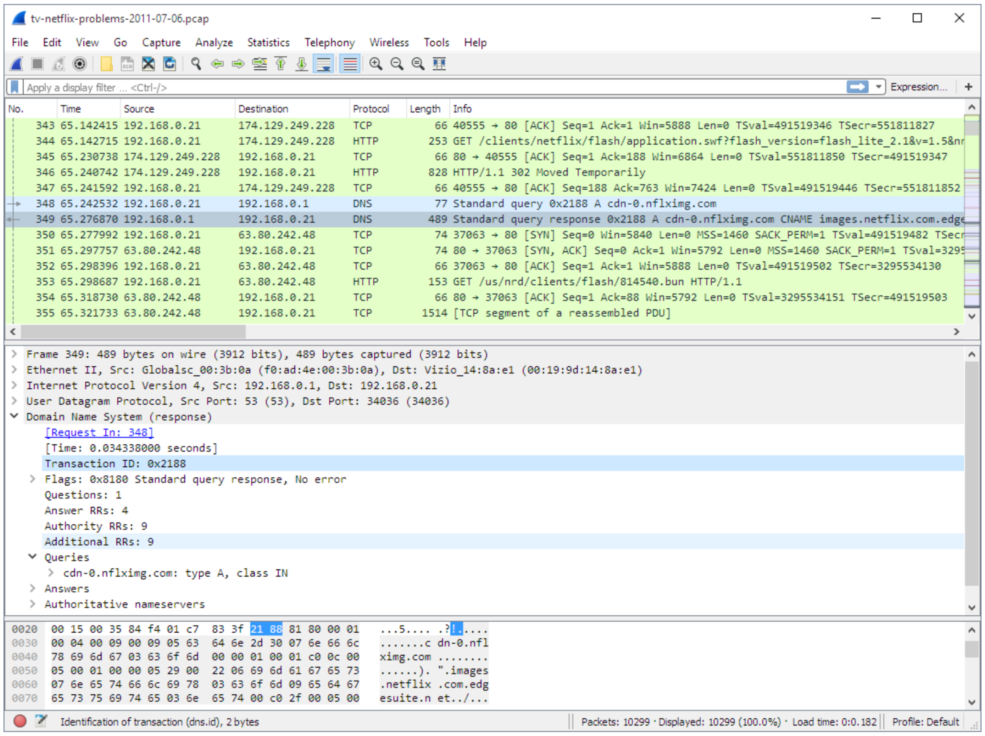
Learn

You are running Wireshark 2.6.2 (v2.6.2-0-g1b3cedbc). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

The list below the input bar contains all the interfaces Wireshark can listen to. Users can select multiple at a time. The green (or blue depending on the version) shark fin at the top of the screen is the starting button and the red square next to it is the stop button.

In the menu bar at the top of the Wireshark GUI, the "view" option can also be used to filter the packets captured. To get information about a specific packet, clicking on it will show some of its contents. It is possible to see ports being used, MAC addresses, encrypted data and more.



```
No.   Time      Source          Destination     Protocol  Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP         66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP       253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP         66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP       828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP         66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS         77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS        489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP         74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP         74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP         66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP       153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP         66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP       1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182

Profile: Default

The filter bar at the top of the screen will take a valid protocol name and filter out all other packets. Users know a name is valid when the bar turns green. It can also filter by IP addresses, times and more.

To export Wireshark data, go to the "file" tab and there are multiple options for what to export and how to do it. It is also possible to save the packets captured during a session.

Sources

- https://www.youtube.com/watch?v=TkCSr30UojM
- https://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallWinInstall.html