

Ping

247...	441.168388	10.188.204.9	142.251.41.14	ICMP	98	Echo (ping) request	id=0x9805, seq=46/11776, ttl=64 (reply in 24703)
247...	441.174249	142.251.41.14	10.188.204.9	ICMP	98	Echo (ping) reply	id=0x9805, seq=46/11776, ttl=58 (request in 24702)
247...	442.173322	10.188.204.9	142.251.41.14	ICMP	98	Echo (ping) request	id=0x9805, seq=47/12032, ttl=64 (reply in 24722)
247...	442.178840	142.251.41.14	10.188.204.9	ICMP	98	Echo (ping) reply	id=0x9805, seq=47/12032, ttl=58 (request in 24721)

– Source IP

- 142.251.41.14

– Destination IP

- 10.188.204.9

– Protocol

- ICMP

– Port

- NONE

nslookup

196...	400.405902	142.250.65.228	10.188.204.9	TCP	66	443 → 49920 [ACK] Seq=4936 Ack=1087 Win=68864 Len=0 TSval=867387841 TSecr=3010652088
196...	400.427608	10.188.204.9	142.250.65.228	TCP	66	49920 → 443 [ACK] Seq=1087 Ack=8790 Win=127168 Len=0 TSval=3010652122 TSecr=867387862

– Source IP

- 142.250.65.228

– Destination IP

- 10.188.204.9

– Protocol

- TCP

– Port

- 49920
- 443

whois

109	9.518105	10.188.204.9	66.253.214.16	DNS	65	Standard query 0x3d76 A whois
110	9.546317	66.253.214.16	10.188.204.9	DNS	140	Standard query response 0x3d76 No such name A whois SOA a.root-servers.net

– Source IP

- 66.253.214.16

– Destination IP

- 10.188.204.9

– Protocol

- DNS

– Port

- 53

NMAP

557...	749.137008	10.188.204.9	142.250.65.228	TCP	78	53130 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2788295170 TSecr=0 SACK_PERM=1
557...	749.137112	10.188.204.9	142.250.65.228	TCP	78	53131 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=545933380 TSecr=0 SACK_PERM=1
557...	749.303378	142.250.65.228	10.188.204.9	TCP	74	80 → 53130 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=505774825 TSecr=
557...	749.303378	142.250.65.228	10.188.204.9	TCP	74	443 → 53131 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=3115343484 TSecr=

- Source IP
 - 142.250.65.228
- Destination IP
 - 10.188.204.9
- Protocol
 - TCP
- Port(s)
 - 53131
 - 80
 - 443

TELNET

917...	1216.101683	213.136.8.188	10.188.204.9	TELNET	1054	Telnet Data ...
--------	-------------	---------------	--------------	--------	------	-----------------

- Source IP
 - 213.136.8.188
- Destination IP
 - 10.188.204.9
- Protocol
 - TELNET
- Port
 - SRC: 213
 - DEST: 55217

CURL

986...	1519.832468	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=1 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832469	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=1401 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832470	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=2801 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832471	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [PSH, ACK] Seq=4201 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832472	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=5601 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832473	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=7001 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832474	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=8401 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832475	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [PSH, ACK] Seq=9801 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832476	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [ACK] Seq=11201 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]
986...	1519.832476	142.250.81.228	10.188.204.9	TCP	1466	80 → 55257 [PSH, ACK] Seq=12601 Ack=79 Win=65536 Len=1400 TSval=2909164315 TSecr=1124747590 [TCP segment]

- Source IP
 - 142.250.81.228
- Destination IP
 - 10.188.204.9
- Protocol
 - TCP
- Port
 - Source
 - 80

- Destination
 - 55257

WGET

168...	1717.057485	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22775610 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057485	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22777058 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057485	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22778506 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057486	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22779954 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057486	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22781402 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057486	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22782850 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057487	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22784298 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057487	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22785746 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057487	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22787194 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057488	198.143.164.252	10.188.204.9	TCP	1514	443 → 55300	[ACK] Seq=22788642 Ack=648 Win=31232 Len=1448 TSval=156100017 TSecr=767269385 [TCP segment of a reassembled PDU]
168...	1717.057488	198.143.164.252	10.188.204.9	TLSv1...	1514	Application Data	[TCP segment of a reassembled PDU]

- Source IP
 - 198.143.164.252
- Destination IP
 - 10.188.204.9
- Protocol
 - TCP
- Port
 - Source
 - 443
 - Destination
 - 55300

TCP 3-way Handshake

1	0.000000	192.168.1.104	216.18.166.136	TCP	74	49859 → 80	[SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 TSval=305762 TSecr=0
2	0.307187	216.18.166.136	192.168.1.104	TCP	74	80 → 49859	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1440 TSval=1315092752 TSecr=305762 WS=512
3	0.307372	192.168.1.104	216.18.166.136	TCP	66	49859 → 80	[ACK] Seq=1 Ack=1 Win=17136 Len=0 TSval=305793 TSecr=1315092752

- Source IP
 - 192.168.1.104
- Destination IP
 - 216.18.166.136
- Protocol
 - TCP
- Port
 - Source
 - 49859
 - Destination
 - 80

HTTP

12	0.333000	192.168.1.2	192.168.1.1	TCP	1314	HTTP/1.1 200 OK	[TCP segment of a reassembled PDU]
13	0.933001	192.168.1.1	192.168.1.2	HTTP	365	[TCP Spurious Retransmission] GET http://www.ups.com/ HTTP/1.1	

Note: For this, I could only find an example from [CloudShark](#)

- Source IP
 - 192.168.1.2
- Destination IP
 - 192.168.1.1
- Protocol
 - TCP & HTTP
- Port
 - Source
 - 50683
 - Destination
 - 80

HTTPS

3	0.000298760	127.0.0.1	127.0.0.1	TCP	74	60883 → 443 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=78771939 TSecr=0 WS=128
4	0.000332608	127.0.0.1	127.0.0.1	TCP	74	443 → 60883 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=78771939 TSecr=...
5	0.000367861	127.0.0.1	127.0.0.1	TCP	66	60883 → 443 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=78771939 TSecr=78771939

- Source IP
 - 127.0.0.1
- Destination IP
 - 127.0.0.1
- Protocol
 - TCP
- Port
 - Source
 - 60883
 - Destination
 - 443