T2-5 Advanced Capture and Display Filtering

April 1, 2008

Tony Fortunato

Sr Network Specialist | The Technology Firm

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

About your Presenter

Tony Fortunato, Sr Network Specialist, The Technology Firm

Certified Fluke Networks and Wireshark Instructor

Website: www.thetechfirm.com

A Senior Network Specialist with experience in performance testing, network design, implementation, and troubleshooting LAN/WAN/Wireless networks, desktops and servers since 1989.

Tony has taught at Colleges/Universities, Networld/Interop and many onsite corporate settings to thousands of analysts.

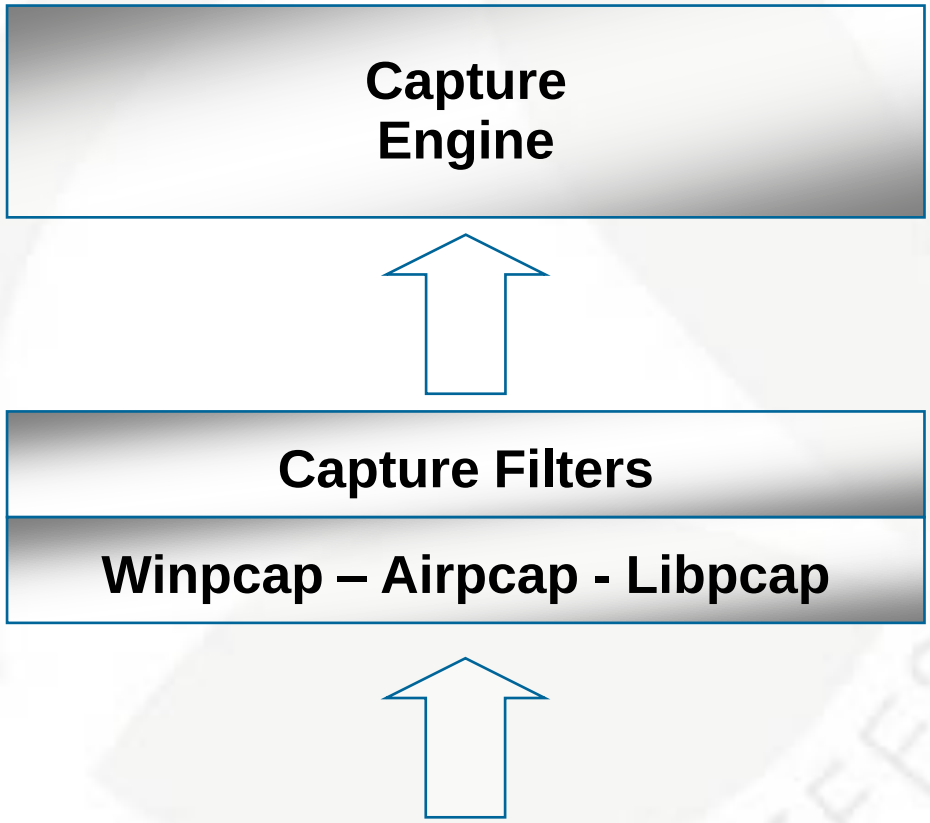
Tony is an authorized and certified Fluke Networks and Wireshark Instructor. His Pine Mountain Group CNA Level I and II certification demonstrates his vendor neutral approach to network design, support and implementations.

Tony has architected, installed and supported various types of Residential Wireless High Speed as well as hundreds of WIFI hotspots.. Tony combines custom programs, open source and commercial software to ensure a simple support infrastructure.

Tony works on networks from 2 to 120,000 nodes and specializes in post installation performance/design review. This process involves using various tools (Protocol analyzers, traffic generators and network management) and working on multi-vendor equipment (switches, routers, servers, etc).

Tony works at customer sites within a range of capacities from project management, network design, consulting, troubleshooting, designing customized courses and assisting with installing physical equipment.

Capturing Traffic



Network

CACE TECHNOLOGIES
www.wiresharkU.com
WIRESHARK UNIVERSITY

Options

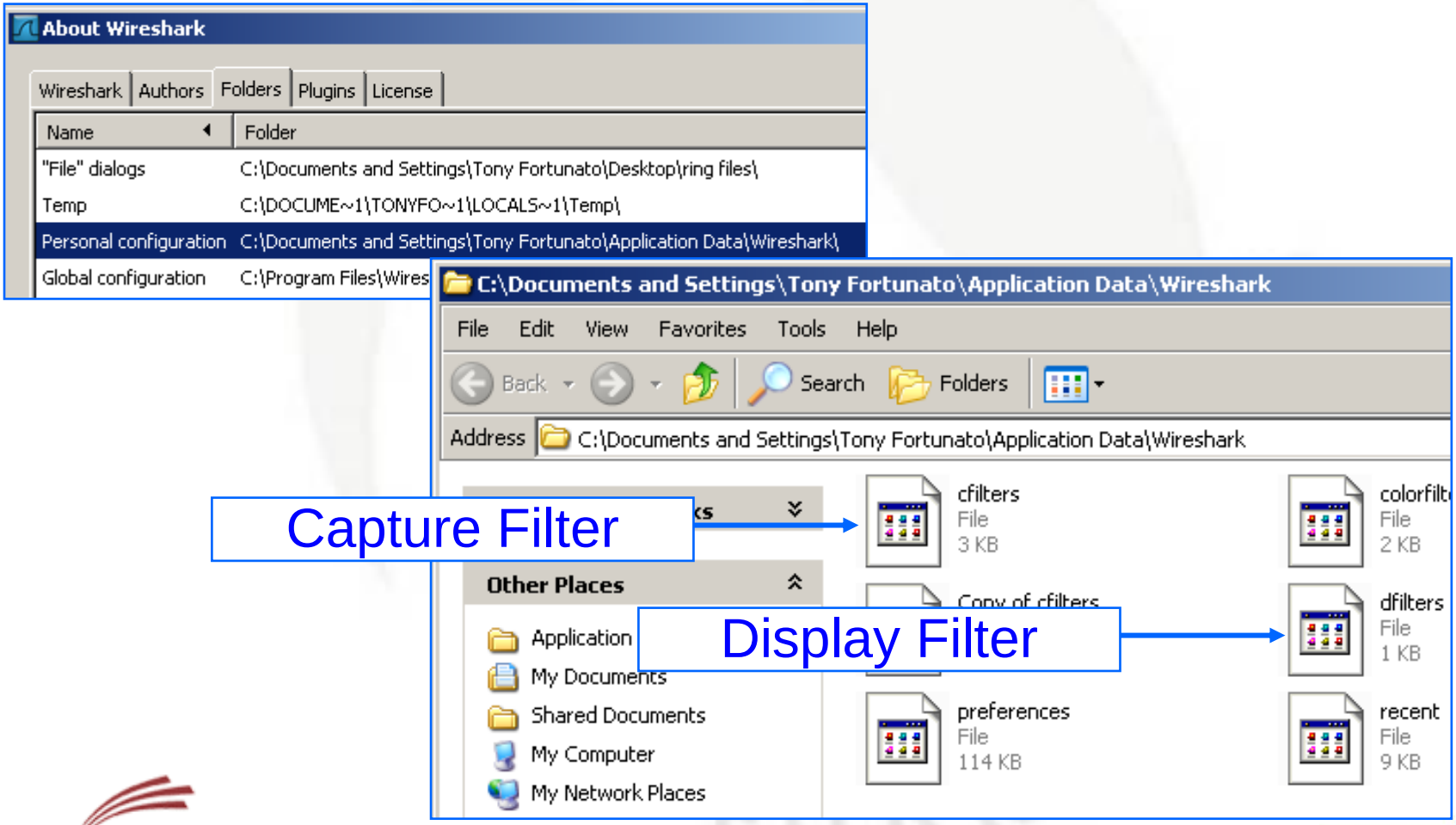
When capturing with Wireshark, you have 2 options;

- Using the GUI
- Using the command prompt and *tshark*
  - *tshark –D*
  - *tshark –i*

CACE TECHNOLOGIES
SHARKFEST '08
www.wiresharkU.com
WIRESHARK UNIVERSITY

Capture Filters

- Based on the tcpdump format
- Location identified in Help -> About under Folders Tab

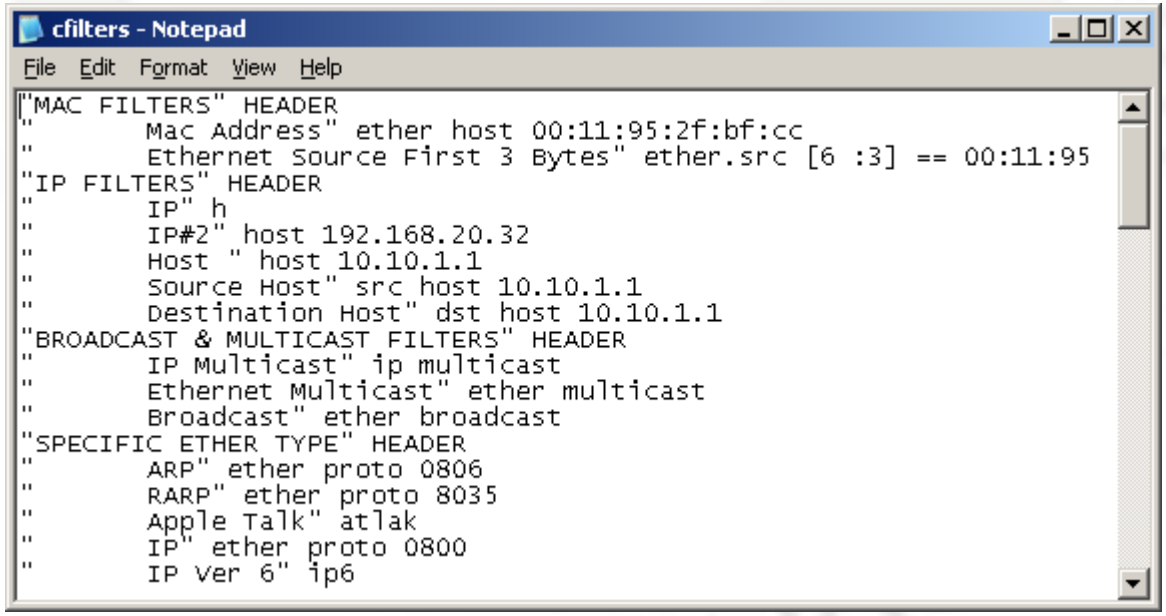


CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY

cfilters file notes

- Make sure you use a text editor, or save in a text format
- Ensure you have a blank line at the end of the file
- Good idea to create a header and indent the related filters


cfilters - Notepad

File Edit Format View Help

```
"MAC FILTERS" HEADER
"        Mac Address" ether host 00:11:95:2f:bf:cc
"        Ethernet Source First 3 Bytes" ether.src [6 :3] == 00:11:95
"IP FILTERS" HEADER
"        IP" h
"        IP#2" host 192.168.20.32
"        Host " host 10.10.1.1
"        Source Host" src host 10.10.1.1
"        Destination Host" dst host 10.10.1.1
"BROADCAST & MULTICAST FILTERS" HEADER
"        IP Multicast" ip multicast
"        Ethernet Multicast" ether multicast
"        Broadcast" ether broadcast
"SPECIFIC ETHER TYPE" HEADER
"        ARP" ether proto 0806
"        RARP" ether proto 8035
"        Apple Talk" atlak
"        IP" ether proto 0800
"        IP Ver 6" ip6
```

Capture Filter Reference

Command	Description
ether host *MAC address*	Capture all packets to and from a MAC *address*
IP Filters	
host *ip address*	Capture all packets to and from an *ip address*
src host *ip address*	Capture all packets from an *ip address*
dst host *ip address*	Capture all packets to an *ip address*
TCP/UDP Filters	
port *port*	Capture all packets to and from a port number
src port *port*	Capture all packets from a port number
dst port *port*	Capture all packets to a port number
IP Network Filters	
net *net*	Capture all packets to and from a *subnet*
src net *net*	Capture all packets from a *subnet*
dst net *net*	Capture all packets to a *subnet*

Capture Filter Examples

Command	Description
ether host 00:15:c5:37:40:60	Capture all packets to and from MAC 00:15:c5:37:40:60
IP Filters	
host 10.44.10.1	Capture all packets to and from 10.44.10.1
host www.wireshark.org	Capture all packets from www.wireshark.org
TCP/UDP Filters	
port 80	Capture all packets to and from TCP/UDP port number 80
portrange 67-68	Capture all DHCP bootps/bootpc
port http	Capture all packets from devices using http
tcp portrange 1200-2000	Capture all packets with TCP port # 1200-2000
IP Network Filters	
net 10.44.10	Capture all packets to and from a subnet 10.44.10
arp	Capture all arp packets
udp	Capture all udp packets
tcp	Capture all tcp packets

Supported Capture Protocols

- arp *Address Resolution Protocol*
- esp *Encapsulating Security Payload*
- icmp *Internet Control Message Protocol*
- icmp6 *Internet Control Message Protocol, for IPv6*
- igmp *Internet Group Management Protocol*
- igrp *Interior Gateway Routing Protocol*
- ip *Internet Protocol*
- ip6 *Internet Protocol version 6*
- pim *Protocol Independent Multicast*
- rarp *Reverse Address Resolution Protocol*
- stp *Spanning Tree Protocol*
- tcp *Transmission Control Protocol*
- udp *User Datagram Protocol*
- vrrp *Virtual Router Redundancy Protocol*

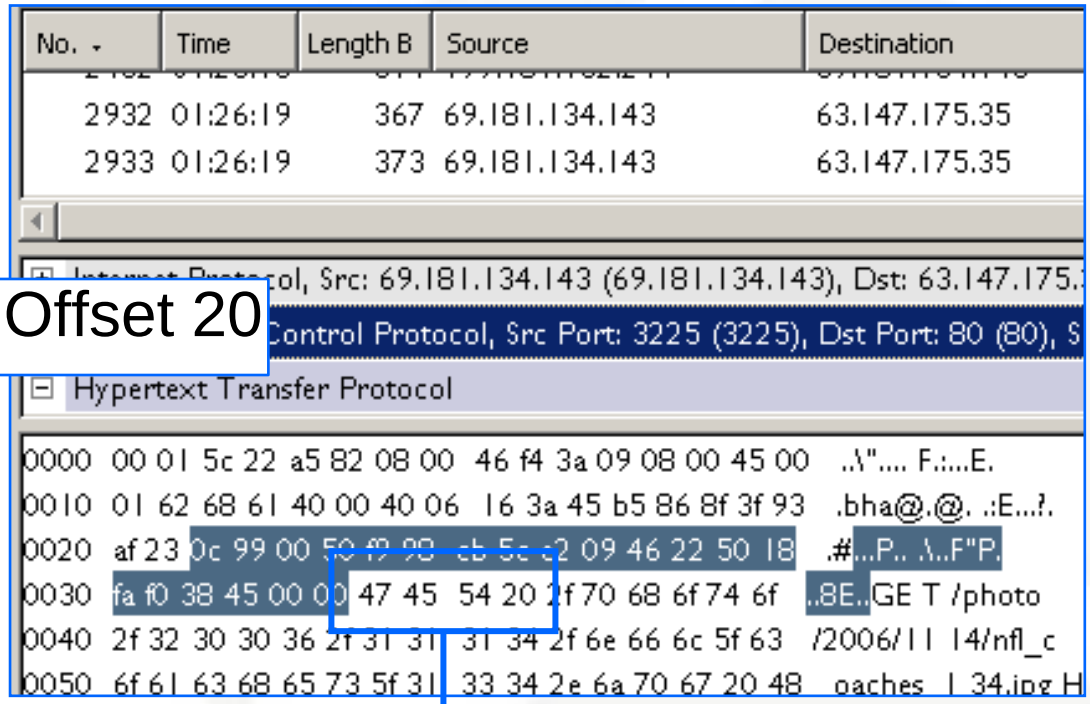
Data Pattern Offsets

To retrieve a single byte from a packet, use square brackets to indicate the offset of that byte from the beginning of a particular protocol. Offsets start at zero (e.g.,tcp[0] gives the first byte in the TCP header and tcp[1] gives the second byte)

TCP Header Layout

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	26	27	28	29	30	31	32
Source Port																Destination Port															
Sequence Number																															
Acknowledgment Number																															
Data Offset				Reserved						URG	ACK	PSH	RST	SYN	FIN	Windows															
Checksum																Urgent Pointer															
Options																								Padding							
Data																															

HTTP Get Offset Example



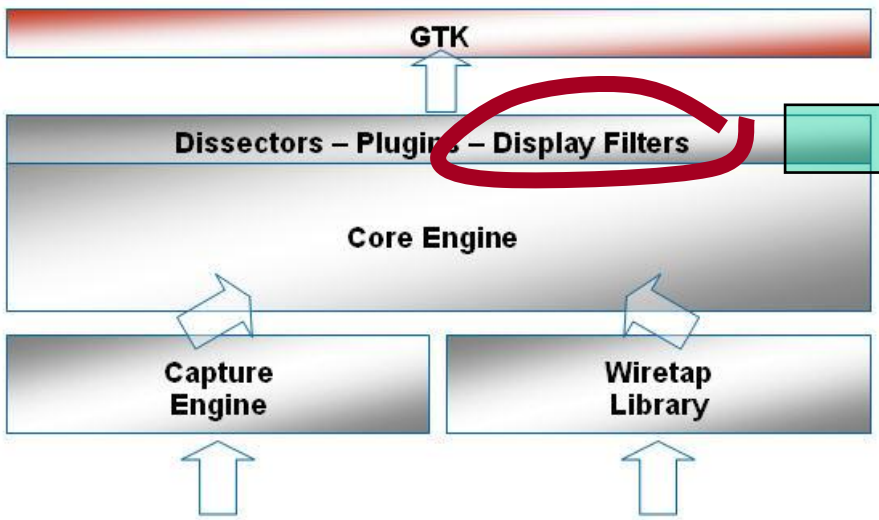
TCP Offset 20

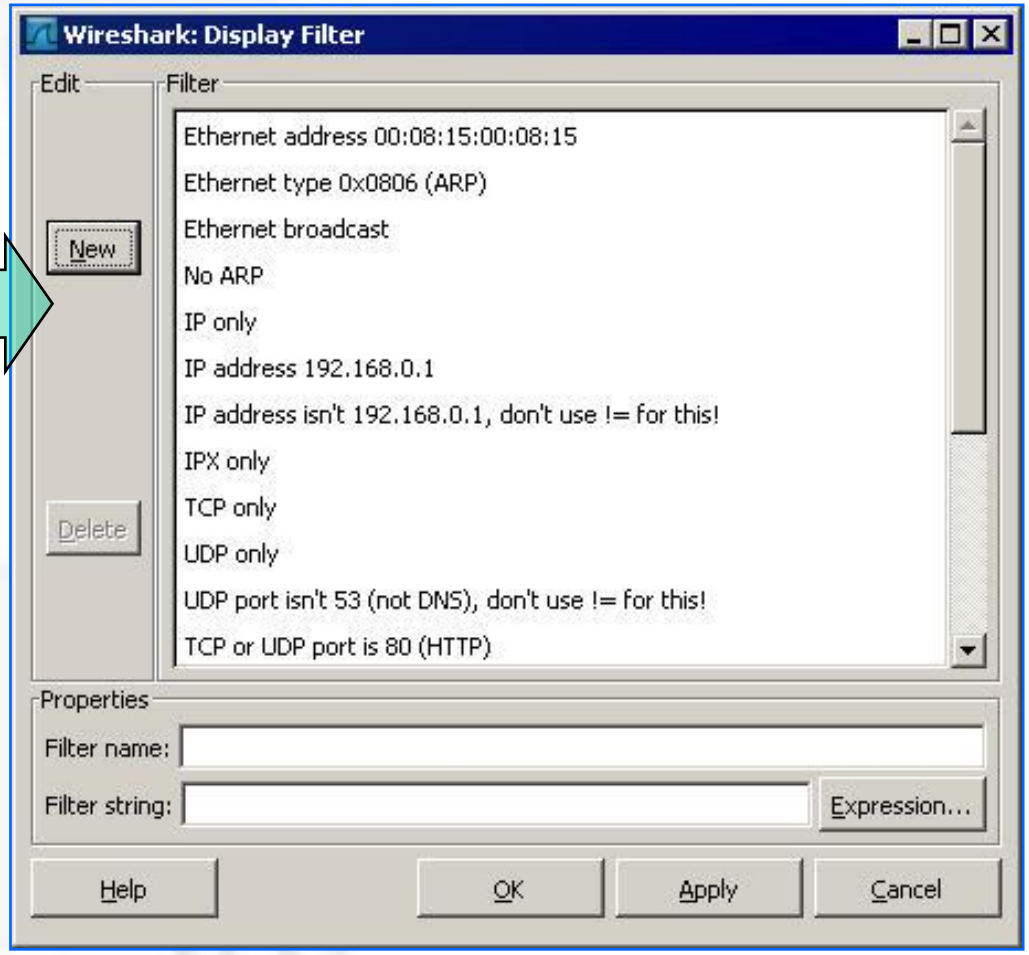
4 Bytes of Data

CACE TECHNOLOGIES
WIRESHARK UNIVERSITY www.wiresharkU.com
SHARKFEST '08

Overview of Display Filters

- Can visit http://www.wireshark.org/docs/dfref





Display Filter Syntax

Visit www.wireshark.org for the master list of Display Filter field names, types, descriptions and versions

Display Filter Reference

Wireshark's most powerful feature is its vast array of display filters (over 51000 as of version 0.99.5). They let you drill drill down to the exact traffic you want to see and are the basis of many of Wireshark's other features, such as the coloring rules.

This is a reference. If you need help using display filters, please see the wireshark-filter and the User's Guide.

Index

2 3 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Display Filter Reference: Transmission Control Protocol

Protocol field name: tcp
Versions: 0.10.0 to 0.99.5
Back to Display Filter Reference

Field name	Type	Description	Versions
tcp.ack	Unsigned 32-bit integer	Acknowledgement number	0.10.0 to 0.99.5
tcp.analysis.ack_lost_segment	None	ACKed Lost Packet	0.10.0 to 0.99.5
tcp.analysis.ack_rtt	Time duration	The RTT to ACK the segment was	0.10.0 to 0.99.5
tcp.analysis.acks_frame	Frame number	This is an ACK to the segment in frame	0.10.0 to 0.99.5
tcp.analysis.duplicate_ack	None	Duplicate	0.10.0 to

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

Operators and Advanced Filters

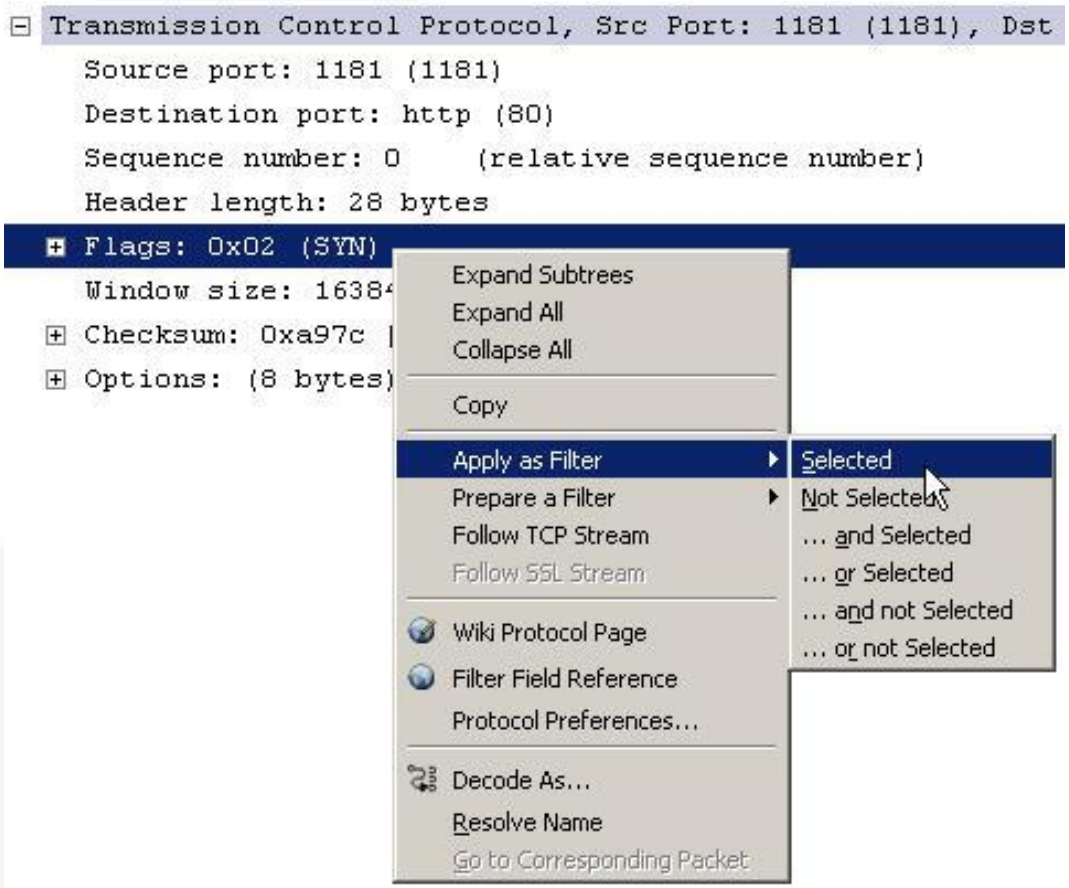
Operators

`==`	or	`eq`	equal to
`||`	or	`or`	or
`>`	or	`gt`	greater than
`>=`	or	`ge`	greater than or equal to
`<=`	or	`le`	less than or equal to
`<`	or	`lt`	less than
`!`	or	`not`	not
`!=`	or	`ne`	not equal to
`contains`			
`matches`			

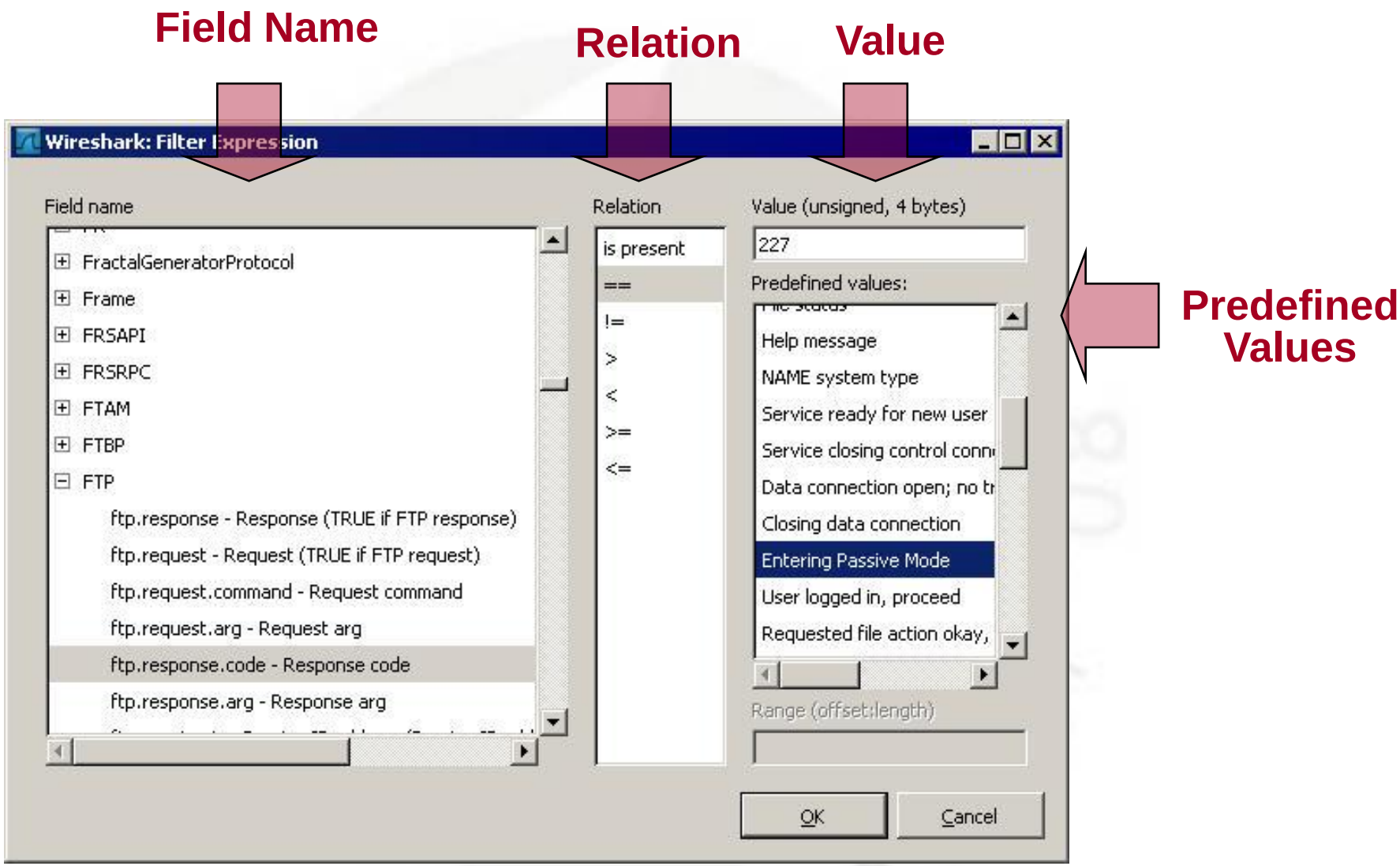
SHARKFEST '08

Build Filters Based on Captured Packet

Right mouse click on any field and either **Apply** or **Prepare** a filter based on the field and value (with an implied ‘equal to’ operator).



Build Filters Based on Expressions



Build Filters from Statistics Reports

I use the ‘Prepare a Filter’ to build my filter

Conversations: novotel full capture.cap

Ethernet: 76 | Fibre Channel | FDDI | IPv4: 52 | IPX | JXTA | SCTP | TCP: 7 | Token Ring | UDP: 193 | USB | WLAN | NCP | RSVP

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Dur
10.0.1.200	128.46.156.117	33			78126	1966	2976524	0.184944000	42
10.0.1.245	239.255.255.250	36			15486	0	0	276.284156999	6.7
10.0.1.239	239.255.255.250	29						121.839433999	197
10.0.1.230	10.255.255.255	10						2.902963000	415
10.0.1.247	224.0.0.251	10						50.612903999	347
10.0.1.205	239.255.255.250	18						270.685227999	8.4
10.0.1.243	10.255.2								
10.0.1.200	72.14.21								
10.0.1.200	10.0.1.2								
10.0.1.239	255.255.								
10.0.1.230	224.0.0.								
10.0.1.239	10.255.2								
10.0.1.9	10.255.2								
10.0.1.52	10.255.2								
10.0.2.0	10.255.2								

Apply as Filter
Prepare a Filter
Find Packet
Colorize Conversation

Selected
Not Selected
... and Selected

A <-> B
A --> B
A <-- B

Name resolution

Help

Tony Fortunato - novotel full capture.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: ip.addr==10.0.1.200 && ip.addr==128.46.156.117 Expression... Clear Apply

No.	Time	Length B	Source	Destination	Protocol	Info
1	0.000000	250	10.0.1.219	10.255.255.255	BROWS	Domain/Workgroup Announ
2	0.184944	1514	128.46.156.117	10.0.1.200	TCP	53186 > 1106 [ACK] Seq=1
3	0.007969	1514	128.46.156.117	10.0.1.200	TCP	53186 > 1106 [ACK] Seq=1
4	0.000032	54	10.0.1.200	128.46.156.117	TCP	1106 > 53186 [ACK] Seq=1
5	0.007989	1514	128.46.156.117	10.0.1.200	TCP	53186 > 1106 [ACK] Seq=2
6	0.195927	54	10.0.1.200	128.46.156.117	TCP	1106 > 53186 [ACK] Seq=1

File: "C:\Documents and Settings\Tony Fortunato\Desktop\dnd\tr... Packets: 5961 Displayed: 5961 Marked: 0

CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

Top 10 Useful Filters

IP Address:	`ip.addr == x.x.x.x`
MAC Address:	`eth.addr == xx:xx:xx:xx:xx:xx`
ICMP!	`icmp`
My MAC Address:	`eth.addr == xx:xx:xx:xx:xx:xx`
DHCP:	`bootp`
High Delta Time:	`frame.time_delta > 1`
TCP Port:	`tcp.port == x`
UDP Port:	`udp.port == x`
TCP ACK RTT:	`tcp.analysis.ack_rtt > 1`
TCP Length: > x < y	`tcp.len > x && tcp.len < y`

Bonus

Not My MAC:	`!eth.addr == xx:xx:xx:xx:xx:xx`

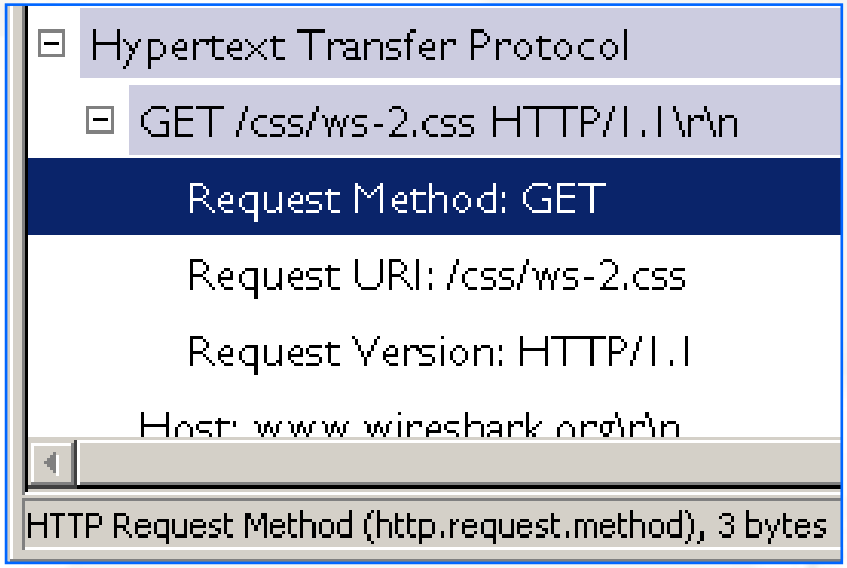
Manually Editing the *dfilters* File

```
"Ethernet address 00:08:15:00:08:15" eth.addr =
"Ethernet type 0x0806 (ARP)" eth.type == 0x0806
"Ethernet broadcast" eth.addr == ff:ff:ff:ff:ff
"No ARP" not arp
"IP only" ip
"IP address 192.168.0.1" ip.addr == 192.168.0.1
"IP address isn't 192.168.0.1, don't use != for
192.168.0.1)
"IPX only" ipx
"TCP only" tcp
"UDP only" udp
"UDP port isn't 53 (not DNS), don't use != for
"TCP or UDP port is 80 (HTTP)" tcp.port == 80
"HTTP" http
"No ARP and no DNS" not arp and !(udp.port == 53
"Non-HTTP and non-SMTP to/from 192.168.0.1" not
(tcp.port == 25) and ip.addr == 192.168.0.1
"Macof window=512" tcp.window_size == 512
"ICMP type 8 code not 0" (icmp.type == 8) && !(i
"Ping code not 0" (icmp.type == 8) && !(icmp.c
```

- Do not append a file extension
- Include blank line after last filter

Display Filters

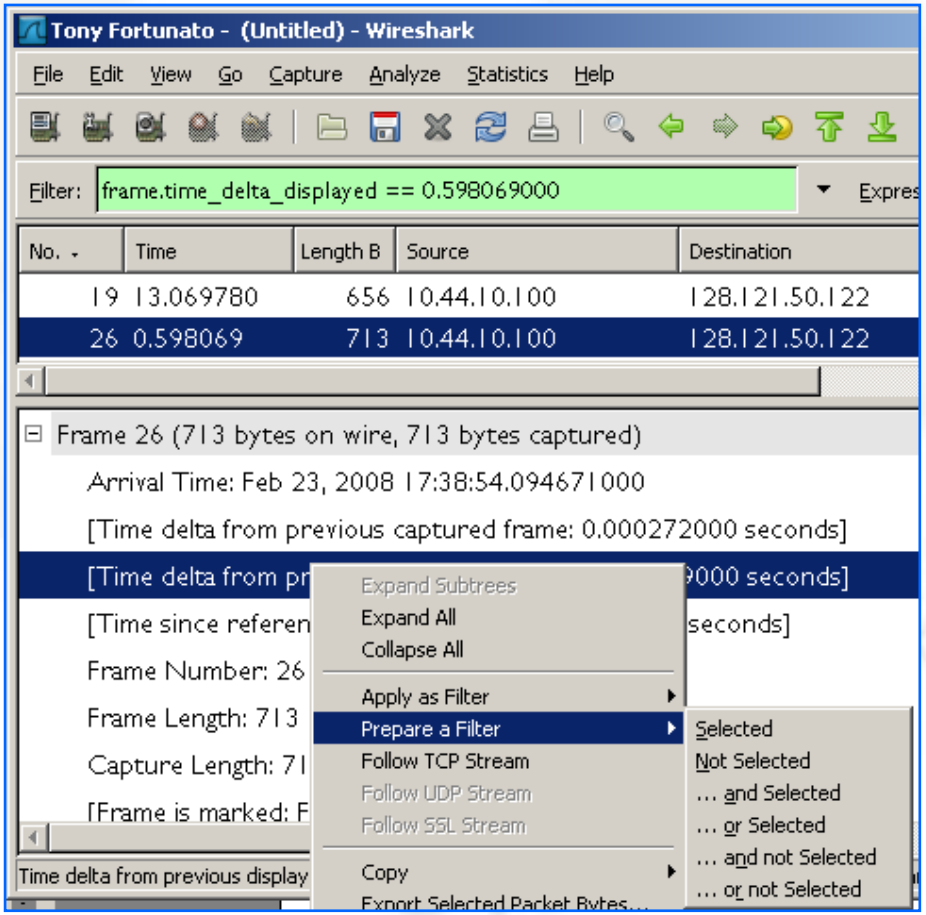
The easiest way to learn is to look at existing traces and reference the field name you are interested in;



CACE TECHNOLOGIES
SHARKFEST '08
www.wiresharkU.com
WIRESHARK UNIVERSITY

Display Filter Time Saver

When I want to build a filter, but don't want to type out a long fieldname, I simply right click on the field name and use the Prepare A Filter-> Selected and then modify the filter from there.

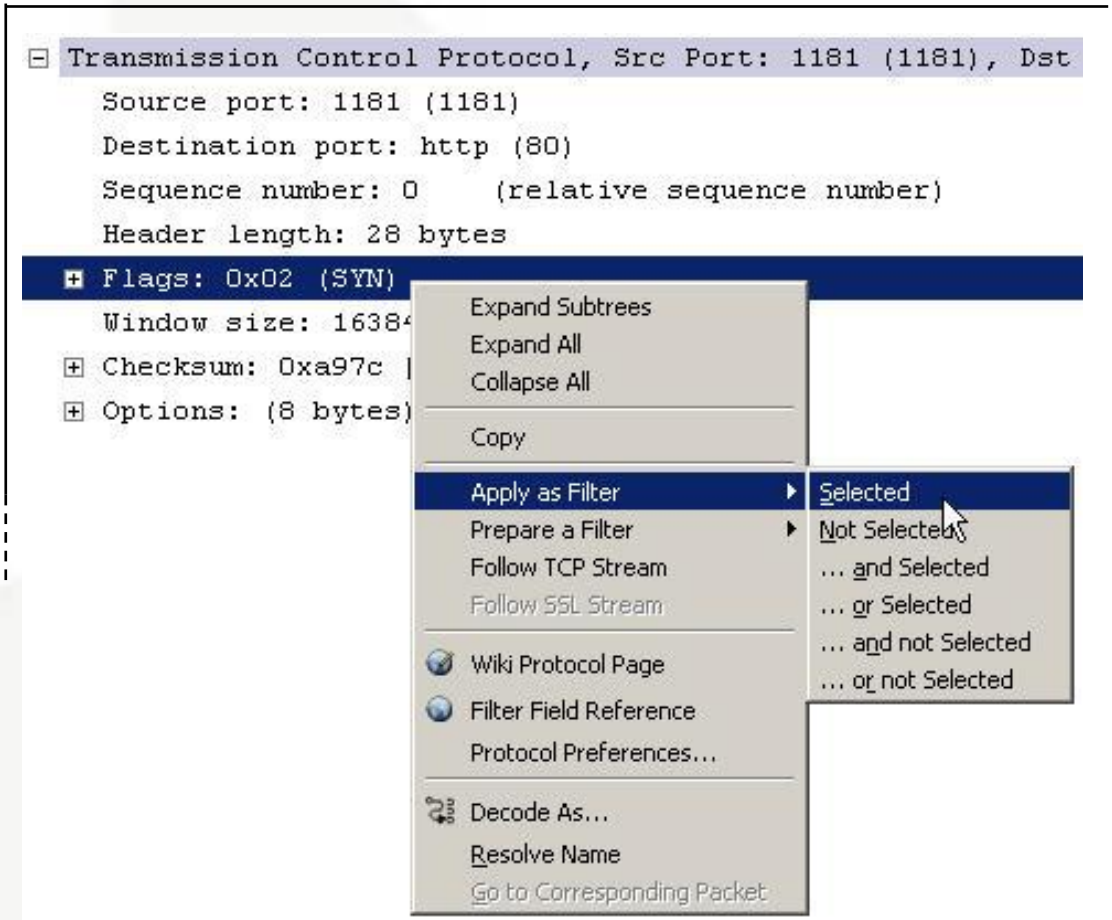


CACE TECHNOLOGIES

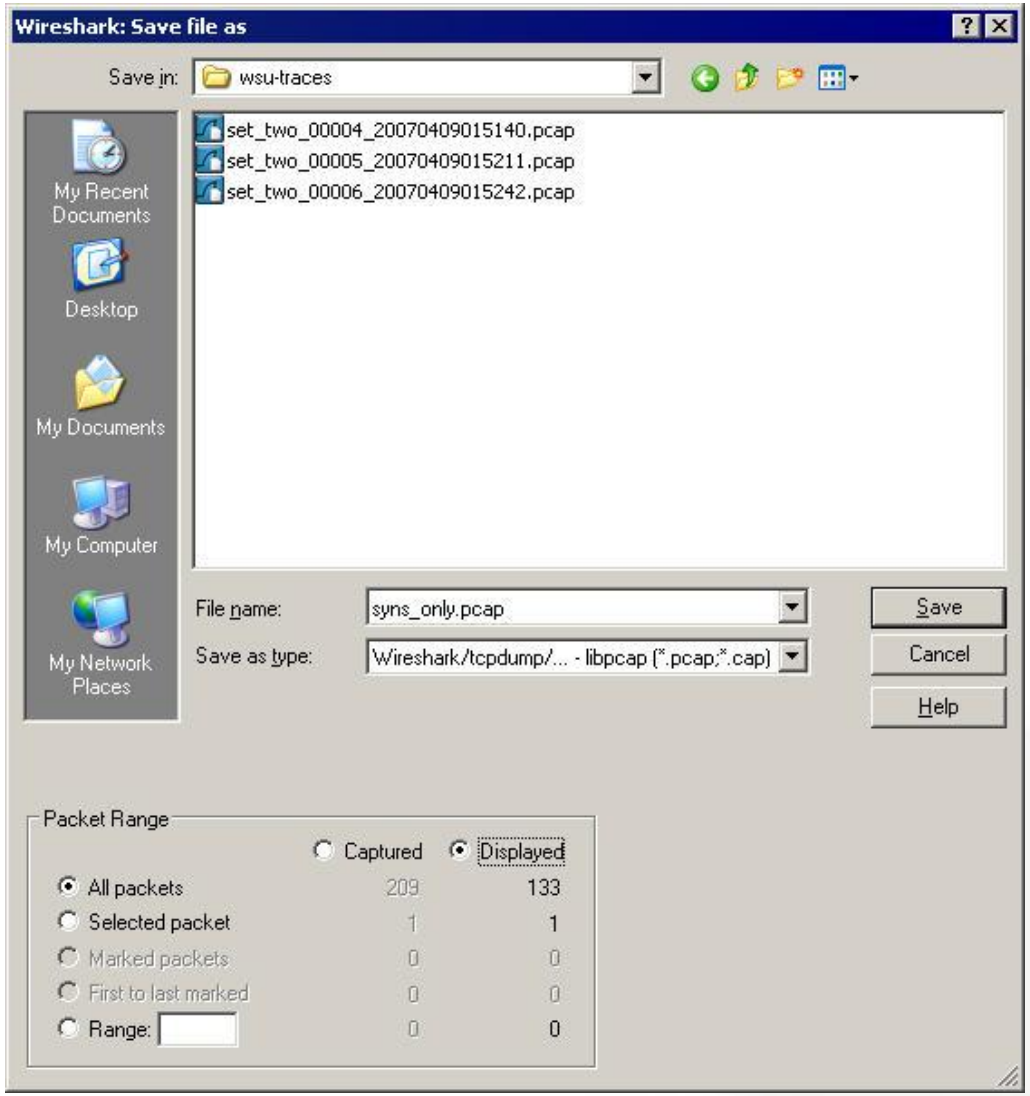
www.wiresharkU.com WIRESHARK UNIVERSITY

Build Filters Based on Packets

Right mouse click on any field and either **Apply** or **Prepare** a filter based on the field and value (with an implied ‘equal to’ operator).



Save Filtered, Marked and Ranges of Packets



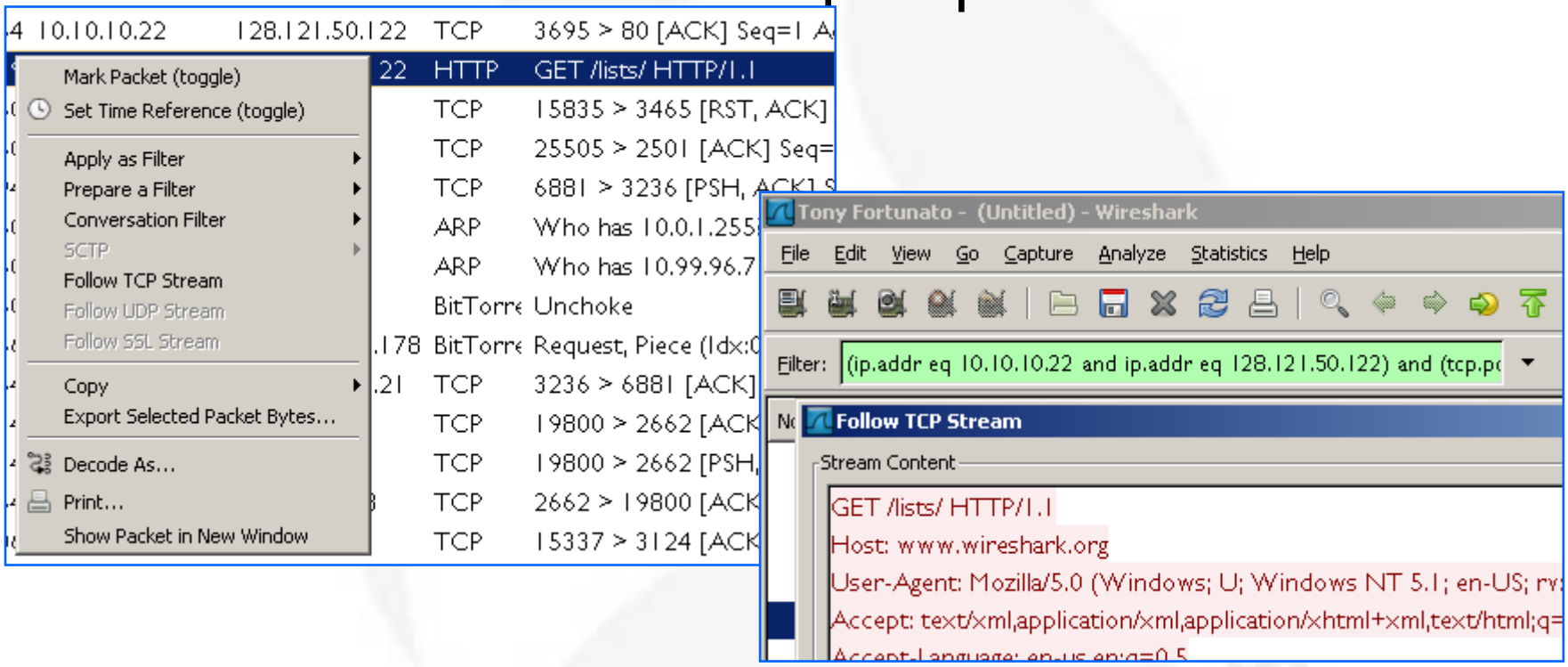
Packet Range Selection

- Captured/Displayed
- All packets
- Selected packets
- Marked packets
- First to last marked packet
- Range

CACE TECHNOLOGIES
www.wiresharkU.com
WIRESHARK UNIVERSITY

Follow the Stream

This feature creates a display filter of the selected Packet's IP address and port pairs

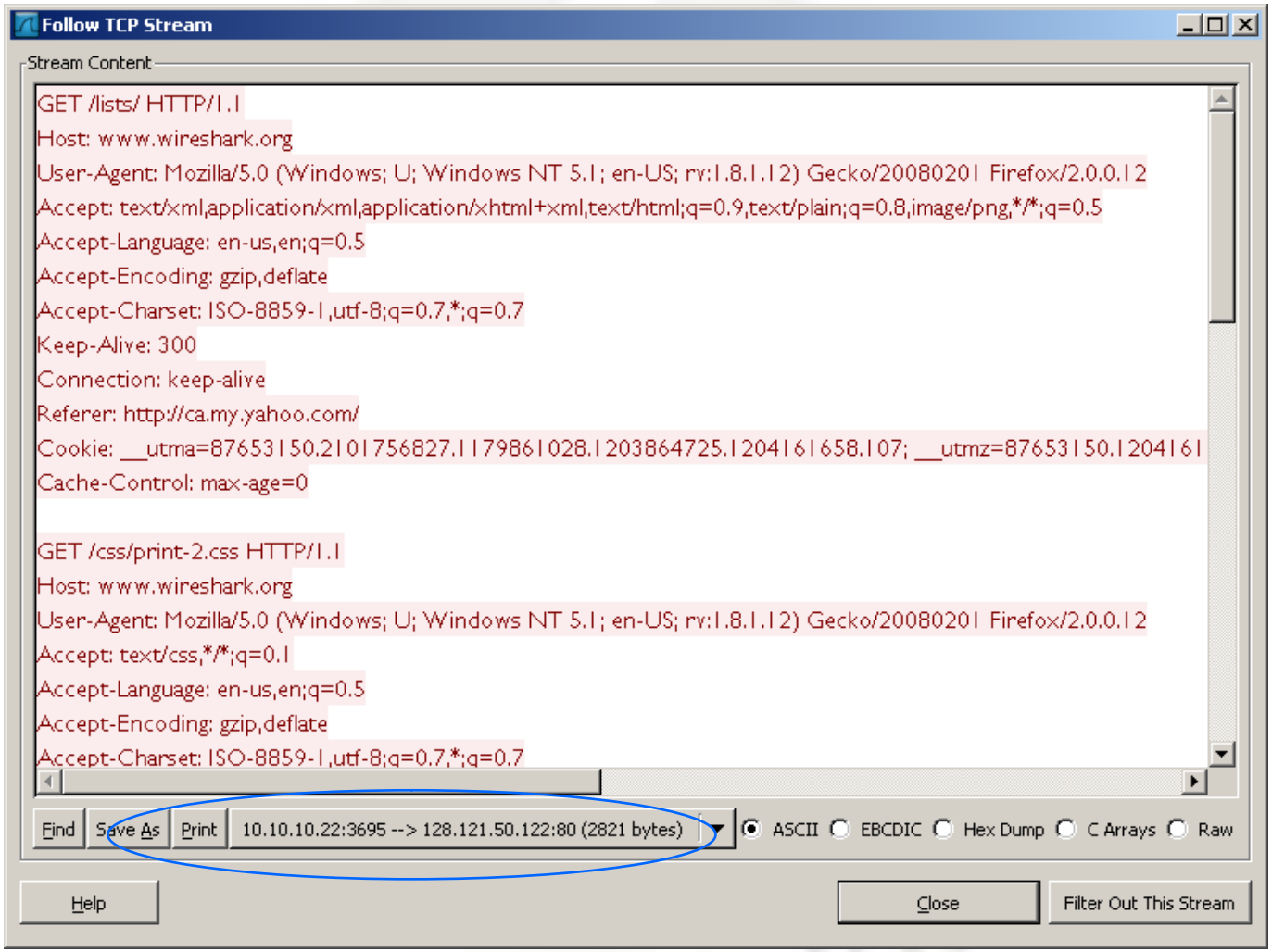


CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

One Way stream

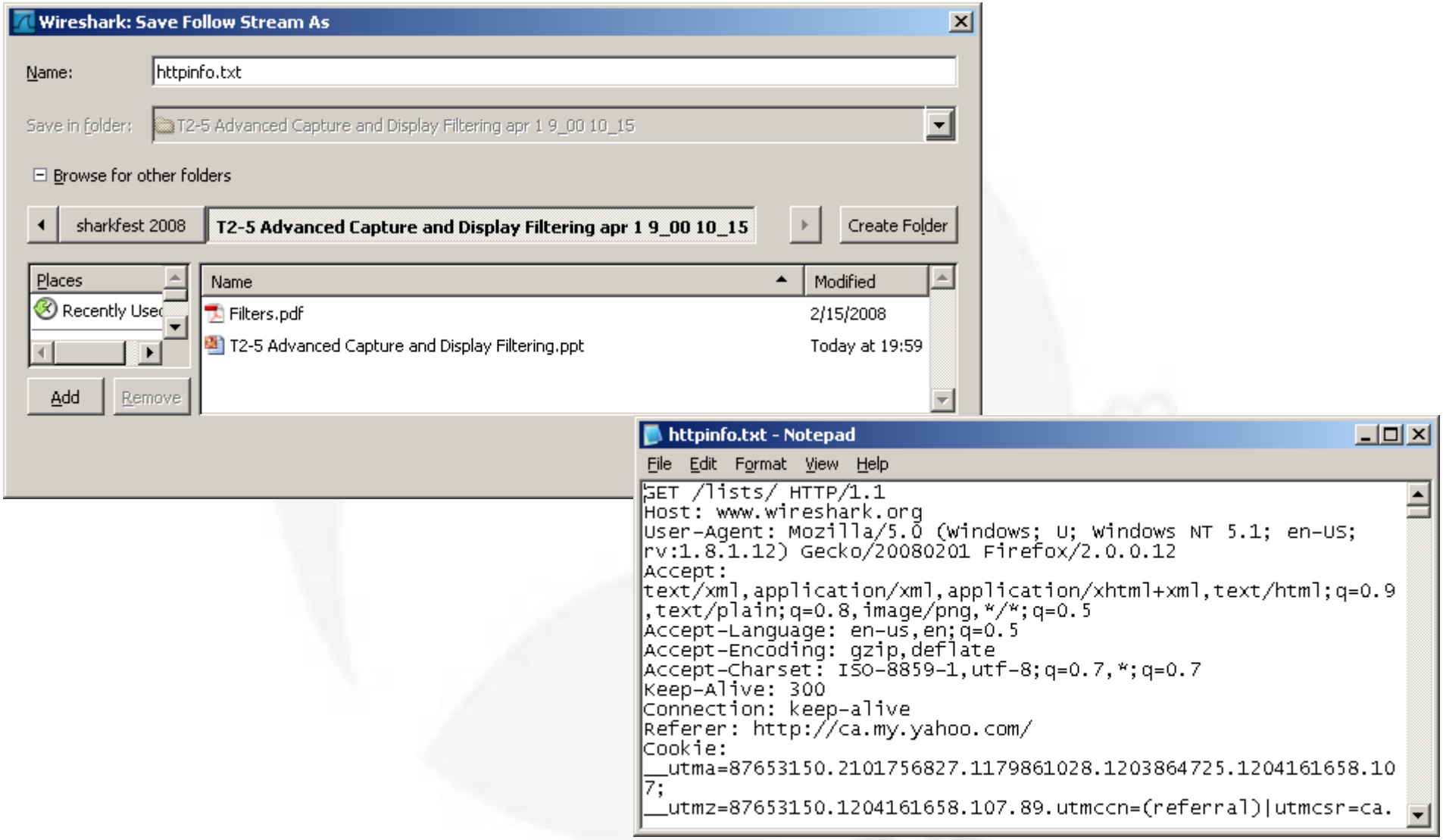
You can select the stream data from the client or Server



CACE TECHNOLOGIES

www.wiresharkU.com WIRESHARK UNIVERSITY

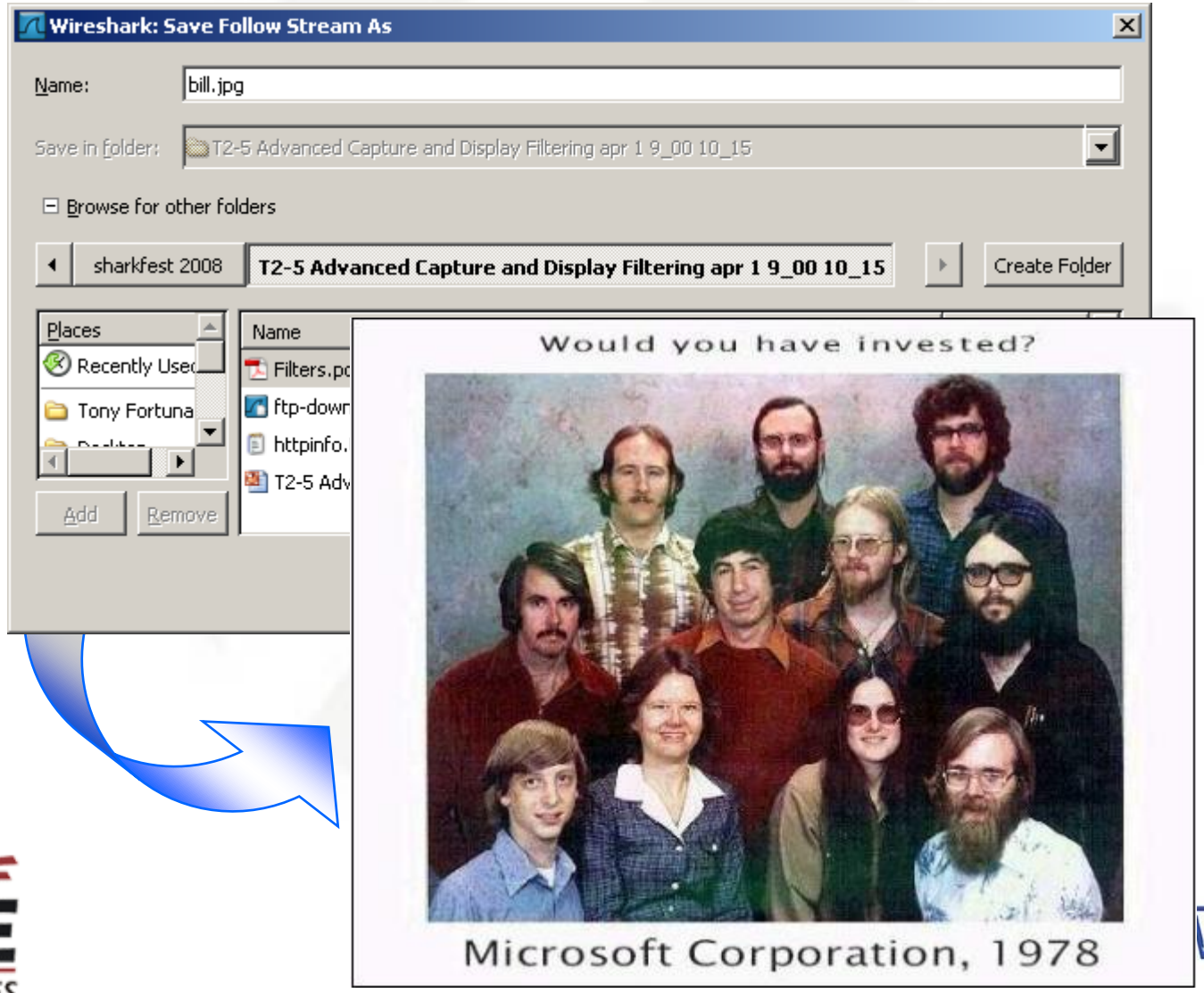
Saving A Stream



Rebuilding a file

ftp-download-good.pcap

You can rebuild files from the stream



HTTP Filter Example

Common filters for HTTP

http.request.version == "HTTP/1.1“

Will return commands and responses

CACE TECHNOLOGIES

SHARKFEST '08

www.wiresharkU.com WIRESHARK UNIVERSITY