Demystifying Networking Department of Computer Science and Engineering Indian Institute of Technology, Bombay

Lecture – 07 Listening to the Internet chatter

So now, you have seen there is a lot of communication that has over the internet, lot of applications trying to connect to their servers and the servers setting responses. So, your laptop itself has a lot of applications apart from the web browser we choose the internet. Now it would be really interesting to see if we could see this actual communication or as we say the chatter happening over the internet between all these devices. And yes, there is a software that can help us just do that, And that software is Wireshark.

(Refer Slide Time: 00:31)



So, basically Wireshark is a software that allows us to capture live internet traffic. And when we say live internet traffic, we can actually see the layer by layer architecture of the traffic, how each layer has its own information and that information later allows the communication to happen. Now, let us go and look at how Wireshark works. (Refer Slide Time: 00:59)

The Wireshark Network A File Edit View Go Cap	alyzer ture Analyze Statistics Telephony Wireless Tools H Zo Q and a construction of the construction of t	łelp		- a x
Apply a doping filter _ <dri-< th=""><th></th><th></th><th></th><th>Epression +</th></dri-<>				Epression +
	Welcome to Wireshark			
	Cantona			
	capture			
	using this filter:			All interfaces shown •
	Bluetooth Network Connection			
	Local Area Connection* 1			
	Npcap Loopback Adapter			
	Local Area Connection* 9			
	VirtualBox Host-Only Network			
	Wi-Fi how			
	Local Area Connection* 2			
	Local Area Connection* 10			
	Local Area Connection* 11			
	Learn			
	Bearly Colds - Milli - Countines and Seconds - Maller	er fiele		
	and a more was Argennie and versioners . When	d no		
	You are running Wireshark 3.6.0 (v3.0.0-0-g837e33de). You rec	eke automatic updates.		
7 Ready to keed or centure			Re Packets	Profile: Default

Now, I am going to open Wireshark. Wireshark is a free software you can download it, once you have installed it, just double click and once you double click it will look for the different type of networks that are available on your computer. For example, on this laptop we have a Wi-Fi card. So, I will select my Wi-Fi as the network interface that I want to monitor. And once I have done that, I will click on this blue colored fin to start capturing the communication.

(Refer Slide Time: 01:29)

🔏 Capturing from Wi-Fi						- σ x	
Fle	Edit View G	o Capture Ana	elyze Statistics	Telephony	Wireless Tools Help		
1	0.0	X & A	*****		14 4 4 E		
A App	ly a display filter	. <0#h/>					Expression
85.	Time	Source	Destination	Protocol	Length Info		
	15 1.945068	192.168.1	239.255.25_	SSDP	216 M-SEARCH * HTTP/1.1		
	15 2.877460	192.168.1	239.255.25_	SSEP	216 M-SEARCH * HTTP/1.1		
	17 3.071371	192.168.1	224.0.0.251	MDIIS	79 Standard query 0xb194 PTR _arduinotcp.local, "QM" question		
	18 3.482596	192.168.1	239.255.25.	SSDP	318 NOTIFY * HTTP/1.1		
	19 4.713478	192.168.1	192.168.1	DB-LS_	246 Dropbox LAW sync Discovery Protocol		
	20 4.923493	192.168.1	192.168.1	MBNS	92 Name query NB WPAD(00)		
	21.4.923493	fe90::508a.	ff02::1:3	LUMIR	84 Standard query 0x8315 A wpad		
	22 4.923494	192.168.1	224.0.0.252	LUMR	64 Standard query 0x8315 A wpad		
	23 4.923494	192.168.1	239.255.25.	SSOP	216 M-SEARCH * HTTP/1.1		
	24 4.923494	192.168.1	192.168.1	MBRS	110 Refresh NB MACBOOKAIR-CCC0<20>		
	25 4.923495	192.168.1	192.168.1	NBIS	110 Retiresh NB WORKGROUP<00>		
	26 5.119285	IntelCor_a_	Broadcast	ARP	42 Who has 169.254.5.233? Tell 192.168.1.121		
	27 5.325387	fe80::6d8a_	ff02::1:3	LUMR	84 Standard query 0x8315 A wpad		
	28 5.325388	192.168.1	224.0.0.252	LUMIR	64 Standard query 0x8315 A wpad		
	29 5.631570	192.168.1	192.168.1	NBNS	92 Name query NB MPADORO		
	38 6.848649	IntelCor_a_	Broadcast	ABP	42 Who has 169.254.5.233? Tell 192.168.1.121		
	31 7.866165	IntelCor_a_	Broadcast	ARP	42 Who has 169.254.5.233? Tell 192.168.1.121		
0000 0010 0020	ff ff ff ff i 88 88 86 6 88 88 86 6	ff ff ff 68 0 M 00 01 68 0 M 00 00 a9 f	7 15 a4 e6 5 7 15 a4 e6 5 e 05 e9	1 08 06 1 c0 a8	80 81 bQ 177 bQy-		
0 7	WHE dwe ca	pture in progress>				Packats: 32 - Displayed: 32 (100.0%)	Profile: Defai

So, as I click here what you see is that a number of packets are being shown, these are basically the communication that is happening from my laptop to different servers.