

adm22-fred-fumble.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: eth.addr==00:06:5b:fe:a0:e8

No.	Rel Time	Delta Time	Size	Source	Destination	Protocol	Info
250	0.012865	0.000003	242	140.107.42.102	140.107.43.150	NBSS	NBSS Continuation Message
251	0.012868	0.000003	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114906718 win=48180 Len=0
252	0.012871	0.000003	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114909638 win=45260 Len=0
253	0.012938	0.000067	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114912558 win=49640 Len=0
254	0.012942	0.000004	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114915478 win=46720 Len=0
255	0.012948	0.000006	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114918398 win=43800 Len=0
256	0.013045	0.000097	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114921318 win=48180 Len=0
257	0.013049	0.000004	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114924238 win=45260 Len=0
258	0.013055	0.000006	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114927158 win=49640 Len=0
259	0.013061	0.000006	60	140.107.43.150	140.107.42.102	TCP	microsoft-ds > colubris [ACK] Seq=198007233 Ack=114930078 win=46720 Len=0
260	0.313741	0.300680	242	140.107.42.102	140.107.43.150	NBSS	[TCP Retransmission] NBSS Continuation Message
261	0.495366	0.181625	74	140.107.42.102	140.107.43.150	ICMP	Echo (ping) request
262	0.917265	0.421899	242	140.107.42.102	140.107.43.150	NBSS	[TCP Retransmission] NBSS Continuation Message
263	2.124244	1.206979	242	140.107.42.102	140.107.43.150	NBSS	[TCP Retransmission] NBSS Continuation Message
264	3.777821	1.653577	204	140.107.42.102	140.107.43.150	SMB	Trans2 Request, FIND_FIRST2[Packet size limited during capture]
265	4.538328	0.760507	392	140.107.42.102	140.107.43.150	NBSS	[TCP Retransmission] NBSS Continuation Message
266	5.872189	1.333861	74	140.107.42.102	140.107.43.150	ICMP	Echo (ping) request
267	9.265683	3.393494	392	140.107.42.102	140.107.43.150	NBSS	[TCP Retransmission] NBSS Continuation Message
268	11.372977	2.107294	74	140.107.42.102	140.107.43.150	ICMP	Echo (ping) request
293	16.871914	4.033850	74	140.107.42.102	140.107.43.150	ICMP	Echo (ping) request
294	22.137446	5.265532	64	Dell_b9:cd:38	DellComp_fe:a0:e8	ARP	who has 140.107.42.102? Tell 140.107.43.45
295	22.137493	0.000047	60	DellComp_fe:a0:e8	Dell_b9:cd:38	ARP	140.107.42.102 is at 00:06:5b:fe:a0:e8
296	22.371711	0.234218	74	140.107.42.102	140.107.43.150	ICMP	Echo (ping) request
297	24.303953	1.932242	62	140.107.42.102	140.107.43.150	TCP	isoft-p2p > microsoft-ds [SYN] Seq=1674863092 win=65535 Len=0 MSS=1460
298	24.304409	0.000456	62	140.107.42.102	140.107.43.150	TCP	avinstalldisc > netbios-ssn [SYN] Seq=2323764079 win=65535 Len=0 MSS=1460
299	25.928690	1.624281	64	Dell_b9:d9:c0	DellComp_fe:a0:e8	ARP	who has 140.107.42.102? Tell 140.107.43.12
300	25.928742	0.000052	60	DellComp_fe:a0:e8	Dell_b9:d9:c0	ARP	140.107.42.102 is at 00:06:5b:fe:a0:e8
301	27.269900	1.341158	62	140.107.42.102	140.107.43.150	TCP	isoft-p2p > microsoft-ds [SYN] Seq=1674863092 win=65535 Len=0 MSS=1460
302	27.371489	0.101589	62	140.107.42.102	140.107.43.150	TCP	avinstalldisc > netbios-ssn [SYN] Seq=2323764079 win=65535 Len=0 MSS=1460
303	27.871521	0.500032	74	140.107.42.102	140.107.43.150	ICMP	Echo (ping) request
304	28.184245	0.312724	64	Dell_b9:d0:1c	DellComp_fe:a0:e8	ARP	who has 140.107.42.102? Tell 140.107.43.80
305	28.184298	0.000053	60	DellComp_fe:a0:e8	IntelCor_51:36:0d	ARP	140.107.42.102 is at 00:06:5b:fe:a0:e8
306	29.493354	1.309056	64	Dell_dc:64:8f	DellComp_fe:a0:e8	ARP	who has 140.107.42.102? Tell 140.107.43.106
307	29.493403	0.000049	60	DellComp_fe:a0:e8	Dell_dc:64:8d	ARP	140.107.42.102 is at 00:06:5b:fe:a0:e8
308	30.021083	0.527680	64	Dell_b9:cd:b9	DellComp_fe:a0:e8	ARP	who has 140.107.42.102? Tell 140.107.43.28
309	30.021140	0.000057	60	DellComp_fe:a0:e8	Dell_b9:cd:b9	ARP	140.107.42.102 is at 00:06:5b:fe:a0:e8
310	33.304883	3.283743	62	140.107.42.102	140.107.43.150	TCP	isoft-p2p > microsoft-ds [SYN] Seq=1674863092 win=65535 Len=0 MSS=1460

Type: IP (0x0800)

- Internet Protocol, Src: 140.107.42.102 (140.107.42.102), Dst: 140.107.43.150 (140.107.43.150)
- Transmission Control Protocol, Src Port: colubris (3490), Dst Port: microsoft-ds (445), Seq: 114930078, Ack: 198007233, Len: 188
 - Source port: colubris (3490)
 - Destination port: microsoft-ds (445)
 - [Stream index: 0]
 - Sequence number: 114930078
 - [Next sequence number: 114930266]
 - Acknowledgement number: 198007233
 - Header length: 20 bytes
 - Flags: 0x18 (PSH, ACK)
 - window size: 64668
 - Checksum: 0x580c [unchecked, not all data available]
 - [SEQ/ACK analysis]
 - [This is an ACK to the segment in frame: 251]
 - [The RTT to ACK the segment was: 0.300873000 seconds]
 - [Number of bytes in flight: 3108]
 - [TCP Analysis Flags]
 - [This frame is a (suspected) retransmission]
 - [Expert Info (Note/Sequence): Retransmission (suspected)]
 - [The RTO for this segment was: 0.300876000 seconds]
 - [RTO based on delta from frame: 250]
- NetBIOS Session Service

```

0000 00 14 4f 86 7d f6 00 06 5b fe a0 e8 08 00 45 00  ..O.}. . . [ . . . . .E.
0010 00 e4 ea 3e 40 00 80 06 a1 02 8c 6b 2a 66 8c 6b  . . .>@. . . . .k*f.k
0020 2b 96 0d a2 01 bd 06 d9 b1 9e 0b cd 59 c1 50 18  +. . . . . . . . . . .Y.P.
0030 fc 9c 58 0c 00 00 20 20 20 20 20 20 20 20 20 20  . . . . . . . . . . .X. . .
0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  . . . . . . . . . . . . . .
0050 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  . . . . . . . . . . . . . .

```

Frame (frame), 128 bytes Packets: 498 Displayed: 404 Marked: 0 Profile: Default