

Introduction to Packet Capture & Analysis

using  & 

Josh Bruntly

Assistant Professor
Marshall University



DIGITAL FORENSICS
INFORMATION ASSURANCE



joshbrunty@hack3rcon8: ~

joshbrunty@hack3rcon8:~\$ whoami

joshbrunty

joshbrunty@hack3rcon8:~\$ nano tellthemaboutyou.txt|

GNU nano 2.2.6

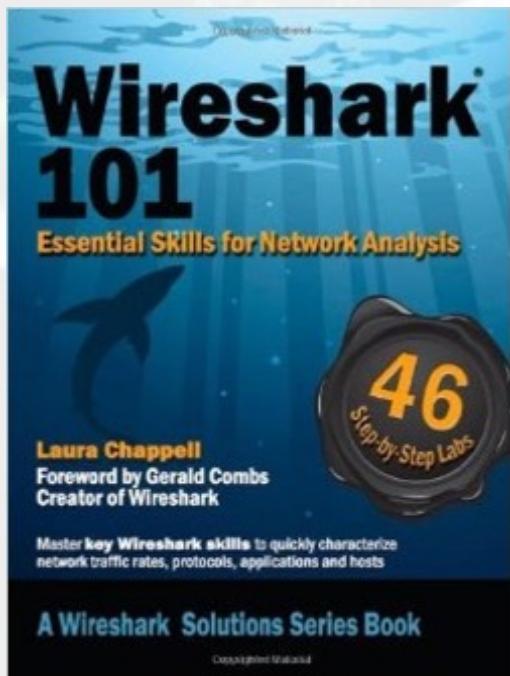
New Buffer

```
* Asst. Professor of Digital Forensics  
  @MarshallU in Huntington, WV  
* Former Digital Forensics Lab Tech Leader/QA Mgr/Examiner  
* I teach: Network Forensics,  
            Intro to Linux,  
            Intro to Digital Forensics courses  
* #1 Troll to @oncee  
* Once stood in line with Bill Gardner at a Burger King■
```

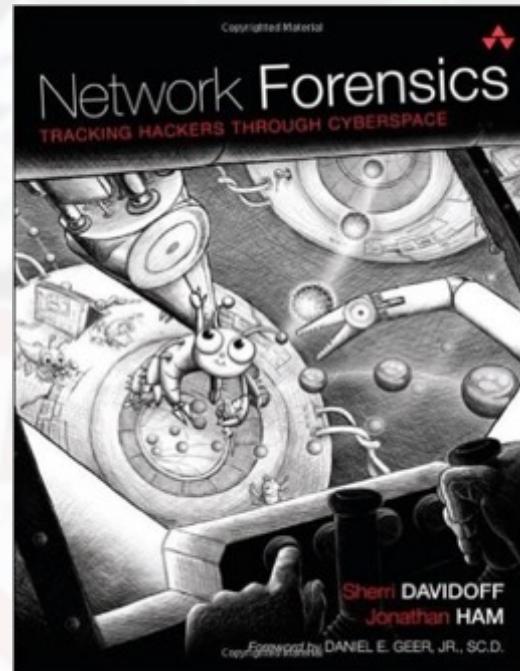
Absenged



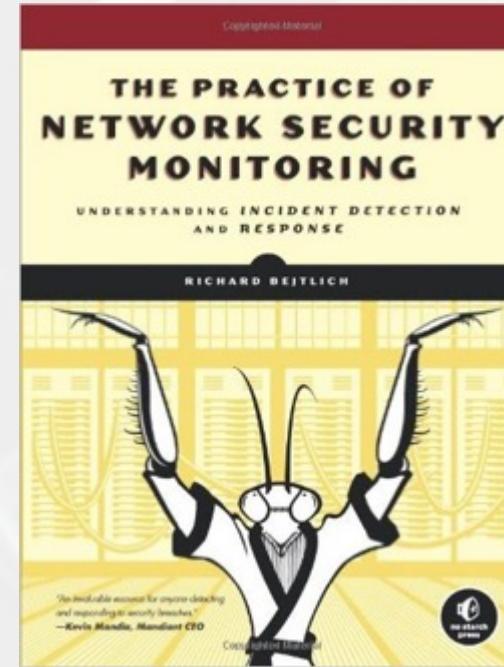
Resources I'd Recommend...



<http://a.co/0Zg87AK>



<http://a.co/dtRtKuA>



<http://a.co/agGV6Ht>



<http://a.co/iavdsQw>



What we will need for this session...

- Kali and/or SIFT Workstation
 - <http://www.kali.org>
 - <https://digital-forensics.sans.org/community/downloads>
- Bash terminal
- A stable internet browser
- Download course materials PowerPoint, PCAP Files
 - [www.github.com/joshbrunty/Hack3rCon8_Wireshark](https://github.com/joshbrunty/Hack3rCon8_Wireshark)
- Wireshark
 - www.wireshark.org
 - Version 2 (preferably)
 - Running in Linux (preferably SANS SIFT or Kali)
 - Linux Users: apt-get install wireshark-qt

What do we use Wireshark for?

- ❑ Wireshark IS used for decoding and analyzing captured traffic
- ❑ Wireshark IS used to extract contents of packets/packet files (pcaps)

What do we *NOT* use Wireshark for?

- ❑ Wireshark IS NOT made to capture large amounts of traffic
- ❑ Wireshark IS NOT a SIEM or Firewall
- ❑ Wireshark IS NOT a real-time network monitoring tool (that's what IDS's are for)



Tools Overview

- **Tcpdump**
 - Unix-based command-line tool used to intercept packets
 - Including **filtering** to just the packets of interest
 - Reads “live traffic” from interface specified using **-i** option ...
 - ... or from a previously recorded **trace file** specified using **-r** option
 - You create files when capturing live traffic using **-w** option
- **Tshark**
 - Tcpdump-like capture program that comes w/ Wireshark
 - Very similar behavior & flags to tcpdump
- **Wireshark**
 - GUI for displaying tcpdump/tshark packet traces



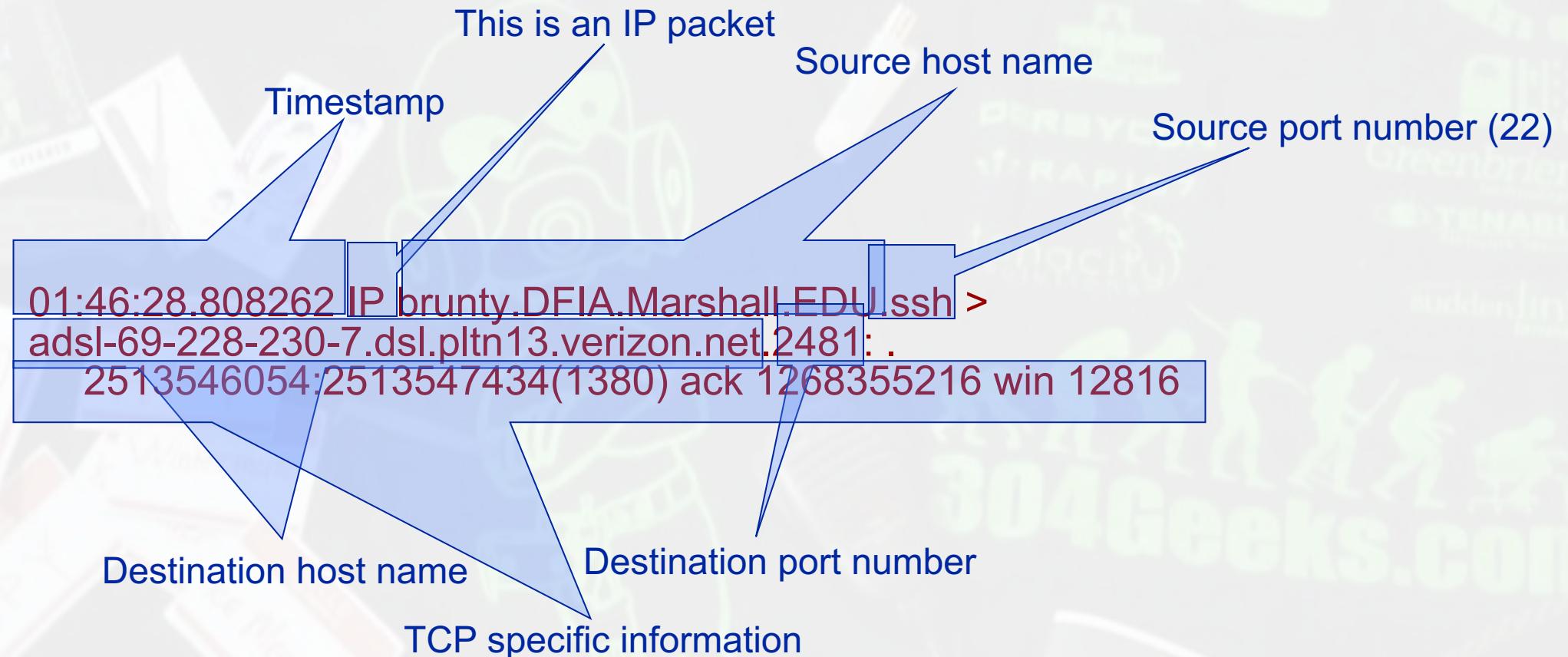
Tcpdump example

- Example run of tcpdump on a Linux machine
- First few lines of the output:

```
01:46:28.808262 IP brunty.DFIA.Marshall.EDU.ssh > ads1-69-228-230-7.dsl.pltn13.verizon.net.2481: . 2513546054:2513547434(1380) ack 1268355216 win 12816
01:46:28.808271 IP brunty.DFIA.Marshall.EDU.ssh > ads1-69-228-230-7.dsl.pltn13.verizon.net.2481: P 1380:2128(748) ack 1 win 12816
01:46:28.808276 IP brunty.DFIA.Marshall.EDU.ssh > ads1-69-228-230-7.dsl.pltn13.verizon.net.2481: . 2128:3508(1380) ack 1 win 12816
01:46:28.890021 IP ads1-69-228-230-7.dsl.pltn13.verizon.net.2481 > brunty.DFIA.Marshall.EDU.ssh: P 1:49(48) ack 1380 win 16560
```



What does a packet convey?



- Different output formats for different packet types

Similar Output from Tshark

```
1190003744.940437 61.184.241.230 -> 128.32.48.169
    SSH Encrypted request packet len=48
1190003744.940916 128.32.48.169 -> 61.184.241.230
    SSH Encrypted response packet len=48
1190003744.955764 61.184.241.230 -> 128.32.48.169
    TCP 6943 > ssh [ACK] Seq=48 Ack=48 Win=65514 Len=0
    TSV=445871583 TSER=632535493
1190003745.035678 61.184.241.230 -> 128.32.48.169
    SSH Encrypted request packet len=48
1190003745.036004 128.32.48.169 -> 61.184.241.230
    SSH Encrypted response packet len=48
1190003745.050970 61.184.241.230 -> 128.32.48.169
    TCP 6943 > ssh [ACK] Seq=96 Ack=96 Win=65514 Len=0
    TSV=445871583 TSER=632535502
```

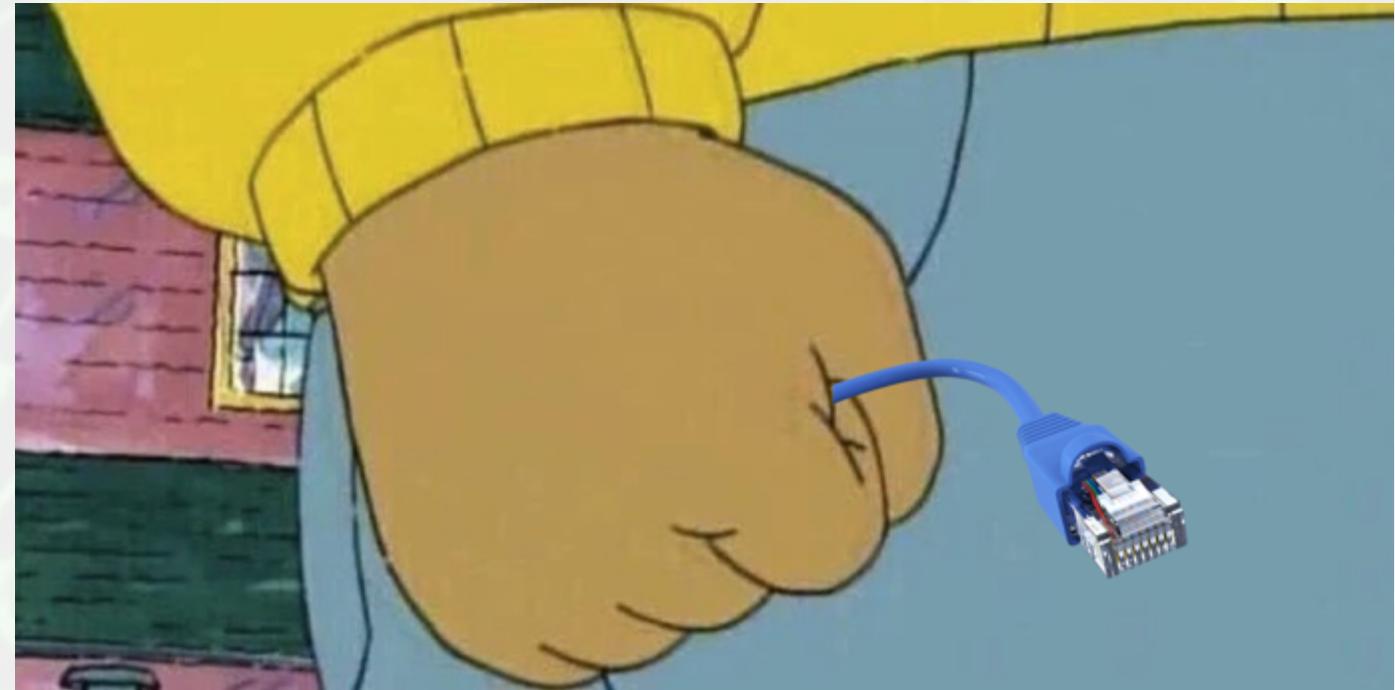


Running tcpdump

- Requires superuser/administrator privileges on Unix
 - <http://www.tcpdump.org/>
 - You can do it on your own Unix machine
 - You can install a Linux OS (SIFT/Kali) in Vmware on your machine
- Tcpdump for Windows
 - WinDump: <http://www.winpcap.org/windump/>
 - Free software
 - Part of Wireshark for Windows install

First Things First....

- We need to connect to the network we're sniffing
- Method 1: "on the wire"
- Method 2: "in the air"



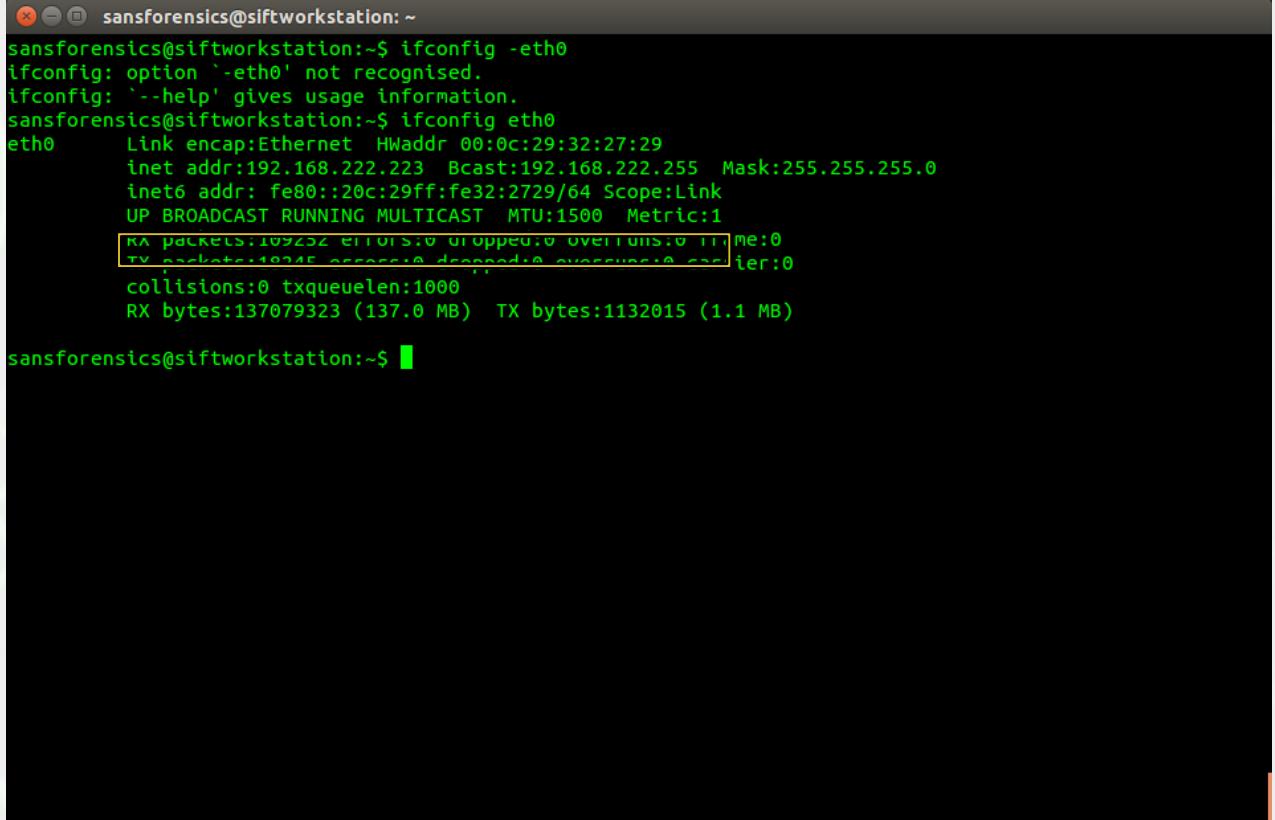
http://www.newegg.com/Product/Product.aspx?Item=9SIA8UD37Y8211&cm_re=Alfa_wireless_adapter_-9SIA8UD37Y8211--Product

<https://www.hak5.org/gear/packet-squirrel>

<http://hackerwarehouse.com/product/lan-tap-pro/>

First Things First....

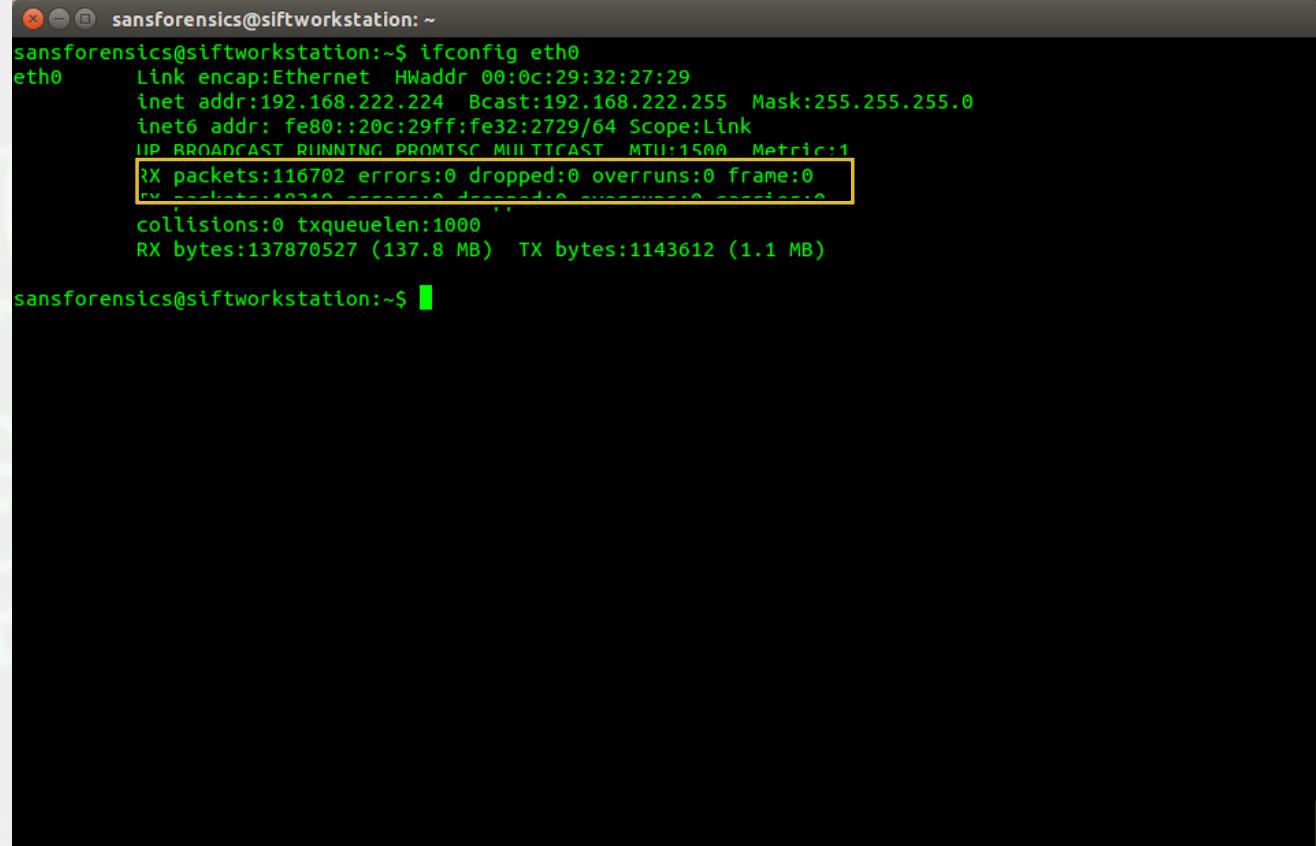
- ❑ In order to capture packets we need to check and see if our capture interface is in promiscuous mode:
 - ❑ \$ sudo ifconfig eth0



```
sansforensics@siftworkstation:~$ ifconfig -eth0
ifconfig: option `--eth0' not recognised.
ifconfig: '--help' gives usage information.
sansforensics@siftworkstation:~$ ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0c:29:32:27:29
          inet addr:192.168.222.223  Bcast:192.168.222.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:2729/64 Scope:Link
                     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                     RX packets:109252 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:18245 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:137079323 (137.0 MB)  TX bytes:1132015 (1.1 MB)
sansforensics@siftworkstation:~$
```

First Things First....

- ❑ If it is not, then we can set it to promiscuous mode
 - ❑ \$ sudo ifconfig eth0 promisc



```
sansforensics@siftworkstation:~$ ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0c:29:32:27:29
          inet addr:192.168.222.224 Bcast:192.168.222.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:2729/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
          RX packets:116702 errors:0 dropped:0 overruns:0 frame:0
          RX bytes:137870527 (137.8 MB) TX bytes:1143612 (1.1 MB)
          collisions:0 txqueuelen:1000
          RX bytes:137870527 (137.8 MB) TX bytes:1143612 (1.1 MB)

sansforensics@siftworkstation:~$
```

Demo 1 – Our 1st Run

- Syntax: *tcpdump [options] [filter expression]*
- I will demonstrate it using our domain here
 - \$ sudo tcpdump -i eth0
 - On your own Unix machine, you can run it using “sudo” or directly run “tcpdump”
- Observe the output



Filters

- ❑ We are often not interested in all packets flowing through the network
- ❑ Use filters to capture only packets of interest to us



Demo 2- Setting a Capture Filter

1. **Capture only udp packets**
 - tcpdump "udp"
2. **Capture only tcp packets**
 - tcpdump "tcp"



Demo 2 (contd.)

1. Capture only UDP packets with destination port 53 (DNS requests)
 - tcpdump "udp dst port 53"
2. Capture only UDP packets with source port 53 (DNS replies)
 - tcpdump "udp src port 53"
3. Capture only UDP packets with source or destination port 53 (DNS requests and replies)
 - tcpdump "udp port 53"



Demo 2 (contd.)

1. Capture only packets destined to **forensics.marshall.edu**
 - `tcpdump "dst host forensics.marshall.edu"`
2. Capture both DNS packets and TCP packets to/from **forensics.marshall.edu**
 - `tcpdump "(tcp and host forensics.marshall.edu) or udp port 53"`



How to write filters

- Refer the tcpdump/tshark man page
 - man pcap-filter (tcpdump)
 - Man wireshark-filter (Tshark/Wireshark)
- Many example webpages on the Internet



So What is Wireshark?

- ❑ Packet sniffer/protocol analyzer
- ❑ Open Source Network Tool
- ❑ Latest version of the ethereal tool

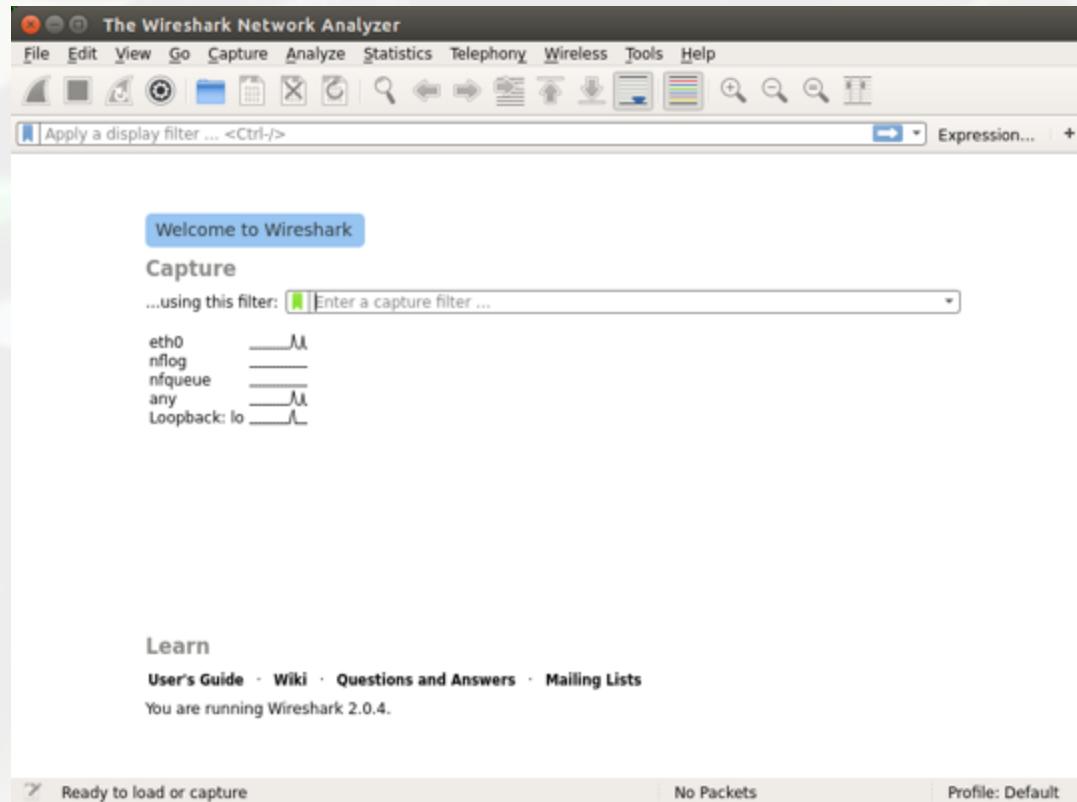


What is tShark?

- The command-line based packet capture tool
- Equivalent to Wireshark except command line (CLI) based



Wireshark Interface



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.30.30.20	10.30.30.255	NTP	90	NTP Version 4, broadcast
2	1.746510	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6a3f4b0c
3	1.746522	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6a3f4b0c
4	1.746526	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6a3f4b0c
5	1.747259	192.168.30.10	192.168.30.108	DHCP	358	DHCP ACK - Transaction ID 0x6a3f4b0c
6	3.962755	192.168.30.101	192.168.30.255	BROWSER	216	Get Backup List Request
7	3.962765	192.168.30.101	192.168.30.255	BROWSER	216	Get Backup List Request
8	3.962769	192.168.30.101	192.168.30.255	BROWSER	216	Get Backup List Request
9	3.962771	192.168.30.101	192.168.30.255	NBNS	92	Name query NB WORKGROUP<1b>
10	3.962774	192.168.30.101	192.168.30.255	NBNS	92	Name query NB WORKGROUP<1b>
11	3.962776	192.168.30.101	192.168.30.255	NBNS	92	Name query NB WORKGROUP<1b>
12	4.327298	192.168.30.108	192.168.30.255	NBNS	110	Registration NB ANN-LAPTOP<00>

Frame 2: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Request)

0000 ff ff ff ff ff ff 00 21 70 4d 4f ae 08 00 45 00! pMD...E.
0010 01 52 13 ac 00 00 00 11 25 ff 00 00 00 00 ff ff .R.....%.
0020 ff ff 00 44 00 43 01 3e 5b 68 01 01 06 00 6a 3f ...D.C.> [h...j?]
0030 4b 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 K.....
0040 00 00 00 00 00 00 00 21 70 4d 4f ae 00 00 00 00! pMD....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00! pMD....



Wireshark Interface

command menus {

display filter specification {

listing of captured packets {

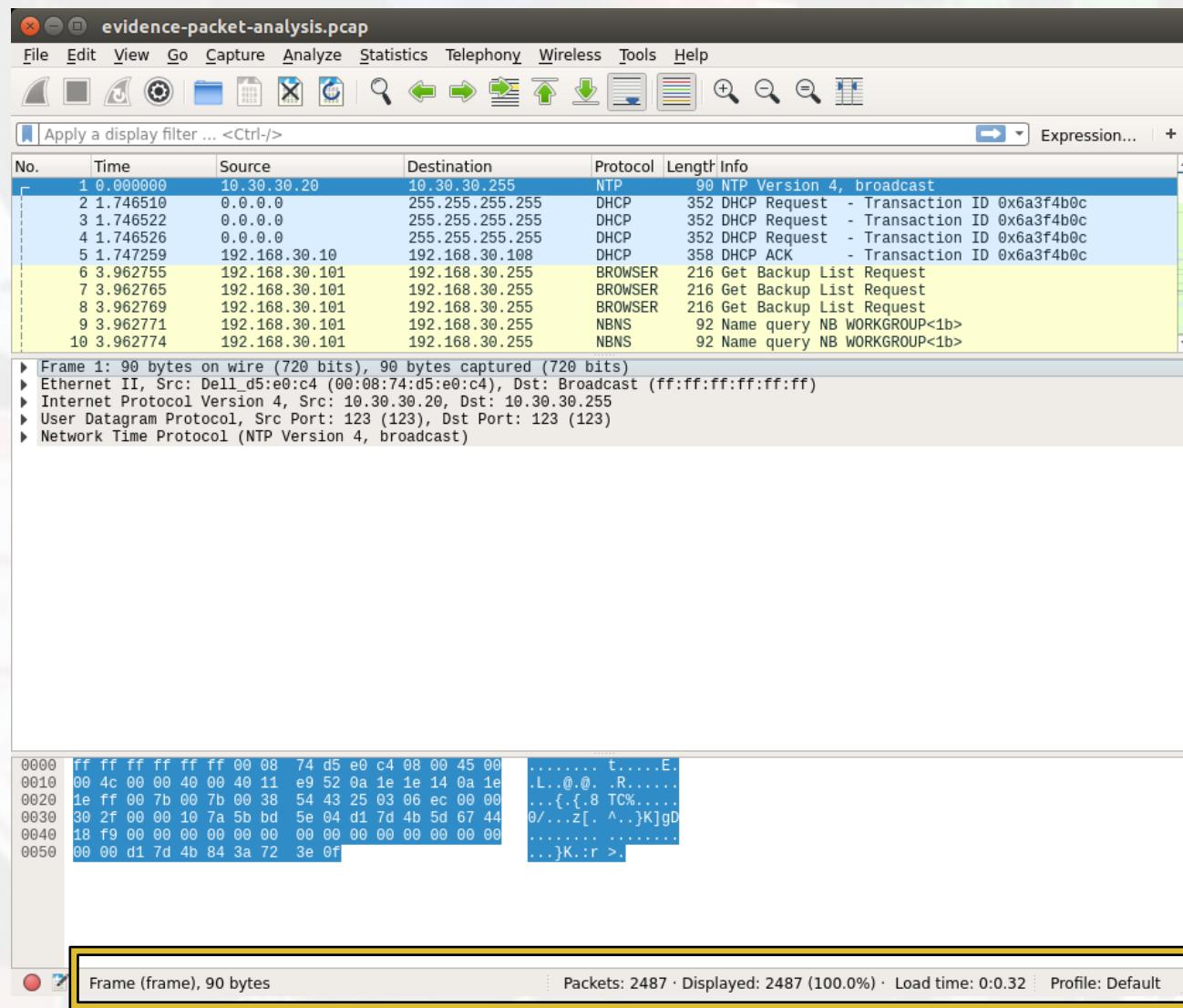
details of selected packet header {

packet content in hexadecimal and ASCII {

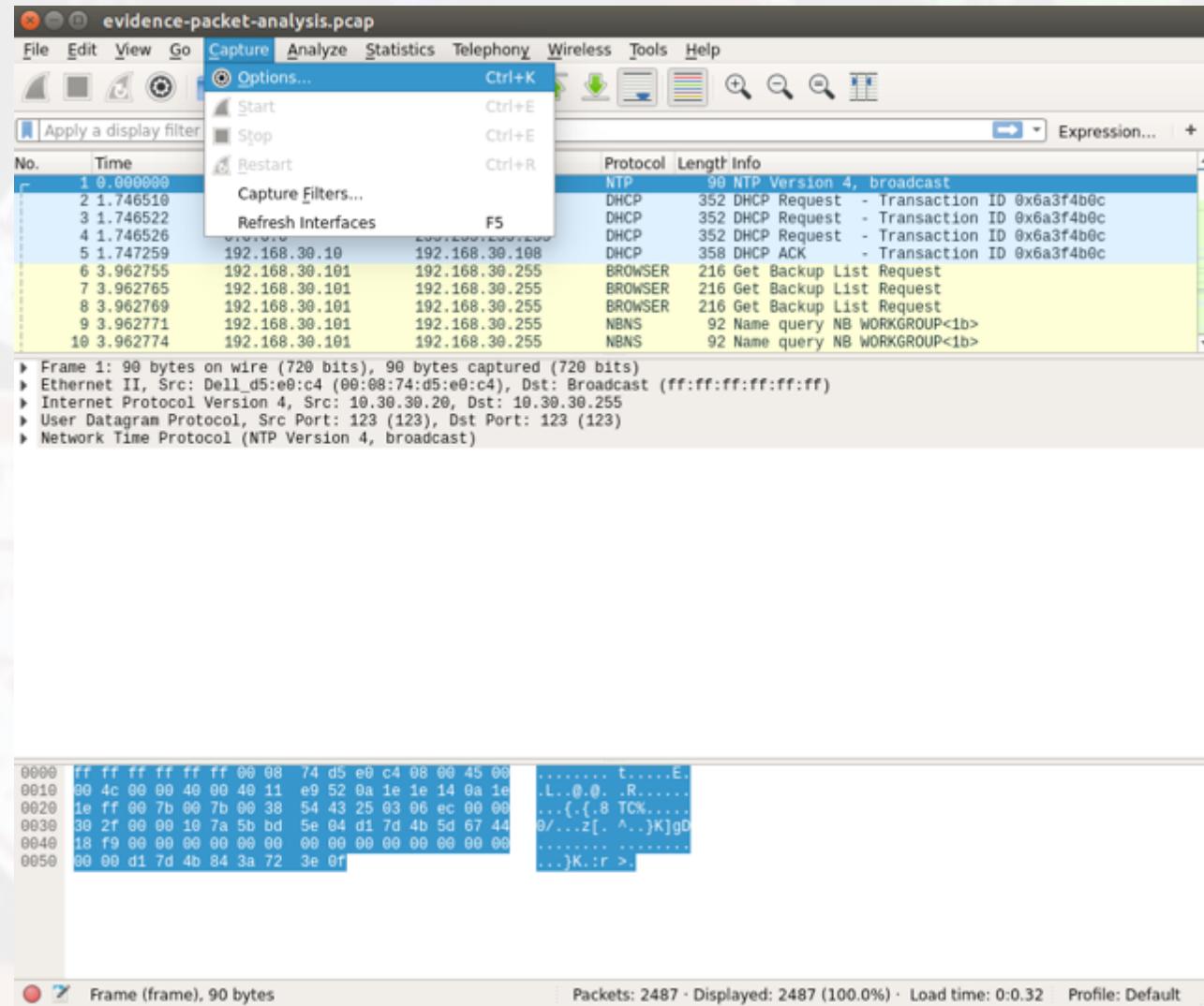
The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard file operations (Open, Save, Print, Copy, Paste, Find, Replace, etc.) and search functions.
- Display Filter:** "evidence-packet-analysis.pcap".
- Panels:**
 - Packet List:** Shows 10 captured packets. The first packet is highlighted in blue. The details pane shows it's an NTP Version 4 broadcast. The bytes and ASCII panes show the raw hex and ASCII data for this packet.
 - Details:** Shows the detailed structure of the selected NTP packet.
 - Bytes:** Shows the raw hex and ASCII representation of the selected packet.
 - ASCII:** Shows the ASCII representation of the selected packet.
- Status Bar:** Frame (frame), 90 bytes; Packets: 2487 · Displayed: 2487 (100.0%) · Load time: 0:0.32 · Profile: Default.

Status Bar



Capture Options



Capture Filter

Wireshark · Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (I)	Buffer (MB)	Monitor Mode	Capture Filter
▶ eth0	---	Ethernet	enabled	default	2	n/a	
nflog	---	Linux netfilter log messages	enabled	default	2	n/a	
nfqueue	---	Raw IPv4	enabled	default	2	n/a	
any	---	Linux cooked	enabled	default	2	n/a	
▶ Loopback: lo	---	Ethernet	enabled	default	2	n/a	

Enable promiscuous mode on all interfaces Manage Interfaces...

Capture filter for selected interfaces:  Enter a capture filter ... Compile BPFs

Start Close Help



Capture Filter examples

host 10.1.11.24

host securewv.com

host 192.168.0.1 and host 10.1.11.1

tcp port http

ip

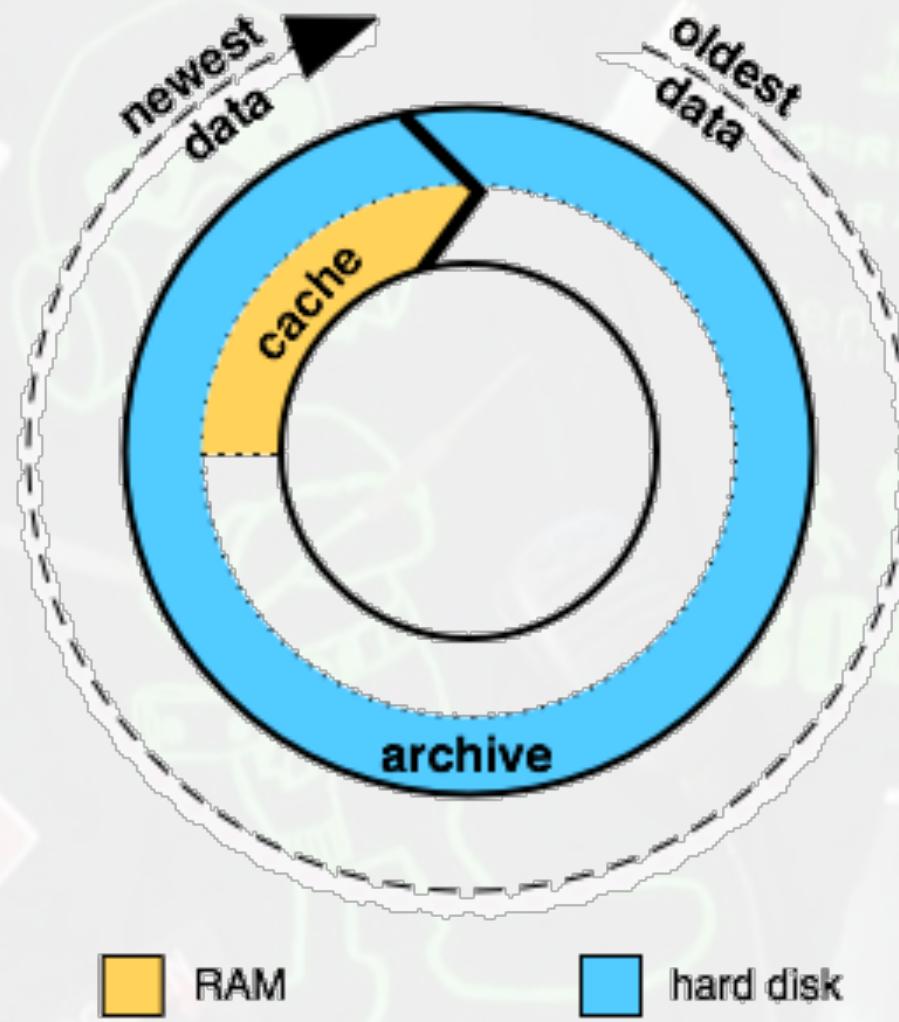
not broadcast not multicast

ether host 00:04:13:00:09:a3

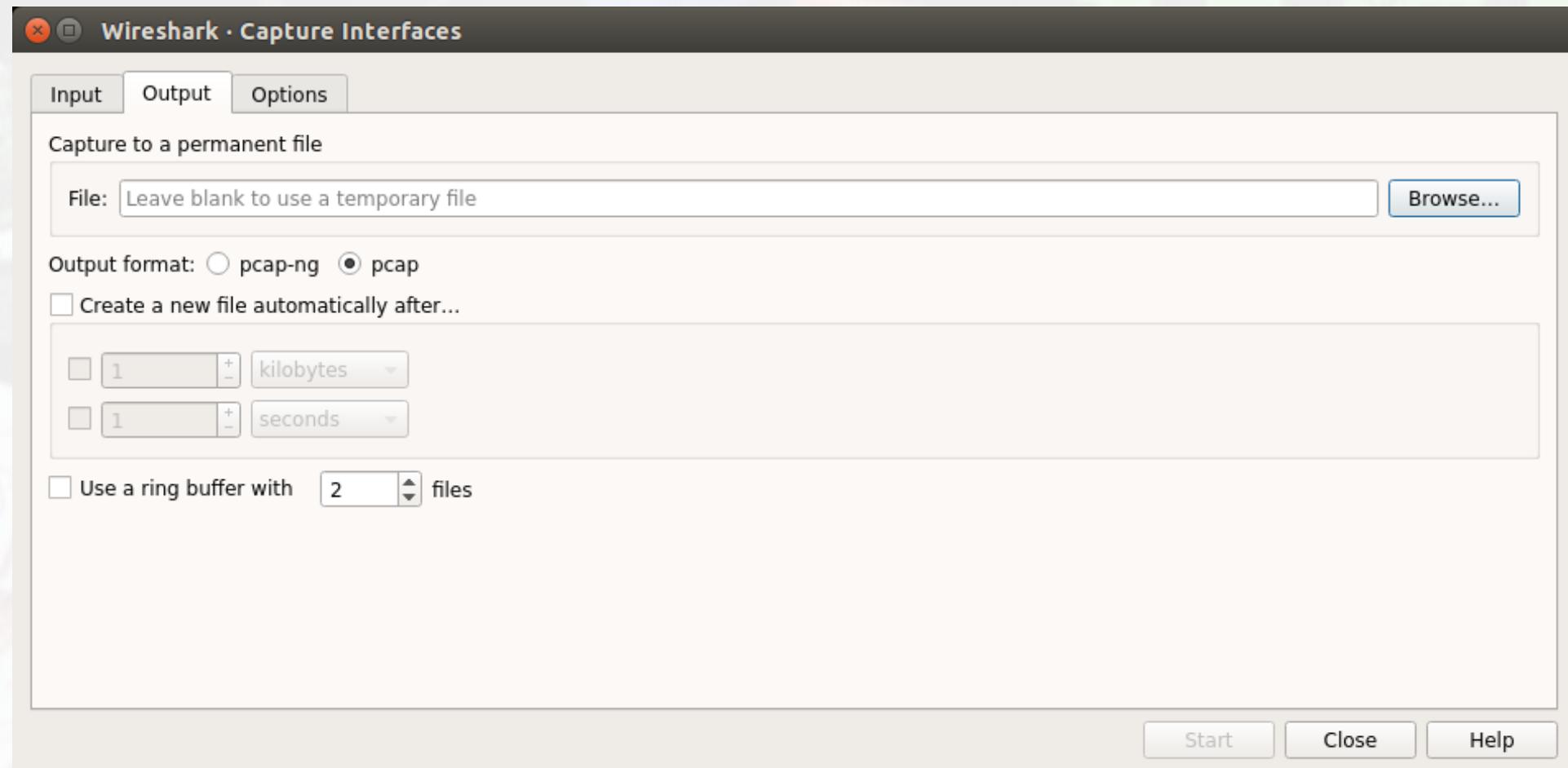
http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf



Capture Buffer



Capture Interfaces (Capture Buffer)



Capture Interfaces

Wireshark · Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (I)	Buffer (MB)	Monitor Mode	Capture Filter
▶ eth0	---	Ethernet	enabled	default	2	n/a	
nflog	---	Linux netfilter log messages	enabled	default	2	n/a	
nfqueue	---	Raw IPv4	enabled	default	2	n/a	
any	---	Linux cooked	enabled	default	2	n/a	
▶ Loopback: lo	---	Ethernet	enabled	default	2	n/a	

Enable promiscuous mode on all interfaces Manage Interfaces...

Capture filter for selected interfaces: Enter a capture filter ... Compile BPFs

Start Close Help



Display Filters (Post-Filters)

- ❑ Display filters (also called post or post-capture filters) only filter the view of what you are seeing. All packets in the capture still exist in the trace
- ❑ Display filters use their own format and are much more powerful than capture filters



Display Filter

evidence-packet-example.pcap

ip.addr==192.168.0.100

No.	Time	Source	Destination	Protocol	Leng	Info
92	2009-09-15 06:26:28.735644	96.7.38.49	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
93	2009-09-15 06:26:28.736797	96.7.38.49	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
94	2009-09-15 06:26:28.736816	192.168.0.100	96.7.38.49	TCP	54	55227 - 80 [ACK] Seq=425 Ack=5841 Win=17640 Len=0
95	2009-09-15 06:26:28.737503	96.7.38.49	192.168.0.100	HTTP	1210	HTTP/1.1 200 OK (JPEG JFIF image)
96	2009-09-15 06:26:28.745037	96.7.38.90	192.168.0.100	TCP	54	89 - 55231 [ACK] Seq=1 Ack=423 Win=6432 Len=0
97	2009-09-15 06:26:28.747806	8.18.91.89	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
98	2009-09-15 06:26:28.748850	8.18.91.89	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
99	2009-09-15 06:26:28.748884	192.168.0.100	8.18.91.89	TCP	54	55226 - 80 [ACK] Seq=425 Ack=2521 Win=17640 Len=0
100	2009-09-15 06:26:28.750095	8.18.91.89	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
101	2009-09-15 06:26:28.751094	8.18.91.89	192.168.0.100	TCP	572	[TCP segment of a reassembled PDU]
102	2009-09-15 06:26:28.751118	192.168.0.100	8.18.91.89	TCP	54	55226 - 80 [ACK] Seq=425 Ack=4299 Win=17640 Len=0
103	2009-09-15 06:26:28.751959	8.18.91.89	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
104	2009-09-15 06:26:28.753176	8.18.91.89	192.168.0.100	HTTP	750	HTTP/1.1 200 OK (JPEG JFIF image)
105	2009-09-15 06:26:28.753210	192.168.0.100	8.18.91.89	TCP	54	55226 - 80 [ACK] Seq=425 Ack=6255 Win=17640 Len=0
106	2009-09-15 06:26:28.754625	209.170.118.41	192.168.0.100	TCP	54	89 - 55233 [ACK] Seq=1 Ack=398 Win=6432 Len=0
107	2009-09-15 06:26:28.756793	209.170.118.41	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]
108	2009-09-15 06:26:28.757860	209.170.118.41	192.168.0.100	TCP	1314	[TCP segment of a reassembled PDU]

► Frame 89: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits)
► Ethernet II, Src: 00:1b:11:ee:75:be, Dst: 00:21:6a:27:ae:dc
► Internet Protocol Version 4, Src: 96.7.38.49, Dst: 192.168.0.100
► Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55227 (55227), Seq: 1, Ack: 425, Len: 1260

0000 00 21 6a 27 ae dc 00 1b 11 ee 75 be 08 00 45 00 .!j'.... ..u...E.
0010 05 14 0a 10 40 00 33 06 f1 8f 60 07 26 31 c0 ab ...@.3. ...&1..
0020 00 64 00 50 d7 bb e9 0c 6d a6 f8 e0 76 95 50 10 .d.P.... m...v.P.
0030 06 48 5e 87 00 00 48 54 54 50 2f 31 2e 31 20 32 .H^...HT TP/1.1 2
0040 38 38 29 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54 00 OK..C content-T
0050 79 70 65 3a 20 69 6d 61 67 65 2f 68 70 65 67 0d ype: ima ge/jpeg.
0060 0a 45 54 61 67 3a 20 22 32 32 39 32 37 39 33 31 .ETag: "22927931
0070 39 32 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 92".Acc ept-Rang
0080 65 73 3a 20 62 79 74 65 73 0d 0a 4c 61 73 74 2d es: byte s.,Last-
0090 4d 6f 64 69 66 69 65 64 3a 20 46 72 69 2c 20 30 Modified : Fri, 0
00a0 36 28 46 65 62 20 32 38 38 39 20 38 33 3a 34 32 6 Feb 20 09 03:42
00b0 3a 31 35 20 47 4d 54 0d 0a 43 6f 68 74 65 6e 74 :15 GMT..Content
00c0 2d 4c 65 6e 67 74 68 3a 28 35 38 38 33 0d 0a 53 -Length: 5883..S
00d0 65 72 76 65 72 3a 20 6c 69 67 68 74 74 70 64 2f erver: 1 ighttpd/
00e0 31 2e 35 2e 30 0d 0a 43 61 63 68 65 2d 43 6f 6e 1.5.0..C acha-Con

evidence-packet-example

Packets: 873 - Displayed: 841 (96.3%) - Load time: 0:0.18 - Profile: Default



Display Filter Examples

```
ip.src==10.1.11.00/24
```

```
ip.dst==10.1.11.00/24
```

```
ip.addr==192.168.1.10 && ip.addr==192.168.1.20
```

```
tcp.port==80 || tcp.port==3389
```

```
!(ip.addr==192.168.1.10 && ip.addr==192.168.1.20)
```

```
(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) &&  
(tcp.port==445 || tcp.port==139)
```

```
(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) &&  
(udp.port==67 || udp.port==68)
```

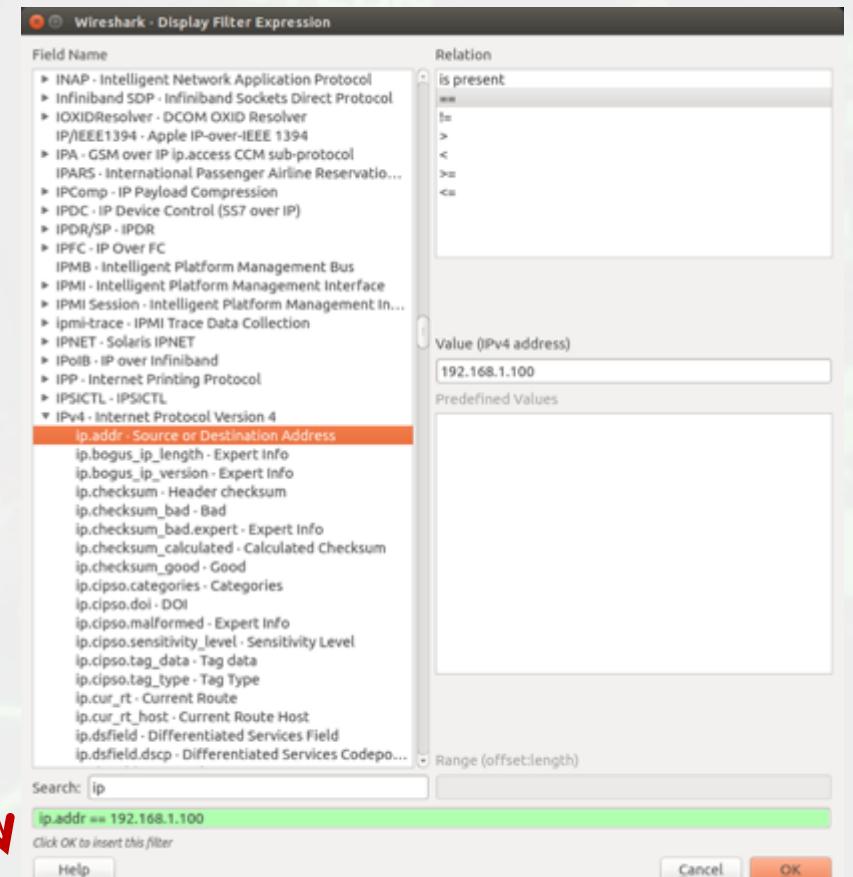
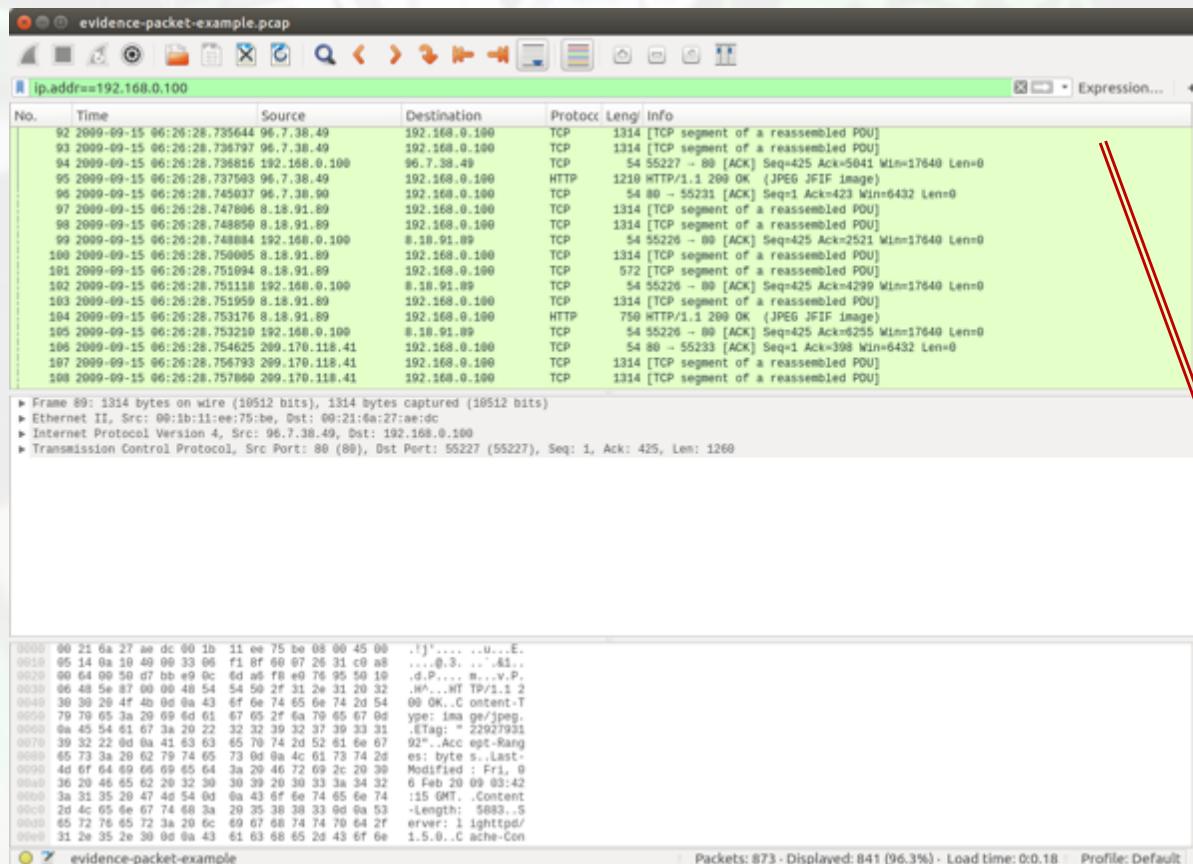
```
tcp.dstport == 80
```

Frame contains search term you are researching for e.g. bruntly



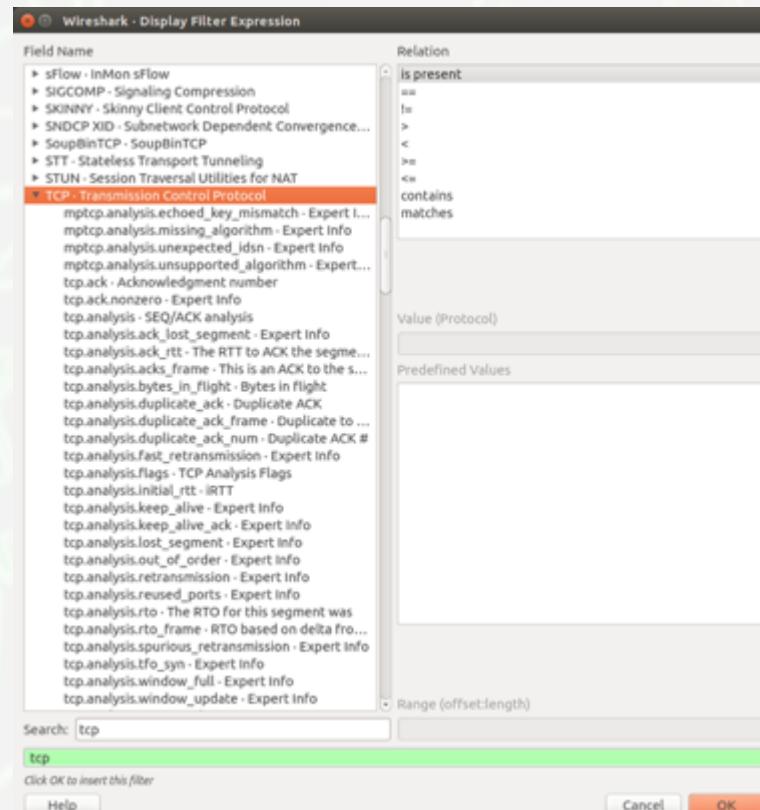
Display Filter

Syntax:	Protocol	String 1	String 2	Comparison operator	Value	Logical Operations	Other expression
Example:	ftp	passive	ip	= =	10.2.3.4	xor	icmp.type



Display Filter

- String1, String2 (Optional settings):
 - Sub protocol categories inside the protocol.
 - Look for a protocol and then click on the "+" character.
- Example:
 - **tcp.srcport == 80**
 - **tcp.flags == 2**
 - SYN packet
 - **Tcp.flags.syn==1**
 - **tcp.flags == 18**
 - SYN/ACK



Display Filter Expressions

- ❑ **snmp || dns || icmp**
 - ❑ Display the SNMP or DNS or ICMP traffics.
- ❑ **tcp.port == 80**
 - ❑ Display packets with TCP source or destination port 80.
- ❑ **tcp.flags**
 - ❑ Display packets having a TCP flags
- ❑ **tcp.flags.syn == 0x02**
 - ❑ Display packets with a TCP SYN flag.

If the filter syntax is correct, it will be highlighted in green, otherwise if there is a syntax mistake it will be highlighted in red.

Filter: `tcp.port == 100`

Filter: `tcp.port = 100`

Six comparison operators are available:

English format:	C like format:	Meaning:
eq	==	Equal
ne	!=	Not equal
gt	>	Greater than
lt	<	Less than
ge	>=	Greater or equal
le	<=	Less or equal

→ Logical expressions:

English format:	C like format:	Meaning:
and	&&	Logical AND
or		Logical OR
xor	^^	Logical XOR
not	!	Logical NOT

Correct syntax

Wrong syntax

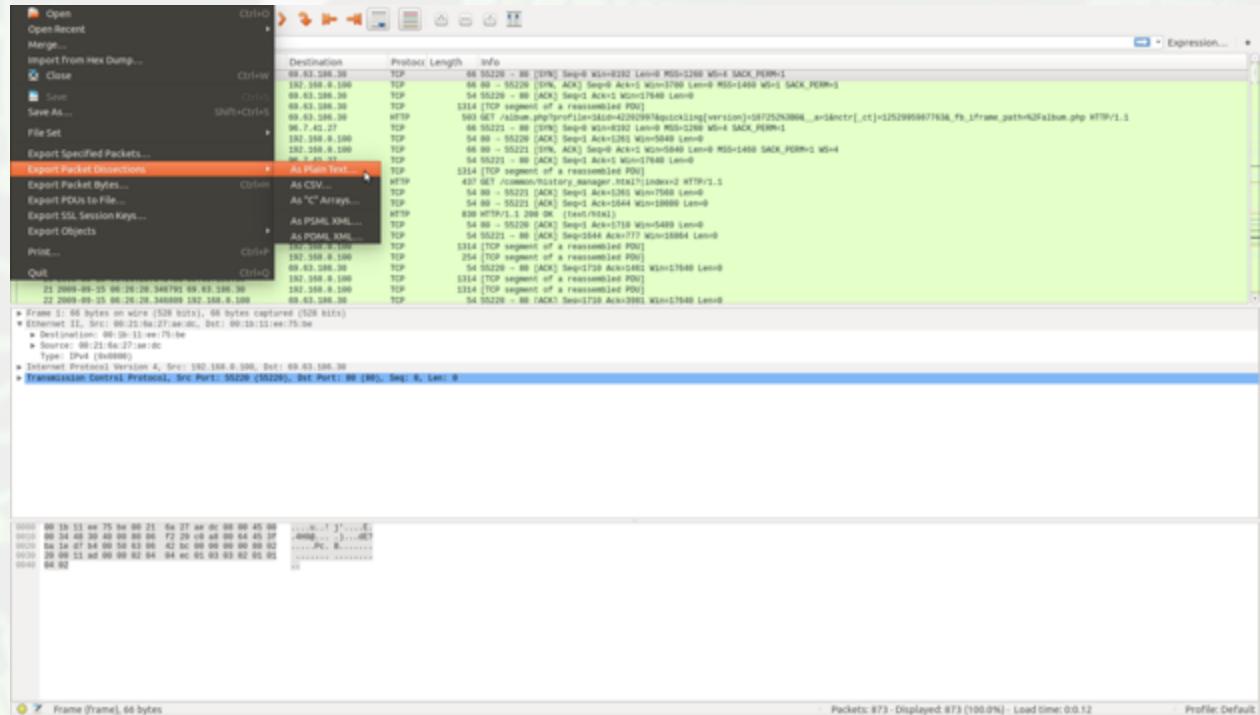
Save Filtered Packets After Using Display Filter

- We can also save all filtered packets in text file for further analysis
- Operation:

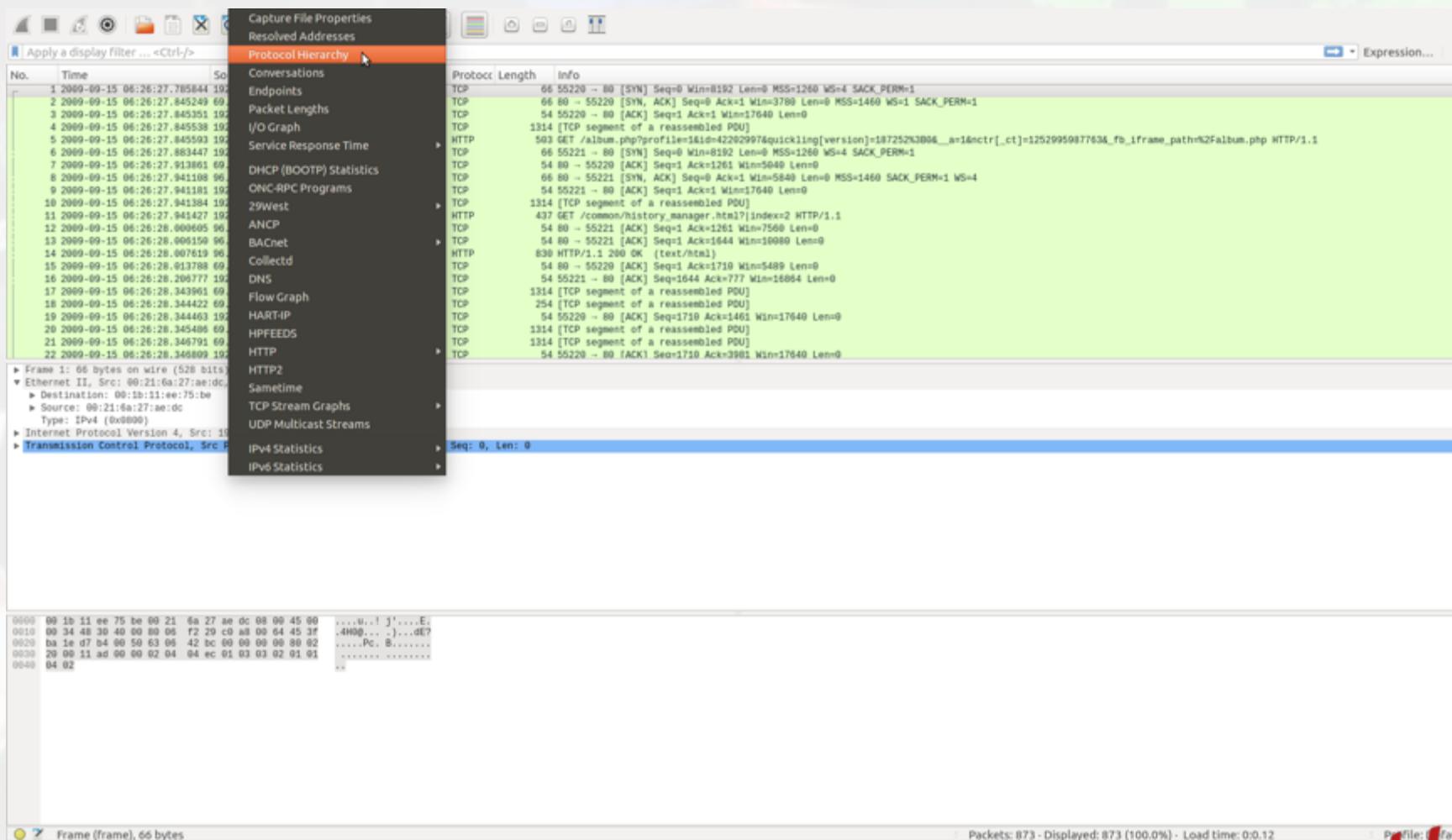
File→Export packet dissections
→as “plain text” file

1). In “packet range” option, select “Displayed”

2). In choose “summary line” or “detail”



Protocol Hierarchy



Protocol Hierarchy

Wireshark - Protocol Hierarchy Statistics - evidence-packet-example

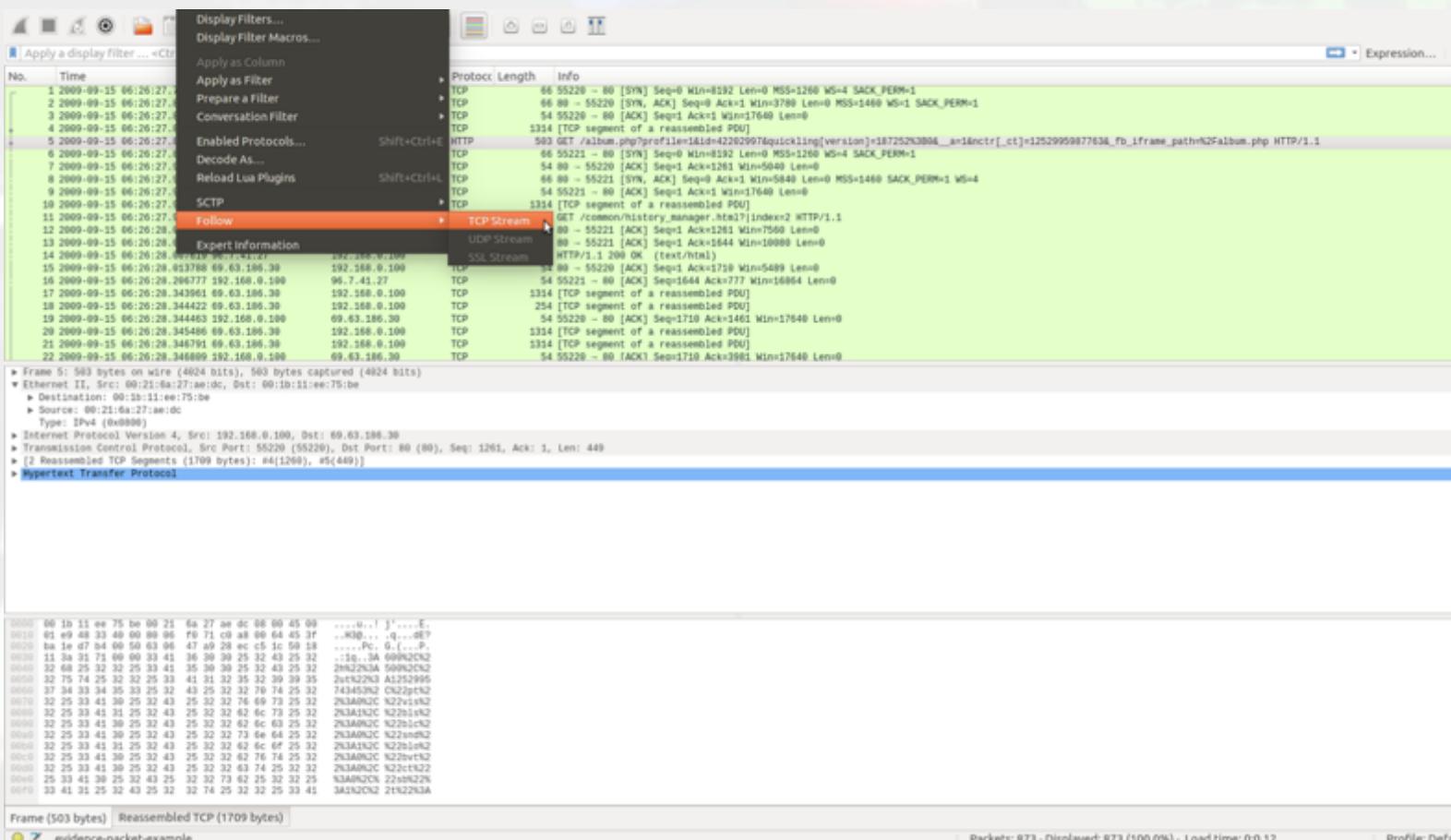
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	873	100.0	503167	96 k	0	0	0
Ethernet	100.0	873	100.0	503167	96 k	0	0	0
Internet Protocol Version 4	98.7	862	99.9	502687	96 k	0	0	0
User Datagram Protocol	6.5	57	3.1	15530	2976	0	0	0
Simple Network Management Protocol	0.5	4	0.1	486	93	4	486	93
Hypertext Transfer Protocol	2.4	21	1.4	6961	1334	21	6961	1334
Domain Name System	3.7	32	1.6	8083	1549	32	8083	1549
Transmission Control Protocol	92.2	805	96.8	487157	93 k	707	428552	82 k
Hypertext Transfer Protocol	11.2	98	11.6	58605	11 k	51	24982	4788
Media Type	0.1	1	0.1	392	75	1	392	75
Line-based text data	2.6	23	3.3	16515	3165	23	16515	3165
JPEG File Interchange Format	2.2	19	2.6	13103	2511	19	13103	2511
Compuserve GIF	0.5	4	0.7	3613	692	4	3613	692
Address Resolution Protocol	1.3	11	0.1	480	92	11	480	92

No display filter.

Help Copy Close



Follow TCP Stream



Follow TCP Stream

red - stuff you sent blue - stuff you get

Wireshark · Follow TCP Stream (tcp.stream eq 0) · evidence-packet-example

```
GET /album.php?profile=1&id=42202997&quickling[version]=187252%3B0&__a=1&nctr[_ct]=1252995987763&_fb_iframe_path=%2Falbum.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/vnd.ms-xpsdocument, application/xml+xml,
application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, /*
Referer: http://www.facebook.com/home.php?
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; InfoPath.2;
.NET CLR 3.5.30729; .NET CLR 3.0.30618)
Accept-Encoding: gzip, deflate
Host: www.facebook.com
Connection: Keep-Alive
Cookie: datr=1252995732-edbc452bccd93a8be5ec16b67ad7704c2d7a525061cc971020a4f; lsd=Au26-;
ABT=2dd086ca2a46e9e50fff44e0ec48cb811st0%3A1253600533%3AB; lxe=brunty11%40marshall.edu; xs=0571f052cf5e4611891c35a695f4d4f5;
c_user=42202997; h_user=dd89ae8ab715; x-referer=http%3A%2F%2Fwww.facebook.com%2Fjosh.brunty%3Fref%3Dprofile; presence=%7B%22%22%3A%2C%
22%22time%22%3A1252995746%2C%22ch%22%3A%7B%22%22%3A%22channel119%22%2C%22p%22%3A80%2C%22sub%22%3A%5B1%5D%2C%22p_42202997%22%3A0%2C%22ri
%22%3A0%7D%2C%22state%22%3A%7B%22p%22%3A0%2C%22w%22%3A600%2C%22%3A500%2C%22ut%22%3A1252995743453%2C%22pt%22%3A0%2C%22v1s%22%3A1%2C
%22bls%22%3A0%2C%22b1c%22%3A0%2C%22sn%22%3A1%2C%22b1o%22%3A0%2C%22bvt%22%3A0%2C%22ct%22%3A0%2C%22sb%22%3A1%2C%22t%22%3A%7B%2D%2C%22f
%22%3Anull%22%22uct%22%3A0%2C%22s%22%3A0%7D%2C%22b1%22%3A%7B%22ac%22%3A3%2C%22a1%22%3A%7B%2D%2C%22ut%22%3A1252995743%2C%22ud%22%3A400%2C
%221c%22%3A1%2C%22uo%22%3A%7B%2D%2C%22cvr%22%3A%7B%22r%22%3A1%2C%22ts%22%3A1252995743%7D%27%7D%77
```

HTTP/1.1 200 OK
Date: Tue, 15 Sep 2009 06:26:29 GMT
Server: Apache/1.3.41.fb2
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip

a
.....
12ed
.\(W.....B7w..v....B0..)o..@.>-'N.....z..)Gr..@ {.{0...m..G..h4..H..I...`..p.C1En.l..+..?Y...v.....-b.Aw.
z..w.\.-.8.E*....mJ.d.)....H..~L.:Z"Q.D.Un).....Ri.d.d..._xZ..8].UZu....R..^....R..P..\$.j,...".2.....a.8.G.....
'...
U'n.. .3j...]i.N.A..h..d..JRh.|c..~.m....E. HHdXA8..V....>!.,..4K...>4..5....v..(q{.Y..!q.|...\.I.<.....KK..\$.vA..%.i.N..@
+....M
...ka*w#&I.....q.p}3.....}..q.V.;..J....1. R?1..g....'C...C..W..d
^X..cx.....(.....~....sR.yEP..6.1....F..d....U.....P..Q;"....Md.....{.....= 1P....]x.....{....z.....
8..D0w.S..g.A.?....M.(....H....6Mt`t. &sKoc+....=
v ..3V ..1nV ..1 ..11 ..6% ..1 ..R ..0 ..f6S ..1 ..7 ..+hntv ..8 ..S2c ..i#Br\ ..c ..17V ..v ..m ..% ..v ..1

2 client pkt(s), 5 server pkt(s), 1 turn.

Entire conversation (6939 bytes) Show data as ASCII Stream 0

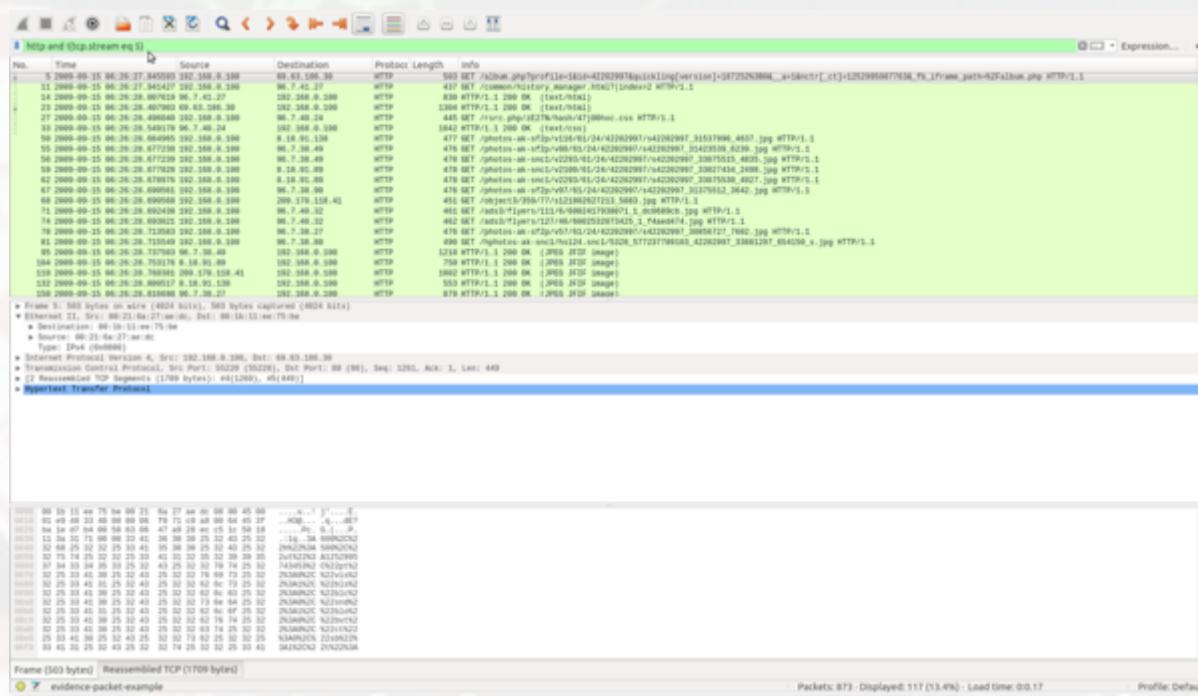
Find: Find Next

Help Hide this stream Print Save as... Close



Filter out/in Single TCP Stream

- When click “filter out this TCP stream” in previous page’s box, new filter string will contain like:
 - http and !(tcp.stream eq 5)
 - So, if you use “tcp.stream eq 5” as filter string, you keep this HTTP session



Expert Info

http and !tcp.stream eq 5

Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols...
Decode As...
Shift+Ctrl+E
Reload Lua Plugins
Shift+Ctrl+L
SCTP
Follow
Shift+Ctrl+F
Expert Information

No. Time Protocol Length Info

5 2009-09-15 06:26:27.1 HTTP 503 GET /album.php?profile=1&id=4202997&quickling[version]=1&7252%3804_a=1&nctr[_ct]=1252995987763&_fb_iframe_path=%2Falbum.php HTTP/1.1
11 2009-09-15 06:26:27.1 HTTP 437 GET /common/history_manager.htm?index=2 HTTP/1.1
14 2009-09-15 06:26:28.0 HTTP 839 HTTP/1.1 200 OK [text/html]
23 2009-09-15 06:26:28.0 HTTP 1304 HTTP/1.1 200 OK [text/html]
27 2009-09-15 06:26:28.0 HTTP 445 GET /src.php/zE27W/hash/4f790mxc.css HTTP/1.1
33 2009-09-15 06:26:28.0 HTTP 1642 HTTP/1.1 200 OK [text/css]
50 2009-09-15 06:26:28.0 HTTP 477 GET /photos-ak-s72p/v16/61/24/42202997/s42202997_31537990_4637.jpg HTTP/1.1
55 2009-09-15 06:26:28.0 HTTP 476 GET /photos-ak-s72p/v80/61/24/42202997/s42202997_31423539_6239.jpg HTTP/1.1
56 2009-09-15 06:26:28.0 HTTP 478 GET /photos-ak-smc1/v229/61/24/42202997/s42202997_33075515_4835.jpg HTTP/1.1
59 2009-09-15 06:26:28.0 HTTP 478 GET /photos-ak-smc1/v210/61/24/42202997/s42202997_33027434_2498.jpg HTTP/1.1
62 2009-09-15 06:26:28.0 HTTP 478 GET /photos-ak-smc1/v229/61/24/42202997/s42202997_33075530_4927.jpg HTTP/1.1
67 2009-09-15 06:26:28.0 HTTP 476 GET /photos-ak-s72p/v87/61/24/42202997/s42202997_31375512_3642.jpg HTTP/1.1
68 2009-09-15 06:26:28.0 HTTP 451 GET /object1/359/77/s121802627211_5881.jpg HTTP/1.1
71 2009-09-15 06:26:28.0 HTTP 461 GET /ads/7/flyers/111/6/0002417938007/1_dc9680cbs.jpg HTTP/1.1
74 2009-09-15 06:26:28.0 HTTP 462 GET /ads/7/flyers/127/46/0002532073425_1_f4acd474.jpg HTTP/1.1
78 2009-09-15 06:26:28.0 HTTP 476 GET /photos-ak-s72p/v87/61/24/42202997/s42202997_30856727_7602.jpg HTTP/1.1
81 2009-09-15 06:26:28.0 HTTP 499 GET /photos-ak-smc1/hn124/sm1/5328_577237789103_42202997_33881297_054150_s.jpg HTTP/1.1
95 2009-09-15 06:26:28.0 HTTP 1210 HTTP/1.1 200 OK [JPG] JPEG image
104 2009-09-15 06:26:28.0 HTTP 759 HTTP/1.1 200 OK [JPG] JPEG image
110 2009-09-15 06:26:28.0 HTTP 1002 HTTP/1.1 200 OK [JPG] JPEG image
112 2009-09-15 06:26:28.0 HTTP 553 HTTP/1.1 200 OK [JPG] JPEG image
132 2009-09-15 06:26:28.0 HTTP 879 HTTP/1.1 200 OK [JPG] JPEG image
150 2009-09-15 06:26:28.0 HTTP 879 HTTP/1.1 200 OK [JPG] JPEG image

* Frame 5: 563 bytes on wire (4024 bits), 563 bytes captured (4024 bits)
* Ethernet II, Src: 00:21:6a:27:ae:dc, Dst: 00:1b:11:ee:75:be
* Destination: 00:1b:11:ee:75:be
* Source: 00:21:6a:27:ae:dc
* Type: IPv4 (0x0800)
* Internet Protocol Version 4, Src: 192.168.0.100, Dst: 69.63.186.0
* Transmission Control Protocol, Src Port: 55220 (55220), Dst Port: 80 (80), Seq: 1261, Ack: 1, Len: 440
* [2] Reassembled TCP Segments (1709 bytes): #4(1260), #5(449)
* Hypertext Transfer Protocol

Frame (503 bytes) | Reassembled TCP (1709 bytes)

0000 00 10 11 ee 75 be 00 25 6a 27 ae dc 08 00 45 00U..! J!....E.
0001 01 e9 48 33 46 00 00 00 00 70 71 c0 a8 00 64 45 3fR0... .Q...@E?
0002 b4 1e d7 b4 00 50 63 06 47 a9 28 ec c5 1c 50 18Pc. G.[...P.
0003 11 3a 31 73 00 00 33 41 36 30 39 25 32 43 25 32 ..1g..3A 69992C62
0004 32 68 25 32 32 25 33 40 25 30 39 25 32 43 25 32 2a732234A 69992C62
0005 32 25 33 41 31 25 32 43 30 32 39 25 32 43 25 32 2a732234A 69992C62
0006 37 34 33 34 35 25 32 43 35 32 33 70 74 25 32 74345932 C23pF63
0007 32 25 33 41 36 25 32 43 25 32 32 76 69 73 25 32 2934692C N22v1sZ2
0008 32 25 33 41 31 25 32 43 25 32 32 62 66 73 25 32 2934192C N22b1sZ2
0009 32 25 33 41 30 25 32 43 25 32 32 62 66 73 25 32 2934692C N22b1sZ2
000A 32 25 33 41 31 25 32 43 25 32 32 73 68 64 25 32 2934692C N22b1sZ2
000B 32 25 33 41 31 25 32 43 25 32 32 62 66 64 25 32 2934192C N22b1sZ2
000C 32 25 33 41 30 25 32 43 25 32 32 62 76 74 25 32 2934692C N22b1sZ2
000D 32 25 33 41 31 25 32 43 25 32 32 62 76 74 25 32 2934692C N22b1sZ2
000E 25 33 41 30 25 32 43 25 32 32 73 68 25 32 32 2934692C N22b1sZ2
000F 33 41 31 25 32 43 25 32 32 74 25 32 32 2934692C N22b1sZ2

Frame (503 bytes) | Reassembled TCP (1709 bytes)

0000 00 10 11 ee 75 be 00 25 6a 27 ae dc 08 00 45 00U..! J!....E.
0001 01 e9 48 33 46 00 00 00 00 70 71 c0 a8 00 64 45 3fR0... .Q...@E?
0002 b4 1e d7 b4 00 50 63 06 47 a9 28 ec c5 1c 50 18Pc. G.[...P.
0003 11 3a 31 73 00 00 33 41 36 30 39 25 32 43 25 32 ..1g..3A 69992C62
0004 32 68 25 32 32 25 33 40 25 30 39 25 32 43 25 32 2a732234A 69992C62
0005 32 25 33 41 31 25 32 43 30 32 39 25 32 43 25 32 2a732234A 69992C62
0006 37 34 33 34 35 25 32 43 35 32 33 70 74 25 32 74345932 C23pF63
0007 32 25 33 41 36 25 32 43 25 32 32 76 69 73 25 32 2934692C N22v1sZ2
0008 32 25 33 41 31 25 32 43 25 32 32 62 66 73 25 32 2934192C N22b1sZ2
0009 32 25 33 41 30 25 32 43 25 32 32 62 66 73 25 32 2934692C N22b1sZ2
000A 32 25 33 41 31 25 32 43 25 32 32 73 68 64 25 32 2934692C N22b1sZ2
000B 32 25 33 41 31 25 32 43 25 32 32 62 76 74 25 32 2934692C N22b1sZ2
000C 32 25 33 41 30 25 32 43 25 32 32 62 76 74 25 32 2934692C N22b1sZ2
000D 32 25 33 41 31 25 32 43 25 32 32 73 68 25 32 32 2934692C N22b1sZ2
000E 33 41 31 25 32 43 25 32 32 74 25 32 32 2934692C N22b1sZ2

Packets: 873 - Displayed: 117 (13.4%) - Load time: 0:0.17

Profile: Default



Expert Info

Wireshark - Expert Information - evidence-packet-example

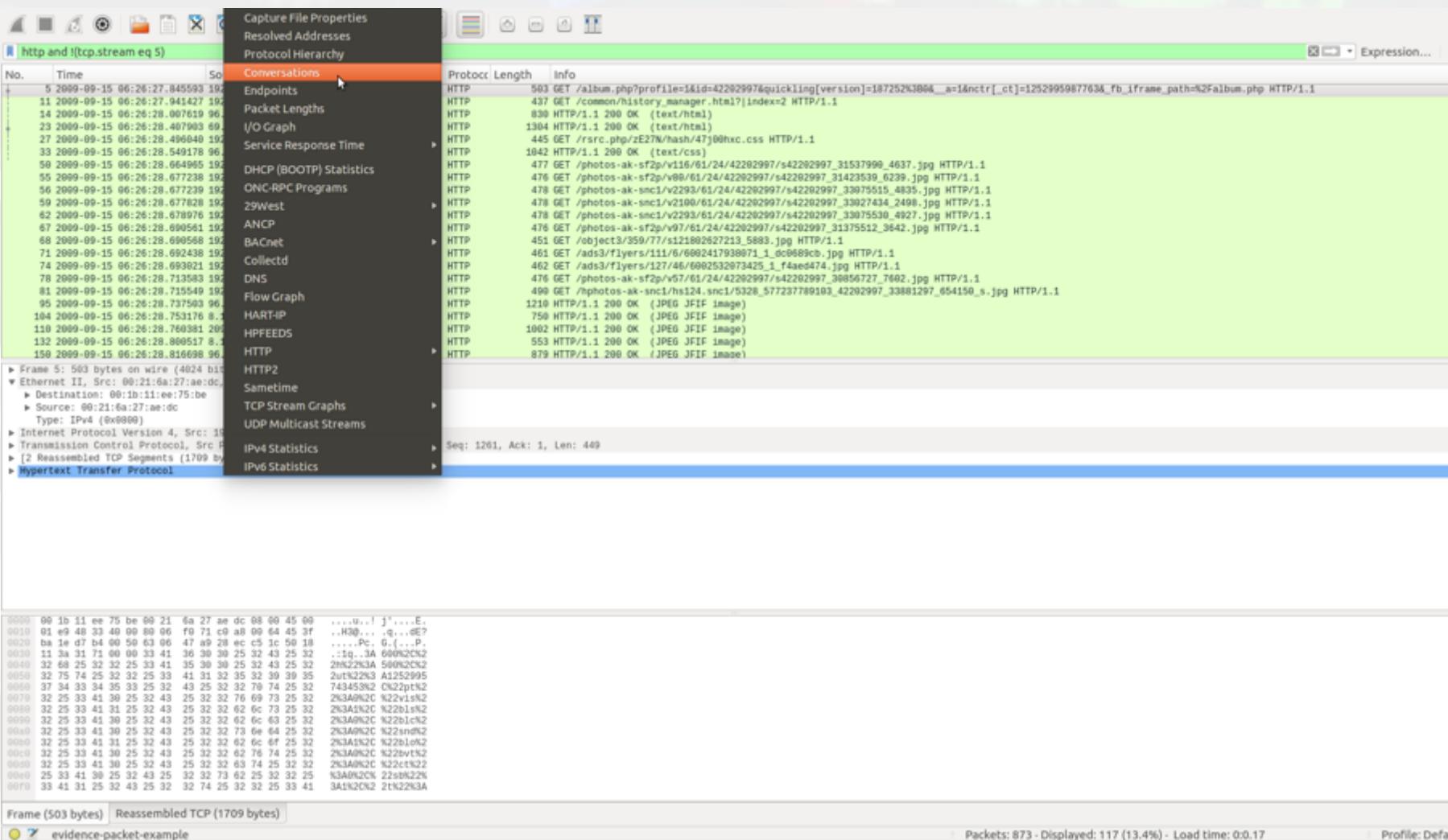
Severity	Group	Protocol	Count
	Sequence	TCP	7
Warn			
392: Previous segment not captured (common at capt...			
394: This frame is a (suspected) out-of-order segment			
453: Connection reset (RST)			
569: Connection reset (RST)			
633: Previous segment not captured (common at capt...			
690: Connection reset (RST)			
864: Connection reset (RST)			
Note	Malformed	HTTP	4
266: HTTP body subdissector failed, trying heuristic s...			
301: HTTP body subdissector failed, trying heuristic s...			
302: HTTP body subdissector failed, trying heuristic s...			
333: HTTP body subdissector failed, trying heuristic s...			
Note	Sequence	TCP	8
592: Duplicate ACK (#1)			
612: Duplicate ACK (#2)			
634: Duplicate ACK (#1)			
657: Duplicate ACK (#2)			
659: Duplicate ACK (#3)			
661: Duplicate ACK (#4)			
663: Duplicate ACK (#5)			
681: This frame is a (suspected) retransmission			
Chat	Sequence	TCP	88
Chat	Sequence	HTTP	119

Display Filter: "http and !(tcp.stream eq 5)"

Limit to Display Filter Search: Show... ▾



Conversations



Conversations

Wireshark · Conversations · evidence-packet-example

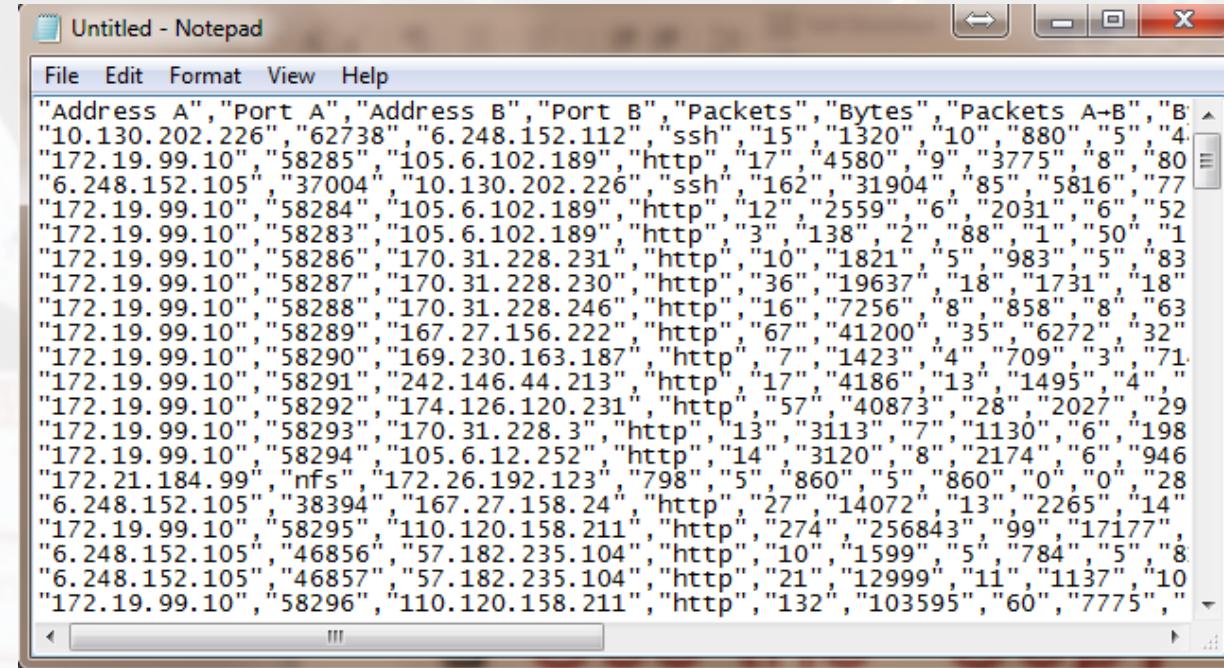
Ethernet · 4	IPv4 · 27	IPv6	TCP · 40	UDP · 18						
Address A	Address B		Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel S	
8.18.91.89	192.168.0.100		25	12 k	14	11 k	11	1466	0.84	
8.18.91.112	192.168.0.100		13	6735	7	5952	6	783	9.94	
8.18.91.120	192.168.0.100		91	69 k	58	67 k	33	2704	21.78	
8.18.91.138	192.168.0.100		14	7447	8	6688	6	759	0.84	
64.236.115.52	192.168.0.100		17	5490	7	3731	10	1759	10.45	
65.55.15.241	192.168.0.100		9	3462	4	2752	5	710	9.55	
65.203.229.40	192.168.0.100		11	1716	5	625	6	1091	9.88	
69.63.176.179	192.168.0.100		53	13 k	24	2996	29	10 k	10.50	
69.63.186.12	192.168.0.100		99	64 k	59	55 k	40	9652	8.20	
69.63.186.30	192.168.0.100		15	7773	8	5674	7	2099	0.00	
96.7.38.27	192.168.0.100		11	5645	6	4941	5	704	0.84	
96.7.38.49	192.168.0.100		51	29 k	29	26 k	22	2519	0.84	
96.7.38.51	192.168.0.100		82	64 k	53	61 k	29	2500	9.00	
96.7.38.80	192.168.0.100		22	11 k	12	9956	10	1436	0.84	
96.7.38.90	192.168.0.100		14	5914	8	5156	6	758	0.84	
96.7.40.18	192.168.0.100		11	5679	6	4982	5	697	10.14	
96.7.40.19	192.168.0.100		39	23 k	21	21 k	18	1920	20.38	
96.7.40.24	192.168.0.100		11	5777	6	5104	5	673	0.66	
96.7.40.32	192.168.0.100		34	21 k	20	20 k	14	1595	0.84	
96.7.41.9	192.168.0.100		81	66 k	52	63 k	29	3026	10.95	
96.7.41.10	192.168.0.100		14	4854	6	1332	8	3522	9.08	
96.7.41.27	192.168.0.100		62	36 k	32	30 k	30	6623	0.05	
192.168.0.1	192.168.0.100		32	8083	16	6786	16	1297	8.16	
192.168.0.1	239.255.255.250		21	6961	21	6961	0	0	9.40	
192.168.0.100	209.170.118.41		10	4429	5	679	5	3750	0.84	
192.168.0.100	192.221.110.126		16	7308	8	837	8	6471	9.30	
192.168.0.100	192.168.0.254		4	486	2	240	2	246	11.71	

Name resolution Limit to display filter

Conversation Types



- ❑ Use the “Copy” button to copy all text into clipboard



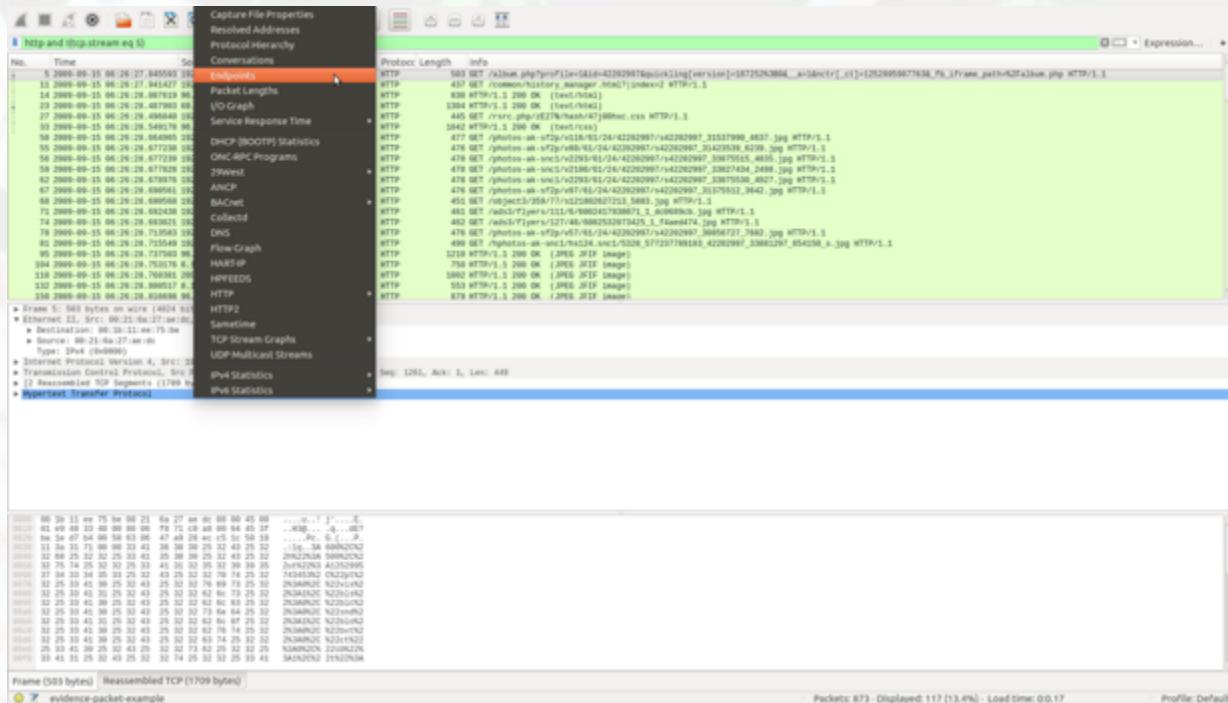
The screenshot shows a Windows Notepad window with the title "Untitled - Notepad". The menu bar includes File, Edit, Format, View, and Help. The main content area displays a large block of text representing network traffic statistics. The data is organized into columns separated by commas, listing various network parameters such as source and destination addresses, ports, and packet counts.

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B
"10.130.202.226"	"62738"	"6.248.152.112"	"ssh"	"15"	"1320"	"10"	"880"
"172.19.99.10"	"58285"	"105.6.102.189"	"http"	"17"	"4580"	"9"	"3775"
"6.248.152.105"	"37004"	"10.130.202.226"	"ssh"	"162"	"31904"	"85"	"5816"
"172.19.99.10"	"58284"	"105.6.102.189"	"http"	"12"	"2559"	"6"	"2031"
"172.19.99.10"	"58283"	"105.6.102.189"	"http"	"3"	"138"	"2"	"88"
"172.19.99.10"	"58286"	"170.31.228.231"	"http"	"10"	"1821"	"5"	"983"
"172.19.99.10"	"58287"	"170.31.228.230"	"http"	"36"	"19637"	"18"	"1731"
"172.19.99.10"	"58288"	"170.31.228.246"	"http"	"16"	"7256"	"8"	"858"
"172.19.99.10"	"58289"	"167.27.156.222"	"http"	"67"	"41200"	"35"	"6272"
"172.19.99.10"	"58290"	"169.230.163.187"	"http"	"7"	"1423"	"4"	"709"
"172.19.99.10"	"58291"	"242.146.44.213"	"http"	"17"	"4186"	"13"	"1495"
"172.19.99.10"	"58292"	"174.126.120.231"	"http"	"57"	"40873"	"28"	"2027"
"172.19.99.10"	"58293"	"170.31.228.3"	"http"	"13"	"3113"	"7"	"1130"
"172.19.99.10"	"58294"	"105.6.12.252"	"http"	"14"	"3120"	"8"	"2174"
"172.21.184.99"	"nfs"	"172.26.192.123"	"798"	"5"	"860"	"5"	"860"
"6.248.152.105"	"38394"	"167.27.158.24"	"http"	"27"	"14072"	"13"	"2265"
"172.19.99.10"	"58295"	"110.120.158.211"	"http"	"274"	"256843"	"99"	"17177"
"6.248.152.105"	"46856"	"57.182.235.104"	"http"	"10"	"1599"	"5"	"784"
"6.248.152.105"	"46857"	"57.182.235.104"	"http"	"21"	"12999"	"11"	"1137"
"172.19.99.10"	"58296"	"110.120.158.211"	"http"	"132"	"103595"	"60"	"7775"

- ❑ Then, you can analyze this text file to get what statistics you want (i.e. grep it)
- ❑ Or you can use a tool like “ngrep” to search against

Find EndPoint Statistics

- Menu “statistics” → “endpoints” → “TCP”



- You can sort by field
- “Tx” : transmit “Rx” : receive

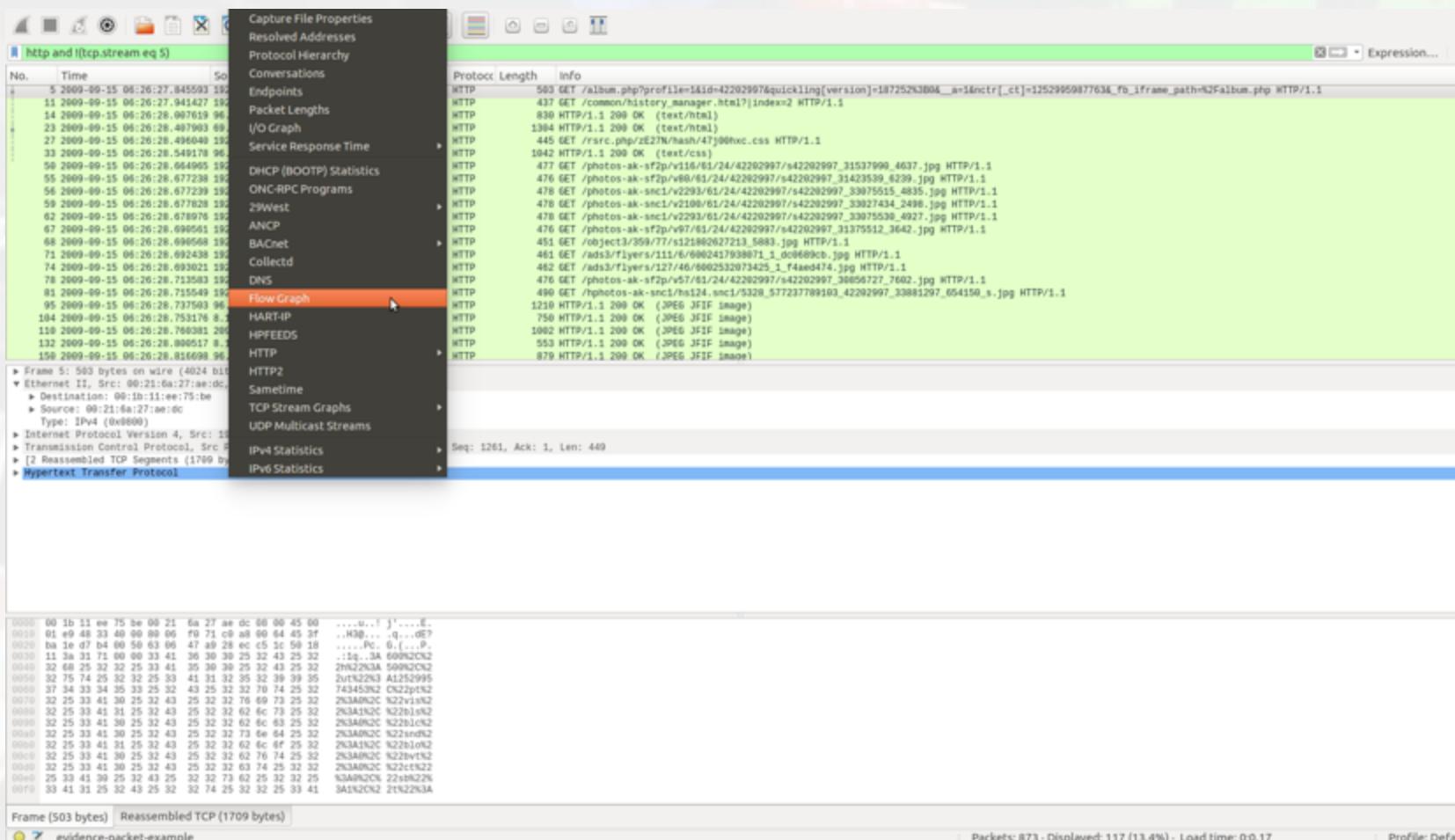


Find EndPoint Statistics

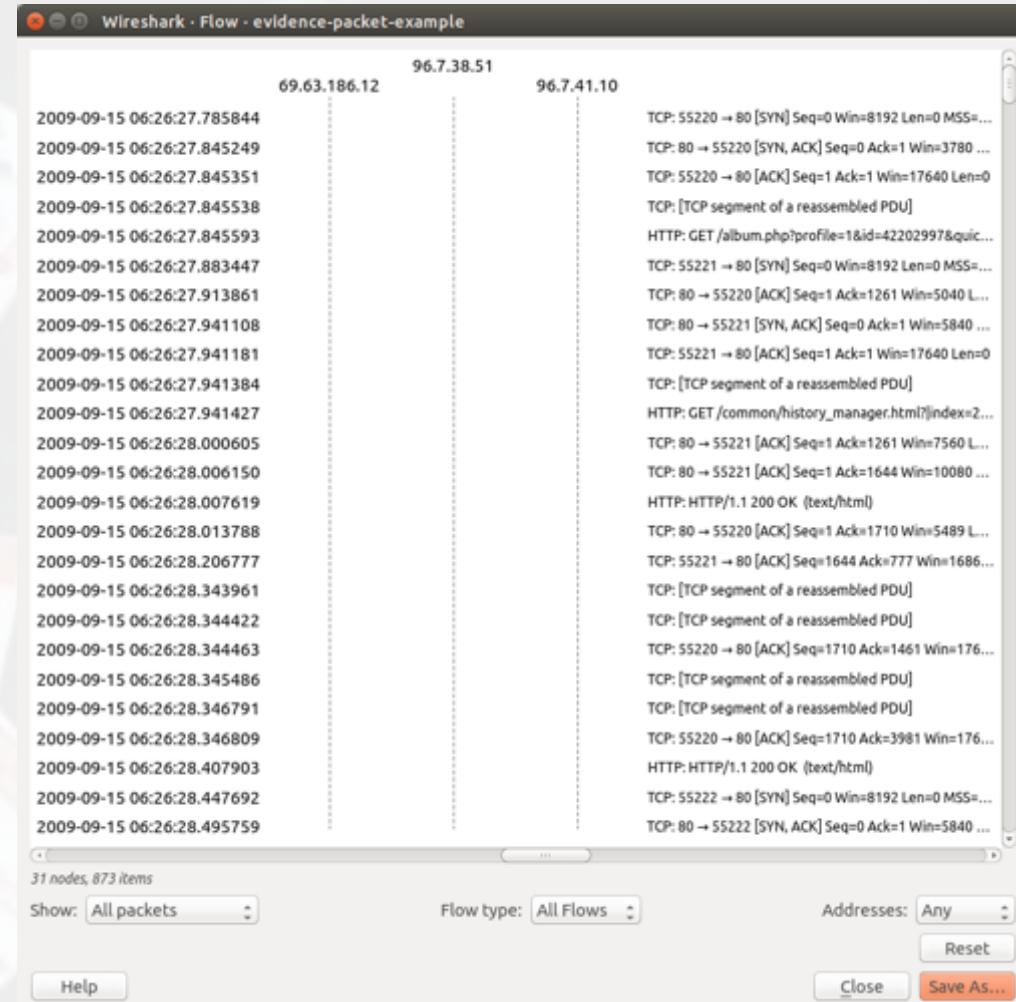
- ❑ Use the “Copy” button to copy all text into clipboard

- Then, you can analyze this text file to get what statistics you want

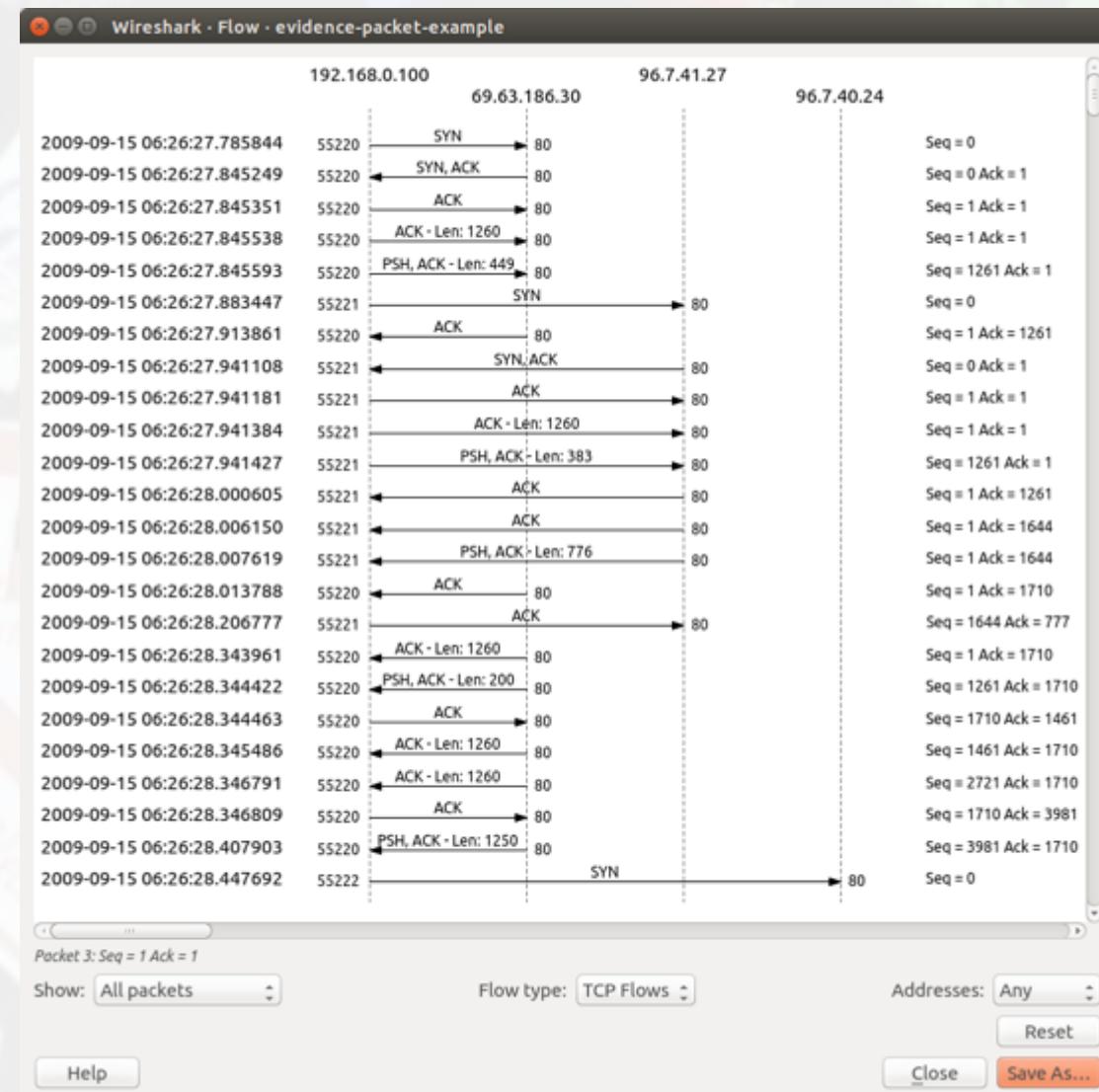
Flow Graphs



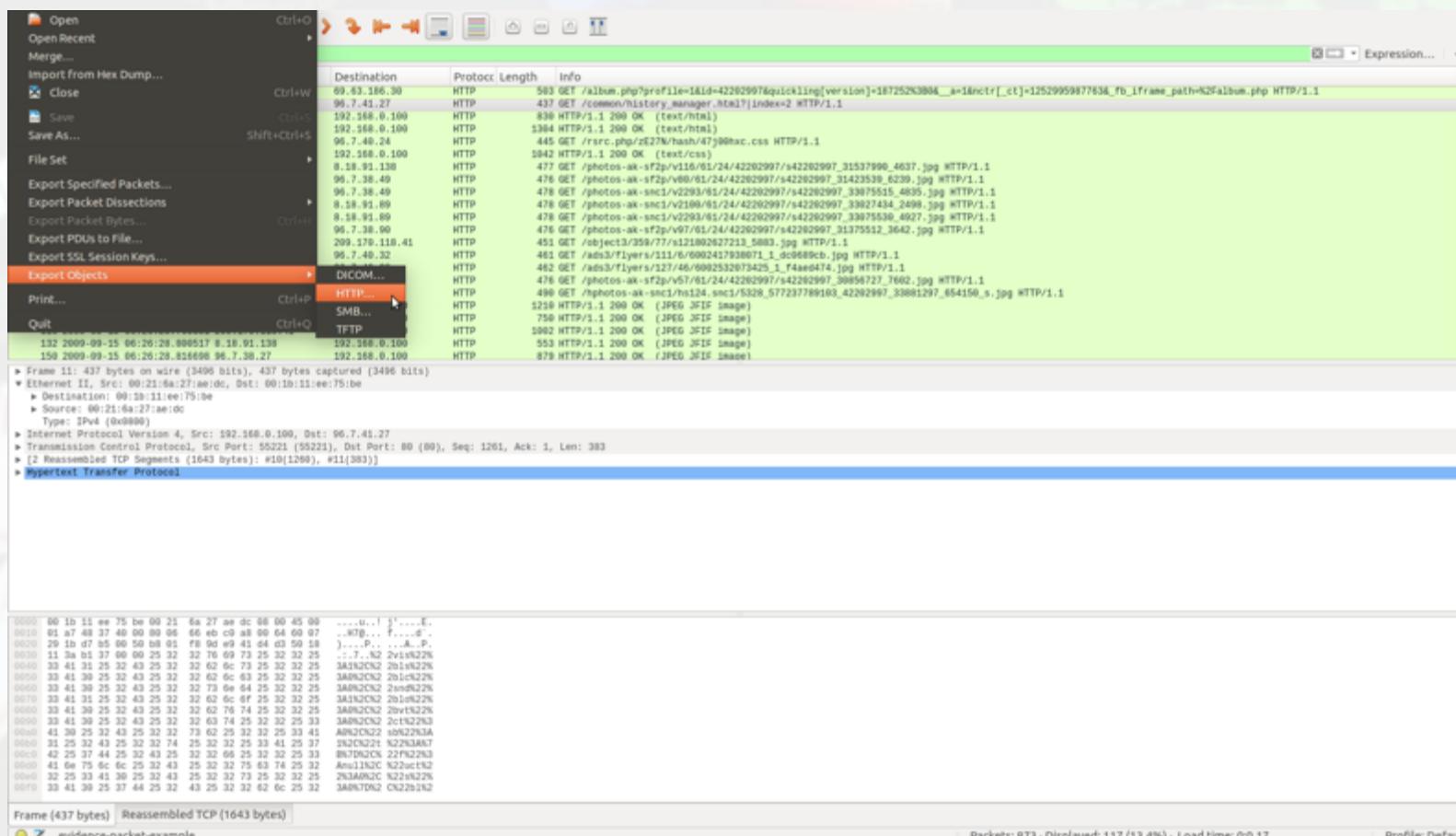
Flow Graphs



Flow Graphs



Export HTTP



Export HTTP Objects

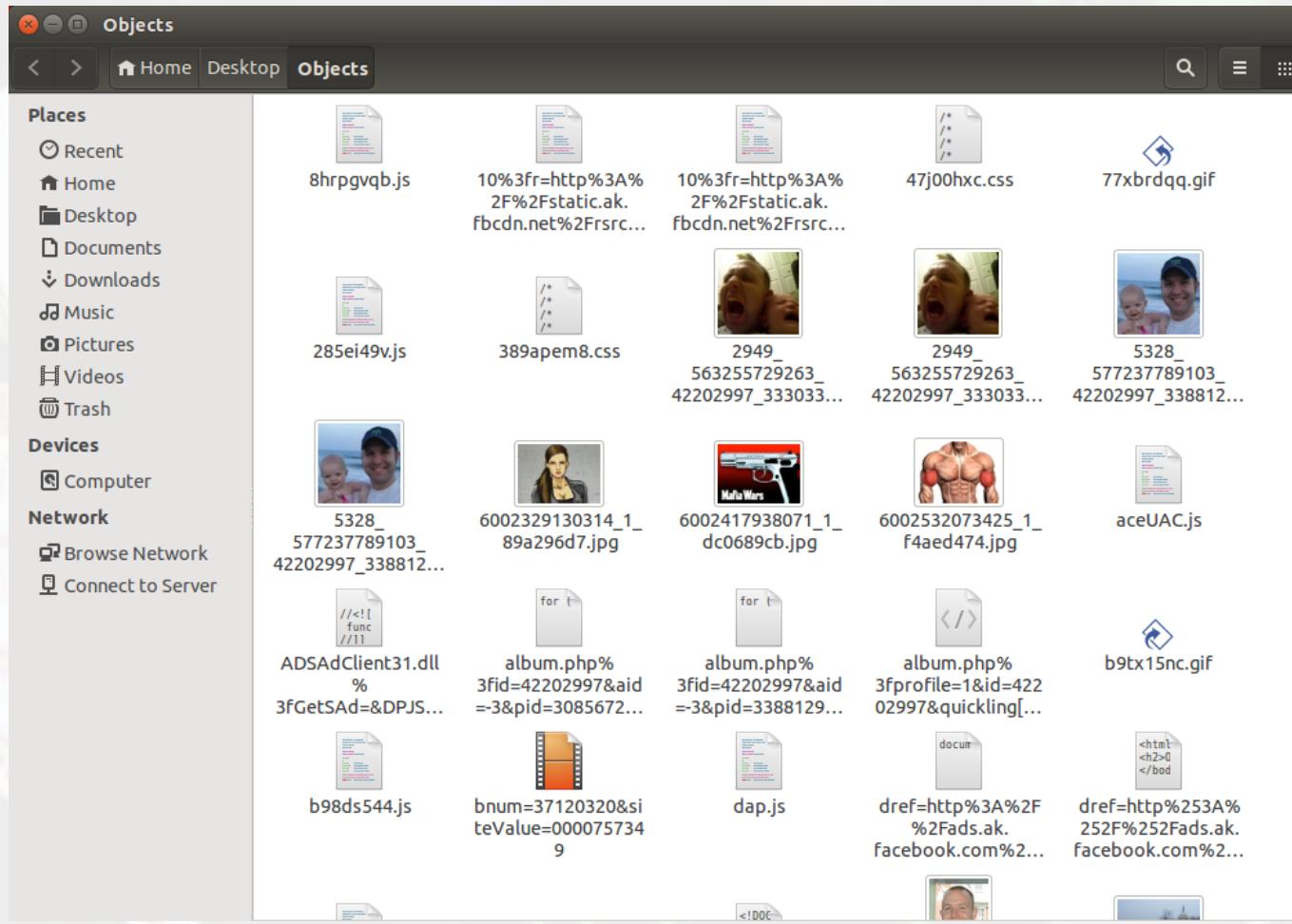
Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
14	static.ak.facebook.com	text/html	581 bytes	history_manager.html?index=2
23	www.facebook.com	text/html	20 kB	album.php?profile=1&id=42202997
33	static.ak.fcdn.net	text/css	15 kB	47j00hxc.css
95	photos-d.ak.fcdn.net	image/jpeg	5883 bytes	s42202997_33075515_4835.jpg
104	photos-c.ak.fcdn.net	image/jpeg	5942 bytes	s42202997_33075530_4927.jpg
110	profile.ak.fcdn.net	image/jpeg	3285 bytes	s121802627213_5883.jpg
132	photos-g.ak.fcdn.net	image/jpeg	5931 bytes	s42202997_31537990_4637.jpg
150	photos-h.ak.fcdn.net	image/jpeg	4292 bytes	s42202997_30856727_7602.jpg
156	creative.ak.fcdn.net	image/jpeg	9288 bytes	6002417938071_1_dc0689cb.jpg
165	creative.ak.fcdn.net	image/jpeg	9191 bytes	6002532073425_1_f4aed474.jpg
168	photos-c.ak.fcdn.net	image/jpeg	3962 bytes	s42202997_33027434_2498.jpg
174	photos-b.ak.fcdn.net	image/jpeg	4493 bytes	5328_577237789103_42202997_33
176	photos-d.ak.fcdn.net	image/jpeg	5300 bytes	s42202997_31423539_6239.jpg
181	photos-b.ak.fcdn.net	image/jpeg	4125 bytes	2949_563255729263_42202997_33
191	photos-a.ak.fcdn.net	image/jpeg	4399 bytes	s42202997_31375512_3642.jpg
230	www.facebook.com	text/html	77 kB	photo.php?pid=33881297&id=4220
243	static.ak.fcdn.net	application/x-javascript	2155 bytes	285ei49v.js
266	static.ak.fcdn.net	image/gif	1900 bytes	ejut8v2y.gif
271	static.ak.fcdn.net	application/x-javascript	41 kB	8hrpgvqb.js
293	photos-b.ak.fcdn.net	image/jpeg	14 kB	5328_577237789103_42202997_33
299	ads.ak.facebook.com	text/html	276 bytes	us-120photo.html
301	static.ak.fcdn.net	image/gif	716 bytes	b9tx15nc.gif
302	static.ak.fcdn.net	image/gif	721 bytes	77xbrdqq.gif
328	ads1.msn.com	application/x-javascript	13 kB	dap.js
333	ads.ak.facebook.com	image/gif	43 bytes	us-120photo.gif

Help Save All Close Save



Export HTTP Objects



HTTP Analysis

The screenshot shows the Wireshark interface with an analysis session titled "http and !(tcp.stream eq 5)". The main pane displays a list of network frames, with frame 117 highlighted. The details pane shows the HTTP request and response for frame 117. The bytes pane shows the raw hex and ASCII data of the selected frame. A context menu is open over frame 117, with the "HTTP" submenu expanded. The "Load Distribution" option is highlighted.

Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BAcnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
Frame 14: 830 bytes on wire (6640 bits)
Ethernet II, Src: 00:01:11:ee:75:be (00:01:11:ee:75:be), Dst: 00:21:6a:27:ae:dc (00:21:6a:27:ae:dc)
Source: 00:01:11:ee:75:be
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 98.21.6a.27, Dst: 10.0.0.1
Transmission Control Protocol, Src Port: 51400, Dst Port: 80
Hypertext Transfer Protocol
Line-based text data: text/html

No. Time Source Destination Info Length
1 2009-09-15 08:26:27.845593 98.21.6a.27 → 10.0.0.1 HTTP /album.php?profile=5&id=42202997&quickling[version]=18725263884_a=1&nctr[_ct]=12529959877638_fb_iframe_path=%2Falbum.php HTTP/1.1 503
2 2009-09-15 08:26:27.941427 10.0.0.1 → 98.21.6a.27 HTTP /common/history_manager.html?index=2 HTTP/1.1 437
3 2009-09-15 08:26:28.007619 98.21.6a.27 → 10.0.0.1 HTTP / 830 HTTP/1.1 200 OK (text/html)
4 2009-09-15 08:26:28.407903 98.21.6a.27 → 10.0.0.1 HTTP / 1304 HTTP/1.1 200 OK (text/html)
5 2009-09-15 08:26:28.496640 98.21.6a.27 → 10.0.0.1 HTTP / 445 GET /rsrc.php/e27m/hish/47j00nn.css HTTP/1.1 162
6 2009-09-15 08:26:28.549179 98.21.6a.27 → 10.0.0.1 HTTP / 1842 HTTP/1.1 200 OK (text/css)
7 2009-09-15 08:26:28.664965 98.21.6a.27 → 10.0.0.1 HTTP / 477 GET /photos-ak-s72p/v116/61/24/42202997/s42202997_31537998_4637.jpg HTTP/1.1 170
8 2009-09-15 08:26:28.672238 98.21.6a.27 → 10.0.0.1 HTTP / 478 GET /photos-ak-s72p/v08/61/24/42202997/s42202997_31423539_6239.jpg HTTP/1.1 170
9 2009-09-15 08:26:28.677239 98.21.6a.27 → 10.0.0.1 HTTP / 478 GET /photos-ak-smc1/v2293/61/24/42202997/s42202997_33075515_4835.jpg HTTP/1.1 170
10 2009-09-15 08:26:28.677828 98.21.6a.27 → 10.0.0.1 HTTP / 478 GET /photos-ak-smc1/v2100/61/24/42202997/s42202997_33027434_2498.jpg HTTP/1.1 170
11 2009-09-15 08:26:28.678976 98.21.6a.27 → 10.0.0.1 HTTP / 478 GET /photos-ak-smc1/v2293/61/24/42202997/s42202997_33075530_4927.jpg HTTP/1.1 170
12 2009-09-15 08:26:28.690561 98.21.6a.27 → 10.0.0.1 HTTP / 478 GET /photos-ak-s72p/v97/61/24/42202997/s42202997_31375512_3642.jpg HTTP/1.1 170
13 2009-09-15 08:26:28.690568 98.21.6a.27 → 10.0.0.1 HTTP / 451 GET /object13/359/77/s123802627213_5883.jpg HTTP/1.1 170
14 2009-09-15 08:26:28.692438 98.21.6a.27 → 10.0.0.1 HTTP / 461 GET /adis3/f1vers/111/r/60002417938071_1_oc6989cb.jpg HTTP/1.1 170
15 2009-09-15 08:26:28.693021 98.21.6a.27 → 10.0.0.1 HTTP / 462 GET /adis3/f1vers/127/46/6002532073425_1_f4aae474.jpg HTTP/1.1 170
16 2009-09-15 08:26:28.713583 98.21.6a.27 → 10.0.0.1 HTTP / 476 GET /photos-ak-smc1/v2100/61/24/42202997/s42202997_330856727_7602.jpg HTTP/1.1 170
17 2009-09-15 08:26:28.715549 98.21.6a.27 → 10.0.0.1 HTTP / 490 GET /photos-ak-smc1/h1/s124.smc1/s5328_577237789103_42262997_330881297_054150_a.jpg HTTP/1.1 170
18 2009-09-15 08:26:28.737593 98.21.6a.27 → 10.0.0.1 HTTP / 1210 HTTP/1.1 200 OK (JPEG/JFIF image) 170
19 2009-09-15 08:26:28.753176 98.21.6a.27 → 10.0.0.1 HTTP / 750 HTTP/1.1 200 OK (JPEG/JFIF image) 170
20 2009-09-15 08:26:28.760301 98.21.6a.27 → 10.0.0.1 HTTP / 1002 HTTP/1.1 200 OK (JPEG/JFIF image) 170
21 2009-09-15 08:26:28.800517 98.21.6a.27 → 10.0.0.1 HTTP / 1002 HTTP/1.1 200 OK (JPEG/JFIF image) 170
22 2009-09-15 08:26:28.816698 98.21.6a.27 → 10.0.0.1 HTTP / 1002 HTTP/1.1 200 OK (JPEG/JFIF image) 170

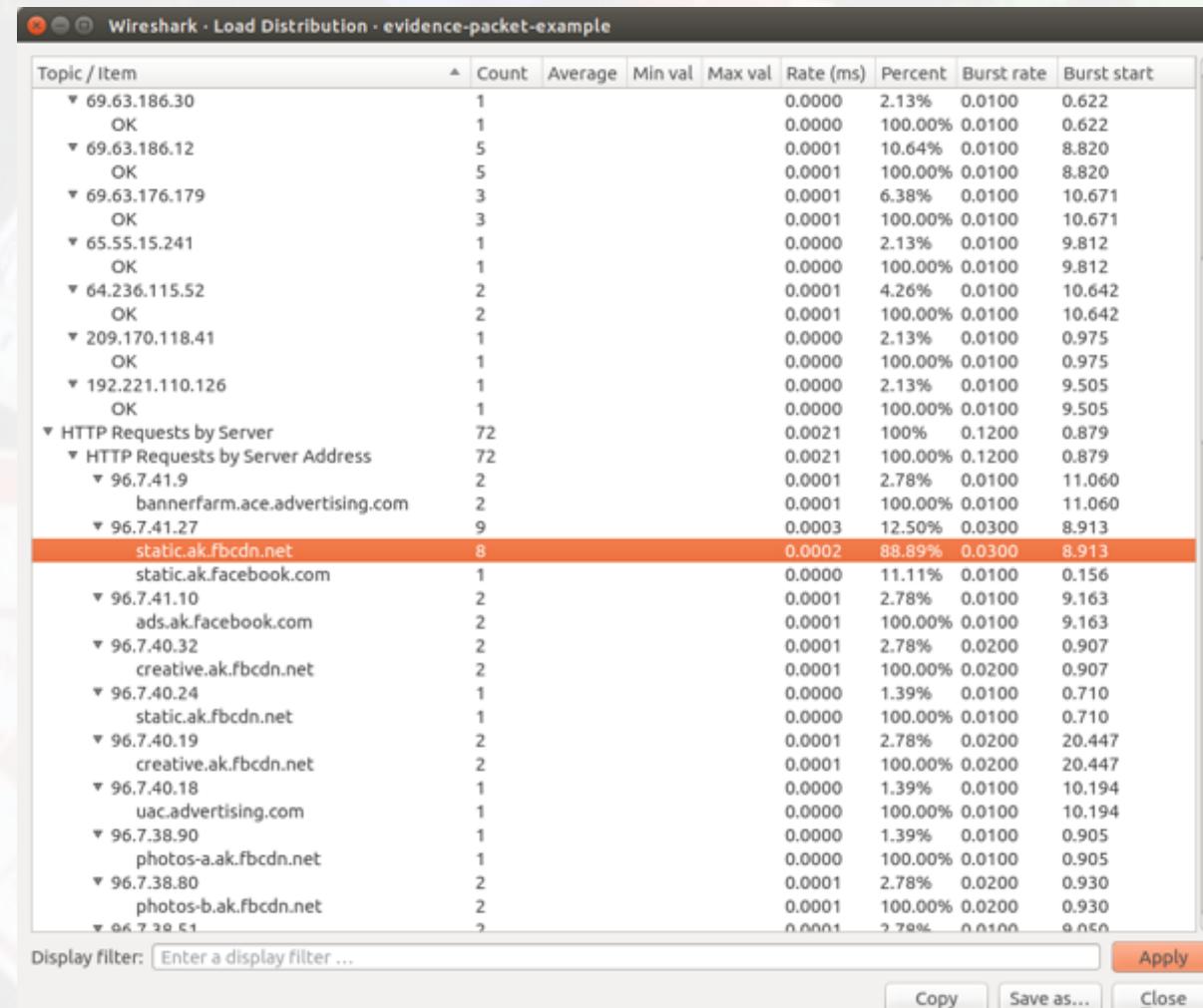
HTTP Requests Load Distribution

Frame (830 bytes) Uncompressed entity body (581 bytes)
evidence-packet-example

Packets: 873 · Displayed: 117 (13.4%) · Load time: 0:0.17 · Profile: Default



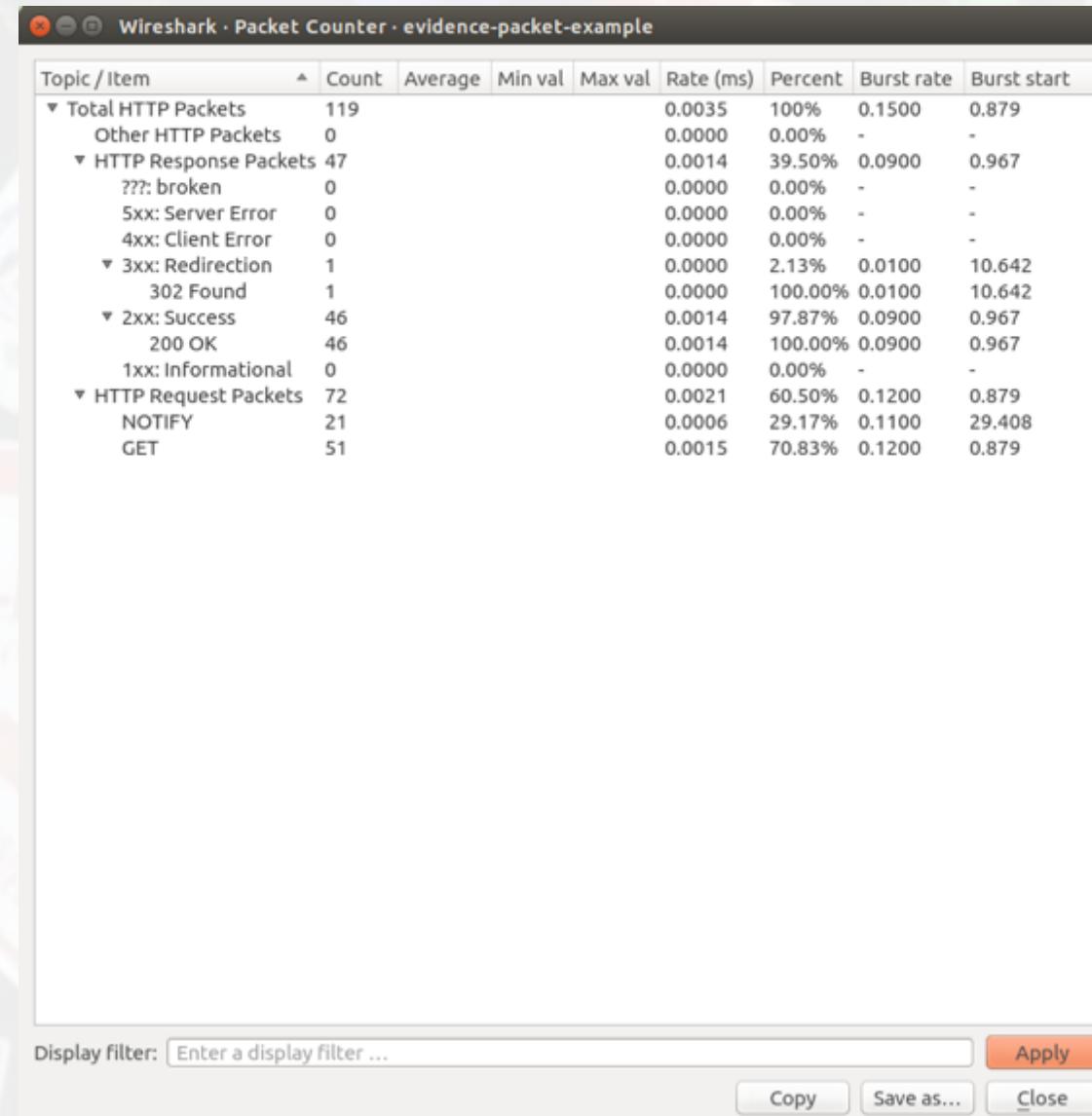
HTTP Analysis – Load Distribution



Use the display filter to only
Show selected traffic



HTTP Analysis – Packet Counter



HTTP Analysis – Requests

Wireshark - Requests - evidence-packet-example

Topic / Item

- ▼ HTTP Requests by HTTP Host
 - ▼ www.facebook.com
 - /photo.php?pid=33881297&id=42202997
 - /photo.php?pid=30856727&id=42202997
 - /album.php?profile=1&id=42202997&quickling[version]=187252%3B0&_a=1&nctr[_ct]=125299598776
 - /album.php?id=42202997&aid=-3&pid=33881297&async=true&page=1&_a=1&nctr[_ct]=12529959976
 - /album.php?id=42202997&aid=-3&pid=30856727&async=true&page=1&_a=1&nctr[_ct]=12529960081
 - /ajax/presence/reconnect.php?reason=6&iframe_loaded=false&post_form_id=4d8d1b737fa21cd43847
 - ▼ view.atdmt.com
 - /APM/iview/112458055/direct;wi.160;hi.600/01?click=
 - ▼ uac.advertising.com
 - /wrapper/aceUAC.js
 - ▼ static.ak.fcdn.net
 - /rsrc.php/zE27N/hash/47j00hxc.css
 - /rsrc.php/zDWGN/hash/389apem8.css
 - /rsrc.php/zDBQC/hash/b9tx15nc.gif
 - /rsrc.php/z9F3Q/hash/8hrpgvqb.js
 - /rsrc.php/z970X/hash/b98ds544.js
 - /rsrc.php/z6JCX/hash/ea556j4i.js
 - /rsrc.php/z5R48/hash/ejut8v2y.gif
 - /rsrc.php/z215A/hash/285ei49v.js
 - /rsrc.php/z1W00/hash/77xbrdqq.gif
 - ▼ static.ak.facebook.com
 - /common/history_manager.html?|index=2
 - ▼ servedby.advertising.com
 - /site=757349/size=160600/u=1/bnum=37120320/hr=2/hl=0/c=0/scres=5/swh=1920x1200/tile=1/f=2/r=1/ctst=1/site=757349/size=160600/u=1/bnum=37120320/hr=2/hl=0/c=0/scres=5/swh=1920x1200/tile=1
 - ▼ rad.msn.com
 - /ADSAAdClient31.dll?GetSAd=&DPJS=0&PG=FBKPHT&AP=1113
 - ▼ profile.ak.fcdn.net
 - /object3/359/77/s121802627213_5883.jpg
 - ▼ photos-h.ak.fcdn.net
 - /photos-ak-sf2p/v57/61/24/42202997/s42202997_30856727_7602.jpg
 - /photos-ak-sf2p/v57/61/24/42202997/n42202997_30856727_7602.jpg
 - ▼ photos-o.ak.fcdn.net

Display filter: Apply

Copy Save as... Close



Improving Wireshark Performance

- Don't use capture filters (use post-capture display filters)
- Increase your read buffer size (if possible)
- Don't update the screen dynamically
- Get a faster computer (do I have to say this!!)
- Run in a linux distro (less overhead)
- Use a TAP (Hak5)
- Don't resolve names (MAC's and IP's) **false positives



Post-Processing Text File

- For saved text-format packet files, further analysis needs coding or special tools (tcpextract works well here)
- One useful Linux tools for packets: Grep & ngrep
 - On Windows: PowerGrep <http://www.powergrep.com/>
 - Command-line based utility for searching plain-text data sets for lines matching a regular expression.



Basic usage of Grep

- Command-line text-search program in Linux
- Some useful usage:
 - Grep 'word' filename # find lines with 'word'
 - Grep -v 'word' filename # find lines without 'word'
 - Grep '^word' filename # find lines beginning with 'word'
 - Grep 'word' filename > file2 # output lines with 'word' to file2
 - ls -l | grep rwxrwxrwx # list files that have 'rwxrwxrwx' feature
 - grep '^[0-4]' filename # find lines beginning with any of the numbers from 0-4
 - Grep -c 'word' filename # find lines with 'word' and print out the number of these lines
 - Grep -i 'word' filename # find lines with 'word' regardless of case
- NGREP also exists for Grep'ing of packet capture files
- Many tutorials on grep online
 - <http://www.cyberciti.biz/faq/howto-use-grep-command-in-linux-unix/>
 - <http://www.thegeekstuff.com/2009/03/15-practical-unix-grep-command-examples/>

Lab Exercise

File: evidence1.pcap

What we should be looking for:

- Determine PC's used
- IP addresses of devices
- Mac Addresses of devices
- Protocols Found in packets
- User-related data
- Exported Files
- Endpoints

Disclaimer: The “investigation” part of this exercise will be covered in Saturday’s “Network Forensics” session



Questions?

