

Bilkent University
CS 479

Network Analysis

Emre Yüce, PhD
HAVELSAN

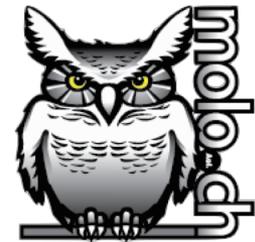
Ankara, February 19

Packet Capture

- Intercepting data packets that is crossing over a specific computer network.
- Data packets can be stored temporarily or permanently for analysis.
- Network cards that support monitor/promiscuous mode is required.

Packet Capture

- Wireshark
- Moloch
- Tshark
- Tcpdump
- Ethereal
- Microsoft Network Monitor



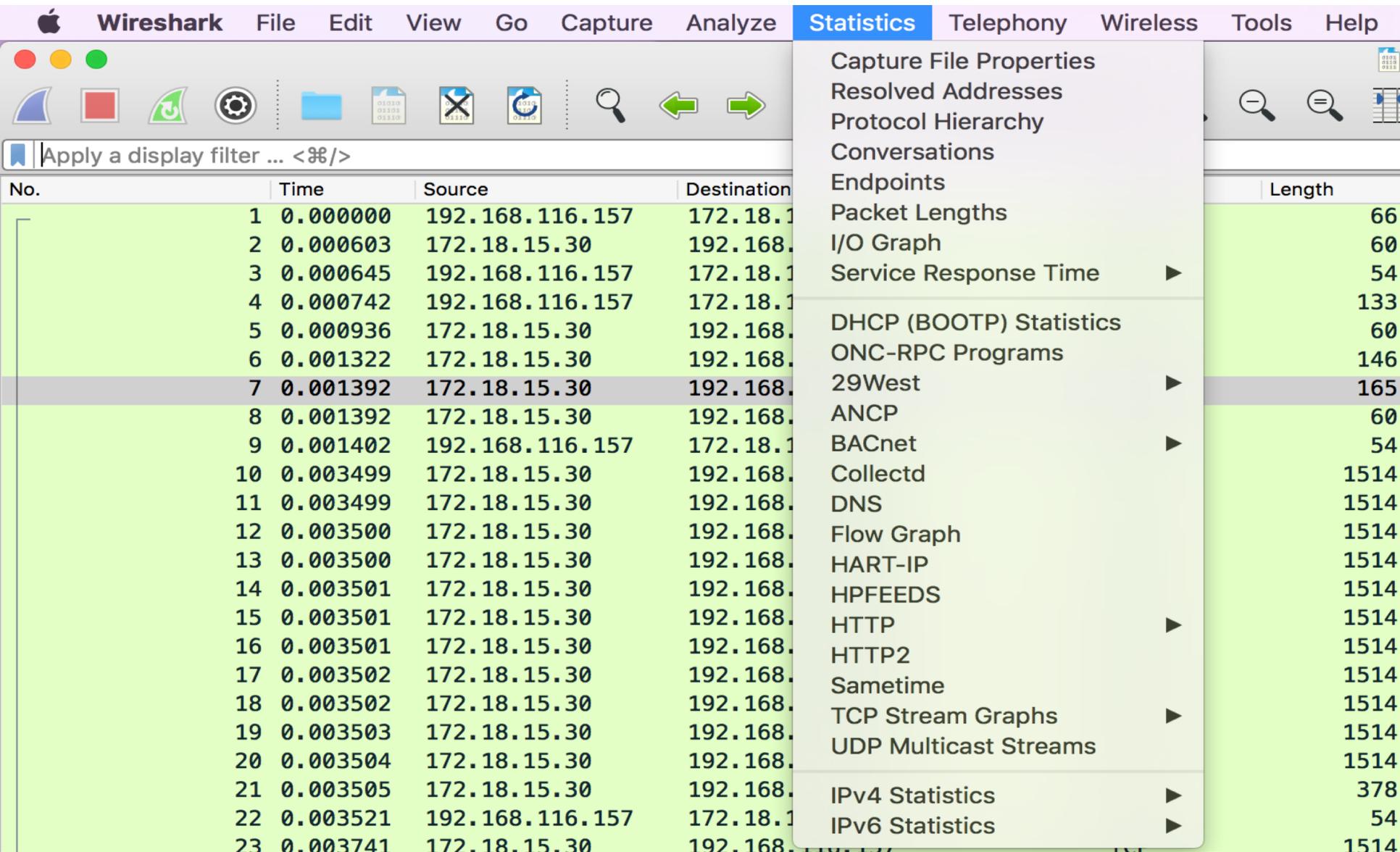
Wireshark

The image shows the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, navigation, and search. Below the toolbar is a filter bar with the text "Apply a display filter ... $\%$". The main display area is a packet list table with columns for No., Time, Source, Destination, Protocol, Length, and Info. The table shows 30 packets. Packet 7 is highlighted in grey and is a TCP segment of a reassembled PDU. Packet 8 is also highlighted in grey and is a TCP segment of a reassembled PDU. Packet 9 is a TCP segment of a reassembled PDU. Packet 10 is a TCP segment of a reassembled PDU. Packet 11 is a TCP segment of a reassembled PDU. Packet 12 is a TCP segment of a reassembled PDU. Packet 13 is a TCP segment of a reassembled PDU. Packet 14 is a TCP segment of a reassembled PDU. Packet 15 is a TCP segment of a reassembled PDU. Packet 16 is a TCP segment of a reassembled PDU. Packet 17 is a TCP segment of a reassembled PDU. Packet 18 is a TCP segment of a reassembled PDU. Packet 19 is a TCP segment of a reassembled PDU. Packet 20 is a TCP segment of a reassembled PDU. Packet 21 is a TCP segment of a reassembled PDU. Packet 22 is a TCP segment of a reassembled PDU. Packet 23 is a TCP segment of a reassembled PDU. Packet 24 is a TCP segment of a reassembled PDU. Packet 25 is a TCP segment of a reassembled PDU. Packet 26 is a TCP segment of a reassembled PDU. Packet 27 is a TCP segment of a reassembled PDU. Packet 28 is a TCP segment of a reassembled PDU. Packet 29 is a TCP segment of a reassembled PDU. Packet 30 is a TCP segment of a reassembled PDU. Below the packet list is a packet details pane showing the structure of the selected packet (Frame 7). The details pane shows the following structure: Ethernet II, Src: Vmware_fc:4c:1e (00:50:56:fc:4c:1e), Dst: Vmware_be:31:e0 (00:0c:29:be:31:e0), Internet Protocol Version 4, Src: 172.18.15.30, Dst: 192.168.116.157, Transmission Control Protocol, Src Port: 80 (80), Dst Port: 58453 (58453), Seq: 93, Ack: 80, Len: 111. The bottom status bar shows "Packets: 8380 · Displayed: 8380 (100.0%) · Load time: 0:0.290" and "Profile: Default".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.116.157	172.18.15.30	TCP	66	58453 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000603	172.18.15.30	192.168.116.157	TCP	60	80 → 58453 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000645	192.168.116.157	172.18.15.30	TCP	54	58453 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.000742	192.168.116.157	172.18.15.30	HTTP	133	GET /milla.exe HTTP/1.0
5	0.000936	172.18.15.30	192.168.116.157	TCP	60	80 → 58453 [ACK] Seq=1 Ack=80 Win=64240 Len=0
6	0.001322	172.18.15.30	192.168.116.157	TCP	146	[TCP segment of a reassembled PDU]
7	0.001392	172.18.15.30	192.168.116.157	TCP	165	[TCP segment of a reassembled PDU]
8	0.001392	172.18.15.30	192.168.116.157	TCP	60	[TCP segment of a reassembled PDU]
9	0.001402	192.168.116.157	172.18.15.30	TCP	54	58453 → 80 [ACK] Seq=80 Ack=206 Win=64035 Len=0
10	0.003499	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
11	0.003499	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
12	0.003500	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
13	0.003500	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
14	0.003501	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
15	0.003501	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
16	0.003501	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
17	0.003502	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
18	0.003502	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
19	0.003503	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
20	0.003504	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
21	0.003505	172.18.15.30	192.168.116.157	TCP	378	[TCP segment of a reassembled PDU]
22	0.003521	192.168.116.157	172.18.15.30	TCP	54	58453 → 80 [ACK] Seq=80 Ack=16590 Win=56616 Len=0
23	0.003741	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
24	0.003741	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
25	0.003742	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
26	0.003742	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
27	0.003743	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
28	0.003743	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
29	0.003743	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]
30	0.003744	172.18.15.30	192.168.116.157	TCP	1514	[TCP segment of a reassembled PDU]

▶ Frame 7: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface 0
▶ Ethernet II, Src: Vmware_fc:4c:1e (00:50:56:fc:4c:1e), Dst: Vmware_be:31:e0 (00:0c:29:be:31:e0)
▶ Internet Protocol Version 4, Src: 172.18.15.30, Dst: 192.168.116.157
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 58453 (58453), Seq: 93, Ack: 80, Len: 111

Statistics



The image shows the Wireshark application interface. The 'Statistics' menu is open, displaying a list of statistical tools. The packet list pane on the left shows 23 captured packets with their respective times, source, and destination IP addresses.

Wireshark Statistics Menu:

- Capture File Properties
- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time ▶
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 29West ▶
- ANCP
- BACnet ▶
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP ▶
- HTTP2
- Sametime
- TCP Stream Graphs ▶
- UDP Multicast Streams
- IPv4 Statistics ▶
- IPv6 Statistics ▶

Packet List:

No.	Time	Source	Destination
1	0.000000	192.168.116.157	172.18.15.30
2	0.000603	172.18.15.30	192.168.116.157
3	0.000645	192.168.116.157	172.18.15.30
4	0.000742	192.168.116.157	172.18.15.30
5	0.000936	172.18.15.30	192.168.116.157
6	0.001322	172.18.15.30	192.168.116.157
7	0.001392	172.18.15.30	192.168.116.157
8	0.001392	172.18.15.30	192.168.116.157
9	0.001402	192.168.116.157	172.18.15.30
10	0.003499	172.18.15.30	192.168.116.157
11	0.003499	172.18.15.30	192.168.116.157
12	0.003500	172.18.15.30	192.168.116.157
13	0.003500	172.18.15.30	192.168.116.157
14	0.003501	172.18.15.30	192.168.116.157
15	0.003501	172.18.15.30	192.168.116.157
16	0.003501	172.18.15.30	192.168.116.157
17	0.003502	172.18.15.30	192.168.116.157
18	0.003502	172.18.15.30	192.168.116.157
19	0.003503	172.18.15.30	192.168.116.157
20	0.003504	172.18.15.30	192.168.116.157
21	0.003505	172.18.15.30	192.168.116.157
22	0.003521	192.168.116.157	172.18.15.30
23	0.003741	172.18.15.30	192.168.116.157

Protocol Hierarchy

Wireshark · Protocol Hierarchy Statistics · natosunum

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	8380	100.0	9801601	544 k	0	0	0
▼ Ethernet	100.0	8380	100.0	9801601	544 k	0	0	0
▼ Internet Protocol Version 4	90.9	7619	99.7	9769495	543 k	0	0	0
▼ User Datagram Protocol	0.3	25	0.0	3102	172	0	0	0
NetBIOS Name Service	0.2	19	0.0	2090	116	19	2090	116
Multicast Domain Name System	0.0	4	0.0	328	18	4	328	18
Bootstrap Protocol	0.0	2	0.0	684	38	2	684	38
▼ Transmission Control Protocol	90.6	7594	99.6	9766393	542 k	7488	9728950	540 k
SSH Protocol	1.3	105	0.4	37310	2074	105	37310	2074
Hypertext Transfer Protocol	0.0	1	0.0	133	7	1	133	7
Address Resolution Protocol	9.1	761	0.3	32106	1784	761	32106	1784

Endpoints

Wireshark · Endpoints · natosunum

UDP · 6 Ethernet · 7 IPv4 · 7 IPv6 TCP · 236

Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Latitude	Longitude
172.18.15.30	7,187	9710 k	6601	9670 k	586	40 k	-	-
192.168.116.1	66	4204	35	2194	31	2010	-	-
192.168.116.2	75	5618	28	1680	47	3938	-	-
192.168.116.145	263	47 k	136	31 k	127	16 k	-	-
192.168.116.157	7,613	9768 k	818	63 k	6795	9704 k	-	-
192.168.116.254	30	2532	1	342	29	2190	-	-
224.0.0.251	4	328	0	0	4	328	-	-

Conversations

Wireshark · Conversations · natosunum

Ethernet · 7 IPv4 · 7 IPv6 TCP · 122 UDP · 3

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
192.168.116.157	58453	172.18.15.30		80	7,174		9701 k	581	31 k	6593	9669 k	0.000000000	0.123720	2034 k	625 M
192.168.116.157	49191	192.168.116.145		22	43		12 k	19	2399	24	10 k	116.641994000	11.577272	1657	7120
192.168.116.157	49189	192.168.116.145		22	23		4429	11	1691	12	2738	112.789231000	15.599484	867	1404
192.168.116.157	49190	192.168.116.145		22	23		4429	11	1691	12	2738	114.755382000	13.571744	996	1613
192.168.116.157	49192	192.168.116.145		22	23		4429	11	1691	12	2738	116.981125000	11.189194	1209	1957
192.168.116.157	49195	192.168.116.145		22	23		4429	11	1691	12	2738	123.616123000	4.289565	3153	5106
192.168.116.157	49193	192.168.116.145		22	22		4283	11	1679	11	2604	118.794746000	9.313576	1442	2236
192.168.116.157	49194	192.168.116.145		22	22		4283	11	1679	11	2604	120.901476000	7.097218	1892	2935
192.168.116.157	49196	192.168.116.145		22	21		4229	10	1625	11	2604	125.736207000	2.153909	6035	9671
192.168.116.157	49197	172.18.15.30	8080		13	9059		5	8579	8	480	128.393120000	0.002059	N/A	N/A
192.168.116.157	58457	192.168.116.1		80	8		474	4	228	4	246	1.014242000	0.002291	N/A	N/A
192.168.116.157	62487	192.168.116.145		22	7		440	4	228	3	212	64.022341000	0.009217	197 k	184 k
192.168.116.157	58454	192.168.116.1		21	2		126	1	66	1	60	0.970715000	0.000174	N/A	N/A
192.168.116.157	58455	192.168.116.1		22	2		126	1	66	1	60	0.982251000	0.000140	N/A	N/A
192.168.116.157	58456	192.168.116.1		23	2		126	1	66	1	60	0.997550000	0.000291	N/A	N/A
192.168.116.157	58458	192.168.116.1		443	2		126	1	66	1	60	1.016441000	0.000079	N/A	N/A
192.168.116.157	58459	192.168.116.1		502	2		126	1	66	1	60	1.028637000	0.000173	N/A	N/A
192.168.116.157	58460	192.168.116.1	3306		2		126	1	66	1	60	1.044821000	0.000161	N/A	N/A
192.168.116.157	58461	192.168.116.1		25	2		126	1	66	1	60	1.060295000	0.000158	N/A	N/A
192.168.116.157	58462	192.168.116.1		567	2		126	1	66	1	60	1.075925000	0.000161	N/A	N/A
192.168.116.157	58463	192.168.116.1		333	2		126	1	66	1	60	1.091946000	0.000316	N/A	N/A
192.168.116.157	58464	192.168.116.1		444	2	126		1	66	1	60	1.107266000	0.000167	N/A	N/A
192.168.116.157	58465	192.168.116.1		555	2	126		1	66	1	60	1.122500000	0.000200	N/A	N/A
192.168.116.157	58466	192.168.116.1		666	2	126		1	66	1	60	1.138050000	0.000158	N/A	N/A
192.168.116.157	58467	192.168.116.1		777	2	126		1	66	1	60	1.153978000	0.000159	N/A	N/A
192.168.116.157	58468	192.168.116.1		8889	2	126		1	66	1	60	1.169386000	0.000138	N/A	N/A
192.168.116.157	58469	192.168.116.1		999	2	126		1	66	1	60	1.184671000	0.000160	N/A	N/A
192.168.116.157	58470	192.168.116.1		366	2	126		1	66	1	60	1.200791000	0.000190	N/A	N/A
192.168.116.157	58471	192.168.116.1		3389	2	126		1	66	1	60	1.216602000	0.000169	N/A	N/A
192.168.116.157	58472	192.168.116.1		8080	2	126		1	66	1	60	1.232318000	0.000164	N/A	N/A
192.168.116.157	58473	192.168.116.1		8081	2	126		1	66	1	60	1.247118000	0.000155	N/A	N/A

Name resolution Limit to display filter

Conversation Types ▾

Help Copy ▾ Follow Stream... Graph...

Close

What do we have?

- Protocols: DNS, HTTP, SSH
- Ports: UDP/53, TCP/22, TCP/80, TCP/8080
- IP Addresses:
 - 172.18.10.41
 - 172.18.10.47
 - 192.168.116.1
 - 192.168.116.2
 - 192.168.116.157 (Victim IP)
 - 192.168.116.158

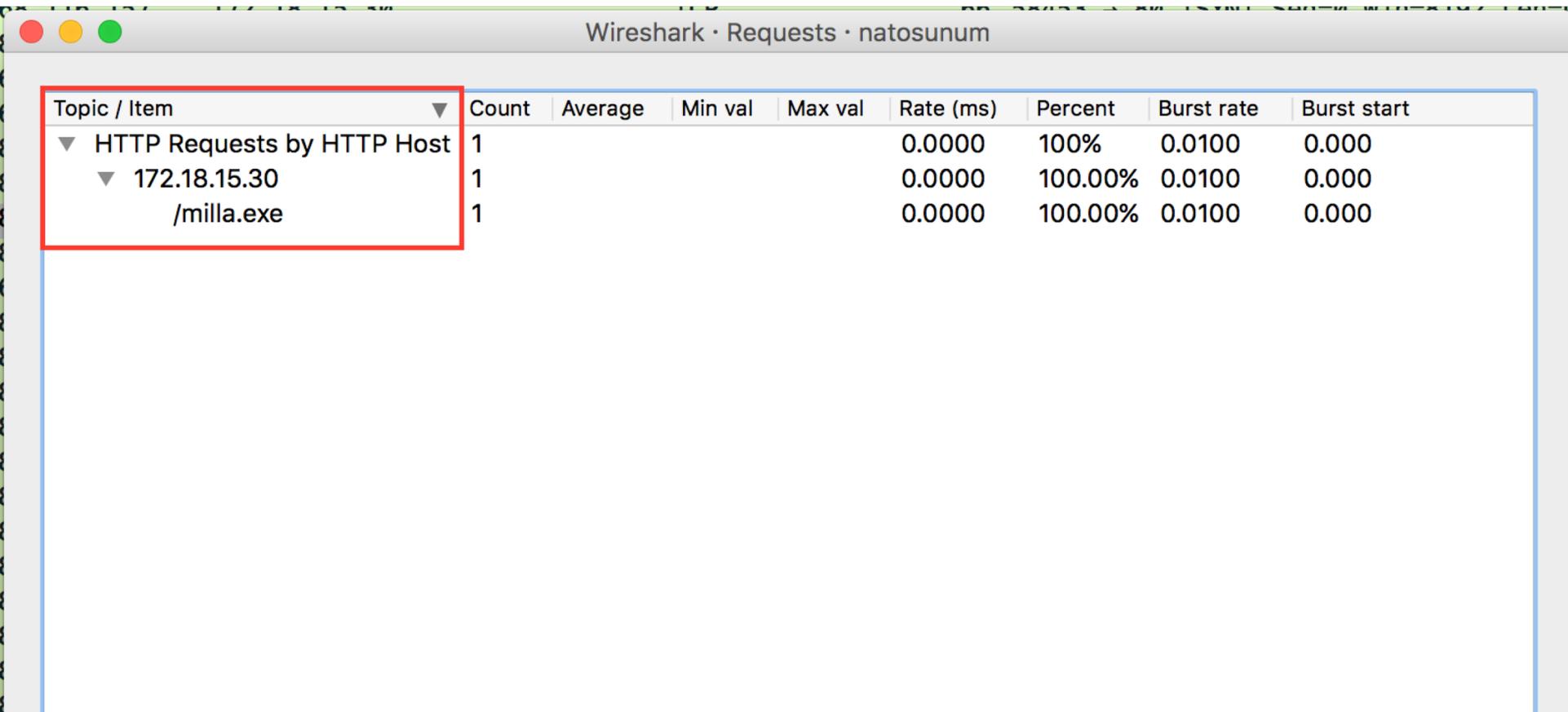
DNS Requests

natosunum_wdns.pcapng

dns

No.	Time	Source	Destination	Protocol	Length	Info
2	1.141351	192.168.116.157	172.18.10.47	DNS	96	Standard query 0x6eee A 71b9b5bc1094ee6eaaee8253e787d654.com
3	1.320916	172.18.10.47	192.168.116.157	DNS	169	Standard query response 0x6eee No such name A 71b9b5bc1094ee6eaaee8253e787d654.com SOA a.gtld-servers.net
4	1.322581	192.168.116.157	172.18.10.47	DNS	96	Standard query 0x16fd A 935d52cde2333a37323bb72ad1841039.com
5	1.517334	172.18.10.47	192.168.116.157	DNS	169	Standard query response 0x16fd No such name A 935d52cde2333a37323bb72ad1841039.com SOA a.gtld-servers.net
6	1.517994	192.168.116.157	172.18.10.47	DNS	96	Standard query 0xc0ee A 6b4f5edb7a0bacde6e1ab303e45b759a.com
7	1.518726	172.18.10.47	192.168.116.157	DNS	163	Standard query response 0xc0ee A 6b4f5edb7a0bacde6e1ab303e45b759a.com A 172.18.10.41 NS ns.16b4f5edb7a0bacde6e1ab303e45b759a.com
8	1.520457	192.168.116.157	172.18.10.47	DNS	96	Standard query 0x0d6e A 4e39298ce8bb79e5243616f7e09aae28.com
9	1.684518	172.18.10.47	192.168.116.157	DNS	169	Standard query response 0x0d6e No such name A 4e39298ce8bb79e5243616f7e09aae28.com SOA a.gtld-servers.net

HTTP Requests



The image shows a Wireshark window titled "Wireshark · Requests · natosunum". The main content is a table of statistics for HTTP requests. A red box highlights the first three rows of the table, which are expanded to show details for the host 172.18.15.30.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ HTTP Requests by HTTP Host	1				0.0000	100%	0.0100	0.000
▼ 172.18.15.30	1				0.0000	100.00%	0.0100	0.000
/milla.exe	1				0.0000	100.00%	0.0100	0.000

TCP Streams

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets from a file named 'natosunum.pcapng'. The packets are organized into TCP streams. A context menu is open over packet 8379, showing options like 'Follow', 'Copy', and 'Protocol Preferences'. The 'Follow' option is selected, and a sub-menu is visible with 'TCP Stream' as the active choice.

No.	Time	Source	Destination	Protocol	Length	Info
7219	1.232318	192.168.116.157	192.168.116.1	TCP	66	58472 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7220	1.232482	192.168.116.1	192.168.116.157	TCP	60	8080 → 58472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7275	1.715626	192.168.116.157	192.168.116.2	TCP	66	58500 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7276	1.716062	192.168.116.2	192.168.116.157	TCP	60	8080 → 58500 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
7787	64.271922	192.168.116.157	192.168.116.145	TCP	66	62504 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7788	64.272417	192.168.116.145	192.168.116.157	TCP	60	8080 → 62504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8151	112.6318...	192.168.116.157	192.168.116.254	TCP	60	8080 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8367	128.3931...	192.168.116.157	172.18.15.30	TCP	60	8080 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8368	128.3936...	172.18.15.30	192.168.116.157	TCP	60	49197 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
8369	128.3936...	192.168.116.157	172.18.15.30	TCP	60	8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8370	128.3937...	192.168.116.157	172.18.15.30	TCP	60	8080 [ACK] Seq=1 Ack=1 Win=64240 Len=2920
8371	128.3940...	172.18.15.30	192.168.116.157	TCP	60	49197 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
8372	128.3940...	172.18.15.30	192.168.116.157	TCP	60	49197 [ACK] Seq=1 Ack=2921 Win=64240 Len=0
8373	128.3940...	192.168.116.157	172.18.15.30	TCP	60	8080 [FIN, PSH, ACK] Seq=2921 Ack=1 Win=64240 Len=5377
8374	128.3942...	172.18.15.30	192.168.116.157	TCP	60	49197 [ACK] Seq=1 Ack=4381 Win=64240 Len=0
8375	128.3942...	172.18.15.30	192.168.116.157	TCP	60	49197 [ACK] Seq=1 Ack=5841 Win=64240 Len=0
8376	128.3942...	172.18.15.30	192.168.116.157	TCP	60	49197 [ACK] Seq=1 Ack=7301 Win=64240 Len=0
8377	128.3942...	172.18.15.30	192.168.116.157	TCP	60	49197 [ACK] Seq=1 Ack=8299 Win=64239 Len=0
8378	128.3951...	172.18.15.30	192.168.116.157	TCP	60	49197 [FIN, PSH, ACK] Seq=1 Ack=8299 Win=64239 Len=0
8379	128.3951...	192.168.116.157	172.18.15.30	TCP	60	8299 Ack=2 Win=64240 Len=0

TCP Streams

Wireshark · Follow TCP Stream (tcp.stream eq 0) · natosunum

```
GET /milla.exe HTTP/1.0
Host: 172.18.15.30
User-Agent: Python-urllib/1.17

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.10
Date: Mon, 07 Nov 2016 14:30:39 GMT
Content-type: application/x-msdownload
Content-Length: 9312483
Last-Modified: Mon, 07 Nov 2016 14:30:21 GMT

MZ.....@.....!.L!This program cannot be run in DOS mode.

$.PE..d.
/.....@.....0....._.....
D.....8.....0..
(.text.....P`.data.....@.P..rda
ta..P..P.....@`@.pdata.....@.0@.xdata..l..P`.data.....@.0@.bss.....
0.....p_idata.D.....@.0..CRT.....h.....@.0..tls.....h....
0.....e.`.rsrc..8.....@.....@.....
0.....
.....fffff.....H..(H.....
1.....H.....H.....H..\.H.....f.8MztxH..
1.....tW.....H.....H..X..H..H..>..H..H.....H.....H..*...8.te1.H..(.....f.Hch<H...
8PE...u...H.f...tEf..._.....R.....1.....@.....H..
).....1.H..(.xt.....D.....1.E.....fffff.....H..8H.....D..L.....H.....H..
...x...H..q...H.D$ H...D...g...H..8.f.AUATUVSH...H.5...1..
...H.T$ D..H..H.E.....eH..%0...H...H.X.1.L.%...H9...M.....A..H..H.;H..u.H.=...
1.....;.....1.....J...H.....H..H..t.E1.....1.....H..
...w...H.....H.....H..
a.....H.....H.....H.....H..H..t^1.....A..A...f.."A.D.H.....f..
w.f.t...t.....f..w.f.....H.....S.f..v.H.....D..E..t..D$\..
.....D..%..E.l$Mc.I..L.....E..H..H.=...i..1.H..f.:.....A.....I...fB.|
B..u.K..H...H.D.H...I..H..H..g...A9...I...J.D-...H..-F...Q~..H..z..H..+...
5...H..H..L.....H.....
.....u..9.....H.....[^_]A\A].....R.....D$`.....H..='.....H..t...H..
].....1.H.....H.....&...H..[...H..
D.....a...m...E1.....@.H..(H.....Z].....H..(.fffff.....H..(H..e.....*)...u.....H..
(.....UH..]f.....UH..H..H.=0...t0H..
.....H..t/H.....H.....H..t...H..
.....H..
]...{...H.....@.UH..].....SH..H..t...H..H..X..H..H.....[9...H..H..[.....WVSH..E1.H..H...X.
0...uDH.s L..A.....X...H..H..t%H.=...H..[^].....H..[^]...VSH..(H..H...
.....H..H;F.s.H..
.....H.F.H..([.f.....ATUVSH..H.9.H..H...))...s..0.H.-...H.....E1..a...0.....
5...H..H..D..L.#.0...A.....H..M..>...H...
.....t'H..H..t..J..H.....H..H..[.]A\A]...D...i...0.....H..I.....0..H.D$P...H.D$X...H.D$`...H.t$ ...0..D$(L.d$0..H.l$
H...A.X...D$8H@.....H..A.A.....H..L..b...6..H.IxH.R.....H..H.....H..
```

1 client pkt(s), 6,590 server pkt(s), 1 turn.

Entire conversation (9312 kB) Show data as ASCII Stream 0

Find: Find Next

Help Hide this stream Print Save as... Close

Detecting Ping Sweep

7295	1.871626	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.3? Tell 192.168.116.157
7296	2.324593	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.4? Tell 192.168.116.157
7297	2.650775	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.3? Tell 192.168.116.157
7298	2.761662	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.5? Tell 192.168.116.157
7299	3.149267	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.4? Tell 192.168.116.157
7300	3.197600	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.6? Tell 192.168.116.157
7301	3.634258	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.7? Tell 192.168.116.157
7302	3.664352	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.3? Tell 192.168.116.157
7303	3.664491	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.5? Tell 192.168.116.157
7304	4.071352	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.8? Tell 192.168.116.157
7305	4.164220	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.4? Tell 192.168.116.157
7306	4.164380	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.6? Tell 192.168.116.157
7307	4.164449	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.7? Tell 192.168.116.157
7308	4.507659	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.9? Tell 192.168.116.157
7309	4.663729	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.5? Tell 192.168.116.157
7310	4.663897	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.8? Tell 192.168.116.157
7311	4.944972	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.10? Tell 192.168.116.157
7312	5.162940	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.6? Tell 192.168.116.157
7313	5.163150	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.7? Tell 192.168.116.157
7314	5.163220	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.9? Tell 192.168.116.157
7315	5.389569	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.11? Tell 192.168.116.157
7316	5.661695	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.8? Tell 192.168.116.157
7317	5.661886	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.10? Tell 192.168.116.157
7318	5.819192	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.12? Tell 192.168.116.157
7319	6.161368	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.9? Tell 192.168.116.157
7320	6.161579	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.11? Tell 192.168.116.157
7321	6.255391	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.13? Tell 192.168.116.157
7322	6.660538	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.10? Tell 192.168.116.157
7323	6.660751	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.12? Tell 192.168.116.157

- ▶ Frame 7177: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- ▶ Ethernet II, Src: Vmware_be:31:e0 (00:0c:29:be:31:e0), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
- ▶ Internet Protocol Version 4, Src: 192.168.116.157, Dst: 192.168.116.1
- ▶ Transmission Control Protocol, Src Port: 58454 (58454), Dst Port: 21 (21), Seq: 0, Len: 0

Detecting Port Scan

No.	Time	Source	Destination	Protocol	Length	Info
7175	0.970576	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.1? Tell 192.168.116.157
7176	0.970708	00:50:56:c0:00:08	00:0c:29:be:31:e0	ARP	60	192.168.116.1 is at 00:50:56:c0:00:08
7177	0.970715	192.168.116.157	192.168.116.1	TCP	66	58454 → 21 [YN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7178	0.970889	192.168.116.1	192.168.116.157	TCP	60	21 → 58454 [ST, ACK] Seq=1 Ack=1 Win=0 Len=0
7179	0.982251	192.168.116.157	192.168.116.1	TCP	66	58455 → 22 [YN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7180	0.982391	192.168.116.1	192.168.116.157	TCP	60	22 → 58455 [ST, ACK] Seq=1 Ack=1 Win=0 Len=0
7181	0.997550	192.168.116.157	192.168.116.1	TCP	66	58456 → 23 [YN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7182	0.997841	192.168.116.1	192.168.116.157	TCP	60	23 → 58456 [ST, ACK] Seq=1 Ack=1 Win=0 Len=0
7183	1.014242	192.168.116.157	192.168.116.1	TCP	66	58457 → 80 [YN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7184	1.015829	192.168.116.1	192.168.116.157	TCP	66	80 → 58457 [YN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 SACK_PERM=1
7185	1.015845	192.168.116.157	192.168.116.1	TCP	54	58457 → 80 [CK] Seq=1 Ack=1 Win=65536 Len=0
7186	1.015972	192.168.116.1	192.168.116.157	TCP	60	[TCP Window update] 80 → 58457 [ACK] Seq=1 Ack=1 Win=262144 Len=0
7187	1.016281	192.168.116.157	192.168.116.1	TCP	54	58457 → 80 [IN, ACK] Seq=1 Ack=1 Win=65536 Len=0
7188	1.016441	192.168.116.157	192.168.116.1	TCP	66	58458 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7189	1.016519	192.168.116.1	192.168.116.157	TCP	60	80 → 58457 [CK] Seq=1 Ack=2 Win=262144 Len=0
7190	1.016520	192.168.116.1	192.168.116.157	TCP	60	80 → 58457 [IN, ACK] Seq=1 Ack=2 Win=262144 Len=0
7191	1.016520	192.168.116.1	192.168.116.157	TCP	60	443 → 58458 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7192	1.016533	192.168.116.157	192.168.116.1	TCP	54	58457 → 80 [CK] Seq=2 Ack=2 Win=65536 Len=0
7193	1.028637	192.168.116.157	192.168.116.1	TCP	66	58459 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7194	1.028810	192.168.116.1	192.168.116.157	TCP	60	502 → 58459 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7195	1.044821	192.168.116.157	192.168.116.1	TCP	66	58460 → 3306 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7196	1.044982	192.168.116.1	192.168.116.157	TCP	60	3306 → 58460 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7197	1.060295	192.168.116.157	192.168.116.1	TCP	66	58461 → 25 [YN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7198	1.060453	192.168.116.1	192.168.116.157	TCP	60	25 → 58461 [ST, ACK] Seq=1 Ack=1 Win=0 Len=0
7199	1.075925	192.168.116.157	192.168.116.1	TCP	66	58462 → 567 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7200	1.076086	192.168.116.1	192.168.116.157	TCP	60	567 → 58462 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7201	1.091946	192.168.116.157	192.168.116.1	TCP	66	58463 → 333 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7202	1.092262	192.168.116.1	192.168.116.157	TCP	60	333 → 58463 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7203	1.107266	192.168.116.157	192.168.116.1	TCP	66	58464 → 444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7204	1.107433	192.168.116.1	192.168.116.157	TCP	60	444 → 58464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

▶ Frame 7177: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: Vmware_be:31:e0 (00:0c:29:be:31:e0), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
▶ Internet Protocol Version 4, Src: 192.168.116.157, Dst: 192.168.116.1
▶ Transmission Control Protocol, Src Port: 58454 (58454), Dst Port: 21 (21), Seq: 0, Len: 0

Detecting SSH Brute Force

The image shows a Wireshark capture of network traffic on port 22. The filter is set to 'tcp.port == 22'. The capture shows a sequence of events where a client attempts to connect to a server. The server responds with a SYN-ACK, but the client sends a RST (Reset) packet, indicating a failed connection attempt. This is highlighted with a red box. The client then sends a SYN packet, and the server responds with a SYN-ACK. The client then sends a packet with the SSH protocol identifier, and the server responds with a protocol mismatch message. This sequence is also highlighted with a red box. The capture ends with a TCP retransmission and an ACK packet.

No.	Time	Source	Destination	Protocol	Length	Info
7751	64.023941	192.168.116.145	192.168.116.157	TCP	60	22 → 62487 [ACK] Seq=1 Ack=7 Win=29312 Len=0
7753	64.031521	192.168.116.145	192.168.116.157	SSH	86	Server: Protocol (SSH-2.0-OpenSSH_7.1p2 Debian-2)
7754	64.031558	192.168.116.157	192.168.116.145	TCP	54	62487 → 22 [RST, ACK] Seq=2 Ack=33 Win=0 Len=0
8134	112.3510...	192.168.116.157	192.168.116.254	TCP	60	49162 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8163	112.7892...	192.168.116.157	192.168.116.145	TCP	60	49189 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8164	112.7897...	192.168.116.145	192.168.116.157	TCP	66	22 → 49189 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
8165	112.7897...	192.168.116.157	192.168.116.145	TCP	54	49189 → 22 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8166	112.7908...	192.168.116.157	192.168.116.145	SSHv2	79	Client: Protocol (SSH-2.0-paramiko_1.17.0)
8167	112.7914...	192.168.116.145	192.168.116.157	TCP	66	22 → 49189 [ACK] Seq=1 Ack=26 Win=29312 Len=0
8168	112.7973...	192.168.116.145	192.168.116.157	SSHv2	86	Server: Protocol (SSH-2.0-OpenSSH_7.1p2 Debian-2)
8169	112.8030...	192.168.116.157	192.168.116.145	SSHv2	654	Client: Key Exchange Init
8170	112.8035...	192.168.116.145	192.168.116.157	SSHv2	998	Server: Key Exchange Init
8171	112.8148...	192.168.116.157	192.168.116.145	SSHv2	326	Client: Diffie-Hellman Key Exchange Init
8172	112.8193...	192.168.116.145	192.168.116.157	SSHv2	902	Server: Diffie-Hellman Key Exchange Reply, New Keys
8173	112.8395...	192.168.116.157	192.168.116.145	SSHv2	70	Client: New Keys
8174	112.8789...	192.168.116.145	192.168.116.157	TCP	66	22 → 49189 [ACK] Seq=1825 Ack=914 Win=31616 Len=0
8175	112.8790...	192.168.116.157	192.168.116.145	SSHv2	118	Client: Encrypted packet (len=64)
8176	112.8793...	192.168.116.145	192.168.116.157	TCP	66	22 → 49189 [ACK] Seq=1825 Ack=978 Win=31616 Len=0
8177	112.8795...	192.168.116.145	192.168.116.157	SSHv2	118	Server: Encrypted packet (len=64)
8178	112.8800...	192.168.116.157	192.168.116.145	SSHv2	150	Client: Encrypted packet (len=96)
8179	112.9189...	192.168.116.145	192.168.116.157	TCP	60	22 → 49189 [ACK] Seq=1889 Ack=1074 Win=31616 Len=0
8182	114.7422...	192.168.116.145	192.168.116.157	SSHv2	134	Server: Encrypted packet (len=80)
8183	114.7553...	192.168.116.157	192.168.116.145	TCP	66	49190 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8184	114.7558...	192.168.116.145	192.168.116.157	TCP	66	22 → 49190 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
8185	114.7558...	192.168.116.157	192.168.116.145	TCP	54	
8186	114.7569...	192.168.116.157	192.168.116.145	SSHv2	79	Client: Protocol (SSH-2.0-paramiko_1.17.0)
8187	114.7571...	192.168.116.145	192.168.116.157	TCP	66	22 → 49190 [ACK] Seq=1 Ack=26 Win=29312 Len=0
8188	114.7630...	192.168.116.145	192.168.116.157	SSHv2	86	Server: Protocol (SSH-2.0-OpenSSH_7.1p2 Debian-2)
8189	114.7636...	192.168.116.157	192.168.116.145	SSHv2	654	Client: Key Exchange Init
8190	114.7638...	192.168.116.145	192.168.116.157	SSHv2	998	Server: Key Exchange Init
8191	114.7767...	192.168.116.157	192.168.116.145	SSHv2	326	Client: Diffie-Hellman Key Exchange Init
8192	114.7791...	192.168.116.145	192.168.116.157	SSHv2	902	Server: Diffie-Hellman Key Exchange Reply, New Keys
8193	114.7940...	192.168.116.157	192.168.116.145	SSHv2	70	Client: New Keys
8194	114.8350...	192.168.116.145	192.168.116.157	TCP	66	22 → 49190 [ACK] Seq=1825 Ack=914 Win=31616 Len=0
8195	114.8350...	192.168.116.157	192.168.116.145	SSHv2	118	Client: Encrypted packet (len=64)
8196	114.8354...	192.168.116.145	192.168.116.157	TCP	66	22 → 49190 [ACK] Seq=1825 Ack=978 Win=31616 Len=0
8197	114.8356...	192.168.116.145	192.168.116.157	SSHv2	118	Server: Encrypted packet (len=64)
8198	114.8360...	192.168.116.157	192.168.116.145	SSHv2	150	Client: Encrypted packet (len=96)
8199	114.8751...	192.168.116.145	192.168.116.157	TCP	60	
8200	114.9508...	192.168.116.145	192.168.116.157	TCP	134	[TCP Retransmission] 22 → 49189 [PSH, ACK] Seq=1889 Ack=1074 Win=31616 Len=80
8201	114.9509...	192.168.116.157	192.168.116.145	TCP	66	49189 → 22 [ACK] Seq=1074 Ack=1969 Win=65536 Len=0 SLE=1889 SRE=1969

Frame 7751: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
Ethernet II, Src: 00:0c:29:03:3a:da, Dst: 00:0c:29:be:31:e0
Internet Protocol Version 4, Src: 192.168.116.145, Dst: 192.168.116.157
Transmission Control Protocol, Src Port: 22 (22), Dst Port: 62487 (62487), Seq: 1, Ack: 2, Len: 0

Data Exfiltration

Wireshark · Follow TCP Stream (tcp.stream eq 121) · natosunum

```
Run Forest! Run!  
{09253D78-41AC-4BE9-ADE4-B81D00FBD1AA} interface found!  
Address: 192.168.116.157  
Network: 192.168.116.157  
[+] Connection to 192.168.116.1 port 80 succeeded!  
[+] Connection to 192.168.116.1 port 8080 succeeded!  
Run Forest! Run!  
{09253D78-41AC-4BE9-ADE4-B81D00FBD1AA} interface found!  
Address: 192.168.116.157  
Network: 192.168.116.157  
[+] Connection to 192.168.116.1 port 80 succeeded!  
[+] Connection to 192.168.116.145 port 22 succeeded!  
1 hosts found.  
192.168.116.145Authentication not successful! 192.168.116.145 root:password  
SSH auth error: Authentication failed.  
Authentication not successful! 192.168.116.145 root:123456a  
SSH auth error: Authentication failed.  
Authentication successful! 192.168.116.145 root:pass123  
Authentication not successful! 192.168.116.145 admin:password  
SSH auth error: Authentication failed.  
Authentication not successful! 192.168.116.145 admin:123456a  
SSH auth error: Authentication failed.  
Authentication not successful! 192.168.116.145 admin:pass123  
SSH auth error: Authentication failed.  
Authentication not successful! 192.168.116.145 admin:Pass12345  
SSH auth error: Authentication failed.  
Authentication not successful! 192.168.116.145 admin:12345!  
SSH auth error: Authentication failed.  
Dns resolv error: [Errno 11004] getaddrinfo failed  
Dns resolv error: [Errno 11004] getaddrinfo failed  
Dns resolv error: [Errno 11004] getaddrinfo failed  
Sending logs to master!172.18.15.30uid=0(root) gid=0(root) groups=0(root)  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.116.145 netmask 255.255.255.0 broadcast 192.168.116.255  
    inet6 fe80::20c:29ff:fe03:3ada prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:03:3a:da txqueuelen 1000 (Ethernet)  
    RX packets 328198 bytes 173010068 (164.9 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 603267 bytes 62444442 (59.5 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 0 (Local Loopback)  
    RX packets 17621 bytes 27268227 (26.0 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 17621 bytes 27268227 (26.0 MiB)
```

Packet 8370. 2 client pkt(s), 0 server pkt(s), 0 turns. Click to select.

Entire conversation (8297 bytes) Show data as ASCII Stream 121

Find: Find Next

Help Hide this stream Print Save as... Close

Data Exfiltration

Wireshark · Follow TCP Stream (tcp.stream eq 121) · natosunum

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:109:./var/run/dbus:/bin/false
mysql:x:106:110:MySQL Server,,:/nonexistent:/bin/false
avahi:x:107:111:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
miredo:x:108:65534:./var/run/miredo:/bin/false
ntp:x:109:112:./home/ntp:/bin/false
stunnel4:x:110:114:./var/run/stunnel4:/bin/false
uidd:x:111:115:./run/uidd:/bin/false
Debian-exim:x:112:116:./var/spool/exim4:/bin/false
statd:x:113:65534:./var/lib/nfs:/bin/false
arpwatch:x:114:119:ARP Watcher,,:/var/lib/arpwatch:/bin/sh
colord:x:115:122:colord colour management daemon,,:/var/lib/colord:/bin/false
epmd:x:116:123:./var/run/epmd:/bin/false
couchdb:x:117:124:CouchDB Administrator,,:/var/lib/couchdb:/bin/bash
dnsmasq:x:118:65534:dnsmasq,,:/var/lib/misc:/bin/false
geoclue:x:119:125:./var/lib/geoclue:/bin/false
pulse:x:120:126:PulseAudio daemon,,:/var/run/pulse:/bin/false
speech-dispatcher:x:121:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/sh
sshd:x:122:65534:./var/run/sshd:/usr/sbin/nologin
snmp:x:123:128:./var/lib/snmp:/usr/sbin/nologin
postgres:x:124:130:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
iodine:x:125:65534:./var/run/iodine:/bin/false
king-phisher:x:126:133:./var/lib/king-phisher:/bin/false
redsocks:x:127:134:./var/run/redsocks:/bin/false
rwho:x:128:65534:./var/spool/rwho:/bin/false
sshd:x:129:135:./nonexistent:/bin/false
rtkit:x:130:136:RealtimeKit,,:/proc:/bin/false
saned:x:131:137:./var/lib/saned:/bin/false
usbmux:x:132:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
Debian-gdm:x:133:139:Gnome Display Manager:/var/lib/gdm3:/bin/false
beef-xss:x:134:140:./var/lib/beef-xss:/bin/false
dradis:x:135:141:./var/lib/dradis:/bin/false
root:$6$0QcGllD0$HpqfdDCV.mCmx.1LubXdqIkj1WYDwE1qGinAaoc1JS0FXDPhJTqg.6hzrqW8y1uTxbnxv8F2Lr7vBW7a0LC430:17112:0:99999:7:::
daemon:*.16820:0:99999:7:::
bin:*.16820:0:99999:7:::
sys:*.16820:0:99999:7:::
sync:*.16820:0:99999:7:::
```

Packet 8373. 2 client pkt(s), 0 server pkt(s), 0 turns. Click to select.

Entire conversation (8297 bytes) Show data as ASCII Stream 121

Find: Find Next

Help Hide this stream Print Save as... Close

EOF