Demystifying Networking Prof. Sridhar Iyer Department of Computer Science and Engineering Indian Institute of Technology, Bombay

Lecture - 66 Port number in Wireshark

Now, that we have talked about concept of application layer, let us see how it actually works.

(Refer Slide Time: 00:07)



Hello and welcome to week 3's video on Port numbers. So, we know port numbers are used to distinguish communication for different applications, for example; the websites used port number 80, so, your browser knows that this packet is being sent to a server and it has come from a server and when your browser is sending out the request it attaches its own port number. So, now we have seen these things in packet tracer. So, what we thought it would be a good idea to actually see them on Wireshark.

(Refer Slide Time: 00:43)

 sue Audjar Sactos Replay Weles Tool Hep 20 S + + = 1 + 1 = 1 = 1 = 1 = 1 = 1	
	C3 - Egrann.
Capture La Marchander Constant -	
LASTR Mar Valle - Mil - Gaustian and Amazon - Malling Late	

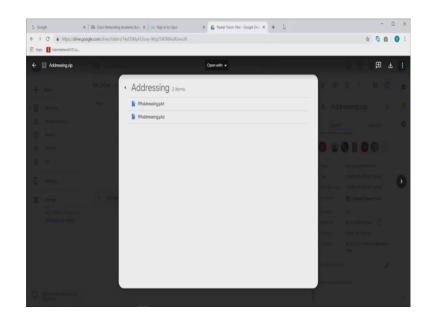
And what we will do is, let us open Wireshark and let us see how on real time traffic we can distinguish traffic for different applications. Now, we will use the Wi-Fi adapter that is used in this card.

(Refer Slide Time: 00:55)

		* II * X		4.4.4.2			
Papers & display Mare						CI - Inre	-
th Tana	Source De	dealer	Yufacal Le	ngh 34e			
3.0,00000	1 192,160.1.1 2			335 MOTOFY * HTTP/1.1			
	192,168.1.1 21			116 NOTIFY * HTTP/1.1			
5 0.012012	192.168.1.1 21	9.255.25. 5	SEP	337 MOTTEY * MITE/1.3			
6.0.029653	192.168.1.1 2	0.255.25. 5	508	128 MOTOFY * HITP/1.1			
	192.168.1.1 7			392 MOTERY * HITE/1.1			
8.0.029650	102.168.1.1 7	0.255.21. 5	520	376 MOTIFY * MITP/1.1			
0.0,029655	192,168.1.1 21	0.255.25. 5	504	337 MOTIFY * WITE/3.3			
10 0.05058-	192.168.1.1 21	0.255.25. 8	SDF	396 KOTIFY * MITEVLIT			
11 0.050590	192.168.1.1 2	0.255.25. 5	808	337 BOT1FY * BIT1P/1.1			
12 0.030583	102,168.1.1 2	9.255.252 5	500	398 MOT3FY * HTTP/3.1			
138,05058	192.168.1.1 23	0.255.25. 5	SOP	376 MOQIFY * HTTP/1.1			
14.0.030588	192,168.1.1 21	0.255.23. 5	300	337 MOTORY * HTTP/1.1			
15.0.050585	192,168.1.1 21	9.255.25, 5	509	486.90T1FY * SITE/1.1			
16 0.036719	192.168.1.1 2	0.255.25. 5	50P	292 MOTIFY * MTTP/1.1			
	192.168.1.1 27			313 MOTIFY * HTTP/1-1			
	192,168:1 2			143 H-SEARCH * WITP/1.1			
19.0.102354	IntelCorf. Br	condcast A	10	42 Mm has 192.168.1.112/ Tell 192.168.1.50			
Daterset Prot		A1072 - 1-1-1	Jost Port	: 1999			
Dier Datagram	e Discovery Frot						
ther Sutagram							
ther Outagram							
ther Outagram							
User Datagram							
ther Outagram							
ther Outagram							
ther Sutagram							
Dier Gutagner Klaudie Servite	e Discoury Prot	ocel 11 6a 38 er		# :× # 4			
Uner Gutagram Kämpla Serein 91.00 Se 00 St 43	7 ff fe an bi	00el 11 0a M er 43 95 00 all	it ie el	6 h h			
Uner Gotagram Kämpla Servin 91 00 Sc 100 St 62 101 ff fa da	7/ ((64 100 11) 11 (0 64 10) 11 12 (0 64 64 11) 12 (0 64 64 11)	011 59 30 err 11 59 30 err 13 59 60 all 13 44 25	81 ie el 53 45 41	ff b 6 52 sls 8-508			
Unit Satagnan Kampla Serviti 91 00 Se 00 81 52 01 11 42 01 11 42	77 (1) (4 100 11) (1) 00 00 04 11) (1) 00 00 04 11) (1) 07 4 00 64 (1) 27 45 55 55	11 5a 3H er 43 5a 60 all 43 5a 60 all 43 5a 71 12 5a	81 6e ef 53 45 43 31 66 6a	IF b = 0.500 52 ± 1.6 №500 48 CH * HTT 9/1.1 0.			
Darr Gatagrae Kangle Servit 91 09 5c 100 81 52 11 fa da 12 11 fa da	P (F) (A (B) (L) (F) (A (B) (L) (F) (F) (A (B) (L) (F) (F) (F) (F) (F) (F) (F) (F) (F) (F)	11 5a 3H er 43 5a 60 all 43 5a 60 all 43 5a 71 12 5a	81 6e ef 53 45 43 31 66 6a	ff b 6 52 sls 8-508	Price II "Speed Holfine"		

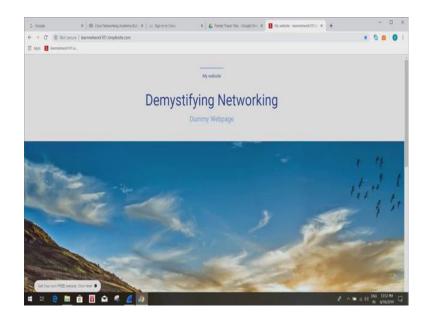
So, we see a lot of traffic that is going around, you have different protocols going around here.

(Refer Slide Time: 01:06)



So, in the mean while what we can try is try opening say some website.

(Refer Slide Time: 01:09)



Let us for example, just open our old dummy website which is this. Now, since we are generated some traffic we can go back and see what is there on Wireshark.

(Refer Slide Time: 01:21)

Capturing from Wi fil Viel Edit View Go Capture Analyze Statistics Telephony	Weeks Tools Hep		- a x
■ # # > □ % © Q + + 当 ¥ 美国 型	4442		
Analy a dealer Ner +Obje			Cal + Expresses
6 Tana Source Destrution Protocol	Length 34s		
2392 27.141224 216.58.203. 192.168.1.58 TOP	68 443 + 53327 [ACK] Seq=213 Ack+4282 Win+32968 Len+8		
2393 27.144862 216.58.203. 192.168.1.50 TCP	68 443 + 51727 [ACK] Sep-213 Acks7782 Wirs-43888 Len-8		
2394 27.146586 216.58.201. 192.168.1.58 TCP	68-663 + 53727 [ACK] Seq-213 Ack-38622 Min-89668 Len-8		
2395 27.146587 216.58.203. 192.168.1.50 TCP	60.443 + 53727 [ACK] Seq=213 Ack+13542 Wit=55480 Len=0		
2396 27.199371 216.58.200, 192.166.1.50 TL5v1.	549 Application Data, Application Data, Application Data		
2307 27.200305 192.168.1.50 216.58.203. TLSv1.	85 Application Deta		
2398 27,203282 216.58,203. 192.168,1,58 TCP	(0.443 + 5)727 [ACK] 5eq-888 Ack-1)573 Win-55488 Len-0		
2399 27,705421 216.58.203. 192.168.1.50 TLSv1.	534 Application Data		
2400 27,799507 216,38,201. 192.168.1.50 TLSvL.			
2401 27.710047 192,168.1.50 216.58.201. TOP	34 53727 + 443 [4(K] Sep-13573 A(k-1489 Wie-17520 Lev-0		
2402 27.714590 216.58.203. 192.168.1.50 TLSv1.	334 Application Data		
2403 27.716999 216.58.201, 192.168.1.50 TLSvL	176 Application Data		
2484 27,715001 216,50,203, 192,168,1,50 TLSv1	93 Application Data		
2485 27.715249 192.168.1.50 216.58.201. TCP	54 53727 + 443 [ACK] Seqv(33573 Ack+28)0 Win+17079 Lem+0		
2406 27.713987 192.168.1.50 216.58.281. TLSv1.			
2407 27.730317 216.58.203. 197.168.1.50 TCP 2408 20.904618 122.1015.1 192.168.1.50 TCP	(0.44) + 53727 [ACK] Sep-1939 ACK-13612 Min-55489 Len-# 94 Dest[Addiso screentable (0.64) Arrentable()		
Internet Protocol Version 4, Sec. 192.168.1.138 User Dutagram Protocol, Sec. Port. 55905, Dat Por			
Simple Service Discovery Protocol			
1000			
0000 00 21 62 (1 00 00 04 11 al 9a (0 al 01 6r a	15 00 🔤 - j0 t. rf ff - k		
ff fa da 61 97 6c 90 6d e4 1a 4d 2d 53 45 6			
43 48 28 2a 20 48 54 54 50 2f 31 2e 31 0d 1			
1011 6f 73 74 3a 20 32 33 30 2e 32 35 35 2e 32			
7 Wife the option is proposit		Packate 2488 - Deplaced 2488 (300 JW)	Public Out

So, what we will try to do is we will try to filter out traffic. Now, we know the protocol that the website is using is HTTP.

(Refer Slide Time: 01:31)

C C	Willi Edit Vew Go Casture Analyze Statistics Telephone	Works Took wep	- 0
Tor Tors Tors <th< th=""><th></th><th></th><th></th></th<>			
001111 00111 000111 </th <th></th> <th></th> <th>Q T T Spran</th>			Q T T Spran
90 28 309 29 20 20 20 20 20 20 20 20 20 20 20 20 20	Tané Seurix Deditation Protocol	Leigh 34	
90 (20 (20 (20 (20 (20 (20 (20 (20 (20 (2	827 18.585820 192,168.1.50 13,249.236. HTTP		
11 10 Add 75 100, 101, 102, 103, 100, 100 100 add 75 100, 101, 101, 101, 101, 101, 101, 101	902 20.020020 192.168.1.50 13.249.236, MTTP	689.621 /e4/05/52304805.design.v15550037416.css/hofd1325535e3ad7b7ce3358b2fc5aac42eb35ab5c031857291	H4668134913830 HTTP/1.1
19 30 AUGU 122, URL 124, URL 1	906 20.021775 192.168.1.50 13.289.236. HTTP	114 GET /d/designs/base/rewsconcept.css WITP/1.1	
20 20 AUGU 2010.41.2012.02.2.4.07 20 20 AUGU 2010.41.2012.02.2.4.07 20 20 AUGU 2010.41.2012.02.0.4.07 20 20 AUGU 2010.41.2012.02.0.4.07 20 20 AUGU 2010.41.2012.02.0.47 20 20 AUGU 2010.41.2012.0.47 20 20 AUGU 2010.41.2012.02.07 20 20 AUGU 2010.41.2012.00.07 20 20 AUGU 2010.41.2012.00	911 20.024725 192.168.1.50 13.249.236. HTTP	539 GET /d/1562644341/designs/base/base.iss HTTP/1.1	
100 0000000000000000000000000000000000	915 20.029262 192.168.1.50 13.249.236, HTTP	112 GET /d/designs/base/somelinks.css WTTP/1.1	
0.20 0.20 <td< td=""><td>927 20.042637 192.168.1.50 13.289.256. HTTP</td><td>612 66T /c/js/jqcery-1.10.2.min.js HTTP/1.1</td><td></td></td<>	927 20.042637 192.168.1.50 13.289.256. HTTP	612 66T /c/js/jqcery-1.10.2.min.js HTTP/1.1	
M J MORY 201, ULL 10 (1), ULL 201, ULL UT D1 (41 / 2014) (20			
Bit B, B, DT, BL, BL, BL, BL, BL, BH, MT Sin QET / Lip/Arrest-Balley, and	932 20.045060 102.168.1.50 13.249.236. HTTP	110 GCT /d/designs/hese/quilljs.css #TTP/1.1	
000 30:000 31:000 32:0000 32:0000 32:0000 32:0000 32:0000 32:0000 32:00000 32:0000 32:0000 32:0000 32:0000 32:0000 32:0000 32:	036 20.069527 192.168.1.50 13.249.256. HTTP	116 GET /d/designs/base/footerlayout5.rxs HTTP/1.1	
M.B. 10.11.2.1.20.7.1.5. 192.00.1.1.000TF SMITPLI 1000 (Enclose1) M.B. 20157011.2.000TF SMITPLI 1000 (Enclose1) M.B. 20150011.2.000TF SMITPLI 1000 (Enclose1) M.B. 2015011.2.000TF SMITPLI 1000 (Enclose1) M.B. 201501.2.000TF		549.6ET /c/3s/#rontendage.win.5s7_sv#ch34ec3572a795bF#148823685F53ad #ITTP/3_1	
en B (1) 5557 (1) 20 (1	968 20.105070 13.249.236. 192.168.1.58 HTTP	54 8077/1.1 200 OK (text/css)	
21 20 2022 202 202 202 202 202 202 202 2	66 20.145139 13.249.236. 192.168.1.58 HTTP	54 0TTP/1.3 200 (K (text/btml)	
000 000 000 000 000 000 000 000 000 00	PM 20, 155578 13, 249, 236. 192, 168, 1, 50 HTTP	465 HTTP/1.1 200 CR (text/css)	
05 82 2036 01 204 201 201 201 201 201 201 201 201 201 201	23 20.162721 102.168.1.50 13.249.236, HTTP		
13 80.7996 (19.10) 13.80.7997 (19.10) 9.4007(1).109 (10.10) 10.90.7996 (19.10) 13 80.7996 (19.10) 13.80.7097 (19.10) 13.80.7097 (19.10) 13.80.7097 (19.10) 14 90.710 (19.10) 13.80.7097 (19.10) 13.80.7097 (19.10) 13.80.7097 (19.10) 14 90.711 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 14 90.711 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 15 90.711 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 16 90.711 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 13.80.700 (19.10) 16 90.711 (19.10) 13.80.700 (19.10) 14.80.700 (19.10) 13.80.700 (19.10) 16 90.711 (19.10) 14.90.700 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 16 90.711 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 16 90.711 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 16 90.711 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 16 90.711 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 14.80.700 (19.10) 16 90.711 (19.10) 14.80	165 20.214602 11.249,236. 192.168.1.50 HTTP	391 WITP/1.1 200 (K (text/javascript)	
01 20 JUNE 2012 (01 JUL 2014 2014 UT UN	95 20.256260 13.249.236. 192.168.1.50 HTTP	\$2.HTTP/1.1 200 CK (application/jevescript)	
01 20 JUNE 2012 (01 JUL 2014 2014 UT UN	13 20.357966 13.249.236. 192.168.1.50 HTTP	54 HTTP/1.1 200 DK (text/css)	
en 196, 116 byts in view (101 bits), 116 bytes optioned (101 bits) in interference 0 meen 176, 102 bytes, 102 bits, 103 bits,	835 20.383092 192.368.1.50 13.249.236, HTTP	128 GET /userPages/pages/Frontend/opt.ocalePage.asox/CultureEps-en-15 HTTP/1.1	
 (43)方柄た液方(6,44)(9,64)(9,64)(9,-1,-4) (44)方柄た液方(6,44)(9,24)(9,-4,4) (44)方(54)(44)(9,24)(44)(9,-4,4)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(44)(9,-4)(14)(14)(14)(14)(14)(14)(14)(14)(14)(1	Transmission Control Protocol, Src Port: 53712, 2 Beassembled TCP Segments (1522 bytes): #635(Dit Port: MM, Seg: 1461, Ack: 1, Len: 62	
● 単体系が2 単単数 単体 (4) 使(4) 単位 2 単(4): (2 車) - (-2): (-4) 単当 (4) 単単(4) 単 (4) 単 (5) 単 (4) = (-2): (-2): (-4) 単当 (4) 単単(4) (2):(-4) (4) (5):(-4) (5): (-2): (-2): (-4) 単当 (-2):(-2):(-2):(-2):(-2):(-2):(-2):(-2):	epertext Transfer Protocol		
 単体気が24 単数 開発 (主気)(中止)(目気)(中)(日本)			
(単体5-5)24(単単単体)(本5-6)4(単立24)(単)(24)-(-2-) (本在14)(単体)(単分)5-5,54(単)(単単体)(単分)(第一(-4-))2-(-2-) (本在15-5)(本(単体)(4-))2-(-4-)(4-)(-2-)-(-2-)(-2-)(-2-)(-			
1 単分気12 単単単単約 (安久 (4) 単定2 4) 特: (2) - (-2) (安仁 (2) 4) 単分 (5) - (5)			
(4) (5) (2) (2) (4) (4) (4) (4) (4) (4) (4) (5) (5) (5) (5) (5) (5) (5) (5) (5) (5			
1 単分気12 単単単単約 (安久 (4) 単定2 4) 特: (2) - (-2) (安仁 (2) 4) 単分 (5) - (5)			
(4) (5) (2) (2) (4) (4) (4) (4) (4) (4) (4) (5) (5) (5) (5) (5) (5) (5) (5) (5) (5			
単分気1240年期時4145(2014年度2月4日年1月4) - 2- (2014日)単分支555(2014年度2月5日日) - 2- (2014日)単分支555(2014日年月2月5日日) - 2- 4月25(2014月) - 3-2-2-2-2-2- 4月25(2014日) - 3-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2			
(4) 41 (3) 49 (3) 25 (3) (4) 49 (5) (5) (4) - 4, - F ₂ (2) - F 4) 27 (5) (5) 49 (4) 40 (4) (5) (5) (5) (4) (5) (5) - (2) (4) (4) (5) (5) (4) (5) (5) (4) (4) (5) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (4) (5) (5) (5) (4) (5) (5) (5) (4) (5) (5) (5) (5) (4) (5) (5) (5) (5) (5) (5) (5) (5) (5) (5			
4 47 78 55 c5 90 99 63 47 48 48 67 38 57 6c 46 56 6p - cg Highelitet w (101 April Remandation (10) (201 April)			
	44 78 55 c5 00 00 63 67 48 48 67 34 57 6c		
	a [114 Autor] Researchied TCP (1222 Sylee)		

So, let us filter out this and let us try to see what is the port number here. So, what we see here is the destination port number is 80 and source port number is 53712. So, what it means here is that this packet is intended to go to a webserver via the protocol HTTP. So, when this packet comes back, then the source the destination port would be this and the source port will be this, that is when it comes back from the server.

(Refer Slide Time: 02:04)

d *Will File Edit View Go Capture Analyze Statistics Telephony	y Weeks Toos Hep		- 0 ×
	EAAAE		
May			Q · Sprann. ·
a Tena Source Destination Protocol	Legit 34		
948 20.057736 192.168.1.50 13.249.236, HTTP	549 SET /c/js/frontendage.min.js7.vv@cb34ec3172a795bf8148823681f53ad HTTP/1.1		
968 28.189878 11.249.236. 192.168.1.58 HTTP	54 HTTP/3.1 200 OK (text/css)		
1866 20.145139 11.249.236. 192.168.1.58 HTTP	54 HTTP/3.3 200 OK (text/html)		
1094 20.155578 13.249.236. 192.168.1.50 HTTP	465 HTTP/1.1 200 CK (text/css)		
1123 20.162721 192,168.1.50 13.249.236. HTTP	114 GET /c/css/experiments/ionicoes.css. HTTP/1.1		
1246 29.216682 13.289.236. 192.168.1.58 HTTP	301 HTTF/1.1 300 OK (text/javascript)		
1295 20.256260 13.249.236. 192.168.1.50 HTTP	54 HTTP/1.1 200 DK (explication/javascript)		
1313 28.357966 13.349.236. 192.168.1.50 HTTP	34 HTTP/1.1 200 GK (Text/css)		
1335 20.103692 192.168.1.50 13.249.236. HTTP	338 GET /userPages/pages/Frontend&ppLocalsPage.aspxHultureRey-en-US HTTP/1.1		
1341 20.395931 13.249.236. 192.168.1.50 HTTP	34 HTTP/1.1 200 OK (text/css)		
1347 20.402702 13.349.236 192.168.1.50 HTTP	54 HT7P/1.1 200 OK (text/css)		
1300 20.616594 11.749.236. 192.168.1.50 HTTP	54.0177/1.1 200 OK (text/cxs)		
1397 20.644478 13.249.236, 192.168.1.50 HTTP	54 WTTP/I.1 200 CK (text/css)		
1407 20,725551 13.249.236. 192.168.1.50 HTTP	54 HTTP/3.1 200 OK (application/x-javascript)		
1417 20.737642 11.249.236, 192.168.1.58 HTTP	54 HTTP/1.1 200 OK (text/cts)		
1421 20.788891 192.168.1.50 13.249.236, HTTP	591.6EY /1/7a/36/282319486667544186/1282319416673173388_styd28861288_3gg_HTTP/1.1		
1426 20.848740 192.168.1.50 172.217.26, HTTP	482-027 /gtm.js?id=678-2896/s078/1.1		
1432 20,852762 102,368,1.50 13,249,236, HTTP Frame 1123: 114 bytes on wire (912 bits), 114 b	222 G&T. /x/css/Honts/Lonicons.ttffvs2.0.1 HTTP/1.1		
Internet Protocol Version 4, Src. 192 168, 500 Transmission Control Protocol, Src Port: 33716 (2 Resconduled TCP Segments (550 bytes): 8112	Dit Port: 80, Seq: 1461, Ack: 1, Len: 60		
Inpertext Transfer Protocol			
ce bi 73 64 fc d0 38 bi fe f2 f9 44 60 M			
1013 00 64 5a 5e 40 00 80 00 e4 59 c0 al 05 32			
ec 48 d1 d4 00 50 b5 % ef 99 5a 25 87 43			
44 78 F9 dd 00 00 48 48 67 34 57 6c 4d 58	as ar op		
Prene (()+ bytes) Assessmithed TCP (1325 Syles)			
Q Z weaters, W-4, 20180830125228, 415414, pisping		Packets: 2634 : Displayed: 38 (3,4%)	Profile: Oxfaul

So, let us try to see some other HTTP request packets and see if we can see. So, see these are all request that are going to the web server.

(Refer Slide Time: 02:13)

🕻 "Will) He Edit Viwi Go Capture Analyze Statistics Telephony	Water Tool time		- 0 ×
Ma			Q Income.
a. Time Source Destination Protocol	Length 3He		
- 940 20.057736 192,168.1.50 13.249.236, HTTP	549 687 /c/js/frontendage.win.js7.vv8cb34ec3177a7956/81488230601553a6	RTTP/1.1	
968 28.185878 13.249.236. 192.168.1.50 HTTP	54 HTTP/3.1 200 OK (text/css)		
1866 20.145139 13.249.236. 192.168.1.58 HTTP	56 HTTP/1.1 200 OK (text/html)		
1094 20.155578 13.249.236. 192.168.1.50 HTTP	465 HTTP/1.1 200 OK (text/css)		
1123 20.162721 192.168.1.50 13.249.236. HTTP	114 GET /c/css/experiments/ionicons.css. HTTP/1.1		
- 1266 20.216602 13.269.236. 192.168.1.50 HTTP	301 HTTP/1.1 200 OK (text/javascript)		
1295 20.256260 13.249.236. 192.168.1.50 HTTP	54 HTIP/1:1 200 DK (application/javascript)		
1313 20.357966 13.249.236. 192.168.1.50 HTTP	54 HTTP/1.1 200 OK (Yest/css)		
1335 20.303692 192.108.1.50 13.249.236. HTTP	138 GET /userPages/pages/FrontendApplocalsPage.aspx?CultureKey-an-US	NTTP/1.1	
1341 20.395931 13.249.236. 192.168.1.50 HTTP	54 HTTP/1.1 200 OK (text/css)		
1347 29.402702 13.349.236. 192.168.1.50 HTTP	54 HTTP/1.1 200 OK (text/cts)		
1300 20.616594 13.249.236. 192.168.1.50 HTTP	54.HTTP/3.3 200.OK (text/css)		
1397 20,644478 13,249,236, 192,168,1.50 HTTP	54 HTTP/I.1 200 CK (trat/css)		
1407 20,725551 11,249,236, 192,168,1.50 HTTP	54 HTTP/1.1 200 OK (application/s-javascript)		
1417 20.737642 11.269.236. 192.168.1.50 HTTP	56 HTTP/1.1 200 CK (test/zas)		
1421 20.788891 192.168.1.50 13.249.236. HTTP	591 GET /1/7a/36/282119486667544186/1282319416673173388styd28881288	jpg HTTP/1.1	
1426 20.848740 192.168.1.50 172.217.26. HTTP	482 GET /gtm.js?id=GTM-2000 NTTP/1.1		
1432 20.852762 192.168.1.50 13.249.236. HTTP	222 GET /c/css/fonts/ionicoes.ttf/v-2.0.1 HTTP/1.1		
Frame 1246: 391 bytes on wire (3128 bits), 391	bytes captured (JI2B bits) on interface 0		
	N:fc:d0), Dut: IntelCor_f2:f0:a4 (38:ba:f8:f2:f0:a4)		
Internet Protocol Version 4, Src: 13.349.236.1. Transmission Control Protocol, Src Port, M. D.	, 051: 192.108.1.50		
	943(767), #944(1468), #945(1468), #946(1176), #947(1468), #948(1468), #	AND	
(int seatempter for seguents (255100 bytes); o	HEI(757), FME(1600), FMES(1600), FMES(175), FME/(1600), FMES(1600), F	HIS(12/6), HYS1(2000), HYS2(2000), HYS3(202), HYS2(2000), HYS3(2	000), MHER(1800), MHEN(181
Line-based text date: text/jewascript (27 lines	A		
Che-boos the each text/lever/she th/ the			
HEAR ME 32 TH SA AT 43 H2 74 , 56 H4 H4 HE 37 20			
10110 33 40 19 19 10 10 33 50 42 88 ee he \$3 7c			
cil bil 3d 20 1a d7 5c 81 fe 26 98 75 17 5d			
111 Be e1 ac ba ad 68 32 dB c7 7a b8 ef 12 d7			
Frame (381 bytes) Ressentitied 109 (201138 bytes) Imumprose	if entity body (\$20602) bytes)		
🔾 🏋 Tranamasan Calittal Protocol (trai), 20 hata		Packata: 2672 - Displayed: 18 (3.4%)	Patie: 04

Now, you see this one here the source port is 80 and the destination port is 53715. So, this means this packet has come from a web server and it has come to the application which was using the port number 53715. So, this way port numbers are used to distinguish different communications that belong to different applications and even if it

is a same web browser and it has multiple tabs here, so, all the tabs would use different port numbers.

So, let us try and see if we can find any other protocol that the laptop is communicating through. So, let us try DNS which is Domain Name Service.

(Refer Slide Time: 02:56)

ie Edit Vew Go Capture Analyze Statistics Telephone		
		DCI - farmer.
Tana Source Destination Protocol	Length Ma	
805 18,545432 192,168,1,58 8,8,8,8 005	78 Standard more ExtBM A same simpletity com	
805 18.545433 192.168.1.50 8.8.8.8 085	64 Standard query Exefit A www.google.analytics.com	
807 18.553957 8.8.8.8 192.168.1.58 DNS	144 Standard guery response fixefif A sam google scalptics com CANNE sam google scalptics 1 google com A 172.217.167.178	
809 18.359329 192.168.1.30 192.168.1.1 DN5	84 Standard guery 0x51/70 A www.progletageorager.com	
814 18.579899 8.8.8.8 192.168.1.50 085	154 Standard guery response Bau63d A learnethork181 simplesite.com A 11,245 216.77 A 13,245 216.44 A 13,245 216.56 A 13,245 236.40	
815 18.579282 8.8.8.8 192.168.1.58 DNS	143 Mandard query response 0x000d A saw simplexits com A 11.349.216.300 A 11.249.236.55 A 11.249.216.56 A 13.249.236.301	
815 18.582791 192,168.1.50 192,168.1.1 DNS	78 Standard query dw070f A css.simplesite.com	
822 18.383342 192.168.1.50 192.168.1.1 085	TE Standard gwery 2x6578 A cdm.simplesite.com	
828 18.591181 192.168.1.50 B.S.S.B. DHS	BE Standard guary Rule70 A www.googletagmanaper.com	
838 18.397447 8.8.8.8 192.168.1.50 005	144 Standard mory response RoScIW A www.googletagmanager.com CNWE www.googletagmanager.l.google.com A 177.217.26.232	
832 18.601640 192.168.1.50 192.168.1.1 D05	20 Standard gurry Busket A commit.facebook.met	
831 18.613299 192, 168.1.10 8.8.8.8 085	78 Standard query RwR704 A css.simplesite.com	
#34 18.615131 192,168.1.50 8.8.8.8 DNS	78 Standard query 0x0070 A cdn.simplesite.com	
837 18.632752 192.168.1.50 8.8.8.8 DNS	80 Standard every RooleD A connect.facebook.net	
838 18.654330 8.8.8.8 192.168.1.50 DNS	128 Standard guary response Exelet A connect, facebook.net CBAME scontent.xx.fbcdx.net A 157.248.35.28	
852 18.747378 8.8.8.8 192.168.1.50 DNS	142 Standard guery response (WMOR A cdr. simplesite.com A 11.249.216.87 A 11.249.216.306 A 11.249.218.111 A 11.249.216.306	
855 18,748218 8.8.8.8 192,166,1.50 045	142 Standard query response BH079F A cis.simplesite.com A 13.245.236.17 A 13.245.236.114 A 13.245.236.54 A 13.245.236.101	
1998 21.227571 192.168.1.50 192.168.1.1 DNS	El Standard exerv Ref130 A staticox facebook com	
Internet Protocol Version 4, Src: B.B.B.B. Dat Uner Datagram Protocol, Src Port: 53, Dat Port Domain Name System (response)		
33 5a ft [2] f5 ad (3 5) 73 64 fc 60 68 69 60 88 55 76 40 66 5a 12 12 65 68 68 88 68 61 72 60 75 67 56 76 66 55 16 68 40 81 80	1 (2) 48 · · · · · · · · · · · · · · · · · ·	
111 00 04 00 00 00 00 03 77 77 77 04 73 59 6d		
45 73 69 74 65 83 63 67 64 00 00 91 00 85		
Y sensitive with 20100010125238 at 6416 property	Patient 200 Department 20 (196)	Folia

And yes we have some packets from DNS. So, again we see here the source port number is 53 and the destination port number is something, this is the response packet.

(Refer Slide Time: 03:06)

Image: Section 1 Section 2 Section 2		
n Tene Doorie Destrution Protocol		D C + Tayram.
	d Lengh Sile	
	70 Standard avery 0x0051 & clivets4.google.com	
2346 24, 150895 192, 168, 1, 50 8, 8, 8, 8 DMS	79 Standard query 0x0051 A clients4.google.com	
2147 24.174448 8.8.8.8 192.168.1.58 DNS	119 Standard Garry Peaperse Bull51 A clientsd.google.com CMAVE clients.l.google.com A 172.217.308.174	
2168 26.911519 192.168.1.58 192.168.1.1 DNS	The Standard query Babelo & drive google. con	
2369 26.933942 192,168.1.58 8.8.8 285	Jis Standard query exberts A drive google.com	
2170 26.953667 H.H.R.H 192.168.1.50 DNS	92 Standard query response dabella A drive.google.com A 218.38.201.174	
2435 37,684856 192,168.1.50 192,168.1.1 085	75 Standard guery Billel2 A su. If avait.com	
2436 17.601117 192,168.1.50 192,168.1.1 DRS	75 Standard spary Bichell AMA su, H. avant.com	
2417 37,719483 192,168.1.50 192,168.1.1 045	R2 Standard purry Bx785e A analytics.ff.avast.com	
2446 49 871899 102 168 1 50 8 8 8 8	82 Standard mery Bu705e A analytics. Ff avant.com	
2447 40.840816 8.8.8.8 192.168.1.50 095	142 Standard guary response Bu705e A analytics.ff.avavt.com CMVE analytics.mil.ff.avavt.com A 5.62.55.2	112 A 5.42.53.222
2471 41.628115 192.168.1.50 8.8.8.8 085	75 Standard query Ph2e22 A tu. Ff. avast.com	
2472 A1,644453 8.8.8.8 192,168,1,58 DM5	256 Standard mory response 8x2x22 A su FF avast com DWE su nol FF avast com A 77,234,45,78 A 5,45,58.	214 A 5.45.58.216 A 5.45.59.215 A 77.234.45.68 A 77.
2473 42,658401 192,168.1.50 8.8.8.8 085	75 Standard every Exctc3 AAAA se.ff.avast.com	
2474 42,668223 8.8.8.8 192,168,1.58 085	96 Standard guery response Buchcl AAAA us.ff.avant.com CMANE nu.eul.ff.avant.com	
2885 146.455. 192.168.1.50 192.168.1.1 085	75 Standard guery Bubcl0 A su.ff.avast.com	
2886 146.455. 192.168.1.58 192.168.1.1 185	75 Standard guery Bytc21 AAAA au Ff. avast.com	
Interset Protocol Version 4, Src. B.B.B.B. Out User Datagram Protocol, Src. Port: 53, Dat Port Domain Name System (response)		
31 5a ft 12 ft at cF 51 77 64 fc an an an	26 W 1 1 - 1	
111 00 82 00 00 40 00 3s 11 Ge 83 08 08 08 08	H ch al P i n	
进标信行分析信制 万砖气动肉肉 卵浆酸酸酸酸油 适合式增强酶 转发酶 苏格兰酸 索兰尔 计算	H (0 48	
00 82 00 00 40 00 3s 11 6e 83 08 08 08 08 01 32 00 75 ds 51 00 5e at cf sf 3f 81 80 00 82 00 00 00 00 81 77 77 72 10 67 6f 6f	61 (4 64)	
111 00 82 00 00 40 00 3s 11 6e 83 08 08 08 08	61 (4 64)	

And let us try to see here yeah. So, we have source port as 53 and destination here and here again the reply has come. So, here what we see is the source port is 53 and destination port is 55987.

(Refer Slide Time: 03:27)

■20100000++SF1000	= 2 2 2	D term
		D - 1 + Deres
	a Legh Me	
2369 26.935942 192.168.1.50 8.8.8.8 045	76 Standard query Bylein A drive.google.com	
2378 26.953667 8.8.8.8 192.168.1.50 085	92 Standard sonry response bubells A drive.googie.com A 226.58.203.174	
M35 37.604856 192.168.1.50 192.168.1.1 DN5	75 Standard guery Bulail A su H.avant.com	
M36 37.605117 192.168.1.50 192.168.1.1 DN5	75 Standard gurry Bochc3 AMA su FF.avast.com	
1437 37.719483 192.168.1.50 192.168.1.1 045	#2 Standard guery #x703e A analytics.ff.evest.com	
A46 40.031899 192.168.1.59 8.0.0 DHS	Al Standard query BuTHSE A analytics.ff.avast.com	
M47 40.840816 8.8.8.8 192.168.1.50 DM5	142 Standard guery response Bo205e A analytics.Ff.avost.com CAVE analytics.mil.Ff.avost.com A 5.62.53.212 A 5.62.53.222	
M71 41.628115 192.168.1.50 8.8.8 DN5	75 Standard mory #x2x22 A so.ff.avast.com	
472 41.544453 B.B.B.B. 192.168.1.50 DH5	256 Standard guery response RuZu222 A su.ff.avast.com (NAVE su.nul.ff.avast.com A 77.234.85.70 A 5.45.58.214 A 5.45.38.216 A 5.45.	58,215 A 77,238,45,60 A 7
473 42,656401 192,163.1,50 8,8.8.8 005	75 Mandard guery Bochc3 AAAA so.ff.evest.com	
474 42.660723 B.B.B.B. 192.168.1.50 DH5	56 Standard guery response Buchc) AAAA su.ff.avant.com CMVHE su.ex1.ff.avant.com	
885 146,455, 192,168,1,50 192,168,1,1 DMS	75 Standard query Bobc30 A su.ff.avast.com	
886 146,455. 192,160.1.50 192,168,1.1 005	75 Standard guery Buic21 AMA su FF.avast.com	
908 151.517. 192.168.1.50 8.8.8.8 005	75 Standard query Bdc30 A vu.ff.avast.com	
909 151.517. 192.168.1.50 H.8.8.8 DN5	75 Standard wary Bolc21 AWA su.ff.avast.com	
910 151.520. 8.8.8.8 192.168.1.50 005	256 Standard guery response Bidicilli & su-FF, avast, com OWVE su, est, FF, avast, com & S45, 58, 214 A 77, 214, 45, 61 & S.45, 58, 215 A 77, 214 In Standard guery response Bidicilli AMA su, FF, avast, com OWVE su, est, FF, avast, com	4,43,81 A 77,234,43,85 A
911 151.521. 0.8.8.8 192.168.1.58 045	to Standard garry response execut www.sp.tt.spatt.com usve_ss.ts1.tt.avast.com	
sternet Protocol Version 4, Src: 192.168.1.56		
eternet Protocol Version 4, Src: 192.368.1.50 Ser Sutagram Protocol, Src Port: 51007, Dat P	8:72:90:00), Dut: Cisco-Li_06:70:00 (18:01:71:06:10:00) 90, Dut: 192.100.1.1	
eternet Protocol Version 4, Src: 192.368.1.50 ser Datagram Protocol, Src Port: 51007, Dat P	8:72:90:00), Dut: Cisco-Li_06:70:00 (18:01:71:06:10:00) 90, Dut: 192.100.1.1	
eternet Protocol Version 4, Src: 192.368.1.50 ser Datagram Protocol, Src Port: 51007, Dat P	8:72:90:00), Dut: Cisco-Li_06:70:00 (18:01:71:06:10:00) 90, Dut: 192.100.1.1	
Interest Pointeal Weslaw A, Sri U, 192, 193, 193 the forgan Pointeal (e_1 for Point 193, e_2 for Point 193, e_3 for Deckin New System (q_{HYY}) V V q_1 for q_2 for q_3 for q_4 for q_4 for q_4 for q_4 for q_2 for q_3 for q_4 for q_4 for q_4 for q_4 for q_4 for q_4 for q_4 for q_4 for q_4 for q_4 for q_4 fo	EX.PPS.40. (b): (Loc LLM-FL-B (LM-SL-70-ML-FL-B)) 80 (5.96) - 1 - 5	
Interest Protocol Version 6, Ser. 19, 103, 103, 30 constraints Protocol Version 6, Ser. 19, 104, 70 particular Name Systems (serry) \tilde{N} (d.1) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) 40 (c. or, 1) to (fr. (2) as 4.01 m) (d.2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (EX.PPS.40. (b): (Loc LLM-FL-B (LM-SL-70-ML-FL-B)) 80 (5.96) - 1 - 5	

And here what we see if for one of the reply is which was 51807, the reply has come back which is with destination port 53. So, this is another example of how different protocols use port numbers and so these are some standard port numbers, 53 is a standard port number for DNS requests. Similarly, 80 is a standard port number for web browser based HTTP request and let us see another protocol. So, let me show you something called ARP.

(Refer Slide Time: 03:59)

∎de:::223,++≣∓ #
Tene Searce Sedimeter
3007 169.117. IntelCor_F. Broadcast
3000 174,96%, Intelfor 6. Broadcast
3018 174.682. IntelCor_6. Broadcast
1022 175.707. IntelCor A. Broadcast
3025 176.610. Intellior_f. Broadcast
3010 178.219_ intelCor_f_ Broadcast
3031 179.102. IntelCor_f. Broadcast
1011 179.533. IntelCor_f. Broadcast
1034 180.118. IntelCor_f_ Broadcast
3035 188.110. IntelCor_f_ Broadcast
3030 101.110. IntelCor_f. Broadcast
1041 185.026. IntelCor_6. Broadcast
3045 185,513. IntelCor_f. Broadcast
1846 185.742. IntelCor_6_ Broadcast
1047 195,104. IntelCor f., Broadcast
1052 186,766. IntelCor 6. Broadcast
1053 187.107. IntelCor f. Broadcast
作并作作并作用311500 用原则和研究用3111510

Now, the interesting thing here is ARP is a protocol which actually does not work on the application and higher layers; it basically just works still the internet layer. So, all you see here is the IP addresses and the MAC address.

(Refer Slide Time: 04:10)

	Capture Analyze Statisti			
	128 4++ 22	100	14442	DCI - Invent
11				D - 1 + Inventor
Ten	Seute Destrution		Length 249	
	IntelCor_F_ Broadcast		42 who has 192.168.1.1127 Tell 192.168.1.50	
	IntelCor_f_ Broadcast		42 when has 292,168.1.1127 Tell 192,168.1.50	
	IntelCor_f_ Broadcast		42 Who has 192.168.1.1877 Tell 192.168.1.58	
	IntelCor_F_ Broadcast		42 who has 192,168.1.1127 Tell 192,168.1.50	
	IntelCor_f_ Broadcast IntelCor f_ Broadcast		42 Mbo Hav 192,168.1.1077 Tell 192,168.1.50 42 Mbo Hav 192,168.1.1077 Tell 192,168.1.50	
	IntelCor.6. Broadcast		42 Min Tax 192,108,1,1097 (211 192,108,1,59 42 Min Tax 192,108,1,1137 (e11 192,168,1,118	
	IntelCor f. Broadcast		42 who has 192,100,1,1127 (011 192,108,1,110 42 who has 192,108,1,107) [211 192,108,1,50	
	IntelCor.6. Broadcast		42 We has 192,108,1,1977 941 192,108,1,38 42 We has 192,148,1,1137 1811 193,168 1,110	
	IntelCor_f_ Broadcast		42 min has 192,168,1,1877 1+11 192,168,1,169	
	IntelCor_6_ Broadcast		42 mm fas 192.108.1.1077 1011 192.108.1.108 42 mm fas 192.108.1.1127 7011 192.308 1.118	
	IntelCor f. Broadcast		42 We fail 192,108,1,1127 (F11 192,108,1,118) 42 We fail 192,108,1,1077 [511 192,168,1,59	
	IntelCor f. Broadcast		42 Mbs Tax 192.108.1.1127 Tell 192.108.1.50 42 Mbs Tax 192.108.1.1127 Tell 192.108.1.50	
	IntelCor f. Broadcast		42 who has 292,168,1,112? Tell 292,168,1,50	
	IntelCor 4. Broadcast		42 who has 192.168.1.1127 Tell 192.168.1.50	
	IntelCor S. Broadcast		42 who has 192.168.1.1127 Tell 192.168.1.110	
	IntelCor_6_ Broadcast		42 kbo has 192,168.1.112/ Tell 192,168.1.110	
Protocol typ Hardware sli Protocol sli Opcode: requ Sender NVC /	zef 4			

Basically what ARP does is it gets the corresponding MAC address for IP address or vice versa. So, we call one as ARP, the other as reverse ARP or reverse Address Resolution Protocol.

So, all the protocols that work on the application layer have these port numbers. So, this is a brief demonstration of port numbers. There is one more crucial concept with port numbers called port address translation, for port address translation what we would want you to do is go through the article on port address translation and try to see what it mean. Once you have read the article, go to the next video and we will talk more about port address translation.

Thank you.