Thomas Murphy Cyb 605-Z3 – Principles of Cybersecurity Wireshark Lab Oct 3, 2016

## Introduction

This lab introduces packet sniffing and packet analysis; the process of capturing any data passed over the local network and looking for any information that may be useful. Packet sniffers can be hardware appliances or software based (Hannah, 2011). A sniffer works by placing the network interface you want to listen to into promiscuous mode, thus reporting all the packets that it sees (Weadock, 2009).

The lab specifically focuses on the use of Wireshark, a graphical packet sniffer, and packet sniffing for security professionals. Wireshark (and tcpdump) enable administrators to view and examine packets in a granular format in either real-time or to a capture file for examination later. This provides a tool for the administrator to find network errors, measure bandwidth, become aware of intrusion attempts and attacks, map and discover network devices, and become aware of protocols and applications being used on the network.

In this lab I'm using CentOS version 7.2 and A VMWare version of Windows 95. I've run Wireshark over my wireless home network with approximately 20 nodes, including cell phones, two Roku devices, a Brother printer, various laptops, and baby monitors. I've also run it on a corporate network (with permission) that contains high sped market data and multicast networking. Lastly I've also captured data at a public wireless hotspot that required no passwords.

# **Objectives**

The objectives of this lab are to execute the Wireshark Lab assignments in order to review and enhance previous learning, as well as to learn through experience, and gain the skills and knowledge about various tools currently available. In order to achieve the objective I've connected to three networks using my Dell Laptop running Centos 7.2 through its wireless network interface. I captured packets over a period of time, both for live capture into capture files for later analysis. I applied various filtering to isolate specific types of network packets and described my finding in detail.

# Definitions

- Wireshark
  - a) **Sniffer** software that intercepts and logs network traffic that it can "see" on a network interface. It's used for capturing and reporting data flows. (Paessler, 1996)
  - b) Protocol a set of agreed upon rules for how data is transmitted. In terms of network protocols, there are protocols for how data is packaged and exchanged across a network. The most common of these protocols is "TCP/IP". There are also application protocols that define how a client and server will communicate upon making a network connection (Hunt 1992),
  - c) **Protocol Analyzer** A tool used to analyze protocol interaction between two systems (Hunt, 1992)
  - d) **Packet** Data that is communicated across a network is broken into small blocks called packets. "Dividing the data into packets helps the sender and receiver of the data decide

which packets arrived in tact". "Dividing data into packets also ensures that multiple network connections can share a network device" (Comer, 1997)

- e) **Packet Filter** A tool used for selectively accepting or blocking data as it passes through a network interface (OpenBSD, 2016)
- f) **Live Capture –** there are two ways to capture data; live and into a file for analysis later on.
- TCP/IP
  - a) **Transport Control Protocol (TCP)** A connection oriented protocol that provides a full-duplex byte stream for user processes. This means, that when a packet is sent to a host, an acknowledgement packet is returned to the sender. (Stevens, 1990)
  - b) **Internet Protocol (IP)** This is generally combined with TCP for the purpose of routing and delivering the TCP packet (Stevens, 1990)
  - c) **Network Stack** A network stack is a reference to the layers of protocols necessary for data communication. When discussing a network stack we generally refer to the OSI model of network communications.



The OSI model is a theoretical model of communication. In the above diagram, you can see how the TCP/IP Network Stack lines up against OSI and shows examples of each layer in the suite. (Erbay, 2016)

d) Packet Header – A packet contains two parts, a header and a payload. The header contains information about where the packet should be sent and details about the contents of the packet, while the payload contains the data the is actually being sent. A typical IPV4 packet contains 20 bytes of data. The 20 bytes of data contain the IP version (4 for IPv4), IP Header Length, type of service, datagram length, an ID tag to

help reconstruct, instructions on fragmentation, fragmentation offset (what part of the packets to start reconstruction), TTL (number of network hops), a header checksum (to help detect errors), source IP address and the destination IP address (Comer, 1997).



**Using Wireshark** 

This section was an introduction for starting Wireshark, finding documentation and beginning to sniff data from a network interface.

#### **Procedure**:

Steps 1 and 2 of the lab are for downloading and installing Wireshark and all other necessary packages. For Wireshark on Centos 7.2 (or any Red Hat Enterprise Linux variant) the command is simply:

```
yum -y install wireshark*
```

Step 3: Upon starting Wireshark we were asked to select our Internet facing interface

The Wirk File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	shark Network Analyzer [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• . 0 x
Filter: Expression Clear Apply Save		
WIRESHARK The World's Most Popular Network Protoco Version 1.10.14 (Git Rev Unknown from unknown)	l Analyzer	
Capture	Files	Online
Capture	Person       Open a previously captured file         Open Recent:              • Sample Captures         A rich assertment of example capture files on the will	Website         Vist the graject's website         Image: Comparison of the second seco
Ready to load or capture No Packets		Profile: Default

Once the NIC was selected, we were able to start capturing network packets:

4			Capturing from wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
File Edit View Go Capture Analyze Statis	stics Telephony Tools Int	ernals Help		
	C   Q (~ ~) ">	$\approx 2$		
Filter:	✓ Expre	ssion Clear	Apply Save	
No. Time Source	Destination	Protoc L	engt_info	
227 40.52030640173.194.66.100	192.168.1.8	TCP	66 https > 47036 [ACX] Sequil622 Ack=7082 Win=1622 Lene TSval=851292656 TSecr=15455257881	
229 40.34234187.173.194.204.134 229 41.98472009:Actionte_20:7a:f7	Spanning-tree-(for-b	r: STP	00 [cnt.gbs / 39:500 [fkc] 34[-907 [kc]-1413 [k1]-40:00 [cm+0] 34:4-30:30[39:00 [39:0] -1:33:208:04	
230 42.39473742 Actionte_20:7a:f7 231 42.51366260 192.168.1.6	Broadcast 173,194,68,138	ARP TLSv1.2	60 Who has 192.168.1.117 Tell 192.168.1.1 100 Application Data	
232 42.51370474 192.168.1.6	173.194.68.138	TLSv1.2	100 [TP] Petransmission] Application Data	
233 42, 54071849: 173, 194, 68, 138 234 42, 54084137(192, 168, 1, 8	173.194.68.138	ICMP	100 Application Unreachable (Host administratively prohibited)	
235 42.72652154.74.125.22.189 236 42.72660094.192.168.1.8	192.168.1.8 74.125.22.189	TLSv1.2	127 Application Data 66 45376 > https://doi.iouxil.ack=123.Win=598.Len=0.TSval=1535270306 TSecr=642393302	
237 42.73697676192.168.1.6	173.194.68.138	TCP	54 unifyadmin > https [ACK] Seq=47 Ack=47 Win=64844 Len=0	
239 43.41864808 Actionte_20:7a:f7	173.194.68.138 Broadcast	ARP	Se (ICP LUD ACK 2072) UNITYSUBINT > NETDS LACK Seger/ ACKEA/ WHEE4844 Leneu	
240 44.03001638 Actionte_20:7a:f7	Spanning-tree-(for-b	ARP	60 Conf. Root = 32768/0/0017f;28:2017a:f8 Cost = 0 Port = 0x8004	
242 44.50087753 Actionte_20:7a:f7	IntelCor_7b:7e:64	ARP	60 Who has 192.168.1.8? Tell 192.168.1.1	
243 44.50094392:IntelCor_7b:7e:64 244 46.08038538:Actionte 20:7a:f7	Actionte_20:7a:f7 Spanning-tree-(for-b	ARP r:STP	42 192.168.1.8 is at a0:88:b4:7b:7e:64 60 Conf. Root = 32769/00107:128:120:7a:18 Cost = 0 Port = 0x8004	
245 47.40279720 192.168.1.8	173.194.207.138	TLSv1.2	112 Application Data	
247 47.42733006:192.168.1.8	173.194.207.138	TCP	112 Application baca 66 33826 > https://doi.org/10.1001/001110000000000000000000000000	1
248 47.99376294 Actionte_20:7a:f7	Spanning-tree-(for-b	r:STP	60 Conf. Root = 32768/0/00:7f:28:20:7a:f8 Cost = 0 Port = 0x8004	
<ul> <li>              Frame 236: 66 bytes on wire (528 bits)      </li> <li>             Ethernet II, Src: IntelCor_7b:7e:64 (a)     </li> </ul>	), 66 bytes captured ( a0:88:b4:7b:7e:64), Ds	28 bits) or :: Actionte	interface 0 20:7a:f7 (00:7f:28:20:7a:f7)	
Internet Protocol Version 4, Src: 192.     Transmission Control Protocol, Src Page	.168.1.8 (192.168.1.8)	Dst: 74.12 Port: http:	(5.22.109 (74.125.22.109) (4d3). Sec. 1. Act: 173. Len: 0	
		rore. neep.	(1997), dog, ay min. 200, Call C	
0000 00 7f 28 20 7a f7 a0 88 b4 7b 7e	64 08 00 45 00(;			
0010 00 34 6e ba 40 00 40 06 a9 1f c0 0020 16 bd b1 40 01 bb fc 1c 7e 6e b2	a8 01 08 4a 7d .4n.( ea bf 01 80 10@	a.@	)	
0030 01 8e ae 8c 00 00 01 01 08 0a 5b 0040 24 d6	82 5d a2 26 4a \$.	[.].(	<i>a</i>	
U 🕅 wip2s0: <live capture="" in="" progress=""> File - Pac</live>	ckets: 248 · Displayed: 248 (	100.0%)	Profile: Dr	afault

From the picture above you can note that the GUI is broken up into three main panels.

- 1. The packet frame This displays general contents in the capture file including, the
  - Number off packets.
  - Time The timestamp of the packet.
  - Source The address where this packet is coming from.
  - Destination The address where this packet is going to.
  - Protocol The protocol name in a short version.
  - Length The length of each packet.
  - Additional information about the packet content. (Wireshark, 2014)
- 2. The "Packet Details" pane This shows the protocols and the protocol fields of the packet. Of special note, any data enclosed in "[" and "]" brackets is generated by Wireshark. Additionally, if Wireshark detects a relationship to another packet, it will create a link to that packet (Wireshark, 2014).
- **3.** The "Packet Bytes" pane This frame contains a hex dump of the entire packet (Wireshark, 2014)

	share consisting Tablebase	. Tala intervala itala	Capturi	ing from wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
E Capture An	aiyze Statistics lelephony	y 1001s internais Help • •≫ % & ⊻   [■		- 4 📅   👹 🔀 🔞   🕫	
Filter:		✓ Expression Clear A	pply Save		
No. Time	Source	Destination	Protoc L	engt Info	
5211 898,699577912	192,168,1,6	74,125,22,100	TCP	54 [TCP Dup ACK 5210#1] raventdm > https [ACK] Seg=202 Ack=3988 Win=65535 Len=0	
5212 898.723173012	192.168.1.6	74.125.22.100	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request	
5213 898.723196182 5314 898.727323494	192.168.1.6	74.125.22.100	TLSv1.2	180 [TCP Retransmission] Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request 211 Application Data	
5215 898.727249355	192.168.1.6	74.125.22.100	TLSv1.2	211 [TCP Retransmission] Application Data	
5216 898.727515657	192.168.1.6	74.125.22.100	TLSv1.2	920 Application Data	
5217 898.727527825 5218 898.727749689	192.168.1.6	74.125.22.100 74.125.22.100	TLSV1.2 TLSV1.2	920 [TCP: Retrainsmission]. Application Data 587 Application Data	
5219 898.727761902	192.168.1.6	74.125.22.100	TLSv1.2	567 [TCP Retransmission] Application Data	
5220 898.749280020	74.125.22.100	192.168.1.6	TLSv1.2	316 New Session Ticket, Change Cipher Spec, Hello Request, Hello Request	
5222 898.749403154 5222 898.749403154	74.125.22.100	192.168.1.6	TLSv1.2	San Destination unreachador (Nost administratively promoted) 116 Application Data	
5223 898.749433612	192.168.1.8	74.125.22.100	ICMP	144 Destination unreachable (Host administratively prohibited)	
5224 898.749449716 5225 898 749474824	74.125.22.100	192.168.1.6	TLSv1.2	96 Application Data 124 Destingtion unsachable (Hest administratively probibited)	
5226 898.749790078	192.168.1.6	74.125.22.100	TCP	54 rayentdm > https [ACK] Seq=1884 Ack=4354 Win=55169 Len=0	
5227 898.749810588	192.168.1.6	74.125.22.100	TCP	54 [TCP Dup ACK 5226#1] raventdm > https [ACK] Seq=1884 Ack=4354 Win=65169 Len=0	
5228 898.750495862 5229 898.750508968	192.168.1.6	74.125.22.100 74.125.22.100	TLSv1.2 TLSv1.2	92 Application Data 92 (TCP Retransmission) Application Data	
5230 898.754638384	74.125.22.100	192.168.1.6	TLSv1.2	92 Application Data	
5231 898.757614254	74.125.22.100	192.168.1.6	TCP	60 https > rayentdm [ACK] Seq=4392 Ack=1884 Win=49362 Len=0	
+ Ename 5225: 124 bytes on with	re (992 bits), 124 byte	es captured (992 hits) or	interface (		
Ethernet II, Src: IntelCor_:	7b:7e:64 (a0:88:b4:7b:	7e:64), Dst: Actionte_20:	7a:f7 (00:7	- 128:20:7a:f7)	
Internet Protocol Version 4,	, Src: 192.168.1.8 (192	2.168.1.8), Dst: 74.125.2	22.100 (74.1)	25.22.100)	
Internet Control Message Pre	otocol				
	1 4 7 7 64 66 66 47	-			
0010 00 6e cd d1 00 00 40 01	89 6c c0 a8 01 08 4a	7d .n@l			
0020 16 64 03 0a 1f ca 00 00 0030 00 00 2d 06 1a a7 4a 7d	00 00 45 00 00 52 50	30 .dERP0			
0040 0a 9a fc 7b 1f dd 11 69	3a fa 50 18 a9 98 ee	af{i :.P			
0050 00 00 17 03 03 00 25 00 0060 25 e0 c5 45 74 d3 b8 ff	e6 54 63 fc la c2 4f	17% f8 %EtTc0.			
0070 b6 26 26 06 e2 01 10 ae	ba 6d e7 47	.&&m.G			
🛑 ಶ wip2s0: <live capture="" in="" progre<="" td=""><td>ss&gt; Fi Packets: 7412 · Di</td><td>isplayed: 7412 (100.0%)</td><td></td><td>Profile: Default</td><td></td></live>	ss> Fi Packets: 7412 · Di	isplayed: 7412 (100.0%)		Profile: Default	

In my first run, I started seeing some communication with 74.125.22.100. I also noticed some retransmission packets and packets containing the following messages:

## destination host is unreachable (host administratively prohibited)

They appeared to be only for ICMP packets, so I imagine they must be blocking those packets using a firewall or other network policy.

Some further investigation provided additional information:



It appears that this is Google:

https://support.google.com/faqs/answer/174717?hl=en

What is 1e100.net? - Google H	lelp - Mozilla Firefox		•	0	S X
G         What is 1e100.net? ×           (         ) @ \u03c6           (         ) @ \u03c6           (         ) @ \u03c6	マロ ( C ) Q. Search ☆ 自 ♥	+	俞	e	=
Google	:		0	6	
Google Help		G	DOGLE	: Ð	
What is 1e100.net? It 100.net is a Google owned domain name used to identify the servers in our network. Following standard industry practice, we make sure each IP address has a corresponding hostname. In October 2009, we stanted using a single domain name to kentify our servers across all Google products, rather than use different product domains such as youble corr. Biogencom. and google corr. We differ for two researces first to kenp things singles; and second, to proactively improve security by protecting against potential threats such as cross-site scripting attacks. Most typical Internet users will never see 1e100.net, but we picked a Googley name for it just in case (1e100 is scientific notation for 1 googo).					
Was this article helpful7 YES NO					
62016 Google - Privacy Policy - Terms of Service English 2					

The lab then asks us to select the STOP button and describe the results in your lab:

4				*wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - @ ×
File Edit View Go Capture Analy	yze Statistics Telephony To	ools Internals Help			
• • 🧉 📕 🧟 🖿 🚺	<b>X</b> G <b>Q</b> 🖗 -	> > ~ _ E			
Filter:	~	Expression Clear App	ly Save		
No. Time	Source	Destination	Protoc	Lengt Info	
45680 5186.741496729	192.168.1.6	173.194.68.139	TLSv1.2	100 Application Data	
45681 5186.741511288	192.168.1.6	173.194.68.139	TLSv1.2	100 [TCP Retransmission] Application Data	
45682 5186.742290065	192.168.1.6	173.194.68.139	TLSv1.2	85 Encrypted Alert	
45683 5186,742307409	192.168.1.6	173.194.68.139	TLSv1.2	85 [TCP Retransmission] Encrypted Alert	
45684 5186.742497897	192.168.1.6	173.194.68.139	TCP	54 rbakcup2 > https [FIN, ACK] Seq=2772 Ack=1037 Win=65337 Len=0	
45685 5186,742511159	192.168.1.6	173.194.68.139	TCP	54 [TCP Out-Of-Order] rbakcup2 > https [FIN, ACK] Seq=2772 Ack=1037 Win=65337 Len=0	
45586 5186.767945588	173.194.68.139	192.168.1.6	TCP	ou https > roakcup2 [Hol] Seq=1037 Win=0 Len=00	
45667 5186,768067452	192.108.1.8	265 265 265 265	DHCD	oz besthation unreachable (nost administratively prohibited) 242 DUCD Discours Transaction (D. 0.9669020	
45689 5187 761902007	Actionte 20:7a:f7	Broadcast	ARP	60 Who has 102-168.1.107 Tail 102-168.1.1	
45690 5187,928244638	192,168,1,6	192, 168, 1, 255	BROWSER	243 Host Announcement RIFESOCK-3MKDZJ, Workstation, Server, NT Workstation	
45691 5187.928285297	192.168.1.6	192.168.1.255	BROWSER	243 Host Announcement BIFFSOCK-3wKDZJ, Workstation, Server, NT Workstation	
45692 5188.034970196	Actionte 20:7a:f7			60 Conf. Root = 32768/0/00:7f:28:20:7a:f8	
45693 5188.750418531	Actionte_20:7a:f7	Broadcast	ARP	60 Who has 192.168.1.107 Tell 192.168.1.1	
45694 5189.774016766	Actionte_20:7a:f7	Broadcast	ARP	60 Who has 192.168.1.10? Tell 192.168.1.1	
45695 5189.948642833	173.194.206.189	192.168.1.8	TLSv1.2	127 Application Data	
45696 5189.948748109	192.168.1.8	173.194.206.189	TCP	66 50738 > https [ACK] Seq=3386 Ack=4609 Win=33536 Len=0 TSval=1540417528 TSecr=714311826	
	Actionte_20:7a:f7			60 Conf. Root = 32768/0/00:7f:28:20:7a:f8	
45698 5190.354374778	192.168.1.8	192.168.1.1	DNS	75 Standard query Oxade9  A play.google.com	
45699 5190.354408368	192.168.1.8	192.168.1.1	DNS	75 Standard query OxeBac AAAA play.google.com	
45700 5190.360754865	192.168.1.8	172.217.2.14	TLSv1.2	1451 Application Data	
45701 5190.365661159	192.168.1.8	172.217.2.14	TLSv1.2	369 Application Data	
45702 5190.375181237	1/2.21/.2.14	192.168.1.8	TOP	00 https > 37070 [Atk] seg=13480 Ack=2912 Win=50944 Lene I SVAL=228467/233 [Sec=154041/940	170 104 004 115
45703 5190, 375854320	192.108.1.1	192.108.1.8	TCD	192 Standard query response uxades - CNAME playgoogle.com A 173.194.204.101 A 173.194.204.102 A 173.194.204.103 A 173	173.194.204.113
45705 5190 378078613	192 168 1 1	192.108.1.8	DMS	00 HCLPS / 3/0/0 [ACL] 36(213400 ACK-3213 W1H-33032 L0H-0 ISVAL-22040/230 H36(1-13404/1343	
45706 5190, 388330664	Actionte 20:7a:f7	Broadcast	ARP	60 Who has 192 1681 117 Tell 192 1681 1	
45707 5190, 408697172	172,217,2,14	192,168,1,8	TLSv1.2	261 Application Data	
45708 5190, 408762256	172,217,2,14	192.168.1.8	TLSv1.2	338 Application Data	
45709 5190, 408783728	172,217,2,14	192.168.1.8	TLSv1.2	112 Application Data	
45710 5190.409159912	192.168.1.8	172.217.2.14	TCP	66 37070 > https [ACK] Seq=3215 Ack=13999 Win=68480 Len=0 TSval=1540417989 TSecr=228467267	
45711 5190.409257662	192.168.1.8	172.217.2.14	TLSv1.2	112 Application Data	
45712 5190.460275466	172.217.2.14	192.168.1.8	TCP	66 https > 37070 [ACK] Seq=13999 Ack=3261 Win=53632 Len=0 TSval=228467321 TSecr=1540417989	
45713 5190.526035462	fe80::625b:b4ff:fe0a	a:lff02::1:2	DHCPv6	110 Solicit XID: 0x171a62 CID: 00030001605bb40a0b69	
45714 5190.530475861	192.168.1.8	75.185.121.120	NTP	90 NTP Version 4, client	
45715 5190.580229616	75.185.121.120	192.168.1.8	NTP	90 NTP Version 4, server	
45716 5191.345837224	Actionte_20:7a:f7	Broadcast	ARP	60 Who has 192.168.1.11? Tell 192.168.1.1	
45717 5191.740175203	Actionte 20:7a:17	IntelCor 7b:7e:64	ARP	60 Who has 192.168.1.67 Tell 192.168.1.1	
+ Frame 45743: 66 bytes on wire	(528 bits), 66 bytes ca	ptured (528 bits) on 1	nterface 0		
+ Ethernet II, Src: IntelCor_/b	:/e:64 (a0:88:b4:/b:/e:6	4), Dst: Actionte_20:/	a: f / (00: /	/11281201/411/)	
+ Internet Protocol Version 4,	SFC: 192.108.1.8 (192.10	8.1.8), Dst: 1/2.21/.4	.09 (1/2.2	21/.4.09/	
Transmission Control Protocol	, SFC POFT: 40018 (40018	), DSt Port: https (44	3), Seq: ∠	20/1, ACK: 2090, Len: 0	
0000 00 7f 28 20 7a f7 a0 88	b4 7b 7e 64 08 00 45 00	(z{~dE.			
0020 04 45 9c 52 01 bb bf 53	ds 5T CU as 01 08 ac d9	.4@.@			
0030 01 07 4f b5 00 00 01 01	08 0a 5b d1 0f 8a fc 28				
0040 ec 13		11	1		
🛑 🗹 Ready to load or capture	Packets: 45743 · Displ	ayed: 45743 (100.0%) · Dro	pped: 191 (0	0.4%) Profile: Default	

I saw https, http, ssh, DNS, DHCP, ARP, TCP and NTP traffic. I also saw some duplicate packets, which according to Wireshark appear to be normal behavior. This will happen if the sending side transmitted a packet correctly, but thinks that it wasn't received at all (Wireshark, 2008).

We are then directed to select capture options; specifically "Update list of packets in real-time" and "Automatically scroll during live capture". For CentOS 7.2, these were already the default options, so I made no changes.

				Wiresh	ark: Capture O	ptions	• • •
Capture							
Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Mon. Mode	Capture Filter
	virbr0 192.168.122.1	Ethernet	enabled	default	2	n/a	
	nflog	Linux netfilter log messages	enabled	default	2	n/a	
	nfqueue	Raw IPv4	enabled	default	2	n/a	
	em1	Ethernet	enabled	default	2	n/a	
0	vmnet1 172.16.185.1 fe80::250:56ff:fec0:1	Ethernet	enabled	default	2	n/a	
□ Captur ✓ Use pr	re on all interfaces romiscuous mode on all ir re Filter:	iterfaces					Manage Interfaces
Capture F	iles						Display Options
File:							Browse ✔ Update list of packets in real time
🗌 Use m	ultiple files	✔ Use pcap-ng format					Automatically scroll during live capture
Next fi	le every	megabyte(s)					III Hide capture info dialog
Ring b	uffer with 2	files					Name Resolution
	apture after	file(s)					✓ Resolve MAC addresses
Stop Capt	ure Automatically Afte	er					Resolve network-layer names
	packet(s)	$\overline{}$					☑ Resolve transport-layer name
0 1	minute(s)	$\overline{\mathbf{v}}$					☑ Use external network name resolver
🕑 Help							🚄 Start 🛛 💥 Close

I played with turning on/off those options. The results were intended to show that packets were updated in the packet frame window in real-time (no buffering) as well as enabling scrolling using the scroll bar on the right side of the screen.

# Filter Packets with the Filter Bar

Our lab now asks us to filter packets. Without filtering, it's difficult to pinpoint what exactly we're looking for because of the glut of information. By narrowing down our search scope, we can more easily find specific things. The GUI contains a "Filter" bar that allows for expressions.

#### Filtering by IP:

9

						wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
File Ed	it Viev	w Go Capture Analyze	Statistics Telephony	Tools Internals Help			
	) 🚺	📕 🔬   🖴 🛅 )	X G   Q 🗇	n 2 2 2 1			
Filter:	ip			Y Expression Clear Ap	ply Save		
No.	Time	e	Source	Destination	Protoc L	engt Info	
19157	9 1208	8,627839728	192.168.1.1	192.168.1.8	DNS	115 Standard guery response 0x3b70 AAAA 2607:f8b0:400d:c06::bd	
19159	8 1209	6.659556947	192.168.1.8	74.121.142.178	TCP	54 [TCP Keep-Alive] 54364 > http [ACK] Seq=1395 Ack=442 Win=30336 Len=0	
19159	9 1209	6.677668425	74.121.142.178	192.168.1.8	TCP	60 [TCP Keep-Alive ACK] http > 54364 [ACK] Seq=442 Ack=1396 Win=32256 Len=0	
19160	2 1209	7.835758291	173.194.66.189	192.168.1.8	TLSv1.2	127 Application Data	
19160	3 1209	7.835849335	192.168.1.8	173.194.66.189	TCP	66 50338 > https [ACK] Seq=2681 Ack=3751 Win=34560 Len=0 TSval=1554376664 TSecr=702342563	
19161	2 1210	6.707576959	192.168.1.8	74.121.142.178	TCP	54 [TCP Keep-Alive] 54364 > http [ACK] Seq=1395 Ack=442 Win=30336 Len=0	
19161	3 1210	6,720688433	74.121.142.178	192.168.1.8	TCP	60 [TCP Keep-Alive ACK] http > 54364 [ACK] Seq=442 Ack=1396 Win=32256 Len=0	
19161	6 12109	9.150363449	173.194.68.189	192.168.1.6	TLSv1.2	115 Application Data	
19161	8 1210	9.150458729	192.168.1.6	173.194.68.189	TCR	443 Destination Unreachable (Not administratively prohibited) 54 A-tiernomew, bitne (ArK) See-1980 Ark-19627 Win-6/242 Len-0	
19161	9 1210	9, 326083621	192.168.1.6	173, 194, 68, 189	TCP	54 TCP Dim ACK 191618411 4-tieronmus - https://doc.	
19162	3 1211	1.602658527	192,168,1,1	239, 255, 255, 250	SSDP	369 NOTIEV * HTTP/1.1	
19162	4 1211	1.605327335	192.168.1.1	239,255,255,250	SSDP	369 NOTIFY * HTTP/1.1	
19162	5 1211	1.605430318	192.168.1.1	239.255.255.250	SSDP	369 NOTIFY * HTTP/1.1	
19162	6 1211	1.606415584	192.168.1.1	239.255.255.250	SSDP	441 NOTIFY * HTTP/1.1	
19162	7 1211	1.606508452	192.168.1.1	239.255.255.250	SSDP	441 NOTIFY * HTTP/1.1	
19162	8 1211	1.607094203	192.168.1.1	239.255.255.250	SSDP	441 NOTIFY * HTTP/1.1	
19162	9 1211	1.607481155	192.168.1.1	239.255.255.250	SSDP	378 NOTIFY * HTTP/1.1	
19163	0 1211	1.607583062	192.168.1.1	239.255.255.250	SSDP	378 NOTIFY * HTTP/1.1	
19163	1 1211	1.608123658	192.168.1.1	239.255.255.250	SSDP	378 NOTIFY * HTTP/1.1	
19163	2 1211	1.608548335	192.168.1.1	239.255.255.250	SSDP	421 NOTIFY * HTTP/1.1	
19163	3 1211	1.608668176	192.168.1.1	239.255.255.250	SSDP	421 NOTIFY * HTTP/1.1	
19163	4 1211	1.615895771	192.168.1.1	239.255.255.250	SSDP	421 NOTIFY * HTTP/1.1	
19163	5 1211.	1.61594/369	192.168.1.1	239.255.255.250	SSUP	433 NOTEPY * HTTP/1.1	
19163	6 1211.	1.615969871	192.168.1.1	239.255.255.250	SSDP	433 NOTIFY # HTTP/1.1	
19163	9 1211	1.010991027	192.108.1.1	239.200.200.200	SSUP	433 NULET * HIP/1.1	
19163	0 1211	1.616047609	192.108.1.1	239.235.235.230	SSUP	417 NULEE * NUEZIE * 1	
19164	0 1211	1 616061420	192 168 1 1	239.255.255.250	SSDP		
19164	1 1211	1.616078783	192.168.1.1	239, 255, 255, 250	SSDP	378 NDTEY * HTTP/1.1	
19164	2 1211	1.616092470	192,168,1,1	239, 255, 255, 250	SSDP	378 NOTIFY * HTTP/1.1	
19164	3 1211	1.616105671	192,168,1,1	239,255,255,250	SSDP	378 NOTIFY * HTTP/1.1	
19164	4 1211	1.616378071	192.168.1.1	239.255.255.250	SSDP	435 NOTIFY * HTTP/1.1	
19164	5 1211	1.616416910	192.168.1.1	239.255.255.250	SSDP	435 NOTIFY * HTTP/1.1	
19164	6 1211	1.616436257	192.168.1.1	239.255.255.250	SSDP	435 NOTIFY * HTTP/1.1	
19164	7 1211	1.616450281	192.168.1.1	239.255.255.250	SSDP	435 NOTIFY * HTTP/1.1	
19164	8 1211	1.616463963	192.168.1.1	239.255.255.250	SSDP	43S NOTIFY * HTTP/1.1	
19164	9 1211	1.616478011	192.168.1.1	239.255.255.250	SSDP	435 NOTIFY * HTTP/1.1	
+ Ename	19157	79. 115 bytes on wire i	(920 hits) 115 hvt/	es cantured (920 hits)	on interface	0	
+ Ether	net II	I. Src: Actionte 20:7a:	:f7 (00:7f:28:20:7a)	f7), Dst: IntelCor 7b:	7e:64 (a0:88	:b4:7b:7e:64)	
+ Inter	net Pr	rotocol Version 4. Src:	: 192.168.1.1 (192.)	168.1.1), Dst: 192.168.	1.8 (192.168	.1.8)	
- User	Datagr	ram Protocol, Src Port:	: domain (53), Dst P	Port: 32874 (32874)			
+ Domai	in Name	e System (response)					
00000 #	10 88 b	b4 7b 7e 64 00 7f 28 3	20 7a f7 08 00 45 00	0{~d ( zE.			
0010 0	0 65 0	00 00 40 00 40 11 b7 :	2e c0 a8 01 01 c0 a8	B .e@.@			
0020 0	01 08 0	00 35 80 6a 00 51 68 4	46 3b 70 81 80 00 0	15.j.Q hF:p			
0030 0	3U U1 0 53 68 6	00 00 00 00 01 36 0e 6 61 6e 6e 65 6c 06 67 4	65 66 67 60 65 68 74 20	3			
🗎 💅 Fil	le: "/tmp	p/wireshark_pcappg_wlp2s0.	Packets: 191922 - Di	splayed: 109900 (57.3%) - C	ropped: 4915 (	2.6%)	rofile: Default

I show that I am only capturing IP packets.

## Filtering by TCP:

4			Capturing from wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - @ ×
File Edit View Go Capture Analyze Sta	atistics Telephony Tools Ir	nternals Help		
0 0 💉 🗖 🙇 🖿 🗙	C   Q 🔄 🔶 🗞	a ⊻	🔲 🔜 o o s 📅   👹 🖄 随   🕫	
Filter: tcp	Y Expr	ession Clear	Apply Save	
No. Time Source	Destination	Protoc L	engt_Info	
602 165.2303566 172.217.2.14	192.168.1.8	TLSv1.2	328 New Session Ticket, Change Cipher Spec, Hello Request, Hello Request	
603 165.2304242! 172.217.2.14	192.168.1.8	TLSv1.2	128 Application Data	
604 165.2304527 172.217.2.14	192.168.1.8	TLSv1.2	108 Application Data	
605 165.2305097(172.217.2.14	192.168.1.8	TLSv1.2	104 Application Data	
606 165.2307673 192.168.1.8	172.217.2.14	TLSv1.2	104 Application Data	
607 165.2463929:172.217.2.14	192.168.1.8	TCP	66 https > 54282 [ACK] Seq=4388 Ack=2232 Win=49408 Len=0 TSval=123096069 TSecr=1555086737	
608 165.3163411 173.194.208.189	192.168.1.8	TLSV1.2	SS7 Application Data	
610 165 3166319(192.168.1.8	1/3.194.208.189	TLEVI 2	66 44998 > nttps [ACK] Seq=343 ACK=10/4 Win=28/ Len=0 [Sval=1555086836 [Sec1=89860446/	
611 165 3165756 102 168 1 8	74 125 22 100	TCND	345 Appleation uses 1972 Partination usessibabla (Uset administrativa)u prabibitad)	_
612 165. 3257268 172. 217. 2. 14	192, 168, 1, 8	TLSv1.2	SR9 Annifestion Data	
613 165, 3258055; 172, 217, 2, 14	192,168,1,8	TLSv1.2	377 Application Data	
614 165, 3258301 172, 217, 2, 14	192,168,1,8	TLSv1.2	112 Application Data	
615 165.3263693 192.168.1.8	172.217.2.14	TCP	66 54282 > https [ACK] Seg=2232 Ack=5218 Win=46336 Len=0 TSval=1555086846 TSecr=123096149	
616 165.3264706(192.168.1.8	172.217.2.14	TLSv1.2	112 Application Data	
617 165.3827386 172.217.2.14	192.168.1.8	TCP	66 https > 54282 [ACK] Seq=5218 Ack=2278 Win=49408 Len=0 TSval=123096206 TSecr=1555086846	
618 165.3827972 173.194.208.189	192.168.1.8	TLSv1.2	506 Application Data	
619 165.3828194 192.168.1.8	173.194.208.189	TCP	66 44598 > https [ACK] Seq=343 Ack=1514 Win=296 Len=0 TSval=1555086902 TSecr=898604534	
620 165.3828461(74.125.22.189	192.168.1.6	TLSv1.2	494 Application Data	
621 165.3829000:192.168.1.8	74.125.22.189	ICMP	522 Destination unreachable (Host administratively prohibited)	
622 165.3830359 192.168.1.6	74.125.22.189	TCP	54 hetplan > https://dxhj.seq=1.ack=1258.win=55555.Len=0	
023 103.3630476.192.106.1.0	74.125.22.105	Annual Line A	Sa [10 bug ack ozzel] hetptan > hetps [kok] Sedel kok-1250 kinobood Ceneo	
+ Frame 9: 127 bytes on wire (1016 b)	ts), 127 bytes captured	(1016 bits)	on Interface 0	
+ Ethernet II, Src: Actionte_20:7a:17	(00:7f:28:20:7a:f7), D	st: IntelCor	7b:7e:64 (a0:88:b4:7b:7e:64)	
+ Internet Protocol Version 4, Src: 1	73.194.66.189 (173.194.)	55.189), DST:	192.106.1.8 (192.106.1.8) [2020] Cont J. tele J. Leve 61	
Fransmission Control Protocol, Src       Secure Secure Lawer	Port: https (443), Dst	Port: 50338 (	30338), Seq: 1, ACK: 1, Len: 51	
- Secure Suckets Layer				
0000 a0 88 b4 7b 7a 64 00 7f - 28 20	72 17 08 00 45 00	(-d ( - 6		
0010 00 71 4c 25 00 00 30 06 8c 32	ad c2 42 bd c0 a8 .gL	N02B	•	
0020 01 08 01 bb c4 a2 f1 ce a5 ed	8d d9 01 2c 80 18			
0030 01 d4 e2 5f 00 00 01 01 08 0a	29 e5 44 46 5c ad	).DF)		
0040 de as 17 03 03 00 38 00 00 00 00	de b1 28 92 11 ea+			
0060 12 1e 63 8d ef 29 1e e2 6e al	7c Od 54 ae 98 cdc	) n. .T		
0070 01 94 fb 9b 36 48 ca 3e 0b f9	44 da 50 c3 17	.6H.>D.P		
		(0.0 201)	in the set of	
Wip2su: <ive capture="" in="" progress=""> H;</ive>	Packets: 045 · Displayed: 233	(30.1%)	Pronie: Derauit	
<b>D</b> 11 <b>I D</b> 01	<b>`</b>	1.		

Filtering by TCP shows application layer data – perhaps the most interesting things I'm looking for from a cyber security perspective.

Filtering by UDP:

					Capturing from wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
File	Edit	View Go Capture Analyze Stat	tistics Telephony Tools	Internals Help		
0	۲	📶 📕 🙋 🖿 🖉 🗙	C Q	?		
Filter	udp	l.	Y Exp	pression Clear	Apply Save	
No.	T	ime Source	Destination	Protoc Le	angt Info	
2	141 3	30.3188423#192.168.1.1	192.168.1.8	DNS	103 Standard query response 0x8c59 A 74.125.22.189	
2	142 3	30.3249906(192.168.1.1	192.168.1.8	DNS	115 Standard query response 0x530a AAAA 2607:f8b0:400d:c06::bd	
2	162 3	38.6379123 0.0.0.0	255.255.255.255	DHCP	342 OHCP Discover - Transaction ID 0x86e880a5	
2	183 3	41.8940205192.108.1.8	199.223.248.98	NTP	SUINIP VERSION 4, CLENT GOINTD Version 4, server	
2	202 3	47.1371755:0.0.0.0	255,255,255,255	DHCP	342 DHCP Discover - Transaction ID 0x85e880a5	
2	219 3	50.5939849-192.168.1.6	192.168.1.1	DNS	75 Standard guery Oxabe2 A plus.google.com	
2	220 3	50.5940035-192.168.1.6	192.168.1.1	DNS	75 Standard query Oxabe2 A plus.google.com	
2	223 3	50.6157037.192.168.1.1	192.168.1.6	DNS	91 Standard query response Oxabe2 A 216.58.219.238	
2	224 3	50.6167278 192.168.1.6	192.168.1.1	DNS	75 Standard query Dx05e2 AAAA plus.google.com	
2	225 3	50.6167518 192.168.1.6	192.168.1.1	DNS	75 Standard query 0x05e2 AAAA plus.google.com	
2	260 3	55 738936210 0 0 0	255 255 255 255	DHCD	103 Standard query response 0x052 AAAA 2007:180018005.801:12008	
2	278.3	63.0553204/192.168.1.8	204.2.134.162	NTP	90 NTP Version 4. reinauction to occessional	
2	279 3	63.1590445 204.2.134.162	192.168.1.8	NTP	90 NTP Version 4, server	
2	284 3	64.6477632.0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x85e880a5	
2	303 3	73.1673782.192.168.1.8	192.168.1.1	DNS	79 Standard query 0x338e A clients6.google.com	
2	304 3	73.1674175 192.168.1.8	192.168.1.1	DNS	79 Standard query 0x13ce A clients6.google.com	
2	305 3	73.1674411:192.168.1.8	192.168.1.1	DNS	79 Standard query Oxb3d4 AAAA clients6.google.com	
2	306 3	73.2682963(192.168.1.1	192.168.1.8	DNS	119 Standard query response 0x338e CNAME clients.l.google.com A 172.217.4.206	
2	307 3	73.2732001192.168.1.1	192.168.1.8	DNS	119 Standard query response 0x12ce UNAME clients.Lgoogle.com A 172,121,42,00	
a Fer	mo 1	242 butes on vine (2226 bit	<li>a) 343 butos contuno</li>	d (2726 bitc)		
T Eth	erne:	II. Src: Apple b4:df:fl (fc	:e9:98:b4:df:f1). Dst	: Broadcast (f	in Internace of first fi	
+ Int	ernet	t Protocol Version 4, Src: 0.	0.0.0 (0.0.0.0), Dst:	255.255.255.2	35 (255,255,255,255)	
⊕ Use	r Dat	tagram Protocol, Src Port: bo	otpc (68), Dst Port:	bootps (67)		
± Boo	tstra	ap Protocol				
				-		
0000	01	11 11 11 11 11 11 12 e9 98 b4 d	1 1 08 00 45 00	E		
0020	ff	ff 00 44 00 43 01 34 79 d4 0	1 01 06 00 86 e8	.D.C.4 y		
0030	80 9	of 00 2a 00 00 00 00 00 00 0	0 00 00 00 00 00	.*	•	
0040	00 0	00 00 00 00 00 tc e9 98 b4 d	1 11 00 00 00 00	•••••		
0060	00 0		0 00 00 00 00 00			
0070	00 0	0 00 00 00 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00			
0080	00 0	0 00 00 00 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00			
0090	00 0		0 00 00 00 00 00			
00b0	00 0		0 00 00 00 00 00		-	
00c0	00 0	0 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00		•	
00000	00 0		0 00 00 00 00 00			
oofo	00 0		0 00 00 00 00 00			
0100	00 0	0 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00			
0110	00 0	00 00 00 00 63 82 53 63 3	5 01 01 37 07 01	c. Sc57.		
9 🗹	wip2s	D: <live capture="" in="" progress=""> Fi P</live>	ackets: 2338 · Displayed: 2	224 (9.6%)	Profile: Default	

Filtering by UDP shows the expected UDP applications (NTP, DNS, DHCP, NFS etc).

### Filtering by HTTP:

			Capturing from wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
File Edit View Go Capture Analyze Sta	atistics Telephony Tools	internals Help	lp	
0 0 💉 🗖 🙇 🗎 🗎 X	C   Q> 3			
Filter: http	V Exp	ression Clea	ear Apply Save	
No. Time Source	Destination	Protoc	Lengt Info	
1503 237.5440006 192.168.1.6	104.236.93.174	HTTP	408 GET /UticaCollege/ HTTP/1.1	
1504 237.5440154 192.168.1.6	104.236.93.174	HTTP	408 [TCP Retransmission] GET /UticaCollege/ HTTP/1.1	
1515 237.5762876(192.168.1.6	104.236.93.174	HTTP	408 GET /Uticacollege/ HTTP/1.1	_
1516 237.5763010 192.168.1.6	104.236.93.174	HTTP	408 (TCP Retrainsmission) Cel /Ottcacottege/ HTP/I.1 408 (CT /Uticacotlege/ HTTP/I.1	
1528 237.6087573 192.168.1.6	104.236.93.174	HTTP	406 [TCP Retransmission] GET /UticaCollege/ HTTP/1.1	
1538 237.6458461 192.168.1.6	104.236.93.174	HTTP	408 GET /UticaCollege/ HTTP/1.1	
1539 237.6458688:192.168.1.6	104.236.93.174	HTTP	408 [TCP Retransmission] GET /UticaCollege/ HTTP/1.1	
1541 237.6735202(104.236.93.174	192.168.1.6	HTTP	4237 MTTP/1.1 200 OK (text/html) AEE (Cf. Groep (d) abs aff HTTP(1)	
1545 237.7657324 192.168.1.6	104.236.93.174	HTTP	455 (F) Petransmission] GET /icons/blank.gif HTTP/1.1	
1546 237.7802221 104.236.93.174	192.168.1.6	HTTP	263 HTTP/1.1 304 Not Modified	
1547 237.7907979:192.168.1.6	104.236.93.174	HTTP	454 GET /icons/back.gif HTTP/1.1	
1548 237.7908190 192.168.1.6	104.236.93.174	HTTP	454 [TCP Retransmission] GET /icons/back.gif HTTP/1.1	
1551 237.8078379 104.236.93.174	192.168.1.6	HITP	263 HTTP/1.1 304 Not Modified	
1556 237.8091594 192.168.1.6	104.236.93.174	HTTP	457 GET /ICONS/IMAGE2.geT MTP/III 457 [TCP Retransmission] GET /icons/image2.gif HTTP/1.1	
1559 237.8254951(104.236.93.174	192.168.1.6	HTTP	264 HTTP/1.1 304 Not Modified	
1564 239.2700034 192.168.1.6	104.236.93.174	HTTP	448 GET /UticaCollege/NetworkTest8.png HTTP/1.1	
1565 239.2700384(192.168.1.6	104.236.93.174	HTTP	448 [TCP Retransmission] GET //ticacollege/NetworkTest8.png HTTP/1.1	
1661 229 42246611104 226 92 174	104.230.93.174	LUNE	Security(1) 200 (M (DMC)	
	Lite) 400 huter cost	and (const hi		
<ul> <li>Frame 1503: 408 bytes on wire (3204)</li> <li>Ethernet II. Src: IntelCor 7h:7e:64</li> </ul>	(a0:88:64:76:70:64). [	Det: Actionte	bits) on interface 0 + 20/2a/f2 (0n/f2 (20/2a/f2)	
Internet Protocol Version 4, Src: 1	92.168.1.6 (192.168.1.6	5), Dst: 104.	4_236.93.174 (104.236.93.174)	
Transmission Control Protocol, Src	Port: stonefalls (2986)	, Dst Port:	: http (80), Seq: 1, Ack: 1, Len: 354	
Hypertext Transfer Protocol				
0000 00 7f 28 20 7a f7 a0 88 b4 7b	7e 64 08 00 45 00	(z{~d		
0010 01 8a 20 a2 40 00 80 06 50 83	c0 a8 01 06 68 ec	.@ P		
0030 fa f0 54 64 00 00 47 45 54 20	2f 55 74 69 63 611	rdGE T /Uti	tica	
0040 43 6f 6c 6c 65 67 65 2f 20 48	54 54 50 2f 31 2e Col	llege/ HTTP/	P/1.	
0050 51 00 0a 48 61 73 74 5a 20 64 0060 66 66 73 6f 63 6b 6f 2e 63 6f	6d 0d 0a 55 73 65 ff:	socko. coml	5.01 .Use	
0070 72 2d 41 67 65 6e 74 3a 20 4d	6f 7a 69 6c 6c 61 r-/	Agent: Mozil	illa	
0090 20 35 2e 31 3b 20 72 76 3a 34	38 2e 30 29 20 47 5.	.1; rv :48.0)		
00a0 65 63 6b 6f 2f 32 30 31 30 30	31 30 31 20 46 69 ec	0/201 00101	1 Fi	
00c0 70 74 3a 20 74 65 78 74 2f 68	74 6d 6c 2c 61 70 pt:	text /html.	Acce	
00d0 70 6c 69 63 61 74 69 6f 6e 2f	78 68 74 6d 6c 2b pli	catio n/xhtm	tul+	
00e0 78 6d 6c 2c 61 70 70 6c 69 63 00f0 78 6d 6c 3b 71 3d 30 2e 39 2c	61 74 69 61 6e 2f xm 2a 2f 2a 3h 71 3d xm	l,appl icatio	10n/ * am	
0100 30 2e 38 0d 0a 41 63 63 65 70	74 2d 4c 61 6e 67 0.1	BAcc ept-La	Lang	
0110 75 61 67 65 3a 20 65 6e 2d 55	53 2c 65 6e 3b 71 ua	ge: en ∘US,er	autid	
wip2s0: <iive capture="" in="" progress=""> F;</iive>	Packets: 3308 · Displayed: 1	34 (4.1%)	Profile: Default	
E 1 (1 )	77 1	41	$\mathbf{I} \mathbf{I} \mathbf{I} \mathbf{I} \mathbf{I} \mathbf{I} \mathbf{I} \mathbf{I} $	1 1

Filtering by "http" shows mostly http traffic. I did encounter an ICMP packet with this filter enabled, which was kind of weird. I have no explanation for this.

## Specifying an IP address:

4	Capturing from wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
File Edit View Go Capture Analyze Statistics Telephony Tools Internals	Help	
● ● 🛋 ■ 🙇   🖿 🗎 × C   Q 🖑 → 🌣 👼	2   🔲 🖬 🗠 🗉 🖉   👪 🕷 🖲   🗃	
Filter: ip.addr == 192.168.1.2	Clear Apply Save	
No. Time Source Destination Pro	toc Lengt Info	
56 21.80676890:192.168.1.2 224.0.0.22 IGM	Pv3 54 Membership Report / Join group 239.255.255.250 for any sources	
1841 273.3031926 192.168.1.2 224.0.0.22 IGM	Pv3 54 Membership Report / Join group 239.255.250 for any sources	
2659 397.5163758-192.168.1.2 224.0.0.22 IGM	Pv3 54 Membership Report / Join group 239.255.255.250 for any sources	
3824 524.6972574192.168.1.2 224.0.0.22 IGM	Pv3 54 Membership Report / Join group 239.255.255.250 for any sources	
4882 647.3735179-192.168.1.2 224.0.0.22 IGM	Pv3 54 Membership Report / Join group 239.255.255.250 for any sources	

Frame 552: 54 bytes on vire (432 bits). 54 bytes captured (432 bits) on interface 0 Ethernet II, Scr. Attointe, 76:0300 (10:97:03976:03)090). Doi:101:00109:0000016) (01:0019:0000016)								
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 224.0.0.22 (224.0.0.22)								
: Internet Urbup Management Protocol								
0000 01 00 5e 00 00 16 10 9f a9 76 30 90 08 00 46 c0v0F.								
0010 00 28 00 00 40 00 10 22 42 4f c0 a8 01 02 e0 00								
0030 00 00 ef ff ff fa								
● 💆 wp2s0: <live capture="" in="" progress=""> Fi; Packets: 5228 - Displayed: 6 (0.1%)</live>	Profile: Default							
When filtering by IP address, I narrow down the packets that have as a source or destination the								

When filtering by IP address, I narrow down the packets that have as a source or destination the specified IP address.

## View Packet Summaries with the Packet List Window

The packet frame in the below picture shows a number of columns.

Column 1 – shows the packet number

Column 2 - shows the time in a number of formats. In the example below, I have chosen the number of seconds since the live capture began. It is accurate to the nanosecond.

Column 3 - is the source IP address (where the packet is coming from)

Column 4 - is the destination IP address (where the packet is going to)

Column 5 - is the protocol

Column 6 - is the length of the packet

Column 7 - is information associated with the packet.

12

			Capturing from	wlp2s0 [V	Wireshark 1.10.14 (Git Rev Unknown from unknown)]	+ - = ×
File	Edit View	Go Capture Analyze Sta	atistics Telephony Tools	Internals H	ielp	
			/ <b>O</b> / S			
				v ~~		
Filte	er:	Save this capture t	file 🗸 🗸 Exp	oression C	Clear Apply Save	
No.	Time	Source	Destination	Protoc	c Lenat Info	
	29 6.15714	42550 192.168.1.1	192.168.1.8	DNS	97 Standard query response 0x19cc A 54.174.160.96	
	30 6.16408	86067 192.168.1.1	192.168.1.8	DNS	97 Standard query response Oxddf8 A 54.174.160.96	
	31 6.16880	01970 192.168.1.1	192.168.1.8	DNS	139 Standard query response 0xc332	
	32 6.17076	65915 54.174.160.96	192.168.1.8	TCP	66 http > 54896 [ACK] Seq=1 Ack=546 Win=19456 Len=0 TSval=705842859 TSecr=52300	157
	33 6.20942	20859 54.174.160.96	192.168.1.8	TCP	660 [TCP segment of a reassembled PDU]	
	34 6.20950	06252 192.168.1.8	54.174.160.96	TCP	66 54896 > http [ACK] Seq=546 Ack=595 Win=30464 Len=0 TSval=52300210 TSecr=7058	42868
	35 6.21234	47944 54.174.160.96	192.168.1.8	HTTP	66 HTTP/1.1 200 OK (application/json)	7050 40000
	36 6.21883	39093 192.168.1.8	54.174.160.96	TCP	66 54896 > NTTP [FIN, ACK] Seq=546 ACK=596 Win=30464 Len=0 ISVal=52300220 ISecr	=/05842868
	39 7 07159	20429 Actionte 20:7a:f7	Broadcast	ARD	42 Who have 102 169 1 112 Tall 102 169 1 1	00220
	39.8.09553	39587 Actionte 20:7a:f7	Broadcast	ARP	42 Who has 192.168.1.11? Tell 192.168.1.1	
	40 8.66924	46045 192.168.1.14	104.236.93.174	TCP	55 [TCP segment of a reassembled PDU]	
	41 8.66926	59222 192.168.1.14	104.236.93.174	TCP	55 [TCP Keep-Alive] abatjss > http [ACK] Seq=1 Ack=1 Win=65535 Len=1	
	42 8.68142	27236 104.236.93.174	192.168.1.14	TCP	66 http > abatjss [ACK] Seq=2 Ack=2 Win=15544 Len=0 SLE=1 SRE=2	
	43 8.68150	08839 192.168.1.8	104.236.93.174	ICMP	94 Destination unreachable (Host administratively prohibited)	
	44 9.01723	39907 Actionte_20:7a:f7	Broadcast	ARP	42 Who has 192.168.1.11? Tell 192.168.1.1	
	45 14.0348	36130(Actionte_20:7a:17	Broadcast	ARP	42 Who has 192.168.1.11? Tell 192.168.1.1	
			Broadcast	01313		
_	46 15.0594	48587. Actionte_20:74:17	Dioddedae	ANP	42 Who has 192.168.1.11? Tell 192.168.1.1	
Er Er	46 15.0594	vtes on wire (336 bits	). 42 bytes captured (1	ARP 336 bits) (	42 who has 192.168.1.11? Tell 192.168.1.1	
Fr     Ft	ame 1: 42 b	oytes on wire (336 bits Src: Actionte 20:7a:17	), 42 bytes captured (3 (00:7f:28:20:7a:f7), [	336 bits) o Ost: Broado	42 Who has 192.168.1.11? Tell 192.168.1.1 on interface O cast (ff:ff:ff:ff:ff)	
+ Fr + Et + Ad	ame 1: 42 b hernet II,	ytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques	), 42 bytes captured (: (00:7f:28:20:7a:f7), [ t)	336 bits) o Dst: Broado	42 WRO NAS 192.108.1.117 Tett 192.108.1.1 on interface O Cast (ff:ff:ff:ff:ff:ff:ff)	_
+ Fr + Et + Ad	ame 1: 42 b hernet II, dress Resol	ytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques	), 42 bytes captured (: (00:7f:28:20:7a:f7), [ t)	336 bits) o Dst: Broado	a2 who has 192.108.1.11? Tell 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Fr + Et + Ad	ame 1: 42 b hernet II, dress Resol	vytes on wire (336 bits Src: Actionte_20:7a:f7 ution Protocol (reques	), 42 bytes captured (3 (00:7f:28:20:7a:f7), [ t)	336 bits) o Dst: Broado	az who has 192.108.1.117 Tell 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Fr + Et + Ad	ame 1: 42 b hernet II, dress Resol	HSSB7.Actionte_20:74:17 Nytes on wire (336 bits Src: Actionte_20:7a:f7 Lution Protocol (reques	), 42 bytes captured (: (00:7f:28:20:7a:f7), [ t)	336 bits) o Ost: Broado	42 WRO NAS 192.108.1.11? Tell 192.108.1.1 on interface O cast (ff:ff:ff:ff:ff:ff)	
+ Fr + Et + Ad	ame 1: 42 b hernet II, dress Resol	HOSDY,ACTIONEE_20:74:17 hytes on wire (336 bits Src: Actionte_20:7a:17 ution Protocol (reques	), 42 bytes captured (? (00:7f:28:20:7a:f7), [ t)	336 bits) o Ost: Broadd	42 WHO has 192.108.1.117 Tell 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Et	ame 1: 42 b hernet II, dress Resol	Hose, Actionte_20:74:17 pytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques	), 42 bytes captured (? (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	a2 who has 192.108.1.11? Tell 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Et	ame 1: 42 b hernet II, dress Resol	Hoso, Actionte_20:74:17 Nytes on wire (336 bits Src: Actionte_20:7a:f7 Lution Protocol (reques	), 42 bytes captured (; (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	42 WRO NAS 192.108.1.11? Tett 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Et + Ad	ame 1: 42 b hernet II, dress Resol	Hoss, Actionte_20:74177 Nytes on wire (336 bits Src: Actionte_20:7a:f7 Lution Protocol (reques	), 42 bytes captured () (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	42 WRO has 192.108.1.11 on interface O cast (ff:ff:ff:ff:ff:ff)	
+ Et + Ad	ame 1: 42 b hernet II, ddress Resol	Hose, Actionte_20:7417 pytes on wire (336 bits Src: Actionte_20:7a:f7 ution Protocol (reques	), 42 bytes captured ( (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	42 who has 192.108.1.117 Tell 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Et + Ad	ame 1: 42 b hernet II, dress Resol	vytes on wire (336 bits Src: Actionte_20:7a:f7 ution Protocol (reques	), 42 bytes captured (; (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	42 WRO NAS 192.108.1.11 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
+ Et + Ad	ame 1: 42 b hernet II, ddress Resol	vytes on wire (336 bits Src: Actionte_20:7a:f7 ution Protocol (reques	), 42 bytes captured (; (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	42 WRO has 192.108.1.11 on interface O cast (ff:ff:ff:ff:ff:ff)	
+ Et + Ad	ame 1: 42 b hernet II, ddress Resol	Nytes on wire (336 bits Src: Actionte_20:7a:f7 ution Protocol (reques	), 42. bytes captured () (00:7f:28:20:7a:f7), [ t)	336 bits) ( Dst: Broadd	42 who has 192.108.1.11 on interface O cast (ff:ff:ff:ff:ff:ff)	
+ Fr + Et + Ad	ame 1: 42 b hernet II, ddress Resol	<pre>system on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques) ff ff ff ff 00 7f 28 20</pre>	<pre>2,000001 ), 42 bytes captured (: (00:7f:28:20:7a:f7), [ t) 7a f7 08 06 00 01</pre>	336 bits) ( Ost: Broadd	42 WRO NAS 192.108.1.11? Tett 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
• Fr + Et + Ad	ame 1: 42 b chernet II, dress Resol	ff ff ff 00 7f 28 20 04 00 01 00 7f 28 20	7a f7 06 06 00 01 7a f7 c0 a8 01 01	ACP 336 bits) ( Jst: Broado 	42 WRO NAS 192.108.1.11? Tett 192.108.1.1	
0000 0010 0020	46 13.0342 ame 1: 42 b hernet II, dress Resol	HSS97, ACCIDATE_20:74177 hytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques ff ff ff ff 00 7f 28 20 04 00 01 00 7f 28 20 00 00 00 c0 a8 01 6b	7a f7 08 06 00 01	Ange 336 bits) ( Dst: Broadd ( z ( z	42 WRO has 192.108.1.11? Tett 192.108.1.1	
• Fr • Et • Ad	46 15,0342 ame 1: 42 b hernet II, idress Resol	ff ff ff 00 7f 28 20 00 00 00 cc a8 01 0b	<pre>// 22 bytes captured (: (00:7f:28:20:7a:f7), [ ) // 28:20:7a:f7), [ // 28:20:7a:f7), [ // 28:20:7a:f7], [ // 28:20:7a:f7],</pre>	Ary 336 bits) ( Dst: Broade	42 WRO NAS 192.108.1.11? Tett 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
• Fr • Et • Ad	46 15,0342 ame 1: 42 b thernet II, ddress Resol	Hoso, Actionte_20:7417 ytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques ff ff ff ff 00 7f 28 20 04 00 01 00 7f 28 20 00 00 00 c0 a8 01 ob	7a f7 08 06 00 01	Ary 336 bits) ( Dst: Broadd	42 WRO NAS 192.108.1.11 on interface 0 cast (ff:ff:ff:ff:ff:ff)	
<ul> <li>€ Fr</li> <li>⊕ Et</li> <li>⊕ Ad</li> <li>00000</li> <li>0010</li> <li>0020</li> </ul>	46 13.0322 ame 1: 42 b hernet II, dress Resol	HSS97, ACTIONEE_20:74177 hytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques ff ff ff ff 00 7f 28 20 04 00 01 00 7f 28 20 00 00 00 c0 a8 01 0b	7a f7 08 06 00 01 7a f7 c0 a8 01 01 	Ang- 336 bits) ( Dst: Broadd	42 who has 192.108.1.11? Tett 192.108.1.1	
<ul> <li>+ Fr</li> <li>+ Et</li> <li>+ Ad</li> <li>0000</li> <li>0010</li> <li>0020</li> </ul>	40 15,0342         ame 1: 42 b         whernet II,         ddress Resol         0 ff ff ff         0 08 00 06         0 00 00 00	Hoss, Actionte_20:7417 ytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques ff ff ff 00 7f 28 20 04 00 01 00 7f 28 20 00 00 00 c0 a8 01 0b	7a f7 08 06 00 01	Arr 336 bits) ( Dst: Broade	42 WRO has 192.108.1.11? Tett 192.108.1.1	
<ul> <li>● Fr</li> <li>● Et</li> <li>● Ad</li> <li>00000</li> <li>0010</li> <li>0020</li> </ul>	46 15,0342 ame 1: 42 b thernet II, dress Resol	HSS97,ACCIONCE_20:74177 ytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques ff ff ff ff 00 7f 28 20 04 00 01 00 7f 28 20 00 00 00 c0 a8 01 ob	7a f7 08 06 00 01 7a f7 c0 a8 01 01	Ary 336 bits) ( Dst: Broadd	42 WRO NAS 192.108.1.11? Tett 192.108.1.1	
<ul> <li>● Fr</li> <li>● Et</li> <li>● Ad</li> <li>00000</li> <li>0010</li> <li>0020</li> </ul>	48 13,0392         ame 1: 42 b         chernet II,         ddress Resol         0 ff ff ff ff         0 08 00 06         0 00 00 00	ff ff ff 00 7f 28 20 00 00 00 c0 a8 01 0b	7a f7 06 06 00 01	Any 336 bits) ( Dst: Broadd	42 WRO NAS 192.108.1.11? Tett 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff:ff)	
• Fr • Et • Ad	46 13.0322 ame 1: 42 b hernet II, idress Resol 0 6f ff ff ff 0 08 00 66 0 00 00 00	Hoss, Actionte_20:7417 pytes on wire (336 bits Src: Actionte_20:7a:f7 .ution Protocol (reques ff ff ff ff 00 7f 28 20 00 00 00 c0 a8 01 0b ne), 42 bytes	<pre>2, 42 bytes captured (: (00:7f:28:20:7a:f7), [ (00:7f:28:20:7a:f7), [ ) 7a f7 08 06 00 01  7a f7 c0 a8 01 01  Packets: 46 · Displayed: 46 (</pre>	Arp 336 bits) ( Dst: Broadd (z (z (z (z (z (z (z (z (z (z	a 2 who has 192.108.1.11? Tett 192.108.1.1 on interface 0 cast (ff:ff:ff:ff:ff:ff:ff) 	

# Study Packet Details with the Packet Details Window

By highlighting a packet in the packet summary window, you can view further information about that packet in the packet details frame.

Here are some of the details of an ARP packet:

		Capturing from w	p2s0 [Wire	shark 1.10.14 (Git Rev Unknown from unknown)]		+ - • ×
File Edit View C	io Capture Analyze Statis	tics Telephony Tools Int	ernals Help			
• • .	📕 🙇   🖪 🛅 🗙 🤇	3   <b>Q</b> 📀 📎 🗞	⊼ ⊻	III 🛛 🖛 III 🖬 🖬 🔛	0	
Filter:		Y Expres	sion Clear	Apply Save		
No. Time	Source	Destination	Protoc Le	engt Info		
31321 12774.73	3351 Actionte 20:7a:f7	Broadcast	ARP	42 Who has 192.168.1.11? Tell 192.168.1.1		
31322 12777.2	7282 Actionte 20:7a:f7	IntelCor 7b:7e:64	ARP	42 Who has 192.168.1.8? Tell 192.168.1.1		
31323 12777.2	7288:IntelCor 7b:7e:64	Actionte 20:7a:f7	ARP	42 192.168.1.8 is at a0:88:b4:7b:7e:64		
31324 12779.72	2358 Actionte 20:7a:f7	Broadcast	ARP	42 Who has 192.168.1.11? Tell 192.168.1.1		
31325 12780.72	2348(Actionte 20:7a:f7	Broadcast	ARP	42 Who has 192.168.1.11? Tell 192.168.1.1		
31326 12781.04	4614:fe80::129f:a9ff:fe70	5::ff02::1	ICMPv6	90 Multicast Listener Query		
31327 12781.05	5266:fe80::a288:b4ff:fe7k	::ff02::16	ICMPv6	90 Multicast Listener Report Message v2		
🖃 Frame 31301: 4	2 bytes on wire (336 bit	ts), 42 bytes captured	(336 bits)	on interface O		1
Interface id	: 0					
Encapsulatio	n type: Ethernet (1)					
Arrival Time	: Oct 3, 2016 17:21:43.	275218512 EDT				
[Time shift	for this packet: 0.00000	00000 seconds]				
Epoch Time:	1475529703.275218512 sec	conds				
[Time delta	from previous captured f	rame: 0.432126441 seco	nds]			
[Time delta	from previous displayed	frame: 0.432126441 sec	onds]			
Time since	reference or first frame	: 12760.733404443 seco	ndsl			
Frame Number	: 31301					
Frame Length	: 42 bytes (336 bits)					
Capture Lend	th: 42 bytes (336 bits)					
[Frame is ma	rked: Falsel					
[Frame is id	nored: Ealsel					
[Protocols i	n frame: eth:arn]					
[Coloring B	le Name: ARP]					
[Coloring R	le String: arnl					
- Ethernet II	Src: Actionte 20:7a:f7 ((	0.7f.28.20.7a.f7) Dst	• Broadcast	(ff.ff.ff.ff.ff.ff)		
Ethermotion:	Broadcast (ff:ff:ff:ff:	(ff.ff)	. Droddedde	(		
E Source: Acti	onte 20.7a.f7 (00.7f.28	20.7a.f7)				
Type: ARP (C	x0806)	201741177				
- Address Besolu	tion Protocol (request)					
Hardware typ	e: Ethernet (1)					
Protocol typ	e: TP (0x0800)					
Hardware siz	e: 6					
Protocol siz	e: 4					
Protocol siz	e: 4 f ff ff 00 7f 28 20 7a	f7 08 06 00 01	( z	•		
0020 00 00 00 00	00 00 00 c0 a8 01 0b	T7 C0 a8 01 01	( z			
🔵 💅 Frame (frame	), 42 bytes Pac	kets: 31381 · Displayed: 31	381 (100.0%)		Profile: Default	

And here are some of the details of a TCP packet:

Capturing from wlp2s0 [Wireshark 1.10.14 (Git Rev Ur	known from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	
● ● <u>▲</u> ■ <u>&amp;</u>   ■ 🗎 × C   Q 🤄 → 🌣 주 ⊻   🗏 🖬 O 🗆 0	
Filter: Expression Clear Apply Save	
No. Time Source Destination Protoc Lengt Info	
31331 12781.70050 192.168.1.14 104.236.93.174 TCP 55 [TCP Keep-Alive]	abatjss > http [ACK] Seq=1 Ack=1 Win=65535 Len=1
31332 12781.70052(192.168.1.14 104.236.93.174 TCP 55 [TCP Keep-Alive]	abatjss > http [ACK] Seq=1 Ack=1 Win=65535 Len=1
31333 12/81./1394 104.236.93.1/4 192.168.1.14 TCP 66 [TCP Keep-Alive A	ck] http > abat]ss [ACK] seq=2 Ack=2 win=15544 Len=0 SLE=1 SHE=2 chable (Host administratively prohibited)
31335 12781.72360(Actionte_20:7a:f7 Broadcast ARP 42 Who has 192.168.1	.11? Tell 192.168.1.1
31336 12782.11086/fe80::d203:4bff:fed0::ff02::16 ICMPv6 130 Multicast Listene	r Report Message v2
Time shift for this packet: 0.000000000 seconds]	
Epoch Time: 1475529724.255762553 seconds	
[Time delta from previous captured frame: 0.013421584 seconds]	
[Time delta from previous displayed frame: 0.013421584 seconds]	
Frame Number: 31333	
Frame Length: 66 bytes (528 bits)	
Capture Length: 66 bytes (528 bits)	
[Frame is ignored: False]	
[Protocols in frame: eth:ip:tcp]	
[Coloring Rule Name: Bad TCP]	
[Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update] Etherpet II. Src: Actionto 20.72.f7 (00.7f:20.20.72.f7). Det: IntelCor.7b.70.64 (20.00.b4.7b.	70.64)
□ Destination: IntelCor 7b:7e:64 (a0:88:b4:7b:7e:64)	76.04)
Address: IntelCor_7b:7e:64 (a0:88:b4:7b:7e:64)	
O default)	
Address: Actionte 20:7a:f7 (00:7f:28:20:7a:f7)	
0 = LG bit: Globally unique address (factory default)	
Type: 1P (0x0800) Thternet Protocol Version 4, Src: 104.236.93.174 (104.236.93.174), Dst: 192.168.1.14 (192.168)	. 1. 14)
Version: 4	
0000 a0 88 b4 7b 7e 64 00 7f 28 20 7a f7 08 00 45 00{~d (zE.	
0010 00 34 d2 a5 40 00 38 06 e7 cd 68 ec 5d ae c0 a8 .4@.8h.]	
0020 01 0e 00 50 0e 48 3d 92 27 e2 e7 66 a0 f2 80 10P.H=. 'f 0030 3c b8 a7 9c 00 00 01 01 05 0a e7 66 a0 f1 e7 66 <ff< td=""><th></th></ff<>	
0040 a0 f2	
🛑 💆 Time delta from previous displayed f   Packets: 32160 · Displayed: 32160 (100.0%)	Profile: Default

The information in the packets differs. Obviously the protocol is labeled differently, but also things like frame length, payload and the TCP packet gives information about what version it's using.

## View Packet Data with the Individual Packet Bytes Window

Using the above examples, the Packet Bytes window is the bottom frame. The data held in the packet bytes window is different because both packets are different. The same as opening a file in a hex editor, the hexadecimal representation is on the left side of the frame, and its ASCII representation is on the right side of the frame. There is a period (".") for hexadecimal information that does not have ASCII characters associated with it.

## **Browse The Internet**

Filter on ip.addr==192.168.1.8 and http., visit htto://www.google.com and perform a search on scurvy



🛱 Frame 308: 812 bytes on wire (6496 bits), 812 bytes captured (6496 bits) on interface O	
Ethernet II, Src: Actionte_20:7a:f7 (00:7f:28:20:7a:f7), Dst: IntelCor_7b:7e:64 (a0:88:b4:7b:7e:64)	
+ Internet Protocol Version 4, Src: 172.217.4.78 (172.217.4.78), Dst: 192.168.1.8 (192.168.1.8)	
🗄 Transmission Control Protocol, Src Port: http (80), Dst Port: 34764 (34764), Seq: 1, Ack: 430, Len: 746	
Hypertext Transfer Protocol	
E HTTP/1.1 200 0K\r\n	
E[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]	
Request Version: HTTP/1.1	
Status Code: 200	
Response Phrase: OK	
Content-Type: application/ocsp-response\r\n	
Date: Mon, 03 Oct 2016 04:29:47 GMT\r\n	
Expires: Fri, 07 Oct 2016 04:29:47 GMT\r\n	
Cache-Control: public, max-age=345600\r\n	
Server: ocsp_responder\r\n	
□ Content-Length: 463\r\n	
[Content length: 463]	
X-XSS-Protection: 1; mode=block\r\n	
X-Frame-Options: SAMEORIGIN/r\n	
\r\n	
[HTP response 1/1]	
[Time since request: 0.033453056 seconds]	
[Request in frame: 306]	
🗄 Online Certificate Status Protocol	
0000 a0 88 b4 7b 7e 64 00 7f 28 20 7a 17 08 00 45 00(+d (zE.	- 1
0040 33 8b 48 54 50 2f 31 20 31 20 32 30 30 20 4f 3.HTTP/1 .1 200 0	
0050 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a KConte nt-Type:	
0060 20 61 / 0 76 59 63 61 /4 69 61 66 21 61 63 /3 application/cos	
0090 31 35 20 30 34 3a 32 39 3a 34 37 20 47 4d 54 0d 16 04:29 :47 0MT.	
00a0 0a 45 78 70 69 72 65 73 3a 20 46 72 69 2c 20 30 .Expires : Fri, 0	
	_

When this action was performed, I found that Google redirected to https – port 443. I then changed my filter to ip.addr==192.168.1.8 and tcp.pprt==443:

				*wlp2s0	s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	+ - = ×
File	Edit View Go Canture Analyze Stal	tistics Telephony Tools	Internals Help			
0	) 💿 🚄 🔳 🔬   🖿 🛅 🗙	G   <b>Q</b> 🗇 🚸 🖇	\$ \$ ¥		o 🖭   👹 🔀 🐻   🕫	
Filte	ip.addr==192.168.1.8 and tcp.port==4	143 👻 Exp	pression Clea	ar Apply Save		
lo.	Time Source	Destination	Protoc Le	engt Info		
2	96 22,12203145 216,58,217,228	192.168.1.8	ILSV1.2	112 Application Data		
2	97 22.12213277 192.168.1.8	216.58.217.228	TCP	66 42134 > https [ACK]	X] Seq=6663 Ack=140501 Win=1557 Len=0 TSval=4995581 TSecr=3265230310	
2	98 22.12222514 192.168.1.8	216.58.217.228	TLSv1.2	112 Application Data		
2	99 22.15137683 216.58.217.228	192.168.1.8	TCP	66 https > 42134 [ACK]	X] Seq=140501 Ack=6709 Win=677 Len=0 TSval=3265230341 TSecr=4995581	
3	00 22.40566724 192.168.1.8	216.58.217.228	TLSv1.2	404 Application Data		
3	01 22.40930721:192.168.1.8	216.58.217.228	TLSv1.2	347 Application Data		
3	02 22.43639471/216.58.217.228	192.168.1.8	TCP	66 https > 42134 [ACK]	X] Seq=140501 Ack=7047 Win=693 Len=0 TSval=3265230626 TSecr=4995865	
3	03 22.43921695 216.58.217.228	192.168.1.8	TCP	66 https > 42134 [ACK]	X] Seq=140501 Ack=7328 Win=709 Len=0 TSval=3265230628 TSecr=4995868	
3	04 22.44684873 216.58.217.228	192.168.1.8	TLSv1.2	112 Application Data		
3	05 22.44698620(216.58.217.228	192.168.1.8	TLSV1.2	104 Application Data		
3	06 22.44702502 192.168.1.8	216.58.217.228	TOP	66 42134 > https [ACK]	K] Seq=/328 ACK=140585 W1n=155/ Len=0  5val=4995906  5ecr=3265230634	
3	07 22.44746509(216.58.217.228	192.168.1.8	TLSV1.2	112 Application Data		
-	08 22.44730085.192.108.1.8	210.58.217.228	TLSVI.2	100 Application Data		
-	03 22.4302/312.132.100.1.0	102 169 1 9	TCD	se bttos > 42124 [ACK]	X] CAR-140531 Ack-7507 Min-775 LAD-0 TSUA-205520055 TSACE-4005007	
	11 22 49120505 216 59 217 228	192.168.1.8	TLSv1 2	116 Application Data	13 364-140031 Mrk=1301 MTH=153 FBH=0 13481-350350000 1361-4033801	
	12 22, 48217590 216, 58, 217, 228	192,168,1,8	TLSv1.2	711 Application Data		
3	13 22.48225422 192.168.1.8	216.58.217.228	TCP	66 42134 > https [ACK]	Τζ] Seg=7507 Ack=141326 Win=1579 Len=Ο TSval=4995941 TSecr=3265230671	
3	14 22.484027841216.58.217.228	192.168.1.8	TLSv1.2	315 Application Data		
3	15 22.48419612(216.58.217.228	192.168.1.8	TLSv1.2	112 Application Data		
_						
⊡ Fr	ame 312: 711 bytes on wire (5688 b	its), 711 bytes captu	red (5688 bit	ts) on interface O		
	Interface id: 0					
	Encapsulation type: Ethernet (1)					
	Arrival Time: Oct 3, 2016 00:40:4	4.482115333 EDT				
	[Time shift for this packet: 0.000	000000 seconds]				
	Epoch 11me: 14/5469644.482115333 s	econds	d1			
	[Time delta from previous captured	frame: 0.000/89956 s	econasj			
	Time decta from previous displaye	d Trame: 0.000/89956	secondsj			
	Erame Number: 212	me. 22.4821/3909 Seco	nus (			
	Frame Langth: 711 bytag (5600 bits	1				
	Capture Length: 711 bytes (5688 bi	ts)				
	[Frame is marked: False]	6.07				
0000	a0 88 b4 7b 7e 64 00 7f 28 20 7	a f7 08 00 45 00	.{~d ( z	E.		
0010	0 02 b9 20 3c 00 00 3a 06 ea 33 d	18 3a d9 e4 c0 a8	<:3.:			
0020	) 01 08 01 bb a4 96 f1 ef 0b 7f f	9 5c 3d bb 80 18				
0030	0 02 d5 78 a9 00 00 01 01 08 0a c	2 91 77 41 00 4c	xwc	).L		
0050	1 53 6d 96 60 18 94 6f aa 76 6d 3	1 1b a0 a2 0c c3 5m	` o vml			
0060	) 9d bb 43 0a ee 51 ac 15 0e 54 f	c 92 26 f2 40 7c	CQT&.			
0070	) a5 b3 e3 b8 fb 8e 8b b7 24 26 3	id cb a0 78 47 77	\$&=>	Gw		
0080	) ad 30 d6 db 32 33 †3 50 7b 86 1	5 54 fb ee 25 34 .0	)23.P {T	.%4		
0090	) e5 05 15 11 /0 /1 80 16 20 /0 e ) la c5 bc e8 ea 2a 05 a5 lc 0d 4	19 bn do fc 21 4c	* T			
oobo	) cc c6 03 fb ff 3a b7 62 ca 25 d	1 71 f8 30 c9 31	:.b .%.q.0	0.1		
00c0	) ec ae 58 50 63 a9 21 82 d2 75 9	6 f5 Oa 2e 1e b9	XPc.!u			
obdo	) ee 55 ee 2a 34 †7 8e a8 28 3d e	1 34 67 f2 10 64 .U	J.*4 (=.4g.	. d		
oof	) b2 5f 7f 95 37 0e 31 44 bd bf f	7 de 44 8b 89 2b	-7.1D D	+		
0100	d5 1c b9 30 63 ad 1a e5 c0 14 1	3 d7 38 b3 e2 91	.0c8.			
0110	77 c0 35 92 1f 36 b6 2c 44 9d 5	b c7 9d d5 aa 48 w.	56., D.[	.H		
0120	0 e5 87 3b †3 bl e8 7c 9a ff Oe 1	2 63 09 23 69 70	; c.#	f1p		
0 🔊	File: "/tmp/wireshark pcapng wlp2s0 P	ackets: 530 · Displayed: 42	23 (79.8%) · Dro	opped: 0 (0.0%)	Profile: Default	

After inspecting the packets I found that my search on scurvy was in fact secure using the SSL connection. I then tried the same experiment with the Microsoft Bing search engine:

16

• - 5 ×

Capturing from wi	o2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)] 🔶 _ 🗟 🗙
File Edit View Go Capture Analyze Statistics Telephony Tools Inte	rnals Help
● ● <u>▲</u> ■ <u>▲</u>   <b>■ = ×</b> C   <b>Q</b> ↔ ↔	ā 🖄 🗐 📑 🖨 🗉 🗹 📅   👪 😫 1 🗃
Filter: http and ip.addr == 172.20.3.76	sion Clear Apply Save
No. Time Source Destination	Protoc Lengt Info
3463 155.1383614 172.20.3.76 204.79.197.200	HTTP 877 POST /fd/ls/GLinkPingPost.aspx?IG=44526A84FF964371BC64BD55DAC4459D&ID=SERP,5138.1&url=https
3466 155.2269320 172.20.3.76 204.79.197.200	HTTP 915 GET /fd/ls/l?IG=44526A84FF964371BC64BD55DAC4459D&Type=Event.CPT&DATA={%22pp%22:{%225%22:%22
3489 155.6545027 204.79.197.200 172.20.3.76	HTTP 1514 [TCP Retransmission] Continuation or non-HTTP traffic
3495 155.9067076 204.79.197.200 172.20.3.76	HTTP 1514 [TCP Previous segment not captured] Continuation or non-HTTP traffic
3497 155.9157664 204.79.197.200 172.20.3.76	HTTP 1514 [TCP Retransmission] Continuation or non-HTTP traffic
3499 155.9161304(204.79.197.200 172.20.3.76	HTTP 1514 Continuation or non-HTTP traffic
3508 156.1767332(204.79.197.200 172.20.3.76	НТТР 71 НТТР/1.1 200 ОК (GIF89a)
3528 156.2797248 172.20.3.76 204.79.197.200	HTTP 1077 POST /fd/ls/lsp.aspx? HTTP/1.1 (text/plain)
3531 156.2803878(172.20.3.76 204.79.197.200	HTTP 1124 GET /rms/Shared.Bundle/jc,nj/eb350d1c/2809c0d7.js?bu=rms+serp+Shared%24shared_c.source%2cSh
3570 157.2466817 204.79.197.200 172.20.3.76	HTTP 305 HTTP/1.1 204 0K
3662 161.2662774 204.79.197.200 172.20.3.76	HTTP 201 [TCP Retransmission] HTTP/1.1 200 OK (application/x-javascript)
7666 493.6737278 172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
8594 556.9058197(172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
8943 589.9559610 172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
8947 590.0057001(172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
8951 590.0394046(172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
9063 600.3531939 172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
9130 605.3201364 172.20.3.76 72.21.91.29	ICMP 590 Destination unreachable (Host administratively prohibited)[Packet size limited during captu
Frame 3466: 915 bytes on wire (7320 bits), 915 bytes capture	d (7320 bits) on interface 0
01c0 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 2a 3h are/n	na. image/*:
01d0 71 3d 30 2e 38 2c 2a 2f 2a 3b 71 3d 30 2e 35 0d q=0.8	·/ *:q=0.5.
01e0 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 .Acce	bt- Language
01t0 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 : en-	JS, en;q=0.5
0200 0d 0a 41 53 53 55 /0 /4 2d 45 56 53 57 54 59 56Acc	pt - Encodin
0220 0/ 3a 20 0/ 7a 09 70 20 20 04 03 00 00 01 74 05 g; g2 0220 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a	pp, de tate
0230 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 73 //www	bi ng.com/s
0240 65 61 72 63 68 3f 71 3d 73 63 75 72 76 79 26 67 earch	ra= scurvy&g
0250 6f 3d 53 75 62 6d 69 74 2b 51 75 65 72 79 26 71 o=Sub	nit +Querý&q
0260 73 3d 62 73 26 66 6f 72 6d 3d 51 42 4c 48 0d 0a s=bs&	for m=QBLH.
10/20 43 bt bt 60 69 65 3a 20 4d 55 49 44 3d 32 36 33 Cooku Wol2s0:	Profile: Default

In this case I was able to view my search within the packet because it was going over a non-encrypted connection. I was also able to view data from the Wikipedia page (first link) as it too was non-encrypted.

# **Analyze Wireshark Data**

a) How many UDP packets did Wireshark capture: 704

Wire	shark: Protoc	ol Hierarch	ny Statisti	cs			⊕	
	D	isplay filter:	none					
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End I
🗆 Frame	100.00 %	8388	100.00 %	13866371	0.296	0	0	
Ethernet	100.00 %	8388	100.00 %	13866371	0.296	0	0	
Internet Protocol Version 6	0.56 %	47	0.03 %	4676	0.000	0	0	
Internet Control Message Protocol v6	0.48 %	40	0.03 %	3860	0.000	40	3860	
🗆 User Datagram Protocol	0.08 %	7	0.01%	816	0.000	0	0	
Domain Name Service	0.05 %	4	0.00 %	486	0.000	4	486	
DHCPv6	0.04 %	3	0.00 %	330	0.000	3	330	
Internet Protocol Version 4	96.84 %	8123	99.90 %	13852063	0.295	0	0	
Internet Group Management Protocol	0.17 %	14	0.01%	744	0.000	14	744	
🗖 User Datagram Protocol	8.39 %	704	0.64 %	88489	0.002	0	0	
Domain Name Service	8.18 %	686	0.60 %	83412	0.002	686	83412	
Hypertext Transfer Protocol	0.14 %	12	0.03 %	4533	0.000	12	4533	
Network Time Protocol	0.05 %	4	0.00 %	360	0.000	4	360	
NetBIOS Name Service	0.02 %	2	0.00 %	184	0.000	2	184	
+ Transmission Control Protocol	87.57 %	7345	99.16 %	13749821	0.293	4293	3818408	
🕂 Internet Control Message Protocol	0.72 %	60	0.09 %	13009	0.000	58	11829	
Address Resolution Protocol	2.53 %	212	0.06 %	8904	0.000	212	8904	
🕀 Logical-Link Control	0.05 %	4	0.00 %	470	0.000	0	0	
802.1X Authentication	0.02 %	2	0.00 %	258	0.000	2	258	
e Help							X	Close

# b) what was the average IP Packet size: 1653.120 bytes

			Wiresh	ark: Summ	агу	+ - • ×
File Name: Length: Format: Encapsulation:			/tmp/wire 1414849 Wireshar Ethernet	eshark_pcap 00 bytes k/ pcapn	ng_wlp2s0_20161003011534_ZiL27g g	
Time First packet: Last packet: Elapsed:			2016-10 2016-10 00:06:15	-03 01:15:34 -03 01:21:49 5	1 9	
Capture OS: Capture application: Capture file comments			Linux 3.1 Dumpca	10.0-327.36. p 1.10.14 (G	1.el7.x86_64 iit Rev Unknown from unknown)	
Interface Dropped Pack wlp2s0 unknown	kets Capture none	Filter Link ty Etherne	pe Packet size t 262144 bytes	limit		
<b>Display</b> Display filter: Ignored packets:					none 0 (0.000%)	
Traffic Packets Between first and last packet Avg. packets/sec Avg. packet size	Captured 8388 375.319 sec 22.349 1653.120 bytes	Displayed 8388	Displayed % 100.000%	Marked	Marked % 0.000%	
Bytes Avg. bytes/sec Avg. MBit/sec	13866371 36945.528 0.296	13866371	100.000%	0	0.000%	
🔞 Help					e Ca	ncel

c) how many packets did Wireshark drop:106

	4				*wlp2s0 [Wireshark 1.10.14 (Git Rev Unknown from unknown)]	• - 5 ×
	File Edit V	riew Go Capture Analyze Sta	tistics Telephony Tools	Internals Help		
Ret         Description         Description         Protect and the second sec		🖌 🔳 🔬 🖪 🖍	C Q 💮 🔊	3 7 21	🗐 🖳 (A. C. C. 📅 ) 🚟 🔀 🐻 (B)	
Net         Description         Description <thdescription< th=""> <thdes< td=""><td></td><td></td><td></td><td></td><td></td><td></td></thdes<></thdescription<>						
No.         Data         Source         Desclaring         Protect Larget hole           201	Hiter:		¥ E	xpression Clear		
21       20202000 184/200/01       100       21 kit2 Accord potts argument little to 2000 (col 4 your) All Col 4 kit2 Accord and a grant and a grant and a grant little to 2000 (col 4 your) A	No. Ti	me Source	Destination	Protoc L	engt (Info - Se (Col Aloneo unateri alegorino) inclp > Robor (Non) segos rock-z natiosar cenno	
2010             2010	23 8.	222973544 54.239.29.188	192.168.1.8	TCP	54 [TCP ACKed unseen segment] http > 45022 [ACK] Seq=1 Ack=2 Win=127 Len=0	· · · · · · · · · · · · · · · · · · ·
0100772214012010111       01007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       0007721010101011       00077210101010110101       000772101010101010101       000772101010101010000       00077210101010100000       00077210101010100000       00077210101010100000       000772010101010100000       0007720100100100000       0007720100100100000       0007720100100100000       00077201001001000000       000772010000000000000000000000000000000	24 8.	750676806 Actionte_20:7a:17	Broadcast	ARP	42 Who has 192,168.1.117 Tell 192,168.1.1	
1       10.007106431192.101.1       102.101.1       006       7 9 Standard quary DobB3 A as .csaleweid.a.com         2       10.00720543122.101.1       102.101.1       102.101.1       102.101.1       102.101.1         3       10.0072054122.101.1       102.101.1 <td>26 10</td> <td>.08779214 192.168.1.8</td> <td>192.168.1.1</td> <td>DNS</td> <td>Az min has issilisting a scalar media.com</td> <td></td>	26 10	.08779214 192.168.1.8	192.168.1.1	DNS	Az min has issilisting a scalar media.com	
2010.007227031152.101.011       102.101.01       105.007277031152.101.011       102.101.010       105.007277031152.011.011       102.101.010       105.007277031152.011.011       102.101.010       105.007277031152.011.011       102.101.010       105.007277031152.011.011       105.0072777031152.011.011       105.0072777031152.011.011       105.0072777031152.011.011       105.0072777031152.011.011       105.0072777777777777777777777777777777777	27 10	.08781643 192.168.1.8	192.168.1.1	DNS	78 Standard query Oxbd81 A as.casalemedia.com	
2010.0002004132.04.00.1       102.060.1.0       DS       105 tendard query response fordade OWE as calculated accomedipacitume to OWE alloss, advancement et al.103.04.40.06.100.01.04.02.04.01.00         2010.0000001192.04.00.1       102.060.1.0       DS       2010.0000001192.04.00.1       102.060.1.0       DS       2010.0000001102.04.00.0       DS       2010.0000001192.04.00.0       DS       2010.0000001192.04.000001192.04.0000001192.04.0000001192.04.00000000001192.04.0000000000000000000000000000000000	28 10	.08782783 192.168.1.8	192.168.1.1	DNS	78 Standard query Oxa3b5 AAAA as.casalemedia.com	
000000000000000000000000000000000000	29 10	.19822190:192.168.1.1	192.168.1.8	DNS	185 Standard query response 0x4a84 CNAME as.casalemedia.com.edgesuite.net CNAME a1853.g.akamai.net A 184.26.44.95 A 184.26.44.103	
0       201000000110011011       100000011001101       1000000110011001101000000000000000000	30 10	.20316474 192.168.1.1	192.168.1.8	DNS	185 Standard query response Oxbd81 CNAME as.casalemedia.com.edgesuite.net CNAME a1853.g.akamai.net A 184.26.44.103 A 184.26.44.95	
30 10:2137:000 184:36:44.103       102:1136:118       107       74 http > 90064 [mi, Aci] Sepo Atci > 10022 4023 Atc2 201403 TSec = 7006948 [M:532         31 10:21337:203 110:118:118       104:20:44.103       107       103 110:2004 142:118:128       104:20:44.103       107       103 110:2004 142:118:128       104:20:44.103       107       103 110:2004 142:118:128       104:20:44.103       107       103 110:2004 142:118:128       1002 110:2004 110:118:128       1002 110:2004 110:118:128       1002 110:2004 120:118:128       1002 110:2004 120:118:128       1002 110:2004 120:118:128       1002 110:2004 120:118:128:128       1002 110:2004 120:118:128       1002 110:200 120:118:128       1002 110:200 120:118:128       1002 110:200 120:118:128       1000 110:118:128<	32 10	.20528091192.168.1.1	192,168,1,8	DNS	24 double 2 mitig (sing) seque with 52200 Lenie o HSS-1400 SACK_PERVer I Svat-705046 Test = 0 #S=126	
31       0.2134324       102.1434324       102.143424       103       104.2054312       104.205431	33 10	.21337400:184.26.44.103	192.168.1.8	TCP	74 http > 60064 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0 MSS=1460 SACK PERM=1 TSval=1472677403 TSecr=7095948 WS=32	
5010.135520-102.106.1.0       104.25.44.103       TCP       1534 [TC segment of a reassembled RUJ]         3010.215520-102.106.1.0       104.25.44.103       TCP       1534 [TC segment of a reassembled RUJ]         3010.215520-102.106.1.0       104.25.44.103       TCP       1534 [TC segment of a reassembled RUJ]         3010.215520-102.106.1.0       104.25.44.103       HTP       526 [T //pprox1/H/1 Reader up reassembled RUJ]         3010.215520-102.106.1.0       104.25.44.103       HTP       526 [T //pprox1/H/1 Reader up reassembled RUJ]         3010.215520-102.106.1.0       104.25.44.103       HTP       526 [T //pprox1/H/1 Reader up reassembled RUJ]         3010.215520-102.106.1.0       104.106.1.0       TCP       104.106.10       HTP         3010.215520-102.106.1.0       104.106.1.0       TCP       104.106.10       HTP       526 [T //pprox1/H/1 Reader up reassembled RUJ]         3010.215520-102.106.1.0       104.106.100       HTP       500 [T //portune 10 [T //p	34 10	.21343334:192.168.1.8	184.26.44.103	TCP	66 60064 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=7095958 TSecr=1472677403	
30       0.2154265       1.08       104.25.44.103       TCP       1514 [TCP sequent for a reaseable RFU]         37       10.21572012.108.1.18       104.25.44.103       TCP       1514 [TCP sequent for a reaseable RFU]         38       10.225525114.20.41.18       104.25.44.103       TCP       1514 [TCP sequent for a reaseable RFU]         38       10.225525114.20.41.18       102.2562       10.2154267212.10.116.11       102.106.117         39       10.225525114.20.41.18       107       0.61 TCP sequent for a reaseable RFU]       108.11422677119 TScr.7705662         30       10.225525114.20.41.410       107.11422677119 TScr.7705662       108.11422677119 TScr.7705662       108.11422677119 TScr.7705662         315.25215261142.352147264 (x081814/34.410.31       107.11422677119 TScr.7705662       108.11422677119 TScr.7705662       108.11422677119 TScr.7705662         315.25215261142.352147264 (x081814/34.7544), 105.114270717 (107.1128)       10.314242677119 TScr.7705662       108.11422677119 TScr.7705662         315.25215261142.35142.35142.35142.35142.351412.	35 10	.21352529-192.168.1.8	184.26.44.103	TCP	1514 [TCP segment of a reassembled PDU]	
0000       0071       242       007       071       242       0000       0000       0071       242       0000       0000       0071       242       0000       0000       0071       242       0000       0000       0000       0000       0000       0071       242       00000       0	36 10	.21354295-192.168.1.8	184.26.44.103	TCP	1514 [TCP segment of a reassembled PDU]	00001000001000000
30 10.20314566:194.201.401.30       102.1031.18       TP       00 http://codestal.001.001.001.1001.1001.1001.1001.1001.	37 10	227448211184 26 44 103	184.20.44.103	TCP	352 OET / CVgNUS YV=/ATT=Teader Ldg_Darseas=181450ar=9/B4221 df22342420/33/042/32231 Lf422/334/2412234223422342234223422342234223422342	\$2+2010\$2+10\$2+01
000         001         202 207 00 10 00 10 00 00 00 00 00 00 00 00 00	39 10	.22814556:184.26.44.103	192.168.1.8	TCP	66 http > 60064 [ACX] Seq=1 Ack=366 Win=35712 Len=0 Tsva1=1472677419 TSer=7055962	
0       71       26       207       71       26       207       71       26       207       71       26       207       71       26       207       71       26       207       71       26       207       71       26       207       27       10	40.10	SAESEE04104 SE 44 105	107 160 1 0	TCD	ISIA [TCD commont of a concernmblad DDU]	_
Control Protocol, Src Part: 60064 (60064), Dat Part: http (80), Seq: 0, Len: 0          0000       00 7f 20 20 7p (f7 a0 60 b4 a7b 7p 66 00 00 45 00 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b4 a7b 7p 66 00 00 45 00 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b4 a7b 7p 66 00 00 45 00 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b4 a7b 7p 66 00 00 45 00 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b1 a 2 cm (4-n-2)         0000       00 7f 12 20 20 7p (f7 a0 60 b1 a 2 cm (4-n-2)         0000       00 1a 2 cm (4-n-2)         0000       00 1a 2 cm (4-n-2)         0000       00 00 00 00 00 00 00 00 00 00 00 00 00	➡ Frame 31:	: 74 bytes on wire (592 bits II, Src: IntelCor_7b:7e:64 Protocol Version 4, Src: 15	<pre>a), 74 bytes captured (a0:88:b4:7b:7e:64), (2.168.1.8 (192.168.1))</pre>	(592 bits) on Dst: Actionte .8), Dst: 184.	interface 0 20:7a:17 (00:71:28:20:7a:17) 6:44.103 (184.26:44.103)	
0000 00 74 28 20 7a f 7 a0 88 b4 7b 7a 64 08 00 a5 00	🕀 Transmiss	sion Control Protocol, Src P	ort: 60064 (60064),	Dst Port: http	(80), Seq: 0, Len: 0	
0000 00 71 20 20 79 f7 a0 86 b4 76 7a 66 69 00 45 00 10 70 5x 17 53 40 00 40 66 7d 57 x0 88 01 68 b1 0000 7x 10 53 5x 10 60 00 00 00 40 00 7x 10 95 5x 00 00 00 00 00 00 00 00 00 7x 10 95 5x 00 00 00 00 00 00 00 00 00 68 6x 00 00 00 00 01 03 00 00 98 6x 00 00 00 00 01 03 00 00 99 5x 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 00 01 03 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 00 00 90 5x 10 00 00 00 00 00 00 00 00 00 00 00 00						
0000       00 7f 28 20 7a f7 a0 88 b6 7b 7a 64 08 00 45 00						
000       00       71       28       20       79       67       68       64       76       77       60       65       74       28       20       70       67       68       64       76       77       63       80       70       67       68       64       76       77       63       80       70       67       68       60       70       60       86       60       70       67       68       60       70       67       68       60       70       67       68       60       70       68       60       70 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<>						
0000 00 71 28 20 7a f7 a0 88 b4 7b 7a 64 08 00 45 00						
0000       00 91 28 20 7a (7 a) 88 b4 7b 7a 64 08 00 45 00      (2, 4-46.         0000       00 2: 17 33 40 00 40 06 7d 57: 00 88 01 08 b8 1a      (3.30,8)         0000       2: 07 sa 80 00 50 1a c3 51 b1 00 00 00 00 40 00						
0000 k0 71 28 20 7a 17 a0 88 b4 7b 7a 66 08 00 45 00 00 87 17 33 48 00 40 05 74 57 c0 88 01 08 b1 34 (-39,8) 14) 0030 72 10 91 55 00 00 02 64 76 54 64 07 08 68 00 65 040 66 80 00 00 00 10 93 05 07 Fama (Fama) 76 here: Exclore: 1938. Disclored: 1938 (100 06). Depend: 10( 1.36)						
0000 00 74 28 20 7a f7 a0 88 b4 7b 7a 64 08 00 45 00						
0000       00 71       20 70       f7 a0       80       b4 7b       7a       64       00       00       a<						
0000       500 7f 28 20 7a f7 a0 88 b4 7b 7a 64 08 00 45 00f       . ( 2 (-dE.         0000       500 7f 28 20 7a f7 a0 88 b4 7b 7a 64 08 00 45 00f       . ( 2 (-dE.         0000       500 7f 28 20 7a f7 a0 88 b4 7b 7a 64 08 00 45 00f       . ( 2 (-dE.         0000       500 7f 28 20 7a f7 a0 80 b1 a c1 51 bf 100 00 00 40 40 00 c1       . ( 3.30 p.) W         0000       500 7f 28 20 00 00 10 c1 63 c0 100       . ( 2 (-dE.         0000       500 7f 28 20 00 00 11 63 c0 100       . ( 2 (-dE.         0000       50 76 00 00 00 10 30 00 00 40 00 c2       . ( 3.30 p.) W         0000       50 10 00 00 00 10 30 00 00 00 00 00 00 00 00 00 00 00 00						
000 71 20 20 70 77 40 80 164 76 74 64 00 00 85 00       .1 2 (-4, -5)         0010 00 5x 17 35 46 00 60 80 74 57 65 48 01 69 181 14       (-30, -5)         0020 72 10 73 50 00 02 04 05 74 57 65 48 01 69 181 14       (-30, -5)         0020 72 10 73 50 00 02 04 05 18 14       (-30, -5)         0020 72 10 73 50 00 02 04 05 00 10 80 00 90       (-30, -5)         0020 72 10 73 50 00 02 04 05 14 04 07 09 10 80 00 90       (-30, -5)         0040 95 10 00 00 00 00 10 03 07       (-30, -5)         0040 95 10 00 00 00 00 10 03 07       (-30, -5)         0040 95 10 00 00 00 00 10 03 07       (-30, -5)         0040 95 10 00 00 00 00 01 03 00 07       (-30, -5)         0040 95 10 00 00 00 00 01 03 00 07       (-30, -5)         0040 95 10 00 00 00 00 00 00 01 03 00 07       (-30, -5)         0040 95 10 00 00 00 00 00 00 00 00 00 00 00 00						
0000       00       71       28       20       7a       67       80       86       7a       7a       80       <						
000 11 20 20 70 f7 40 88 b4 76 74 69 80 04 85 00             0010 10 5x 17 35 45 00 40 56 74 57 61 48 01 66 b18 14             0020 00 5x 17 35 45 00 60 20 40 50              0020 10 5x 17 35 45 00 60 20 40 50              0020 00 72 10 91 50 00 00 20 40 50              0020 00 00 00 01 03 03 07              0040 66 80 00 00 00 01 03 03 07              0040 66 80 00 00 00 01 03 03 07              0040 66 80 00 00 00 01 03 03 07              0040 67 80 00 00 00 00 01 03 03 07              0040 67 80 00 00 00 00 01 03 03 07              0040 67 80 00 00 00 00 01 03 03 07              0040 67 80 00 00 00 00 00 00 00 00 01 03 03 07						
0000       00 71 82 20 78 f7 80 88 b4 76 78 65 00 80 85 20       .1 2 (-d. E.         0000       00 51 71 33 84 00 80 67 86 50 57 86 5						
0000 00 71 20 20 74 7 40 66 ke ha 70 74 66 60 90 45 00 45 00						
0010 00 2: 17 32 40 00 40 06 74 57 6 25 0 a 80 0 06 18 1 4 3 38 4, 1 4 38 4	0000 00 7	f 28 20 7a f7 a0 88 b4 7b 7	e 64 08 00 45 00	. ( z		
0020 (2 0 °) is a 0 (3 °) is (3 °) is (5 °) is (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0010 00 3		0 a8 01 08 b8 1a			
0040 es te 00 00 00 1 03 03 07 F	0020 20 6	7 ea a0 00 50 1a c3 51 b† 0 0 91 52 00 00 02 04 05 b4 0	0 00 00 00 a0 02 ,			
🖉 Frans (Frans) 78 hitse : : : : : : : : : : : : : : : : : : :	0040 46 B	c 00 00 00 00 01 03 03 07	F		<b>a</b>	
🗮 🛠 Frama (Frama) 7.6 hutar : : Barkate: 9388. Dirolauad: 9388 (100.064) . (Tyronoad: 106 (1.364)						
🗮 Forma (Fama) 7.6 https://www.illands.com/www						
🖉 Forma (frama) 7/8 hutae : Baskate: 9388. Nienlausel: 9388 (100.0%) . (Ymnnad: 106 (1.3%)						
🚔 🛠 Fame (Frame) 78 hutes : Backets 8988 - Disclassed-8988 (100.0%) - promeet-106 (1.9%)						
	e M Frame	(frame) 74 hytes	lackate: 8388 . Dieplaund	8388 (100.0%)	Deallar Defect	

### d) what does a flow graph show:

•				wlp2s0 - Graph Analysis
Time	80::b4:326f:2702: ff02::16	192.168.1.5 224.0.0.251 224.0.0.251	192.168.1.8 ff ff02:fb 74.201.141.151	22:: Comment
0.000000000	Multicast Listengr			CMPv6: Multicast Listener Report Message v2
0.000814943		Membership Report./		IGNEVS: Membership Report / Join group 224.0.0.251 for any sources
0.182633191		Standard guery 0x00		MONS Standard guery 0x0000 PTR sleep-proxy udp.local, "OH" guestion
184267241		Standard guery 0x00		MDNS: Standard guery 0x0000 PTR sleep-provy uda.local. "OH" guestion
007027793			58222 > http [ACK]	TCP: 58222 > Mtp (ACK) Seg=1 Acks1 Wn=237 Len=0 TSval=7086752 TSecr=2297942739
007062220			58224 > http (ACK)	TP: 5824 > Mm (4/4) Senit 4/40 Mm 231 Level T5-als 206352 T6-rm 22874/2746
017554419			FTCP ACKed upseep s	TTP: TTP: A/Ved upream rearrant/LHM > 50136 (A/V) Sen-1 Ark-2 Min-E71 Lan-4 TSush-2107052757 TSarr
017647538			FTCP ACKed unseen s	THE PERIAD INCOMENDATION OF A STATE PERIAD VALUE AND A MOUNT LINEAR TRANSPORTER THAN
2.004062646	Multicast Listener		(502517	<ul> <li>CMMA Multicall listense deserved Message V2</li> </ul>
000002040	(6)	Mémbershin Bennit /		<ul> <li>STATUS Humbership Research (July and TAL 2018) for any asymptotic status (July any asymptotic status (July any asymptotic status (July asymptotic status (J</li></ul>
0000032849		Bouter Solicitation		Startes, Permership report ( ) and prove 22 and any sources
3990110100	(4)	Quedad guary (v00		A Contract and a second of the
104307708		Standard query 0x00		Parties Standard query endotes in its proof programmers of a query fill and the section
5.1342077JB	113630		33372 > http://	When a summary query sources of the
624960100			TCP ACKed unse	AD TTP: ITTP: ACKed uppersynametric bits > 33322 Markin Senal Arken Wanabis Lanud Tousie 31155870 TSerre
102000000000			45024 >	bit two shares a law (style search and se
9.4079623946 9.307056694			45022 >	HTT TYPE ACCOUNTS AND A
8.207050684			(45122)* ITCP ACK	The first study is the product study of the
8.22284/669			(45124)************************************	True: [LP: Avea unseen segment] http:> 45024 [arXii Seq=1.40042 with 127 Lemm
8.222973544			(46122)	The first for an entries and the second seco
10.087792146			(35110)	The service service were a service and the service of the service serv
10.08/810433			(56342)7	and units standard query weeks a statementation of
10.087827831			05110	Les ones surreare query unados www.es.casaremesia.com
10.198221902			(35114)	And UNX: Standard query response survays Change as catalemedia com expensite net Change autora gi examaline Der public finandard puery response survays (Change as catalemedia com expensite net Change autora) en publication of the survay response of the survay of the survay and the survay autora of the survay autora of the survay of the survay response of the survay of the survay autora of the survay autora of the survay autora of the survay of the survay of
10.203164740			(56342)	The subscript bury regions which cover as transmission term operations are cover alors a manual are
10.203445/14			(60162)	Cr. Store A unit [214] Schen sturg 2010 Schen Holenten Sock/ Educat Longe (02246) 1961-6 Mont26
10.205280917			(35118)	uno: Standarte query response suazos. Cueve as casalimento a com operante nel Cueve alos 3, acaman nel
10.213374005			(60344)	TCP. Http 5 6006 [STR, ACK] Seq=0 ACHT WH-2000 CENIO MSS-1400 SACK PERM-1 (SUB-14/2077403 TSec
10.213433343			(60162)	The second state (second state and state
10-218525294			(60314))	The first account of a measurement ready
10.213542954			(60164)	I.C. [I.C. adjustic or a reasonition roug
10.21/60/320			(60154)	H11P: Vc1 / typnikt/withinineeersag_parses/initiation/microscid52253142007937052C5220tbf522534578522pa
0.227448218			(60314)	TUP: http://tipic.com/interview.com/intervie
0.228140362			(60162)	Ter, may in source (which dependent memory) a communication (2017419 T3607=7053962 Web communication of a second-local data memory).
10.345205948			(63263)	The second
10.345321788			1601645	10.7: 50096 P mtp (ALA) 500-3003 ACM-1442 Wm-22120 Ltm-U 15V0-7036030 T56(7=1472677536
10.345435842			(60154)	HTTP: HTTP/11 400 UK. (EKK)/WWRCPEC
10.345452589			(603340)	TCP: 50594 > MD [ACX] 560=3593 ACK=1532 Wm=35072 Len=U Tsva=7096090 TSecr=1472677536
10.387848026			(58163)	um: DNs: standard query ox/CoT A securepublids.g.doublecitik.net
10.387878108			(58143)	AMU DNS Standard query 0x3353 AAAA securepubads.g.doublectick.net
10.387999106			(5241)	DNI: Standard query build3: A securepubado.g.diubleckck.net
10.389303129			(60366)	TCP: souse > mtp [stm] seqwo wine_syzuu Leneo MSS=Lesu SACK_PERM=1 TSval=7096134 TSetr=0 WS=128

A flow graph shows the data flow of a connection. By scrolling to the right, I can see things like retransmits or drops.

e) list the flow graph options



# **Analysis Questions**

1. How can security professionals use Wireshark?

By using Wireshark, you can view the raw data of a packet for file signatures we discussed in our hex lab, or spot instructions for execution of malicious code. Another way to use Wireshark is to discover DoS attacks or ssh brute force attacks. By capturing an overwhelming number of a certain type of incoming packets you can take steps to block the source IP address. If I saw a large number or packets going to a remote destination IP address, I would investigate to make sure corporate data was not being removed from an unauthorized source.

In addition, I could monitor incoming and outgoing traffic based on protocol and create rules. For SMTP as an example, I could monitor for attachments of a certain size or content.

2. List three ways attackers can use Wireshark.

1) To map the network

2) Discover protocols that are in use

3) Find clear text communications for username and password discovery

3. Does Wireshark capture all the traffic on the Internet? If so, explain why. If not, which traffic does it capture?

No, Wireshark captures traffic that passes its network interface either directly or on a hub, as well as broadcast and multipath traffic (Weadock, 2009).

4. Write Wireshark filters to:

- a) View all traffic for 10.10.10.2.
- Filter = ip.addr = 10.10.10.2b) View icmp traffic from any address. Filter = icmp

5. Has this lab changed your perspective on your privacy while browsing the Internet? Describe why or why not.

It hasn't changed my perspective of privacy on the Internet; because of my job, I've been exposed to packet sniffers and understand their capabilities. That said, this lab gave me an opportunity to dive in a lot deeper than I had previously and look at some of the features that Wireshark has. So, basically I have a more, well rounded understanding of packet sniffing and filtering then I had previously.

# Conclusion

Through the exercises, I learned about the capabilities of the Wireshark packet sniffer. I was able to capture packet data and inspect individual packets. I gained a better understanding about the contents of a packet, and how I can gather useful information from using the Wireshark sniffer and putting what I learned into the context of how a network is used and what kinds of data I'm expecting to see.

# References

Adrian Hannah (2011 Nov. 14) Packet Sniffing Basics. Retrieved from <u>http://www.linuxjournal.com/content/packet-sniffing-basics</u>

Glenn Weadock (2009 Sept 30). Wireshark and Promiscuous Mode - Why you may not be seeing all the traffic you think you should. Retrieved from <a href="http://www.networkworld.com/article/2231903/microsoft-subnet/wireshark-and-promiscuous-mode.html">http://www.networkworld.com/article/2231903/microsoft-subnet/wireshark-and-promiscuous-mode.html</a>

Paessler (1996) "Packet Sniffing; Packet Sniffing With PRTG Network Monitor" Retrieved from <u>https://www.paessler.com/packet\_sniffing</u>

Craig Hunt (1992). TCP/IP Network Administration. Sebastopol, CA: O'Reilly & Associates

Douglas E. Comer (1997). Computer Networks and Internets with Internet Applications; Third Edition. Upper Saddle River, New Jersey. Prentice Hall

OpenBSD Documentation (2016 Sept 1), PF Users Guide, Retrieved from <u>https://www.openbsd.org/faq/pf/filter.html</u>

W. Richard Stevens (1990). UNIX Network Programming. Englewood Cliffs, NJ. Prentice Hall

Sahin Erbay 2016, July 26) Internet Protocal Suite (TCP/IP and OSI Models); Retrieved from <a href="http://sahinerbay.com/2016/02/26/internet-protocol-suite-tcpip-and-osi-models/">http://sahinerbay.com/2016/02/26/internet-protocol-suite-tcpip-and-osi-models/</a>

Wireshark (2008 April 12) Duplicate Packets. Retrieved from <a href="https://wiki.wireshark.org/DuplicatePackets">https://wiki.wireshark.org/DuplicatePackets</a>

Wireshark (2014). Wireshark User's Guide. Retrieved from <u>https://www.wireshark.org/docs/wsug\_html\_chunked/</u>