CS 447: Networks and Data Communications Project #02

Assigned Date	:	: Friday, October 24, 2014											
Due Date	:	Wednesday, October 29, 2014 @ 02:59:59 p.m.											

Overview

The objective of this project assignment is to expose you to the wireshark packet sniffer/analyzer. As for that matter, there is no direct programming involved in this assignment, making this a much simpler assignment with a very short deadline. Having said that, you are highly encouraged to visit the wireshark wiki at http://wiki.wireshark. org/ to learn more about Wireshark and get a feel for its true power as a networking tool.

Procedure

- 1. Install Wireshark on your local computer, if you haven't done already, by downloading the appropriate installer from https://www.wireshark.org/. (On Windows machines, you are also required install WinPcap, which should be prompted as an option during the default Windows Wireshark installation.)
- 2. Start Wireshark but do not start capturing. Enter http as the filter. Also select the appropriate network interface to capture traffic, if you machine has multiple interfaces.
- 3. Start your browser. Clear the browser cache. Enter the following URL at the address bar but <u>don't</u> hit Enter for now. http://www.cs.siue.edu/~tgamage/CS447/
- 4. Switch back to Wireshark and hit Start to begin capturing traffic.
- 5. Switch to the browser again and hit enter to visit the course home page.
- 6. Once the page is fully loaded, switch back over to Wireshark and stop the traffic capture.
- 7. Save your packet capture (*.pcapng)

At this point, your Wireshark window should look similar to the following.

🛋 *W	reless Netwo	ork Connect	ion [W	ireshark	1.12.1 (/1.12.1-0	-g01b	65bf fro	om master-	1.12)]								X
Eile	Edit <u>V</u> iew	Go Capt	ure <u>A</u> r	nalyze	Statistics	Telep	hony	Tools	Internals	Help			_		_	_		
•) 🖌 🔳	1 B	2	۲	0, 1	• •	<u>ې</u>	F 4] ⊕	Q Q 🖻	👹 🗹	- 🌆	% 😫				
Filter	http								▼ Expre	ssion	Clear Appl	y Save						
No.	Time	Sou	rce			Destinat	ion		Prot	ocol Lei	ngth Info							*
	2 1.217	14600 fe8	30::b8	18e:a6	1:ba2f	ff02:	: C		SSI)P	208 M-SE	ARCH * H	ІТТР/1	1				
	4 4.227	36200 fe8	30::b8	8e:a6	1:ba2f	ff02:	:c		SSE	P	208 M-SE	ARCH * H	ITTP/1	.1				
	14 5.168	97500192	2.168.	1.90		146.1	63.15	50.3	HTT	P	366 GET	/~tgamag	e/CS4	47/ HT	rp/1.1			E
	5/ 5.2/1.	23000 140	0.163.	150.3		192.1	58.1.	90	HTT	P	350 HTTP	/1.1 200	OK	(text/	ntml)		UTTO /1	
	59 5.2/I	55100 192	2.168.	1.90		146.1	03.15	0.3	HII	P	3/1 GET	/~tgamag	e/js/	Jquery	-1.9.1.	m1n. js	HIIP/1	. L
	72 5.308	29600 192	1.108.	1.90		146.1	03.13 63.15	0.3	111	P 'D	449 GET	/~Lyamag	e/css	dayony	dnonot	sruse=	nobile,	ueski TD/1
	74 5 208	74200 192	168	1 00		146.1	62 15	0.5		P 10	250 CET	/~tgamag	e/ js/	jquery		1 1	2. js ni	10/1.
	86 5 355	07800 103	2 168	1 90		74 12	5 60	95	HTT	- D	384 GET	/~cgamag /css?fam	ilv-0	rete%2	Pound	нттр/1	1	
1	17 5.363	36100 146	5.163.	150.3		192.1	58.1.	90	HTT	P P	201 HTTP	/1.1 200	OK	(annli	ation/	iavasc	rint)	
1	51 5 397	18700 146	5 163	150 3		192 1	58 1	90	HTT	P	536 HTTP	/1 1 200	OK	(annli	ation/	iavasc	rint)	
î	68 5, 398	58700 146	5.163.	150.3		192.1	58.1.	90	HTT	°P	324 HTTP	/1.1 200	OK	(appli	at ion/	iavasc	ript)	
1	87 5.405	09600 74	125.6	9,95		192.1	68.1.	90	HTT	P	658 HTTP	/1.1 200	OK	(text/	ss)			
2	49 5.464	58800 146	5.163.	150.3		192.1	68.1.	90	HTT	P :	L063 HTTP	/1.1 200	ок	(appli)	ation/	javasc	ript)	
2	51 5.465	51200 192	2.168.	1.90		146.1	63.15	50.3	HTT	P	393 GET	/~tgamag	e/ima	iges/pd	F.png H	TTP/1.	1	
2	52 5.466	19300 192	2.168.	1.90		146.1	63.15	50.3	HTT	P	396 GET	/~tgamag	e/ima	iges/s1	ides.pr	IG HTTP	/1.1	
2	53 5.466	62300 192	2.168.	1.90		146.1	63.15	50.3	HTT	P	394 GET	/~toamao	e/ima	aes/me	nu. pna	HTTP/1	.1	Ŧ
🗉 Er:	ame 2: 20	08 bytes	on wi	ire (1	664 b	ts),	208 k	oytes	capture	d (166	4 bits)	on inter	face	0				
🗉 Et	nernet I:	E, Src:	Intelo	cor_ae	:fc:c	5 (74:	e5:0k	:ae:1	fc:c6),	DSt: I	Pv6mcast	_Oc (33:	33:00	:00:00	0c)			
🗉 In	ternet Pr	otocol	versio	on 6,	Src: 1	e80::	b88e:	:a61:	ba2f:2eb	5 (fe8	0::b88e:	a61:ba2f	:2eb5), Dst	ff02:	:c (ff	02::c)	
🗄 US	er Datagr	am Prot	ocol,	Src P	ort:	2211	(5221	L1), I	Ost Port	: 1900	(1900)							
🗄 Hy	pertext 1	Fransfer	Proto	lood														
0000	33 33 0	0 00 00	0c 74	4 e5	Ob ae	fc c6	86 0	id 60	00 33	t.	`							
0020	0a 61 b	ba 2f 2e	b5 ff	02	00 00	00 00	00 0	00 00	00 .a	. /								
0030	00 00 0	00 00 00	Oc cb	5 f 3	07 6c	00 9a	1f 9	97 4d	2d		.1м	-						
0040	53 45 4	1 52 43	48 20) 2a	20 48	54 54	50 2	ef 31	2e SE	ARCH *	HTTP/1							
0050	5d 3a 3	7a 46 0F	30 00	i 0a	53 54	3a 75	72 6	ie 3a	4d 1:	1900.	ST:urn:	й						
0070	69 63 7	2 6f 73	6f 66	5 74	20 57	69 6e	64 6	if 77	73 ic	rosoft	window	s						
0080	20 50 6	5 65 72	20 40	e 61	6d 65	20 52	65 7	3 6f	6C P	eer Na	me Reso							
00a0	56 34 3	la 49 50	56 36	5 3a	4c 69	6e 6b	40 6	if 63	61 V4	:IPV6:	LinkLoc	a						
00b0	6c 0d 0	a 4d 61	6e 3a	22	73 73	64 70	3a e	4 69	73 1.	.Man:"	ssdp:di	s						
00c0	63 6f 7	6 65 72	22 Od	1 0a	4d 58	3a 33	0d 0)a Od	0a co	ver"	MX:3	•						
0 💅	File: "C:\Us	ers\THOSHI	~1\App[Data\Lo	cal\T	Packets:	804 · E	Displaye	d: 54 (6.7%	· Dropp	ed: 0 (0.0%)							
			1.000										_	_	_	_	_	

Deliverables

Your task is to reconstruct the TCP segment headers and the IP Datagram headers that corresponds to your packet capture. Consult the course textbook for details of TCP and IP header fields. You must attempt to fill in as much information as possible in as much detail as possible. For example, if you have evidence of IP fragmentation (which is highly likely), you must show that using separate datagrams corresponding to each fragment.

In addition, you are required to submit your saved packet capture as evidence of your work.

The due date of this assignment is **Wednesday, October 29, 2014 @ 02:59:59 p.m.**. A Moodle dropbox will be opened for your submission. A complete solution comprises of:

- A short report **in PDF format** that lists your reconstructed TCP segments headers and IP datagram headers. Provide an explanation of your observations. List the number of TCP segments and IP datagrams that was required for your HTTP data exchange.
- The RTT of the data exchange based on your traffic capture
- Your traffic capture evidence in .pcapng format

Similar to the last assignment, submit a compressed tarball that includes your PDF report and the captured traffic file. To create a compressed tarball of the directory source, use the following command: tar -zcvf name111-pr1.tar.gz source/. Obviously, change the name to your last name and 111 to the last three digits of your SIUE ID.