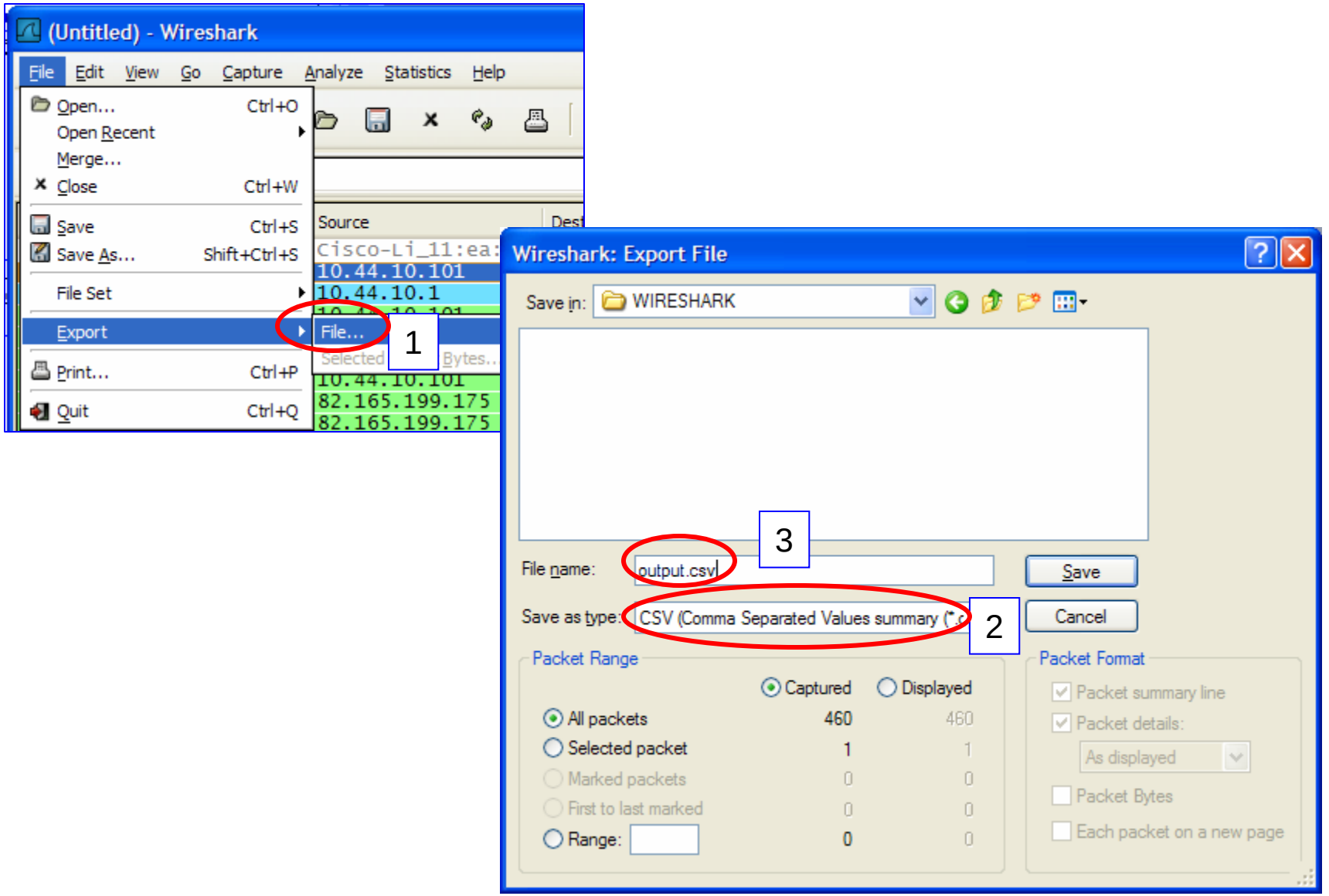
Wireshark Reporting

Tony Fortunato, The Technology Firm
Ray Tompkins, Analysis Solutions

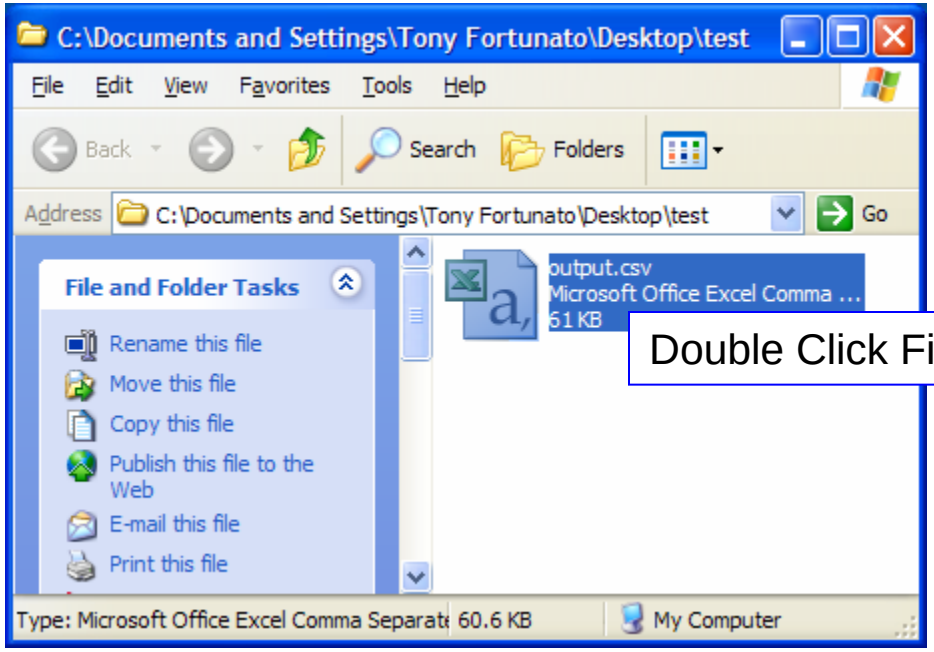
Reporting

- 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.

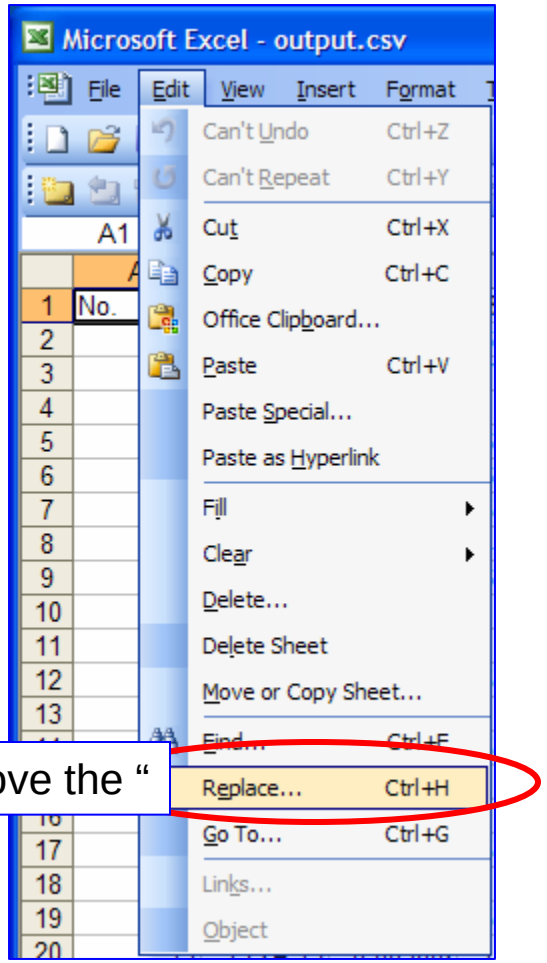
Create the text file



Open the Text file



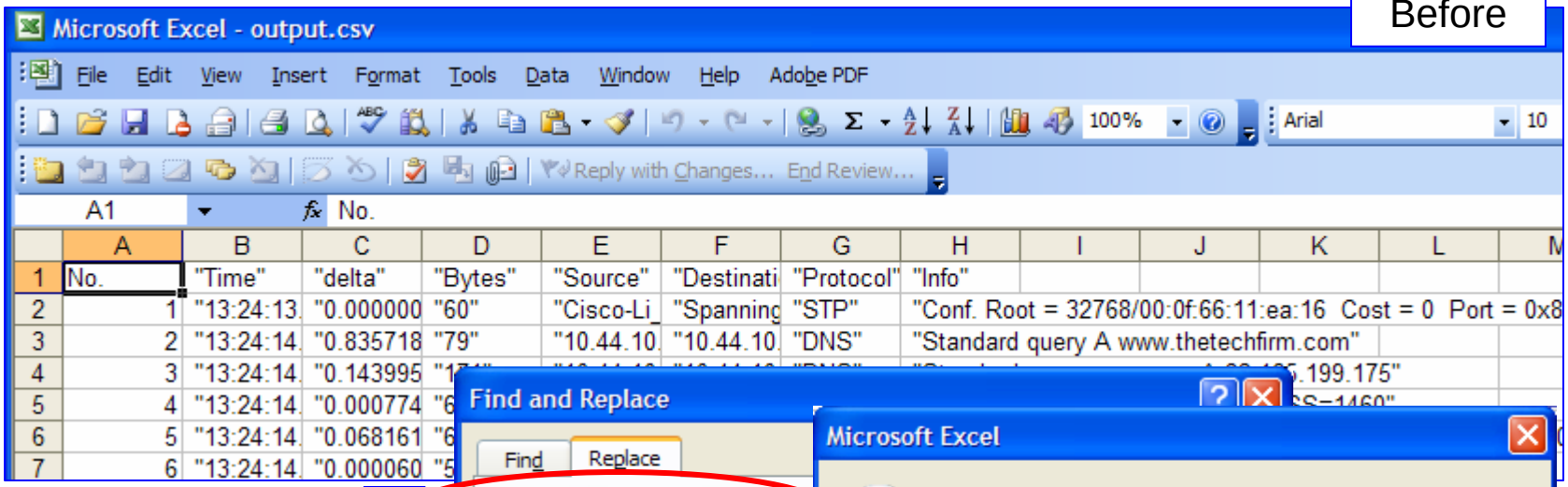
Double Click Filename



We will use Replace Ctrl+H to remove the “

Remove Quotes

Before



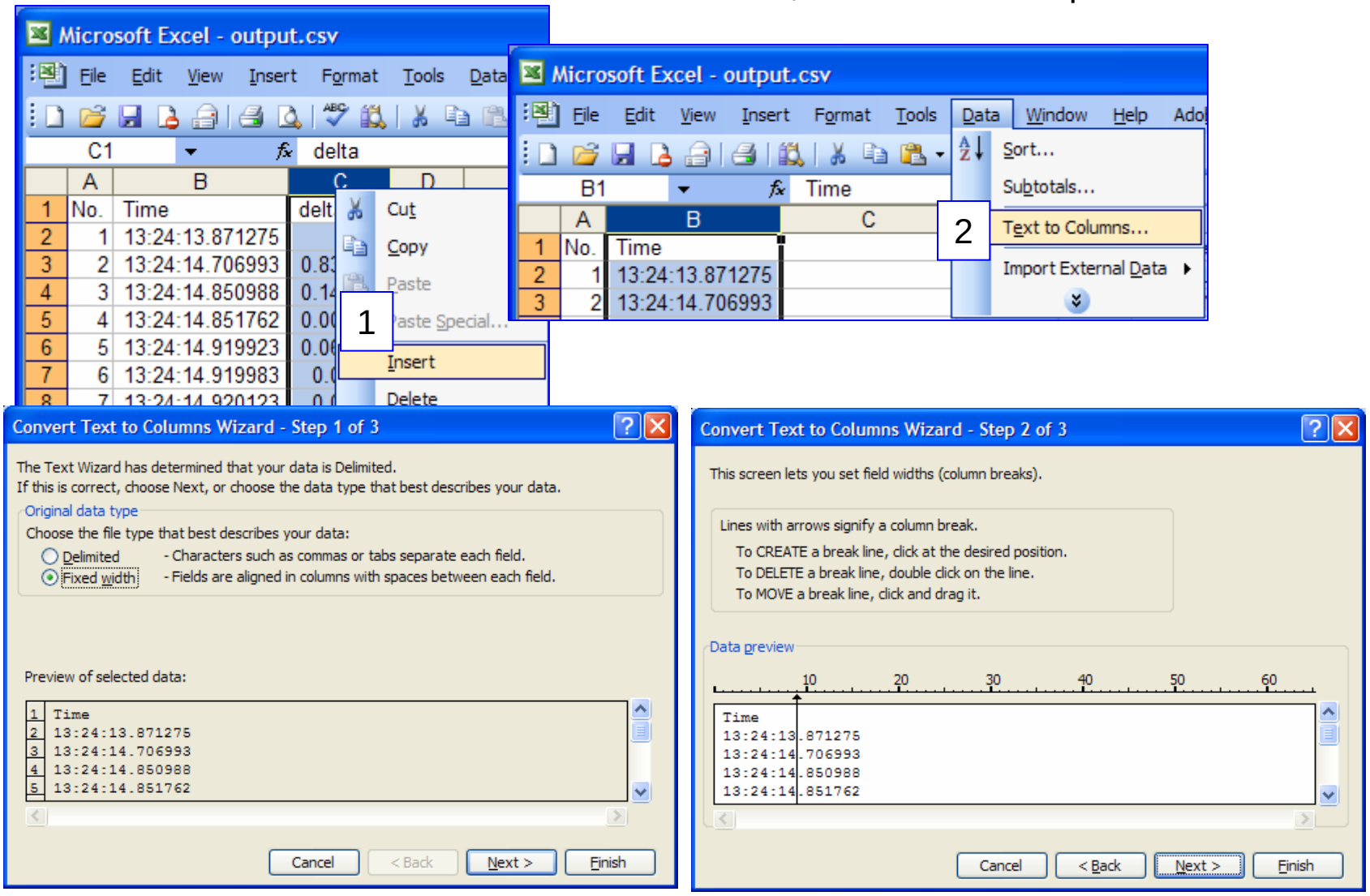
	A	B	C	D	E	F	G	H
1	No.	"Time"	"delta"	"Bytes"	"Source"	"Destinati	"Protocol"	"Info"
2	1	"13:24:13.	"0.000000	"60"	"Cisco-Li_	"Spanning	"STP"	"Conf. Root = 32768/00:0f:66:11:ea:16 Cost = 0 Port = 0x8
3	2	"13:24:14.	"0.835718	"79"	"10.44.10.	"10.44.10.	"DNS"	"Standard query A www.thetechfirm.com"
4	3	"13:24:14.	"0.143995					.199.175"
5	4	"13:24:14.	"0.000774					
6	5	"13:24:14.	"0.068161					
7	6	"13:24:14.	"0.000060					

After

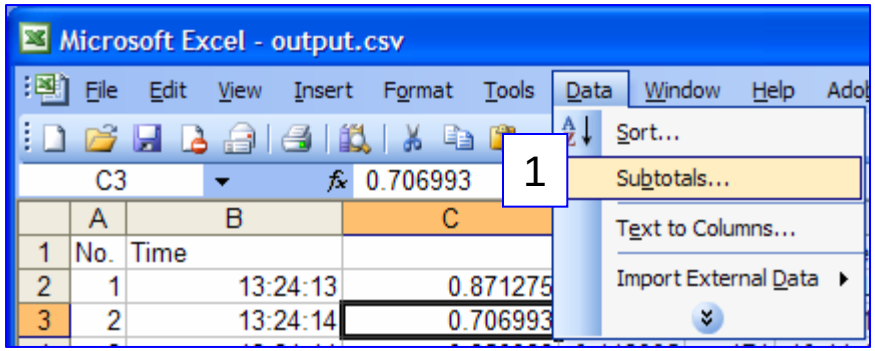
	A	B	C	D	E	F	G	H
1	No.	Time	delta	Bytes	Source	Destinatio	Protocol	Info
2	1	13:24:13.8	0	60	Cisco-Li_	Spanning-	STP	Conf. Root = 32768/00:0f:66:11:ea:16 Cost = 0 Port = 0x8
3	2	13:24:14.7	0.835718	79	10.44.10.	10.44.10.	DNS	Standard query A www.thetechfirm.com
4	3	13:24:14.8	0.143995	171	10.44.10.	10.44.10.	DNS	Standard query response A 82.165.199.175
5	4	13:24:14.8	0.000774	62	10.44.10.	82.165.19	TCP	2191 > 80 [SYN] Seq=0 Len=0 MSS=1460
6	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
7	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
8	7	13:24:14.9	0.00014	459	10.44.10.	82.165.19	HTTP	GET / HTTP/1.1

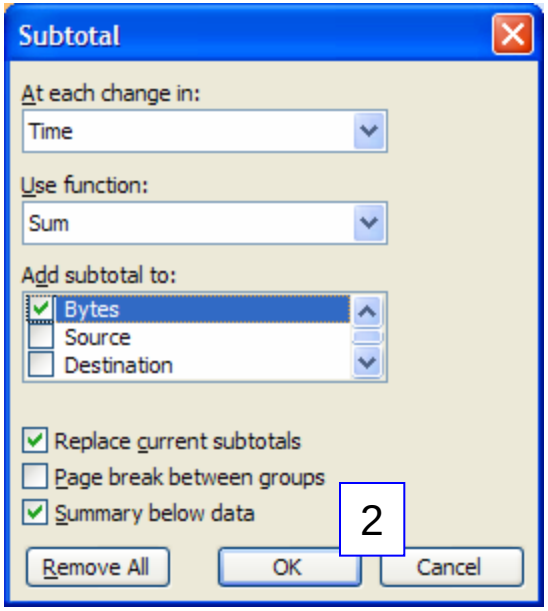
Reformat Time

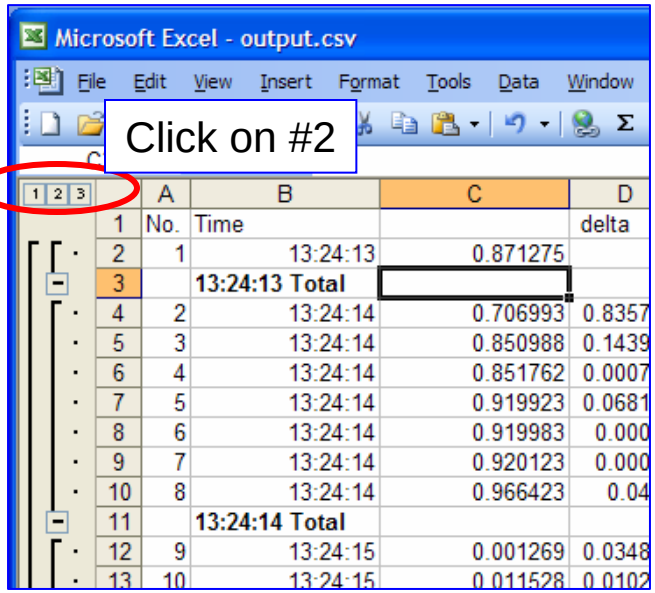
- Excel will not understand the sub-second values, so we have to separate it.

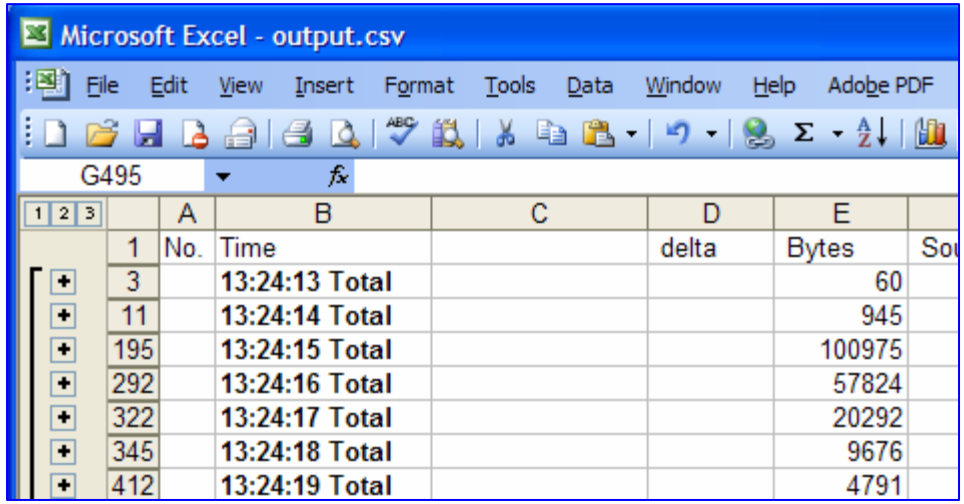


Create Subtotals









Graph