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

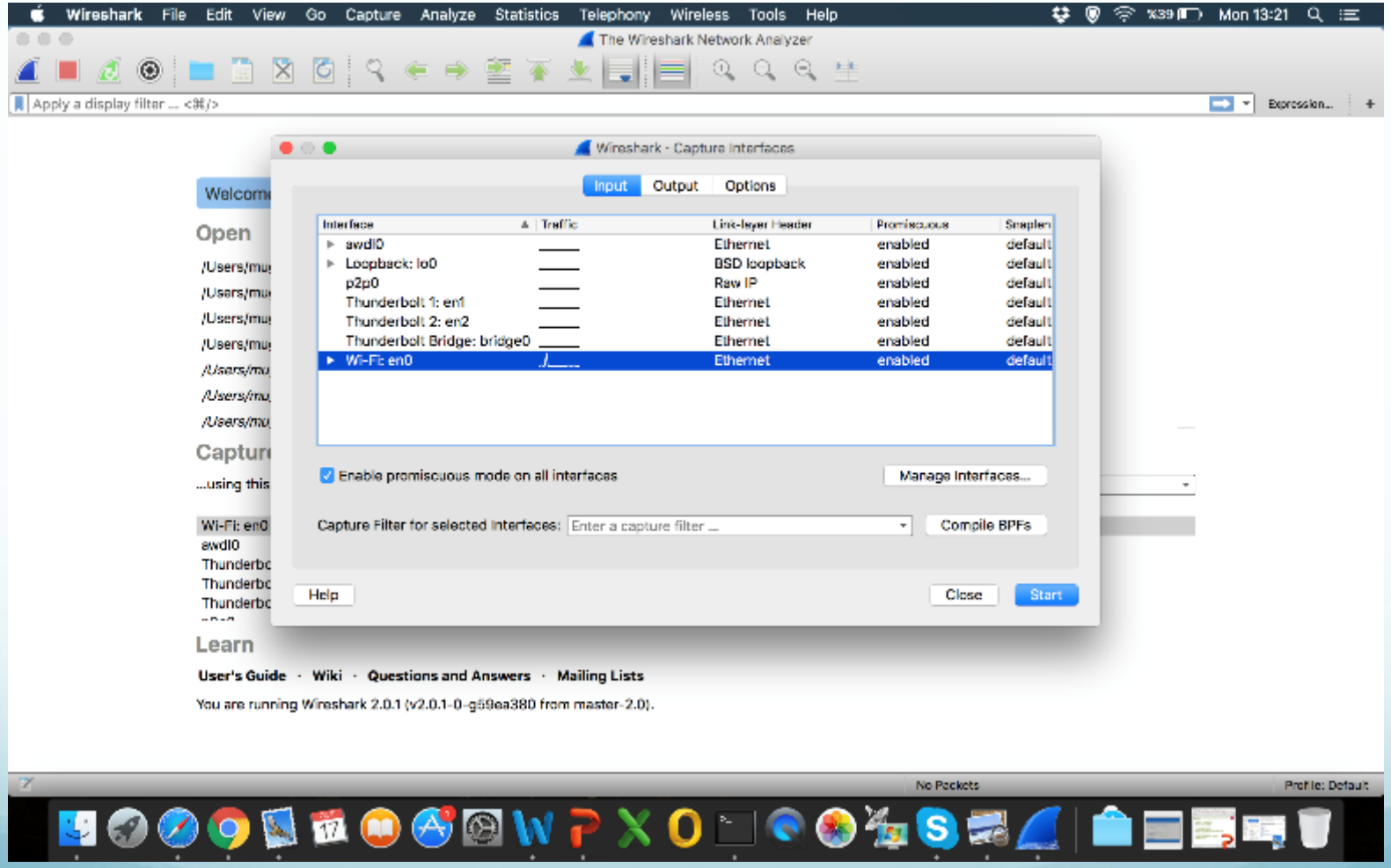
INTRODUCTION
What is Wireshark?

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

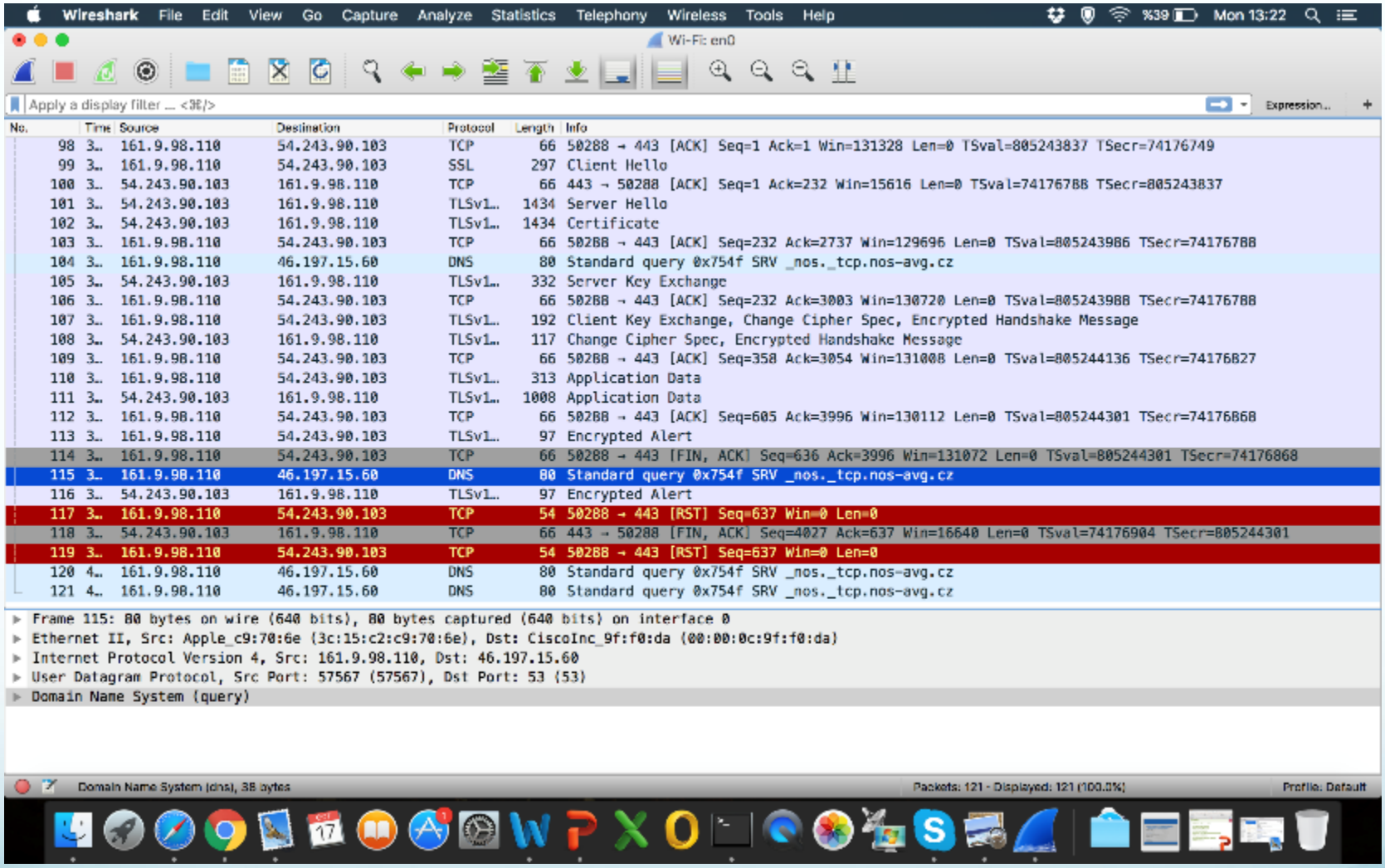
INTRODUCTION
Building and Installation

- 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



TRAFFIC MONITORING

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help %33 Mon 14:03

Wi-Fi: en0

dns

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

```
▶ 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)
```

Packets: 121 · Displayed: 67 (47.1%) · Dropped: 0 (0.0%) Profile: Default

TRAFFIC MONITORING

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

Wi-Fi: en0

dns

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…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
28	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
29	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
30	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
31	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
32	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
33	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
34	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
35	0…	161.9.98.1			80	Standard query 0x754f SRV _nos._tcp.nos-avg.cz
36	0…	161.9.98.1				…RV _nos._tcp.nos-avg.cz
37	0…	161.9.98.1				…RV _nos._tcp.nos-avg.cz
38	0…	161.9.98.1				…RV _nos._tcp.nos-avg.cz
39	0…	161.9.98.1				…RV _nos._tcp.nos-avg.cz
40	1…	161.9.98.1				…RV _nos._tcp.nos-avg.cz
41	1…	161.9.98.1				…RV _nos._tcp.nos-avg.cz
42	1…	161.9.98.1				…A e9097.g.akamaiedge.net
43	1…	160.75.2.2				…0x90ed A e9097.g.akamaiedge.net A 104.84.194.219

Frame 23: 80 bytes on
Ethernet II, Src: App …:9f:f0:da)
Internet Protocol Ver
User Datagram Protoco
Domain Name System (query)

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… ⌘H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences ▶
Decode As…
Go to Linked Packet
Show Linked Packet in New Window

1 Color 1
2 Color 2
3 Color 3
4 Color 4
5 Color 5
6 Color 6
7 Color 7
8 Color 8
9 Color 9
10 Color 10
New Conversation Rule…

Domain Name System (dns), 38 bytes | Packets: 121 · Displayed: 57 (47.1%) · Dropped: 0 (0.0%) | Profile: Default

TRAFFIC MONITORING

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

Wi-Fi: en0

ip.src==161.9.98.110

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)
```

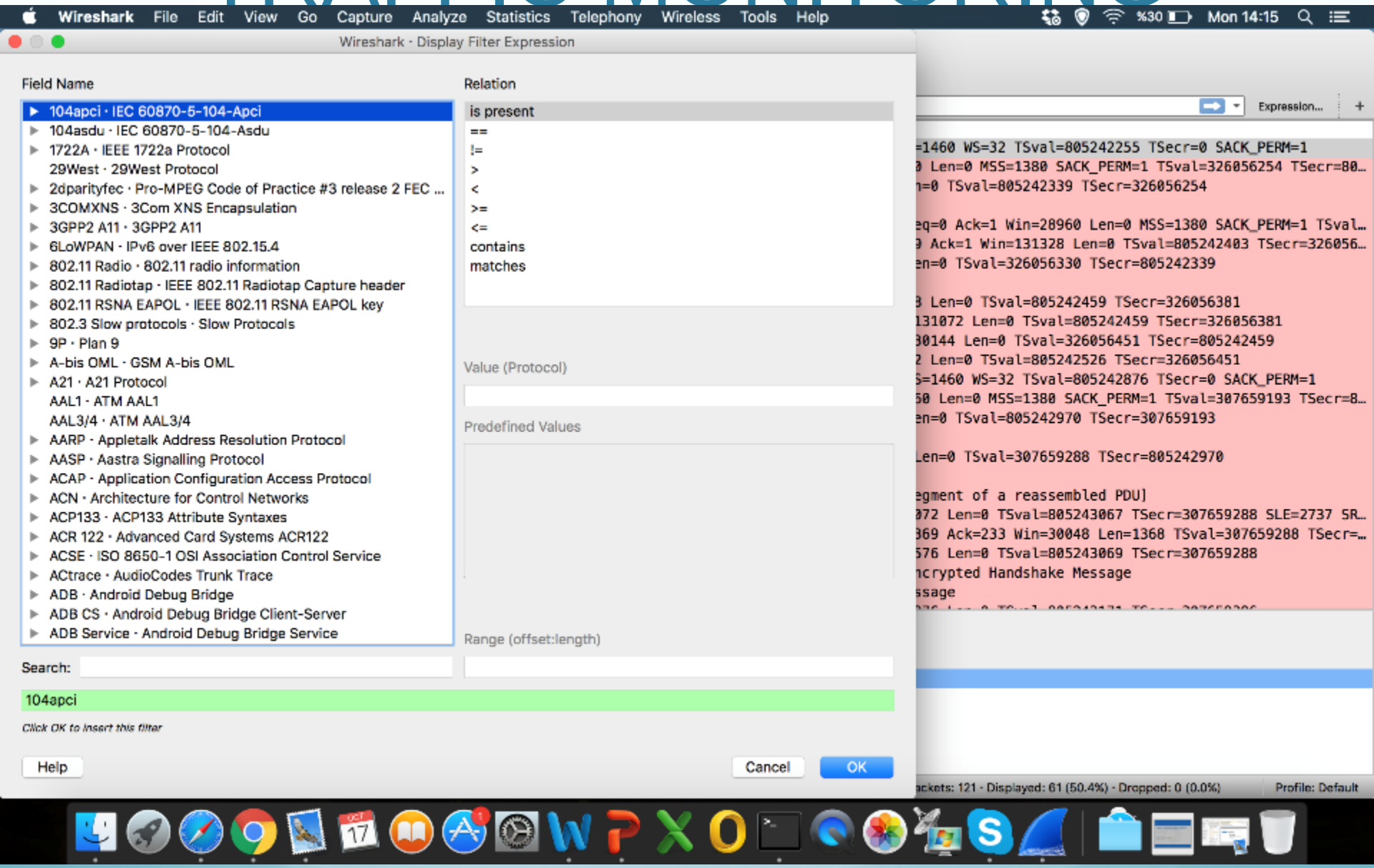
Packets: 121 · Displayed: 89 (73.6%) · Dropped: 0 (0.0%) Profile: Default

TRAFFIC MONITORING
Filtering Packets

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

* Taken from Wireshark User Guide

TRAFFIC MONITORING



TRAFFIC MONITORING

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

Wi-Fi: en0

ip.src==161.9.98.110

Wireshark · Capture Filters

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

Help Cancel OK

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

TRAFFIC MONITORING

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

Wi-Fi: en0

ip.src==161.9.98.110

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		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		=463 Win=131072 Len=0 TSval=805242526 TSecr=326056451
59	2…	161.9.98.110	46.197.15.60	DNS		os._tcp.nos-avg.cz
60	2…	161.9.98.110	160.75.2.20	DNS		3.b.akamaiedge.net
62	2…	161.9.98.110	23.6.123.158	TCP		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		=1 Win=131328 Len=0 TSval=805242970 TSecr=307659193
65	2…	161.9.98.110	23.6.123.158	TLSv1…		
69	2…	161.9.98.110	23.6.123.158	TCP		k=1369 Win=131072 Len=0 TSval=805243067 TSecr=307659288 SLE=2737 SR…
71	2…	161.9.98.110	23.6.123.158	TCP		k=3857 Win=128576 Len=0 TSval=805243069 TSecr=307659288
72	2…	161.9.98.110	23.6.123.158	TLSv1…		Cipher Spec, Encrypted Handshake Message
74	2…	161.9.98.110	23.6.123.158	TCP		k=3932 Win=130976 Len=0 TSval=805243171 TSecr=307659396
75	2…	161.9.98.110	23.6.123.158	TLSv1…		
76	2…	161.9.98.110	46.197.15.60	DNS		os._tcp.nos-avg.cz
77	2…	161.9.98.110	239.255.255.250	SSDP		
80	2…	161.9.98.110	23.6.123.158	TCP		720 Len=0 TSval=805243479 TSecr=307659705
81	2…	161.9.98.110	23.6.123.158	TLSv1…		
82	2…	161.9.98.110	23.6.123.158	TCP		n=131072 Len=0 TSval=805243479 TSecr=307659705
83	2…	161.9.98.110	160.75.2.20	DNS		api-production.elasticbeanstalk.com
84	2…	161.9.98.110	160.75.2.20	DNS		as-api-production.elasticbeanstalk.com
86	3…	161.9.98.110	23.6.123.158	TCP		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		os._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

Mark/Unmark Packet ⌘M
Ignore/Unignore Packet ⌘D
Set/Unset Time Reference ⌘T
Time Shift... ⇧⌘T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

TCP Stream
UDP Stream
SSL Stream

```
▶ 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 number: 589    (relative sequence number)
```

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

TRAFFIC MONITORING

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

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

```
GET /gls/gms HTTP/1.1
User-Agent: AVGAVM-MAC101106 1504822 OSLOC=1033 LOC=1033 PKG=121 PKP=0 PROD=AV VER=1504822 LIC=3UXYT-
BGX6U-HDFQI-QZJAY-WYOSV-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

Expression...

```
=1460 WS=32 TSval=805242255 TSecr=0 SACK_PERM=1
0 Len=0 MSS=1380 SACK_PERM=1 TSval=326056254 TSecr=80…
n=0 TSval=805242339 TSecr=326056254

eq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval…
9 Ack=1 Win=131328 Len=0 TSval=805242403 TSecr=326056…
en=0 TSval=326056330 TSecr=805242339

3 Len=0 TSval=805242459 TSecr=326056381
131072 Len=0 TSval=805242459 TSecr=326056381
30144 Len=0 TSval=326056451 TSecr=805242459
2 Len=0 TSval=805242526 TSecr=326056451
```

ackets: 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_en0_20161017132105_X5fEOq

57567 Standard query 0x... 53
62389 Standard query 0x90ed A e9097.g.aka... 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 50286 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=805242255 TSecr=0 SACK_PERM=1 80
50286 80 → 50286 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=326056254 TSecr=80524225... 80
50286 50286 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=805242339 TSecr=326056254 80
50286 GET /gls/gms HTTP/1.1 80
57567 Standard query 0x... 53
50286 [TCP Out-Of-Order] 80 → 50286 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=3260563... 80
50286 [TCP Dup ACK 48#1] 50286 → 80 [ACK] Seq=589 Ack=1 Win=131328 Len=0 TSval=805242403 TSecr=326056254 80
50286 80 → 50286 [ACK] Seq=1 Ack=589 Win=30144 Len=0 TSval=326056330 TSecr=805242339 80

Packet 44: ARP: Who has 161.9.99.254? Tell 161.9.98.110

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

Reset

Help Close Save As...

```
▶ 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

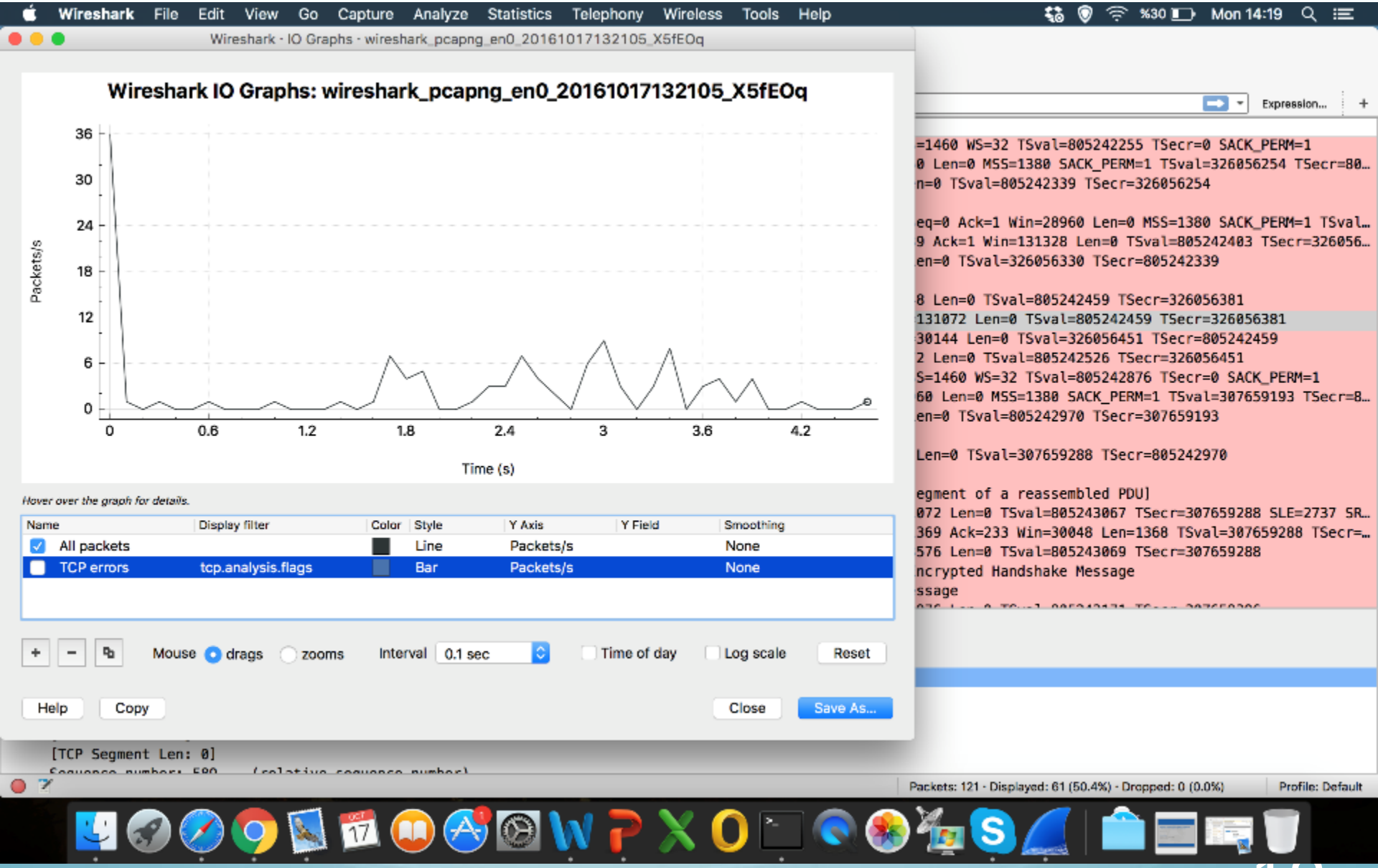
Wireshark · Protocol Hierarchy Statistics · wireshark_pcapng_en0_20161017132105_X5fEOq

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	61	100.0	14985	54 k	0	0
Ethernet	100.0	61	100.0	14985	54 k	0	0
Internet Protocol Version 4	100.0	61	100.0	14985	54 k	0	0
Transmission Control Protocol	100.0	61	100.0	14985	54 k	40	4028
Secure Sockets Layer	31.1	19	65.2	9776	35 k	18	9444
Secure Sockets Layer	1.6	1	2.2	332	1208	1	332
Hypertext Transfer Protocol	3.3	2	7.9	1181	4299	1	654
Malformed Packet	1.6	1	3.5	527	1918	1	527

Display filter: tcp

Help Copy Close

TRAFFIC MONITORING



TRAFFIC MONITORING