

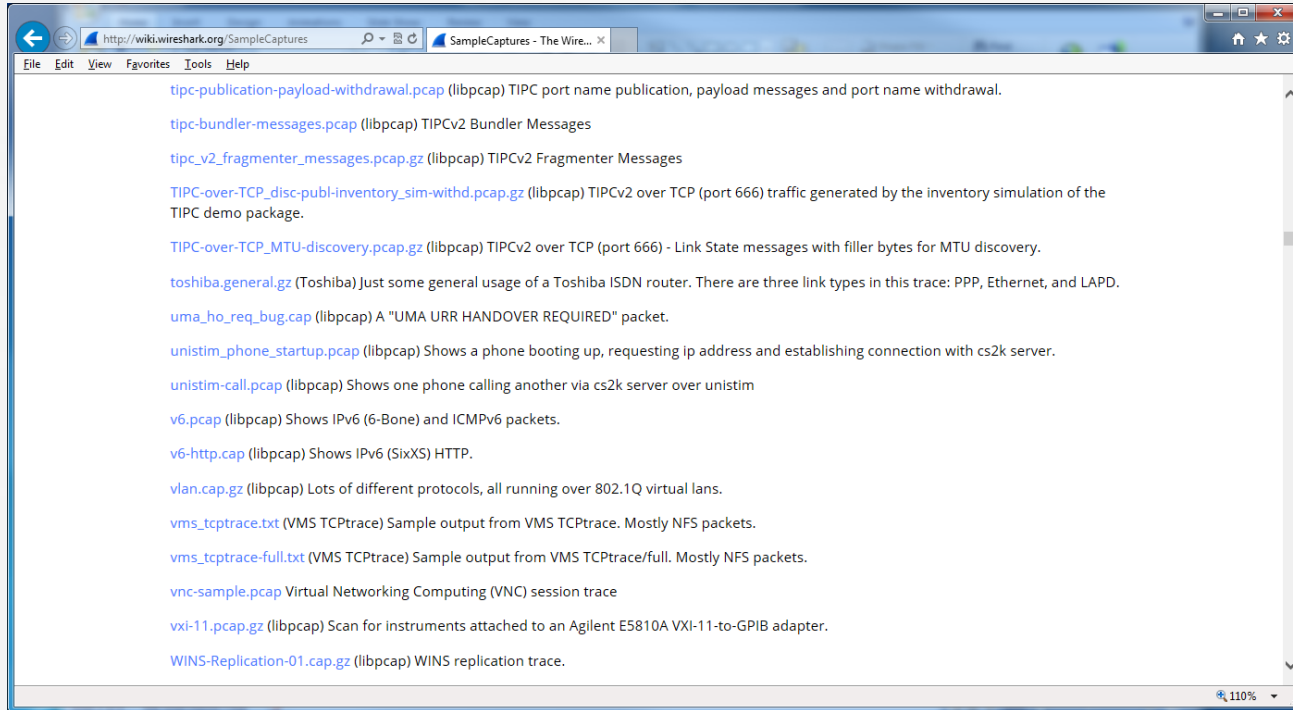


Sample Captures

Wireshark Sample Captures

- » **Use Sample Capture filters to learn how to make filters**
 - Download samples to learn how they were made
- » **Use Sample Capture filters to learn how to troubleshoot problems**
 - Download samples to learn why they were made

Wireshark Sample Captures



Wireshark Sample Captures

» Go to the Wireshark wiki

- Find the wiki online @ <http://wiki.wireshark.org/SampleCaptures>
- Review the available captures
- Submit captures!

» Find and download captures, analyze!

- Download and load what you would like to see

Wireshark Sample Captures

The screenshot displays the Wireshark interface with a packet capture of an ICMPv6 Echo (ping) request. The packet list pane shows a standard query response from 3ffe:507:0:1:200:86:3ffe:501:4819::42 to 3ffe:507:0:1:200:86:dns. The packet details pane shows the Internet Protocol Version 6 header and the ICMPv6 Echo (ping) payload. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info	New Column
1	0.00000	3ffe:507:0:1:200:86:3ffe:501:4819::42	DNS	DNS	90	standard query 0x0006 ANY itojun.org	1999-03-11 08:45:02.141757
2	0.073515	3ffe:501:4819::42	3ffe:507:0:1:200:86:dns	DNS	510	standard query response 0x0006 NS coconut.itojun.org NS tiger.hirc	1999-03-11 08:45:02.215272
3	5.352508	fe80::200:86ff:fe05fe80::260:97ff:fe07	fe07	ICMPv6	86	Neighbor solicitation for fe80::260:97ff:fe07:69ea from 00:00:86:051999-03-11 08:45:07.494265	
4	5.352839	fe80::260:97ff:fe07	fe80::200:86ff:fe05	ICMPv6	78	Neighbor Advertisement fe80::260:97ff:fe07:69ea (rtr, sol)	1999-03-11 08:45:07.494596
5	5.478595	sh1.iijlab.net	3ffe:507:0:1:200:86	ICMPv6	86	Neighbor Solicitation for 3ffe:507:0:1:200:86ff:fe05:80da from 00:6:1999-03-11 08:45:07.620352	
6	5.479045	3ffe:507:0:1:200:86	sh1.iijlab.net	ICMPv6	78	Neighbor Advertisement 3ffe:507:0:1:200:86ff:fe05:80da (sol)	1999-03-11 08:45:07.620802
7	6.617560	3ffe:507:0:1:200:86	3ffe:501:4819::42	DNS	93	standard query 0x0006 MX www.yahoo.com	1999-03-11 08:45:08.759317
8	6.752573	3ffe:501:4819::42	3ffe:507:0:1:200:86:dns	DNS	358	standard query response 0x0006 MX 0 mrl.yahoo.com	1999-03-11 08:45:08.894330
9	10.364948	3ffe:507:0:1:200:86	sh1.iijlab.net	ICMPv6	86	Neighbor Solicitation for 3ffe:507:0:1:260:97ff:fe07:69ea from 00:0:1999-03-11 08:45:12.506705	
10	10.365231	sh1.iijlab.net	3ffe:507:0:1:200:86	ICMPv6	78	Neighbor Advertisement 3ffe:507:0:1:260:97ff:fe07:69ea (rtr, sol)	1999-03-11 08:45:12.506988
11	10.490052	fe80::260:97ff:fe07	fe80::200:86ff:fe05	ICMPv6	86	Neighbor Solicitation for fe80::200:86ff:fe05:80da from 00:60:97:071999-03-11 08:45:12.631809	
12	10.490554	fe80::200:86ff:fe05	fe80::260:97ff:fe07	ICMPv6	78	Neighbor Advertisement fe80::200:86ff:fe05:80da (sol)	1999-03-11 08:45:12.632311
13	12.297384	fe80::260:97ff:fe07	ff02::9	RIPng	1206	Command Response, Version 1	1999-03-11 08:45:14.439141
14	16.109457	3ffe:507:0:1:200:86	3ffe:501:4819::42	DNS	95	standard query 0x2c72 AAAA kiwi.itojun.org	1999-03-11 08:45:18.251214
15	16.121831	3ffe:501:4819::42	3ffe:507:0:1:200:86:dns	DNS	282	standard query response 0x2c72 AAAA 3ffe:501:410:0:2c0:dfff:fe47:31999-03-11 08:45:18.263588	
16	16.124364	3ffe:507:0:1:200:86	kiwi.itojun.org	TCP	94	exp2 > ssh [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=1 TSval=576087 TS1999-03-11 08:45:18.266121	

Frame 9: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Megahert_05:80:da (00:00:86:05:80:da), Dst: 3com_07:69:ea (00:60:97:07:69:ea)
Internet Protocol Version 6, Src: 3ffe:507:0:1:200:86ff:fe05:80da (3ffe:507:0:1:200:86ff:fe05:80da), Dst: sh1.iijlab.net (3ffe:507:0:1:260:97ff:fe07:69ea)
0110 = Version: 6
.... 0000 0000 = Traffic class: 0x00000000
.... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 32
Next header: ICMPv6 (58)
Hop limit: 255
Source: 3ffe:507:0:1:200:86ff:fe05:80da (3ffe:507:0:1:200:86ff:fe05:80da)
[Source SA MAC: Megahert_05:80:da (00:00:86:05:80:da)]
Destination: sh1.iijlab.net (3ffe:507:0:1:260:97ff:fe07:69ea)
[Destination SA MAC: 3com_07:69:ea (00:60:97:07:69:ea)]
[Source geoIP: unknown]
[Destination geoIP: unknown]
Internet Control Message Protocol v6
0000 00 60 97 07 69 ea 00 00 86 05 80 da 86 dd 60 00?
0010 00 00 00 20 38 ff 3f fe 05 07 00 00 00 01 02 00?
0020 86 ff fe 05 80 da 3f fe 05 07 00 00 00 01 02 60?
0030 07 ff fe 07 69 ea 87 00 95 2d 00 00 00 00 3f fe?
0040 05 07 00 00 00 01 02 60 97 ff fe 07 69 ea 01 01?
0050 00 00 86 05 80 da?

Questions?