BVM Engineering College, VV Nagar

Gujarat Technological University

CYBER SECURITY

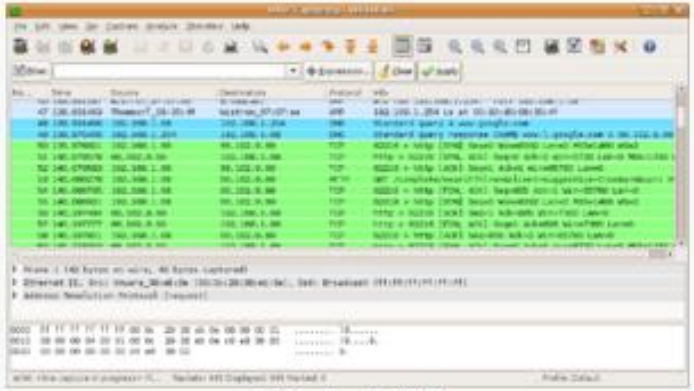
Presentation

Chaitanya Tejaswi (140080111013)

What's Wireshark?

Wireshark is a free
graphical
front-end
open source
network packet analyzer

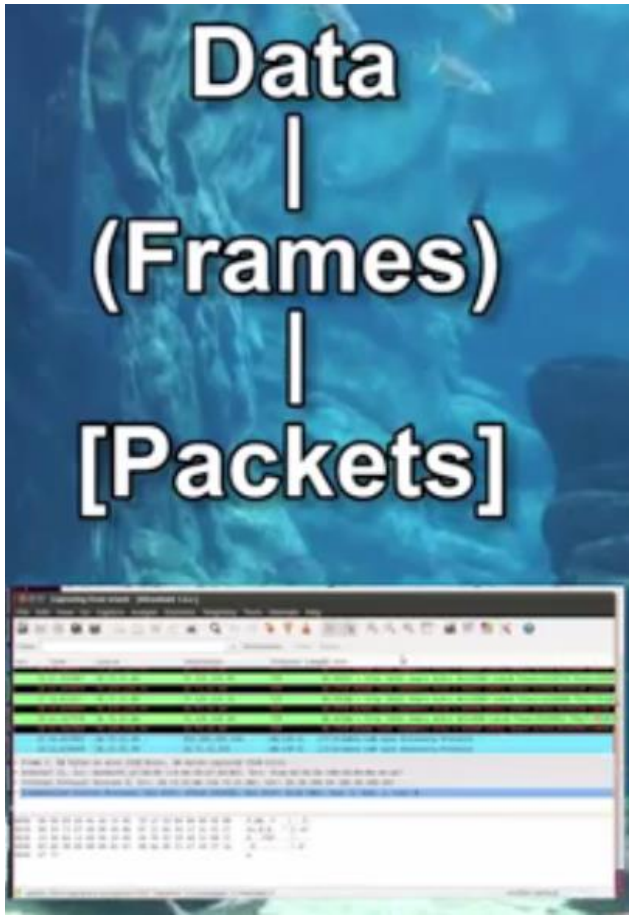
Wireshark



Wireshark GUI

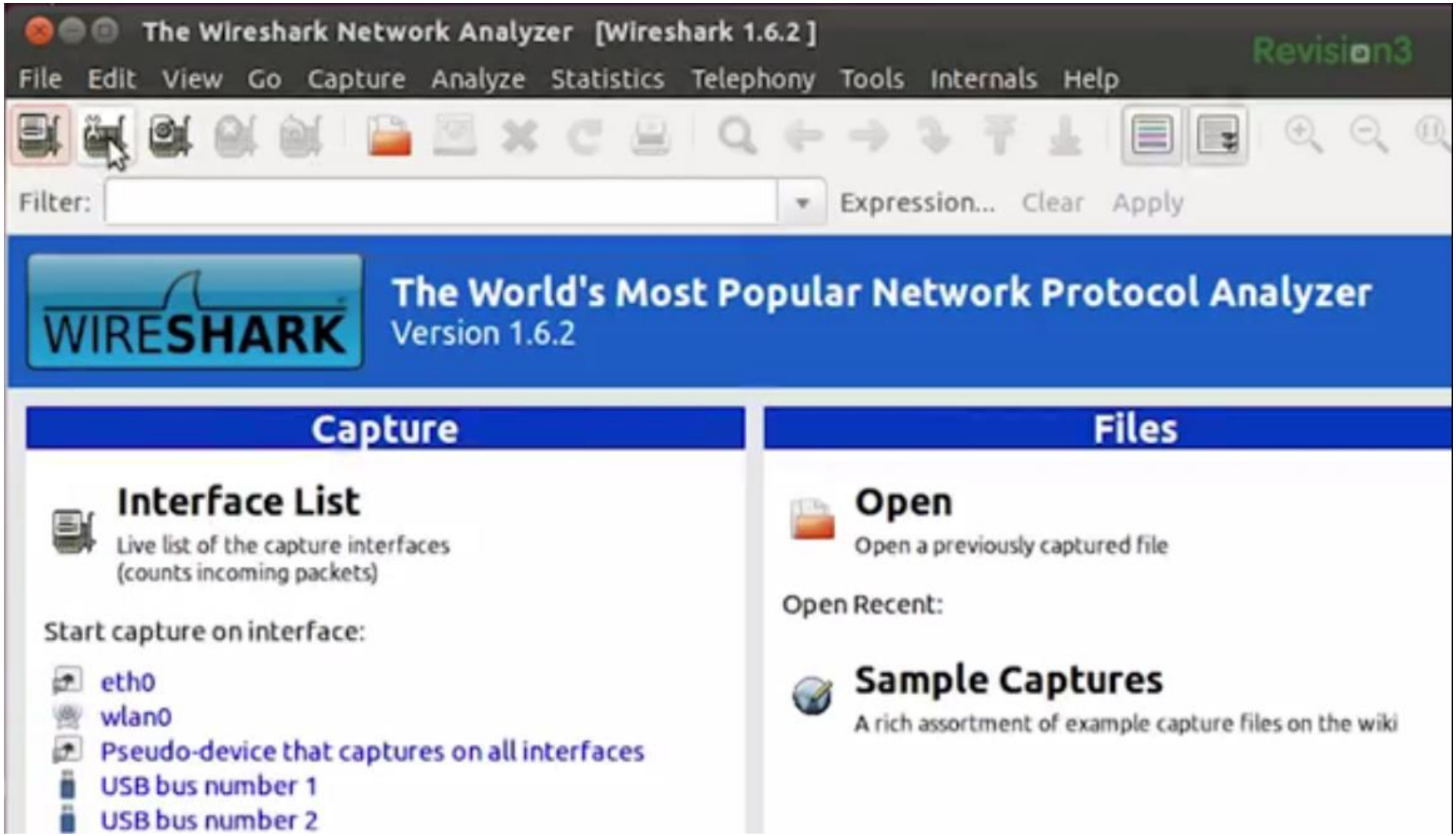
Original author(s)	Gerald Combs[1]
Developer(s)	The Wireshark team
Initial release	Around 1998; 18 years ago
Stable release	2.2.0 / 7 September 2016; 25 days ago[2]
Written in	C, C++
Operating system	Cross-platform
Type	Packet analyzer
License	GNU GPL[3]
Website	www.wireshark.org
Repository	code.wireshark.org/review/gitweb?p=wireshark.git

What does it do?

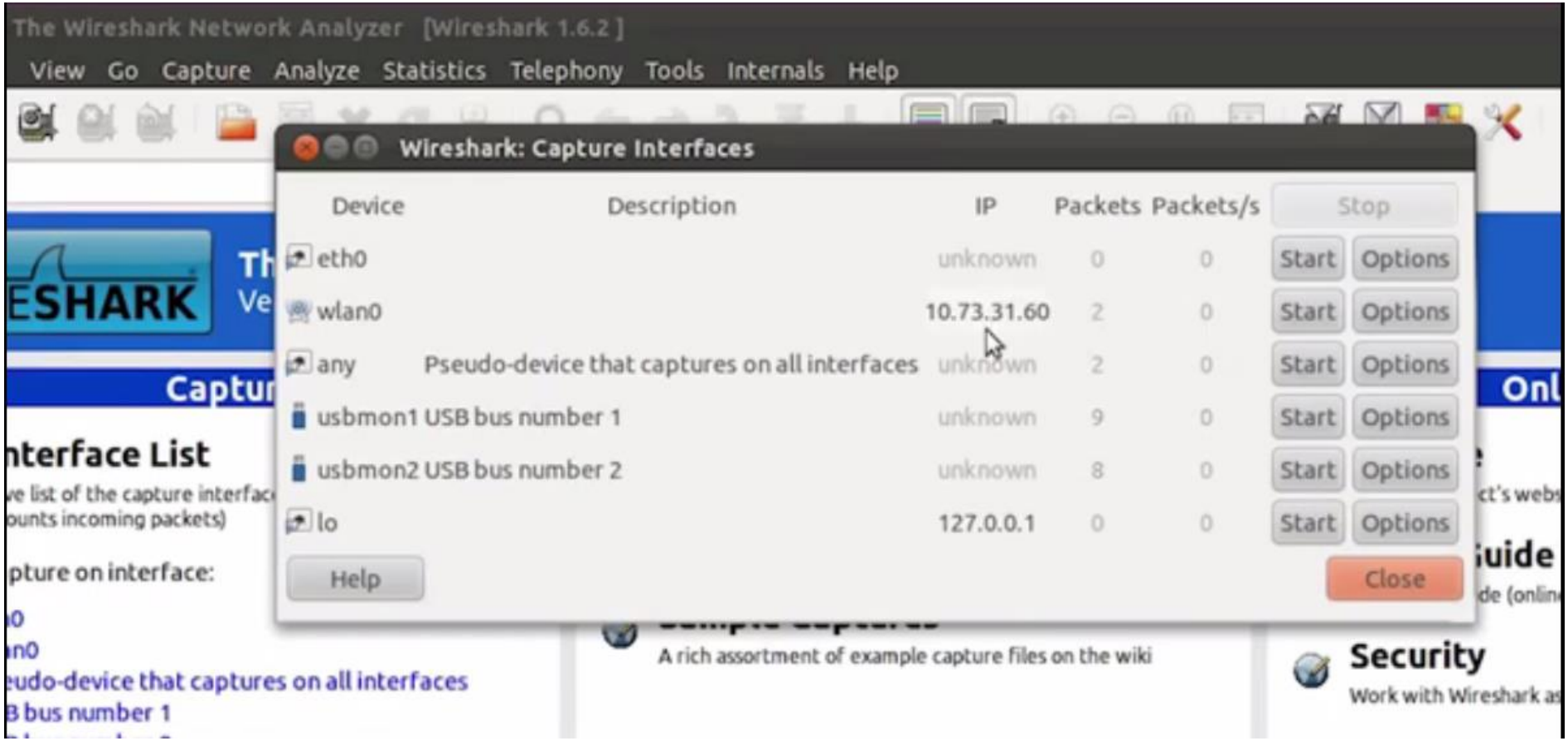


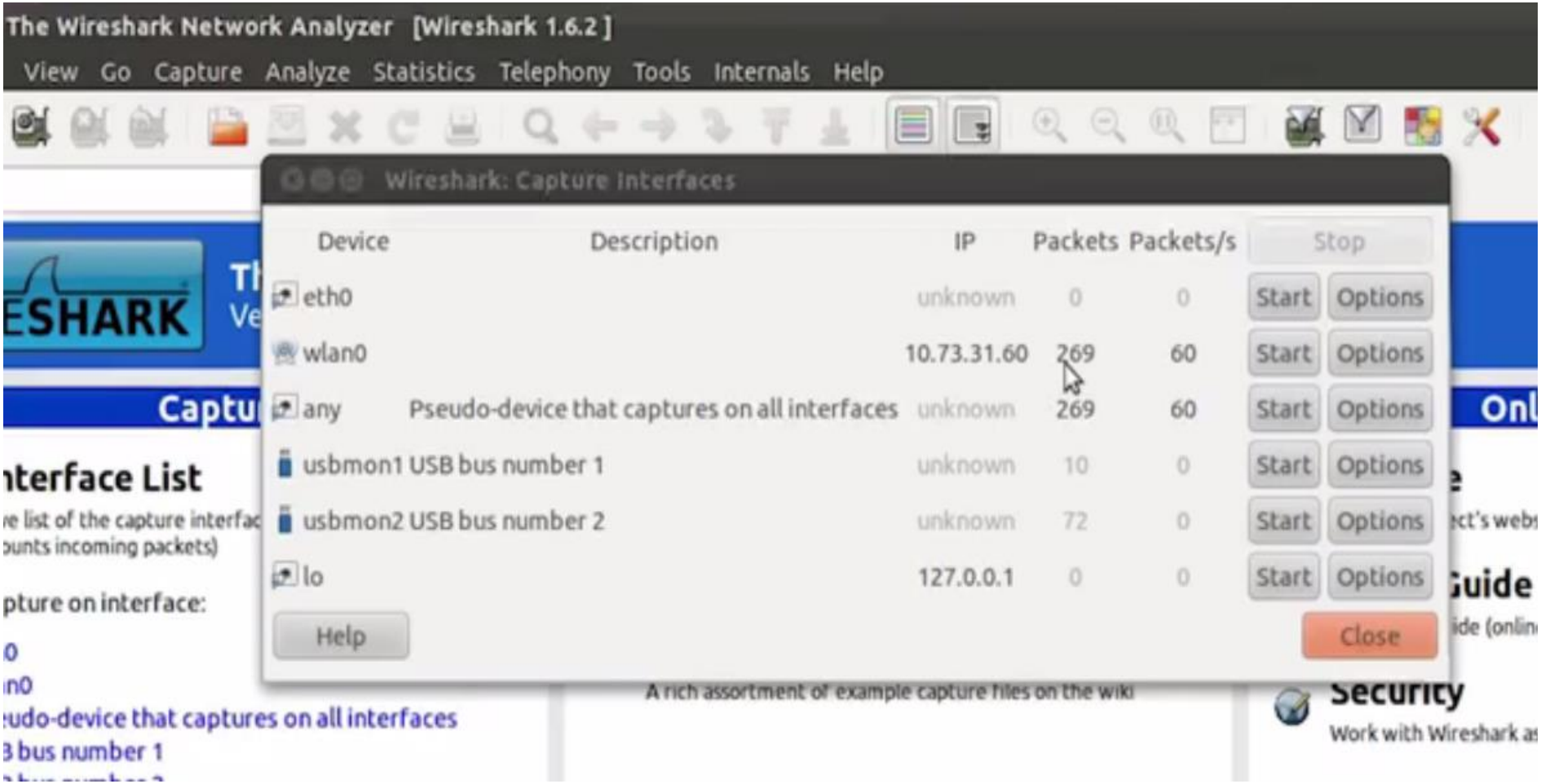
Hunts for packets in the TCP-IP Layer and keeps a track of whatever it finds

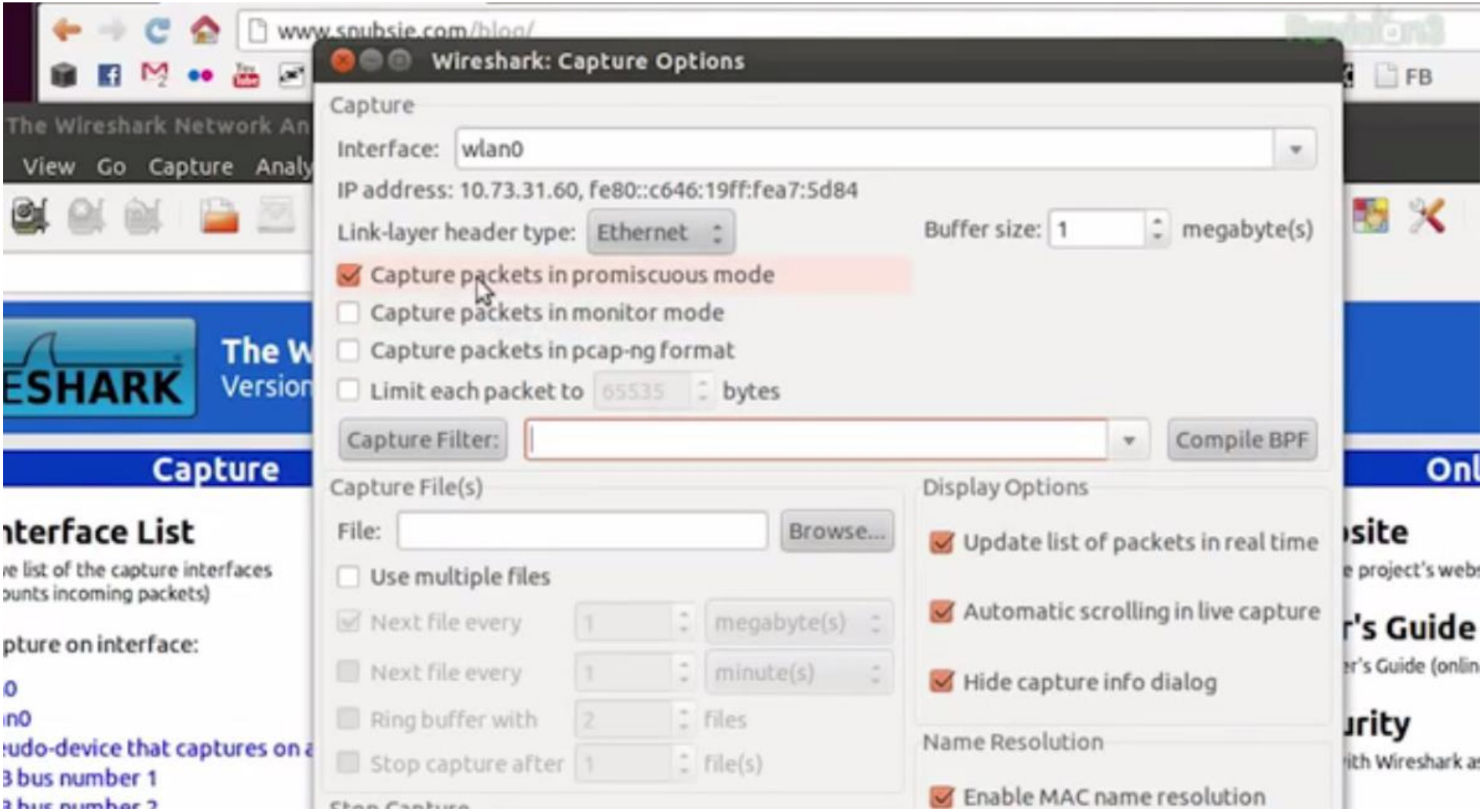
Interface


The Wireshark Network Analyzer [Wireshark 1.6.2]
Revision3
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.6.2
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start capture on interface:
eth0
wlan0
Pseudo-device that captures on all interfaces
USB bus number 1
USB bus number 2
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki

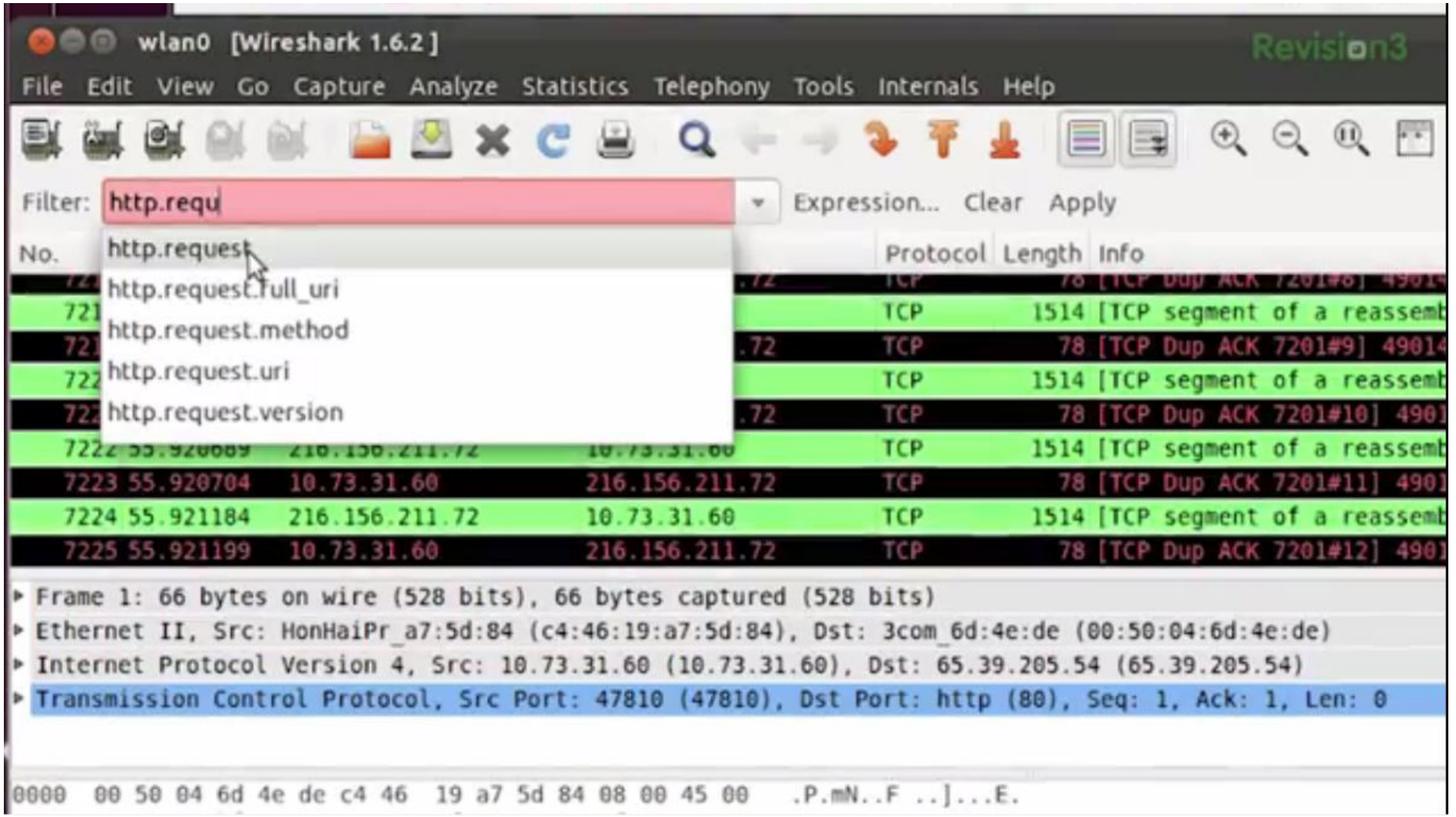
Capture Interface

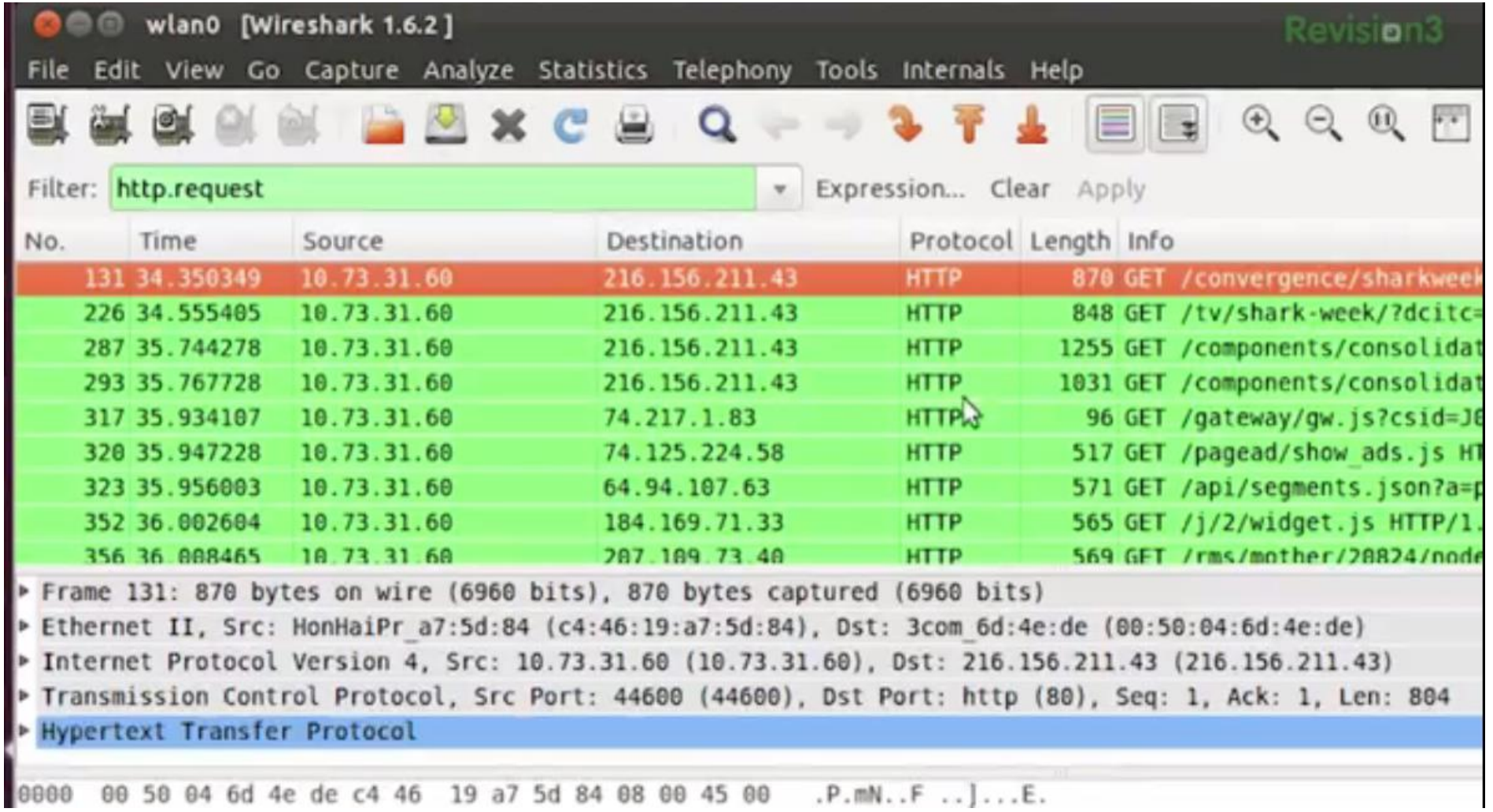


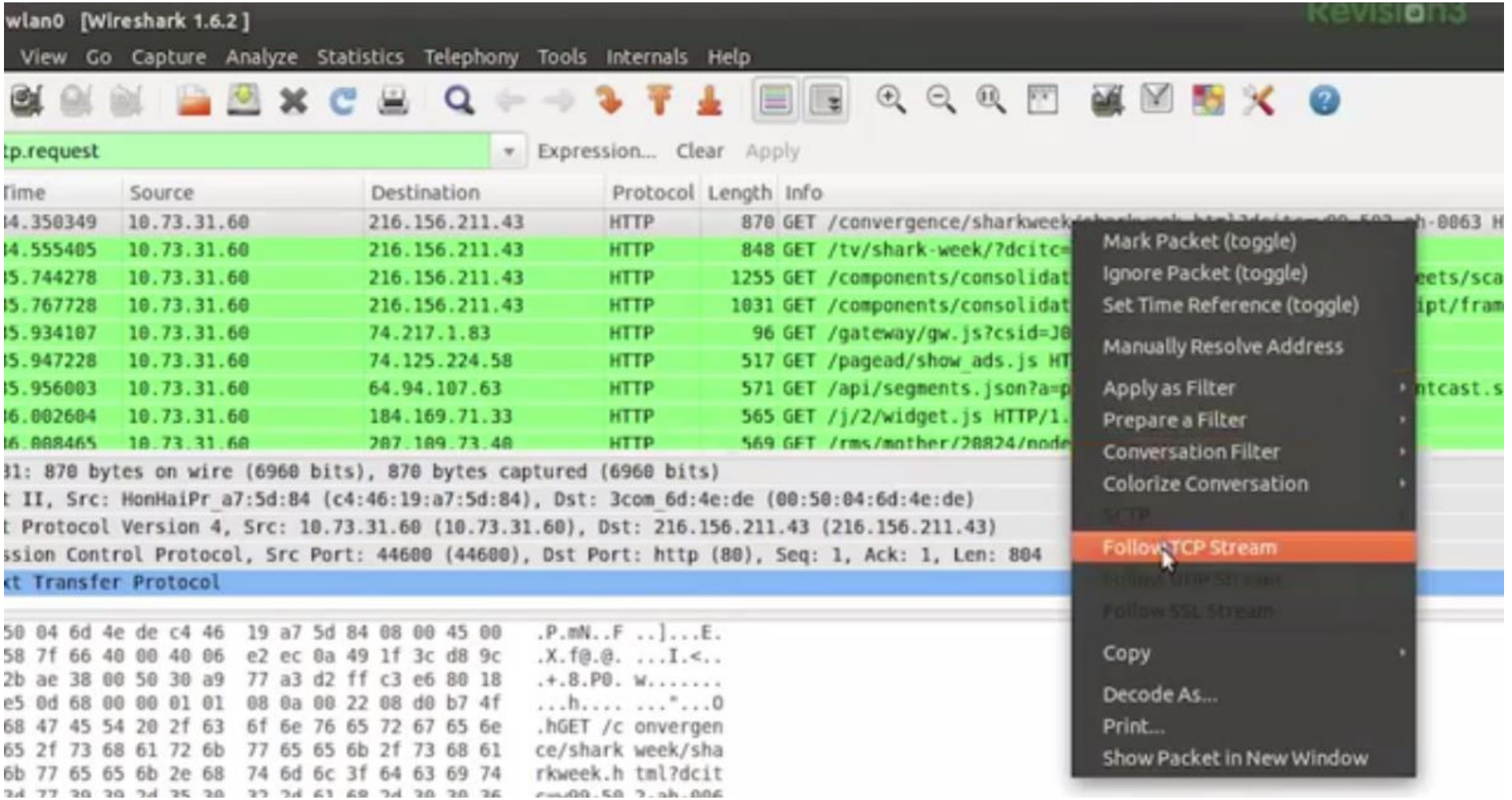

The Wireshark Network Analyzer [Wireshark 1.6.2]
View Go Capture Analyze Statistics Telephony Tools Internals Help
Wireshark: Capture Interfaces
Device Description IP Packets Packets/s
Stop
eth0 unknown 0 0 Start Options
wlan0 10.73.31.60 269 60 Start Options
any Pseudo-device that captures on all interfaces unknown 269 60 Start Options
usbmon1 USB bus number 1 unknown 10 0 Start Options
usbmon2 USB bus number 2 unknown 72 0 Start Options
lo 127.0.0.1 0 0 Start Options
Help
Close
nterface List
pture on interface:
udo-device that captures on all interfaces
3 bus number 1
A rich assortment of example capture files on the wiki
Security
Work with Wireshark as

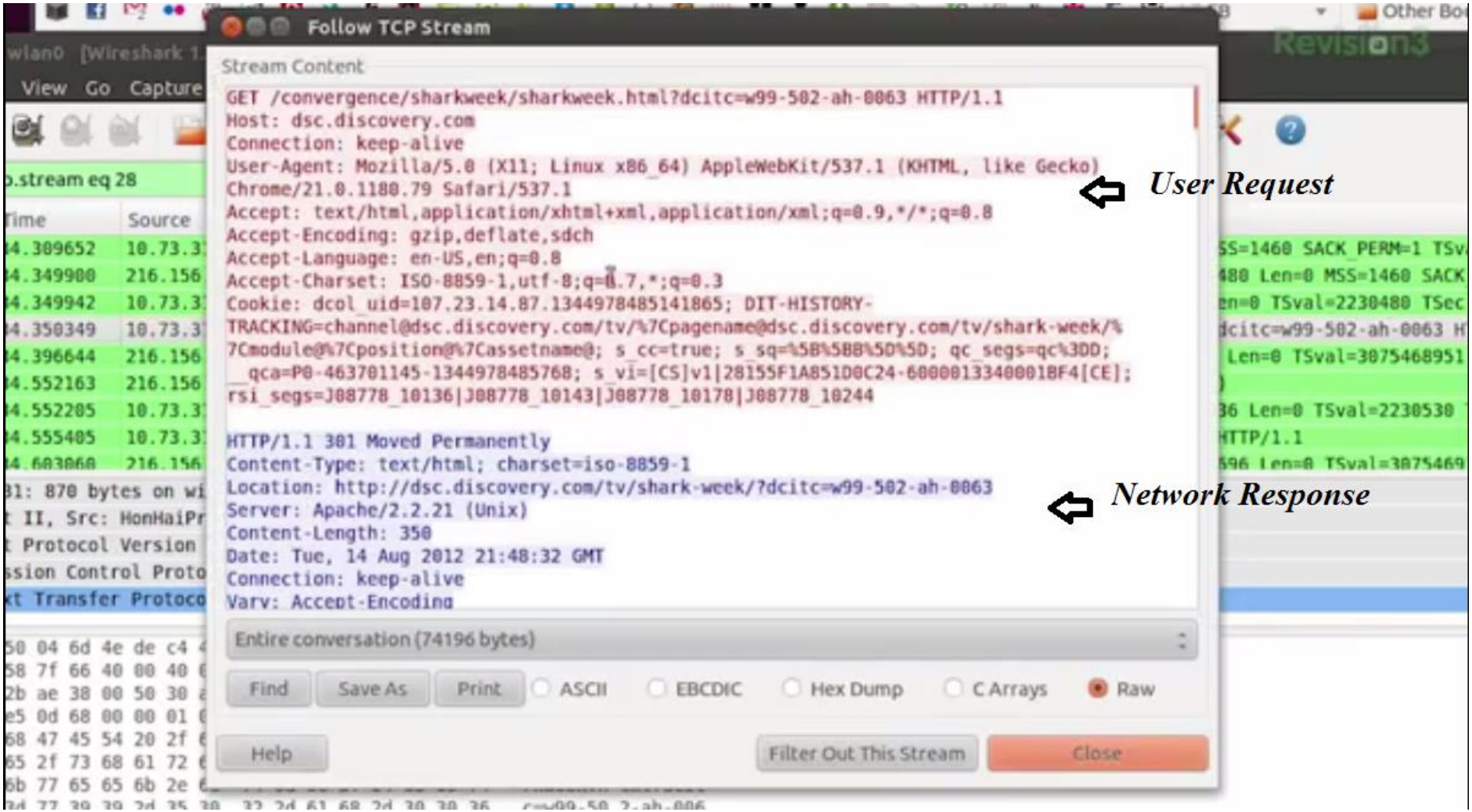

www.snubsie.com/blog/
FB
The Wireshark Network An
View Go Capture Analy
ESHARK
The W
Version
Capture
nterface List
e list of the capture interfaces
ounts incoming packets)
pture on interface:
0
n0
udo-device that captures on a
3 bus number 1
Wireshark: Capture Options
Capture
Interface: wlan0
IP address: 10.73.31.60, fe80::c646:19ff:fea7:5d84
Link-layer header type: Ethernet
Buffer size: 1 megabyte(s)
Capture packets in promiscuous mode
Capture packets in monitor mode
Capture packets in pcap-ng format
Limit each packet to 65535 bytes
Capture Filter:
Compile BPF
Capture File(s)
File:
Browse...
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Onl
site
project's webs
r's Guide
r's Guide (onlin
urity
ith Wireshark as

Example: HTTP Request




wlan0 [Wireshark 1.6.2]
Revision3
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
131 34.350349 10.73.31.60 216.156.211.43 HTTP 870 GET /convergence/sharkweek
226 34.555405 10.73.31.60 216.156.211.43 HTTP 848 GET /tv/shark-week/?dcitc=
287 35.744278 10.73.31.60 216.156.211.43 HTTP 1255 GET /components/consolidat
293 35.767728 10.73.31.60 216.156.211.43 HTTP 1031 GET /components/consolidat
317 35.934107 10.73.31.60 74.217.1.83 HTTP 96 GET /gateway/gw.js?csid=J0
320 35.947228 10.73.31.60 74.125.224.58 HTTP 517 GET /pagead/show_ads.js HT
323 35.956003 10.73.31.60 64.94.107.63 HTTP 571 GET /api/segments.json?a=p
352 36.002604 10.73.31.60 184.169.71.33 HTTP 565 GET /j/2/widget.js HTTP/1.
356 36.008465 10.73.31.60 207.109.73.40 HTTP 569 GET /rms/mother/20824/node
Frame 131: 870 bytes on wire (6960 bits), 870 bytes captured (6960 bits)
Ethernet II, Src: HonHaiPr_a7:5d:84 (c4:46:19:a7:5d:84), Dst: 3com_6d:4e:de (00:50:04:6d:4e:de)
Internet Protocol Version 4, Src: 10.73.31.60 (10.73.31.60), Dst: 216.156.211.43 (216.156.211.43)
Transmission Control Protocol, Src Port: 44600 (44600), Dst Port: http (80), Seq: 1, Ack: 1, Len: 804
Hypertext Transfer Protocol
0000 00 50 04 6d 4e de c4 46 19 a7 5d 84 08 00 45 00 .P.mN..F ..]...E.


wlan0 [Wireshark 1.6.2]
View Go Capture Analyze Statistics Telephony Tools Internals Help
tp.request
Expression... Clear Apply
Time Source Destination Protocol Length Info
4.350349 10.73.31.60 216.156.211.43 HTTP 870 GET /convergence/sharkweek
4.555405 10.73.31.60 216.156.211.43 HTTP 848 GET /tv/shark-week/?dcitc=
5.744278 10.73.31.60 216.156.211.43 HTTP 1255 GET /components/consolidat
5.767728 10.73.31.60 216.156.211.43 HTTP 1031 GET /components/consolidat
5.934107 10.73.31.60 74.217.1.83 HTTP 96 GET /gateway/gw.js?csid=J0
5.947228 10.73.31.60 74.125.224.58 HTTP 517 GET /pagead/show_ads.js HT
5.956003 10.73.31.60 64.94.107.63 HTTP 571 GET /api/segments.json?a=p
6.002604 10.73.31.60 184.169.71.33 HTTP 565 GET /j/2/widget.js HTTP/1.
31: 870 bytes on wire (6960 bits), 870 bytes captured (6960 bits)
t II, Src: HonHaiPr_a7:5d:84 (c4:46:19:a7:5d:84), Dst: 3com_6d:4e:de (00:50:04:6d:4e:de)
t Protocol Version 4, Src: 10.73.31.60 (10.73.31.60), Dst: 216.156.211.43 (216.156.211.43)
ssion Control Protocol, Src Port: 44600 (44600), Dst Port: http (80), Seq: 1, Ack: 1, Len: 804
t Transfer Protocol
50 04 6d 4e de c4 46 19 a7 5d 84 08 00 45 00 .P.mN..F ..]...E.
58 7f 66 40 00 40 06 e2 ec 0a 49 1f 3c d8 9c .X.f@.@. ...I.<..
2b ae 38 00 50 30 a9 77 a3 d2 ff c3 e6 80 18 .+.8.P0. w.......
e5 0d 68 00 00 01 01 08 0a 00 22 08 d0 b7 4f ...h.... ..."...O
68 47 45 54 20 2f 63 6f 6e 76 65 72 67 65 6e .hGET /c onvergen
65 2f 73 68 61 72 6b 77 65 65 6b 2f 73 68 61 ce/shark week/sha
6b 77 65 65 6b 2e 68 74 6d 6c 3f 64 63 69 74 rkweek.h tml?dcit
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
Follow TCP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window


Follow TCP Stream
Stream Content
GET /convergence/sharkweek/sharkweek.html?dcitc=w99-502-ah-0063 HTTP/1.1
Host: dsc.discovery.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.1 (KHTML, like Gecko)
Chrome/21.0.1180.79 Safari/537.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: dcol_uid=107.23.14.87.1344978485141865; DIT-HISTORY-
TRACKING=channel@dsc.discovery.com/tv/%7Cpagename@dsc.discovery.com/tv/shark-week/%
7Cmodule@%7Cposition@%7Cassetname@; s_cc=true; s_sq=%5B%5BB%5D%5D; qc_segs=qc%3DD;
__qca=P0-463701145-1344978485768; s_vi=[CS]v1|28155F1A851D0C24-6000013340001BF4[CE];
rsi_segs=J08778_10136|J08778_10143|J08778_10178|J08778_10244
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=iso-8859-1
Location: http://dsc.discovery.com/tv/shark-week/?dcitc=w99-502-ah-0063
Server: Apache/2.2.21 (Unix)
Content-Length: 350
Date: Tue, 14 Aug 2012 21:48:32 GMT
Connection: keep-alive
Vary: Accept-Encoding
Entire conversation (74196 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close
User Request
Network Response

CLI Options