
Wireshark Reporting

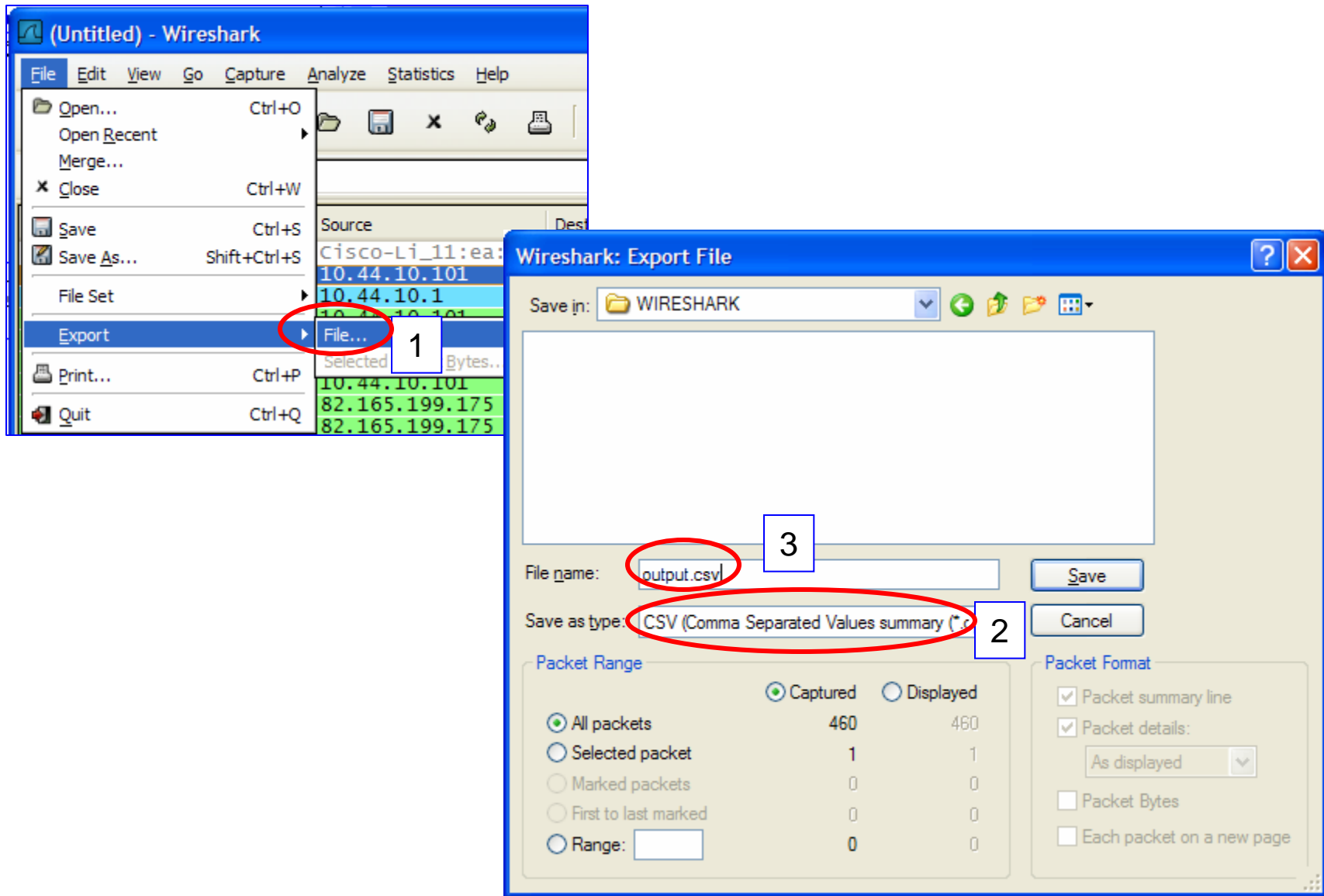


Tony Fortunato, The Technology Firm
Ray Tompkins, Analysis Solutions

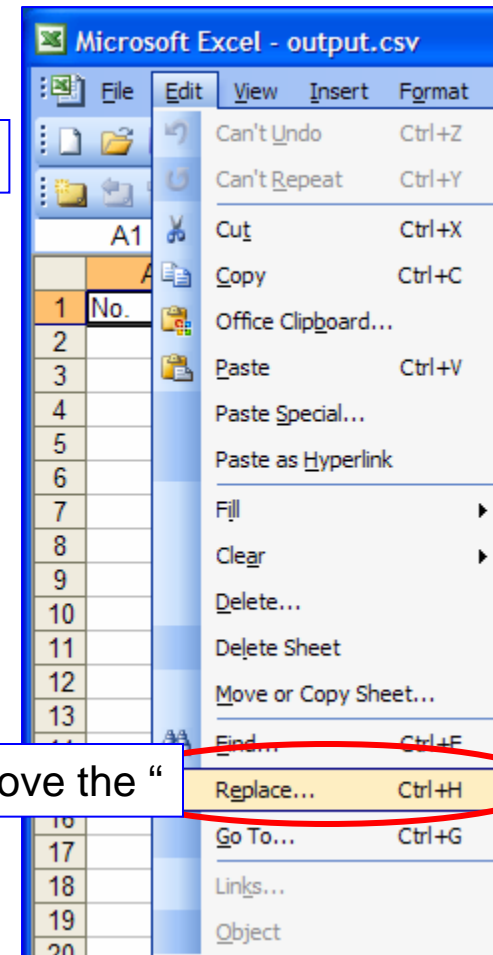
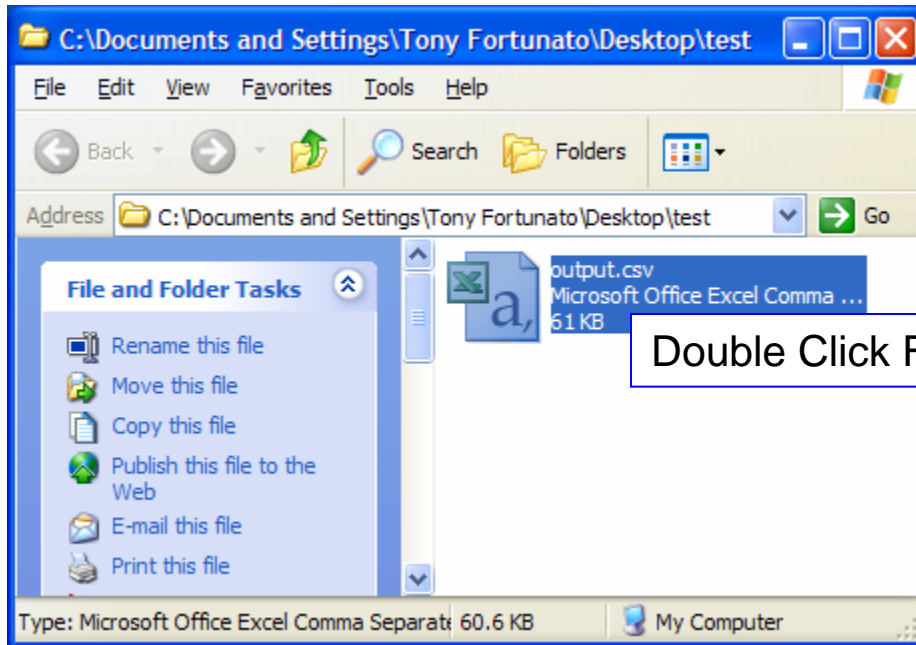
Reporting

- The most difficult part of protocol analysis is visualizing what the frames mean.
- In this section we will take a trace file and import it into Excel.

Create the text file



Open the Text file



Remove Quotes

Before

1

2

After

No.	Time	delta	Bytes	Source	Destination	Protocol	Info
1	13:24:13.8	0	60	Cisco-Li	Spanning	STP	Conf. Root = 32768/00:0f:66:11:ea:16 Cost = 0 Port = 0x8
2	13:24:14.7	0.835718	79	10.44.10.	10.44.10.	DNS	Standard query A www.thetechfirm.com
3	13:24:14.8	0.143995	171	10.44.10.	10.44.10.	DNS	Standard query response A 82.165.199.175
4	13:24:14.8	0.000774	62	10.44.10.	82.165.19	TCP	2191 > 80 [SYN] Seq=0 Len=0 MSS=1460
5	13:24:14.9	0.068161	60	82.165.19	10.44.10.	TCP	80 > 2191 [ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
6	13:24:14.9	0.00006	54	10.44.10.	82.165.19	TCP	2191 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
7	13:24:14.9	0.00014	459	10.44.10.	82.165.19	HTTP	GET / HTTP/1.1

Reformat Time

- Excel will not understand the sub-second values, so we have to separate it.

The screenshot illustrates the process of reformatting time data in Excel. The main window shows a spreadsheet with columns A, B, and C. Column A contains 'No.', B contains 'Time', and C contains 'delta'. A context menu is open over column C, with 'Text to Columns...' highlighted. A second window shows the 'Convert Text to Columns Wizard - Step 2 of 3' dialog box, where a column break is being set for the 'Time' field.

Convert Text to Columns Wizard - Step 1 of 3

The Text Wizard has determined that your data is Delimited. If this is correct, choose Next, or choose the data type that best describes your data.

Original data type

Choose the file type that best describes your data:

- Delimited - Characters such as commas or tabs separate each field.
- Fixed width - Fields are aligned in columns with spaces between each field.

Preview of selected data:

	Time
1	Time
2	13:24:13.871275
3	13:24:14.706993
4	13:24:14.850988
5	13:24:14.851762

Convert Text to Columns Wizard - Step 2 of 3

This screen lets you set field widths (column breaks).

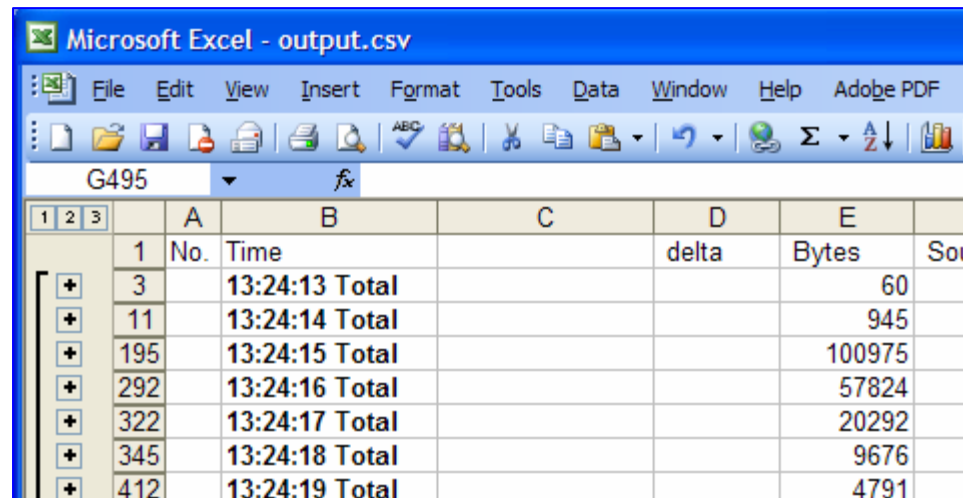
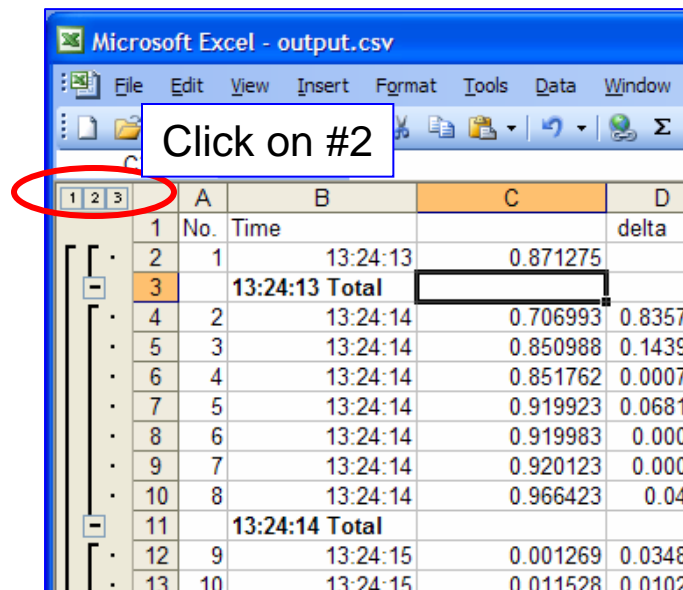
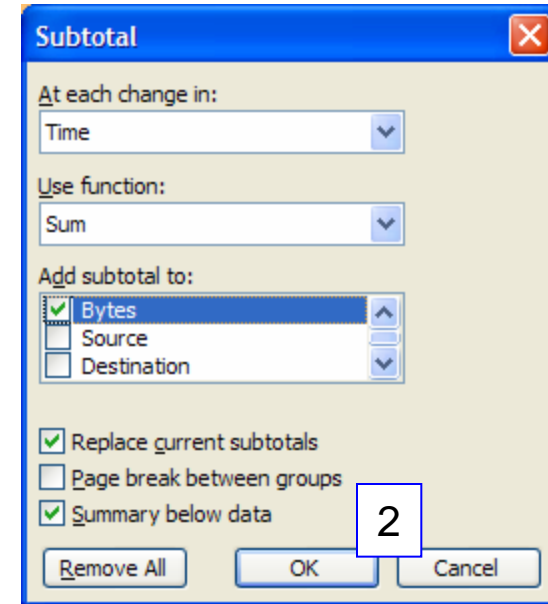
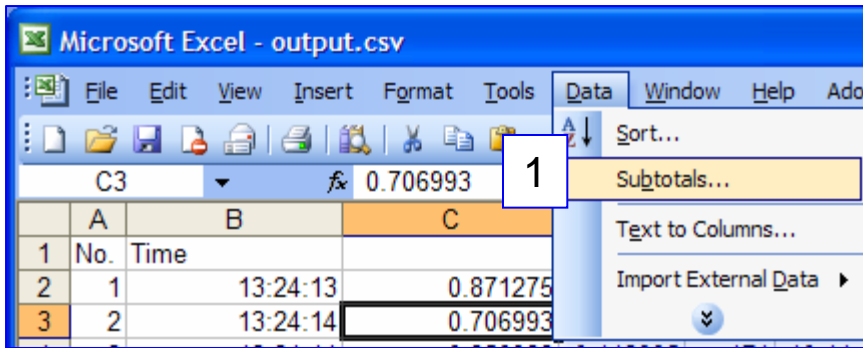
Lines with arrows signify a column break.

To CREATE a break line, click at the desired position.
To DELETE a break line, double click on the line.
To MOVE a break line, click and drag it.

Data preview

	Time
1	Time
2	13:24:13.871275
3	13:24:14.706993
4	13:24:14.850988
5	13:24:14.851762

Create Subtotals



Graph

