Ain: - Experiments on Parket capture book: Wirespark

Parket Sniffer: -

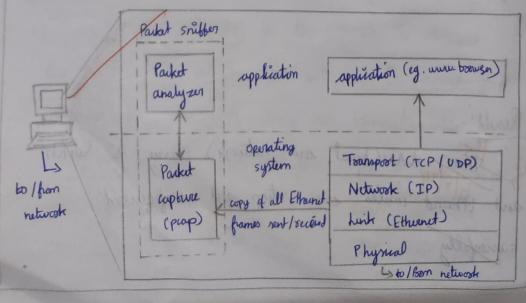
\* Snifts menager being seht locrewed from by

your computer.

- \* Stool and display the contents of the various pootsocol fields in the menages.
  - \* Parine porgram.
    - heren sends parkets itself
    - no parkets addressed to it
    - seceives a copy of all parkets.

Parket Souther Diognostic Tools:

- \* Top dump
  - Eg: tapdump en x host 10.129.41.2 wexes.out
- \* Whie shart
  - wire shark or exe 3. out



Capturing network truffic :-

After downloding and installing wireshank lanch it and double-distr the name of a network inference to capture.

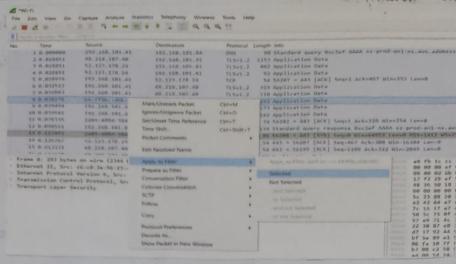
- Select hocal Ased Connection in
- 2) no to capture -> option
- 3) Select stop capture automatically after 100 packets
- 3) Save the parkets.

## Output :-

Ten-	Source	Destination.		
5. E.360600			Protocol	Length lato
	150.368,301.41	192,160,301,04	1115.	M Stanford every declar AAAA as-productives, each adobase, com
2.9.102512	45.218.107.20	192.166.101.41	TLS=1.3	1153 Application Data
		197.168.181.41	71.5-1.2	482 deplication flats
		192,168,181,41	T1.5v2.2	93 Application Outs
	197.169.101.41	52.123.178.24	TEP	34 54207 - 443 (ACK) Seq+3 Ack-407 Min-253 curve
	172.168.201.41	48.218.107.40	TL5v1.2	319 Application Data
7 ALEXUSAS	192 168 161 61	46.218.107.40	T15-1-2	110 Application Date
0.000076	54 FFSb: 185b: 300	2407 4054 354 3346	715v1.2	293 Application Data
	170.160,161.41	52.123.178.24	TL9v1.2	173 Application Data
		57-123-170-24	TL5v1.2	241 application Data
	3499-4862-354-53151-	64: 1790: -066: 520	TCP	74 56202 - 441 (ACK) Sount Askn220 Nino256 Lanco
2.0.00051	292,360,505,64	172,168,101,41	DVS.	174 Standard query response Onchef AAAA sarprod-ant-no.eus. adobers.com AAAA 64:ff9b::3445.1375 AAAA 64:ff9b::3647.6665 AAAA 64:ff9b::364
H. E12813	2403 4067 304 33551	54 (196 ) 3445-3372	TCP.	m 54/200 + 443 [573] Sept Mirachtory Lend (55/141) 85/276 Sult FISM
A R. 126767	57 133 176.24	192 368 301 A1	TCP-	54 443 + 54207 [ACK] Sequido? Askx 300 Mirrs 10 384 (most)
0.021231	48,318,107,40	192.160.101.41	100	54 44) - 56105 (ACR) Seq-1100 ACR-122 Min-2045 (en-0
2,012,010		192.165.101.41	11541.2	99 Application Data
7.8E-8039458	64-7736-3445-3573	2409 4604 384 350bill	106	85 443 + 50206 [179, 4/8] Seq.6 Schol Min.2683 Lench H56-1376 SACV FF28 W5-256
P.427271	52.225.178.24	192, 166, 101, 41	TL5v1.2	100 Application Data
W. 421255	2683 3863 5811	2485 4564 NAC 354	ICP.	00 443 - 50201 [579, ACK] Sep-0 Ackel MineSSSSS Lemon MV5-1270 MoneYet NATH FROM
P RESIDER	2681-1861-14	2489 4884 384 3345	TOP	86 443 - 56283 [SNA, ACK] Sequél dabai Win-65535 Lance MSi-179 Mingle Sack Clem
F-421121	24H-2013447(37)31-	2401-4654-384-33451-		86 463 - 50134 [579, ACK] Sone-Gackel Wirescape Cores Manager Manager Manager Manager
2.631756	2489 4664 184 13ch	64.ff8b::3445:1373		78 56208 - 443 [ACK] Sep-1 Acks] Min-64768 Len-0
	0.000012 0.000012 0.000012 0.000012 0.000012 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.000001 0.0000001 0.0000001 0.00000000	1 R. STORMEN S. S. 22 S. T. S. 24 S.	\$ 8,000.00 \$1,000.10 \$2,000.00 \$10.00	\$ 0.00000000000000000000000000000000000

Filtering Parkets:-

The most basis way to apply a filter is by bypany it into the filter box at the top of the window and chiling toply (or preming Enter). We can also apply fitter key selecting the parket -> Apply as Filter -> Schukel.

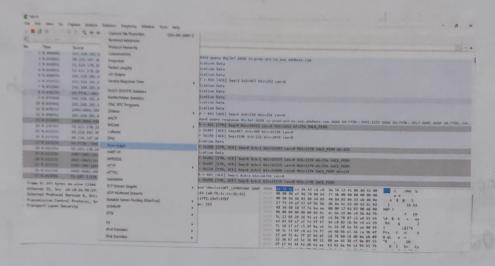


Chit a packet to relat it and you can dig down

No	Time 1 0.000000 2 0.02851 3 0.02851 4 0.02851 5 0.028924 6 0.032513 7 0.032841	192.168.101.41 48.218.107.40 52.123.178.24 52.123.178.24 192.168.101.41 192.166.101.41	197.168.101.41 192.168.101.41 192.168.101.41 52.123.178.24 48.218.107.40	DNS TLSv1.2 TLSv1.2 TLSv1.2 TCP TLSv1.2	482 Application pata 92 Application to the second of the s
	8 0.036276 9 0.030494 10 0.030541 11 0.078335 12 0.090551 13 0.112893 14 0.126767 15 0.613131	64:ff9b::d6b:380 192.165.101.41 192.166.101.41 2409:460d:284:33cb: 192.168.401.84 2409:460d:384:33cb: 52.124.178.24 48.218.197.40	2409.408d;384)33cb: 52.123.178.24 52.123.178.24 64.179b::d6b:360 192.168.301.41 64.179b::3465:3373 192.168.101.41 192.168.101.41	TLSv1.2 TLSv1.2 TCP DNS TCP TCP	110 Application Data 129 Application Data 123 Application Data 124 Application Data 125 Application Data 126 Application Data 126 Standard query response Oscilef ANAA ascypcod anima. Amer. Andobuss.com AAAA 64:ffg 126 Standard query response Oscilef ANAA ascypcod anima. Amer. Andobuss.com AAAA 64:ffg 126 Standard query response Oscilef ANAA ascypcod anima. Amer. Andobuss.com AAAA 64:ffg 127 Standard query response Oscilef ANAA ascypcod anima. 128 Standard query response Oscilef ANAA ascypcod anima.
Fr Et In	chernet II, Src:	on wine frame as	173 bytes captured (13 (eB:fb:1c:cc:1b:43), D	84 bits)	on interface \Device\BF_(A988FD6F-0005-415A-A71C-7A803459E918). Id 9

Flow Grouph: We can see the flow graph of the parkets by clicking on the statistics and relating the flow graph and it displays the flow graph and it displays the flow graph and it displays the flow graph of the parkets.

Output:-



See	192,162,101.41		48.218.107.40		64.89b;:d6i.300	
		192.168.101.64		52.123.178.24	10000000	Comment
MONTHS .	And Department of the	Manager of Committee of				
28657	55 m	Appelled tex				DMS Stambard query Sector AAAA do groot-got-roleadus NS-12 Appriation Sets
100001	-	Appelle	30			Table Application date
V5053	SEE A CONTRACTOR OF THE PARTY O	ARTHR	10			NATA Application date
2074	200	BUT AND DOCUMENT AN	HERMINISTER.			
12513	-	58 m 50				TOP SEED! — HES JACKS BEAM ALEXAND SETTINGS LAND. TURN THE PROPERTY OF THE PRO
12047	SER PROPERTY.	1000000				Table Appropriates
10276					N 41	CONTRACTOR DES
19454	Mar mercenness	AUT SEC.	in.		3 4	
9541	and principles	1000	(4)			Total 2 Approximen Date
1115					Mills - Advances	TOTAL AND NATIONAL DISS.  NO. 1 AUGUST 1800 - AND AND SHOP I AND AND SHOULD MAKE A MAKE THE PARTY AND
951	AND ADDRESS OF THE PARTY.	CONTRACTOR OF STREET			40	
1401						Deligible and among print over the fact to
6367	100					TO SETS - NO SING Sept STANDED LOT AT SETS
1121	(ret w	set of the Property State and Association and Association and				107-445 - 1620" (ACH) Sep-467 Apr-208 (En-1628)
100	-	500 Sept. Sept.				VIN ARE - 18100 (ACC) Sept 1155 April 223 (01-2240)
1131						Tarta Aperiator Data
1131	201			M		NO. 40 - MARK DAY, ADD THE P. ASSAULT AND A SECTION ASSAULT
1121				Total Control of the		Tablic Appropriate Data
	-					SPARE - MIT DIS ACCUPANT STREET
		Company of the contract of the				
		CONTRACTOR OF A PROPERTY OF TAXABLE	/ /			
t to properly the			Flow type: Ad I	266		Addresses. Any
et 20 75% and -362 until to deplay fit		Lamond HISS + 1870 HIS + 258 EACH, PARM	Flow type All I	loss -		Agazen

Create a Filter to display only DNS packets and provide the flow graph.

## Possedure :-

- -> Go to capture -> option.
- -> Select stop capture automatically after los parkets.
- -> Then chits start cupture.
- -> Search DNS parkets in search ban.
- -> To see flow graph with Statistics -> Flow graph.
- -> Sure the parkets.

Capturing and Filtering:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools He

d	ns					
No.	dns	Source	Destination	Protocol	Length	Info
70	dnsserver 80	192.168.101.41	192.168.101.84	DNS		Sta
	2 0.028851	48.218.107.40	192.168.101.41	TLSv1.2		
	3 0.028851	52.123.178.24	192.168.101.41	TLSv1.2		
	4 0.028851	52.123.178.24	192.168.101.41	TLSv1.2		Арр
	5 0.028974	192.168.101.41	52.123.178.24	TCP		562
	6 0.032513	192.168.101.41	48.218.107.40	TLSv1.2		
	7 0.032843 8 0.038276	192.168.101.41	48.218.107.40	TLSv1.2	110	-
	9 0.039494	64:ff9b::d6b:380	2409:408d:384:33cb:	TLSv1.2	293	
	0.039494	192.168.101.41	52.123.178.24	TLSv1.2	173	

die .	Source	Destruction	-	
departer	TN1-160-581-61	197 108 101 44		Length late
33 e.esessa	377-365-381-64	197 168 101 41	DNS	
106 15,738520	101.105.131.41	197.145.101.41	06	176 Mandard query response Rechef AMA to Account
107 12 739011	\$10,255,101.45	192 105 101 54	Dis	16 Standard query response for all AMA is produced on an abbasic con 26 Standard query response for all AMA is produced on an abbasic con 36 Standard query public à assistance and produced on an abbasic con 36 Standard query public à assistance and are produced on an abbasic con 36 Standard query public à AMA acut and 36 Standard query public à AMA acut an 36 Standard query public à acut an 36 Standard query public à AMA acut acut acut acut acut acut acut acut
1527.00.5521	387-195-101-42	192 166 181 64	Ditte	74 Standard query Bribait AMAN assets.acc.com
101 Dr. B41525	310,160,101,41	197 108 101 04	Dres	16 Mishfard Query Post-N. Abbs states and
THE DR. MINELTS	\$31,366,361.84		CRS.	
137 80 565510	192,166 101,46	150.160.501.41	1365	
124 26 300339	202-100-101-64	174 105 101-41	596	Office and the state of the sta
145 24-510552	252,168,101,04	1941349-101-01	DNS	277 Mandard quary response dutted & section and top their starts own one edge-top not 1200 to 2 startings not 2 49 da 110 150 a
the ser Premiers	And then 185 44	257.055.101.41	Ensi	403 Standard geory resource duties and a state out of the control
117 20 750675	381,165,101,41	177 518 301 54	Dies.	91 Mandard many desired & see all county
125 26 Maries	101-105-201-04	192,166,101,84	DNS	
19.21-3e3855	197-165-601-41	192-160-301-61	205	436 Mandard query residence de los a
20 21.153120	274, 198, 161, 84	352 266 201 34	DHS.	PI Standard guary duball also
20 44.574527	107 116 101 41	152 165.101.41	CHIS	on become more could and existence for consistent can be limited from the consistency of the limited are required that a publication of the limited can shall also existence from the consistency of the limited can shall also existence for consistent on the limited can require about also existence from the limited can be consistent on the limited can require about a first and existence from the limited can be consistent on the
21 24 575177	212-116-101-41	153 368 305.64	150	
37 24 BYSSA	197 (65 18) AL	252 268 102.86	DHS	100 Manufard owner in the control against against a part abarragement of the control of the cont
		1767, 1607, 1603, 164	2005	187 Mandard query delayer And 1912; (put.gr.globel as et sharepoint con 187 Mandard query delayer And 1912; (put.gr.globel as et sharepoint con 187 Mandard many deliver And 1912; (put.gr.globel as et sharepoint con
21.04.80h3/2	251,356,301.41	112.355.501.84	DNS	182 Mandard American Street Street Street and Pt. Chargestint Loss
14 14 128578	192.195.191.64	292-169-101-41	400	17) of collect con-
25 24.528574	239 218 192,86	250.168.302.43	DMA.	161 Manager
29 24,936973	191.166.101.44	299-168-101-01	Disk	191 Stander despression from L. 5 (1916) specify global are in française and Comp. 1910. Spec. From Agricultural Standers and Comp. 191

Insputing: Flow Graph: correct the test to being topy transming cale concept on the binary data and O Received program should need the expert atal frameway who we the berand data Result! -Thus, the experiments on parket apture touts tike capturing; inspecting, filtering and displaying flow graph in wirehark is succenfully exented.