Design Engineering of Computer Systems Professor. Mythili Vutukuru Computer Science and Engineering Indian Institute of Technology, Bombay Lecture 37 (Week 5, Tutorial 2) Learning Wireshark

Hi, everyone. In this video, we will learn about Wireshark. Wireshark is a very useful utility which helps us to capture all the network packets which are passing through an interface cards on our computer.

(Refer Slide Time: 00:29)







Image: Section of the sectin of the section of the	Activities 🖉 Wireshark 🕶	Thu 12:56	Q - 👂 🔥 🔋 🕪 🔒 -
Image: Set Var 0 Counter Apple Settis Teacher Var 1 Image: Setie Teacher Var 1 <td< th=""><th></th><th>*wip2s0</th><th></th></td<>		*wip2s0	
Image:	File Edit View Go Capture Analyze Statistics Telephony	Wireless Tools Help	
Port Transmission Production		TINE AAAT	
Dis. Tare Source Destination Process (supplie) 10 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 10 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 10 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 10 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 10 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 11 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 11 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 12 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 12 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 13 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 13 Tare (supplie) Tare (supplie) Tare (supplie) Tare (supplie) 14 Tare (supplie)<	p.addr == 103.21.127.134		Expression +
1 11/2 11	No. Time Source Destination	Protocol Length Info	
<pre></pre>	A F 18 7.016500590 192.168.116.33 183.21.127.	134 TCP 74.47270 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3555558068 TSecr=0	wS=128
2 / 2012/07 2012/07.01 10.2.2.2.1.1.1 10.2.2.2.2.1.1 10.2.2.2.1.1	21 7.694775289 183.21.127.134 192.168.116 22 7.694812438 192.168.116.33 183.21.127	.33 TCP 74 443 → 47278 [SYN, ACK] Seq18 ACK=1 N1n=50168 Len=8 MSS=1378 SACK_PERM=1 TSva1=42885147 134 TCP 56 47278 - A13 [ACK] Seq11 Ack=1 Min=54256 Len=8 TSva1=3555559847 TSec=4288514758	59 TSecr=3555558908 WS=128
<pre>0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 * 0 *</pre>	23 7.697167790 192.168.116.33 183.21.127.	134 TLSv1.2 583 Client Hello	
1 2	44 7.173928864 103.21.127.134 192.168.116	.33 TCP 66 443 - 47270 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=4200514840 TSecr=3555559049	
1 1	45 7.180960593 103.21.127.134 192.168.110 46 7 181092670 192 168 116 92 193 21 197	.33 TLSv1.2 1424 Server Hello 154 TFD 86 47270 - A43 [ATV] Sec.518 Ark:1350 Win:63104 Lemb TSup[:]5555550133 TSec.74200514842	
0 7 medan, mb202/001/002508 MpUND02000 0 100 meda (b) 100 meda	40 7.181832870 192.108.110.33 183.21.127. 47 7.181113700 183.21.127.134 192.168.116	134 TCP 06 41210 - 443 [HLK] 359-310 HLK-1336 HLH-63164 LEH-6 TSVAL-3050505133 1561-4260514642 (33) TCP 1424 443 - 47270 [ACK] Seg=1359 Ack=518 Win=64768 Leh=1358 TSVal=4280514842 TSecr=355555904	9 [TCP segment of a reassembled
1 11110000 100 11111111111111111111111	48 7.181131885 192.168.116.33 183.21.127.	1)# TCP 66 47270 - 443 [ACK] Seq=518 Ack=2717 Win=61824 Len=0 TSval=3555559133 TSecr=4200514842	
<pre>1 * 1 * 1 * 1 * 1 * 1 * 1 * 1 * 1 * 1 *</pre>	49 7.181348692 103.21.127.134 192.168.116	.33 TLSv1.2 1894 Certificate, Server Key Exchange, Server Hello Done	
1 2. Status 1 20 21 20 21 20 21 20 21 20 21 20 21 20 21 20 21 20 21 20 21 20 21 20 20 20 20 20 20 20 20 20 20 20 20 20	51 7 186423167 192 168 116 33 183 21 127	134 TLP 06 41270 - 443 [MLA] 300-310 MLA-3743 NLH-03104 L0H-0 TSV8L-333333133 TS01-4200314042 134 TLSV1.2 159 Client Key Exchange Change Cinher Spec. Encrypted Handshake Messane	
1 21 4810201 22 32 481123 103 22 17 18 103 103 22 17 18 103 103 103 103 103 103 103 103 103 103	68 7.264007426 103.21.127.134 192.168.116	.33 TLSv1.2 340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
0 7 wirzbard, wijzbal (2022)(00125588, Mg/MK0/paparg) (104 7 wirzbard, wijzbal (2022)(00125588, Mg/MK0/paparg) (104 7 wirzbard, wijzbal (2022)(00125588, Mg/MK0/paparg)	61 7.264032891 192.168.116.33 183.21.127.	134 TCP 66 47270 - 443 [ACK] Seq=611 Ack=4019 Win=63072 Len=0 TSval=3555559216 TSecr=4200514930	
O T method, mplob/2020004125988.Mg/MR0pcopr O T method, mplob/202000412598.Mg/MR0pcopr O T method, mplob/20200412598.Mg/MR0pcopr O T method, mplob/20200412598.Mg/MR0pcopr	82 7.487376692 192.168.116.33 183.21.127.	134 TLSv1.2 541 Application Data	
 Prevention Proceeding Version 4, Sec 120, 2014 (2014), 301 (2014) (2014) (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Sec 12, Lew 1 (2014) Prevention Control Proceeding Version 4, Lew 1 (2014) Prevention Control Proceeding Version 4, Lew 1 (2014) Prevention Control Proceeding Version 4, Lew 1 (2014) Prevention Con	 Frame 16: 74 bytes on wire (592 bits), 74 bytes capt Ethernet IT Src: IntelCar 9: 45:1e (5: 5f:67:9c:45) 	ured (392 D1LS) ON INCETTAGE 0 1e) Det: 52:74:31:49:hf:f5 (52:74:31:49:hf:f5)	
 Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Srt Pert: 440, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src Pert: 4778, Set; B, Lee; E Transmission Control Presson, Src	Internet Protocol Version 4, Src: 192.168.116.33, Ds	1: 103.21.127.134	
10 10 11<	Transmission Control Protocol, Src Port: 47278, Dst	Port: 443, Seq: 0, Len: 0	
10 20 21 24<			
10 7 wrechard, mp2ad, 20220104125508, Mp2MeD pagang Partice 100- Doplayed: 1713 (87.7%) - Dropped: 0 (0.7%) Partice 100- Doplayed: 1713 (87.7%) - Dropped: 0 (0.7%) Partice 100- Doplayed: 1713 (87.7%) - Dropped: 0 (0.7%) Partice 100- Doplayed: 1713 (87.7%) - Dropped: 0 (0.7%) Partice 100- Doplayed: 1713 (87.7%) - Dropped: 0 (0.7%)	0000 52 74 31 a9 bf f5 5c 5f 67 9c 45 1e 88 00 45 00	Rt1\ g (EE-	
1000 fs 16 of 15 is 10 00 02 54 is 35 14 of 12 00 02 0	0028 7f 86 b8 a6 81 bb de f1 2e 9a 00 00 80 80 80 a0 02	- delle - Eld	
 W 3 26 00 10 00 00 00 00 00 00 00 00 00 00 00	8638 fa f0 0f 96 00 00 02 04 05 b4 04 02 08 0a d3 ed		
10 7 wirezbark, wj2/zd 20220106125588, MpUMEO progred 0 (0.0%) Prefile: D	0648 85 38 00 00 89 00 01 03 83 07	8	
10 7 wreshark, wjoża 20220106125508 MpUNEO.pcapag Packets: 1910 - Doplayer: 1913 (49.7%) - Dopped: 0 (0.0%) Prafec. D			
10 7 wirebark, wijzlań 20220106125588. Mpl/MEO progred 0 (0.0%) Prefile: D			
19 7 wreshark, wjóżaj 20220106225508 MpUNEO pospog 19 7 wreshark, wjóżaj 20220106225508 MpUNEO pospos 0 (0.0%) Prafile: D			
 Pro 7 wirebark, wjoźcó 20220106125588, MpUNEO propred 0 (0.0%) Profile: D Profile: 1910 - Doplayed. 1/13 (#3.7%) - Dopped 0 (0.0%) Profile: D 			
1 7 wireshark, wp2a9_20220106225588_MpUME0.pcapeg 0(0.0%) Profile: D			
2 0 7 wirebark, wijzla 20220106125588, MpUMEO property 0 (0.0%) Prefile: D			
10 7 wireshark, wip2ig/20220061255588 MgUME0 pooper 0 (0.0%) Profile D	S.C.		
FEIO 7 wireshark wip2x0 20220106125508 MgUWE0 pcaping Packets: 1910 - Displayed: 1713 (89.7%) - Dropped: 0 (0.0%) Profile: D			
W wresnark_wip2su_2u22u2us125sus_wguweu.pcapng Packets: 1910 - Displayed: 1/13 (89.7%) - Dropped: 0 (0.0%) Profile: D		0	
	Wreshark_wipzsu_20220106125508_MgUWE0.pcapng	Packets: 1910 - Displayed: 1713 (89	(%) - Uropped: U (U.U%) Profile: Defau

10 C	Edit View Go C	apture Analyze Stat	istics Telephony Wire	less Tools He	lp .			
6		PORT	*****		0,0,0,1			
ip.a	ddr == 103.21.127	134						Fanression +
No	Timo	Source	Dectination	Bratacal I	conth lefe			
NU.	45 7 189960593	183 21 127 134	192 168 116 33	TI Sv1 2	1424 Server Hello			_
	46 7.181832678	192.168.116.33	183.21.127.134	TCP	66 47270 - 443 [ACK	[] Seq=518 Ack=1359 Win=63104 Len=0 TSval=3555559133	3 TSecr=4280514842	
	47 7.181113700	103.21.127.134	192.168.116.33	TCP	1424 443 - 47270 [ACK	K] Seq=1359 Ack=518 Win=64768 Len=1358 TSval=4288514	1842 TSecr=3555559049 [TCP segment (of a reassembled
	48 7.181131885	192.168.116.33	183.21.127.134	TCP	66 47270 - 443 [ACK	K] Seq=518 Ack=2717 Win=61824 Len=0 TSval=3555559133	3 TSecr=4280514842	
	49 7.181348692	103.21.127.134	192.168.116.33	TLSv1.2	1894 Certificate, Ser	rver Key Exchange, Server Hello Done	T0 120251 1012	
	51 7.186423167	192.168.116.33	183.21.127.134	TLSv1.2	159 Client Key Frcha	x] Stq-510 Ack-3/45 Win-53104 Len-0 Towar-300000132 ande. Change Cinber Spec. Encrypted Handshake Messar	39 13001-4200314042	
	68 7.264007426	103.21.127.134	192.168.116.33	TLSv1.2	340 New Session Tick	ket, Change Cipher Spec, Encrypted Handshake Message	2	
	61 7.264832891	192.168.116.33	183.21.127.134	TCP	66 47270 - 443 [ACK	[] Seq=611 Ack=4019 Win=63872 Len=0 TSval=3555559210	5 TSecr=4280514938	
	82 7.407376692	192.168.116.33	183.21.127.134	TLSv1.2	541 Application Data	1		
	83 7.488857505	103.21.127.134	192.168.116.33	TCP	1424 443 - 47270 [ACK	K] Seq=4019 Ack=1006 Win=64384 Len=1358 TSval=428065	L5153 TSecr=3555559359 [TCP segment	of a reassembled
	84 7.4888853950	192.108.110.33	183.21.127.134	TCP	00 47270 - 443 [ALK	S SEQ=1880 ACK=5377 W1R=03184 Len=0 ISVal=350050944 S Sen=5377 Ack=1886 Win=64384 Len=1358 TSval=458051	10 15007=4268515153 15153 TSecr=35555550350 (TCP comment	of a reassembled
	86 7.488239356	192.168.116.33	183.21.127.134	TCP	66 47270 - 443 [ACK	Seg=1886 Ack=6735 Win=63184 Len=0 TSval=355555944	10 TSecr=4288515153	or a respensive.
	87 7.488527857	103.21.127.134	192.168.116.33	TCP	1424 443 - 47270 [ACK	Seq=6735 Ack=1006 Win=64384 Len=1358 TSval=420051	15153 TSecr=3555559359 [TCP segment	of a reassembled.
> Fra	me 82: 541 bytes	on wire (4328 bits	s), 541 bytes capture	ed (4328 bits)	on interface 8			
> Eth	ernet II, Src: 1	ntelCor_9c:45:1e (!	5c:5f:67:9c:45:1e), [Ost: 52:74:31	a9:bf:f5 (52:74:31:a9	0:bf:f5)		
> Int	ernet Protocol V	Version 4, Src: 192	.168.116.33, Dst: 103	3.21.127.134	Anh. 1040 1 175			
> ITE	ure Seckets Law	a protocol, sic po	rt: 47270, DSt POrt:	445, 584; 61.	, ACK: 4019, LMI: 4/5			
1 244	and because baye	4						
1	l\$							
	13							
	1è							
	1è							
	12							
	4							
	4							
	ų							
8938	l} 52 74 31 a9 bf	15 5c 5f 67 9c 45	1e 88 00 45 00 Rt1	L \ g E 1				
8008 8018 8028	↓ 52 74 31 a9 bf 62 0f 1b 57 49 7f 86 84 68 11	15 5c 5f 67 9c 45 09 40 66 62 2d c6 16 de f1 3 fd 39	1e 88 00 45 00 Rt1 a8 74 21 67 15 f. g. hg & 18	L_g.E8 ₩8-8t! 9.9	-			
8018 8018 8028 8038	↓ 52 74 31 a9 bf 62 0f 1b 57 40 7f 86 b8 a6 61 61 f5 79 fd 89	15 5c 5f 67 9c 45 00 40 06 02 2d c0 bb de 11 30 fd 39 0 61 01 08 6a d3	1e 88 00 45 00 RtJ a8 74 21 67 15 fc 9c b9 80 18 d 87 bf f2 3	L_g.E8 ₩8-8	- - -			
8008 8018 8028 8038 8038 8038 8048	52 74 31 a9 bf 62 6f 1b 57 46 7f 68 b8 a6 61 61 f5 79 fd 89 7 72 17 68 88	f5 5c 5f 67 9c 45 69 40 06 02 2d c0 bb de f1 30 fd 39 69 61 01 68 6a d3 1 d6 68 69 69 60	1e 88 09 45 00 R1 a8 74 21 67 15 fc 9c b9 60 18 ed 87 bf ff 23 08 89 60 61 65 yr	L_g.E8 ₩9-9	:- 			
0010 0010 0029 0038 0038 0048 0050	52 74 31 89 bf 62 6f 1b 57 40 7f 68 b6 86 79 ff 80 61 f5 79 ff 80 79 72 21 76 88 37 6f 99 1c 5e	15 5c 5f 67 9c 45 09 40 06 02 2d c0 b6 ef 13 0f d 39 09 01 01 08 6a d3 01 d6 09 06 09 60 56 95 93 df cc 16 a7	1e 88 00 45 00 Rt1 a8 74 21 67 15 fc 9c b9 80 18 ed 87 bf ff 23 - 9 80 80 e0 15 5 yr 64 bd da 97 3d 7.	Lg.E8 ₩8-8	- - - - - - - - 			
8008 9018 9028 9038 9048 9058 9058	52 74 31 a9 bf 62 6f 1b 57 40 7f 68 b8 a6 11 15 79 f61 00 79 72 17 68 08 79 79 19 16 56 12 4b af 30 8d	T5 5c 5f 67 9c 45 00 40 06 02 2d 00 bb de f1 30 fd 30 01 01 08 00 00 00 01 01 08 00 00 00 01 01 08 00 09 00 ff ce f6 a7 c9 a7 69 42 cc da	1e 88 00 45 00 Rt1 a8 74 21 47 15 fc 8c b9 80 18 e0 87 60 01 45 yr 64 bd 48 97 3d 7 b64 bd 48 97 3d 7	L_g.E8 ₩8-8				
9098 9019 9029 9038 9058 9058 9058 9058 9058	52 74 31 a9 bf 62 6f 1b 57 40 7f 80 b8 a6 61 61 75 79 fd 08 73 76 79 51 85 73 76 99 1c 5e 12 4b af 30 88 88 cc 81 68 63 88 8c 81 68 88	15 5c 5f 67 9c 45 00 40 06 62 2d 00 00 01 01 68 6a 33 00 01 01 88 6a 33 05 48 00 c 76 6a 7 03 47 69 43 2t cc 36 09 43 1f 24 55 6d fr 47 6 % 15 17	1e 08 00 45 00 Rt a6 74 21 67 15 15 05 16 90 10 ed 87 bf ff 23 ed 87 bf ff 23 ed 85 bf ff 23 50 eb 55 56 ec 55 58 fb 59 f8 3a 55 46 84 49 ed 80 bf 10 a 10 bf 10 bf 10 bf 10 10	L				
8998 8618 8628 8638 8648 8658 8658 8658 8658 8658 8658 865	52 74 31 49 bf 62 of 1b 57 49 71 80 b6 a6 61 15 79 76 40 79 72 17 63 68 37 0f 99 16 83 37 0f 99 16 43 38 cc 81 dd 13 71 26 18 68 28 63 01 af 45 46	15 5C 57 67 9c 45 00 40 66 62 2d c0 bb de 11 30 fd 30 64 30 64 30 65 56 <td>1e 85 60 45 00 Rt a8 74 21 67 15 fr 9c b9 00 18 d8 75 ff 73 - y 30 88 60 01 65 yr 35 66 ce 7 35 66 58 76 7 75 64 34 19 0 67 76 b9 77 b0 68 67 76 56 61 41 90 0 67 76 b9 78 b9 78 0 75 56 61 41 90 0 67 76 b9 78 b9 78 0 78 56 59 78 30 0 75 56 61 41 90 0 67 76 b9 78 b9 78 0 78 56 59 78 50 0 75 56 51 41 90 0 67 76 56 50 0 75 56 50 10 0 75 56 50 0 75</td> <td>L</td> <td>- - - - - - - - - - - - </td> <td></td> <td></td> <td></td>	1e 85 60 45 00 Rt a8 74 21 67 15 fr 9c b9 00 18 d8 75 ff 73 - y 30 88 60 01 65 yr 35 66 ce 7 35 66 58 76 7 75 64 34 19 0 67 76 b9 77 b0 68 67 76 56 61 41 90 0 67 76 b9 78 b9 78 0 75 56 61 41 90 0 67 76 b9 78 b9 78 0 78 56 59 78 30 0 75 56 61 41 90 0 67 76 b9 78 b9 78 0 78 56 59 78 50 0 75 56 51 41 90 0 67 76 56 50 0 75 56 50 10 0 75 56 50 0 75	L	- - - - - - - - - - - - 			
80008 8619 8629 8648 8648 8658 8658 8678 8678 8668 8678 8638	2 52 74 31 a9 bf 62 6f 1b 57 40 7f 68 b8 a6 11 15 79 fd 00 79 72 17 63 08 79 6f 90 1e 5e 12 4b af 30 86 28 66 61 af 45 46 68 5c 68 11 68 45	15 5c 5f 67 9c 45 00 40 66 62 21 60 00 61 30 61 30 61 30 00 61 30 61 30 61 30 61 30 61 30 61 30 61 30 61 30 61 30 61 50 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 7	10 00 45 00 842 a0 74 21 67 55 67 58 56 50 56 68 76 56 <td>L _ g E Etg</td> <td></td> <td></td> <td></td> <td></td>	L _ g E Etg				
8008 8019 8029 8038 8048 8058 8058 8058 8058 8058 8058 805	52 74 31 a9 bf 62 of 1b 57 49 7f 86 b6 a6 79 fd 89 79 72 17 68 07 79 12 17 68 79 91 65 56 83 77 64 99 16 56 88 cc 81 49 48 88 cc 81 49 48 46 52 64 4f 66 65 64 4f 66 65 54 78 29 56	15 5c 5f 67 9c 45 00 40 06 62 2d 00 00 00 01 01 60 60 2d 00 00 <td>10 05 00 45 00 RT all 74 21 47 15 61 05 16 0 01 1 61 05 16 10 01 1 61 05 16 10 01 1 73 06 05 50 60 00 1 75 56 61 41 30 0 65 61 60 10 10 1 74 10 05 00 00 0 75 56 61 41 30 0 65 61 60 00 0 74 10 05 00 0 75 56 00 0 74 10 0 75 56 0 75 56 0 74 10 0 75 56 0 74 10 0 75 56 0 75 10 00 00 00 00 00 00 00 00 00 00 00 00</td> <td>L··\ blight = 0-9 6 6 6 6 6 6 6 6 6 6 6 6 6 7 6 7 6 7 -</td> <td></td> <td></td> <td></td> <td></td>	10 05 00 45 00 RT all 74 21 47 15 61 05 16 0 01 1 61 05 16 10 01 1 61 05 16 10 01 1 73 06 05 50 60 00 1 75 56 61 41 30 0 65 61 60 10 10 1 74 10 05 00 00 0 75 56 61 41 30 0 65 61 60 00 0 74 10 05 00 0 75 56 00 0 74 10 0 75 56 0 75 56 0 74 10 0 75 56 0 74 10 0 75 56 0 75 10 00 00 00 00 00 00 00 00 00 00 00 00	L··\ blight = 0-9 6 6 6 6 6 6 6 6 6 6 6 6 6 7 6 7 6 7 -				
80038 8019 8028 8058 8058 8058 8058 8058 8058 8058	b 52 74 31 49 bf 52 64 11b 57 48 77 69 bla 60 61 15 79 76 18 15 79 76 18 12 4b af 39 81 52 04 4f 39 84 58 cc 81 40 43 71 28 18 68 26 64 0f e 65 45 04 67 e 65 46 49 04 97 bc 53 at 40 49 07 bc	15 55 51 67 92 45 00 40 66 62 24 60 80 </td <td>10 08 00 45 00 Rt a0 74 21 67 15 67 9c to 30 01 60 08 00 01 65 yr 64 bd da 97 34 7. 58 f0 59 f0 3a 65 55 60 ct 55 yr 64 bd da 97 34 7. 58 f0 59 f0 3a 64 74 bc 53 ct 55 66 34 190 q8 64 74 bc 53 ct 64 64 22 64 fc 64 22 64 fc 64 22 65 fc 64 25 fc 64 25</td> <td>L ↓ 0 E · . (0 9 ·</td> <td></td> <td></td> <td></td> <td></td>	10 08 00 45 00 Rt a0 74 21 67 15 67 9c to 30 01 60 08 00 01 65 yr 64 bd da 97 34 7. 58 f0 59 f0 3a 65 55 60 ct 55 yr 64 bd da 97 34 7. 58 f0 59 f0 3a 64 74 bc 53 ct 55 66 34 190 q8 64 74 bc 53 ct 64 64 22 64 fc 64 22 64 fc 64 22 65 fc 64 25	L ↓ 0 E · . (0 9 ·				
80058 8618 8628 8648 8058 8058 8058 8058 8058 8058 8068 806	L2 522 74 31 a9 bf 62 6f 1b 57 40 7f 68 b6 a6 61 15 79 fd 60 79 72 17 65 63 12 4b 47 30 86 24 12 4b 47 30 86 24 12 4b 47 30 86 24 12 4b 47 30 86 24 15 16 40 47 30 16 50 52 47 16 53 44 9 47 55 40 49 47 fc 18 55 43 77 fc 18	15 5c 5f 67 9c 45 00 46 61 33 64 32 35 64 35 35 64 32 35 64 32 35 64 32 35 64 32 35 64 35 36 46 35 36 46 46 46 46 46 46 46 46 46 46 46 47 47 46 47 46 46 46 47 47 46 47 46 47 46 47 46 47 47 46 47 46 47 47 47 46 47 46 47 46 47 46 47 47 47 47 47 47 47 47 47 47 47 47 47 47 48 47 47 47 48 48 48 48 48 48 48 </td <td>1e 05 00 45 00 RCI a8 74 21 67 15 06 bb 00 13 08 00 01 45 01 08 00 01 45 01 08 00 01 45 01 07 15 16 00 05 05 06 00 05 05 00 05 05 00 05 05 00 05 05 00 05 05 00 05 05 00 05 00 00 00000000</td> <td>1\ 1\ 1</td> <td></td> <td></td> <td></td> <td></td>	1e 05 00 45 00 RCI a8 74 21 67 15 06 bb 00 13 08 00 01 45 01 08 00 01 45 01 08 00 01 45 01 07 15 16 00 05 05 06 00 05 05 00 05 05 00 05 05 00 05 05 00 05 05 00 05 05 00 05 00 00 00000000	1\ 1\ 1				
80058 8618 8628 8648 8058 8058 8058 8058 8058 8058 8058 80	b 52 74 31 49 bf 62 74 51 49 bf 62 6f 1b 57 49 76 86 b6 46 17 68 b6 46 17 68 b6 46 17 68 b6 47 17 68 b6 47 17 68 b6 87 17 68 b6 87 17 68 b6 87 17 68 b6 87 18 68 7 18 68 7 19 69	15 55 57 67 90 40 60 82 24 60 85 17 95 80 2 7 12 80 90 90 80 85 17 95 10 82 7 12 80 10 10 10 10 10 10 10 10 10 10 10 <td>10 100 45 00 45 10 74 21 67 15 17 92 10 00 10 10 10 17 17 17 10 10 10 17 17 10 10 10 17 17 10 10 10 16 10 17 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10</td> <td>L _ g E - E Bill E </td> <td></td> <td></td> <td></td> <td></td>	10 100 45 00 45 10 74 21 67 15 17 92 10 00 10 10 10 17 17 17 10 10 10 17 17 10 10 10 17 17 10 10 10 16 10 17 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10	L _ g E - E Bill E 				
9098 8019 9029 9048 9058 9058 9058 9058 9058 9058 9058 905	52 74 11 00 17 40 52 74 11 00 17 40 52 74 10 57 40 71 68 169 07 40 71 68 169 07 40 73 76 169 10 16 56 83 62 61 10 12 10 10 16 84 52 60 84 52 60 85 62 61 10 10 10 85 62 61 10 10 85 62 61 10 10 85 62 61	15 55 51 67 52 15 16 46 66 52 13 12 12 13 13 12 12 13 13 12 12 13 12 13 13 13 12 13 </td <td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td> <td>1</td> <td>с м м м м м м м м м м м м м м м м м м м</td> <td></td> <td></td> <td></td>	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	1	с м м м м м м м м м м м м м м м м м м м			
9058 9018 9029 9058 9058 9058 9058 9058 9038 9088 9088 9088 9088 9088 9088 908	2 52 74 11 a9 bf 62 74 11 a9 bf 62 67 14 15 74 91 76 15 a6 a6 37 0 f 96 16 56 58 75 74 10 58 75 75 75 75 75 75 75 75 75 75 75 75 75	15 5.5 5.1 6.7 5.4 00 4.0 6.0 6.2 2.1 6.0 0.6 0.7 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6 0.6	10 88 60 45 60 81 10 74 21 67 55 7 10 80 10 17 7 5 10 90 10 10 17 21 5 10	1. _ g ∈ ti 0.9. 0.9. 0.10 ti 0.10 ti 0.10 ti 0.10 ti 0.10 ti 0.10 ti 1.0 ti 0.10 ti 1.0		Burdent 101	19. Decisioni 1113 88 No. Decesso II.	10.0%1 Brokke Datas
8058 8019 8029 8038 8048 8058 8058 8058 8058 8058 8058 805	22 74 11 00 11 1 52 74 11 00 11 1 77 61 10 05 4 17 75 10 10 5 4 17 75 10 10 5 4 17 75 11 00 12 1 17 12 11 00 12 1 17 15 11 00 12 1 17 15 11 00 12 1 17 15 11 00 12 1 15 10 10 1 15 10 10 10 10 10 10 10 10 10 10 10 10 10	15 55 57 67 56 43 68 52 43 68 54 68 56<	10 08 00 45 00 RC a8 74 21 67 55 75 95 17 67 23 07 15 76 95 17 67 23 76 95 17 67 23 76 45 16 45 76 45 16 16 76 45 16 16 76 45 16 16 76 45	↓ 0 E 6 № 0 9		Packets: 131	2: Displayet: 1713 (09 7%) - Droppet: 0	0.0%) Profile: Defaul
00088 0019 0029 0046 0058 0058 0038 0038 0048 0048 0048 0048 0048 004	2 52 74 11 a9 Dr 62 74 11 a9 Dr 76 20 dr 15 7 a0 18 a6 17 75 16 a8 17 7 17 8 a8 17 7 17 18 a8 17 8 18 a6 17 7 17 18 a8 18 46 17 7 17 18 48 18 46 17 25 16 38 18 46 17 25 16 38 26 47 6 26 47 6 27 6 27 6 28 48 28	15 50 17 10<	10 80 00 45 00 etc. 10 74 147 15 10 75 149 05 10 75 14 10 75 14 10 75 14 10 75 14 10 75 15 10	L · _ g : E · - g Mg : g · - g ·		Packets: 191	5: Displayed: 1713 (08,7%) - Displayed: 0	0.0%) Profile: Defaul
80038 8019 8028 8048 8058 8058 8058 8058 8058 8058 805	2 52 74 31 a0 bf 52 74 31 a0 bf 52 67 b5 74 51 67 5 19 67 51 75 19 67 51 75 19 67 51 75 19 67 51 75 19 67 51 74 63 51 24 bd 51 86 52 64 64 67 53 64 97 6 53 64 97 6 54 64 97 6 55 64 97 6 55 64 97 6 55 64 97 7 56 64 97 6 57 6 57 67 6 57	75 55 57 67 56 55 50 44 66 52 26 55 50 54 56 <td>10 00 45 00 RC1 a0 74 15 5 - a0 70 15 16 - a0 70 10 10 - a0 80 10 13 - a0 80 10 13 - a0 50 60 40 - a0 50 60 - - a0 54 61 40 - a0 54 61 41 - a0 54 61 12 16 - a0 54 61 12 16 - - a0 54 51 16 5 -</td> <td>L</td> <td>5 6 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8</td> <td>Packets 190</td> <td>D: Doşlayet: 1713 (18,7%) - Dropoet: 01</td> <td>0.0%) Profile: Defaul</td>	10 00 45 00 RC1 a0 74 15 5 - a0 70 15 16 - a0 70 10 10 - a0 80 10 13 - a0 80 10 13 - a0 50 60 40 - a0 50 60 - - a0 54 61 40 - a0 54 61 41 - a0 54 61 12 16 - a0 54 61 12 16 - - a0 54 51 16 5 -	L	5 6 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	Packets 190	D: Doşlayet: 1713 (18,7%) - Dropoet: 01	0.0%) Profile: Defaul



So, I will open a terminal and start wireshark. You can install wireshark using sudo app install wireshark. I have already installed it. So, I will directly open it using root privilege. So, let us enter the password. So, this is the wireshark interface. So, I will start the packet capturing using this button. So, let us try to open some website, let us say, cse.iitb.ac.in. And you can see that there are lots of packets which we can see in wireshark. So, they have various different IP addresses.

Let us first find what is the IP address of cse.iitb.ac.in. I will copy this IP address and I will stop this packet capturing and filter paste on the IP address. So, I will write ip.addr == this. So, now we can see tool packets were exchanged between my computer and the cse server. So, if we have a look at the first three packets we can identify that this is the three way handshake.

So, this is the IP address of my router and it sends to destination one TCP packet, the SYN packet and the server responds with an acknowledgement over the SYN packet and then my computer again sends the acknowledgement packet to complete the three way handshake. So, that is how the communication begins with the cse server and then it sends lots of other packets.

Let us first see what were other different fields. So, this is the time field which shows at what time relative to the beginning of packet capture, this transmission took place and it shows the source and destination, then which protocol was used. So, we can see there are two mainly, TCP and TLS. The TLS stands for transport layer security protocol, and then the length of the packet and then some information.

So, let us try to see some application data packet. So, this is one application data packet. And you can see that because it is a TLS packet, there is a secure sockets layer on top of the TCP layer. So, here we can go through various headers that are there in this packet. So, let us open this TCP header. So, here it shows us the source port, the destination port, the sequence number and the acknowledgement number and various other things such as checksum.

Similarly, we can go through other headers such as IP header, Ethernet header or the frame header. And here if you see the payload we cannot make any sense of it because this is encrypted application data. So, let us try to see if we can access some unsecure website and if we can make sense of the payload data.

(Refer Slide Time: 03:31)





So, what I will do here is I will open http website. Now, most of the website today use https, so the s stands for secure. So, they will encrypt the packet data before sending it over the network. But here I have copied one URL which is still using http. This is the website. And if I go to this log in page then here we can see that there is a red line on the lock and here it shows us that connection is not secure, because it is using http.

Let us start the capture and I will continue without saving and I will remove this filter also. And now if I enter some username and password, let us see, I enter username and password as _____password and if I log in, I will just choose do not save. So, it says username and password do not match, but we do not care. I will stop the capture. And now let us filter based on TCP packets which contains the word username. So, here it shows me this packet and you can see that we can clearly make sense of all this data because this is not encrypted. And if I click here then it shows me that the username is username and password is __password.

So, I can clearly see the password if I just snoop over the network traffic. So, that is one of the reason why it is suggested to use public wifi networks cautiously because someone might be snooping on the router and if we happen to visit some insecure website then the person can easily know ID password.

So, that was it for this video. Thanks and have a nice day.