

# Wire shark

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter - <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
93	4.548794	Dell_34:34:27	Broadcast	ARP	60	Who has 10.30.74.212? Tell 10.30.74.93
94	4.548794	Dell_34:34:27	Broadcast	ARP	60	Who has 10.30.74.97? Tell 10.30.74.93
95	4.584852	10.30.74.87	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
96	4.808625	JuniperR_a6:27:a1	Broadcast	ARP	60	Who has 10.30.74.99? Tell 10.30.75.254
97	4.843402	JuniperR_a6:27:a1	Broadcast	ARP	60	Who has 10.30.74.112? Tell 10.30.75.254
98	5.881548	Cisco_c6:08:17	PVST+	STP	64	RST. Root = 32768/423/c4:7e:e0:c6:88:80 Cost = 0 Port = 0x8017
99	5.167476	JuniperR_a6:27:a1	Broadcast	ARP	60	Who has 10.30.75.49? Tell 10.30.75.254
100	5.200439	Dell_14:63:74	Broadcast	ARP	60	Who has 10.30.74.97? Tell 10.30.75.178
101	5.236843	HP_31:74:cf	Broadcast	ARP	60	Who has 10.30.75.19? Tell 10.30.74.252
102	5.236843	HP_31:74:cf	Broadcast	ARP	60	Who has 10.30.75.151? Tell 10.30.74.252
103	5.492589	JuniperR_a6:27:a1	Broadcast	ARP	60	Who has 10.30.74.112? Tell 10.30.75.254
104	5.454732	Dell_34:34:27	Broadcast	ARP	60	Who has 10.30.75.34? Tell 10.30.74.93
105	5.454732	Dell_34:34:27	Broadcast	ARP	60	Who has 10.30.74.212? Tell 10.30.74.93
106	5.454732	Dell_34:34:27	Broadcast	ARP	60	Who has 10.30.74.97? Tell 10.30.74.93
107	5.464104	JuniperR_83:7b:ff	Spanning-tree-(for-...	STP	60	RST. Root = 32768/0/04:a7:41:92:e7:3b Cost = 64000 Port = 0x81f1
108	5.503511	JuniperR_a6:27:a1	Broadcast	ARP	60	Who has 10.30.74.99? Tell 10.30.75.254
109	5.516629	10.30.74.96	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
110	5.586628	10.30.74.87	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
111	5.687535	Cisco_49:ea:98	PVST+	STP	64	RST. Root = 32768/423/40:14:82:49:ea:80 Cost = 0 Port = 0x8018
112	6.003112	JuniperR_a6:27:a1	Broadcast	ARP	60	Who has 10.30.74.112? Tell 10.30.75.254

> Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF\_{A68550F8-0893-467...}

> Ethernet II, Src: Dell\_2a:54:f2 (74:86:e2:2a:54:f2), Dst: JuniperR\_a6:27:a1 (30:7c:5e:a6:27:a1)

> Internet Protocol Version 4, Src: 10.30.74.96, Dst: 10.20.30.31

> Transmission Control Protocol, Src Port: 63267, Dst Port: 7680, Seq: 1, Ack: 1, Len: 4

> Data (4 bytes)

0000 30 7c 5e a6 27 a1 74 86 e2 2a 54 f2 00 00 45 00 0|...t...T...E  
0010 00 2c a5 a5 40 00 00 00 00 00 0a 1e 4a 60 0a 14 ...@... ..J...  
0020 1e 1f f7 23 1e 00 1d e0 d7 ef cc ae 4c 27 50 18 ...P... ..L'P...  
0030 04 01 7c cf 00 00 00 00 00 00

Activate Windows  
Go to Settings to activate Windows.

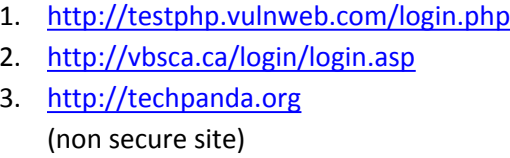
Login | Personal Contacts Manager v1.0

Email\*

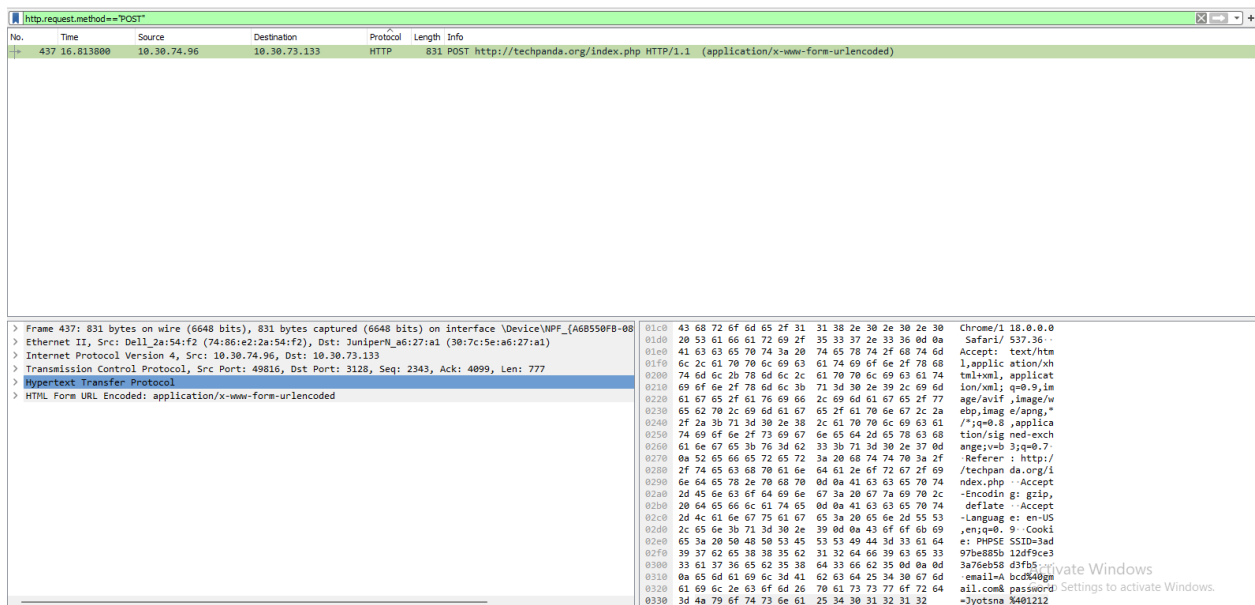
Password\*

☐ Remember me

Submit



```
http.request.method=="POST"
```



No.	Time	Source	Destination	Protocol	Length	Info
69	4.569295	10.30.74.96	10.30.73.133	TCP	66	50054 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
70	4.569621	10.30.73.133	10.30.74.96	TCP	66	3128 → 50054 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
135	11.283573	10.30.74.96	10.30.73.133	TCP	66	50055 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
136	11.284184	10.30.73.133	10.30.74.96	TCP	66	3128 → 50055 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
228	17.155609	10.30.74.96	10.30.73.133	TCP	66	50056 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
229	17.155939	10.30.73.133	10.30.74.96	TCP	66	3128 → 50056 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
323	22.638458	10.30.74.96	10.30.73.133	TCP	66	50057 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
324	22.638743	10.30.73.133	10.30.74.96	TCP	66	3128 → 50057 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
473	28.083530	10.30.74.96	10.30.73.133	TCP	66	50058 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
474	28.083969	10.30.73.133	10.30.74.96	TCP	66	3128 → 50058 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
613	31.065277	10.30.74.96	10.30.73.133	TCP	66	50059 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
614	31.065560	10.30.73.133	10.30.74.96	TCP	66	3128 → 50059 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
660	31.417986	10.30.74.96	10.30.73.133	TCP	66	50060 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
661	31.418252	10.30.73.133	10.30.74.96	TCP	66	3128 → 50060 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
704	31.534909	10.30.74.96	10.30.73.133	TCP	66	50061 → 3128 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
705	31.535246	10.30.73.133	10.30.74.96	TCP	66	3128 → 50061 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
916	34.973976	10.30.74.96	10.30.73.133	TCP	66	50062 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
917	34.981202	10.30.73.133	10.30.74.96	TCP	66	3128 → 50062 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128
1055	41.645808	10.30.74.96	10.30.73.133	TCP	66	50063 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1056	41.646270	10.30.73.133	10.30.74.96	TCP	66	3128 → 50063 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=128

<pre>&gt; Frame 69: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A6B550F8-0B93-46 &gt; Ethernet II, Src: Dell_2a:54:f2 (74:86:e2:2a:54:f2), Dst: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1) &gt; Internet Protocol Version 4, Src: 10.30.74.96, Dst: 10.30.73.133 &gt; Transmission Control Protocol, Src Port: 50054, Dst Port: 3128, Seq: 0, Len: 0</pre>	<pre>0000 30 7c 5e a6 27 a1 74 86 e2 2a 54 f2 08 00 45 00 0 A...T...E- 0010 00 34 f0 c1 40 00 80 06 00 00 0a 1e 4a 60 0a 1e  4... ..]... 0020 49 85 c3 b6 0c 38 2f 3c fd d8 00 00 00 00 00 02  I...8/c..... 0030 fa f0 a8 47 00 00 02 04 05 b4 01 03 03 08 01 01  ...G..... 0040 04 02 ..</pre>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

No.	Time	Source	Destination	Protocol	Length	Info
777	37.219569	10.30.74.96	10.30.73.133	TCP	89	49580 → 3128 [PSH, ACK] Seq=2880 Ack=1544 Win=8195 Len=35
778	37.219683	10.30.74.96	10.30.73.133	TCP	89	49580 → 3128 [PSH, ACK] Seq=2915 Ack=1544 Win=8195 Len=35
843	40.053204	10.30.73.133	10.30.74.96	TCP	374	3128 → 49580 [PSH, ACK] Seq=1544 Ack=2950 Win=796 Len=320
844	40.053882	10.30.73.133	10.30.74.96	TCP	124	3128 → 49580 [PSH, ACK] Seq=1864 Ack=2950 Win=796 Len=70
846	40.054099	10.30.74.96	10.30.73.133	TCP	93	49580 → 3128 [PSH, ACK] Seq=2950 Ack=1934 Win=8193 Len=39
928	42.240698	10.30.74.96	10.30.73.133	TCP	2231	49584 → 3128 [PSH, ACK] Seq=5153 Ack=1880 Win=8195 Len=2177
929	42.240802	10.30.74.96	10.30.73.133	TCP	117	49584 → 3128 [PSH, ACK] Seq=7330 Ack=1880 Win=8195 Len=63
939	42.509354	10.30.73.133	10.30.74.96	TCP	573	3128 → 49584 [PSH, ACK] Seq=1880 Ack=7393 Win=1241 Len=519
940	42.509354	10.30.73.133	10.30.74.96	TCP	374	3128 → 49584 [PSH, ACK] Seq=2399 Ack=7393 Win=1241 Len=320
941	42.509354	10.30.73.133	10.30.74.96	TCP	285	3128 → 49584 [PSH, ACK] Seq=2719 Ack=7393 Win=1241 Len=231
942	42.509354	10.30.73.133	10.30.74.96	TCP	303	3128 → 49584 [PSH, ACK] Seq=2950 Ack=7393 Win=1241 Len=249
944	42.512679	10.30.74.96	10.30.73.133	TCP	89	49584 → 3128 [PSH, ACK] Seq=7393 Ack=3199 Win=8190 Len=35
945	42.512744	10.30.74.96	10.30.73.133	TCP	89	49584 → 3128 [PSH, ACK] Seq=7428 Ack=3199 Win=8190 Len=39
992	45.308094	10.30.73.133	10.30.74.96	TCP	277	3128 → 49584 [PSH, ACK] Seq=3199 Ack=7467 Win=1241 Len=223
993	45.308279	10.30.74.96	10.30.73.133	TCP	89	49584 → 3128 [PSH, ACK] Seq=7467 Ack=3422 Win=8195 Len=35
994	45.308682	10.30.73.133	10.30.74.96	TCP	296	3128 → 49584 [PSH, ACK] Seq=3422 Ack=7467 Win=1241 Len=242
996	45.309182	10.30.73.133	10.30.74.96	TCP	169	3128 → 49584 [PSH, ACK] Seq=3664 Ack=7502 Win=1241 Len=115
998	45.309220	10.30.74.96	10.30.73.133	TCP	93	49584 → 3128 [PSH, ACK] Seq=7502 Ack=3779 Win=8193 Len=39
999	45.311587	10.30.74.96	10.30.73.133	TCP	941	49584 → 3128 [PSH, ACK] Seq=7541 Ack=3779 Win=8193 Len=687
1002	45.565402	10.30.73.133	10.30.74.96	TCP	277	3128 → 49584 [PSH, ACK] Seq=3779 Ack=8428 Win=1241 Len=223

> Frame 3: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{A6B550F8-...}

> Ethernet II, Src: JuniperNet\_a6:27:a1 (30:7c:5e:a6:27:a1), Dst: Dell\_2a:54:f2 (74:86:e2:2a:54:f2)

> Internet Protocol Version 4, Src: 10.30.73.133, Dst: 10.30.74.96

> Transmission Control Protocol, Src Port: 3128, Dst Port: 50142, Seq: 2921, Ack: 1, Len: 1460

```

0000  74 86 e2 2a 54 f2 30 7c   5e a6 27 a1 08 00 45 00   t--T@ ^---E
0010  05 dc 49 6e 40 00 3f 06   44 8d 0a 1e 49 05 0a 1e   -In@? : D--I--
0020  4a 60 bc 38 c3 de cc 9c   29 92 0a 3e 7c 1b 50 18   J' 8----->-P
0030  00 83 9f f0 60 30 99 52   87 2f 19 50 40 fc cf d0 a9   --9R -IPB-
0040  75 se 6d 74 fc cb d7 83   b1 01 36 00 ee 7f 69      u-nmt-----6-i
0050  41 53 50 c1 bd 73 a9 de   cb 19 39 b6 ad 56 74 ab   ASP s---9-Vt-
0060  bf 92 2b af c2 ce 95 f0   c3 9a e5 dd ab ff 2e 11   +-----K-L-
0070  16 16 47 52 c8 31 c5 4c   92 95 89 46 a4 d7 07 86   -GR-1L---F---
0080  1b 32 af b1 2f 15 e7 19   18 0d 4c 7e c8 ad 01 65   -2----L-e-e
0090  69 ea 18 96 00 d9 16 28   83 5f 45 c7 6d dd 9d 80   i-----(-E-m-
00a0  db 76 66 30 7f 4c 45 21   81 71 c1 e2 3e ec fo ad   -xf0 LE! q-->-
00b0  5b 12 98 bc 2f b7 75 a5   44 38 0e 6c 99 04 e3 4b   [.../u D8-1-K
00c0  45 62 f2 7a 19 70 10 89   a1 67 00 05 92 54 eb 0f   Eb z p-----Tr-
00d0  3b 7c e3 eb 19 1d 6c 41   4c 98 9f f3 af e5 9e b7   j|-----IA L-e-e-
00e0  92 84 71 40 ed 50 18 40   e1 d5 14 a1 a3 d5 cf af   -qB P @-----
00f0  6e e3 a5 79 e9 5c 1c b7   96 57 bb 56 25 b2 4f 38   n-y[- yMVK 0-
0100  8f 99 54 3c b7 6c 03 1b   7e 96 d3 f8 38 f4 28 39   -Tc-1- n--8-(9
0110  3a 67 63 c9 31 5a 41 fa   92 03 b9 81 32 84 dc 74   :gc-12A- ----2-t
0120  6f a1 52 23 53 8c 49 d0   94 3b e3 ac f2 ff c1 ad   o RRS-I- -----
0130  40 0d fa 49 a3 62 cf 85   37 3b 5d 33 15 98 36 46   @-I-b- ? ]3--6F
0140  46 fe 74 bd 4b 05 9f 04   5c bd bf af 9a b9 07 09   K-t K- < V-g-6-
0150  e1 54 7f cc d6 3a 13 be   94 6f 69 e1 29 00 98 64   T-----o1->-d
0160  20 ff 4d 92 0b fd 18 4a   52 75 c0 34 3a bb 4e 39   N-----Ru d-1-B
0170  e1 ad ae c8 98 c0 c8 58   92 3a 41 e6 7c 34 70 96   X-A:1A:40-
```

tcp && ip.addr== 10.30.74.96

No.	Time	Source	Destination	Protocol	Length	Info
7773	204.223830	10.30.74.96	10.30.73.133	TLSv1.3	2482	Application Data
7774	204.223921	10.30.74.96	10.30.73.133	TLSv1.3	863	Application Data
7775	204.224210	10.30.73.133	10.30.74.96	TCP	60	3128 → 62216 [ACK] Seq=144044 Ack=167909 Win=102144 Len=0
7776	204.235189	10.30.73.133	10.30.74.96	TLSv1.3	398	Application Data
7777	204.236072	10.30.73.133	10.30.74.96	TLSv1.3	429	Application Data, Application Data
7778	204.236199	10.30.74.96	10.30.73.133	TCP	54	62216 → 3128 [ACK] Seq=167909 Ack=144763 Win=261888 Len=0
7779	204.237149	10.30.73.133	10.30.74.96	TLSv1.3	85	Application Data
7780	204.238209	10.30.73.133	10.30.74.96	TLSv1.3	398	Application Data
7781	204.238323	10.30.74.96	10.30.73.133	TCP	54	62216 → 3128 [ACK] Seq=167909 Ack=145138 Win=261632 Len=0
7782	204.240226	10.30.73.133	10.30.74.96	TLSv1.3	85	Application Data
7783	204.247932	10.30.73.133	10.30.74.96	TCP	553	3128 → 63598 [PSH, ACK] Seq=14817 Ack=4212 Win=888 Len=499
7784	204.248533	10.30.73.133	10.30.74.96	TCP	591	3128 → 63598 [PSH, ACK] Seq=15316 Ack=4212 Win=888 Len=537
7785	204.248557	10.30.74.96	10.30.73.133	TCP	54	63598 → 3128 [ACK] Seq=4212 Ack=15853 Win=8190 Len=0
7786	204.264446	10.30.74.96	10.30.73.133	TCP	128	63598 → 3128 [PSH, ACK] Seq=4212 Ack=15853 Win=8190 Len=74
7787	204.264782	10.30.73.133	10.30.74.96	TCP	60	3128 → 63598 [ACK] Seq=15853 Ack=4286 Win=888 Len=0
7788	204.274982	10.30.73.133	10.30.74.96	TLSv1.3	399	Application Data
7789	204.274982	10.30.73.133	10.30.74.96	TLSv1.3	85	Application Data
7790	204.275034	10.30.74.96	10.30.73.133	TCP	54	62216 → 3128 [ACK] Seq=167909 Ack=145545 Win=262656 Len=0
7792	204.480069	10.30.73.133	10.30.74.96	TLSv1.3	425	Application Data, Application Data
7797	204.448121	10.30.74.96	10.30.73.133	TCP	54	62216 → 3128 [ACK] Seq=167909 Ack=145916 Win=262400 Len=0

> Frame 29: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF\_{A6B550FB-0893-...} on 00:00:00:00:00:00  
> Ethernet II, Src: Dell\_2a:54:f2 (74:86:e2:2a:54:f2), Dst: JuniperN\_a6:27:a1 (30:7c:5e:a6:27:a1)  
> Internet Protocol Version 4, Src: 10.30.74.96, Dst: 10.30.73.133  
> Transmission Control Protocol, Src Port: 63598, Dst Port: 3128, Seq: 1, Ack: 1, Len: 70

0000 30 7c 5e a6 27 a1 74 86 e2 2a 54 f2 08 00 45 00 0|'^'.t:..\*T...E-  
0010 00 6e 07 e3 40 00 80 06 00 00 0a 1e 4a 60 0a 1e .n. @... ..J'..  
0020 49 85 f8 6e 0c 38 31 0b 42 3d 2b cc a3 f2 50 18 I..n 81- B+...P-  
0030 1f fd a8 81 00 00 17 03 03 00 41 d9 49 35 22 0e ..... ..A'IS"  
0040 cf e9 4f b9 b1 e1 96 b0 63 62 cf 26 63 fe a3 af ..0..... cb.&c...  
0050 7e ea 41 05 63 27 ff bf c8 bc 09 82 84 f2 b2 09 ~A:c'.....  
0060 e3 74 3c c3 8f 26 aa b6 91 8a f0 39 17 4c 9f 80 .t<.&... ..9-L...  
0070 29 b1 a8 ca ae b2 90 b5 f1 d0 d0 be )..... ..

## Summary of packets

28/10/25:09:11:15	10.30.73.133	10.30.74.96	ILP	00 3128 → 62216 [ACK] Seq=144044 Ack=167909 Win=102144 Len=0
Frame 29: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{A6B550FB-0893-...} on 00:00:00:00:00:00				
Ethernet II, Src: Dell_2a:54:f2 (74:86:e2:2a:54:f2), Dst: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1)				
Internet Protocol Version 4, Src: 10.30.74.96, Dst: 10.30.73.133				
Transmission Control Protocol, Src Port: 63598, Dst Port: 3128, Seq: 1, Ack: 1, Len: 70				

0000 30 7c 5e a6 27 a1 74 86 e2 2a 54 f2 08 00 45 00 0|'^'.t:..\*T...E-  
0010 00 6e 07 e3 40 00 80 06 00 00 0a 1e 4a 60 0a 1e .n. @... ..J'..  
0020 49 85 f8 6e 0c 38 31 0b 42 3d 2b cc a3 f2 50 18 I..n 81- B+...P-  
0030 1f fd a8 81 00 00 17 03 03 00 41 d9 49 35 22 0e ..... ..A'IS"  
0040 cf e9 4f b9 b1 e1 96 b0 63 62 cf 26 63 fe a3 af ..0..... cb.&c...  
0050 7e ea 41 05 63 27 ff bf c8 bc 09 82 84 f2 b2 09 ~A:c'.....  
0060 e3 74 3c c3 8f 26 aa b6 91 8a f0 39 17 4c 9f 80 .t<.&... ..9-L...  
0070 29 b1 a8 ca ae b2 90 b5 f1 d0 d0 be )..... ..

Activate Windows  
Go to Settings to activate Windows.

wireshark\_EthernetIIFQD02.pcapng

Packets: 28787 · Displayed: 17055 (59.2%)

Profile: Default