

Viewing TCP/IP Protocols and Wireshark

Jerome Reaux Jr.

University Of Advancing Technology

NTW102

Professor B

2/27/2023

Wireshark NIC1 Running for 30 seconds

368	34.714755	23.223.242.13	192.168.5.28	TCP	66 443 → 65023 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
369	34.952433	192.168.5.28	151.101.1.91	TCP	55 64825 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
370	34.962623	151.101.1.91	192.168.5.28	TCP	66 443 → 64825 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
371	35.099539	192.168.5.28	142.250.189.10	TCP	55 65034 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembled PDU]
372	35.109761	142.250.189.10	192.168.5.28	TCP	66 443 → 65034 [ACK] Seq=1 Ack=2 Win=271 Len=0 SLE=1 SRE=2
373	35.339105	192.168.5.39	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
374	35.437967	192.168.5.28	23.212.64.43	TCP	55 65037 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
375	35.470586	23.212.64.43	192.168.5.28	TCP	66 443 → 65037 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
376	35.553816	192.168.5.28	23.212.64.43	TCP	55 65039 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
377	35.584964	23.212.64.43	192.168.5.28	TCP	66 443 → 65039 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
378	35.769943	192.168.5.28	168.61.75.116	TCP	55 65041 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembled PDU]
379	35.789223	168.61.75.116	192.168.5.28	TCP	66 443 → 65041 [ACK] Seq=1 Ack=2 Win=2053 Len=0 SLE=1 SRE=2
380	35.805423	192.168.5.5	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
381	36.080938	52.111.245.2	192.168.5.28	TLSv1.2	105 Application Data
382	36.090384	Cisco_00:45:07	Spanning-tree-(for- STP	60 Conf. Root = 32768/5/00:22:be:83:fb:00 Cost = 7 Port = 0x8007	
383	36.139294	192.168.5.28	52.111.245.2	TCP	54 64995 → 443 [ACK] Seq=1 Ack=205 Win=1027 Len=0
384	36.217409	192.168.5.28	13.107.6.171	TCP	55 65042 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembled PDU]
385	36.225553	13.107.6.171	192.168.5.28	TCP	66 443 → 65042 [ACK] Seq=1 Ack=2 Win=16385 Len=0 SLE=1 SRE=2
386	36.354467	192.168.5.39	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
387	36.402241	192.168.5.28	52.109.0.136	TCP	55 65043 → 443 [ACK] Seq=1 Ack=1 Win=1029 Len=1 [TCP segment of a reassembled PDU]
388	36.420476	52.109.0.136	192.168.5.28	TCP	66 443 → 65043 [ACK] Seq=1 Ack=2 Win=2053 Len=0 SLE=1 SRE=2
389	36.555849	192.168.5.28	104.69.86.228	TCP	55 65048 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
390	36.555849	192.168.5.28	104.69.86.228	TCP	55 65049 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
391	36.555849	192.168.5.28	104.69.86.228	TCP	55 65051 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
392	36.587080	192.168.5.28	52.109.2.130	TCP	55 65053 → 443 [ACK] Seq=1 Ack=1 Win=1029 Len=1 [TCP segment of a reassembled PDU]
393	36.589121	104.69.86.228	192.168.5.28	TCP	66 443 → 65051 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
394	36.590799	104.69.86.228	192.168.5.28	TCP	66 443 → 65048 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
395	36.591160	104.69.86.228	192.168.5.28	TCP	66 443 → 65049 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
396	36.605673	52.109.2.130	192.168.5.28	TCP	66 443 → 65053 [ACK] Seq=1 Ack=2 Win=2047 Len=0 SLE=1 SRE=2
397	36.618324	192.168.5.28	104.69.86.228	TCP	55 65052 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
398	36.651554	104.69.86.228	192.168.5.28	TCP	66 443 → 65052 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
399	36.656072	192.168.5.28	104.69.86.228	TCP	55 65050 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
400	36.687337	192.168.5.28	104.69.86.228	TCP	55 65047 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF{...}

> IEEE 802.3 Ethernet

> Logical-Link Control

> Spanning Tree Protocol

0000 01 80 c2 00 00 00 b4 14 89 80 45 07 00 26 42 42E...&BB

0010 03 00 00 00 00 00 00 05 00 22 be 83 fb 00 00 00 ".....

0020 00 07 80 05 b4 14 89 80 45 00 80 07 02 00 14 00E.....

0030 02 00 0f 00 00 00 00 00 00 00 00 00

How many packets total packets were captured? Include a screenshot of the 30s mark of packets.

There was 400 Packets captured in the 30 second period

Wireshark NIC1 Running for 5 minutes

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the detailed view of the selected packet (No. 6242), including the Ethernet II header, Internet Protocol (IP) header, and Transmission Control Protocol (TCP) header.

No.	Time	Source	Destination	Protocol	Length	Info
6223	300.107107	192.168.5.32	192.168.5.28	TCP	60	7680 → 65168 [ACK] Seq=2 Ack=77 Win=2102272 Len=0
6224	300.161599	Cisco_80:45:07	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/5/00:22:be:83:fb:00 Cost = 7 Port = 0x8007
6225	300.581400	Cisco_80:45:07	Cisco_80:45:07	LOOP	60	Reply
6226	300.939661	192.168.5.28	52.108.8.12	TLSv1.2	2718	Application Data
6227	300.939693	192.168.5.28	52.108.8.12	TLSv1.2	100	Application Data
6228	300.939706	192.168.5.28	52.108.8.12	TLSv1.2	2310	Application Data
6229	300.950886	52.108.8.12	192.168.5.28	TCP	60	443 → 65024 [ACK] Seq=60665 Ack=837726 Win=16385 Len=0
6230	300.950903	52.108.8.12	192.168.5.28	TCP	60	443 → 65024 [ACK] Seq=60665 Ack=840436 Win=16385 Len=0
6231	300.950937	52.108.8.12	192.168.5.28	TCP	60	443 → 65024 [ACK] Seq=60665 Ack=841252 Win=16381 Len=0
6232	300.951248	52.108.8.12	192.168.5.28	TLSv1.2	100	Application Data
6233	300.986121	52.108.8.12	192.168.5.28	TLSv1.2	685	Application Data
6234	300.986121	52.108.8.12	192.168.5.28	TLSv1.2	92	Application Data
6235	300.986146	192.168.5.28	52.108.8.12	TCP	54	65024 → 443 [ACK] Seq=841252 Ack=61380 Win=2058 Len=0
6236	300.987136	192.168.5.28	52.108.8.12	TLSv1.2	96	Application Data
6237	300.995379	52.111.245.2	192.168.5.28	TLSv1.2	105	Application Data
6238	300.998250	52.108.8.12	192.168.5.28	TCP	60	443 → 65024 [ACK] Seq=61380 Ack=841294 Win=16381 Len=0
6239	301.038345	192.168.5.28	52.111.245.2	TCP	54	65079 → 443 [ACK] Seq=1 Ack=1624 Win=1027 Len=0
6240	301.070867	192.168.5.28	20.189.173.6	TCP	55	[TCP Keep-Alive] 65036 → 443 [ACK] Seq=14023 Ack=749 Win=1026 Len=1
6241	301.089342	20.189.173.6	192.168.5.28	TCP	66	[TCP Keep-Alive ACK] 443 → 65036 [ACK] Seq=749 Ack=14024 Win=16384 Len=0 SLE=14023 SRE=14024
6242	301.155526	192.168.5.28	192.168.10.71	TCP	66	[TCP Retransmission] 65167 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6243	302.048441	40.104.2.130	192.168.5.28	TLSv1.2	102	Application Data
6244	302.053531	192.168.5.28	40.104.2.130	TLSv1.2	96	Application Data
6245	302.053549	192.168.5.28	40.104.2.130	TLSv1.2	96	Application Data
6246	302.072122	40.104.2.130	192.168.5.28	TCP	60	443 → 64930 [ACK] Seq=8519 Ack=23635 Win=16382 Len=0
6247	302.171429	Cisco_80:45:07	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/5/00:22:be:83:fb:00 Cost = 7 Port = 0x8007
6248	302.359940	192.168.5.28	40.104.2.130	TLSv1.2	3779	Application Data
6249	302.378477	40.104.2.130	192.168.5.28	TCP	60	443 → 64930 [ACK] Seq=8519 Ack=27360 Win=16385 Len=0
6250	302.420379	40.104.2.130	192.168.5.28	TLSv1.2	230	Application Data
6251	302.421920	40.104.2.130	192.168.5.28	TLSv1.2	789	Application Data
6252	302.421944	192.168.5.28	40.104.2.130	TCP	54	64930 → 443 [ACK] Seq=27360 Ack=9430 Win=1022 Len=0
6253	302.422684	40.104.2.130	192.168.5.28	TLSv1.2	92	Application Data
6254	302.472806	192.168.5.28	40.104.2.130	TCP	54	64930 → 443 [ACK] Seq=27360 Ack=9468 Win=1022 Len=0
6255	304.121064	52.111.245.2	192.168.5.28	TLSv1.2	105	Application Data

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF...
> Ethernet II, Src: Cisco_80:45:07 (b4:14:89:80:45:07), Dst: Cisco_80:45:07 (b4:14:89:80:45:07)
> Configuration Test Protocol (loopback)
> Data (40 bytes)

How many different protocols did you observe?

I observed 16 Different Protocols in the 5-minute window

List them. Include a screenshot.

1. CDP
2. DCERPC
3. DNS
4. DRSUAPI
5. HTTP
6. ICMPv6
7. LLMNR
8. LOOP

9. MDNS

10. MS-DO

11. OCSP

12. QUIC

13. SSDP

14. STP

15. TCP

16. TLSv1.2

Screenshots of some protocols

6098	283.280086	192.168.5.28	192.168.10.11	DNS	89 Standard query 0x2807 A word-edit.officeapps.live.com
6099	283.280332	192.168.5.28	192.168.10.11	DNS	89 Standard query 0xb7d4 HTTPS word-edit.officeapps.live.com
6102	283.280552	192.168.10.11	192.168.5.28	DNS	232 Standard query response 0x2807 A word-edit.officeapps.live.c
6103	283.282244	192.168.10.11	192.168.5.28	DNS	200 Standard query response 0xb7d4 HTTPS word-edit.officeapps.li
48	2.867170	192.168.5.28	192.168.10.11	DRSUAPI	322 DsBind request
49	2.867529	192.168.10.11	192.168.5.28	DRSUAPI	258 DsBind response
50	2.867602	192.168.5.28	192.168.10.11	DRSUAPI	306 DsCrackNames request
51	2.868091	192.168.10.11	192.168.5.28	DRSUAPI	370 DsCrackNames response
53	2.868127	192.168.5.28	192.168.10.11	DRSUAPI	194 DsUnbind request
54	2.868448	192.168.10.11	192.168.5.28	DRSUAPI	194 DsUnbind response
38	2.864473	192.168.5.28	192.168.10.11	EPH	222 Map request, DRSUAPI, 32bit NDR
39	2.864750	192.168.10.11	192.168.5.28	EPH	322 Map response, DRSUAPI, 32bit NDR, DRSUAPI, 32bit NDR
4427	184.314554	192.168.5.28	192.229.211.108	HTTP	288 GET /MFewTzBNMEswSTA3BgUrdgMCgUABBSAUQYBMq2awn1Rh6Doh%2FsBY
129	5.650060	fe80::6b84:4243:cab...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
130	5.654700	fe80::6b84:4243:cab...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
141	5.964680	fe80::6b84:4243:cab...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
180	10.169892	fe80::75ad:1fd6:41e...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
181	10.175486	fe80::75ad:1fd6:41e...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
192	10.248749	fe80::75ad:1fd6:41e...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
5675	268.235498	fe80::3edd:b87d:125...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
5677	268.241292	fe80::3edd:b87d:125...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
5704	268.574192	fe80::3edd:b87d:125...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
135	5.655643	fe80::6b84:4243:cab...	ff02::1:3	LLMNR	91 Standard query 0xa57f ANY REVANITE-06
136	5.655692	192.168.5.37	224.0.0.252	LLMNR	71 Standard query 0xa57f ANY REVANITE-06
186	10.177012	fe80::75ad:1fd6:41e...	ff02::1:3	LLMNR	91 Standard query 0xa4690 ANY REVANITE-07
187	10.177093	192.168.5.25	224.0.0.252	LLMNR	71 Standard query 0xa4690 ANY REVANITE-07
5681	268.242351	fe80::3edd:b87d:125...	ff02::1:3	LLMNR	91 Standard query 0xa4954 ANY REVANITE-18
5682	268.242421	192.168.5.9	224.0.0.252	LLMNR	71 Standard query 0xa4954 ANY REVANITE-18
1	0.000000	Cisco_80:45:07	Cisco_80:45:07	LOOP	60 Reply

5225	249.410681	192.168.5.9	192.168.5.28	MS-DO	129	Handshake Message (Request)
5383	259.789294	192.168.5.28	192.168.5.32	MS-DO	129	Handshake Message (Request)
6167	289.791572	192.168.5.9	192.168.5.28	MS-DO	129	Handshake Message (Request)
6219	300.106840	192.168.5.28	192.168.5.32	MS-DO	129	Handshake Message (Request)
4429	184.329993	192.229.211.108	192.168.5.28	OCSF	791	Response
1693	66.153680	192.168.5.28	142.250.72.138	QUIC	1292	Initial, DCID=f5e7cbebfa7f3585, PKN: 1, CRYPTO, PING, PING,
1694	66.153830	192.168.5.28	142.250.72.138	QUIC	124	0-RTT, DCID=f5e7cbebfa7f3585
1695	66.153967	192.168.5.28	142.250.72.138	QUIC	625	0-RTT, DCID=f5e7cbebfa7f3585
1697	66.173312	142.250.72.138	192.168.5.28	QUIC	1292	Handshake, SCID=f5e7cbebfa7f3585
1698	66.173312	142.250.72.138	192.168.5.28	QUIC	848	Protected Payload (KP0)
1700	66.174936	142.250.72.138	192.168.5.28	QUIC	234	Protected Payload (KP0)
1701	66.174936	142.250.72.138	192.168.5.28	QUIC	66	Protected Payload (KP0)
1702	66.174936	142.250.72.138	192.168.5.28	QUIC	64	Protected Payload (KP0)
1704	66.175302	192.168.5.28	142.250.72.138	QUIC	120	Handshake, DCID=f5e7cbebfa7f3585
1705	66.175362	192.168.5.28	142.250.72.138	QUIC	73	Protected Payload (KP0), DCID=f5e7cbebfa7f3585
1706	66.175423	192.168.5.28	142.250.72.138	QUIC	73	Protected Payload (KP0), DCID=f5e7cbebfa7f3585
1707	66.186408	142.250.72.138	192.168.5.28	QUIC	162	Protected Payload (KP0)
1708	66.221125	142.250.72.138	192.168.5.28	QUIC	421	Protected Payload (KP0)
1709	66.221213	142.250.72.138	192.168.5.28	QUIC	219	Protected Payload (KP0)
1710	66.221302	192.168.5.28	142.250.72.138	QUIC	77	Protected Payload (KP0), DCID=f5e7cbebfa7f3585
1712	66.232206	142.250.72.138	192.168.5.28	QUIC	67	Protected Payload (KP0)
1716	66.256809	192.168.5.28	142.250.72.138	QUIC	74	Protected Payload (KP0), DCID=f5e7cbebfa7f3585
1717	66.267538	142.250.72.138	192.168.5.28	QUIC	64	Protected Payload (KP0)
1718	66.267652	192.168.5.28	142.250.72.138	QUIC	75	Protected Payload (KP0), DCID=f5e7cbebfa7f3585
276	13.272619	192.168.5.28	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
315	14.287027	192.168.5.28	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
373	15.239936	192.168.5.28	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

6240	301.070807	192.168.5.28	20.189.173.6	TCP	55	[TCP Keep-Alive] 65036 → 443 [ACK] Seq=14023 Ack=749 Win=1024
6241	301.089342	20.189.173.6	192.168.5.28	TCP	66	[TCP Keep-Alive ACK] 443 → 65036 [ACK] Seq=749 Ack=14024 Win=1024
6242	301.155526	192.168.5.28	192.168.10.71	TCP	66	[TCP Retransmission] 65167 → 9997 [SYN] Seq=0 Win=64240 Len=0
6246	302.072122	40.104.2.130	192.168.5.28	TCP	60	443 → 64930 [ACK] Seq=8519 Ack=23635 Win=16382 Len=0
6249	302.378477	40.104.2.130	192.168.5.28	TCP	60	443 → 64930 [ACK] Seq=8519 Ack=27360 Win=16385 Len=0
6252	302.421944	192.168.5.28	40.104.2.130	TCP	54	64930 → 443 [ACK] Seq=27360 Ack=9430 Win=1022 Len=0
6254	302.472806	192.168.5.28	40.104.2.130	TCP	54	64930 → 443 [ACK] Seq=27360 Ack=9468 Win=1022 Len=0
6	0.456657	52.108.0.40	192.168.5.28	TLSv1.2	87	Application Data
19	2.041905	40.104.2.130	192.168.5.28	TLSv1.2	102	Application Data
65	2.933308	192.168.5.28	20.190.190.132	TLSv1.2	264	Client Hello (SNI=login.microsoftonline.com)
66	2.933367	192.168.5.28	20.190.190.132	TLSv1.2	264	Client Hello (SNI=login.microsoftonline.com)
70	2.940003	20.190.190.132	192.168.5.28	TLSv1.2	1370	Server Hello, Certificate, Certificate Status, Server Key Exchange

5 protocols

1. TCP- Transmission Control Protocol (TCP) is a crucial communication protocol in computer networks, ensuring reliable data delivery, data integrity, and efficient data exchange between devices through sequencing, acknowledgments, error detection, and flow control.

2. MS – DO - Microsoft Disk Operating System, a Microsoft-developed single-user, single-tasking computer operating system, was introduced in 1981 and became widely used on IBM PC-compatible computers, playing a crucial role in the early personal computing era.

3. DNS - The Domain Name System (DNS) protocol, operating on UDP port 53, converts domain names into IP addresses, allowing users to access websites and services using human-readable names, distributing domain authority across servers.

4. TLSv1.2 - Transport Layer Security protocol version 1.2 (TLSv1.2) is a cryptographic protocol that ensures secure communication over networks using strong encryption algorithms and key exchange mechanisms. It is widely used for secure web browsing, email, and other online services, protecting against eavesdropping and data tampering.

5. HTTP - The Hypertext Transfer Protocol (HTTP) is a fundamental web communication protocol that facilitates data exchange between clients and servers, enabling content retrieval and display, operating on a request-response model.