Wireshark Developer and User Conference

B-1: I've Just Downloaded Wireshark… Now What?

Tuesday June 14, 2011 - 10:15am - 11:30am

Betty DuBois

Principal Consultant | DuBois Training & Consultant, LLC
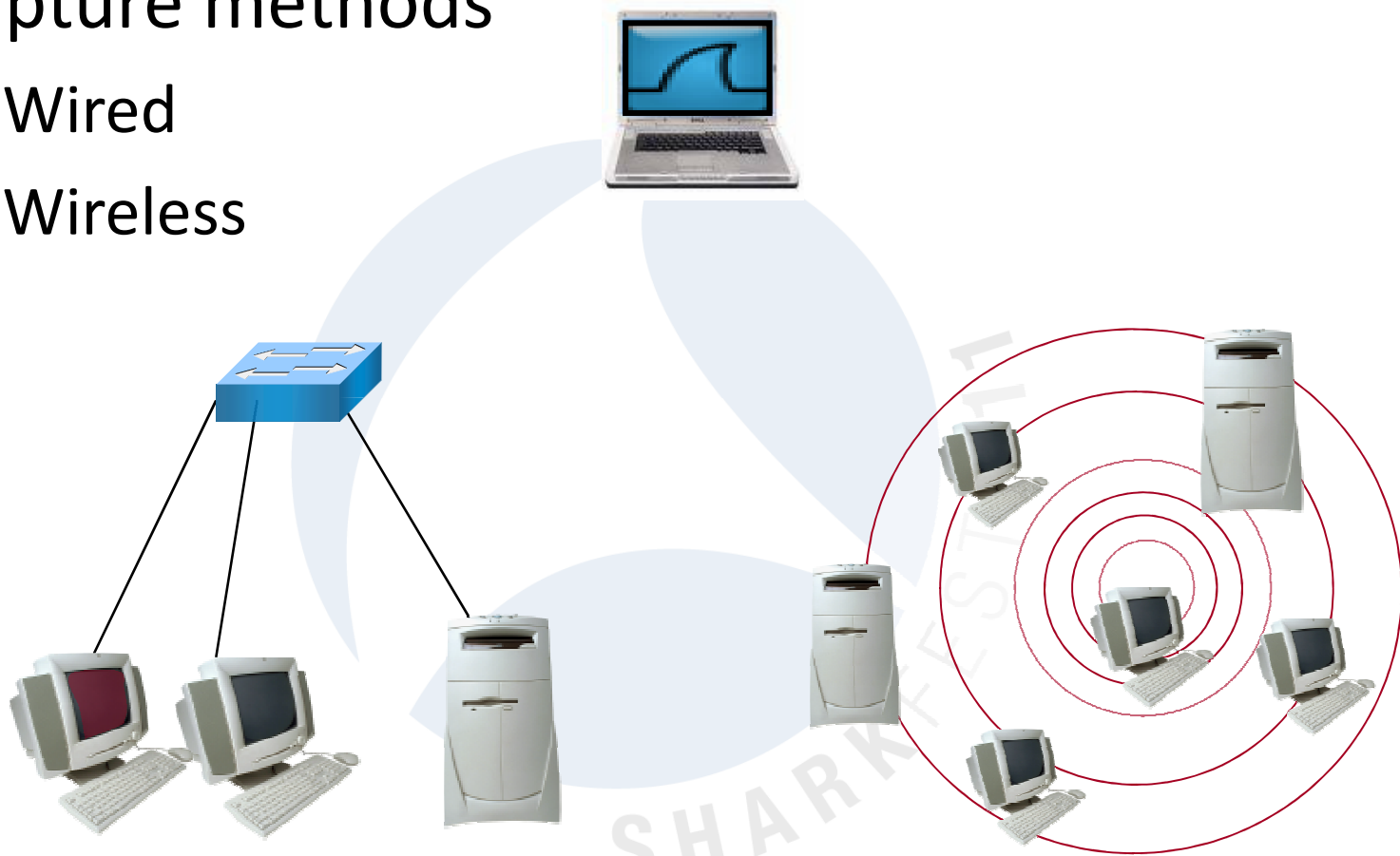
Betty@DTCpackets.com

SHARKFEST '11
Stanford University
June 13-16, 2011

Agenda

- **Data Capture**
  - Capture methods
    - Caveats
  - Capture interfaces

- **Data Analysis**
  - Statistics
    - Summary Information
    - Protocol hierarchy
    - Conversations
    - Endpoints
  - Basic display filtering
  - Reassembly
  - Coloring rules

Data Capture – How do I get the data?

- Capture methods
  - Wired
  - Wireless

Data Capture – How do I get the data?

- ## Capture Caveats
  - ### Wired
    - Mirrors/Monitors/SPANs
    - Taps
    - Hubs
  - ### Wireless
    - Promiscuous vs. rfmon/monitor mode
    - AirPcap

Data Capture - Options

- Which interface to use?

- What about permissions?
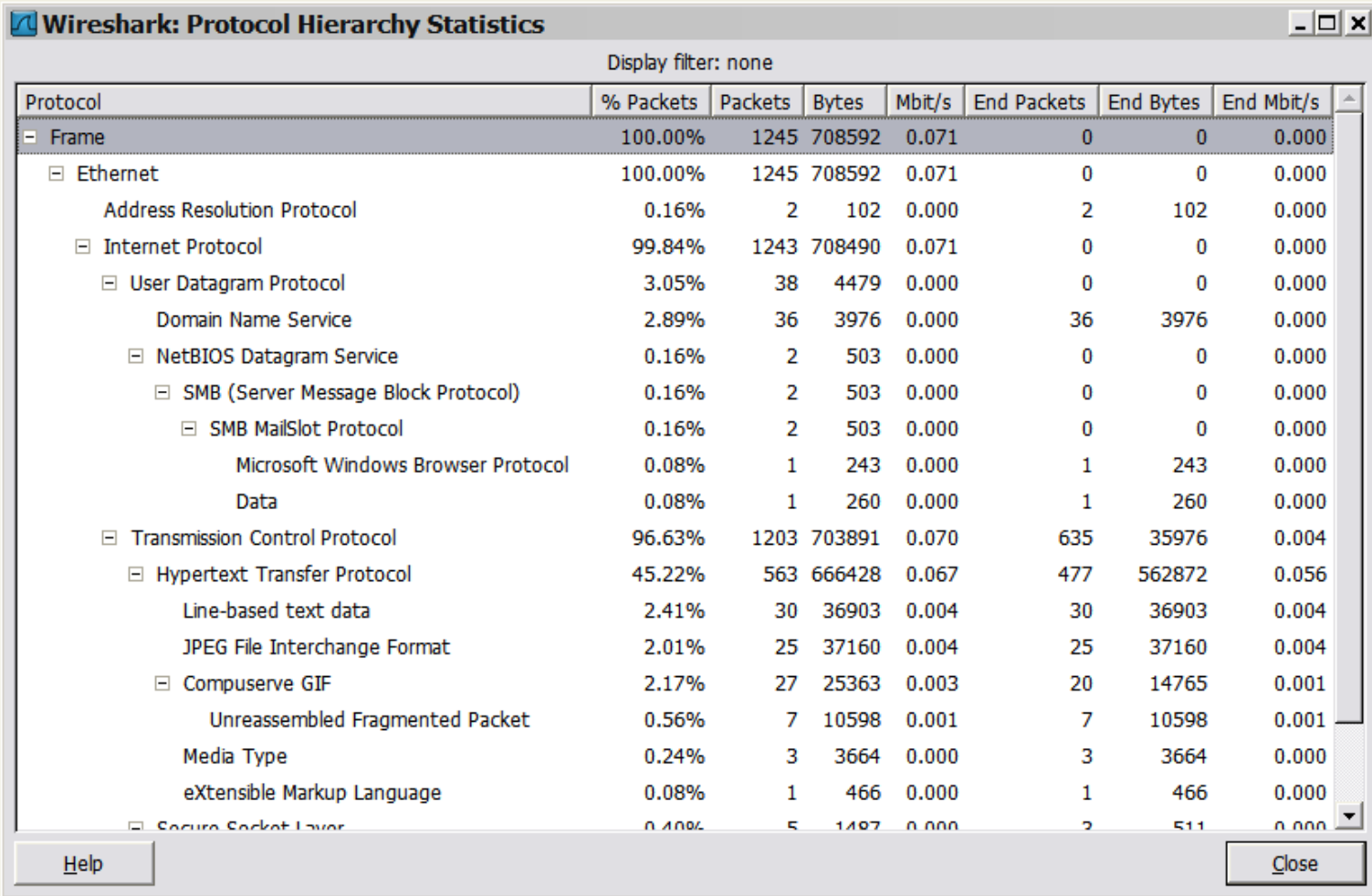
Data Analysis

- ## Don'ts
  - Don't get caught in the vortex!
  - Don't start by scrolling through the packets

- ## Do's
  - Use Statistics to baseline your environment
  - Use Statistics to determine where your focus should be
  - Use filtering to focus

Data Analysis – Statistics > Protocol Hierarchy

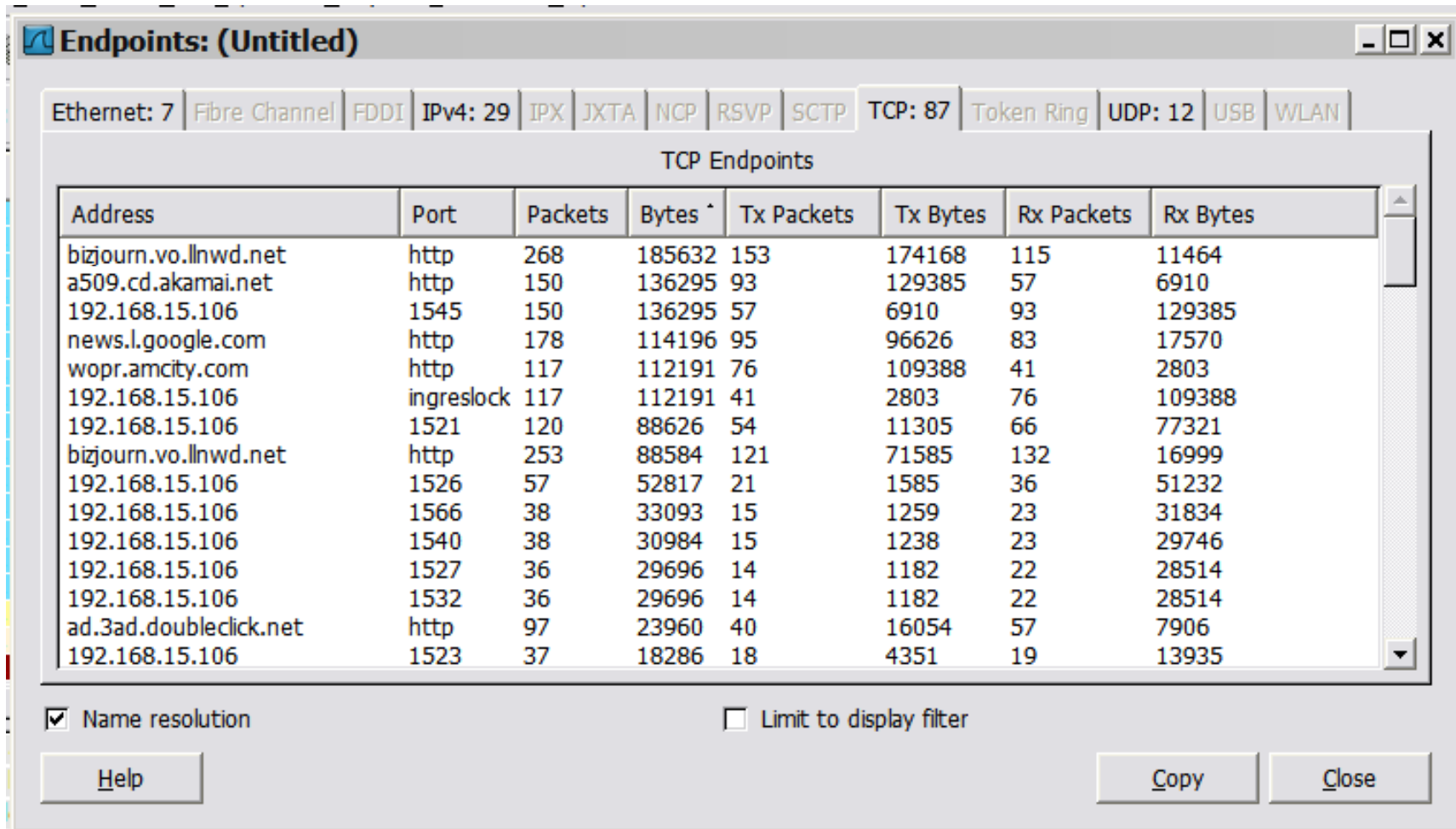

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	1245	708592	0.071	0	0	0.000
Ethernet	100.00%	1245	708592	0.071	0	0	0.000
Address Resolution Protocol	0.16%	2	102	0.000	2	102	0.000
Internet Protocol	99.84%	1243	708490	0.071	0	0	0.000
User Datagram Protocol	3.05%	38	4479	0.000	0	0	0.000
Domain Name Service	2.89%	36	3976	0.000	36	3976	0.000
NetBIOS Datagram Service	0.16%	2	503	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.16%	2	503	0.000	0	0	0.000
SMB MailSlot Protocol	0.16%	2	503	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.08%	1	243	0.000	1	243	0.000
Data	0.08%	1	260	0.000	1	260	0.000
Transmission Control Protocol	96.63%	1203	703891	0.070	635	35976	0.004
Hypertext Transfer Protocol	45.22%	563	666428	0.067	477	562872	0.056
Line-based text data	2.41%	30	36903	0.004	30	36903	0.004
JPEG File Interchange Format	2.01%	25	37160	0.004	25	37160	0.004
Compuserve GIF	2.17%	27	25363	0.003	20	14765	0.001
Unreassembled Fragmented Packet	0.56%	7	10598	0.001	7	10598	0.001
Media Type	0.24%	3	3664	0.000	3	3664	0.000
eXtensible Markup Language	0.08%	1	466	0.000	1	466	0.000
Secure Socket Layer	0.40%	5	1487	0.000	3	511	0.000

Help   Close

Data Analysis – Statistics > End Points

- Add GeoIP info - Instructions on wiki.wireshark.org

Data Analysis – Statistics > Conversations

Data Analysis – Basic Display Filters

- Filter Bar – Auto-complete since 1.2
  - The Filter bar will change colors to signify if your syntax is correct
    - Green is correct
    - Red is incorrect
    - Yellow is questionable
  - The Filter dropdown will let you chose your 10 most recent filters by default
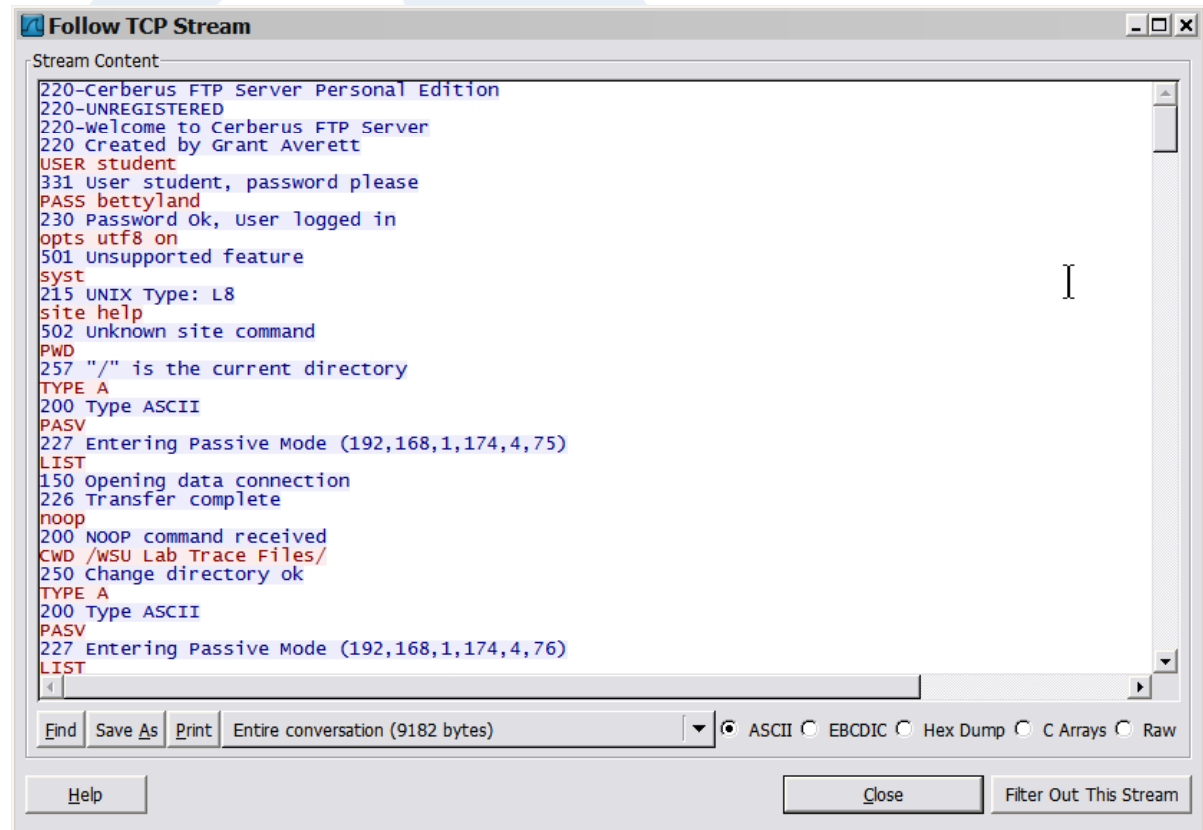   - You can increase this in Edit>Preferences
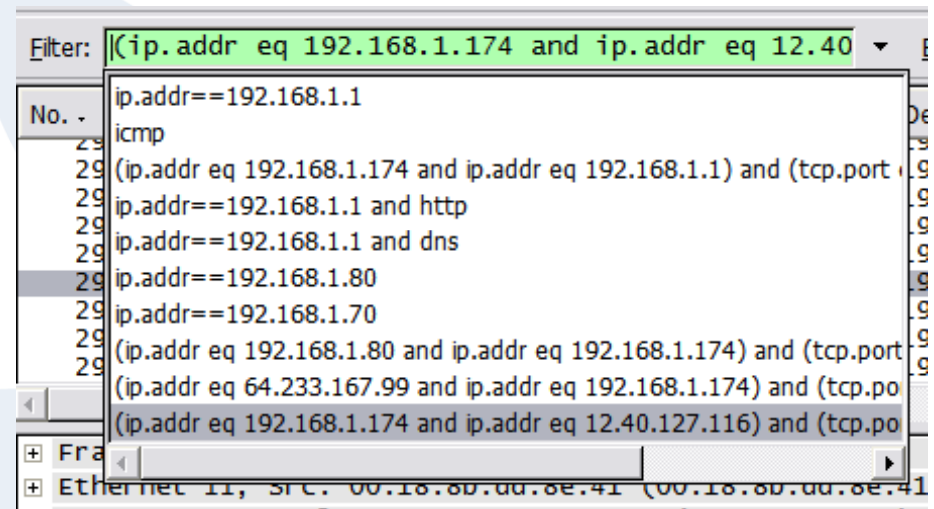
Data Analysis – Basic Display Filters

- ## When in doubt, right-click.
  - Find the fields you are interested in first, then build your filters with a right-click.
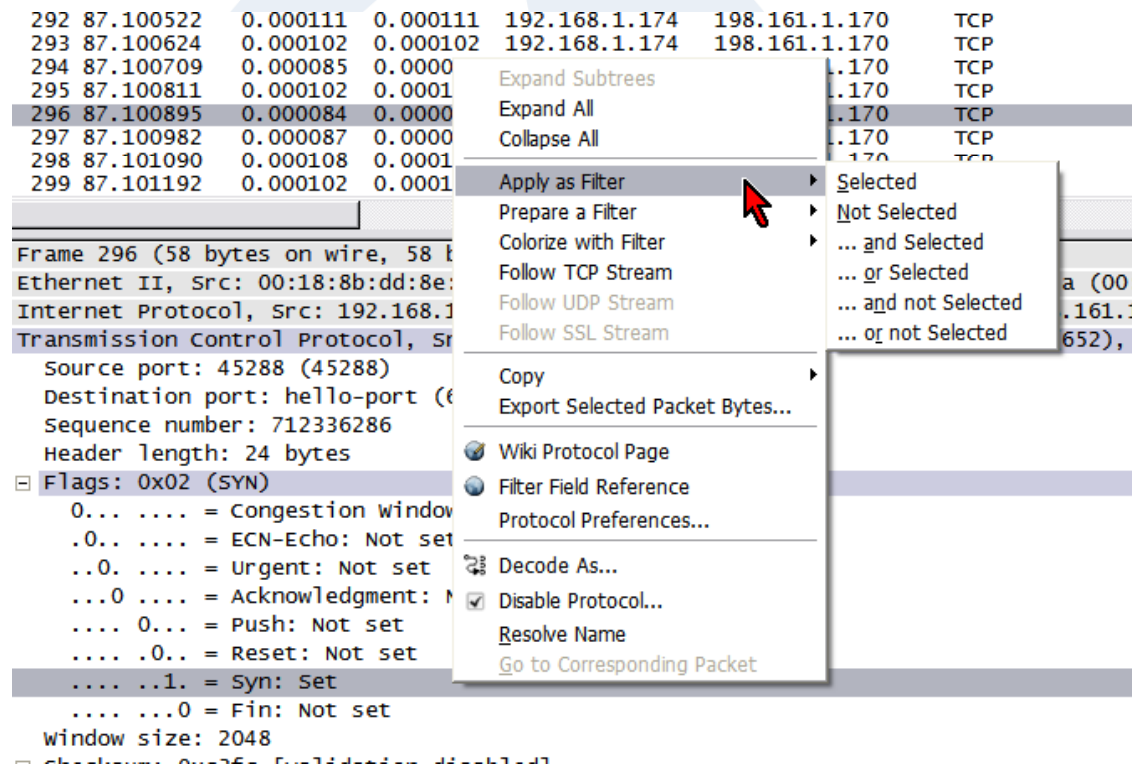
Data Analysis - Reassembly

- Follow the Streams – Favorite feature in Wireshark

- Available stream types:
  - TCP
  - UDP
  - SSL

Data Analysis – Coloring Rules

- Colors help you focus on specific protocols, and/or to spot errors quickly.

Data Analysis – Coloring Rules

- Rules to live by:
  - Color rules are read like an ACL
    - First rule in the list to apply wins, even if multiple rules apply
  - Rule sets can be shared among friends with Import/Export
  - Use an empty rule set if you normally use a complex rule set, but commonly turn off your colors. Your files will load faster.
  - Check out Laura's presentation on customization at 2pm today!!
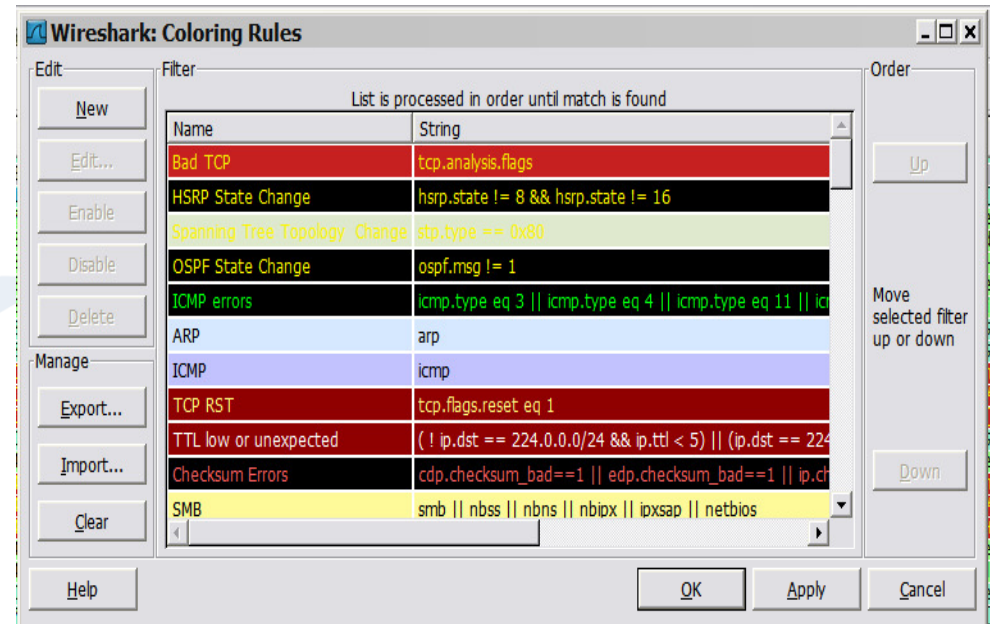
Q & A

- Questions?????

Thanks For Coming!

Enjoy the rest of the conference.