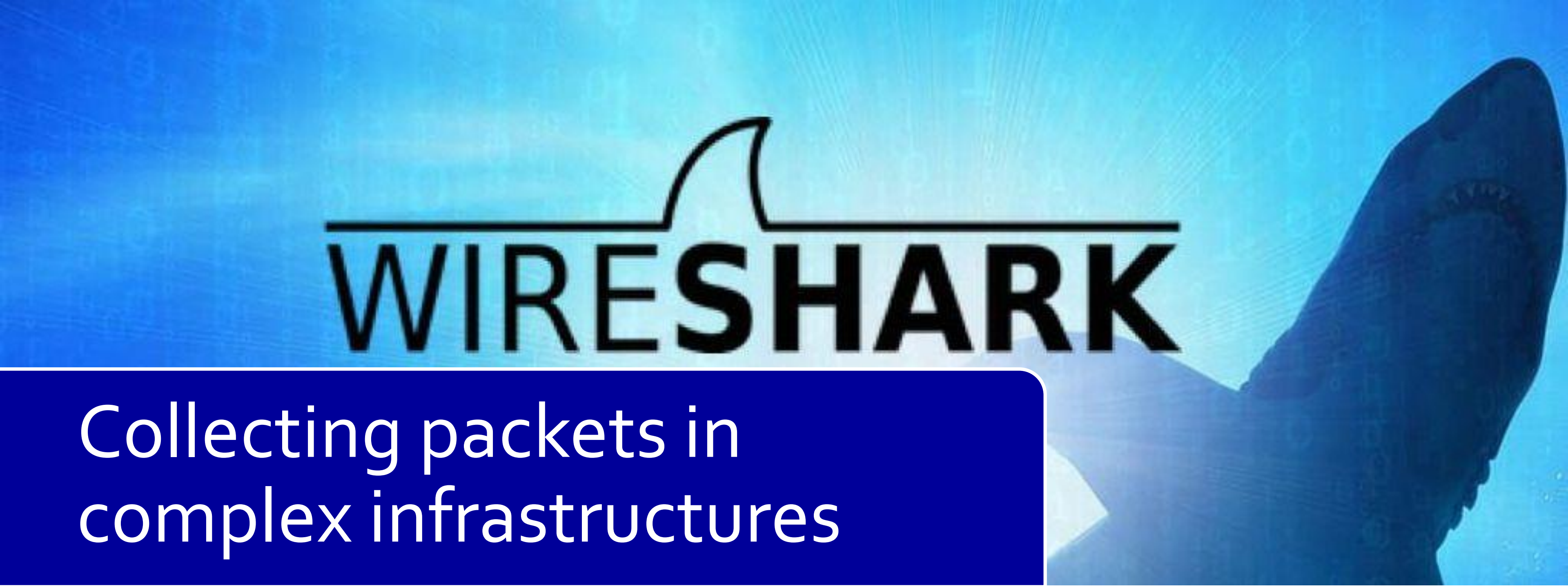


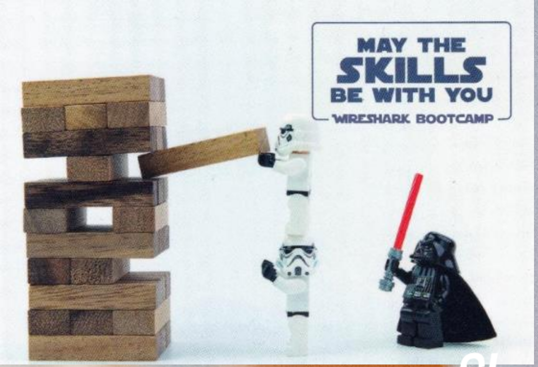
Collecting packets in complex infrastructures

Wireshark Users NL – Meetup

André Luyer – February 25th 2020

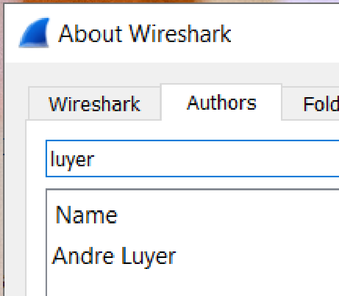
Rabobank

About me



Rabobank

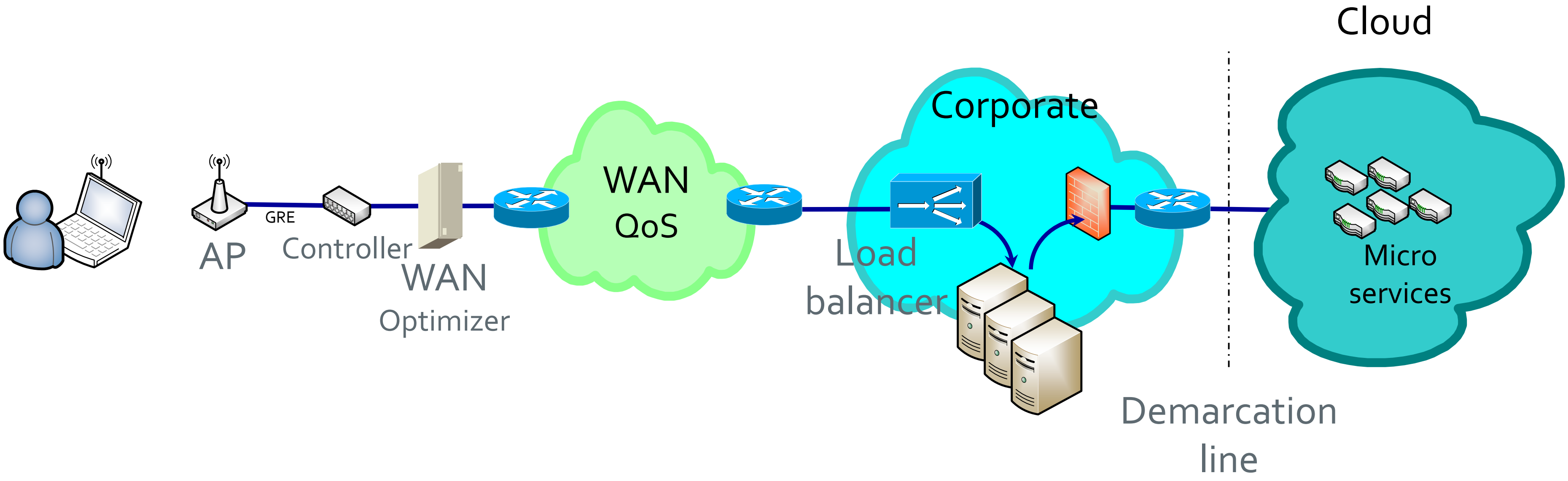
SharkFest'19 EUROPE
Nov 4-8 • Estoril, Portugal



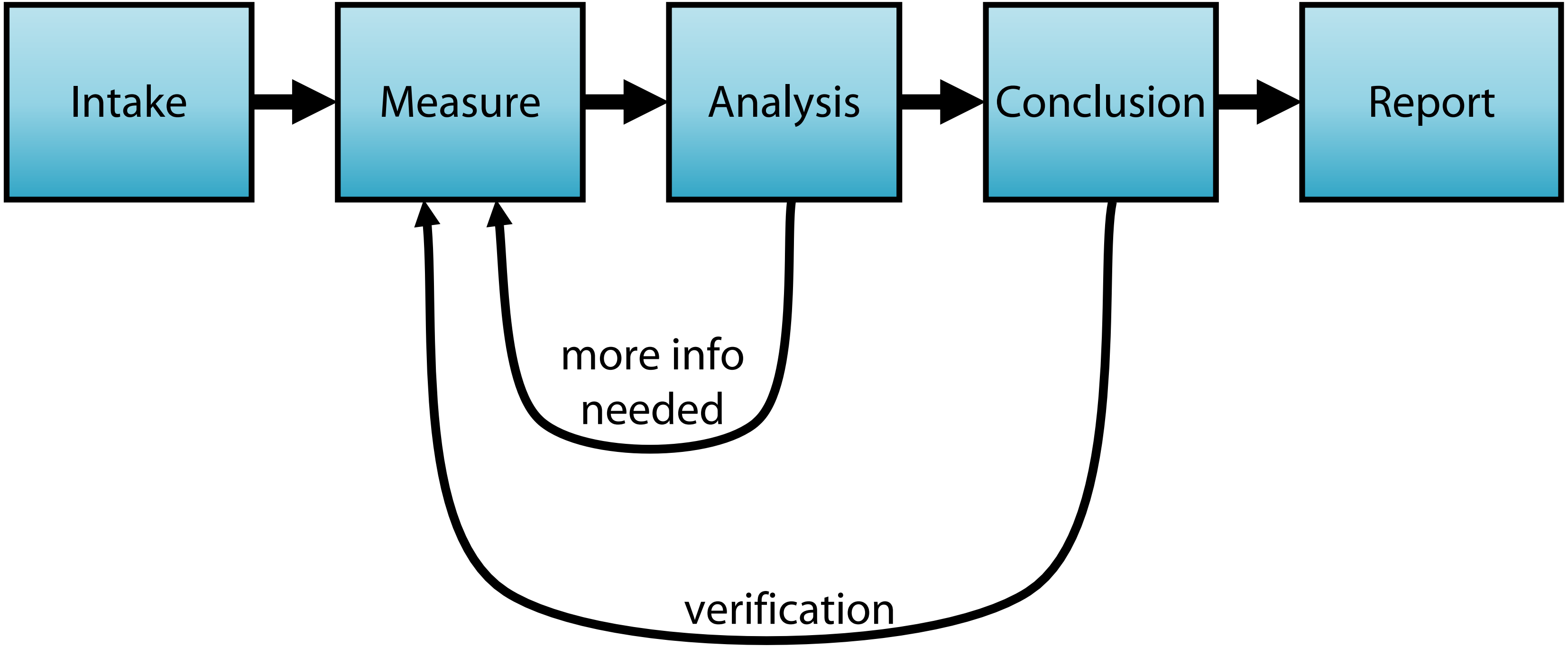
luyer

Name
Andre Luyer

Infrastructure



Troubleshoot process



Intake

Measure

Analysis

Conclusion

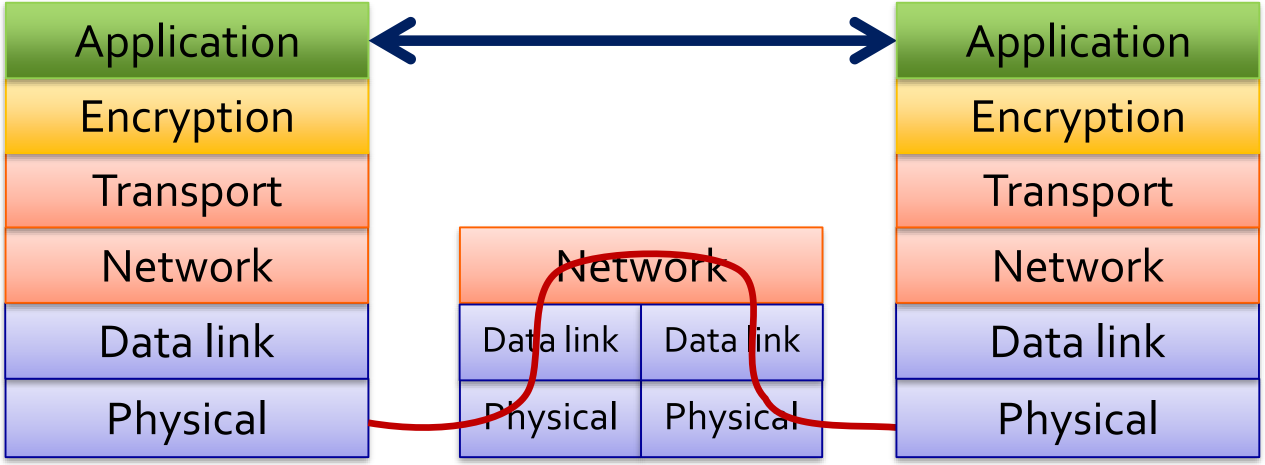
Report

more info needed

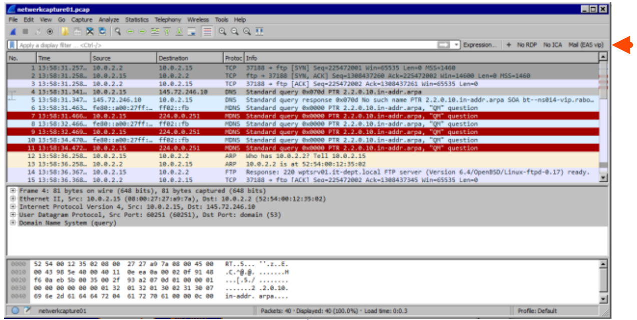
verification

Benefit of network captures

- Use network capture to analyse higher level protocols
- Log file entry may be unclear or incomplete – what is the real cause?
- Exact timing versus timestamps in log file (start? end? delayed?)
- Shows who is causing delays, fault conditions, performance issues, etc.
- Bottom-up analysis
- “Packets never lie”



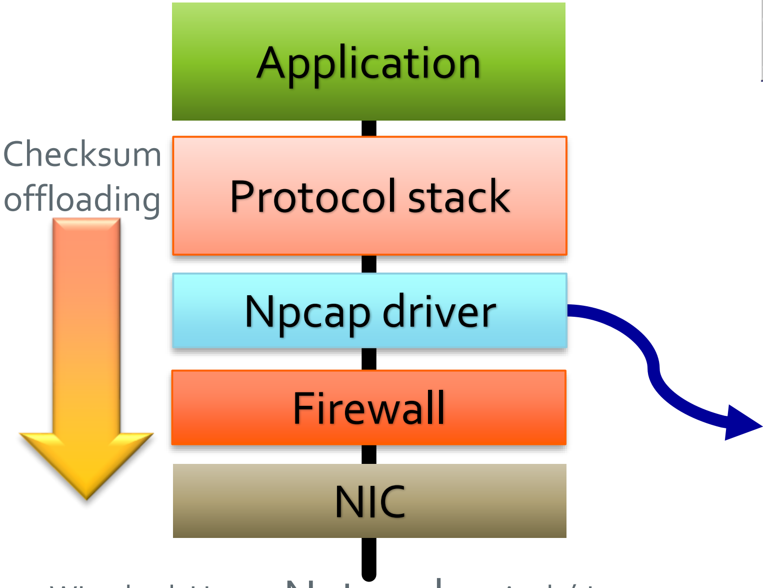
Capturing network packets locally

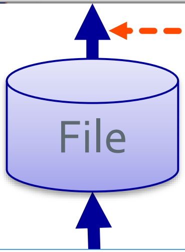


netwerkcapture01.pcap

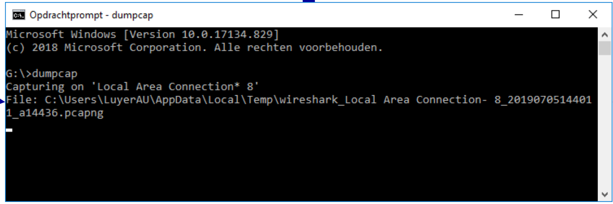
```
No. Time            Source             Destination    Protoc Info
  1 13:58:31.257… 10.0.2.2           10.0.2.15      TCP    37188 → ftp [SYN] Seq=225472001 Win=65535 Len=0 MSS=1460
  2 13:58:31.258… 10.0.2.15          10.0.2.2       TCP    ftp → 37188 [SYN, ACK] Seq=1308437260 Ack=225472002 Win=14600 Len=0 MSS=1460
  3 13:58:31.258… 10.0.2.2           10.0.2.15      TCP    37188 → ftp [ACK] Seq=225472002 Ack=1308437261 Win=65535 Len=0
  4 13:58:31.341… 10.0.2.15          145.72.246.10  DNS    Standard query 0x070d PTR 2.2.0.10.in-addr.arpa
  5 13:58:31.347… 145.72.246.10      10.0.2.15      DNS    Standard query response 0x070d No such name PTR 2.2.0.10.in-addr.arpa SOA bt--ns014-vip.rabo…
  6 13:58:31.463… fe80::a00:27ff:…   ff02::fb       MDNS   Standard query 0x0000 PTR 2.2.0.10.in-addr.arpa, "QM" question
  7 13:58:31.466… 10.0.2.15          224.0.0.251    MDNS   Standard query 0x0000 PTR 2.2.0.10.in-addr.arpa, "QM" question
  8 13:58:32.466… fe80::a00:27ff:…   ff02::fb       MDNS   Standard query 0x0000 PTR 2.2.0.10.in-addr.arpa, "QM" question
  9 13:58:32.469… 10.0.2.15          224.0.0.251    MDNS   Standard query 0x0000 PTR 2.2.0.10.in-addr.arpa, "QM" question
 10 13:58:34.470… fe80::a00:27ff:…   ff02::fb       MDNS   Standard query 0x0000 PTR 2.2.0.10.in-addr.arpa, "QM" question
 11 13:58:34.472… 10.0.2.15          224.0.0.251    MDNS   Standard query 0x0000 PTR 2.2.0.10.in-addr.arpa, "QM" question
 12 13:58:36.258… 10.0.2.15          10.0.2.2       ARP    Who has 10.0.2.2? Tell 10.0.2.15
 13 13:58:36.258… 10.0.2.2           10.0.2.15      ARP    10.0.2.2 is at 52:54:00:12:35:02
 14 13:58:36.367… 10.0.2.15          10.0.2.2       FTP    Response: 220 wptsrv01.it-dept.local FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
 15 13:58:36.368… 10.0.2.2           10.0.2.15      TCP    37188 → ftp [ACK] Seq=225472002 Ack=1308437345 Win=65535 Len=0

⊞ Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
⊞ Ethernet II, Src: 10.0.2.15 (08:00:27:27:a9:7a), Dst: 10.0.2.2 (52:54:00:12:35:02)
⊞ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 145.72.246.10
⊞ User Datagram Protocol, Src Port: 60251 (60251), Dst Port: domain (53)
⊞ Domain Name System (query)

0000  52 54 00 12 35 02 08 00  27 27 a9 7a 08 00 45 00   RT..5... ''.z..E.
0010  00 43 98 5e 40 00 40 11  0e ea 0a 00 02 0f 91 48   .C.^@.@. .......H
0020  f6 0a eb 5b 00 35 00 2f  93 a2 07 0d 01 00 00 01   ...[.5./ ........
0030  00 00 00 00 00 00 01 32  01 32 01 30 02 31 30 07   .......2 .2.0.10.
0040  69 6e 2d 61 64 64 72 04  61 72 70 61 00 00 0c 00   in-addr. arpa....

netwerkcapture01    Packets: 40 · Displayed: 40 (100.0%) · Load time: 0:0.3    Profile: Default
```

Display filter





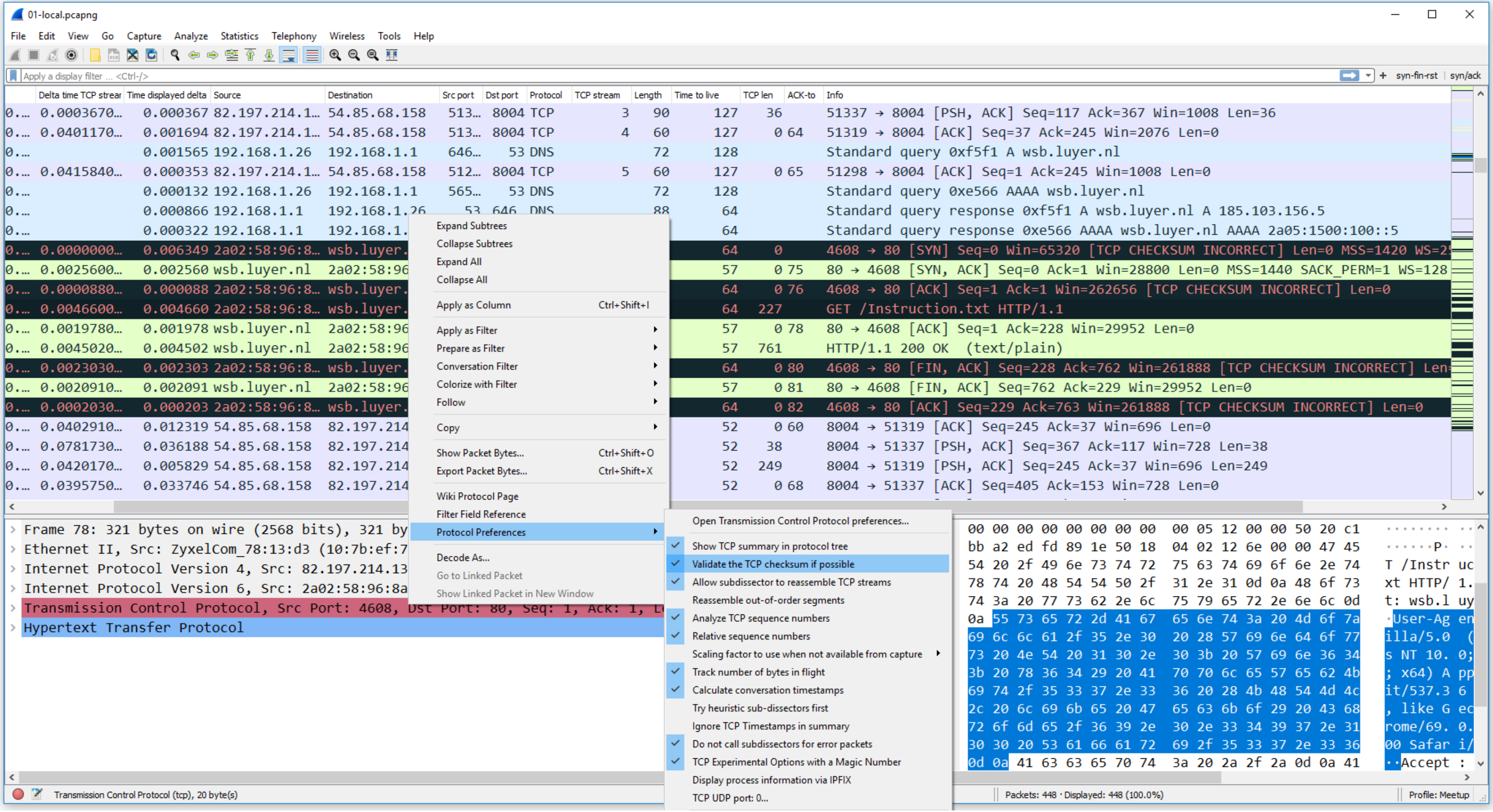
Read filter



```
Microsoft Windows [Version 10.0.17134.829]
(c) 2018 Microsoft Corporation. Alle rechten voorbehouden.

G:\>dumpcap
Capturing on 'Local Area Connection* 8'
File: C:\Users\LuyerAU\AppData\Local\Temp\wireshark_Local Area Connection- 8_2019070514401
1_a14436.pcapng
_
```

Capture filter

Dumpcap



```
    Delta time TCP strear Time displayed delta Source        Destination    Src port Dst port Protocol TCP stream Length Time to live TCP len ACK-to Info
0... 0.0003670...  0.000367 82.197.214.1... 54.85.68.158   513...  8004 TCP   3  90  127  36    51337 → 8004 [PSH, ACK] Seq=117 Ack=367 Win=1008 Len=36
0... 0.0401170...  0.001694 82.197.214.1... 54.85.68.158   513...  8004 TCP   4  60  127   0 64 51319 → 8004 [ACK] Seq=37 Ack=245 Win=2076 Len=0
0...               0.001565 192.168.1.26   192.168.1.1     646...    53 DNS      72  128        Standard query 0xf5f1 A wsb.luyer.nl
0... 0.0415840...  0.000353 82.197.214.1... 54.85.68.158   512...  8004 TCP   5  60  127   0 65 51298 → 8004 [ACK] Seq=1 Ack=245 Win=1008 Len=0
0...               0.000132 192.168.1.26   192.168.1.1     565...    53 DNS      72  128        Standard query 0xe566 AAAA wsb.luyer.nl
0...               0.000866 192.168.1.1    192.168.1.26     53   646  DNS      88   64        Standard query response 0xf5f1 A wsb.luyer.nl A 185.103.156.5
0...               0.000322 192.168.1.1    192.168.1.                              64        Standard query response 0xe566 AAAA wsb.luyer.nl AAAA 2a05:1500:100::5
0... 0.0000000...  0.006349 2a02:58:96:8... wsb.luyer.                             64   0     4608 → 80 [SYN] Seq=0 Win=65320 [TCP CHECKSUM INCORRECT] Len=0 MSS=1420 WS=2
0... 0.0025600...  0.002560 wsb.luyer.nl   2a02:58:96                              57   0 75  80 → 4608 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440 SACK_PERM=1 WS=128
0... 0.0000880...  0.000088 2a02:58:96:8... wsb.luyer.                             64   0 76  4608 → 80 [ACK] Seq=1 Ack=1 Win=262656 [TCP CHECKSUM INCORRECT] Len=0
0... 0.0046600...  0.004660 2a02:58:96:8... wsb.luyer.                             64 227     GET /Instruction.txt HTTP/1.1
0... 0.0019780...  0.001978 wsb.luyer.nl   2a02:58:96                              57   0 78  80 → 4608 [ACK] Seq=1 Ack=228 Win=29952 Len=0
0... 0.0045020...  0.004502 wsb.luyer.nl   2a02:58:96                              57 761     HTTP/1.1 200 OK  (text/plain)
0... 0.0023030...  0.002303 2a02:58:96:8... wsb.luyer.                             64   0 80  4608 → 80 [FIN, ACK] Seq=228 Ack=762 Win=261888 [TCP CHECKSUM INCORRECT] Len=
0... 0.0020910...  0.002091 wsb.luyer.nl   2a02:58:96                              57   0 81  80 → 4608 [FIN, ACK] Seq=762 Ack=229 Win=29952 Len=0
0... 0.0002030...  0.000203 2a02:58:96:8... wsb.luyer.                             64   0 82  4608 → 80 [ACK] Seq=229 Ack=763 Win=261888 [TCP CHECKSUM INCORRECT] Len=0
0... 0.0402910...  0.012319 54.85.68.158   82.197.214                              52   0 60  8004 → 51319 [ACK] Seq=245 Ack=37 Win=696 Len=0
0... 0.0781730...  0.036188 54.85.68.158   82.197.214                              52  38     8004 → 51337 [PSH, ACK] Seq=367 Ack=117 Win=728 Len=38
0... 0.0420170...  0.005829 54.85.68.158   82.197.214                              52 249     8004 → 51319 [PSH, ACK] Seq=245 Ack=37 Win=696 Len=249
0... 0.0395750...  0.033746 54.85.68.158   82.197.214                              52   0 68  8004 → 51337 [ACK] Seq=405 Ack=153 Win=728 Len=0
```

```
> Frame 78: 321 bytes on wire (2568 bits), 321 by
> Ethernet II, Src: ZyxelCom_78:13:d3 (10:7b:ef:7
> Internet Protocol Version 4, Src: 82.197.214.13
> Internet Protocol Version 6, Src: 2a02:58:96:8a
> Transmission Control Protocol, Src Port: 4608, Dst Port: 80, Seq: 1, Ack: 1, L
> Hypertext Transfer Protocol
```

- ☑ Show TCP summary in protocol tree
- ☑ Validate the TCP checksum if possible
- ☑ Allow subdissector to reassemble TCP streams
- ☐ Reassemble out-of-order segments
- ☑ Analyze TCP sequence numbers
- ☑ Relative sequence numbers
- Scaling factor to use when not available from capture
- ☑ Track number of bytes in flight
- ☑ Calculate conversation timestamps
- ☐ Try heuristic sub-dissectors first
- ☐ Ignore TCP Timestamps in summary
- ☑ Do not call subdissectors for error packets
- ☑ TCP Experimental Options with a Magic Number
- ☐ Display process information via IPFIX
- TCP UDP port: 0...

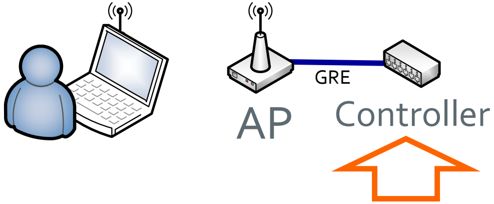
```
00 00 00 00 00 00 00 00  00 05 12 00 00 50 20 c1   ········· ··
bb a2 ed fd 89 1e 50 18  04 02 12 6e 00 00 47 45   ······P· ··
54 20 2f 49 6e 73 74 72  75 63 74 69 6f 6e 2e 74   T /Instr uc
78 74 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   xt HTTP/ 1.
74 3a 20 77 73 62 2e 6c  75 79 65 72 2e 6e 6c 0d   t: wsb.l uy
0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag en
69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (
73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0;
3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A pp
69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6
2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ec
72 6f 6d 65 2f 36 39 2e  30 2e 33 34 39 37 2e 31   rome/69. 0.
30 30 20 53 61 66 61 72  69 2f 35 33 37 2e 33 36   00 Safar i/
0d 0a 41 63 63 65 70 74  3a 20 2a 2f 2a 0d 0a 41   ··Accept :
```

Transmission Control Protocol (tcp), 20 byte(s)

Packets: 448 · Displayed: 448 (100.0%)

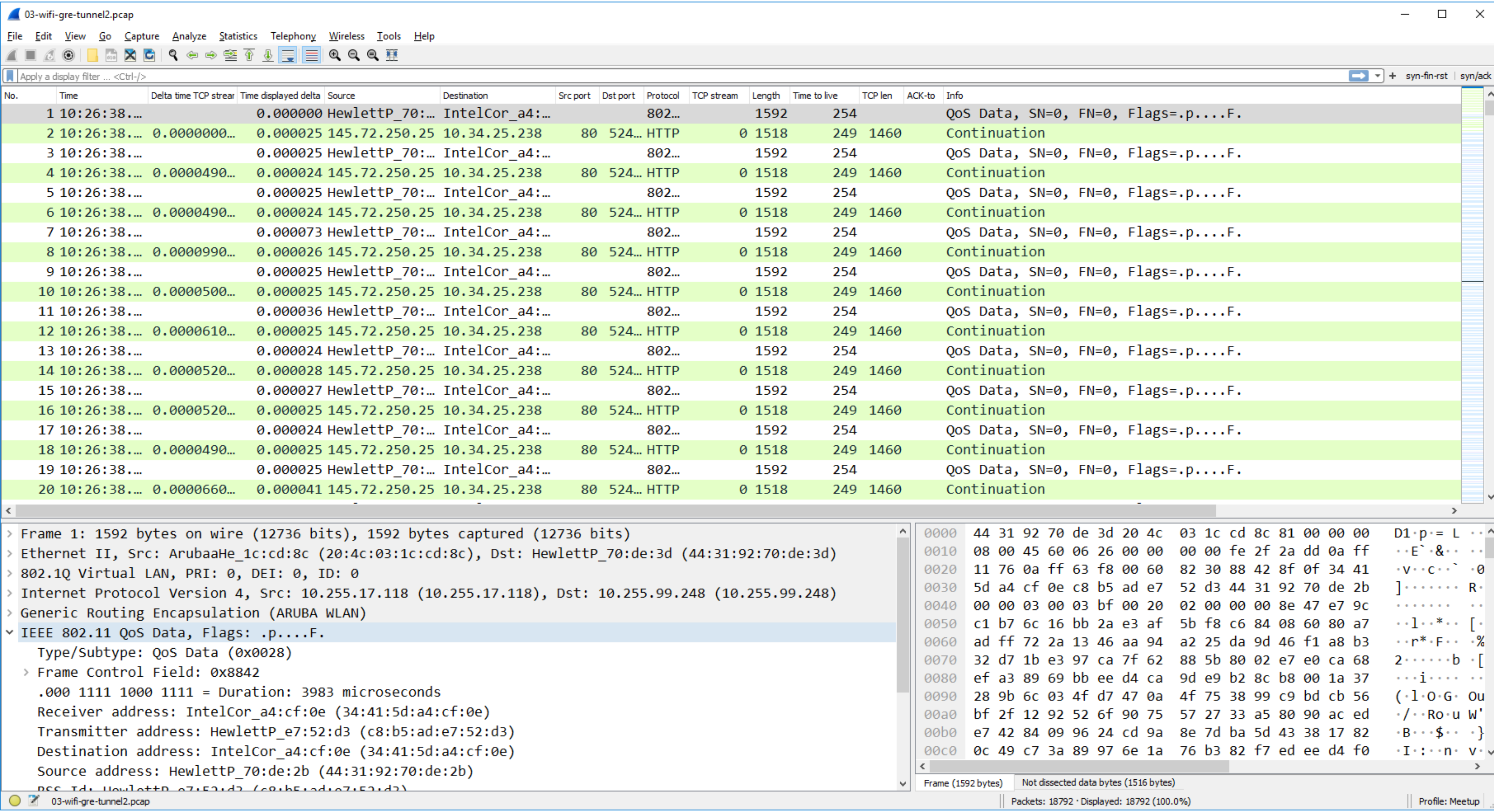
Profile: Meetup

Wi-Fi traffic using Controller



- Shows IEEE 802.11 data within GRE tunnel
- Shows Wi-Fi packets *actually* send & received by Access Point
- Plus unencrypted traffic leaving the tunnel
- Capturing 'from air' requires specialized hardware, multi channel capture

- For Wi-Fi capture on laptop – if supported by hardware – see: https://wiki.wireshark.org/CaptureSetup/WLAN



No.	Time	Delta time TCP strear	Time displayed delta	Source	Destination	Src port	Dst port	Protocol	TCP stream	Length	Time to live	TCP len	ACK-to	Info
1	10:26:38.…		0.000000	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
2	10:26:38.…	0.0000000…	0.000025	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
3	10:26:38.…		0.000025	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
4	10:26:38.…	0.0000490…	0.000024	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
5	10:26:38.…		0.000025	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
6	10:26:38.…	0.0000490…	0.000024	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
7	10:26:38.…		0.000073	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
8	10:26:38.…	0.0000990…	0.000026	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
9	10:26:38.…		0.000025	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
10	10:26:38.…	0.0000500…	0.000025	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
11	10:26:38.…		0.000036	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
12	10:26:38.…	0.0000610…	0.000025	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
13	10:26:38.…		0.000024	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
14	10:26:38.…	0.0000520…	0.000028	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
15	10:26:38.…		0.000027	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
16	10:26:38.…	0.0000520…	0.000025	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
17	10:26:38.…		0.000024	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
18	10:26:38.…	0.0000490…	0.000025	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation
19	10:26:38.…		0.000025	HewlettP_70:…	IntelCor_a4:…			802…		1592	254			QoS Data, SN=0, FN=0, Flags=.p....F.
20	10:26:38.…	0.0000660…	0.000041	145.72.250.25	10.34.25.238	80	524…	HTTP	0	1518	249	1460		Continuation

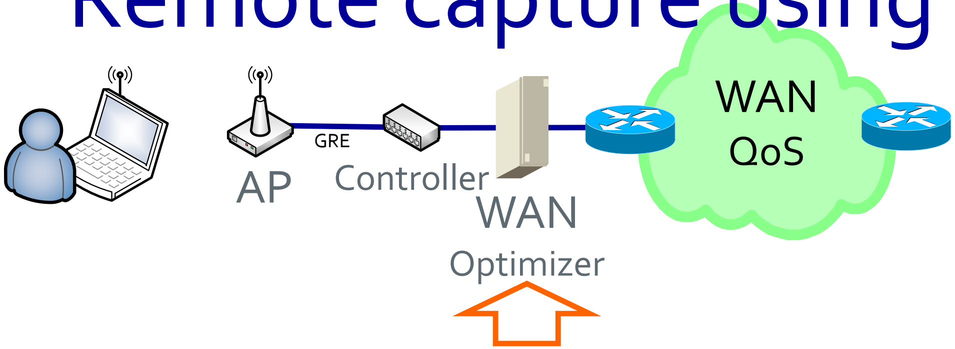
```
> Frame 1: 1592 bytes on wire (12736 bits), 1592 bytes captured (12736 bits)
> Ethernet II, Src: ArubaaHe_1c:cd:8c (20:4c:03:1c:cd:8c), Dst: HewlettP_70:de:3d (44:31:92:70:de:3d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
> Internet Protocol Version 4, Src: 10.255.17.118 (10.255.17.118), Dst: 10.255.99.248 (10.255.99.248)
> Generic Routing Encapsulation (ARUBA WLAN)
v IEEE 802.11 QoS Data, Flags: .p....F.
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8842
    .000 1111 1000 1111 = Duration: 3983 microseconds
    Receiver address: IntelCor_a4:cf:0e (34:41:5d:a4:cf:0e)
    Transmitter address: HewlettP_e7:52:d3 (c8:b5:ad:e7:52:d3)
    Destination address: IntelCor_a4:cf:0e (34:41:5d:a4:cf:0e)
    Source address: HewlettP_70:de:2b (44:31:92:70:de:2b)
    BSS Id: HewlettP_e7:52:d3 (c8:b5:ad:e7:52:d3)
```

```
0000  44 31 92 70 de 3d 20 4c  03 1c cd 8c 81 00 00 00   D1·p·= L ··
0010  08 00 45 60 06 26 00 00  00 00 fe 2f 2a dd 0a ff   ··E`·&·· ··
0020  11 76 0a ff 63 f8 00 60  82 30 88 42 8f 0f 34 41   ·v··c··` ·0
0030  5d a4 cf 0e c8 b5 ad e7  52 d3 44 31 92 70 de 2b   ]······· R·
0040  00 00 03 00 03 bf 00 20  02 00 00 00 8e 47 e7 9c   ········ ··
0050  c1 b7 6c 16 bb 2a e3 af  5b f8 c6 84 08 60 80 a7   ··l··*·· [·
0060  ad ff 72 2a 13 46 aa 94  a2 25 da 9d 46 f1 a8 b3   ··r*·F·· ·%
0070  32 d7 1b e3 97 ca 7f 62  88 5b 80 02 e7 e0 ca 68   2······b ·[
0080  ef a3 89 69 bb ee d4 ca  9d e9 b2 8c b8 00 1a 37   ···i···· ··
0090  28 9b 6c 03 4f d7 47 0a  4f 75 38 99 c9 bd cb 56   (·l·O·G· Ou
00a0  bf 2f 12 92 52 6f 90 75  57 27 33 a5 80 90 ac ed   ·/··Ro·u W'
00b0  e7 42 84 09 96 24 cd 9a  8e 7d ba 5d 43 38 17 82   ·B···$·· ·}
00c0  0c 49 c7 3a 89 97 6e 1a  76 b3 82 f7 ed ee d4 f0   ·I·:··n· v·
```

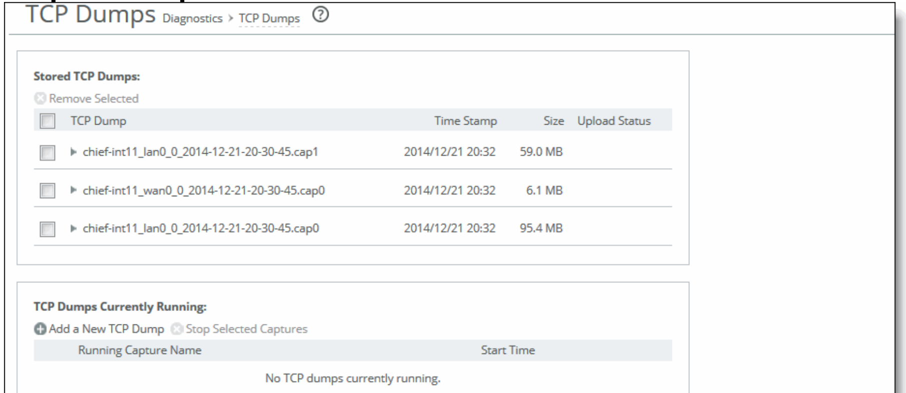
Frame (1592 bytes) | Not dissected data bytes (1516 bytes)

03-wifi-gre-tunnel2.pcap | Packets: 18792 · Displayed: 18792 (100.0%) | Profile: Meetup

Remote capture using WAN Optimizer



- Do ‘remote capture’ using WAN optimizer, saves a lot of (traveling) time
- Most boxes (WAN Opt, Firewalls, Load balancers, proxies, …) are Linux based and provide a (GUI) interface to tcpdump command.



TCP Dumps Diagnostics › TCP Dumps

Stored TCP Dumps:

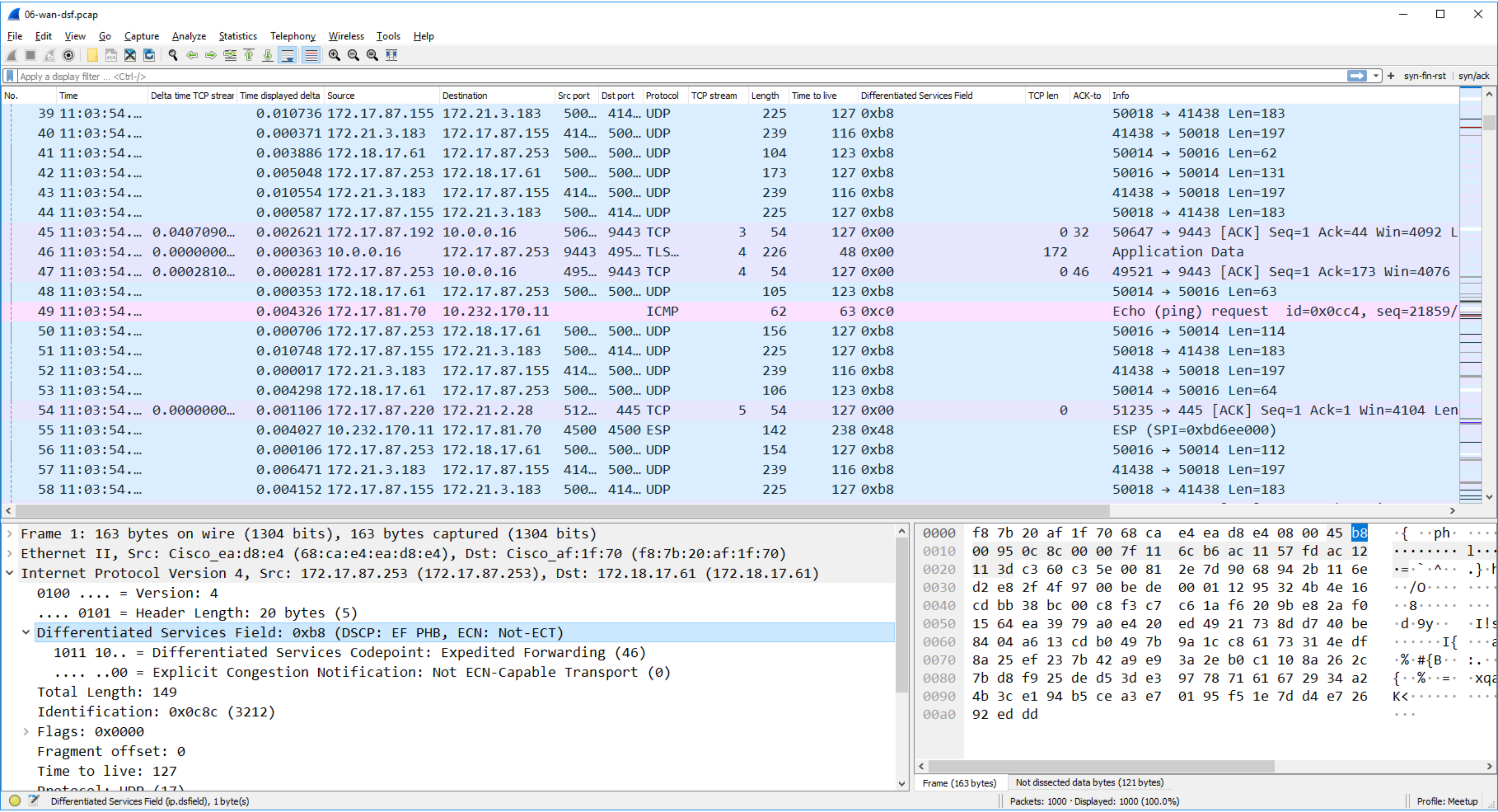
Remove Selected

□	TCP Dump	Time Stamp	Size	Upload Status
□	▸ chief-int11_lan0_0_2014-12-21-20-30-45.cap1	2014/12/21 20:32	59.0 MB	
□	▸ chief-int11_wan0_0_2014-12-21-20-30-45.cap0	2014/12/21 20:32	6.1 MB	
□	▸ chief-int11_lan0_0_2014-12-21-20-30-45.cap0	2014/12/21 20:32	95.4 MB	

TCP Dumps Currently Running:

Add a New TCP Dump Stop Selected Captures

Running Capture Name	Start Time
No TCP dumps currently running.	



06-wan-dsf.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
+ syn-fin-rst syn/ack

No.	Time	Delta time TCP strear	Time displayed delta	Source	Destination	Src port	Dst port	Protocol	TCP stream	Length	Time to live	Differentiated Services Field	TCP len	ACK-to	Info
39	11:03:54.…		0.010736	172.17.87.155	172.21.3.183	500…	414…	UDP		225	127	0xb8			50018 → 41438 Len=183
40	11:03:54.…		0.000371	172.21.3.183	172.17.87.155	414…	500…	UDP		239	116	0xb8			41438 → 50018 Len=197
41	11:03:54.…		0.003886	172.18.17.61	172.17.87.253	500…	500…	UDP		104	123	0xb8			50014 → 50016 Len=62
42	11:03:54.…		0.005048	172.17.87.253	172.18.17.61	500…	500…	UDP		173	127	0xb8			50016 → 50014 Len=131
43	11:03:54.…		0.010554	172.21.3.183	172.17.87.155	414…	500…	UDP		239	116	0xb8			41438 → 50018 Len=197
44	11:03:54.…		0.000587	172.17.87.155	172.21.3.183	500…	414…	UDP		225	127	0xb8			50018 → 41438 Len=183
45	11:03:54.…	0.0407090…	0.002621	172.17.87.192	10.0.0.16	506…	9443	TCP	3	54	127	0x00	0	32	50647 → 9443 [ACK] Seq=1 Ack=44 Win=4092 L
46	11:03:54.…	0.0000000…	0.000363	10.0.0.16	172.17.87.253	9443	495…	TLS…	4	226	48	0x00	172		Application Data
47	11:03:54.…	0.0002810…	0.000281	172.17.87.253	10.0.0.16	495…	9443	TCP	4	54	127	0x00	0	46	49521 → 9443 [ACK] Seq=1 Ack=173 Win=4076
48	11:03:54.…		0.000353	172.18.17.61	172.17.87.253	500…	500…	UDP		105	123	0xb8			50014 → 50016 Len=63
49	11:03:54.…		0.004326	172.17.81.70	10.232.170.11			ICMP		62	63	0xc0			Echo (ping) request id=0x0cc4, seq=21859/
50	11:03:54.…		0.000706	172.17.87.253	172.18.17.61	500…	500…	UDP		156	127	0xb8			50016 → 50014 Len=114
51	11:03:54.…		0.010748	172.17.87.155	172.21.3.183	500…	414…	UDP		225	127	0xb8			50018 → 41438 Len=183
52	11:03:54.…		0.000017	172.21.3.183	172.17.87.155	414…	500…	UDP		239	116	0xb8			41438 → 50018 Len=197
53	11:03:54.…		0.004298	172.18.17.61	172.17.87.253	500…	500…	UDP		106	123	0xb8			50014 → 50016 Len=64
54	11:03:54.…	0.0000000…	0.001106	172.17.87.220	172.21.2.28	512…	445	TCP	5	54	127	0x00	0		51235 → 445 [ACK] Seq=1 Ack=1 Win=4104 Len
55	11:03:54.…		0.004027	10.232.170.11	172.17.81.70	4500	4500	ESP		142	238	0x48			ESP (SPI=0xbd6ee000)
56	11:03:54.…		0.000106	172.17.87.253	172.18.17.61	500…	500…	UDP		154	127	0xb8			50016 → 50014 Len=112
57	11:03:54.…		0.006471	172.21.3.183	172.17.87.155	414…	500…	UDP		239	116	0xb8			41438 → 50018 Len=197
58	11:03:54.…		0.004152	172.17.87.155	172.21.3.183	500…	414…	UDP		225	127	0xb8			50018 → 41438 Len=183

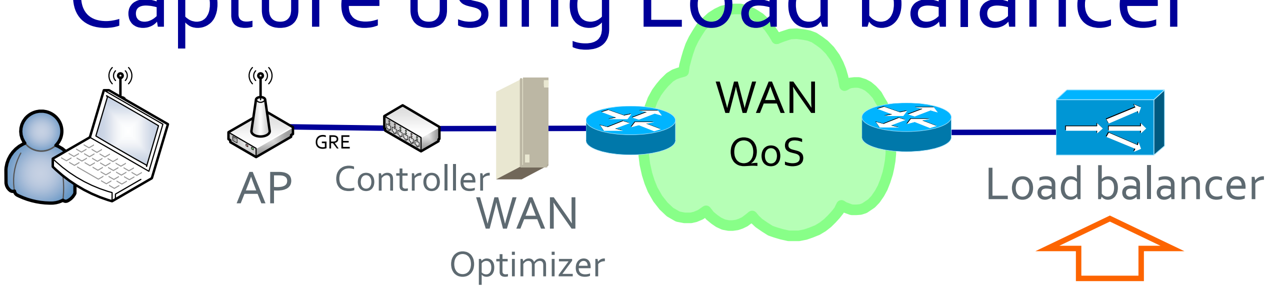
```
> Frame 1: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits)
> Ethernet II, Src: Cisco_ea:d8:e4 (68:ca:e4:ea:d8:e4), Dst: Cisco_af:1f:70 (f8:7b:20:af:1f:70)
v Internet Protocol Version 4, Src: 172.17.87.253 (172.17.87.253), Dst: 172.18.17.61 (172.18.17.61)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
      1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 149
    Identification: 0x0c8c (3212)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 127
    Protocol: UDP (17)
```

```
0000  f8 7b 20 af 1f 70 68 ca  e4 ea d8 e4 08 00 45 b8   ·{ ··ph· ····
0010  00 95 0c 8c 00 00 7f 11  6c b6 ac 11 57 fd ac 12   ········ l···
0020  11 3d c3 60 c3 5e 00 81  2e 7d 90 68 94 2b 11 6e   ·=·`·^·· .}·h
0030  d2 e8 2f 4f 97 00 be de  00 01 12 95 32 4b 4e 16   ··/O···· ····
0040  cd bb 38 bc 00 c8 f3 c7  c6 1a f6 20 9b e8 2a f0   ··8····· ···
0050  15 64 ea 39 79 a0 e4 20  ed 49 21 73 8d d7 40 be   ·d·9y··  ·I!s
0060  84 04 a6 13 cd b0 49 7b  9a 1c c8 61 73 31 4e df   ······I{ ···a
0070  8a 25 ef 23 7b 42 a9 e9  3a 2e b0 c1 10 8a 26 2c   ·%·#{B·· :.··
0080  7b d8 f9 25 de d5 3d e3  97 78 71 61 67 29 34 a2   {··%··=· ·xqa
0090  4b 3c e1 94 b5 ce a3 e7  01 95 f5 1e 7d d4 e7 26   K<······ ····
00a0  92 ed dd                                           ···
```

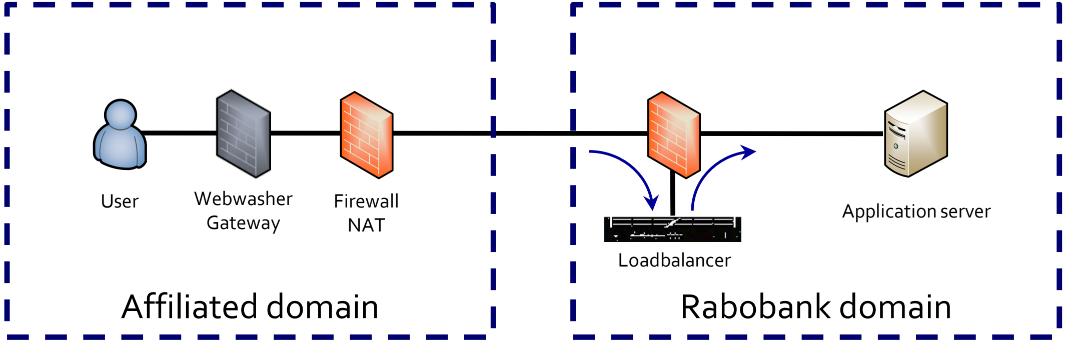
Frame (163 bytes) | Not dissected data bytes (121 bytes)

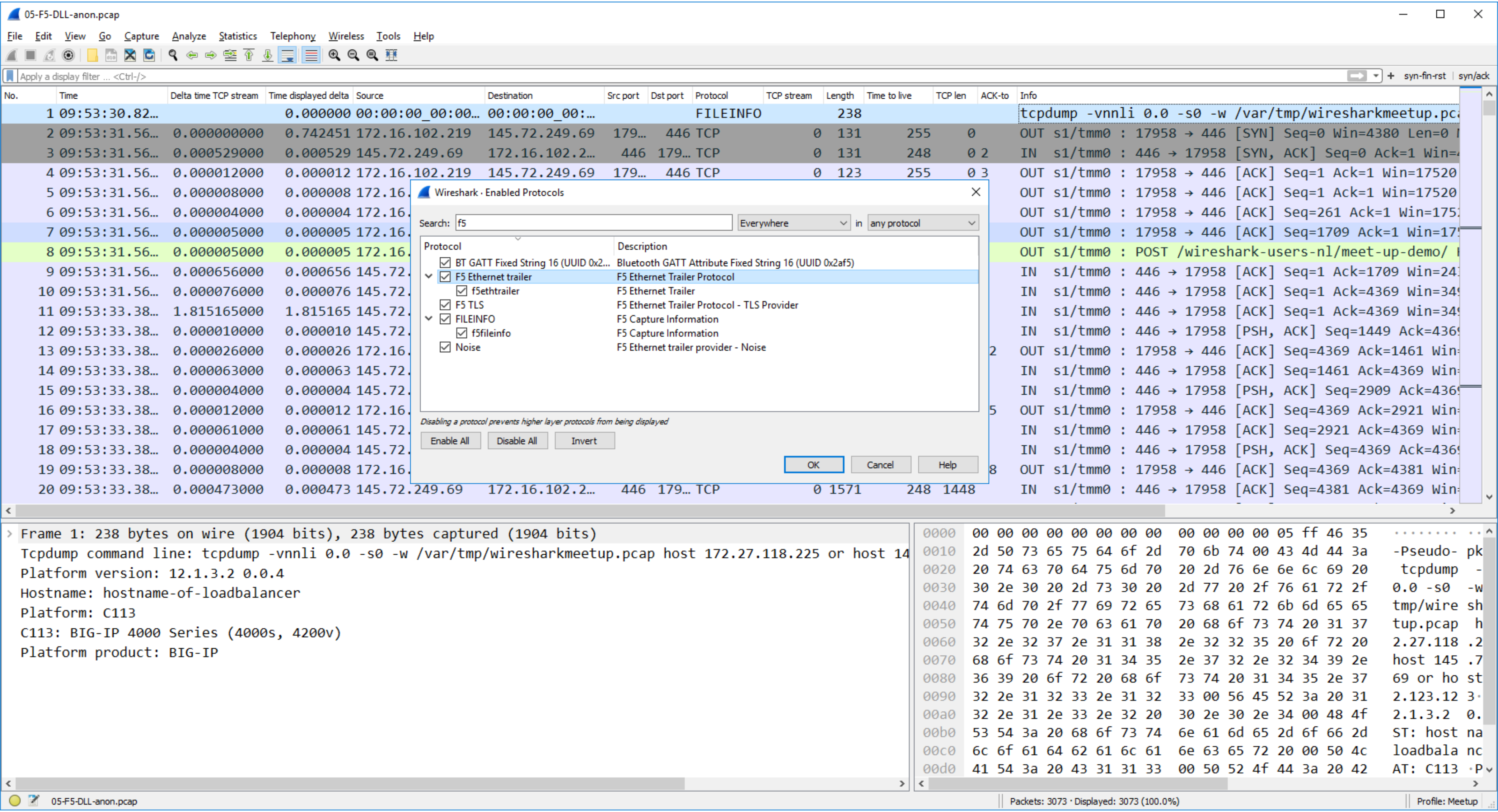
Differentiated Services Field (ip.dsfield), 1 byte(s) | Packets: 1000 · Displayed: 1000 (100.0%) | Profile: Meetup

Capture using Load balancer



- Some manufactures add extra info into the capture file
- For F5 Networks: enable protocol (menu Analyze / Enabled Protocols)
- Example case:




05-F5-DLL-anon.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
syn-fin-rst
syn/ack

```
No.  Time          Delta time TCP stream  Time displayed delta  Source           Destination      Src port  Dst port  Protocol  TCP stream  Length  Time to live  TCP len  ACK-to  Info
  1 09:53:30.82…                 0.000000 00:00:00_00:00… 00:00:00_00:…       FILEINFO         238                           tcpdump -vnnli 0.0 -s0 -w /var/tmp/wiresharkmeetup.pca
  2 09:53:31.56… 0.000000000 0.742451 172.16.102.219 145.72.249.69  179…  446 TCP    0  131   255    0     OUT s1/tmm0 : 17958 → 446 [SYN] Seq=0 Win=4380 Len=0 I
  3 09:53:31.56… 0.000529000 0.000529 145.72.249.69  172.16.102.2…  446 179… TCP    0  131   248    0 2   IN  s1/tmm0 : 446 → 17958 [SYN, ACK] Seq=0 Ack=1 Win=
  4 09:53:31.56… 0.000012000 0.000012 172.16.102.219 145.72.249.69  179…  446 TCP    0  123   255    0 3   OUT s1/tmm0 : 17958 → 446 [ACK] Seq=1 Ack=1 Win=17520
  5 09:53:31.56… 0.000008000 0.000008 172.16.                                                         OUT s1/tmm0 : 17958 → 446 [ACK] Seq=1 Ack=1 Win=17520
  6 09:53:31.56… 0.000004000 0.000004 172.16.                                                         OUT s1/tmm0 : 17958 → 446 [ACK] Seq=261 Ack=1 Win=175
  7 09:53:31.56… 0.000005000 0.000005 172.16.                                                         OUT s1/tmm0 : 17958 → 446 [ACK] Seq=1709 Ack=1 Win=17
  8 09:53:31.56… 0.000005000 0.000005 172.16.                                                         OUT s1/tmm0 : POST /wireshark-users-nl/meet-up-demo/ I
  9 09:53:31.56… 0.000656000 0.000656 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [ACK] Seq=1 Ack=1709 Win=24
 10 09:53:31.56… 0.000076000 0.000076 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [ACK] Seq=1 Ack=4369 Win=34
 11 09:53:33.38… 1.815165000 1.815165 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [ACK] Seq=1 Ack=4369 Win=34
 12 09:53:33.38… 0.000010000 0.000010 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [PSH, ACK] Seq=1449 Ack=436
 13 09:53:33.38… 0.000026000 0.000026 172.16.                                                    2    OUT s1/tmm0 : 17958 → 446 [ACK] Seq=4369 Ack=1461 Win
 14 09:53:33.38… 0.000063000 0.000063 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [ACK] Seq=1461 Ack=4369 Win
 15 09:53:33.38… 0.000004000 0.000004 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [PSH, ACK] Seq=2909 Ack=436
 16 09:53:33.38… 0.000012000 0.000012 172.16.                                                    5    OUT s1/tmm0 : 17958 → 446 [ACK] Seq=4369 Ack=2921 Win
 17 09:53:33.38… 0.000061000 0.000061 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [ACK] Seq=2921 Ack=4369 Win
 18 09:53:33.38… 0.000004000 0.000004 145.72.                                                         IN  s1/tmm0 : 446 → 17958 [PSH, ACK] Seq=4369 Ack=436
 19 09:53:33.38… 0.000008000 0.000008 172.16.                                                    8    OUT s1/tmm0 : 17958 → 446 [ACK] Seq=4369 Ack=4381 Win
 20 09:53:33.38… 0.000473000 0.000473 145.72.249.69  172.16.102.2…  446 179… TCP    0 1571   248 1448     IN  s1/tmm0 : 446 → 17958 [ACK] Seq=4381 Ack=4369 Win
```

Wireshark · Enabled Protocols

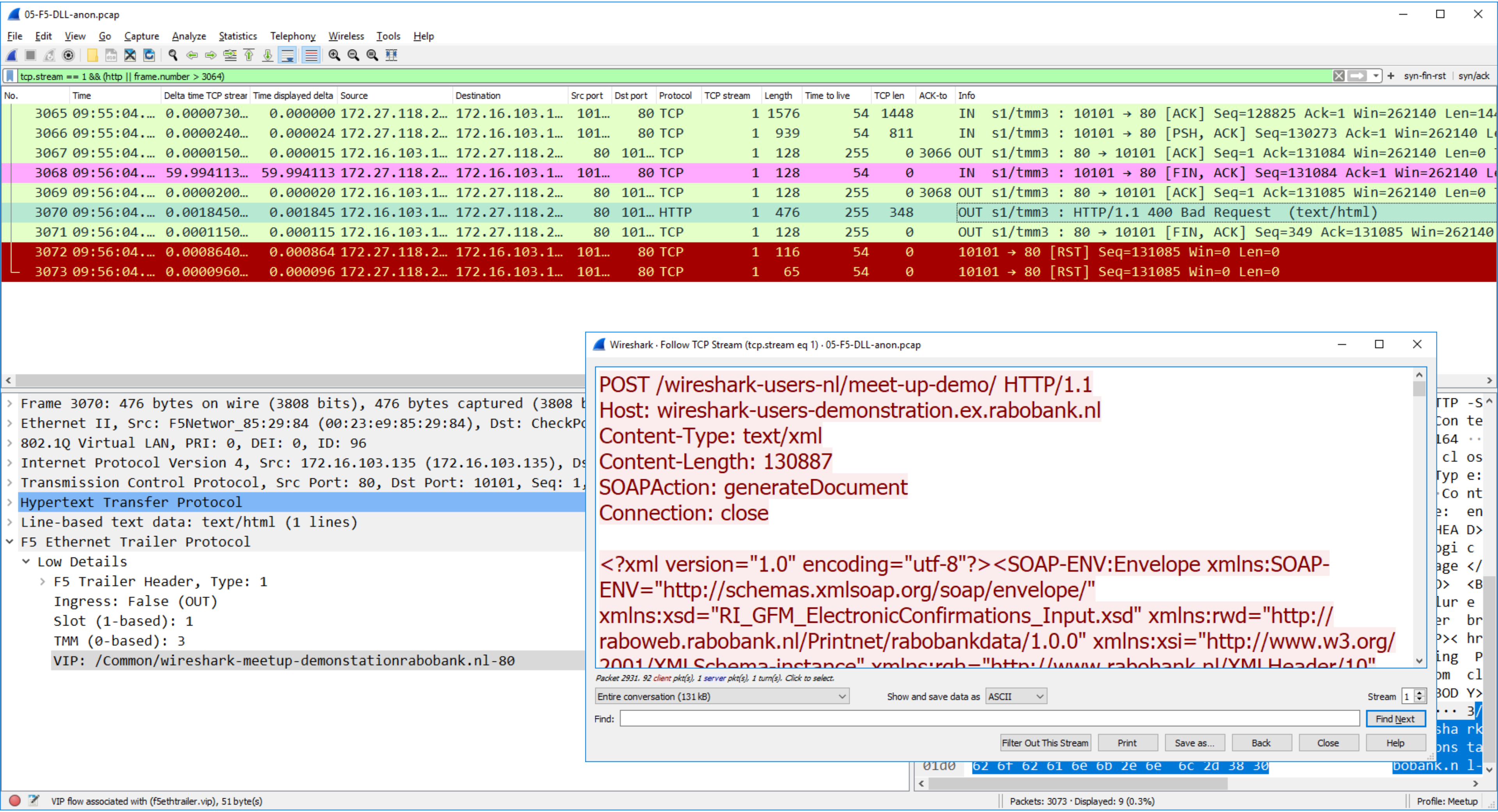
Search: f5 Everywhere in any protocol

Protocol	Description
☑ BT GATT Fixed String 16 (UUID 0x2…	Bluetooth GATT Attribute Fixed String 16 (UUID 0x2af5)
☑ F5 Ethernet trailer	F5 Ethernet Trailer Protocol
☑ f5ethtrailer	F5 Ethernet Trailer
☑ F5 TLS	F5 Ethernet Trailer Protocol - TLS Provider
☑ FILEINFO	F5 Capture Information
☑ f5fileinfo	F5 Capture Information
☑ Noise	F5 Ethernet trailer provider - Noise

Disabling a protocol prevents higher layer protocols from being displayed

```
Frame 1: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)
Tcpdump command line: tcpdump -vnnli 0.0 -s0 -w /var/tmp/wiresharkmeetup.pcap host 172.27.118.225 or host 14
Platform version: 12.1.3.2 0.0.4
Hostname: hostname-of-loadbalancer
Platform: C113
C113: BIG-IP 4000 Series (4000s, 4200v)
Platform product: BIG-IP
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 05 ff 46 35   ········ ··
0010  2d 50 73 65 75 64 6f 2d  70 6b 74 00 43 4d 44 3a   -Pseudo- pk
0020  20 74 63 70 64 75 6d 70  20 2d 76 6e 6e 6c 69 20    tcpdump -
0030  30 2e 30 20 2d 73 30 20  2d 77 20 2f 76 61 72 2f   0.0 -s0  -w
0040  74 6d 70 2f 77 69 72 65  73 68 61 72 6b 6d 65 65   tmp/wire sh
0050  74 75 70 2e 70 63 61 70  20 68 6f 73 74 20 31 37   tup.pcap  h
0060  32 2e 32 37 2e 31 31 38  2e 32 32 35 20 6f 72 20   2.27.118 .2
0070  68 6f 73 74 20 31 34 35  2e 37 32 2e 32 34 39 2e   host 145 .7
0080  36 39 20 6f 72 20 68 6f  73 74 20 31 34 35 2e 37   69 or ho st
0090  32 2e 31 32 33 2e 31 32  33 00 56 45 52 3a 20 31   2.123.12 3·
00a0  32 2e 31 2e 33 2e 32 20  30 2e 30 2e 34 00 48 4f   2.1.3.2  0.
00b0  53 54 3a 20 68 6f 73 74  6e 61 6d 65 2d 6f 66 2d   ST: host na
00c0  6c 6f 61 64 62 61 6c 61  6e 63 65 72 20 00 50 4c   loadbala nc
00d0  41 54 3a 20 43 31 31 33  00 50 52 4f 44 3a 20 42   AT: C113 ·P
```



05-F5-DLL-anon.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
+ syn-fin-rst | syn/ack

```
tcp.stream == 1 && (http || frame.number > 3064)
```

```
No.  Time          Delta time TCP strear  Time displayed delta  Source          Destination     Src port  Dst port  Protocol  TCP stream  Length  Time to live  TCP len  ACK-to  Info
3065 09:55:04.... 0.0000730...  0.000000 172.27.118.2... 172.16.103.1... 101...   80 TCP    1 1576  54 1448      IN  s1/tmm3 : 10101 → 80 [ACK] Seq=128825 Ack=1 Win=262140 Len=14
3066 09:55:04.... 0.0000240...  0.000024 172.27.118.2... 172.16.103.1... 101...   80 TCP    1  939  54  811      IN  s1/tmm3 : 10101 → 80 [PSH, ACK] Seq=130273 Ack=1 Win=262140 L
3067 09:55:04.... 0.0000150...  0.000015 172.16.103.1... 172.27.118.2...  80 101... TCP    1  128 255    0 3066 OUT s1/tmm3 : 80 → 10101 [ACK] Seq=1 Ack=131084 Win=262140 Len=0
3068 09:56:04.... 59.994113... 59.994113 172.27.118.2... 172.16.103.1... 101...   80 TCP    1  128  54    0      IN  s1/tmm3 : 10101 → 80 [FIN, ACK] Seq=131084 Ack=1 Win=262140 L
3069 09:56:04.... 0.0000200...  0.000020 172.16.103.1... 172.27.118.2...  80 101... TCP    1  128 255    0 3068 OUT s1/tmm3 : 80 → 10101 [ACK] Seq=1 Ack=131085 Win=262140 Len=0
3070 09:56:04.... 0.0018450...  0.001845 172.16.103.1... 172.27.118.2...  80 101... HTTP   1  476 255  348      OUT s1/tmm3 : HTTP/1.1 400 Bad Request  (text/html)
3071 09:56:04.... 0.0001150...  0.000115 172.16.103.1... 172.27.118.2...  80 101... TCP    1  128 255    0      OUT s1/tmm3 : 80 → 10101 [FIN, ACK] Seq=349 Ack=131085 Win=262140
3072 09:56:04.... 0.0008640...  0.000864 172.27.118.2... 172.16.103.1... 101...   80 TCP    1  116  54    0      10101 → 80 [RST] Seq=131085 Win=0 Len=0
3073 09:56:04.... 0.0000960...  0.000096 172.27.118.2... 172.16.103.1... 101...   80 TCP    1   65  54    0      10101 → 80 [RST] Seq=131085 Win=0 Len=0
```

```
> Frame 3070: 476 bytes on wire (3808 bits), 476 bytes captured (3808 b
> Ethernet II, Src: F5Networ_85:29:84 (00:23:e9:85:29:84), Dst: CheckPo
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 96
> Internet Protocol Version 4, Src: 172.16.103.135 (172.16.103.135), Ds
> Transmission Control Protocol, Src Port: 80, Dst Port: 10101, Seq: 1,
> Hypertext Transfer Protocol
> Line-based text data: text/html (1 lines)
v F5 Ethernet Trailer Protocol
  v Low Details
    > F5 Trailer Header, Type: 1
      Ingress: False (OUT)
      Slot (1-based): 1
      TMM (0-based): 3
      VIP: /Common/wireshark-meetup-demonstationrabobank.nl-80
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · 05-F5-DLL-anon.pcap

```
POST /wireshark-users-nl/meet-up-demo/ HTTP/1.1
Host: wireshark-users-demonstration.ex.rabobank.nl
Content-Type: text/xml
Content-Length: 130887
SOAPAction: generateDocument
Connection: close

<?xml version="1.0" encoding="utf-8"?><SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="RI_GFM_ElectronicConfirmations_Input.xsd" xmlns:rwd="http://
raboweb.rabobank.nl/Printnet/rabobankdata/1.0.0" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xmlns:rgh="http://www.rabobank.nl/XMLHeader/10"
```

Packet 2931. 92 client pkt(s), 1 server pkt(s), 1 turn(s). Click to select.

Entire conversation (131 kB)   Show and save data as ASCII   Stream 1

Find:
Find Next
Filter Out This Stream Print Save as... Back Close Help

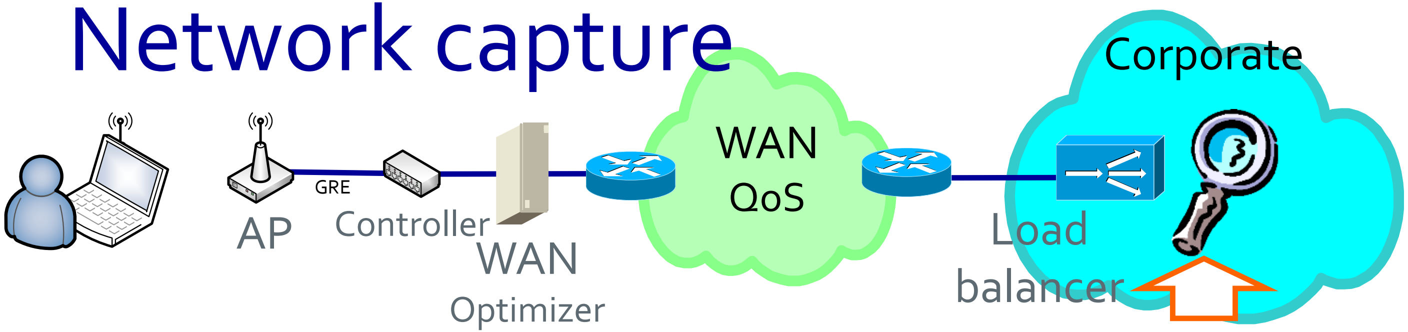
```
01d0  62 6f 62 61 6e 6b 2e 6e  6c 2d 38 30   bobank.n l-
```

VIP flow associated with (f5ethtrailer.vip), 51 byte(s)

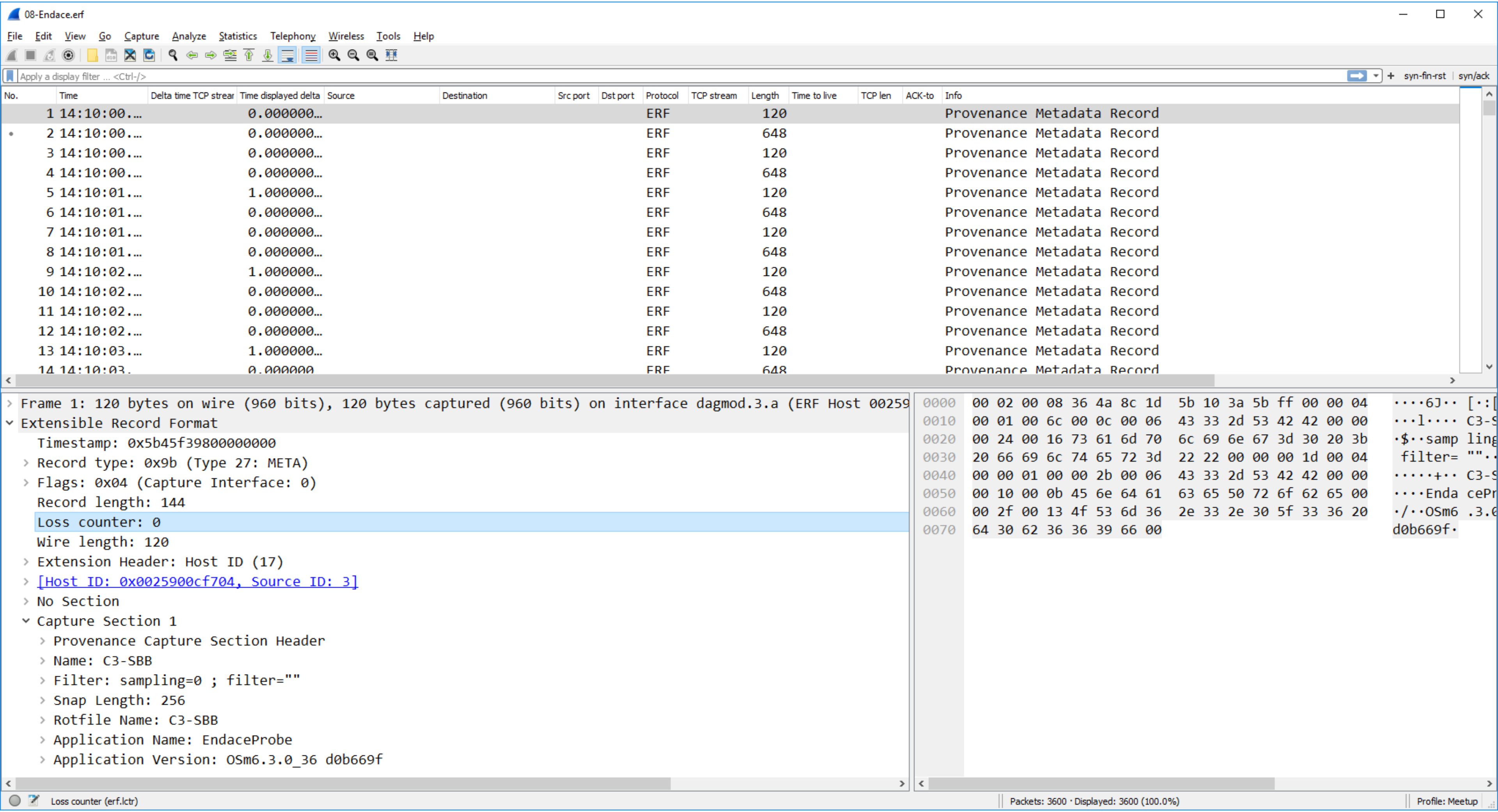
Packets: 3073 · Displayed: 9 (0.3%)

Profile: Meetup

Network capture



- Using Mirror port on switch / router
- Better: specialized hardware
- Have a history by using rotation files
- High speeds: may need to snap packets or apply specific filter
- Example: extra info in ERF file format by Endace



No.	Time	Delta time TCP strear	Time displayed delta	Source	Destination	Src port	Dst port	Protocol	TCP stream	Length	Time to live	TCP len	ACK-to	Info
1	14:10:00.…		0.000000…					ERF		120				Provenance Metadata Record
2	14:10:00.…		0.000000…					ERF		648				Provenance Metadata Record
3	14:10:00.…		0.000000…					ERF		120				Provenance Metadata Record
4	14:10:00.…		0.000000…					ERF		648				Provenance Metadata Record
5	14:10:01.…		1.000000…					ERF		120				Provenance Metadata Record
6	14:10:01.…		0.000000…					ERF		648				Provenance Metadata Record
7	14:10:01.…		0.000000…					ERF		120				Provenance Metadata Record
8	14:10:01.…		0.000000…					ERF		648				Provenance Metadata Record
9	14:10:02.…		1.000000…					ERF		120				Provenance Metadata Record
10	14:10:02.…		0.000000…					ERF		648				Provenance Metadata Record
11	14:10:02.…		0.000000…					ERF		120				Provenance Metadata Record
12	14:10:02.…		0.000000…					ERF		648				Provenance Metadata Record
13	14:10:03.…		1.000000…					ERF		120				Provenance Metadata Record
14	14:10:03.…		0.000000…					ERF		648				Provenance Metadata Record

```
> Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface dagmod.3.a (ERF Host 00259
v Extensible Record Format
    Timestamp: 0x5b45f39800000000
  > Record type: 0x9b (Type 27: META)
  > Flags: 0x04 (Capture Interface: 0)
    Record length: 144
    Loss counter: 0
    Wire length: 120
  > Extension Header: Host ID (17)
  > [Host ID: 0x0025900cf704, Source ID: 3]
  > No Section
  v Capture Section 1
    > Provenance Capture Section Header
    > Name: C3-SBB
    > Filter: sampling=0 ; filter=""
    > Snap Length: 256
    > Rotfile Name: C3-SBB
    > Application Name: EndaceProbe
    > Application Version: OSm6.3.0_36 d0b669f
```

```
0000  00 02 00 08 36 4a 8c 1d  5b 10 3a 5b ff 00 00 04   ····6J·· [·:[
0010  00 01 00 6c 00 0c 00 06  43 33 2d 53 42 42 00 00   ···l···· C3-S
0020  00 24 00 16 73 61 6d 70  6c 69 6e 67 3d 30 20 3b   ·$··samp ling
0030  20 66 69 6c 74 65 72 3d  22 22 00 00 00 1d 00 04    filter= ""··
0040  00 00 01 00 00 2b 00 06  43 33 2d 53 42 42 00 00   ·····+·· C3-S
0050  00 10 00 0b 45 6e 64 61  63 65 50 72 6f 62 65 00   ····Enda cePr
0060  00 2f 00 13 4f 53 6d 36  2e 33 2e 30 5f 33 36 20   ·/··OSm6 .3.0
0070  64 30 62 36 36 39 66 00                            d0b669f·
```

Loss counter (erf.lctr)

Packets: 3600 · Displayed: 3600 (100.0%)

Profile: Meetup

Tap versus Port Mirroring

Tap

- + Propagates all link level errors to sniffer
  (not required for application debugging)
- + Quick and easy used locally
- + Meets security requirements
- + No influence on dataflow or equipment

- – Network needs to be interrupted (twice)

Port Mirroring (SPAN)

- + No interruption of service
- + Cheap and easy to implement

- – Link level errors not visible
- – Packet order and timing is *not* guaranteed
- – SPAN is handled with low priority, thus copied packets may be dropped (this is not reported or measured)

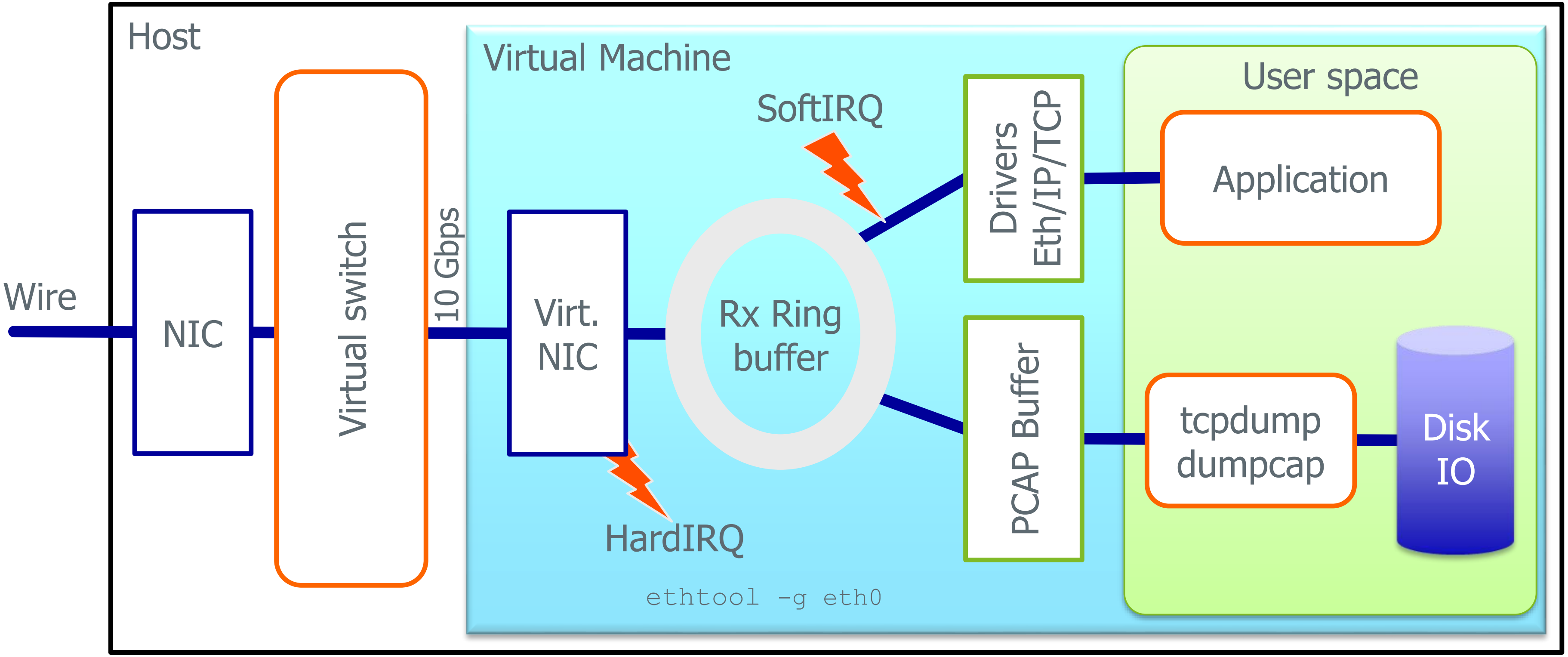
Software based network capture

e.g. dumpcap, tcpdump, netsh trace

- + Very easy to use at moments notice
- + Cheap and easy to implement
- + No interruption of service
- + Capture localhost traffic, e.g. apps running in a (Docker) container

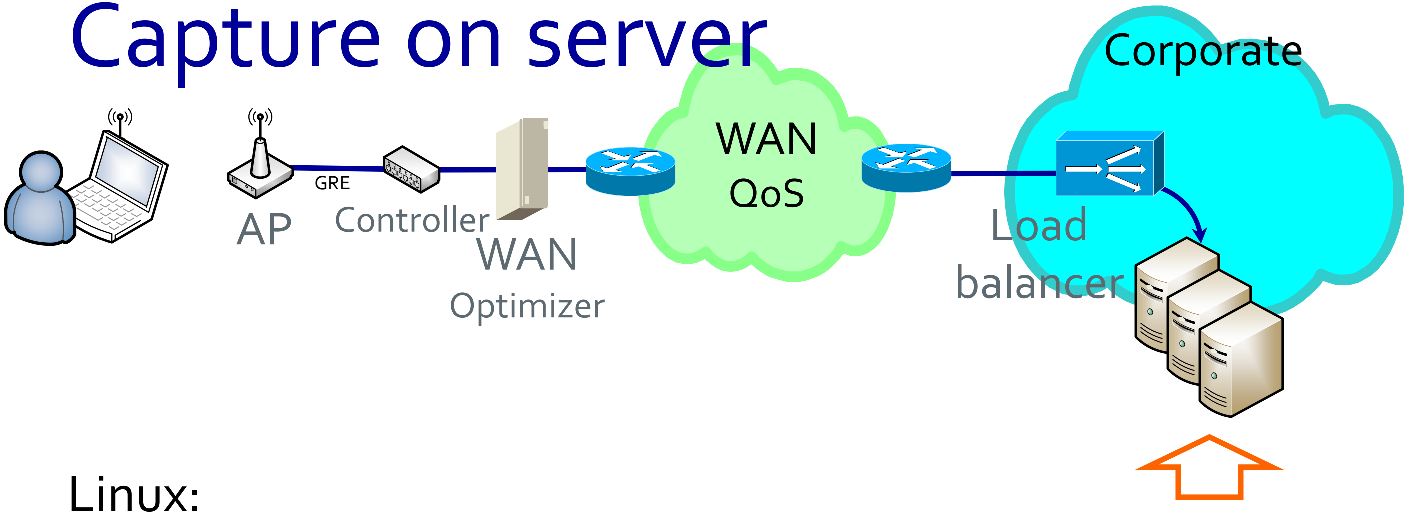
- – Requires administrative rights (sudo)
- – Extra load on the server (CPU, disk IO) may influence the behavior of the application
- – OS Kernel must be tuned when NIC(s) operates at 10 Gbps
  Dropped packets in *kernel* due to (ring) buffer overrun makes analysis very hard

RX capture mechanism (simplified)



```
ethtool -g eth0
```

Capture on server

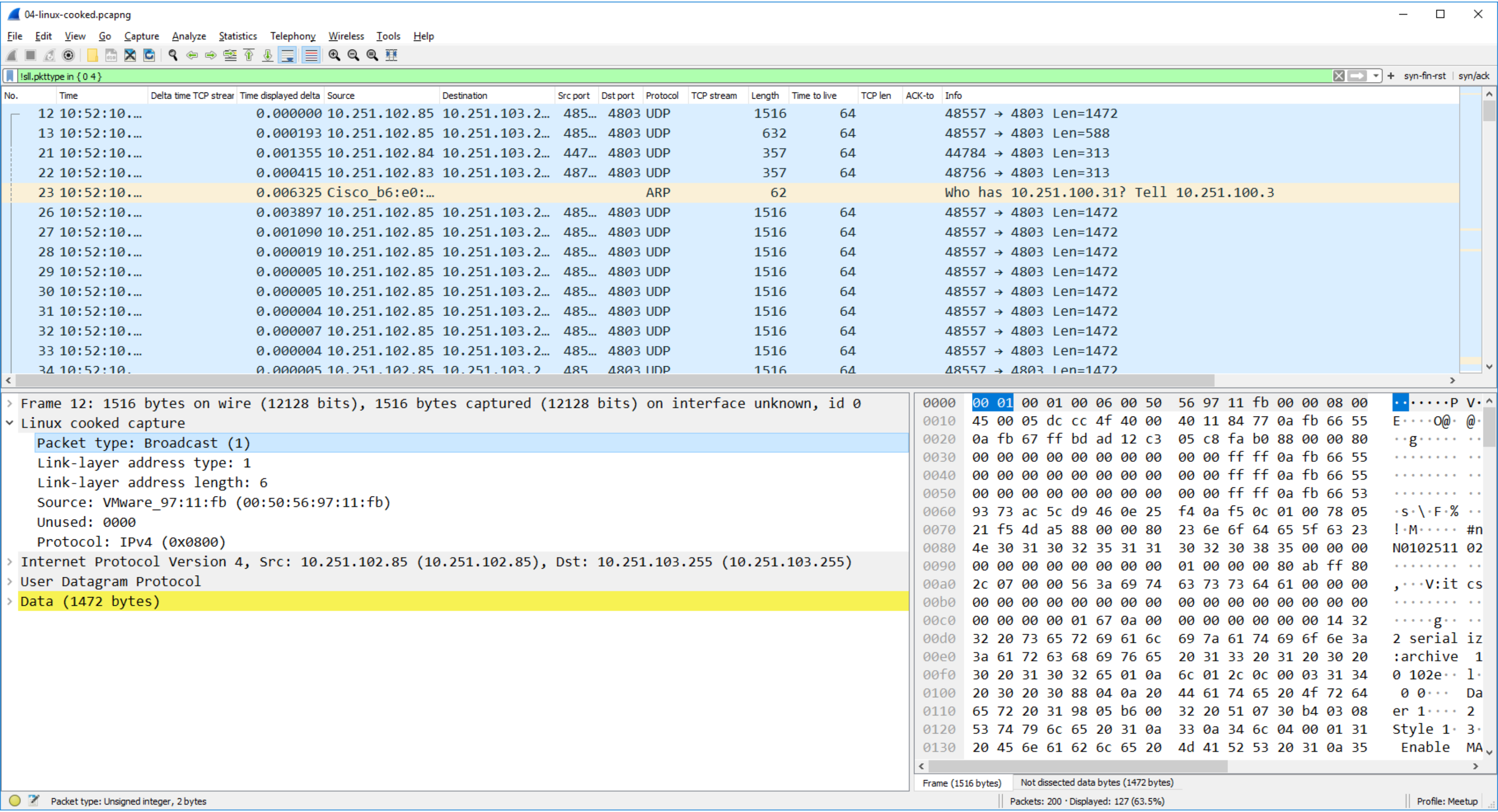


Linux:

```
sudo nice -n -18 tcpdump -s0 -i any -B 16384 -Z $(whoami) -w …
```

Windows:

```
start /realtime "Dumpcap - stop with Control-C" ^
    "%ProgramFiles%\Wireshark\dumpcap" -q -i4 -w "file.pcapng"
netsh trace start capture=yes fileMode=single maxsize=0 ^
   tracefile="%COMPUTERNAME%_%DATE:/=-%_%TIME::=-%.etl"
```



!sll.pkttype in {0 4}

No.	Time	Delta time TCP strear	Time displayed delta	Source	Destination	Src port	Dst port	Protocol	TCP stream	Length	Time to live	TCP len	ACK-to	Info
12	10:52:10.…		0.000000	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
13	10:52:10.…		0.000193	10.251.102.85	10.251.103.2…	485…	4803	UDP		632	64			48557 → 4803 Len=588
21	10:52:10.…		0.001355	10.251.102.84	10.251.103.2…	447…	4803	UDP		357	64			44784 → 4803 Len=313
22	10:52:10.…		0.000415	10.251.102.83	10.251.103.2…	487…	4803	UDP		357	64			48756 → 4803 Len=313
23	10:52:10.…		0.006325	Cisco_b6:e0:…				ARP		62				Who has 10.251.100.31? Tell 10.251.100.3
26	10:52:10.…		0.003897	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
27	10:52:10.…		0.001090	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
28	10:52:10.…		0.000019	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
29	10:52:10.…		0.000005	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
30	10:52:10.…		0.000005	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
31	10:52:10.…		0.000004	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
32	10:52:10.…		0.000007	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
33	10:52:10.…		0.000004	10.251.102.85	10.251.103.2…	485…	4803	UDP		1516	64			48557 → 4803 Len=1472
34	10:52:10.		0.000005	10.251.102.85	10.251.103.2	485	4803	UDP		1516	64			48557 → 4803 Len=1472

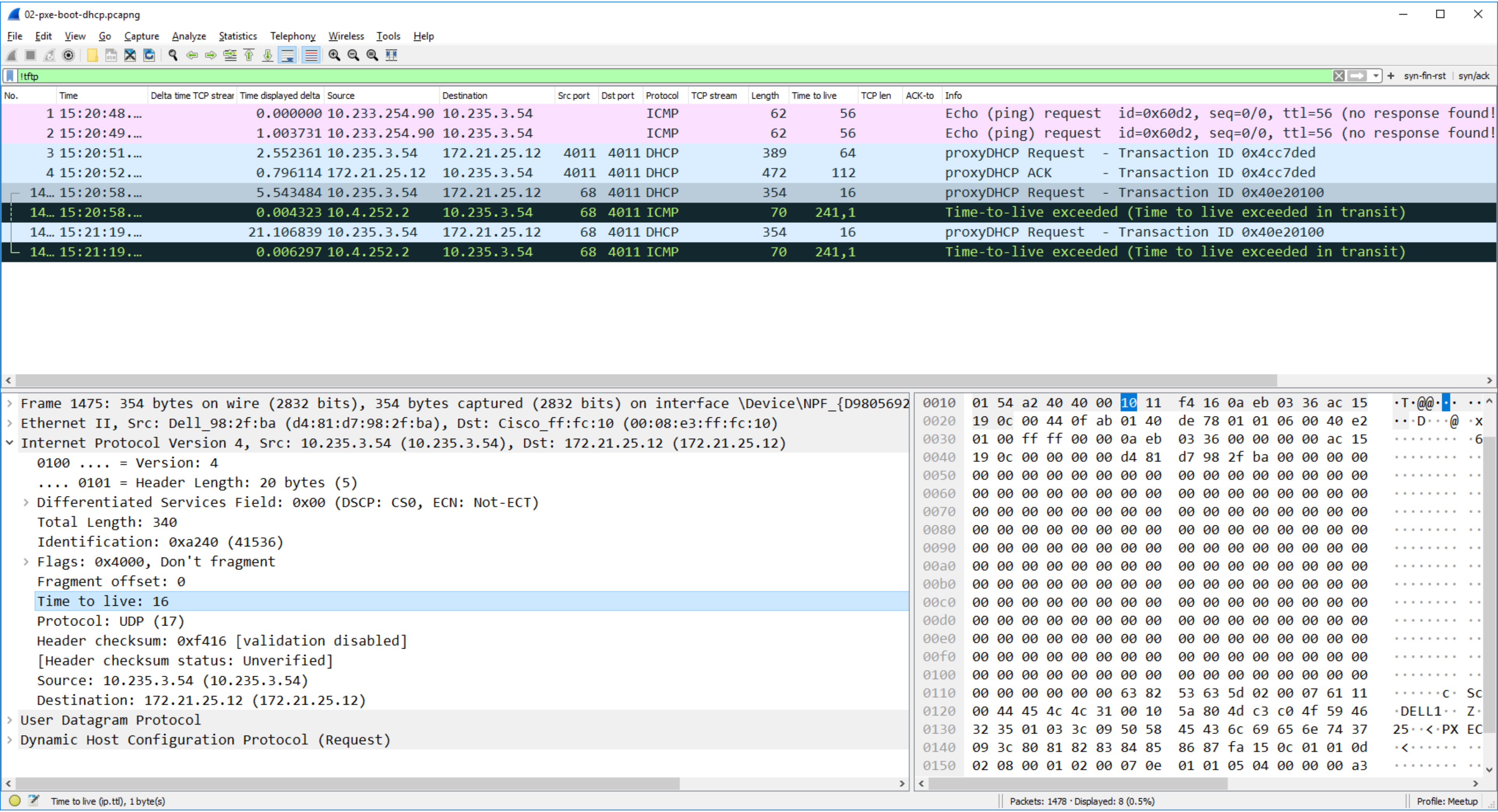
```
> Frame 12: 1516 bytes on wire (12128 bits), 1516 bytes captured (12128 bits) on interface unknown, id 0
v Linux cooked capture
    Packet type: Broadcast (1)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: VMware_97:11:fb (00:50:56:97:11:fb)
    Unused: 0000
    Protocol: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.251.102.85 (10.251.102.85), Dst: 10.251.103.255 (10.251.103.255)
> User Datagram Protocol
> Data (1472 bytes)
```

```
0000  00 01 00 01 00 06 00 50  56 97 11 fb 00 00 08 00   ·······P V·
0010  45 00 05 dc cc 4f 40 00  40 11 84 77 0a fb 66 55   E····O@· @·
0020  0a fb 67 ff bd ad 12 c3  05 c8 fa b0 88 00 00 80   ··g····· ··
0030  00 00 00 00 00 00 00 00  00 00 ff ff 0a fb 66 55   ········ ··
0040  00 00 00 00 00 00 00 00  00 00 ff ff 0a fb 66 55   ········ ··
0050  00 00 00 00 00 00 00 00  00 00 ff ff 0a fb 66 53   ········ ··
0060  93 73 ac 5c d9 46 0e 25  f4 0a f5 0c 01 00 78 05   ·s·\·F·% ··
0070  21 f5 4d a5 88 00 00 80  23 6e 6f 64 65 5f 63 23   !·M····· #n
0080  4e 30 31 30 32 35 31 31  30 32 30 38 35 00 00 00   N0102511 02
0090  00 00 00 00 00 00 00 00  01 00 00 00 80 ab ff 80   ········ ··
00a0  2c 07 00 00 56 3a 69 74  63 73 73 64 61 00 00 00   ,···V:it cs
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ··
00c0  00 00 00 00 01 67 0a 00  00 00 00 00 00 00 14 32   ·····g·· ··
00d0  32 20 73 65 72 69 61 6c  69 7a 61 74 69 6f 6e 3a   2 serial iz
00e0  3a 61 72 63 68 69 76 65  20 31 33 20 31 20 30 20   :archive  1
00f0  30 20 31 30 32 65 01 0a  6c 01 2c 0c 00 03 31 34   0 102e·· l·
0100  20 30 20 30 88 04 0a 20  44 61 74 65 20 4f 72 64    0 0···  Da
0110  65 72 20 31 98 05 b6 00  32 20 51 07 30 b4 03 08   er 1···· 2
0120  53 74 79 6c 65 20 31 0a  33 0a 34 6c 04 00 01 31   Style 1· 3·
0130  20 45 6e 61 62 6c 65 20  4d 41 52 53 20 31 0a 35    Enable  MA
```

Packet type: Unsigned integer, 2 bytes

Packets: 200 · Displayed: 127 (63.5%)

Profile: Meetup



02-pxe-boot-dhcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!tftp
syn-fin-rst
syn/ack

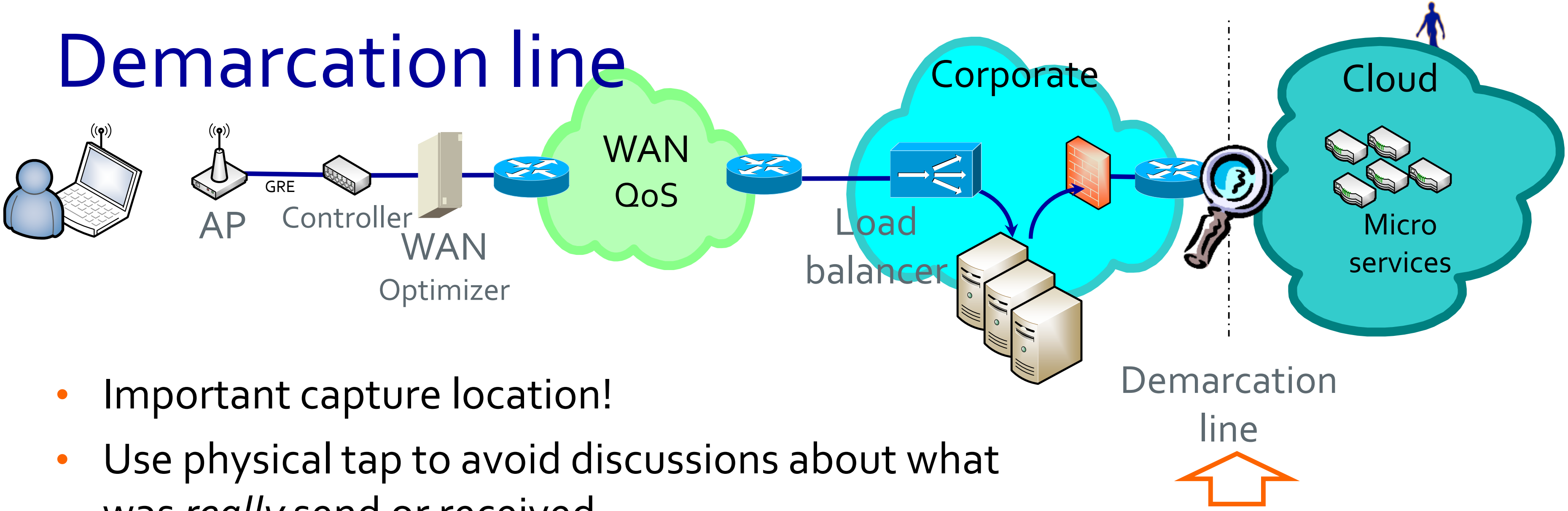
```
No.  Time         Delta time TCP strear Time displayed delta Source         Destination    Src port Dst port Protocol TCP stream Length Time to live TCP len ACK-to Info
   1 15:20:48.…                         0.000000 10.233.254.90 10.235.3.54                    ICMP                  62     56                 Echo (ping) request  id=0x60d2, seq=0/0, ttl=56 (no response found!
   2 15:20:49.…                         1.003731 10.233.254.90 10.235.3.54                    ICMP                  62     56                 Echo (ping) request  id=0x60d2, seq=0/0, ttl=56 (no response found!
   3 15:20:51.…                         2.552361 10.235.3.54   172.21.25.12   4011     4011   DHCP                 389     64                 proxyDHCP Request  - Transaction ID 0x4cc7ded
   4 15:20:52.…                         0.796114 172.21.25.12  10.235.3.54    4011     4011   DHCP                 472    112                 proxyDHCP ACK      - Transaction ID 0x4cc7ded
  14… 15:20:58.…                        5.543484 10.235.3.54   172.21.25.12     68     4011   DHCP                 354     16                 proxyDHCP Request  - Transaction ID 0x40e20100
  14… 15:20:58.…                        0.004323 10.4.252.2    10.235.3.54      68     4011   ICMP                  70  241,1                 Time-to-live exceeded (Time to live exceeded in transit)
  14… 15:21:19.…                       21.106839 10.235.3.54   172.21.25.12     68     4011   DHCP                 354     16                 proxyDHCP Request  - Transaction ID 0x40e20100
  14… 15:21:19.…                        0.006297 10.4.252.2    10.235.3.54      68     4011   ICMP                  70  241,1                 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 1475: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface \Device\NPF_{D9805692
> Ethernet II, Src: Dell_98:2f:ba (d4:81:d7:98:2f:ba), Dst: Cisco_ff:fc:10 (00:08:e3:ff:fc:10)
v Internet Protocol Version 4, Src: 10.235.3.54 (10.235.3.54), Dst: 172.21.25.12 (172.21.25.12)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 340
    Identification: 0xa240 (41536)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 16
    Protocol: UDP (17)
    Header checksum: 0xf416 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.235.3.54 (10.235.3.54)
    Destination: 172.21.25.12 (172.21.25.12)
> User Datagram Protocol
> Dynamic Host Configuration Protocol (Request)
```

```
0010  01 54 a2 40 40 00 10 11  f4 16 0a eb 03 36 ac 15   ·T·@@···  ··
0020  19 0c 00 44 0f ab 01 40  de 78 01 01 06 00 40 e2   ···D···@  ·x
0030  01 00 ff ff 00 00 0a eb  03 36 00 00 00 00 ac 15   ········  ·6
0040  19 0c 00 00 00 00 d4 81  d7 98 2f ba 00 00 00 00   ········  ··
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ··
0110  00 00 00 00 00 00 63 82  53 63 5d 02 00 07 61 11   ······c·  Sc
0120  00 44 45 4c 4c 31 00 10  5a 80 4d c3 c0 4f 59 46   ·DELL1··  Z·
0130  32 35 01 03 3c 09 50 58  45 43 6c 69 65 6e 74 37   25··<·PX  EC
0140  09 3c 80 81 82 83 84 85  86 87 fa 15 0c 01 01 0d   ·<······  ··
0150  02 08 00 01 02 00 07 0e  01 01 05 04 00 00 00 a3   ········  ··
```

```
Time to live (ip.ttl), 1 byte(s)        Packets: 1478 · Displayed: 8 (0.5%)        Profile: Meetup
```

Demarcation line



- Important capture location!
- Use physical tap to avoid discussions about what was *really* send or received
- Needed to *prove* ‘our’ or ‘their’ problem

TLS encrypted traffic

- Use SSLKEYLOGFILE environment variable to store the session keys by Chrome/Firefox/Opera/curl/Java (lib)/OpenSSL of GnuTLS based appl., etc.
- Not available in Windows native TLS library Secure Channel (SChannel)
- Linux

  ```
  SSLKEYLOGFILE=$(realpath $keylogfile) firefox
  ```
- Windows

  ```
  set SSLKEYLOGFILE=%CD%\key-%DATE:/=-%_%TIME::=-%.log
  chrome.exe
  ```
- Make sure app is not already running (pkill firefox | taskkill /f /im chrome.exe)

Embed session keys in pcapng

Since Wireshark 3.0 you can embed the TLS key log file in a pcapng file. This makes it much easier to distribute capture files with decryption secrets, and makes switching between capture files easier since the TLS protocol preference does not have to be updated.

For example:

```
editcap --inject-secrets tls,keys.txt in.pcap out.pcapng
```

Anonymize capture

- Useful when you need to share capture with supplier
- Use TraceWrangler www.tracewrangler.com
- For sanitization, anonymization or scrubbing of packet captures

Thank you. Questions?

https://www.linkedin.com/in/andreluyer

Rabobank

SSLKEY capture & analyse (Windows)

```
rem Capture with SSLKEYLOGFILE - AU Luyer - 2018-09-10
set timestamp=%DATE:/=-%_%TIME::=-%
start /realtime "Dumpcap - stop with Control-C" ^
  "%ProgramFiles%\Wireshark\dumpcap" -B 16 -q -i1 -i2 -w ^
  "trace-%timestamp%.pcapng"
rem make sure the browser is not already running (in the background)...
taskkill /f /im chrome.exe
timeout 3

rem Set logfile. Must be absolute path!
set SSLKEYLOGFILE=%CD%\key-%timestamp%.log
start "Chrome-tls" "%ProgramFiles%\Google\Chrome\Application\chrome.exe" ^
  --disable-http2 https://sharkfesteurope.wireshark.org/

rem Using option tls.keylog_file allows for temporary use without altering
  the configuration.
echo start "Wireshark" "%ProgramFiles%\Wireshark\wireshark.exe" ^
  -r "trace-%timestamp%.pcap" -o tls.keylog_file:"key-%timestamp%.log" ^
  -Y "tls && http" > "start-wireshark-%timestamp%.cmd"
```

SSLKEY capture & analyse (Linux)

```bash
#!/bin/bash
# Capture with SSLKEYLOGFILE - AU Luyer - 2018-09-10
timestamp=$(date +%F_%H-%M-%S)
pcapfile=trace_$timestamp.pcapng
keylogfile=keys_$timestamp.log

sudo nice -n -18 dumpcap -B 16 -q -i any -w - > $pcapfile &
# -w - > == workaround "Permission denied" bug.
echo $!
sleep 3

SSLKEYLOGFILE=$(realpath $keylogfile) firefox https://sharkfest.wireshark.org/ &
# Logfile must be absolute path!

script=start_wireshark_$timestamp.sh
echo "wireshark -r $pcapfile -o tls.keylog_file:$keylogfile -Y 'tls &&
   (http||http2)' &" > $script && chmod +rx $script
echo "Stop capture with: sudo pkill dumpcap"
```