



UDP & TCP Streams

Wireshark Streams

» Troubleshooting with Wireshark

» Following streams

- Allows you to view data at a higher level, such as the application layer of the OSI model

» TCP streams

- View an entire conversation between clients
- View TCP information at the application layer

TCP Streams

The screenshot displays a network traffic analysis tool (Wireshark) with a 'Follow TCP Stream' window open. The background shows a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, Info, and New Column. The 'Follow TCP Stream' window shows the content of a selected stream, including the request and response headers and body. The response is a multipart/byteranges response with two parts, each with its own Content-Type and Content-Range headers. The dialog also includes options for finding, saving, printing, and filtering the stream.

No.	Time	Source	Destination	Protocol	Length	Info	New Column
7	0.312500000	213.19.160.190	81.131.67.131	TCP	62	http > netsteward [SYN, ACK] Seq=0 Ack=1 win=584	2005-07-16 10:29:30.112500000
8	0.312500000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:30.112500000
10	0.343750000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:30.143750000
47	1.937500000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:31.737500000
51	1.968750000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:31.768750000
52	2.125000000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:31.925000000
56	2.343750000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:32.143750000
57	2.562500000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:32.362500000
76	3.796875000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:33.596875000
77	3.796875000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:33.596875000
79	4.078125000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:33.878125000
81	4.078125000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:33.878125000
92	4.906250000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:34.706250000
100	5.078125000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:34.878125000
221	11.158203000	213.19.160.190	81.131.67.131	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:40.958203000
222	11.158203000	81.131.67.131	213.19.160.190	TCP	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0	2005-07-16 10:29:40.958203000

Stream Content

```
GET /msdownload/update/v5/psf/windowsxp-sp2-x86fre-usa-2180_056b2b38baf5620be85ddd58141b073bc0b06a1d.psf HTTP/1.1
Accept: */*
Accept-Encoding: identity
Range: bytes=27434481-27434687,27524096-27527101
User-Agent: Microsoft BITS/6.6
Host: au.download.windowsupdate.com
Connection: Keep-Alive

HTTP/1.1 206 Partial Content
Date: Sat, 16 Jul 2005 09:29:32 GMT
ETag: "d45e21d7a17ac41:8037"
Last-Modified: Thu, 05 Aug 2004 04:08:19 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Type: multipart/byteranges; boundary=5284138D3F7
Connection: keep-alive

--5284138D3F7
Content-Type: application/octet-stream
Content-Range: bytes 27434481-27434687/772792554

S...R.O<K...lB...
{...0..h.8.Ps3L...0...W.X...A.&Y0Qid.1h.vc...R...L9.t.v.:n:'.@>...w.:dnd...
C...F...>>B>X.<...(.C.Ci.'nF,l.]>]...p.o...U.7d.'Z.]...+R..T..j...
\g/.X...&.....)
--5284138D3F7
Content-Type: application/octet-stream
Content-Range: bytes 27524096-27527101/772792554
```

Entire conversation (4049 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

UDP Streams

» Troubleshooting with Wireshark

» Following streams

- Allows you to view data at a higher level, such as the application layer of the OSI model

» UDP streams

- View an entire conversation between clients
- View UDP information at the application layer

UDP Streams

The screenshot displays a network analysis tool interface with a packet list on the left and a detailed view of a selected packet on the right. The packet list shows a sequence of DNS messages between 192.168.170.8 and 192.168.170.8. The selected packet is a standard query response (length 98) containing a list of domain names.

No.	Time	Source	Destination	Protocol	Length	Info	New Column
1	0.000000	192.168.170.8	192.168.170.20	DNS	70	standard query 0x1032 TXT google.com	2005-03-30 04:47:46.496046
2	0.000530	192.168.170.20	192.168.170.8	DNS	98	standard query response 0x1032 TXT	2005-03-30 04:47:46.496576
3	4.005228					com	2005-03-30 04:47:50.501268
4	4.837358					X 40 smtp4.goo	2005-03-30 04:47:51.333401
5	12.817188					s.com	2005-03-30 04:47:59.313231
6	12.956288						2005-03-30 04:47:59.452255
7	20.824888					192.66.in-addr.	2005-03-30 04:48:07.320873
8	20.825388					TR 66-192-9-10	2005-03-30 04:48:07.321379
9	2.189988					sd.org	2005-03-30 04:49:18.685951
10	2.238888					204.152.190.1	2005-03-30 04:49:18.734862
11	108.965888					netbsd.org	2005-03-30 04:49:35.461181
12	109.202888					AAA 2001:4f8:4	2005-03-30 04:49:35.698849
13	169.027888					netbsd.org	2005-03-30 04:50:35.523440
14	169.027888					AAA 2001:4f8:4	2005-03-30 04:50:35.523827
15	178.239888					oogle.com	2005-03-30 04:50:44.735890
16	178.256888					NAME www.1.goo	2005-03-30 04:50:44.752428
17	187.853888					.google.com	2005-03-30 04:50:54.349862

The detailed view shows the stream content of the selected packet, which is a DNS query response. The content is displayed in a hex dump format, with the raw bytes shown in the main window and the ASCII representation shown in the bottom pane. The ASCII pane shows the following text:

```
2.....google.com.....2.....google.com.....v=spf1 ptr ?  
all.o.....google.com.....o.....google.com.....(  
.smtp4.....(  
.smtp5.....(  
.smtp6.....(  
.smtp1.....(  
.smtp2.....(  
.smtp3.....X.....X.....%.....@.....X.....@.....V.....X.....Bf...l.....X.....9.....X.....  
%.....X.....9.I.....google.com.....I.....google.com.....10  
4.9.192.66.in-addr.arpa.....104.9.192.66.in-addr.arpa.....Q  
%.66-192-9-104.gen.twtelecom.net.u.....www.netbsd.org.....u.....www.netbs  
d.org.....@.....www.netbsd.org.....www.netbsd.or  
g.....Q.....R.k.9.....www.netbsd.org.....9.....www.netbs  
d.org.....QD.....y.....www.1.....R.k.....www.google.com.....www.go  
gle.com.....y.....www.1.....R.k.....www.google.com.....www.1.goo  
gle.com.....www.example.com.....www.example.com.....&  
m.....www.example.notginh.....&m.....www.example.notginh.....ww  
w.isc.org.....www.isc.org.....X.....
```

Questions?