

BLG 433E COMPUTER COMMUNICATIONS: WIRESHARK TUTORIAL

Instructor: Assoc. Prof. Berk CANBERK
Teaching Assistant: Yusuf ÖZÇEVİK

SPRING 2018-2019

OUTLINE

- **Introduction**
 - What is Wireshark?
 - Building and Installing Wireshark
- **Traffic Monitoring**
 - Capturing Packets
 - Analyzing Packets
 - Filtering Packets etc.

INTRODUCTION

What is Wireshark?

- Network packet analyzer [1]
 - Capture network packets
 - Display that packet data as detailed as possible
- Some examples:
 - Network administrators use it to *troubleshoot network problems*
 - Network security engineers use it to *examine security problems*
 - Developers use it to *debug protocol implementations*
 - People use it to *learn network protocol* internals

[1] Wireshark User Guide

INTRODUCTION

What is Wireshark?

- Wireshark:
 - **is not** an intrusion detection system
 - **does not** manipulate things on the networks,
 - only “measure” things from the network

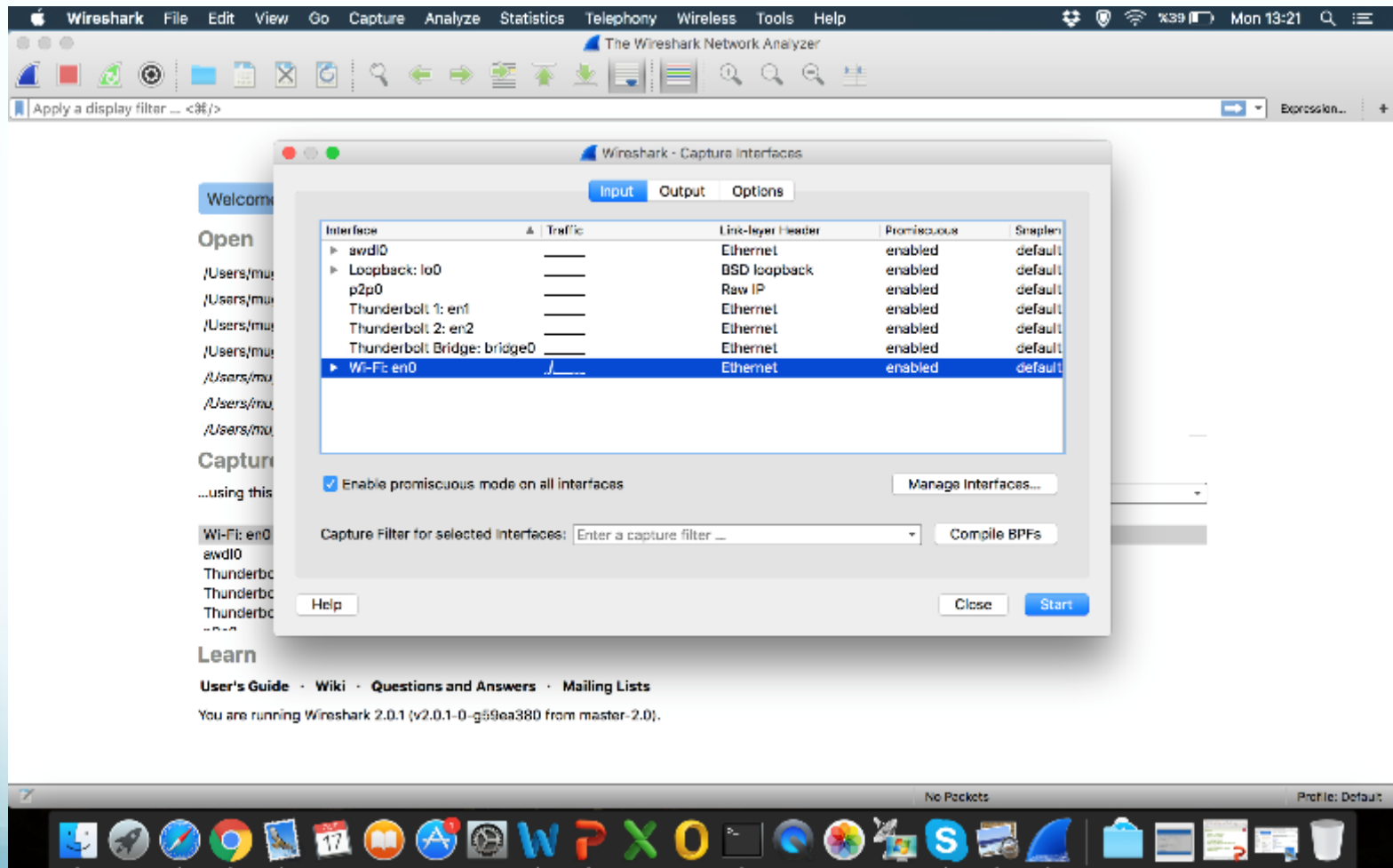
INTRODUCTION

Building and Installation

- Microsoft Windows
- UNIX/Linux
 - <https://www.wireshark.org/download.html>.
 - `$ tar xaf wireshark-2.4.5.tar.xz`
 - `$ cd wireshark-2.4.5`
 - `$./configure`
 - `$ make`
 - `$ make install`

TRAFFIC MONITORING

Capturing Packets



TRAFFIC MONITORING

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows 'Wi-Fi en0' and 'Mon 13:22'. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'Apply a display filter ... <36/>'. The packet list shows a sequence of events including an SSL/TLS handshake (Client Hello, Server Hello, Certificate, Key Exchange, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message, Application Data) and a DNS query for 'SRV _nos._tcp.nos-avg.cz'. The packet details pane shows the selected packet (No. 115) and its structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data for the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
98	3..	161.9.98.110	54.243.90.103	TCP	66	50288 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=805243837 TSecr=74176749
99	3..	161.9.98.110	54.243.90.103	SSL	297	Client Hello
100	3..	54.243.90.103	161.9.98.110	TCP	66	443 → 50288 [ACK] Seq=1 Ack=232 Win=15616 Len=0 TSval=74176788 TSecr=805243837
101	3..	54.243.90.103	161.9.98.110	TLSv1..	1434	Server Hello
102	3..	54.243.90.103	161.9.98.110	TLSv1..	1434	Certificate
103	3..	161.9.98.110	54.243.90.103	TCP	66	50288 → 443 [ACK] Seq=232 Ack=2737 Win=129696 Len=0 TSval=805243986 TSecr=74176788
104	3..	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
105	3..	54.243.90.103	161.9.98.110	TLSv1..	332	Server Key Exchange
106	3..	161.9.98.110	54.243.90.103	TCP	66	50288 → 443 [ACK] Seq=232 Ack=3003 Win=130720 Len=0 TSval=805243988 TSecr=74176788
107	3..	161.9.98.110	54.243.90.103	TLSv1..	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
108	3..	54.243.90.103	161.9.98.110	TLSv1..	117	Change Cipher Spec, Encrypted Handshake Message
109	3..	161.9.98.110	54.243.90.103	TCP	66	50288 → 443 [ACK] Seq=350 Ack=3054 Win=131008 Len=0 TSval=805244136 TSecr=74176827
110	3..	161.9.98.110	54.243.90.103	TLSv1..	313	Application Data
111	3..	54.243.90.103	161.9.98.110	TLSv1..	1008	Application Data
112	3..	161.9.98.110	54.243.90.103	TCP	66	50288 → 443 [ACK] Seq=605 Ack=3996 Win=130112 Len=0 TSval=805244301 TSecr=74176868
113	3..	161.9.98.110	54.243.90.103	TLSv1..	97	Encrypted Alert
114	3..	161.9.98.110	54.243.90.103	TCP	66	50288 → 443 [FIN, ACK] Seq=636 Ack=3996 Win=131072 Len=0 TSval=805244301 TSecr=74176868
115	3..	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
116	3..	54.243.90.103	161.9.98.110	TLSv1..	97	Encrypted Alert
117	3..	161.9.98.110	54.243.90.103	TCP	54	50288 → 443 [RST] Seq=637 Win=0 Len=0
118	3..	54.243.90.103	161.9.98.110	TCP	66	443 → 50288 [FIN, ACK] Seq=4027 Ack=637 Win=16640 Len=0 TSval=74176904 TSecr=805244301
119	3..	161.9.98.110	54.243.90.103	TCP	54	50288 → 443 [RST] Seq=637 Win=0 Len=0
120	4..	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
121	4..	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz

Frame 115: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Ethernet II, Src: Apple_c9:70:6e (3c:15:c2:c9:70:6e), Dst: CiscoInc_9f:f0:da (00:00:0c:9f:f0:da)
Internet Protocol Version 4, Src: 161.9.98.110, Dst: 46.197.15.60
User Datagram Protocol, Src Port: 57567 (57567), Dst Port: 53 (53)
Domain Name System (query)

Domain Name System (dns), 80 bytes

Packets: 121 - Displayed: 121 (100.0%)

Profile: Default

TRAFFIC MONITORING

The image shows a Wireshark traffic capture interface on a Mac. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the time as Mon 14:03 and battery level at 33%. The main display area shows a list of captured packets, with the 'dns' filter applied. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
34	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
35	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
36	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
37	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
38	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
39	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
40	1...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
41	1...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
42	1...	161.9.98.110	160.75.2.20	DNS	82	Standard query 0x90ed A e9097.g.akamaiedge.net
43	1...	160.75.2.20	161.9.98.110	DNS	98	Standard query response 0x90ed A e9097.g.akamaiedge.net A 104.84.194.219
50	1...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
59	2...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
60	2...	161.9.98.110	160.75.2.20	DNS	82	Standard query 0xe5f8 A e1793.b.akamaiedge.net
61	2...	160.75.2.20	161.9.98.110	DNS	98	Standard query response 0xe5f8 A e1793.b.akamaiedge.net A 23.6.123.158
76	2...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
83	2...	161.9.98.110	160.75.2.20	DNS	99	Standard query 0xaa11 A zas-api-production.elasticbeanstalk.com
84	2...	161.9.98.110	160.75.2.20	DNS	99	Standard query 0x1c50 AAAA zas-api-production.elasticbeanstalk.com
87	3...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
94	3...	160.75.2.20	161.9.98.110	DNS	181	Standard query response 0x1c50 AAAA zas-api-production.elasticbeanstalk.com SOA ns-1235.awsdns...
95	3...	160.75.2.20	161.9.98.110	DNS	227	Standard query response 0xaa11 A zas-api-production.elasticbeanstalk.com A 54.243.98.123 A 107...
104	3...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
115	3...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
120	4...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
121	4...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz

The packet details pane for the selected packet (No. 95) shows the following information:

- Frame 95: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface 0
- Ethernet II, Src: CiscoInc_03:14:41 (8c:60:4f:03:14:41), Dst: Apple_c9:70:6e (3c:15:c2:c9:70:6e)
- Internet Protocol Version 4, Src: 160.75.2.20, Dst: 161.9.98.110
- User Datagram Protocol, Src Port: 53 (53), Dst Port: 59362 (59362)
- Domain Name System (response)

The bottom status bar shows: Packets: 121 - Displayed: 57 (47.1%) - Dropped: 0 (0.0%) Profile: Default. The Mac dock at the bottom contains various application icons including Finder, Safari, Chrome, and others.

TRAFFIC MONITORING

The image shows a Wireshark traffic monitoring interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the interface language as 'Wi-Fi: en0' and the time as 'Mon 14:00'. The main display area shows a list of captured packets, with the 'dns' filter applied. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info. A context menu is open for packet 23, showing options like 'Expand Subtrees', 'Expand All', 'Collapse All', 'Apply as Column', 'Apply as Filter', 'Prepare a Filter', 'Conversation Filter', 'Colorize with Filter', 'Follow', 'Copy', 'Export Packet Bytes...', 'Wiki Protocol Page', 'Filter Field Reference', 'Protocol Preferences', 'Decode As...', 'Go to Linked Packet', 'Show Linked Packet in New Window', and 'New Conversation Rule...'. The 'Colorize with Filter' option is selected, and a sub-menu is open showing color options 1 through 10. The bottom status bar shows 'Domain Name System (dns), 38 bytes' and 'Packets: 121 - Displayed: 57 (47.1%) - Dropped: 0 (0.0%)'.

No.	Time	Source	Destination	Protocol	Length	Info
20	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
21	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
22	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
23	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
24	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
25	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
26	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
27	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
28	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
29	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
30	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
31	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
32	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
33	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
34	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
35	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
36	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
37	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
38	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
39	0...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
40	1...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
41	1...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
42	1...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
43	1...	160.75.2.22	160.75.2.22	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz

Domain Name System (dns), 38 bytes

Packets: 121 - Displayed: 57 (47.1%) - Dropped: 0 (0.0%)

Profile: Default

TRAFFIC MONITORING

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the interface as 'Wi-Fi: en0' and the time as 'Mon 14:04'. The packet list pane on the left shows a filter 'ip.src==161.9.98.110'. The main packet list pane displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet details pane at the bottom shows the structure of the first packet (Frame 1), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).

No.	Time	Source	Destination	Protocol	Length	Info
55	1...	161.9.98.110	104.84.194.219	TCP	66	50286 → 80 [ACK] Seq=589 Ack=462 Win=130848 Len=0 TSval=805242459 TSecr=326056381
56	1...	161.9.98.110	104.84.194.219	TCP	66	50286 → 80 [FIN, ACK] Seq=589 Ack=462 Win=131072 Len=0 TSval=805242459 TSecr=326056381
58	1...	161.9.98.110	104.84.194.219	TCP	66	50286 → 80 [ACK] Seq=590 Ack=463 Win=131072 Len=0 TSval=805242526 TSecr=326056451
59	2...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
60	2...	161.9.98.110	160.75.2.20	DNS	82	Standard query 0xe5f8 A e1793.b.akamaiedge.net
62	2...	161.9.98.110	23.6.123.158	TCP	78	50287 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=805242876 TSecr=0 SACK_PERM=1
64	2...	161.9.98.110	23.6.123.158	TCP	66	50287 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=805242970 TSecr=307659193
65	2...	161.9.98.110	23.6.123.158	TLSv1	298	Client Hello
69	2...	161.9.98.110	23.6.123.158	TCP	78	50287 → 443 [ACK] Seq=233 Ack=1369 Win=131072 Len=0 TSval=805243067 TSecr=307659288 SLE=2737 SR...
71	2...	161.9.98.110	23.6.123.158	TCP	66	50287 → 443 [ACK] Seq=233 Ack=3857 Win=128576 Len=0 TSval=805243069 TSecr=307659288
72	2...	161.9.98.110	23.6.123.158	TLSv1	408	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
74	2...	161.9.98.110	23.6.123.158	TCP	66	50287 → 443 [ACK] Seq=575 Ack=3932 Win=130976 Len=0 TSval=805243171 TSecr=307659396
75	2...	161.9.98.110	23.6.123.158	TLSv1	343	Application Data
76	2...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
77	2...	161.9.98.110	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
80	2...	161.9.98.110	23.6.123.158	TCP	66	50287 → 443 [ACK] Seq=852 Ack=4273 Win=130720 Len=0 TSval=805243479 TSecr=307659705
81	2...	161.9.98.110	23.6.123.158	TLSv1	119	Encrypted Alert
82	2...	161.9.98.110	23.6.123.158	TCP	66	50287 → 443 [FIN, ACK] Seq=905 Ack=4273 Win=131072 Len=0 TSval=805243479 TSecr=307659705
83	2...	161.9.98.110	160.75.2.20	DNS	99	Standard query 0xaa11 A zas-api-production.elasticbeanstalk.com
84	2...	161.9.98.110	160.75.2.20	DNS	99	Standard query 0x1c50 AAAA zas-api-production.elasticbeanstalk.com
86	3...	161.9.98.110	23.6.123.158	TCP	66	[TCP Retransmission] 50287 → 443 [FIN, ACK] Seq=905 Ack=4273 Win=131072 Len=0 TSval=805243588 T...
87	3...	161.9.98.110	46.197.15.60	DNS	80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
91	3...	161.9.98.110	23.6.123.158	TCP	54	50287 → 443 [RST] Seq=905 Win=0 Len=0
92	3...	161.9.98.110	23.6.123.158	TCP	54	50287 → 443 [RST] Seq=905 Win=0 Len=0

Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Ethernet II, Src: Apple_c9:70:6e (3c:15:c2:c9:70:6e), Dst: CiscoInc_9f:f0:da (00:00:0c:9f:f0:da)
Internet Protocol Version 4, Src: 161.9.98.110, Dst: 46.197.15.60
User Datagram Protocol, Src Port: 57567 (57567), Dst Port: 53 (53)
Domain Name System (query)

Packets: 121 - Displayed: 89 (73.6%) - Dropped: 0 (0.0%) Profile: Default

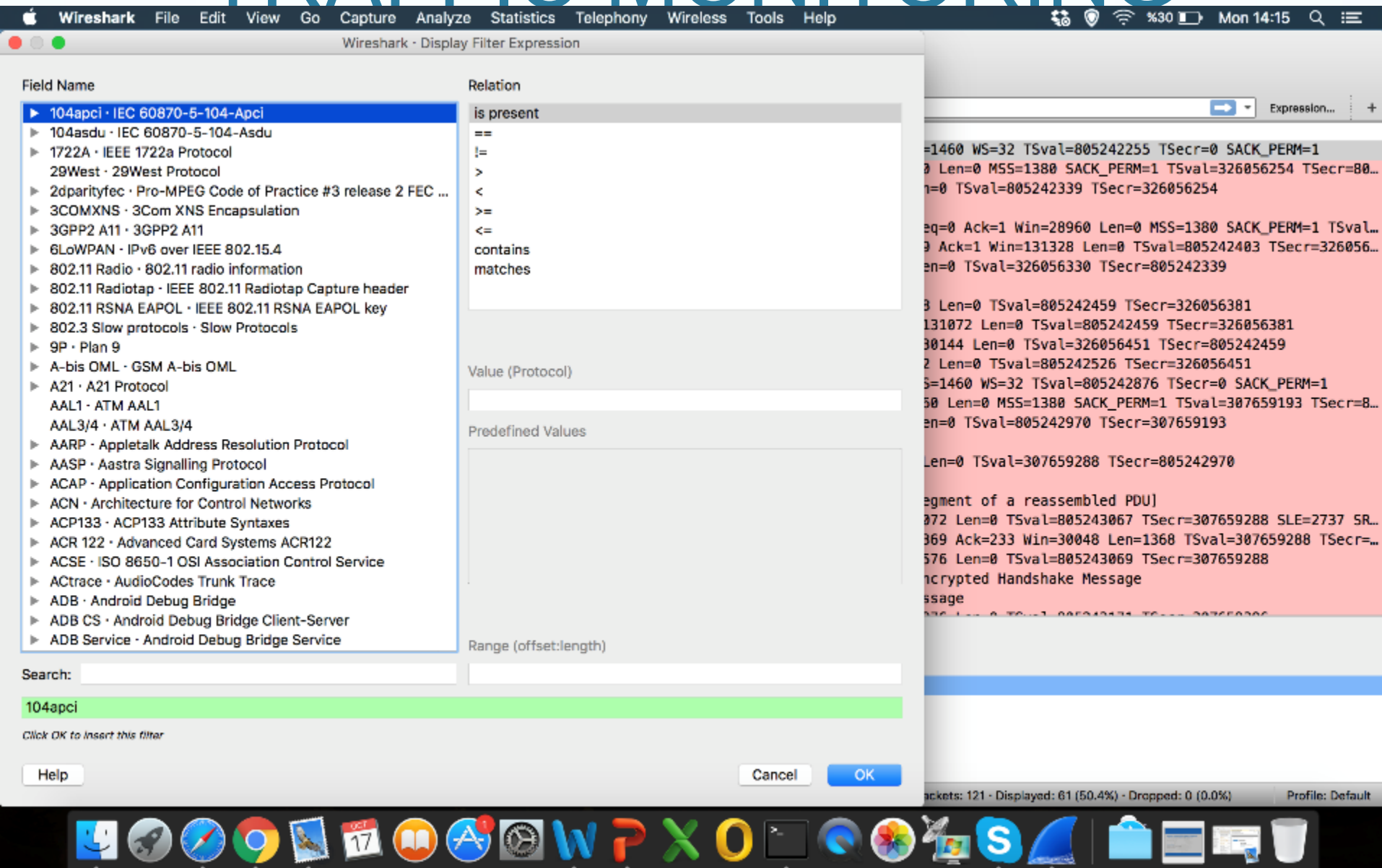
TRAFFIC MONITORING

Filtering Packets

English	C-like	Description and example
eq	==	Equal. <code>ip.src==10.0.0.5</code>
ne	!=	Not equal. <code>ip.src!=10.0.0.5</code>
gt	>	Greater than. <code>frame.len > 10</code>
lt	<	Less than. <code>frame.len < 128</code>
ge	>=	Greater than or equal to. <code>frame.len ge 0x100</code>
le	<=	Less than or equal to. <code>frame.len <= 0x20</code>

* Taken from Wireshark User Guide

TRAFFIC MONITORING



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the time as Mon 14:15 and battery level at 30%.

The main window is divided into three panes:

- Field Name List:** A list of network protocols. The '104apci' protocol is selected and highlighted in blue. Below it, a search bar contains the text '104apci', and a green bar indicates the filter '104apci' is applied.
- Relation:** A dropdown menu showing 'is present' as the selected relation. Other options include '==', '!=', '>', '<', '>=', '<=', 'contains', and 'matches'.
- Value (Protocol):** A text input field for specifying the protocol value.

The bottom pane shows a list of network packets. The selected packet (104apci) is highlighted in blue. The packet details pane on the right shows the structure of the selected packet, including fields like 'Len=0', 'MSS=1380', 'SACK_PERM=1', 'TSval=805242255', 'TSecr=0', and 'SACK_PERM=1'.

The bottom status bar indicates 'Packets: 121 - Displayed: 61 (50.4%) - Dropped: 0 (0.0%)' and 'Profile: Default'.

TRAFFIC MONITORING

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. The selected packet (No. 58) is a TCP ACK segment from 161.9.98.110 to 104.84.194.219. A 'Capture Filters' dialog box is open, showing a list of filters. The filter 'my_host_filter' with the expression 'ip.src==161.9.98.110' is selected. The packet details pane on the right shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

Wireshark Interface Elements:

- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard network analysis tools like capture, pause, and zoom.
- Filter Bar:** Shows the current filter: `ip.src==161.9.98.110`.
- Packet List:** Displays captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** Shows the hierarchical structure of the selected packet (Frame 58: 66 bytes on wire).
- Packet Bytes:** Shows the raw data of the selected packet.

Capture Filters Dialog Box:

Name	Filter
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org
my_host_filter	ip.src==161.9.98.110

Packet Details (Frame 58):

- Ethernet II, Src: Apple_08:00:5e:00:53:00, Dst: 104.84.194.219
- Internet Protocol Version 4, Src: 161.9.98.110, Dst: 104.84.194.219
- Transmission Control Protocol, Src Port: 50286, Dst Port: 80, Seq: 589, Ack: 462, Len: 0

TRAFFIC MONITORING

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the interface as 'Wi-Fi: en0' and the time as 'Mon 14:08'.

The main packet list pane shows a table of captured packets. The selected packet is number 56, a TCP segment from 161.9.98.110 to 104.84.194.219, sequence number 50286, acknowledgment number 80. A context menu is open over this packet, offering actions such as 'Mark/Unmark Packet', 'Ignore/Unignore Packet', 'Set/Unset Time Reference', 'Time Shift...', 'Packet Comment...', 'Edit Resolved Name', 'Apply as Filter', 'Prepare a Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', 'Follow', 'Copy', 'Protocol Preferences', 'Decode As...', and 'Show Packet in New Window'. The 'Follow' option is currently selected, and a sub-menu is visible showing 'TCP Stream', 'UDP Stream', and 'SSL Stream'.

The packet details pane at the bottom shows the structure of the selected packet:

- Frame 56: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Apple_c9:70:6e (3c:15:c2:c9:70:6e), Dst: CiscoInc_9f:f0:da (00:00:0c:9f:f0:da)
- Internet Protocol Version 4, Src: 161.9.98.110, Dst: 104.84.194.219
- Transmission Control Protocol, Src Port: 50286 (50286), Dst Port: 80 (80), Seq: 589, Ack: 462, Len: 0
 - Source Port: 50286
 - Destination Port: 80
 - [Stream index: 0]
 - [TCP Segment Len: 0]
 - Sequence numbers: 589 (relative sequence number)

The bottom status bar indicates 'Packets: 121 - Displayed: 89 (73.6%) - Dropped: 0 (0.0%)' and 'Profile: Default'.

TRAFFIC MONITORING

The image shows a Wireshark network traffic capture. The main pane displays a selected packet (Packet 54) which is an HTTP GET request. The details pane on the right shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) message. The packet is a client request to a server, and the details pane shows the various fields of the HTTP message, such as the request line, headers, and body.

Wireshark - Follow TCP Stream (tcp.stream eq 0) · wireshark_pcapng_en0_20161017132105_X5fEOq

GET /gls/gms HTTP/1.1
User-Agent: AVGAVM-MAC101106 1504822 OSL0C=1033 LOC=1033 PKG=121 PKP=0 PROD=AV VER=1504822 LIC=3UXYT-BGX6U-HDFQI-QZJAY-WY0SV-B EVA=fbe52ac EDA=20151202134630 DIAG=1
Host: update-mac-av.avg.com
Accept-Encoding: identity, deflate, gzip
x-avg-date: 20161017
x-avg-gms: 1-5f600a40-1fa1-4fa9-a9fe-550a946f20b1-e89c6077c23425fd7cae3cd5e693482ce65a8afa-1
x-avg-id: 76-9391237835
x-avg-it: 201512021346
x-avg-mid: c66ee2e9a880493eb096f48859bd6628-3af9f23f3344cdb705fbacc376929b82
x-avg-mkid: AVG+1
x-avg-ocm: 0-0
x-avg-zenid: 5f600a40-1fa1-4fa9-a9fe-550a946f20b1-db07-2

HTTP/1.1 200 OK
Server: Apache
X-AVG-Set-Config: fmw.gms/global_gms_flag=b"1"
X-AVG-MKID: AVG+1
X-AVG-GEO: TR,34
Vary: X-AVG-ID, Accept-Encoding, User-Agent
Content-Encoding: gzip
X-AVG: ls-fe-prod-edc-self001.mgm.avg.com
Content-Length: 20
Content-Type: text/plain
Expires: Mon, 17 Oct 2016 10:21:09 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Mon, 17 Oct 2016 10:21:09 GMT
Connection: keep-alive

Packet 54. 1 client pkt(s), 1 server pkt(s), 1 turn. Click to select.

Entire conversation (1049 bytes) Show data as ASCII Stream 0

Find: Find Next

Help Hide this stream Print Save as... Close

Packets: 121 · Displayed: 12 (9.9%) · Dropped: 0 (0.0%) Profile: Default

TRAFFIC MONITORING

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark · Flow · wireshark_pcapng_enQ_20161017132105_X5fEOq

57567 Standard query 0x... 53
62389 Standard query 0x90ed A e9097.g.aks... 53
62389 Standard query response 0x90ed A e9... 53
Who has 161.9.99...
161.9.99.254 is at 00:00:0c:9f:f0:da
50286 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=805242255 TSecr=0 SACK_PERM=1
80 → 50286 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 SACK_PERM=1 TSval=328056254 TSecr=805242255
50286 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=805242339 TSecr=328056254
GET /pls/gms HTTP/1.1
57567 Standard query 0x... 53
50286 [TCP Out-Of-Order] 80 → 50286 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 SACK_PERM=1 TSval=3280563...
50286 [TCP Dup ACK 48#1] 50286 → 80 [ACK] Seq=589 Ack=1 Win=131328 Len=0 TSval=805242403 TSecr=328056254
80 → 50286 [ACK] Seq=1 Ack=589 Win=30144 Len=0 TSval=328056330 TSecr=805242339

Packet 44: ARP: Who has 161.9.99.254? Tell 161.9.98.110

Show: All packets Flow type: All Flows Addresses: Any

Help Close Save As... Reset

Internet Protocol Version 4, Src: 161.9.98.110, Dst: 104.84.194.219
Transmission Control Protocol, Src Port: 50286 (50286), Dst Port: 80 (80), Seq: 0, Len: 0
Source Port: 50286
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)

Packets: 121 · Displayed: 61 (50.4%) · Dropped: 0 (0.0%) Profile: Default

TRAFFIC MONITORING

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the interface is on Wi-Fi (en0) and the time is Mon 14:17.

The main window displays a packet list on the left, a protocol hierarchy in the center, and packet details on the right. The packet list shows a sequence of packets, with packet 56 selected. The protocol hierarchy shows the following structure:

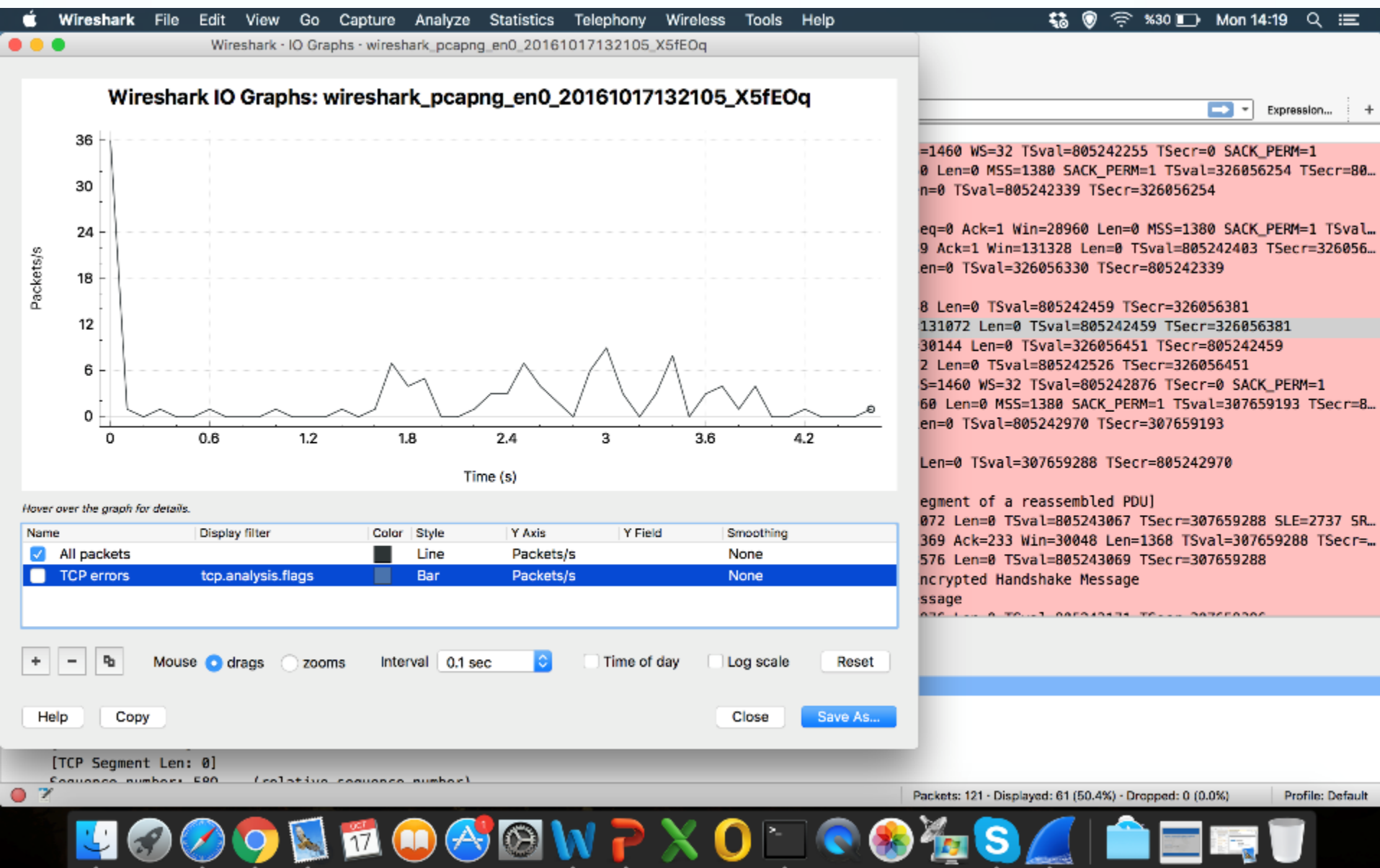
- Frame (100.0% packets, 61 packets, 100.0% bytes, 14985 bytes, 54 k bits/s, 0 end packets, 0 end bytes)
 - Ethernet (100.0% packets, 61 packets, 100.0% bytes, 14985 bytes, 54 k bits/s, 0 end packets, 0 end bytes)
 - Internet Protocol Version 4 (100.0% packets, 61 packets, 100.0% bytes, 14985 bytes, 54 k bits/s, 0 end packets, 0 end bytes)
 - Transmission Control Protocol (100.0% packets, 61 packets, 100.0% bytes, 14985 bytes, 54 k bits/s, 40 end packets, 4028 end bytes)
 - Secure Sockets Layer (31.1% packets, 19 packets, 65.2% bytes, 9776 bytes, 35 k bits/s, 18 end packets, 9444 end bytes)
 - Secure Sockets Layer (1.6% packets, 1 packet, 2.2% bytes, 332 bytes, 1208 bits/s, 1 end packet, 332 end bytes)
 - Hypertext Transfer Protocol (3.3% packets, 2 packets, 7.9% bytes, 1181 bytes, 4299 bits/s, 1 end packet, 654 end bytes)
 - Malformed Packet (1.6% packets, 1 packet, 3.5% bytes, 527 bytes, 1918 bits/s, 1 end packet, 527 end bytes)

The packet details pane for the selected packet (Frame 56) shows the following information:

- Source Port: 80
- Destination port: 80
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 580 (relative sequence number)

The bottom status bar indicates that 121 packets were captured, 61 (50.4%) are displayed, and 0 (0.0%) were dropped. The profile is set to Default.

TRAFFIC MONITORING



TRAFFIC MONITORING

