

Example Wireshark trace

I set a Wireshark filter to trace only “ARP packets” received by my desktop PC. *It is not important to understand what an ARP packet is.* What is important to understand is how a trace file can be manipulated. Note that time stamps are cumulative seconds.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	SunMicro_87:8f:cd	Broadcast	ARP	Who has 131.247.2.81? Tell 131.247.3.6
2	0.029774	SunMicro_1d:9c:2c	Broadcast	ARP	Who has 131.247.3.5? Tell 131.247.3.2
3	0.278170	Dell_37:10:7b	Broadcast	ARP	Who has 131.247.2.191? Tell 131.247.3.16
4	0.532537	SunMicro_8f:d1:0d	Broadcast	ARP	Who has 131.247.2.32? Tell 131.247.2.27
5	0.558530	HewlettP_94:e9:77	Broadcast	ARP	Who has 131.247.210.252? Tell 131.247.2.188
6	0.571416	Cisco_72:8d:c0	Broadcast	ARP	Who has 131.247.3.142? Tell 131.247.3.254
7	0.705754	Dell_48:a0:89	Broadcast	ARP	Who has 131.247.3.16? Tell 131.247.2.94
8	0.797557	Cisco_72:8d:c0	Broadcast	ARP	Who has 131.247.2.99? Tell 131.247.3.254
9	0.999826	SunMicro_87:8f:cd	Broadcast	ARP	Who has 131.247.2.81? Tell 131.247.3.6

To cut out the timestamps I used the Unix cut command (I did remove the leading spaces first):

```
c:\work>cut -d" " -f2 < x > y
c:\work\type y
0.000000
0.029774
0.278170
0.532537
0.558530
0.571416
0.705754
0.797557
0.999826
```

Cumulative time stamps can be converted to “delta” time stamps using clktod.c:

```
c:\work\clktod < y > z
c:\work\type z
0.000000
0.029774
0.248396
0.254367
0.025993
0.012886
0.134338
0.091803
0.202269
```