Bilkent University
CS 479

Network Analysis

Emre Yüce, PhD
HAVELSAN

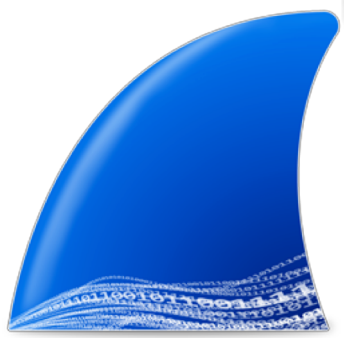
Ankara, February 19

Packet Capture

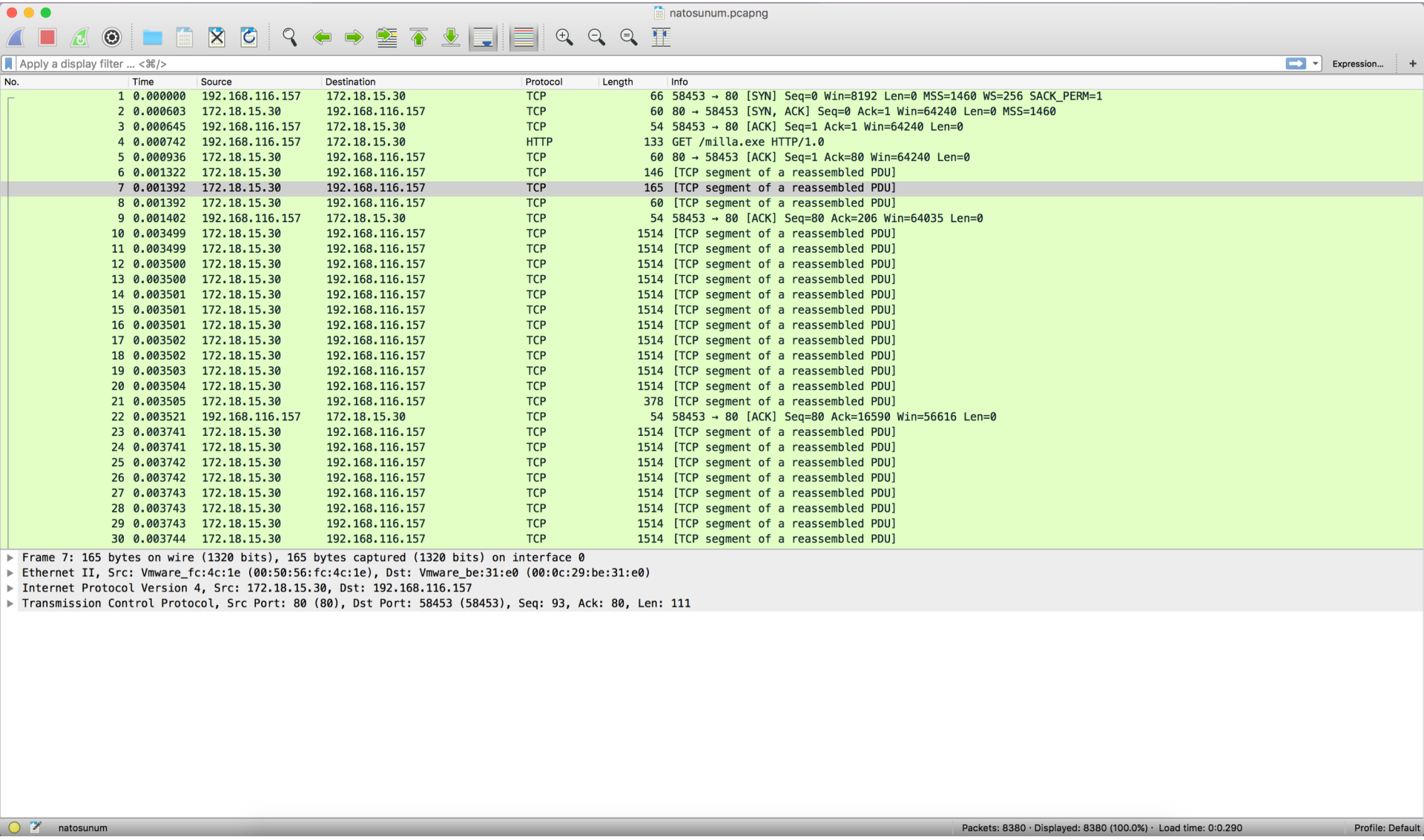
- Intercepting data packets that is crossing over a specific computer network.
- Data packets can be stored temporarily or permanently for analysis.
- Network cards that support monitor/promiscuous mode is required.

Packet Capture

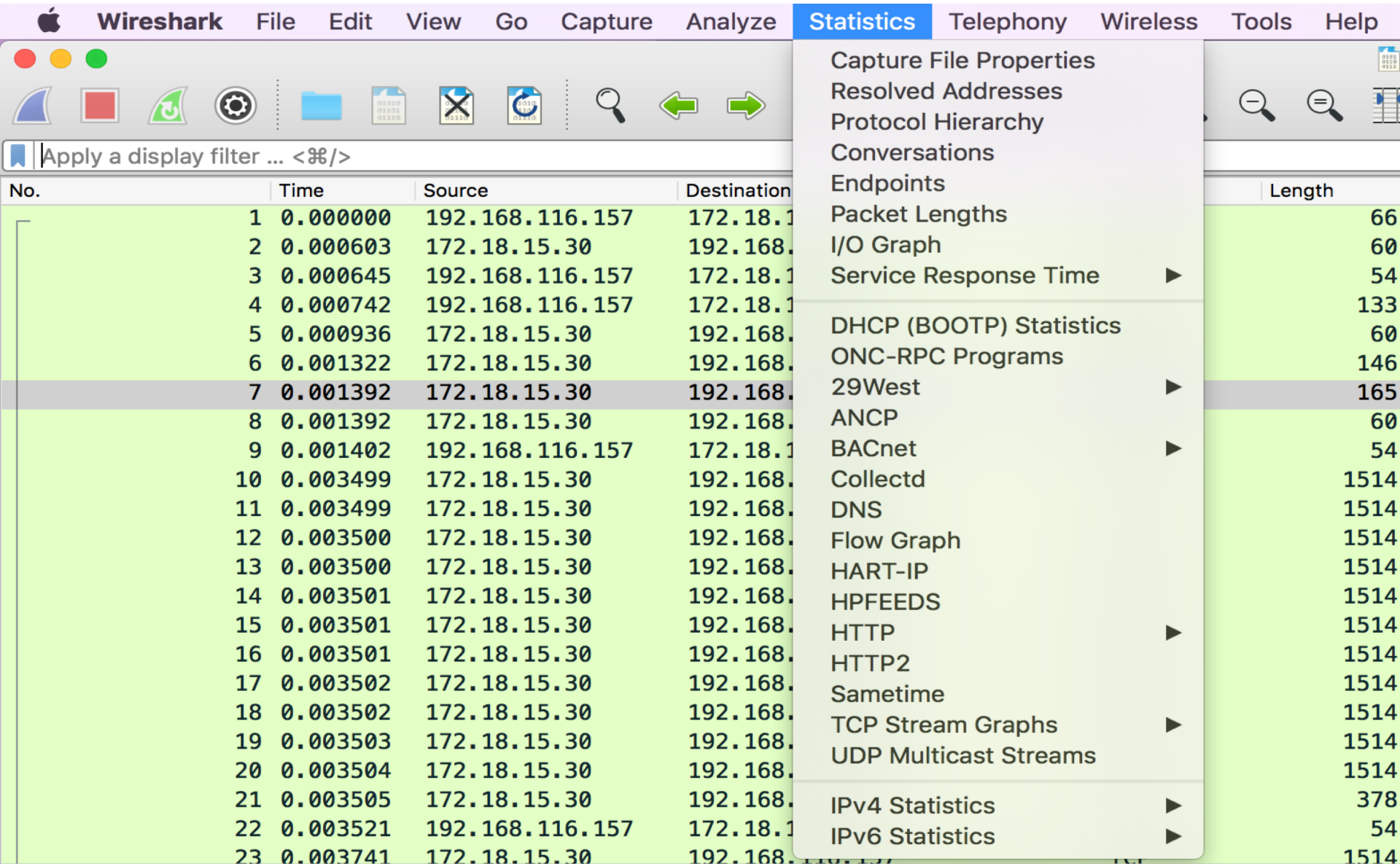
- Wireshark
- Moloch
- Tshark
- Tcpdump
- Ethereal
- Microsoft Network Monitor



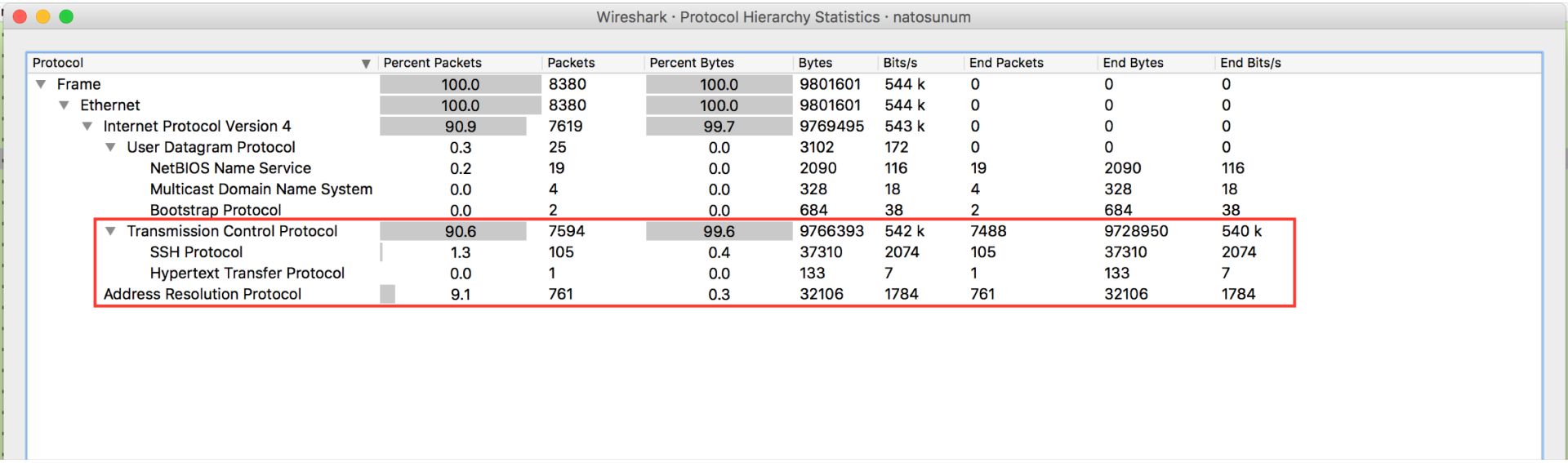
Wireshark


natosunum.pcapng
Apply a display filter ... <⌘/>
Expression...
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
natosunum
Packets: 8380 · Displayed: 8380 (100.0%) · Load time: 0:0.290
Profile: Default

Statistics

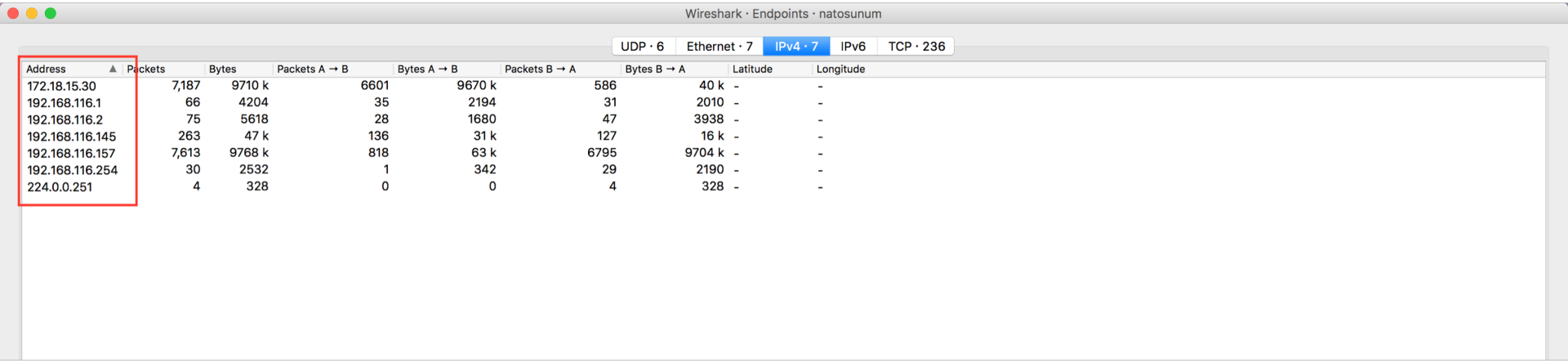

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Apply a display filter ... <⌘/>
No. Time Source Destination Length
1 0.000000 192.168.116.157 172.18.1 66
2 0.000603 172.18.15.30 192.168. 60
3 0.000645 192.168.116.157 172.18.1 54
4 0.000742 192.168.116.157 172.18.1 133
5 0.000936 172.18.15.30 192.168. 60
6 0.001322 172.18.15.30 192.168. 146
7 0.001392 172.18.15.30 192.168. 165
8 0.001392 172.18.15.30 192.168. 60
9 0.001402 192.168.116.157 172.18.1 54
10 0.003499 172.18.15.30 192.168. 1514
11 0.003499 172.18.15.30 192.168. 1514
12 0.003500 172.18.15.30 192.168. 1514
13 0.003500 172.18.15.30 192.168. 1514
14 0.003501 172.18.15.30 192.168. 1514
15 0.003501 172.18.15.30 192.168. 1514
16 0.003501 172.18.15.30 192.168. 1514
17 0.003502 172.18.15.30 192.168. 1514
18 0.003502 172.18.15.30 192.168. 1514
19 0.003503 172.18.15.30 192.168. 1514
20 0.003504 172.18.15.30 192.168. 1514
21 0.003505 172.18.15.30 192.168. 378
22 0.003521 192.168.116.157 172.18.1 54
23 0.003741 172.18.15.30 192.168. 1514

Protocol Hierarchy



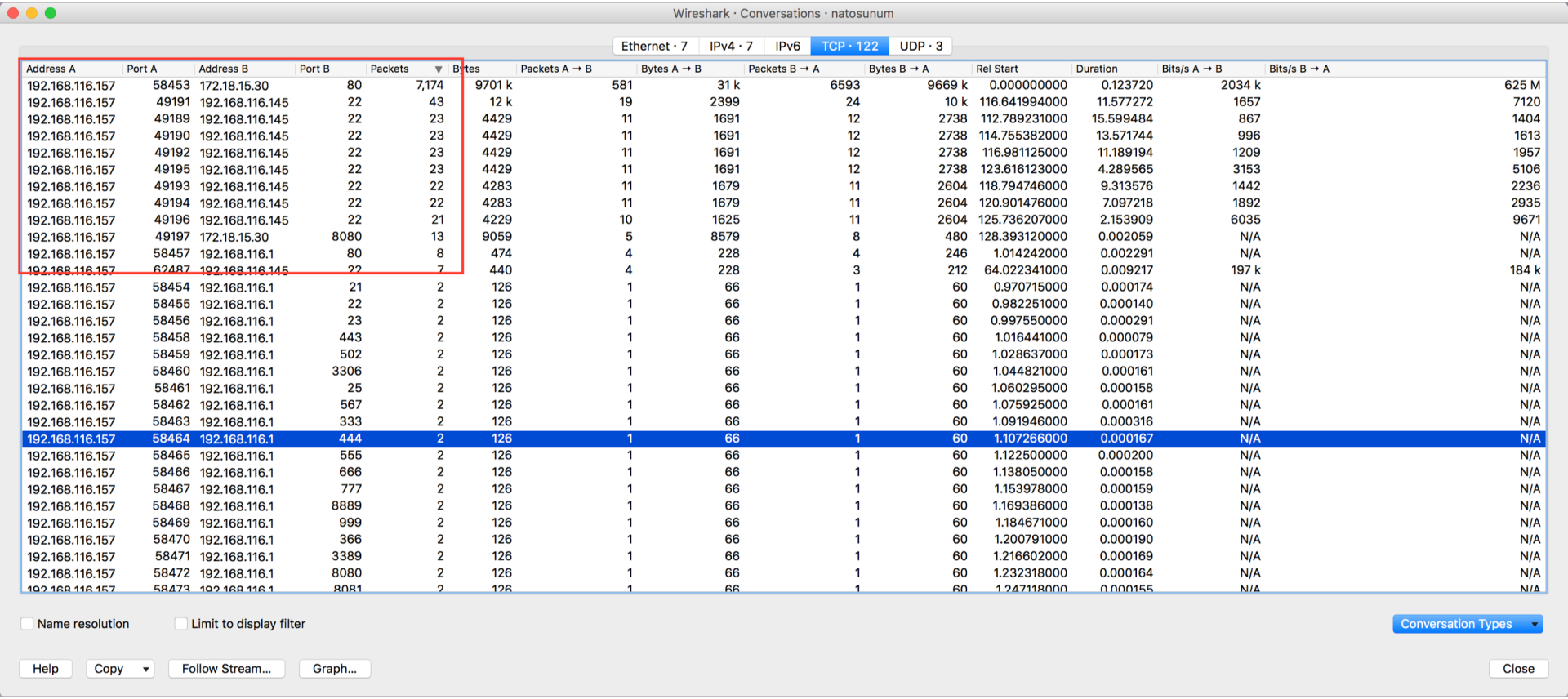
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	8380	100.0	9801601	544 k	0	0	0
▼ Ethernet	100.0	8380	100.0	9801601	544 k	0	0	0
▼ Internet Protocol Version 4	90.9	7619	99.7	9769495	543 k	0	0	0
▼ User Datagram Protocol	0.3	25	0.0	3102	172	0	0	0
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



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

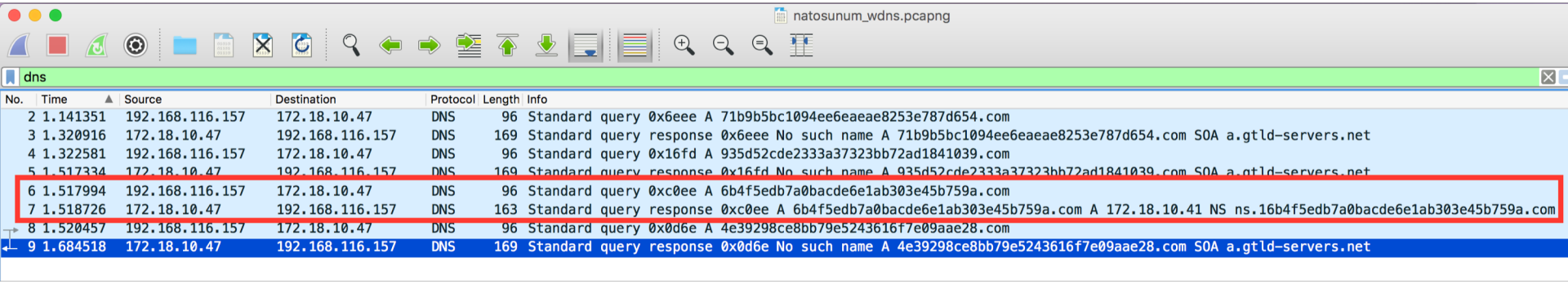


Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.116.157	58453	172.18.15.30	80	7,174	9701 k	581	31 k	6593	9669 k	0.000000000	0.123720	2034 k	625 M
192.168.116.157	49191	192.168.116.145	22	43	12 k	19	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

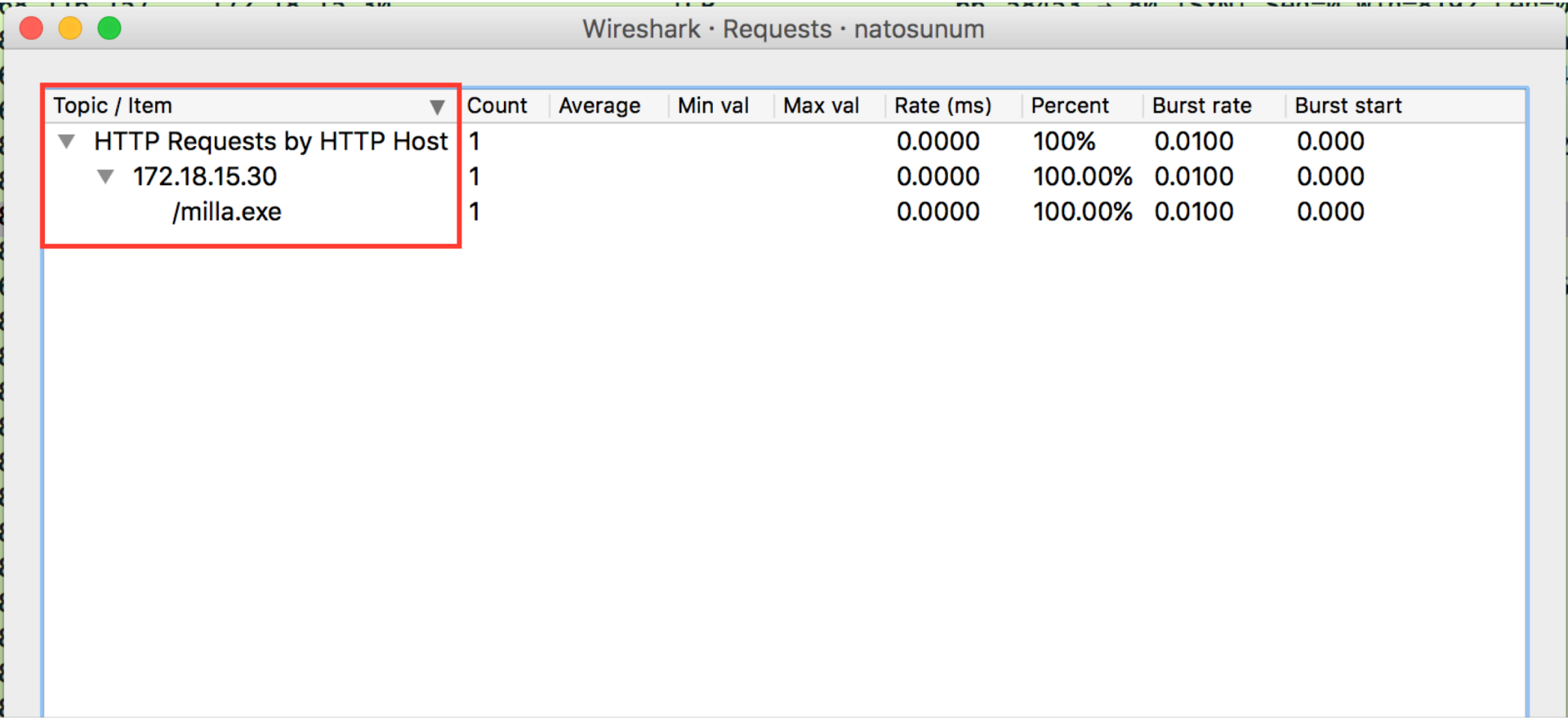
What do we have?

- 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

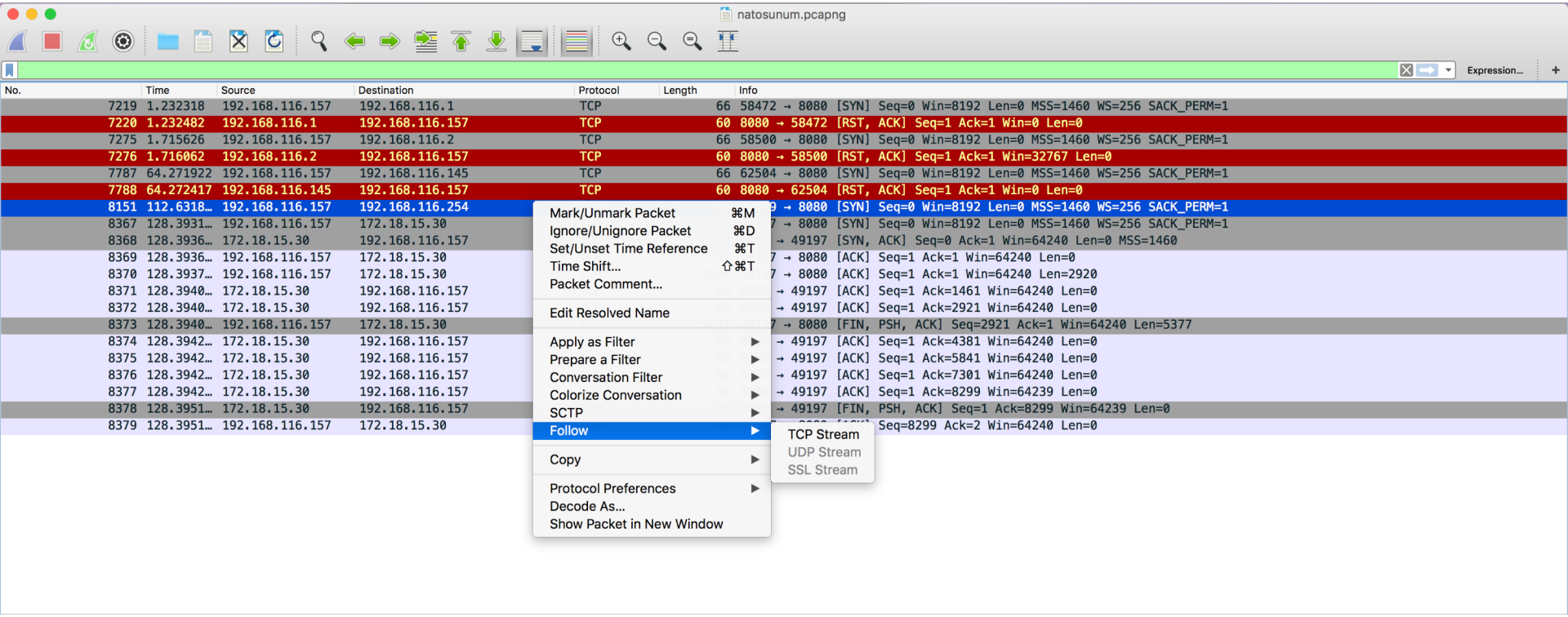
DNS Requests



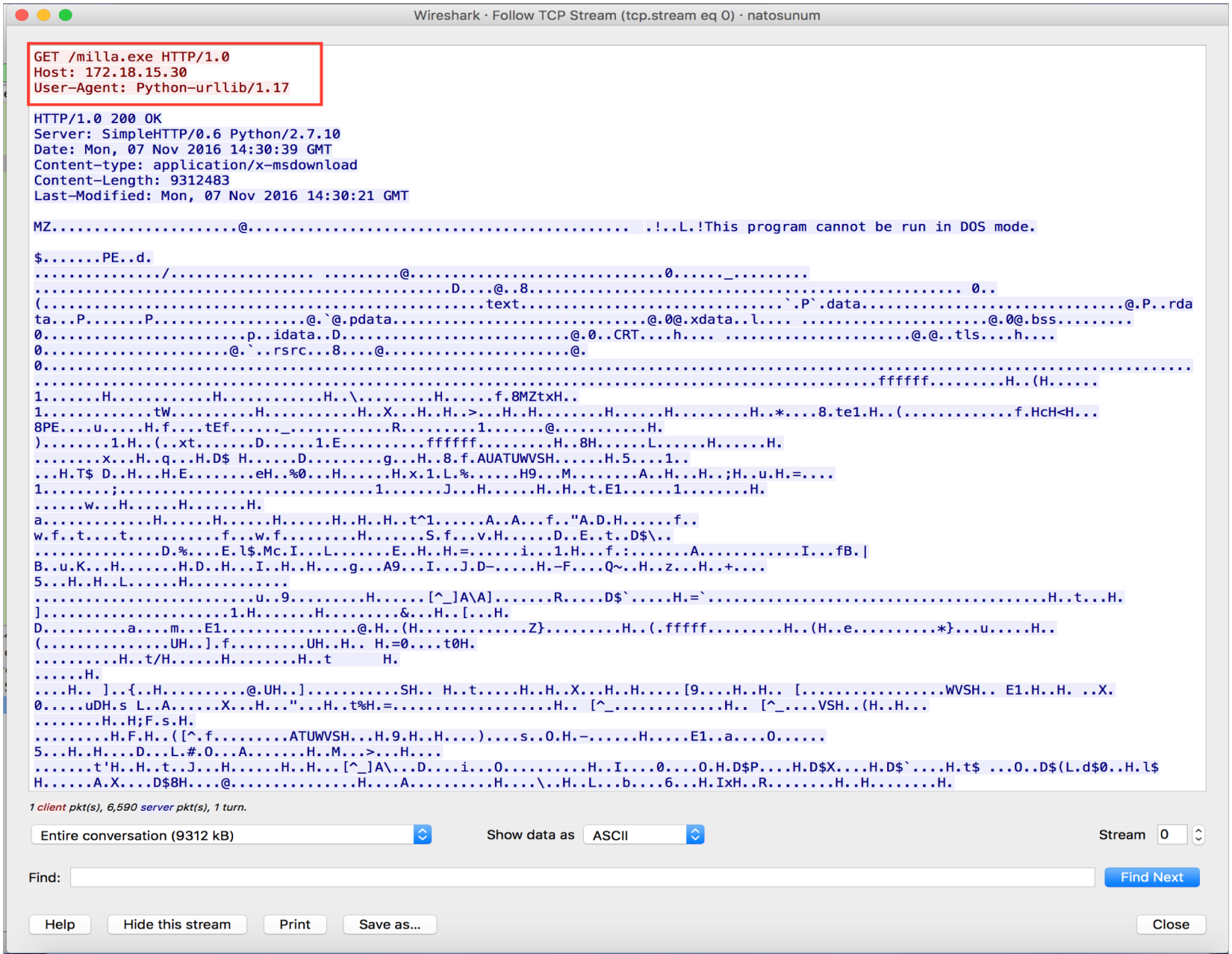
HTTP Requests



TCP Streams


natosunum.pcapng
Expression...
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 9 → 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 7 → 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 → 49197 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
8369 128.3936… 192.168.116.157 172.18.15.30 7 → 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8370 128.3937… 192.168.116.157 172.18.15.30 7 → 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=2920
8371 128.3940… 172.18.15.30 192.168.116.157 → 49197 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
8372 128.3940… 172.18.15.30 192.168.116.157 → 49197 [ACK] Seq=1 Ack=2921 Win=64240 Len=0
8373 128.3940… 192.168.116.157 172.18.15.30 7 → 8080 [FIN, PSH, ACK] Seq=2921 Ack=1 Win=64240 Len=5377
8374 128.3942… 172.18.15.30 192.168.116.157 → 49197 [ACK] Seq=1 Ack=4381 Win=64240 Len=0
8375 128.3942… 172.18.15.30 192.168.116.157 → 49197 [ACK] Seq=1 Ack=5841 Win=64240 Len=0
8376 128.3942… 172.18.15.30 192.168.116.157 → 49197 [ACK] Seq=1 Ack=7301 Win=64240 Len=0
8377 128.3942… 172.18.15.30 192.168.116.157 → 49197 [ACK] Seq=1 Ack=8299 Win=64239 Len=0
8378 128.3951… 172.18.15.30 192.168.116.157 → 49197 [FIN, PSH, ACK] Seq=1 Ack=8299 Win=64239 Len=0
8379 128.3951… 192.168.116.157 172.18.15.30 Seq=8299 Ack=2 Win=64240 Len=0
Mark/Unmark Packet ⌘M
Ignore/Unignore Packet ⌘D
Set/Unset Time Reference ⌘T
Time Shift... ⇧⌘T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream

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.
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

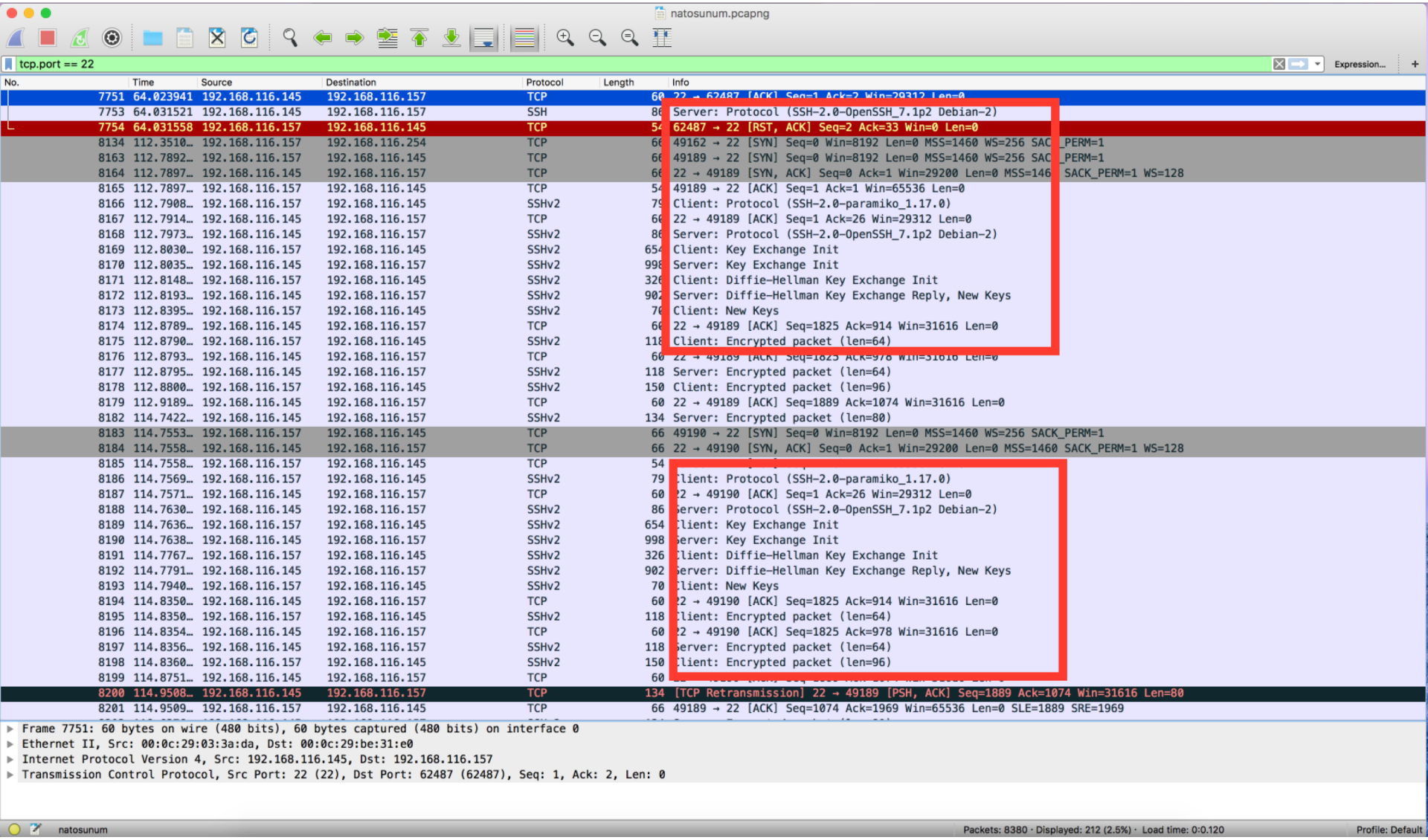
▶ Frame 7177: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: Vmware_be:31:e0 (00:0c:29:be:31:e0), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
▶ Internet Protocol Version 4, Src: 192.168.116.157, Dst: 192.168.116.1
▶ Transmission Control Protocol, Src Port: 58454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

Detecting Port Scan

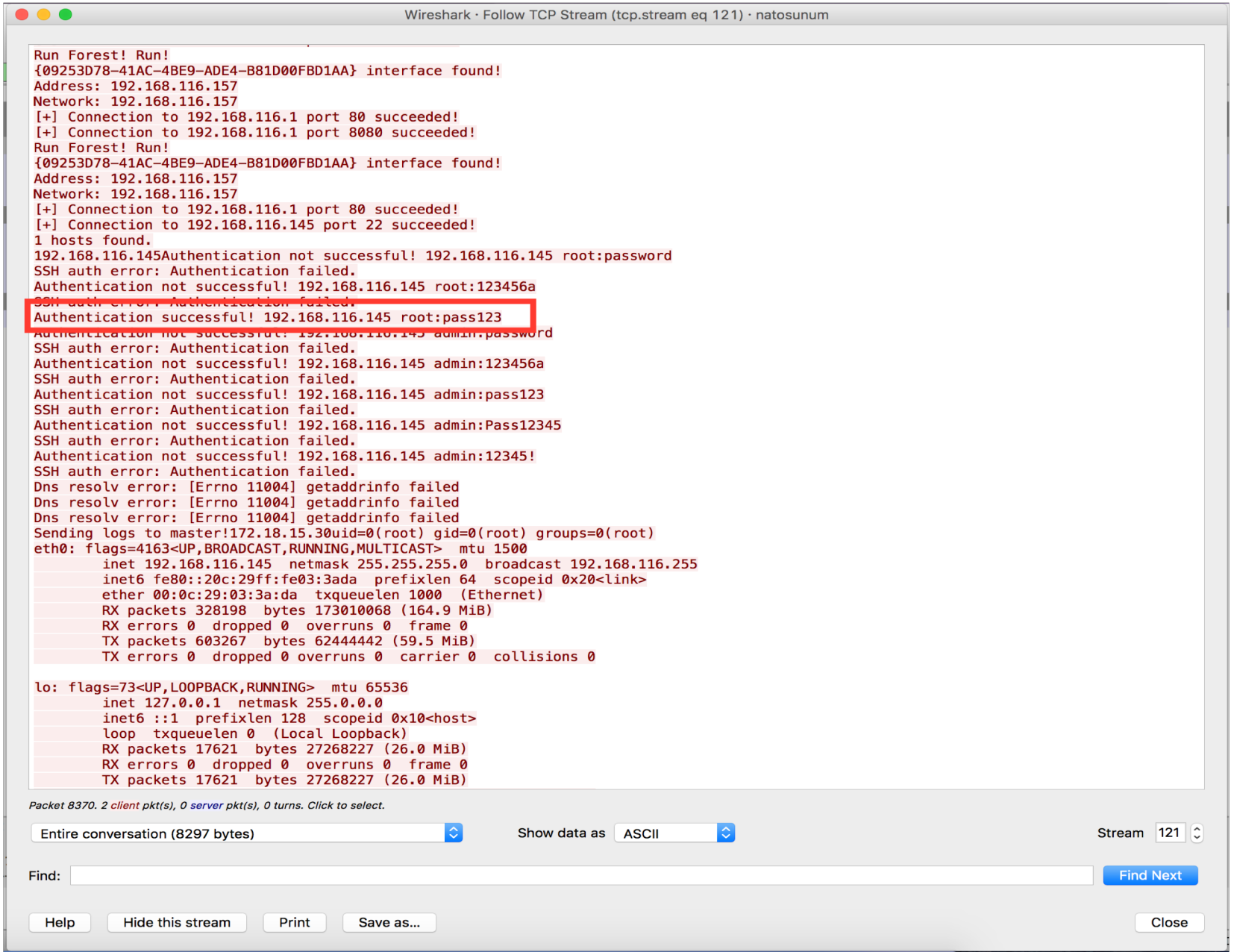
No.	Time	Source	Destination	Protocol	Length	Info
7175	0.970576	00:0c:29:be:31:e0	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.116.1? Tell 192.168.116.157
7176	0.970708	00:50:56:c0:00:08	00:0c:29:be:31:e0	ARP	60	192.168.116.1 is at 00:50:56:c0:00:08
7177	0.970715	192.168.116.157	192.168.116.1	TCP	66	58454 → 21 [SYN] 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 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7179	0.982251	192.168.116.157	192.168.116.1	TCP	66	58455 → 22 [SYN] 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 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7181	0.997550	192.168.116.157	192.168.116.1	TCP	66	58456 → 23 [SYN] 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 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7183	1.014242	192.168.116.157	192.168.116.1	TCP	66	58457 → 80 [SYN] 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 [SYN, 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 [ACK] 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 [FIN, 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 [ACK] Seq=1 Ack=2 Win=262144 Len=0
7190	1.016520	192.168.116.1	192.168.116.157	TCP	60	80 → 58457 [FIN, 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 [ACK] 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 [SYN] 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 [RST, 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

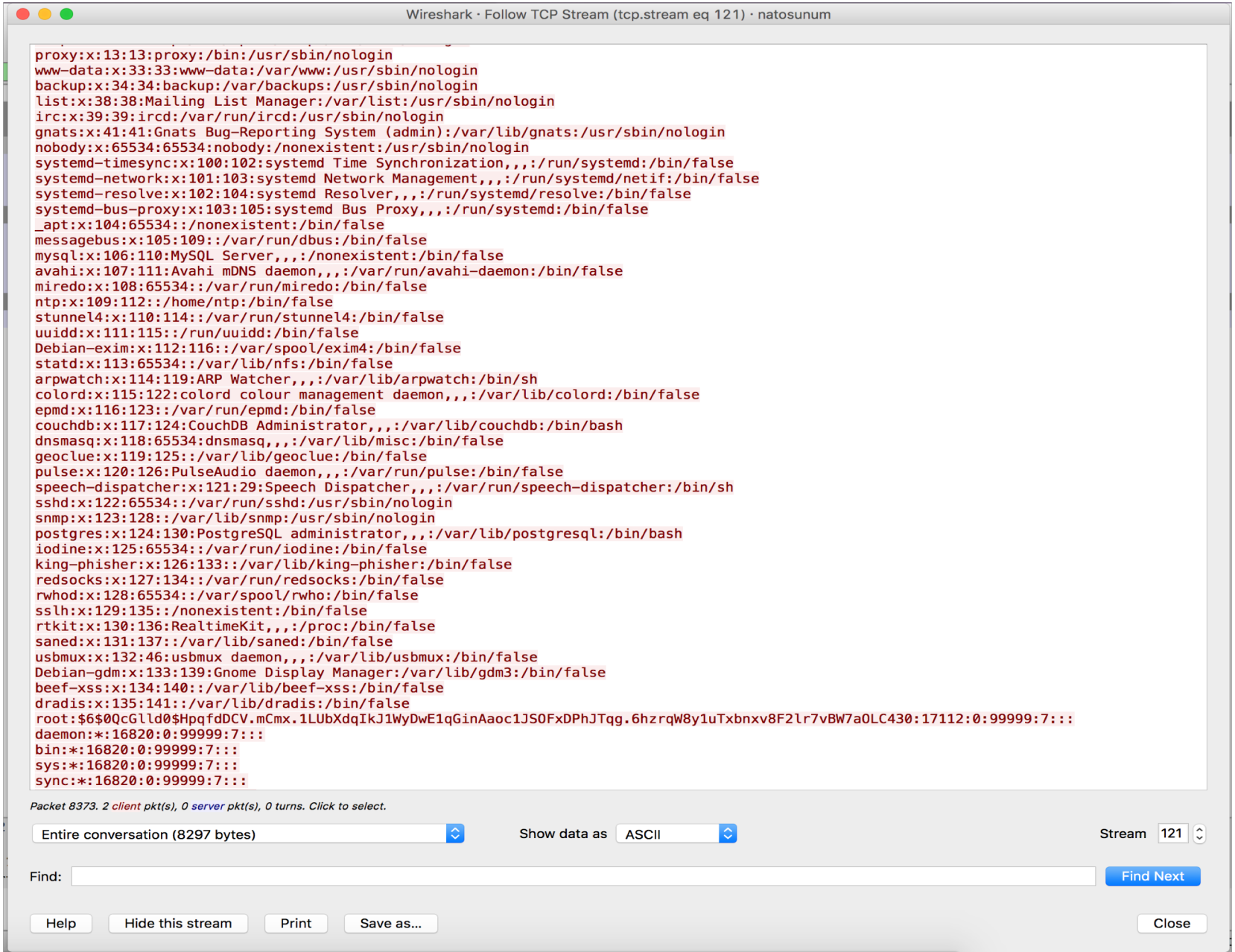
Detecting SSH Brute Force



Data Exfiltration



Data Exfiltration



EOF