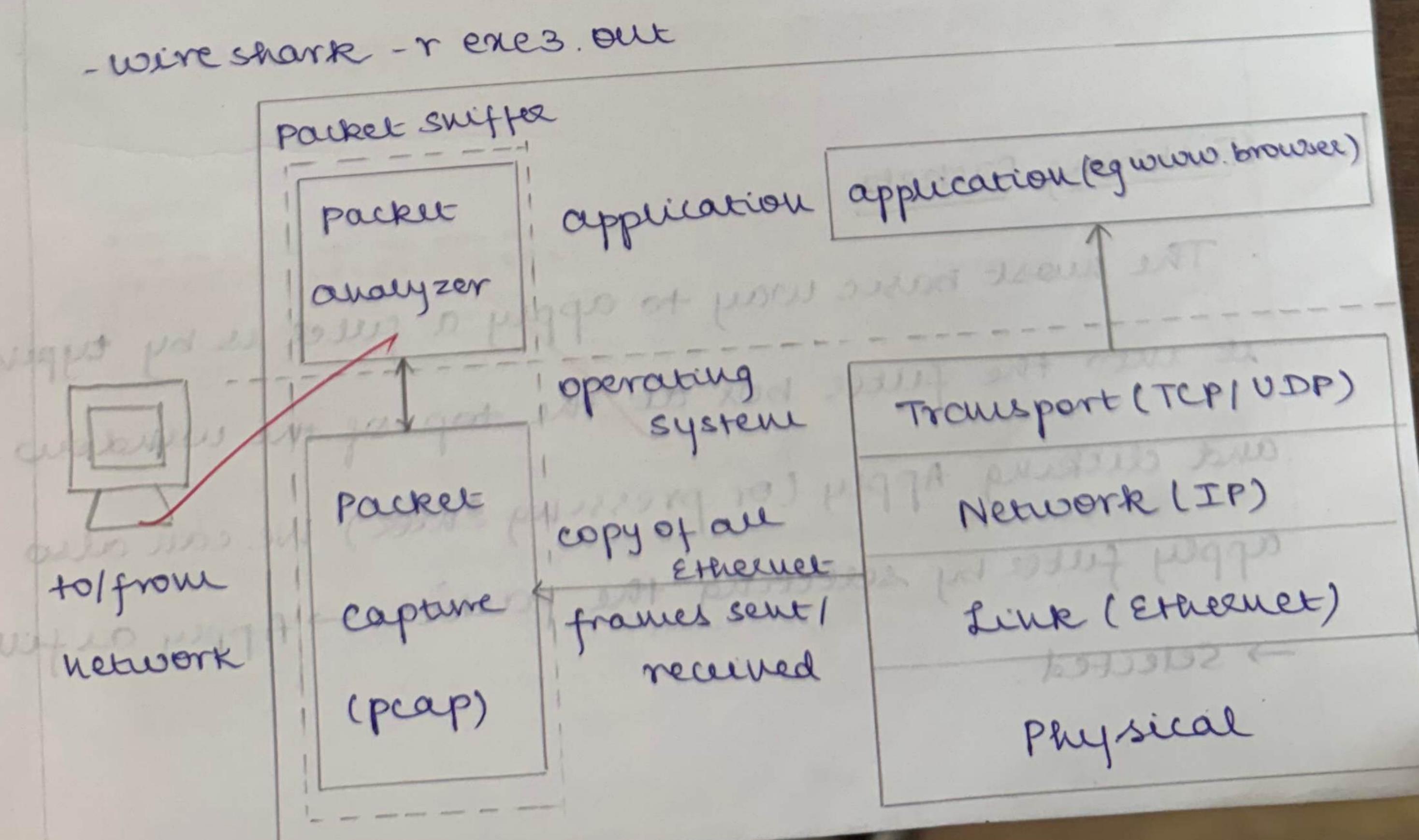
AIM: BESTER CHEST BUSTERS BUS BUSTERS BUSTERS Experiments on packet capture tools: wireshark.

packet suiffer:

- * sniffs messages being sent/received from 1 by 033331323 237A 113393 333395 /A your computer. 1100000 6. 94113910 OF 015 (5.
- * store and display the contents of the various protocol fields in the messages. good est ours (A
- * passive program
 - -never sends packets itself.
 - no packets addressed to it.
 - receives a copy of all packets

Packet suiffes structure Diagnostic. Tools:

- * Typ dump
 - Eg: tcpdump-enx host 10.129.41.2 wexes. out
- * wire shark



capturing Network Traffic: After downloading and installing wireshark lay it and double-click the name of a network inference to capture

Procedure:

Mehta.

State of

the bull

continue

court de

lelines

- 393 91192 7271 2212 259938 4921 87 3312 4 1) select Local Area connection is wire shark
- 2) Go to capture -> option
- DY 201 10 22 MEDICON PAR CONCERTE OF THE YOU 3) select stop capture automatically after 100 packets
- 4) save the packets.

129841 21251209 BOULES 2249N-

37713 8 4 30 7 - 34 100 00 000

729209

22/1/1/2 JUNE 1991

Capturing term ton-IS or East View Go Capture Analyze S or E C C C Q de no [acutics Selephorty Wireless to	
Appello o Magaziny selver + C146-75		
Tomp Source 1 0 0000000 002 168 103 A2 2 0 02001	192,168,101,41 192,168,101,41 192,168,101,41 192,168,101,40 68,218,107,40 68,218,107,40 68,218,107,40 52,123,178,24 52,123,178,24 52,123,178,24 52,123,178,24 52,123,178,24 192,168,101,41	Description of the second description of the second with the second with the second se

Filtening Packets. voisser 1990

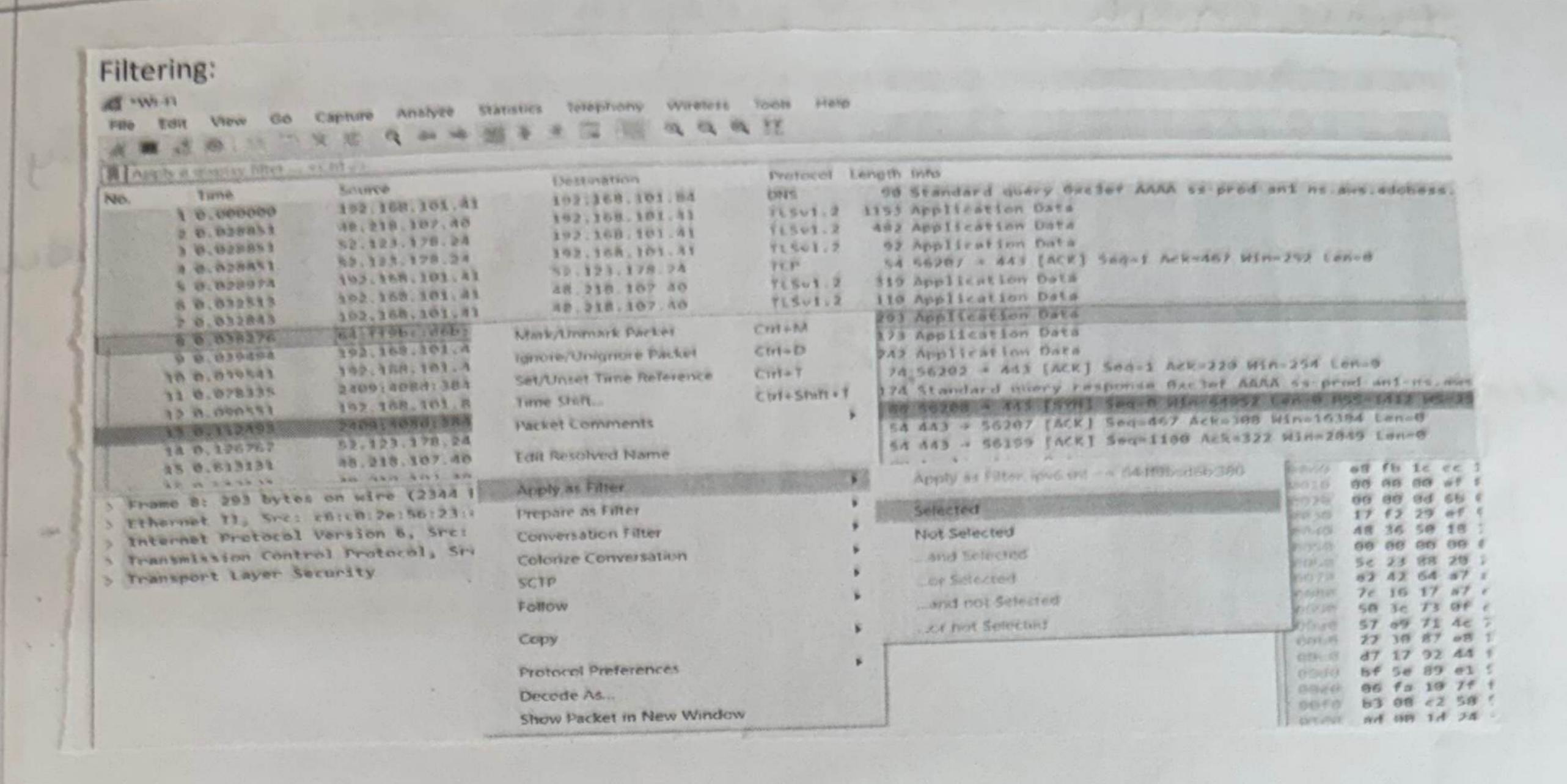
The most basic way to appey a fitter is by typing it into the fitter box at the top of the window

and clicking Apply (or pressing Enter). We can also

apply futer by selecting the packet - Apply as fitter

-> selected.

lavia jusq



38 8.822151 64:ff%b::3445:1373 2486:488d:384:33cb:. TLSv1.2 128 Certificate B2 8.825631 64:ff%b::3445:1373 2486:488d:384:33cb:. TLSv1.2 373 Server Key Exchange, Server Hello Done B2 8.825631 64:ff%b::3445:1373 2486:488d:384:33cb:. TLSv1.2 373 Server Key Exchange, Change Cipher Spec, Encrypted Handshake Message	Time 2 8.828851 3 8.828851 4 9.828851 6 9.832513 7 0.832883 8 9.838276 9 9.839488 18 9.613131 18 9.613131 24 9.815912 29 9.822151	Source 48.218,107.48 52.173.178.24 52.123.178.24 192.168.101.41 192.168.101.41 64:ff9b::d6b:380 192.168.101.41 48.218.107.40 52.123.178.24 2409:408d:384:33cb: 64:ff9b::3485:1373	192.168.101.41 192.168.101.41 192.168.101.41 48.218.107.40 48.218.107.40 2409:408d:384:33cb: 52.123.178.24 52.123.178.24 192.168.101.41 192.168.101.41	TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2 TLSV1.2	2 319 Application Data 2 319 Application Data 2 110 Application Data 2 293 Application Data 2 173 Application Data 2 174 Application Data 2 188 Application Data 2 188 Application Data 2 188 Application Data 3 269 Client Hello (SNIuss-prod-anl-ns.aws.adobess.com) 3 4124 Server Hello
33 0.834449 2409:408d:384:33Cb: 64:1176:3344.33Cb: 64:1176:344.33Cb: 64:1176:344.33C		64: 1196::3445:1373	2409:408d:384:33cb:	TLSv1.2	2 373 Server Key Exchange, Server Hello Done 2 167 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Inspecting Pachels:

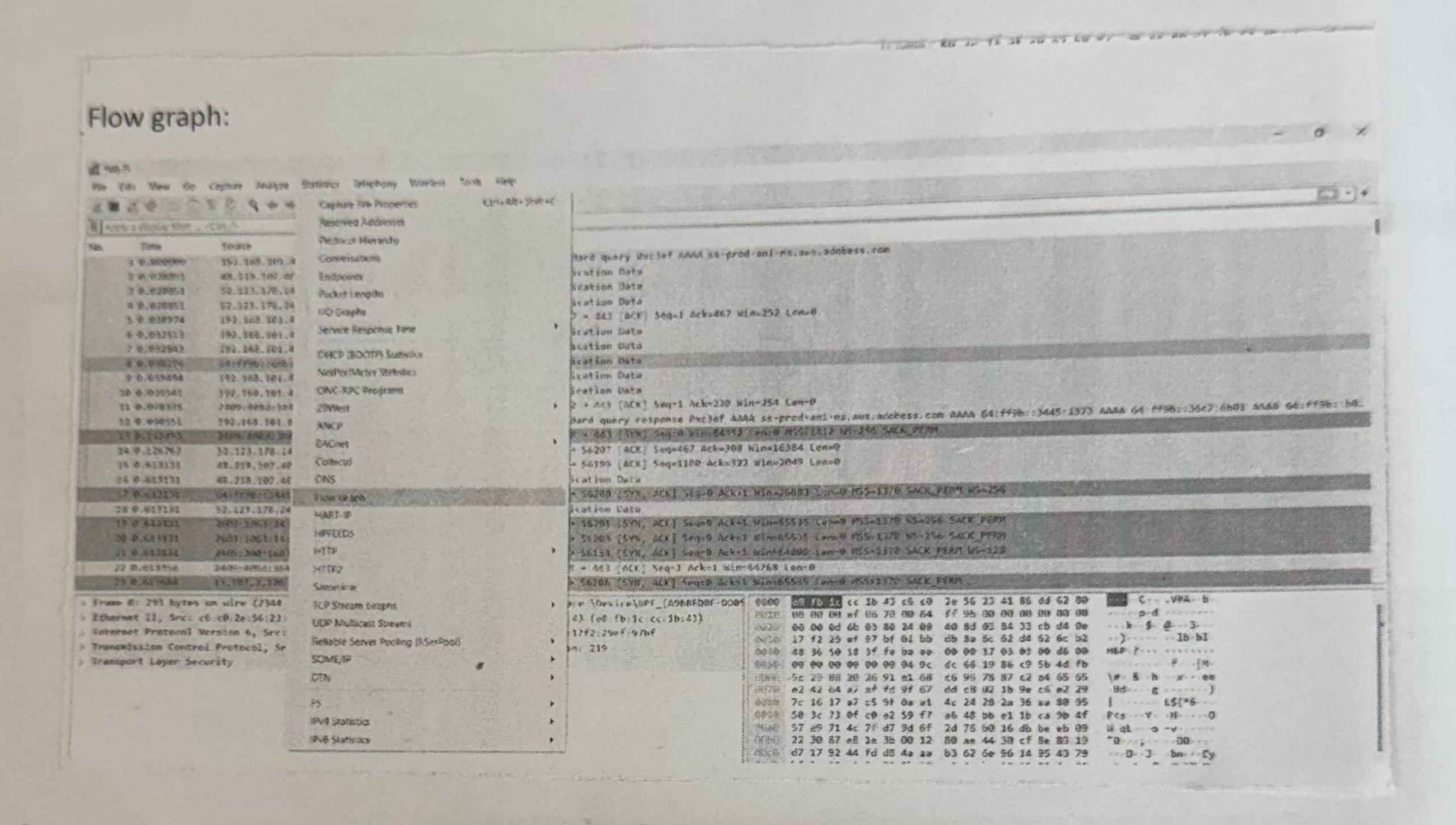
click a packet to select it and you can dig down to view its details.

Inspecting: Capture Analyze Statistics Telephony Wireless Tools Help CRES DEZZ S W # MET L I B S S S I Apply a display bites ... LCsd-/s Protocol Length Info Destination Source Time 90 Standard query 0xc3ef AAAA ss-prod-ani-ns.aus.adobess.com 192.168.101.84 192.168.101.41 1 0.000000 1153 Application Data: TLSv1.2 192,168,101.41 48.218,107.40 2 8.028851 482 Application Data 115v1.2 192.168.101.41 52,123,178,24 3 6.028851 92 Application Data TLSV1.2 192.168.101.41 52.123.178.24 4 0.028851 54 56207 - 443 [ACK] Sen=1 Ack-467 Win-252 Len=0 TEP 52,123,178.24 192.168.101.41 5 0.028974 319 Application Data 11542.2 48.218.187.49 192.168.101.41 6 6 432513 110 Application Data 11541.2 48.218.107.49 192.168.191.41 7 0.032843 2A09:488d:384:33cb:... 715v1.2 293 Application Data £4:ff9b::d6b:380 8 0.038276 17) Application Data TLSV1.2 392.168.101.41 52.123.178.24 9 0.039494 242 Application Data TL5v1.2 52,123,178.24 192.168.101.41 10 0.039541 74 56202 - 443 [ACK] Seq=1 Ack=220 Win=254 Len=0 2409:408d:384:33Lb: 64:ff9b::d6b:380 TEP 11 0.078335 174 Standard query response Exclet AAAA ss-prod-anl-ns.aus.adobess.com AAAA 64:ff9b DNS 192.168.101.41 192,168,101,84 12 0.090551 86 56208 + 443 [SYNT Segre Win-64952 Lense MSS-1412 WS-256 SACK PERM 7409:488d:384:33cb:_ 64:ff9b::3445:1373 105 23 0.112493 54 443 - 56207 [ACK] Seq=467 Ack=308 Win=16384 Len=0 TCP 192.168.101.41 52,123,178,24 14 0.126767 54 443 + 56109 [ACK] Seg=1100 Ack=322 Win=2049 Len=0 TEP 48.218.107.40 192.168.101.41 15 0.613131 > Frame 9: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF_{A988FD@F-DO@5-415A-A71C-7A@03459E93B}, id 0

-) Ethernet II, Src: AzureWayeTec_cc:1b:43 (e8:fb:1c:cc:1b:43), Dst: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41)
-) Internet Protocol Version 4, Src: 192.168.101.41, Ost: 52.123.178.24
- Transmission Control Protocol, Src Port: 56207, Dst Port: 443, Seq: 1, Ack: 467, Len: 119
 Transport Layer Security

From Graph:

We can see the from graph of the packets by clicking on the statistics and selecting the from graph of the graph and it displays the from graph of the packets.



Time	192 168 101 41	192.168.101.84	48.218.107.40	52.123.178.24	64.99brc6b.380	Comment
0.003000	MANUFACTURE OF STREET	or the Andrew product resourceston.		CONTRACTOR DESCRIPTION		DMS: Standard query DMSet AAAA se proprient insuestant
0.028851	Will p	Application Date				Ti Self-2 Apprission Subs.
028851	M207 -	Application (Sept.		417		TUSO & Application Comp.
028851	5000	A00/20/20 20 20 20 20 20 20 20 20 20 20 20 20 2		443		Tulis 1.2: Apprication Date
028924	54307	19,250 = 44.1 (42.30 Seq 24.444, 1974-29.5	2099			YOP SERVE - 44% (MCH2 Serger E Accessed William 25%) Land
032503	442	September 1 49	× 443			7,271.2 Apportation Date
(5284)	2020	Nett Asker Dally				FLSVA & Application State
38276					AND AND	possession (Fig. 705x2 & Appelication Date)
39494	3420			443		TuSelf-2: Appriorition Date
19541	40	Zingki mini Sain				TLEVAS Application Date
78335					36000 - 440 ACC S	69-1 402" TOP 19202 - 463 (200) Sepan Assault 2 Workship
10551	Acres Services and the	NAME OF STATE ASSOCIATION OF THE PARTY OF TH				
3493						SMS Vandard query response the het AAAA, as grou
That I	MET	- 3023" MC13 Zec+45" Ad-274 VA-475 VA	(Bray			With Maria — and Sanit Superior State of the Control
91	3210	343 - 54 90 JVX (544 = 115) Aprel 12 West 2015 (554)	443			TCR-465 - \$6207 JACKS Sequeler Actuality Works
181	200	Appropriate these				76,74 445 - 54,109 (ACA) Seque 17,30 ASSAULT MICH.
35						Tuber & Application Date.
b)	1400	Approximation Days				NOR AND IN TRACTOR SPECIAL SERVICE SER
31	Amandelia de la companya de la comp			**1		%%22 Applitation Sola
tume make a manual	and the same of th		Annual An	The state of the s		308-443 - 3020 (SIN ACQ 844-0 ALV-) "VIO

create a filter to display only DNS parkets and provide the flow graph:

procedure:

- -> 010 to capture -> option
- select stop captive automatically after 100 paints
- -> Then click start capture
- -> search DNS packets in search bor.
- -> To see frow graph click statistics -> Flow graph
- -> save the packets.

9 0.039494

Domain Numer System (query

capturing and Filtering:

For DNS: *Wi-Fi File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help PEGGRAFIE QQUI dns Protocol Length Info dns Destination Source No. 90 Sta dnsserver DNS 192.168.101.84 192.168.101.41 1153 App TLSv1.2 192.168.101.41 48.218.107.40 2 0.028851 TLSv1.2 482 App 192.168.101.41 52.123.178.24 3 0.028851 92 App TLSv1.2 192.168.101.41 52.123.178.24 4 0.028851 54 562 TCP 52.123.178.24 192.168.101.41 5 0.028974 319 App 48.218.107.40 TLSv1.2 192.168.101.41 6 0.032513 110 App TLSv1.2 48.218.107.40 192.168.101.41 7 0.032843 293 App 2409:408d:384:33cb:... TLSv1.2 64:ff9b::d6b:380 8 0.038276

192.168.101.41

第 在 图 150 至 2		* 并且自然我!		13 = 2
6				
pm	Source	Description	Protocol	Length Irdy
ancienes persons	192 168 101.41	191 158 101 84	995	56 Stendard query 8xc34f Abba 52-prod-an2-na, aux. adobess com
12 6.058551	192.168.161.84	192.168.191.41	DNS	578 Standard numry response Brider Add suspred on the aux adobers the hand 64: ffsb : 1445: 1373 Add 64: ffsb: 1867-6501 Add in ffsb: in
105 10.738520	197.168.101.41	199,188,191,84.	086	74 Standard query Gallel & assets.mon.tom
107 15.735001	192.458.101.41	192.165.191.84	2015	76 Standard query Brötist AAAA assets esm. som
100 20 045529	193,168,181-41	197.165.101.84	BM5 .	76 Standard query Robotic AAAA atsexs.aso.com
199 26.649529	192 168 101 41	192.165.161.84	DNS	74 Standard query 0x19:1 A satela.man.com
3.18 20.060379	192,168,161,64	197,168-181-41	1955	74 Standard query Pasponce Sulfet A access son com course assets son com edgelog bet Chine 928378. 4 absendedge set A 40. 64. 7196: 3
113 26-100339	192,165 103.64	167 166 151 41	\$115	
116 20.100109	192.168.101.66	192.168.161.41	D95	
115 29 130322	192,168,101.88	102,108,103,44	245	ANY Standard spury response waters when events may use them was not been assess that
116 26 799083	192.168.181.41	192 168 103 64	DAS	52 Standard gurry Dr. 5695 A my microsoftpersonal content 5000
27 28 259673	192,169,101,41	167.158.101.64	915	91 Standard query babal? Aska my. microsoftpersonalcontent.com
113 20 305619	LVZ-165.191.85	177.158-191.41	DUS	93 Standard query response Widovs A my microsoftpersonalcontent.com Class los itunderd query response Widovs A my microsoftpersonalcontent.com Class los Cause Los Cau
19 23 10,5916	192,349 101 45	297 358 593 84	065	21 Standard Query Debut? Abob my microsoftpersonal content con
29 21.653128	192,160.191.84	197, 168, 191, 41	945	21 Standard query response Pabel? Abbb my.microsoftpersonalcontent.com (NAME lists-m.tm-et-sharepoint.com Chara 104024 inviste-gr.q
20 24.574027	192,168,161.65	107.158.101.84	916	101 Standard query DESC11 A 191767-15va.gr. global. 48'75. Nodec Wolley.
	157.168 101.41	197 348 101 64	085	in: Standard gues / Dx159c 4444 191767-lpvd.gr.global.sa-rt.sharopoint.com
	192,160,101,41	197 -168 -101 -64	045	102 Stondard query RelS91 4646 191767-ipv4-pr.global.agrat.aburapoint.com
EF DELINESPER	592.164.101.41	191 154 191 64	5915	102 Standard query Brocil A 191767-16v4.gr.global as-rt.sharepoint.com
	197,168.181.86	192,168,191,41	205	102 Standard query Process 0x159x AAA 191767-1804.gr.global.wa-re.shurupolue.com Chief 191767-1804.furm.dprodagdios.au-re.shurupolue.com Chief 191767-1804.furm.dprodagdios.au-re.shurupolue.com Chief 191767-1804.furm.dprodagdios.au-re.shurupolue.com Chief 191767-1804.furm.dprodagdios.au-re.shurupolue.com
AN ANCONOLOGY	197.168.101.84	192.368.303.43	DNS	173 Standard query response 0x159x AAAR 191767-1914-Hr. Richar. Marris than Child 141767-1914. (urm. darqueoditis un rt. sharepoint ties Standard query response 0x151 A 191767-1914-Hr. Richar. Marris than execute the Child 141767-1914. (urm. darqueoditis un rt. sharepo
	192.199.101.84	202.268.201.41	305	121 Standard query response Ballies AAA 121767 prd. gr. global as rt. sharegoint.com Chies 131767 prd. farm. dprodugdles as rt. sharegoint.com Chies.

popular an withouth or encount and more mand

TLSv1.2

52.123.178.24

173 App

Inspecting:

e ane", Ju

COM

23211

» PA

d previous town	AV H		CONTRACTOR DATE OF THE PARTY OF
	PARED MODEL		DATE OF TANKE STANDARD AND AND AND AND AND AND AND AND AND AN
Seaso	one manufactures		CHALL CONTROL WAR A POPULAR DICES AS NO SE PROCESS
L'ES KOD	one and the state of the state of the state of		Chica Stanton's main Double in Management Long
C-002031	Add a second sec		THE DAMES DAME HALL SHEET MACHINE
173878	un marron de recursos de la companya		While Deprovement to the second or the second
DEPREM			ESSO DISPOSED BURGO DE LA CASA ANTINOMINA
0.001239	Name of the second seco		DOLYGO SERVICE AND PROPER DESCRIPTION OF THE SERVICE S
5-6455/9	Marin phone and the same of th		grap classical plans recognition to the television recognition of
aniayra	ON SHE STEEL ST. AND		CHIE STANKING FROM MODELY & BANKS HOUSE !
TWIZE	COLUMN TO THE PERSON AND ADDRESS OF THE PERSON ADDRESS		(Disk Sprished Busy) resorted Substantial House propin north
find) rs	And September of the second of		CONTRACTOR SUN SOURS & MUNICIPALITY
316123	drift American in the American		CHES EMPTHEN DON'T MALL TO CHISTOPHE TO THE
7/05/01	egh butters appetite an appetite of		END SUPPLIED GOVE ANDROOM BURRED & PULLED AND AND AND AND AND AND AND AND AND AN
COLLA	Depresentation and the second section in		CONFERENCE HAVE TO BEET SALES SHOWN FOR THE PROPERTY SALES SHOWN FOR THE P
neco			THE STATE SHOW SELD IN WAS IT ELLER AS INCHES
1011254	The Manual of the Control of the Con		Cuc continue tent proper to a compact to the Com Mar
CALINO.	The latest temperature and the second		OND SWEET LIP, ATTOCKED WITH THE OWN OF THE
14515	NOW DESCRIPTION OF THE PARTY OF		
300	an terminate with the same		Comp placement that on operative states that the debates
P5843	Due short-new and we revere the		Care datable a complete the base to
16172	TO BE SEED OF THE PROPERTY OF THE SEED OF		CHO DE 4011 SUPY MARKE NOW SLAVE OF CALLER
am re	- STATE OF SECOND STONE SECOND		
es se a serviced par	TOTAL TOTAL PROGRAMMENT TO SECURITION OF THE PROPERTY.		Administra July
nn Graffestes Dies		Fless Agent Ad Picture	Recel Disprais Depos Come His

27 27 2011 2011

Flow Graph:

4 704		TO STATE OF THE PARTY OF THE PA	FILE					- 0 x
in Ads 100 - 20	CONTRACTOR STATE	sules tricken states	u lan n					
	1 0 10 1 m	Service Constitution of the Constitution of th						
# 41 S	X P Y P P III	14.2 . 五日日	411		Street !			75-47.
lens			-					自己・一・
Sien	Signer	Denneton	Person	serge ato				
ים מינאלינים נ	(0) 161 (0) (0)	1)/ 143 105 105	90	and trimpland greety that he's paste and one on any state of the				
14 6 MADE	174 110 101.30	LA. 213 - BELL UIT	70	Its resolved many proposes truly again as product as exclusion	par con	LUL AS 159 1540-1110	CLLC 2011/9-1 HET-1822 &	WA 64 99 05 1100
186 16-7135/F	197 (64 10) 41	19/ 134 391 PT	250	N STANLEY BURNS BURNS & HARLE DEN. 100				
107 5F (1103)	197 100 101 41	177.109.131.00	UNO	The between genery Badens and a state of a con				
HELLED ON PHE	117 710 101 11	14 111 111 VIT	200	14 Michael winers appear has assertation and				
TOD ST CANADO	112.165.161.41	180 (CV 152 24	975	the Francisco query Dilling & arrests reso, the				
IN NO MOUTS	131.140 101 34	IN IN IN SI	200)	200 Middle of many response trites A surely randers Care exist	the partie	existency and cooks als	DAN d. phopleter on a 54.	64 111 197 B 49.
113 30 198230	101 144 144 144	1231 1134 111, 41	205	and Secretaria mater opposite tradule apply estern new sea cours of				
110 20 101717	104 114-161 44	Tra 111 171.41	- 966	EN SCHOOL WALL CANDING CLERC & REPORT AND THE PROPERTY OF THE		Designation of the Party of the		
ात व्य पालाम	177.110 DFL-50	HILLIE THE AL	295	at sometion want resource describe have office our con the el				
715 0 (VE)	12.114 012 101	111 110 101 FO	345	re soundard quary expects a resolution transportant son				
117 PS THOUTI	150 160 101.01	TIZ-U1: 121 10	that	to brandara many basall was so elerated wer sensions and ele				
110 DT PRASS	D4 767 101 M	110 114 117 10	200	400 bisodard giora resonno codos a on elerosoftsorsonaltentes		שתו ווונו בונו מושו	epulse ion trung 194844-ip	rhoto er global .
117 200 lette	es on alen 19200 Ale	200 bytes contami	e ferme ale	.) in the level of the second of the and the second the second	Han .	on 64 14 45 10 61 46 40	7- 12 27 E AL 10 C AZ	£ 700 £
				of a Did (of the Schieffers)			34 TO LO AU 69 14 (0 48	1 40 cl
		BE 141 34 GVL 191		e = C Sitt Canara Science any			79 10 Sc or 01 80 00 01	0) 110
			200 200 03				79 73 60 74 73 91 64 73	a costa si
	101 300 Per 1 31, C	At June 1 41513			455.5	to 03 03 06 66 00 00 10	00 01 18 04 60 05 69 67	A DEAR
alo dane Esitos	(PRIDUCLE)						18 23 15 15 M 20 EK 81	m o carlo a
					pina (CO 01 61 61 61 67 69 EA	63 85 89 85 79 81 Co 85	e tip od gaben o
					BEEFE ?	76 62 50 75 60 60 99 81	60 to 92 8f 66 58 fr 42	1
							RI CO SI CO OI CO PO SA	
	In the second second			THE RESIDENCE OF THE PARTY OF T	Action 4	\$7 80 CO KS CO 14 00 S	01 en 10 en en en 18 en	Bo 6 7
							AN OF ME DE LI Se DO ME	

Result:

Thus, the experiments on packet capture tools like capturing, inspecting, futering and displaying flow graph in wireshark is successfully executed.