Viewing TCP/IP Protocols and Wireshark

Ramon Lopez Jr

Department of Cyber Security: University of Advancing Technology

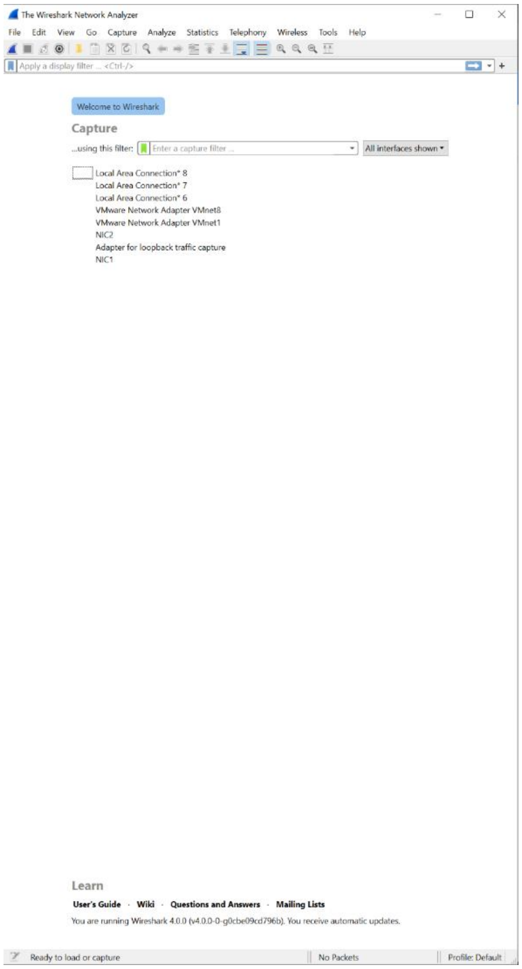
NTW102: Foundations of Network Engineering

Professor Jeremy Bunce

October 16th, 2022

Viewing TCP/IP Protocols and Wireshark

In the field of networking, capturing packets is a vital technique for analyzing network performance and identifying suspicious activity. By examining network traffic, IT professionals can determine whether the network is functioning properly or if unauthorized actions are occurring. One of the most widely used tools for this task is Wireshark, a powerful network protocol analyzer.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

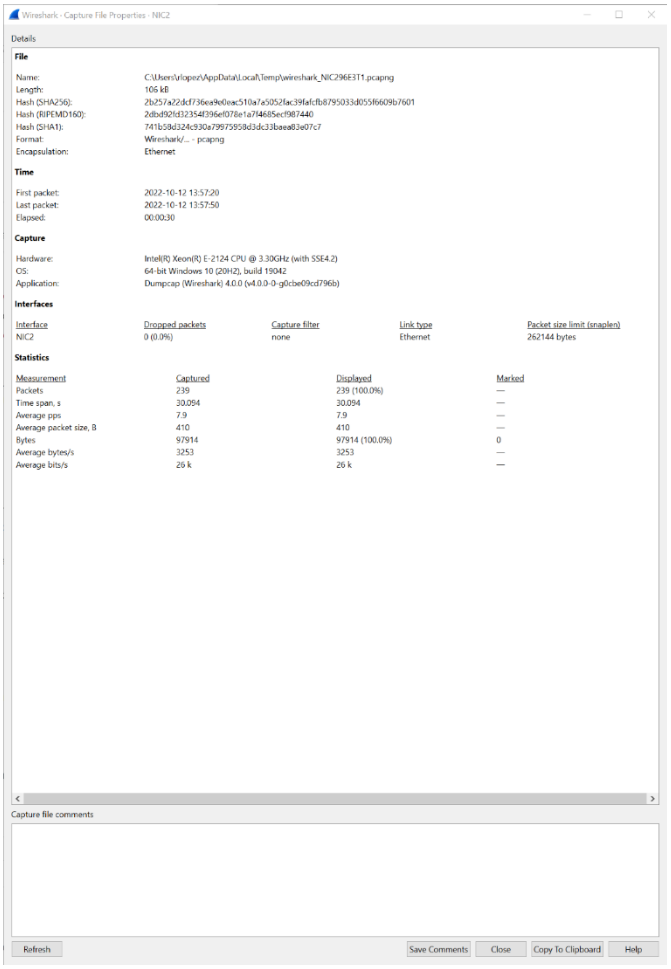
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
NIC2
Adapter for loopback traffic capture
NIC1

You are running Wireshark 4.0.0 (v4.0.0-0-g0cbe09cd796b). You receive automatic updates.

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

Image of Wireshark opened and ready to go

Using Wireshark



File

Name: C:\Users\rlopez\AppData\Local\Temp\wireshark_NIC296E3T1.pcapng
Length: 106 kB
Hash (SHA256): 2b257a22dcf736ea9e0eac510a7a5052fac39fafcfb8795033d055f6609b7601
Hash (RIPEMD160): 2dbd92fd32354f396ef078e1a7f4685ecf987440
Hash (SHA1): 741b58d324c930a79975958d3dc33baea83e07c7
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2022-10-12 13:57:20
Last packet: 2022-10-12 13:57:50
Elapsed: 00:00:30

Capture

Hardware: Intel(R) Xeon(R) E-2124 CPU @ 3.30GHz (with SSE4.2)
OS: 64-bit Windows 10 (20H2), build 19042
Application: Dumpcap (Wireshark) 4.0.0 (v4.0.0-0-g0cbe09cd796b)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
NIC2	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

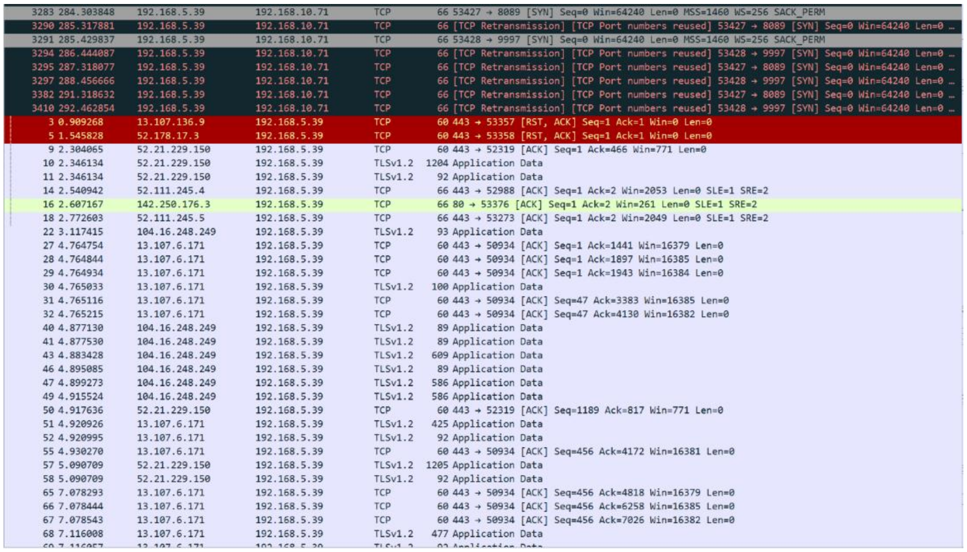
Measurement	Captured	Displayed	Marked
Packets	239	239 (100.0%)	—
Time span, s	30.094	30.094	—
Average pps	7.9	7.9	—
Average packet size, B	410	410	—
Bytes	97914	97914 (100.0%)	0
Average bytes/s	3253	3253	—
Average bits/s	26 k	26 k	—

The image above displays the Wireshark interface prepared to begin packet capture. In the initial test, packets were captured over a 30-second period. Upon completion, Wireshark reported a total of 239 packets collected. Following this, a longer five-minute capture session was conducted. Although the exact number of packets captured is not recalled, the range was approximately 300 to 3,000 packets. During this session, Wireshark identified a variety of protocols—12 in total. These included:

- **ARP:** Resolves IPv4 addresses to MAC (Media Access Control) addresses.

- **CDP (Cisco Discovery Protocol):** Enables inspection of connected devices without physical access, allowing users to retrieve information such as device type and software version.
- **DNS:** Resolves domain names to their corresponding IP addresses.
- **LLDP (Link Layer Discovery Protocol):** Identifies and communicates device capabilities and configurations on the local network.
- **NBSS (NetBIOS Session Service):** Handles session-layer communication and naming services, using 16-byte names for unique identification.

Other protocols observed included LOOP, SMB2, SSDP, STP, TCP, and TLS versions 1.2 and 1.3.



```
3283 284.303848   192.168.5.39     192.168.10.71    TCP        66 53427 → 8089 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3290 285.317881   192.168.5.39     192.168.10.71    TCP        66 [TCP Retransmission] [TCP Port numbers reused] 53427 → 8089 [SYN] Seq=0 Win=64240 Len=0 …
3291 285.429837   192.168.5.39     192.168.10.71    TCP        66 53428 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3294 286.444087   192.168.5.39     192.168.10.71    TCP        66 [TCP Retransmission] [TCP Port numbers reused] 53428 → 9997 [SYN] Seq=0 Win=64240 Len=0 …
3295 287.318077   192.168.5.39     192.168.10.71    TCP        66 [TCP Retransmission] [TCP Port numbers reused] 53427 → 8089 [SYN] Seq=0 Win=64240 Len=0 …
3297 288.456666   192.168.5.39     192.168.10.71    TCP        66 [TCP Retransmission] [TCP Port numbers reused] 53428 → 9997 [SYN] Seq=0 Win=64240 Len=0 …
3382 291.318632   192.168.5.39     192.168.10.71    TCP        66 [TCP Retransmission] [TCP Port numbers reused] 53427 → 8089 [SYN] Seq=0 Win=64240 Len=0 …
3410 292.462854   192.168.5.39     192.168.10.71    TCP        66 [TCP Retransmission] [TCP Port numbers reused] 53428 → 9997 [SYN] Seq=0 Win=64240 Len=0 …
   3 0.909268     13.107.136.9     192.168.5.39     TCP        60 443 → 53357 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   5 1.545828     52.178.17.3      192.168.5.39     TCP        60 443 → 53358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   9 2.304065     52.21.229.150    192.168.5.39     TCP        60 443 → 52319 [ACK] Seq=1 Ack=466 Win=771 Len=0
  10 2.346134     52.21.229.150    192.168.5.39     TLSv1.2  1204 Application Data
  11 2.346134     52.21.229.150    192.168.5.39     TLSv1.2    92 Application Data
  14 2.540942     52.111.245.4     192.168.5.39     TCP        66 443 → 52988 [ACK] Seq=1 Ack=2 Win=2053 Len=0 SLE=1 SRE=2
  16 2.607167     142.250.176.3    192.168.5.39     TCP        66 80 → 53376 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
  18 2.772603     52.111.245.5     192.168.5.39     TCP        66 443 → 53273 [ACK] Seq=1 Ack=2 Win=2049 Len=0 SLE=1 SRE=2
  22 3.117415     104.16.248.249   192.168.5.39     TLSv1.2    93 Application Data
  27 4.764754     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=1 Ack=1441 Win=16379 Len=0
  28 4.764844     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=1 Ack=1897 Win=16385 Len=0
  29 4.764934     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=1 Ack=1943 Win=16384 Len=0
  30 4.765033     13.107.6.171     192.168.5.39     TLSv1.2   100 Application Data
  31 4.765116     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=47 Ack=3383 Win=16385 Len=0
  32 4.765215     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=47 Ack=4130 Win=16382 Len=0
  40 4.877130     104.16.248.249   192.168.5.39     TLSv1.2    89 Application Data
  41 4.877530     104.16.248.249   192.168.5.39     TLSv1.2    89 Application Data
  43 4.883428     104.16.248.249   192.168.5.39     TLSv1.2   609 Application Data
  46 4.895085     104.16.248.249   192.168.5.39     TLSv1.2    89 Application Data
  47 4.899273     104.16.248.249   192.168.5.39     TLSv1.2   586 Application Data
  49 4.915524     104.16.248.249   192.168.5.39     TLSv1.2   586 Application Data
  50 4.917636     52.21.229.150    192.168.5.39     TCP        60 443 → 52319 [ACK] Seq=1189 Ack=817 Win=771 Len=0
  51 4.920926     13.107.6.171     192.168.5.39     TLSv1.2   425 Application Data
  52 4.920995     13.107.6.171     192.168.5.39     TLSv1.2    92 Application Data
  55 4.930270     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=456 Ack=4172 Win=16381 Len=0
  57 5.090709     52.21.229.150    192.168.5.39     TLSv1.2  1205 Application Data
  58 5.090709     52.21.229.150    192.168.5.39     TLSv1.2    92 Application Data
  65 7.078293     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=456 Ack=4818 Win=16379 Len=0
  66 7.078444     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=456 Ack=6258 Win=16385 Len=0
  67 7.078543     13.107.6.171     192.168.5.39     TCP        60 443 → 50934 [ACK] Seq=456 Ack=7026 Win=16382 Len=0
  68 7.116008     13.107.6.171     192.168.5.39     TLSv1.2   477 Application Data
  69 7.116057     13.107.6.171     192.168.5.39     TLSv1.2    92 Application Data
```

During the five-minute scan, numerous IP destinations were observed. Among the first ten identifiable destinations, the following examples were noted:

- 192.168.10.71

- 13.107.136.9

- 52.21.229.150

These are only a small sample of the many addresses that appeared during the capture session.

References

@kmbh. "What Is Cisco Discovery Protocol (CDP)?" *GeeksforGeeks*, 1 Nov. 2021, www.geeksforgeeks.org/what-is-cisco-discovery-protocol-cdp/#:~:text=Benefits%20of%20CDP%3A%201%20It%20allows%20the%20use. Accessed 13 Oct. 2022.

Mills, Matt. "ARP Protocol: How It Works and Why It Is so Important | ITIGIC." *Itigic.com*, 24 Oct. 2021, itigic.com/arp-protocol-how-it-works-and-why-it-is-so-important/#:~:text=In%20short%2C%20the%20ARP%20protocol%20is%20used%20to. Accessed 13 Oct. 2022.

---. "What Is the DNS Protocol and Why Is It so Important? | ITIGIC." *Itigic.com*, 13 Oct. 2021, itigic.com/what-is-dns-protocol-and-why-is-it-so-important/#:~:text=DNS%20is%20the%20acronym%20for%20the%20domain%20name. Accessed 13 Oct. 2022.

"What Is LLDP? | Comprehensive Guide to LLDP with Benefits." *EDUCBA*, 9 Dec. 2019, www.educba.com/what-is-lldp/.

"What Is NetBIOS Session Service (NBSS)? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/25190/netbios-session-service-nbss#:~:text=A%20system%20with%20NBSS%20implementation%20has%20the%20following. Accessed 13 Oct. 2022.