



Expert Advanced Features

The Wireshark Expert

- » **What else can you do with the Expert?**
- » **Further customization**
 - Change the Packets List pane to show severity
 - Color-coded icons in the Expert window
 - Create preferences and profile settings

The Wireshark Expert

FTPv6-1.cap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 3 Expression... Clear Apply Save New Label

No.	Time	Source	Destination	Protocol	Expert	Length	Info
8	0.312500000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=1 Ack=1 win=8760 Len=0
10	0.343750000	81.131.67.131	213.19.160.190	HTTP	Chat	354	GET /msdownload/update/v5/psf/windowsxp-sp2-x86fre-usa-2180.
47	1.937500000	213.19.160.190	81.131.67.131	TCP		54	http > netsteward [ACK] Seq=1 Ack=301 win=6432 Len=0
51	1.968750000	213.19.160.190	81.131.67.131	HTTP	Chat	353	HTTP/1.1 206 Partial Content
52	2.125000000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=301 Ack=300 win=8461 Len=0
56	2.343750000	213.19.160.190	81.131.67.131	HTTP		370	Continuation or non-HTTP traffic
57	2.562500000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=301 Ack=616 win=8145 Len=0
76	3.796875000	213.19.160.190	81.131.67.131	HTTP		1514	Continuation or non-HTTP traffic
77	3.796875000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=301 Ack=2076 win=8760 Len=0
79	4.078125000	213.19.160.190	81.131.67.131	HTTP		1514	Continuation or non-HTTP traffic
81	4.078125000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=301 Ack=3536 win=8760 Len=0
92	4.906250000	213.19.160.190	81.131.67.131	HTTP		268	Continuation or non-HTTP traffic
100	5.078125000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=301 Ack=3750 win=8546 Len=0
221	11.158203000	213.19.160.190	81.131.67.131	TCP	Chat	54	http > netsteward [FIN, ACK] Seq=3750 Ack=301 win=6432 Len=0
222	11.158203000	81.131.67.131	213.19.160.190	TCP	warn	54	netsteward > http [ACK] Seq=301 Ack=3751 win=8546 Len=0
349	16.296875000	81.131.67.131	213.19.160.190	TCP	Chat	54	netsteward > http [RST] Seq=301 win=0 Len=0

Frame 51: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits)

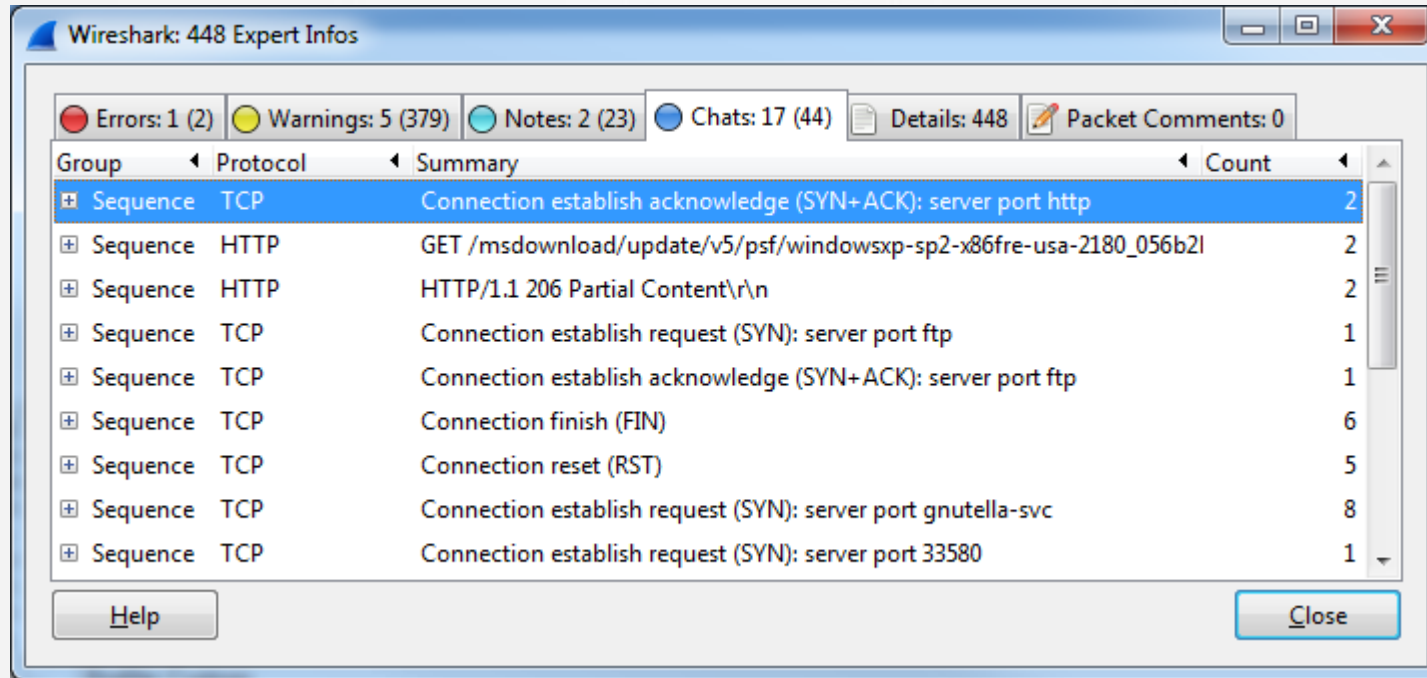
- Ethernet II, Src: 1a:43:20:00:01:00 (1a:43:20:00:01:00), Dst: Xerox_00:00:00 (01:00:01:00:00:00)
- Internet Protocol Version 4, Src: 213.19.160.190 (213.19.160.190), Dst: 81.131.67.131 (81.131.67.131)
- Transmission Control Protocol, Src Port: http (80), Dst Port: netsteward (2810), Seq: 1, Ack: 301, Len: 299
- Hypertext Transfer Protocol

The Wireshark Expert

» Wireshark Expert tabs icon marking

- Errors - Red
- Warnings - Yellow
- Notes – Light blue
- Chats – Blue
- Details – Note icon
- Packet comments – Note and pencil icon

The Wireshark Expert



The screenshot shows the 'Wireshark: 448 Expert Infos' window. At the top, there are summary statistics: Errors: 1 (2), Warnings: 5 (379), Notes: 2 (23), Chats: 17 (44), Details: 448, and Packet Comments: 0. Below this is a table with columns for Group, Protocol, Summary, and Count. The first row is selected and highlighted in blue.

Group	Protocol	Summary	Count
+	Sequence TCP	Connection establish acknowledge (SYN+ACK): server port http	2
+	Sequence HTTP	GET /msdownload/update/v5/psf/windowsxp-sp2-x86fre-usa-2180_056b2l	2
+	Sequence HTTP	HTTP/1.1 206 Partial Content\r\n	2
+	Sequence TCP	Connection establish request (SYN): server port ftp	1
+	Sequence TCP	Connection establish acknowledge (SYN+ACK): server port ftp	1
+	Sequence TCP	Connection finish (FIN)	6
+	Sequence TCP	Connection reset (RST)	5
+	Sequence TCP	Connection establish request (SYN): server port gnutella-svc	8
+	Sequence TCP	Connection establish request (SYN): server port 33580	1

Buttons for 'Help' and 'Close' are located at the bottom of the window.

Questions?