Lab: Using a Protocol Analyzer (Wireshark)

Purpose: The purpose of this lab is to become familiar with a protocol analyzer such as Wireshark, formally know as Ethereal. Wireshark is available for various operating systems including Windows, Linux and Macintosh. Wireshark can be downloaded free, at http://www.wireshark.org/

Version used for this assignment: Version 0.99.6a (SVN Rev 22276

Step 1: Setting up TCP preferences.

By default, Wireshark will show us relative TCP Sequence and Acknowledgement numbers starting with 1. To view the actual TCP Sequence and Acknowledgement numbers sent and received we need to disable this option.

- Choose Edit >> Preferences
- Click on Protocols
- Click on TCP
- Disable "Relative sequence number and window scaling" (be sure it is not checked)



	Wireshark: Preferences	5	the paster party of	10 ····	
	TALI	^	Transmission Control Proto	ocol	
	ТСАР			Show TCP summary in protocol tree:	V
	ТСР			Validate the TCP checksum if possible:	V
	TCPENCAP TDS			Allow subdissector to reassemble TCP streams:	V
İ	Teredo			Analyze TCP sequence numbers:	V
	TIPC			Relative sequence numbers and window scaling:	
	TNS				
	Token-Ring			Try heuristic sub-dissectors first:	
	TDVT				

Step 2: Starting the Wireshark Capture

- First time choose:: • Capture \rightarrow Options
- Subsequent times choose:: • Capture \rightarrow Start





Beginning the capture of frames and packets:

- If you have more than one Ethernet NIC card installed, be sure to choose the proper interface.
- Disable "MAC name resolution" (be sure it is not checked)
- Disable "Network name resolution" (be sure it is not checked)
- Click "Start" to begin the capture (Note: Before clicking on "Start" you may wish to have a web browser open. After you click "Start" type in the URL of the web site you wish to download.)

wiresnark: Captur	e Options										
Capture											
Interface: 00 VE	Network Connection:	\Device\NPF_{3FF3BBE2	-486F-4C4D-BA82-376F2B16C76E}								
IP address: 1 Intel(R) PRO/100 VE Network Connection: \Device\NPF_{3FF3BBE2-486F-4C4D-BA82-376F											
Link-layer h Microsoft: \Device\NPF_{43AF14EB-A59F-4EB6-94A7-9B2A842B92AE}											
Capture r	Capture of MS Tunnel Interface Driver: \Device\NPF_{01932300-A931-4EB1-9B15-48428E3DD7D2}										
Limit each pack	Imit each packet to IbX Imit butes										
Capture Filter:											
Capture File(s)			Display Options								
File:		<u>B</u> rowse	☑ Update list of packets in real time								
Use <u>m</u> ultiple file	s		Automatia and Uine in Live conture								
Next file every	1	megabyte(s) 🔻	Automatic scrolling in live capture								
Next file every	1	minute(s) 🔻	Hide capture info dialog								
✓ Ring buffer with	2	files									
Stop capture aft	er 1	file(s)	Name Resolution								
Stop Capture			Enable MAC name resolution								
🔲 after 1	_ ▼ pa	cket(s)	Enable network name resolution								
🔲 after 1	r	negabyte(s) 🔻									
🔲 after 1	r	ninute(s) 💌	Enable transport name resolution								
<u>H</u> elp			<u>Start</u> <u>C</u> ancel								

At this point Wireshark begins capturing packets including unicasts directed for the MAC address of your Ethernet NIC, broadcasts for all devices, multicasts, and unknown unicasts (unicasts flooded by the switch when the Destination MAC address is not in its MAC Address Table).

2-	2-29-08-TCP-3-WAY.pcap - Wireshark																			
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> na	lyze	<u>S</u> tatisti	cs <u>H</u> e	elp											
	ë.	e i	e	1	D	8	x	¢,	8	٩	\$	⇔	Ø	₽	₽		J	€,	Q,	
<u>F</u> ilter	:										•	<u>E</u> xpr	ession.	<u>C</u> lea	Арр	oly				
No.	,	Time		Sou	rce				Desti	ination				Proto	col	Info				
	1	0.000	000	Cis	co-L	i_09	:4e:0)f	Spa	nning	-tre	e-(f	or-br	STP		Conf	. Root	=	32768/	1
	2	0.344	369	192	2.168	.1.1	01		207	.62.1	87.7			ТСР		4932	3 > ht	tp	[SYN]	1
	3	0.362	769	207	7.62.	187.	7		192	.168.	1.10	1		тср		http	> 493	23	[SYN,	
	4	0.363	085	192	2.168	.1.1	01		207	.62.1	87.7			TCP		4932	3 > ht	tp	[ACK]	
	5	0.363	715	192	2.168	.1.1	01		207	.62.1	87.7			HTTP		GET	/~rgra	zia	ni/ H⊺	1
	6	0.385	774	207	.62.	187.	7		192	.168.	1.10	1		TCP		http	> 493	23	[ACK]	
	- 7	0.386	514	207	7.62.	187.	7		192	.168.	1.10	1		HTTP		HTTP	/1.1 3	04	Not Mo	4
	8	0.386	823	192	2.168	.1.1	01		207	.62.1	87.7			TCP		4932	3 > ht	tp	LFIN,	
	9	0.386	867	207	.62.	187.	7		192	.168.	1.10	1		TCP		http	> 493	23	LFIN,	
	10	0.386	934	192	2.168	.1.1	01		207	.62.1	87.7			TCP		4932	3 > ht	tp	[ACK]	
	11	0.395	171	192	2.168	.1.1	01		207	.62.1	87.7			TCP		4932	4 > ht	tp	[SYN]	-
< _						1	11												•	
🕀 FI	rame	2 (66	byt	es on	wire	, 66	i byte	es ca	pture	d)										
🗏 🗉 E'	ther	net II	, sr	c: Qu	antaC	o_04	:a2:	1e (O	0:1b:	24:04	1:a2:	1e),	Dst	: Cis	CO-L.	i_09:4	le:0f	(00:	:0f:66	:01
+	Dest	tinati	on:	Cisco	-Li_0	9:46	:0f	(00:0	f:66:	09:46	≥:0f)									
(F)	Sou	rce: 0	uant	aCo 04	4:a2:	1e (00:1	b:24:	04:a2	:1e)										
	TVD	о• тр	(0x0	800)		(/										
	i yp	e. 1F	(0.00	-1 ~		07 1	CO 1	1.01	(102	160 1	1.01	۱ n		107 C	1 1 0	7 7 /-	07 67	107	7 7)	
	iter	net pr	0100	01, S	-C: 1	92.1	.08.1.	. 101	(192.	108.1		, U	SU: 2	207.0	2.18/		.07.62	. 18/	• ()	
• T	ransi	missio	n Co	ntrol	Prot	000	, Sro	c Por	t: 49	323 ((4932	3),	Dst F	Port:	ntt	p (80)), Seq	: 49	986985	63

If you want to capture specific types of packets such as HTTP, FTP or ICMP, perform that operation now.

Examples:



Using a web browser, go to a web site of your choosing,

Step 3: Stopping the Wireshark Capture

Click the Stop button or icon to end the capture.



Step 4: Looking at a Wireshark Frame

The amount of information captured can be overwhelming. You can use the "Capture Filter" option in the Options screen where you selected the interface. The amount of frames captured can also be limited by capturing frames in a lab with only a few computers instead of a production network.

2-2	9-08-	TCP-3-	WAY.p	ocap - W	Vireshar	k					-	-			-				x
<u>F</u> ile	<u>E</u> dit	View	<u>G</u> o	<u>C</u> aptur	re <u>A</u> na	alyze	<u>S</u> tatisti	cs <u>H</u>	lelp										
	1	0	@		Þ	8	x	¢,	<u>–</u>	٩	4		> 💫	₫	⊉		Ð,	Q,	
Eilter:												▼ <u>E</u>	pression	n <u>C</u> l	ear <u>A</u> j	pply			
No		Time		So	urce				Des	tinatio	n			Pro	tocol	Info			Â
	1	0.00	0000	Ci 10	sco-L	.i_09	:4e:0)f	Spa 20	annii 7 62	1g-tr	'ee-((for-b	r ST	P	Conf. Root	tn	32768	/
	3	0.36	2769	20	07.62.	187.	7		192	2.16	3.1.1	101		тс	Р	http > 493	323	[SYN,	
	4	0.36	3085	19	$\frac{168}{12}$	3.1.1	01		207	7.62.	187.	7		TC	Р тр	49323 > ht	tp	[ACK]	.
	6	0.38	5774	20)7.62.	187.	7		192	2.16	3.1.1	01		тс	P	http > 493	323	[ACK]	. 1
	7	0.38	6514	20)7.62.	187.	7		192	2.16	3.1.1	101		HT	TP	HTTP/1.1 3	304	Not M	c
	- 8 9	0.38	0823 6867	20	02.108	187.	7		20/	7.02. 2.16	3.1.1	01			P P	49323 > nt http > 493	:тр 123	LEIN, EETN.	
	10	0.38	6934	19	2.168	3.1.1	.01		207	7.62	187.	7		TC	P	49323 > ht	tp	[ACK]	
	11	0.39	5171	19	02.168	3.1.1	.01		207	7.62.	187.	7		TC	P	49324 > ht	tp	[SYN]	-
-							11												·
Et ⊕ ⊕	herr Dest Sour Type	inat ce: Pot P	I, Si ion: Quan (Oxi	rc: Qu Cisco taCo_(0800)	uanta D-Li_0 D4:a2	Co_04 09:40 :1e (1:a2:1 2:0f ((00:11	Le (((00:(p:24	00:1b 0f:66 :04:a	:24: :09: 2:1e	04:a 4e:0)	2:1e f)), Dst	207	SCO-	Li_09:4e:0f	(00:	:0f:60	5
	Vers	ion:	4		51 С.	192.1		101	(192	.100		<u>, (</u>	030.	207.	02.1	07.7 (207.02	. 10/	• ()	
	Неас	ler 1	engtl	h: 20	byte:	s													=
÷	Diff	eren	tiat	ed Ser	vice	s Fie	eld: (0x00	(DSC	P 0x	00:	Defa	ult; E	CN:	0x00)			
	Tota	l Le	ngth	: 52	.o ch	(20)	- 7 \												
	Laer		Cat 10 v04	on: U) (Don't	KUAOD	(200 ment	->												
	Frag	iment	off	set: ())	gillerin	.,												
	Time	to	live	: 128	-														
	Prot	:oco1	: тсі	P (0x0	06)														
÷	Неас	ler c	heck	sum: (0xa40	5 [co	prrect	:]											-
•									111									•	
0000	00	OF 6	6 09	4e 0	f 00	1b	24 04	a2	1e 08	3 00	45 0	0	f.N		\$.E.			-
0010	bb	07 C	0 ab	00 5	0 80 0 1d	b9	a4 05 89 43	00	00 00	00	80 0)2	.4.K@	Р	.c	e.>			=
0030	20	00 9	a ca	00 0	0 02	04	05 b4	01	03 03	3 02	01 0)1		•••		•••			
0040	04	02											••						Ŧ
Interne	t Prot	ocol (i	p), 20 ł	oytes							P: 162	D: 162	M: 0						

No		Time	Source	Destination	Protocol	Info
	1	0.000000	Cisco-Li_09:4e:0f	Spanning-tree-(for-br	STP	Conf. Root = 32768/00:0f:6
	2	0.344369	192.168.1.101	207.62.187.7	TCP	49323 > http [SYN] Seq=498
	3	0.362769	207.62.187.7	192.168.1.101	TCP	http > 49323 [SYN, ACK] Se
	- 4	0.363085	192.168.1.101	207.62.187.7	TCP	49323 > http [ACK] Seq=498
	5	0.363715	192.168.1.101	207.62.187.7	НТТР	GET /~ raziani/ HTTP/1.1
	6	0.385774	207.62.187.7	192.168.1.101	ТСР	http > 49323 [ACK] Seq=219
	- 7	0.386514	207.62.187.7	192.168.1.101	HTTP	HTTP/1.1 304 Not Modified
	8	0.386823	192.168.1.101	207.62.187.7	TCP	49323 > http [FIN, ACK] Se
	9	0.386867	207.62.187.7	192.168.1.101	TCP	http > 49323 [FIN, ACK] Se
	10	0.386934	192.168.1.101	207.62.187.7	TCP	49323 > http [ACK] Seq=498
	11	0.395171	192.168.1.101	207.62.187.7	TCP	49324 > http [SYN] Seq=325

Select a specific frame/packet. For example the packet with the encapsulated application protocol HTTP.

Inside the Wireshark frame is the data, which is usually another protocol with data. This encapsulation process most likely started with an application header (HTTP, etc.) with the original data. Below is an example.



To view this information for each protocol, the Ethernet frame and the encapsulated upper layer protocols, click on the "+" sign next to that protocol. For example, to see the fields within the Ethernet frame click the "+" sign next to Ethernet II (the type of Ethernet frame). The "+" sign will turn into a "-" sign and display the particular information.

To see other layers, click the appropriate "+" sign next to the protocol.



To view the data, look at the information in both Hexadecimal and ASCII.

	Circe	кэu		~~~	uvu	Ц ч	vi i	رباب										
🗉 Ну	pert	ext	Tr	ans	fer	Pr	oto	col										
Đ	GET	/~r	gra	zia	.ni/	НТ	ТР/	1.1	∖r\n									
	Acce	pt	im	age	/gi	f,	ima	ge/>	(-xb	itm	ap,	im	age	/jp	eg,	ima		applicatio
•				-		111							-					
0030	40	29	8d	0a	00	00	47	45	54	20	2f	7e	72	67	72	61	@)GE	⊤ /~rgra
0040	7a	69	61	6e	69	2f	20	48	54	54	50	2f	31	2e	31	0d	ziani/ H	TTP/1.1.
0050	0a	41	63	63	65	70	74	3a	20	69	6d	61	67	65	2f	67	.Accept:	image/g
0060	69	66	2c	20	69	6d	61	67	65	2f	78	2d	78	62	69	74	if, imag	e/x-xbit
0070	6d	61	70	2c	20	69	6d	61	67	65	2f	6a	70	65	67	2c	map, ima	ge/jpeg,
0080	20	69	6d	61	67	65	2f	70	6a	70	65	67	2c	20	61	70	image/p	ipeq, ap
0090	70	6c	69	63	61	74	69	6f	6e	2f	78	2d	6d	73	2d	61	plicatio	n/x-ms-a
00a0	70	70	6c	69	63	61	74	69	6f	6e	2c	20	61	70	70	6c	pplicati	on, appl
00b0	69	63	61	74	69	6f	6e	2f	76	6e	64	2e	6d	73	2d	78	ication/	vnd.ms-x
00c0	70	73	64	6f	63	75	6d	65	6e	74	2c	20	61	70	70	6c	psdocume	nt, appl
00d0	69	63	61	74	69	6f	6e	2f	78	61	6d	6c	2b	78	6d	6c	ication/	xam]+xm]
00e0	2c	20 73	61 2d	70 78	70 62	6C 61	69 70	63 20	61 20	74 61	69 70	6f 70	6e	2f 60	78 63	2d	, applic	ation/x-

Various statistics and graphs can be displayed	Statistics Help
from the Statistics menu.	Dummary
	Protocol Hierarchy
	Conversations
	Endpoints
	IO Graphs
	Conversation List
	Endpoint List
	Service <u>R</u> esponse Time
To view only the packets associated with a specific	<u>Analyze</u> <u>Statistics</u> <u>H</u> elp
TCP session, such as	☑ <u>D</u> isplay Filters
downloading a web page,	Apply as Filter
TCP Stream Be sure you	Prepare a Filter
have one of the packets	Firewall ACL Rules
selected for that stream before applying this option.	✓ Enabled Protocols Shift+Ctrl+R
	දී Decode <u>A</u> s
	दे <u>U</u> ser Specified Decodes
	<u>F</u> ollow TCP Stream
	<u>F</u> ollow SSL Stream
	Expert Info
	Expert Info <u>C</u> omposite

Step 5: Saving output to a text file

Outcome: Save an "expanded" Ethernet frame to a text file and print out the file. This Ethernet frame can include:

- Ethernet frame
- IP packet
- TCP/UDP header
- Application header and/or Data

To save the Ethernet frames to a text file, choose File >> Export >> File. .

<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>Go</u> <u>C</u> apture <u>A</u>	nalyze <u>S</u> tat	istics <u>H</u> elp
Ð	<u>O</u> pen	Ctrl+O	🖉 🗴	ି ଜୁଣ୍ଡ 🖾 🖾
	Open <u>R</u> ecent	+		+ U U
	<u>M</u> erge			Destinati
×	<u>C</u> lose	Ctrl+W	8.1.101	207.62
<u> </u>			187.7	192.16
	Save	Ctrl+S	8.1.101	207.62
	Save As	Shift+Ctrl+S	8.1.101	207.62
	50VC <u>A</u> 5	Shire Carro	.187.7	192.16
	File Set	•	.187.7	192.16
	The Sec		8.1.101	207.62
	<u>E</u> xport	•	File	
	D.1.1	0.1.0	Selected Pa	cket Bytes Ctrl+H
	Print	Ctrl+P	Objects	•
	0	Chillio O		
-	Quit	Ctri+Q	b (2667)	

To save a single expanded frame/packet:

- File name: Be sure to use the file extension .txt
- o Packet Range: Selected packet
- o Click on Displayed (This will be the current frame/packet selected in the display)
- Packet Format:
 - o Be sure Packet Details is clicked (check in the box)
 - o Choose: All expanded
- o Click "Save"



To save a range of expanded frame/packets:

- File name: Be sure to use the file extension .txt
- o Packet Range: Range
- o Click on Captured
- Range: First frame/packet last frame packet. (Example: 2-4)
- o Packet Format:
 - o Be sure Packet Details is clicked (check in the box)
 - o Choose: All expanded
- o Click "Save"

Sample Output

Time Destination Protocol Info No. Source TCP 49323 > http [SYN] Seq=498698563 Len=0 MSS=1460 WS=2 2 0.344369 192.168.1.101 207.62.187.7 Frame 2 (66 bytes on wire, 66 bytes captured) Arrival Time: Mar 1, 2008 14:11:23.257549000 [Time delta from previous captured frame: 0.344369000 seconds] [Time delta from previous displayed frame: 0.344369000 seconds] [Time since reference or first frame: 0.344369000 seconds] Frame Number: 2 Frame Length: 66 bytes Capture Length: 66 bytes [Frame is marked: False] [Protocols in frame: eth:ip:tcp] [Coloring Rule Name: HTTP] [Coloring Rule String: http || tcp.port == 80] Ethernet II, Src: QuantaCo_04:a2:1e (00:1b:24:04:a2:1e), Dst: Cisco-Li_09:4e:0f (00:0f:66:09:4e:0f) Destination: Cisco-Li_09:4e:0f (00:0f:66:09:4e:0f) Address: Cisco-Li_09:4e:0f (00:0f:66:09:4e:0f) Source: QuantaCo_04:a2:1e (00:1b:24:04:a2:1e) Address: QuantaCo_04:a2:1e (00:1b:24:04:a2:1e) Type: IP (0x0800) Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 207.62.187.7 (207.62.187.7) Version: 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00)0. = ECN-Capable Transport (ECT): 00 = ECN-CE: 0 Total Length: 52 Identification: 0x0a6b (2667) Flags: 0x04 (Don't Fragment) 0... = Reserved bit: Not set .1.. = Don't fragment: Set ..0. = More fragments: Not set Fragment offset: 0 Time to live: 128 Protocol: TCP (0x06) Header checksum: 0xa405 [correct] [Good: True] [Bad : False] Source: 192.168.1.101 (192.168.1.101) Destination: 207.62.187.7 (207.62.187.7) Transmission Control Protocol, Src Port: 49323 (49323), Dst Port: http (80), Seq: 498698563, Len: 0 Source port: 49323 (49323) Destination port: http (80) Sequence number: 498698563 Header length: 32 bytes Flags: 0x02 (SYN) 0... = Congestion Window Reduced (CWR): Not set .0.. = ECN-Echo: Not set ..0. = Urgent: Not set ...0 = Acknowledgment: Not set 0... = Push: Not set0.. = Reset: Not set1. = Syn: Set0 = Fin: Not set Window size: 8192 Checksum: 0x9aca [correct] [Good Checksum: True] [Bad Checksum: False] Options: (12 bytes) Maximum segment size: 1460 bytes NOP Window scale: 2 (multiply by 4) NOP NOP SACK permitted