



# Using the Expert

# The Wireshark Expert

## » What is the Expert?

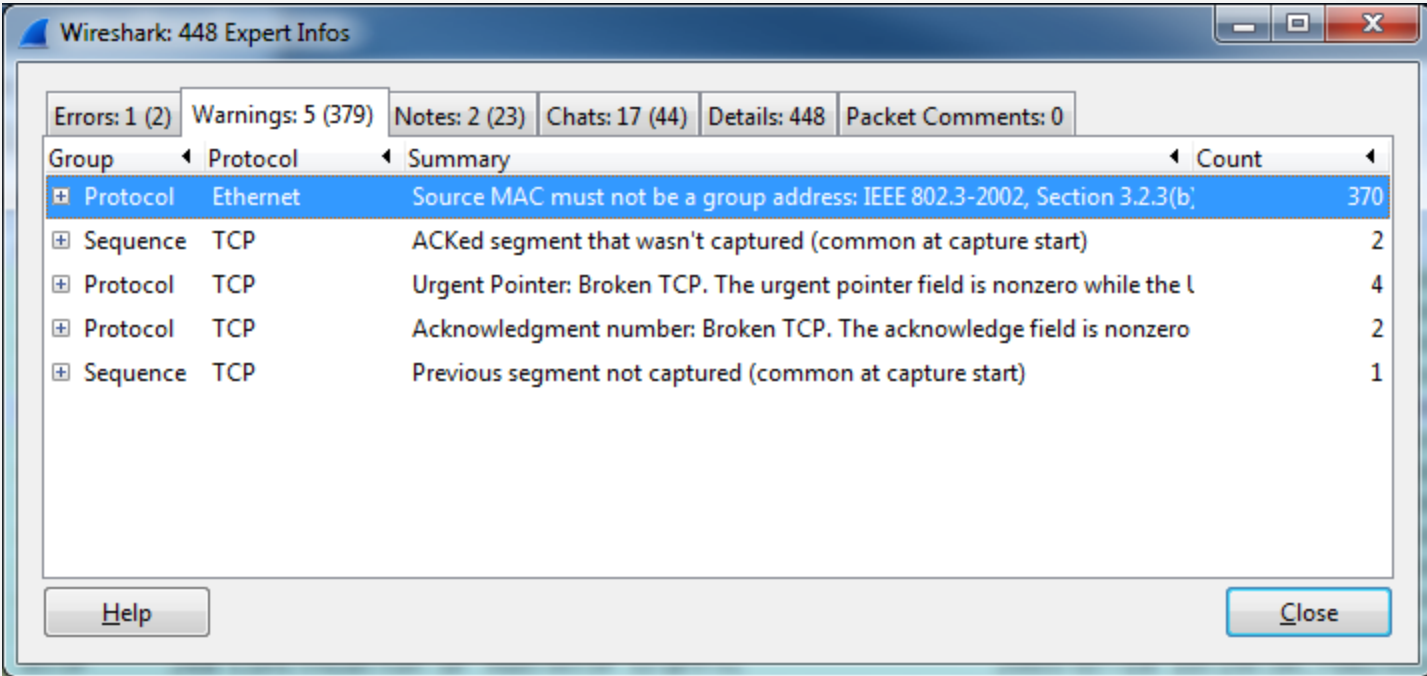
## » Why use the Expert?

- Baseline possible problems
- Remember, false positives
- Information can be limited based on protocol

## » What can you find?

- Clues to possible issues on your network

# The Wireshark Expert



The screenshot shows the 'Wireshark: 448 Expert Infos' window. At the top, there are tabs for 'Errors: 1 (2)', 'Warnings: 5 (379)', 'Notes: 2 (23)', 'Chats: 17 (44)', 'Details: 448', and 'Packet Comments: 0'. Below the tabs is a table with columns for 'Group', 'Protocol', 'Summary', and 'Count'. The table contains the following data:

Group	Protocol	Summary	Count	
+	Protocol	Ethernet	Source MAC must not be a group address: IEEE 802.3-2002, Section 3.2.3(b)	370
+	Sequence	TCP	ACKed segment that wasn't captured (common at capture start)	2
+	Protocol	TCP	Urgent Pointer: Broken TCP. The urgent pointer field is nonzero while the l	4
+	Protocol	TCP	Acknowledgment number: Broken TCP. The acknowledge field is nonzero	2
+	Sequence	TCP	Previous segment not captured (common at capture start)	1

At the bottom of the window, there are 'Help' and 'Close' buttons.

# The Wireshark Expert

## » Wireshark Expert tabs

- Errors
- Warnings
- Notes
- Chats
- Details
- Packet comments

# The Wireshark Expert

The screenshot shows the Wireshark interface with the Expert Info pane open. The pane title is "Wireshark: 448 Expert Infos". At the top, there are tabs for "Errors: 1 (2)", "Warnings: 5 (379)", "Notes: 2 (23)", "Chats: 17 (44)", "Details: 448", and "Packet Comments: 0". Below these tabs is a table with columns for "Group", "Protocol", "Summary", and "Count". The table lists several entries under the "Sequence" group, all with "TCP" as the protocol and "Retransmission (suspected)" as the summary. The entry for packet 353 is selected, and a context menu is open over it, showing options like "Apply as Filter", "Prepare a Filter", "Find Frame", "Colorize Procedure", "Internet Search", and "Copy". The "Internet Search" option is currently selected in the menu. Below the table, there are "Help" and "Close" buttons. The background shows the main packet list and packet details pane.

No.	Group	Protocol	Summary	Count
	Sequence	TCP	Retransmission (suspected)	16
	Packet:		83	1
	Packet:		210	1
	Packet:		353	1
	Packet:		354	1
	Packet:		355	1
	Packet:		356	1
	Packet:		400	1
	Packet:		401	1

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

# Questions?