

How to capture the packet using Ethereal.

1. What is Ethereal ?

Ethereal is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

2. Where to get Ethereal ?

You can get the latest copy of the program from the Ethereal website: <u>http://www.ethereal.com/download.html</u>

3. Installing Ethereal

You must follow two steps:

-. Install WinPcap.

You will find a single installer exe called something like "auto-installer", which can be installed under various Windows systems. This installer is located at: <u>http://winpcap.polito.it/install/Default.htm</u>. You should download the latest released version (the latest one not marked "beta") and execute it.

-. Install Ethereal.

http://www.ethereal.com/download.html#binaries. Download the installer and execute it.



4. Capturing Network Data

-. By starting Ethereal and then selecting Start... from the Capture menu this brings up the Capture Options dialog box.

Capture packets in promiscuous mode Limit each packet to 00	t's Packet Scheduler) – \(_ ♥) megabyte(s) ▼
IP address: 210.221.197.10 Link-layer header type Ethernet ≥ Buffer size: IP Capture packets in promiscuous mode Link teach packet to 50 Begapture Filter: Capture Filter: Capture Filter: Capture Filter: Filer: P Use multiple files Thint file avery 1 amegabyte(s)	
Case layer Header type Ethernet 2 Buffer size 1 If Capture packets in promiscuous mode Limit each packet to 68 bytes If Capture Pitter Capture P	megabyte(s)
Capture packets in promiscuous mode Limit each packet to 50 bytes Capture Filter Capture Filter Filty Filty Vise multiple files Filty	megabyte(s)
Limit each packet to	
IP Capture Filter Display Capture Filter Display Filer Energy T Use multiple files T Use T Next file every 1 Image/hyter(c) Image/hyter(c)	<u>.</u>
Capture File(s) File: Display File: Display Di	*
File: Browse File: Comparison of the second seco	
C Use multiple files □ Plent file avery 1 1 megabyte(c) ↓ □ △	Options
Flient file every	tate list of packets in real time
L HART DE RARA	
E Next file every 1 1 1 execute(a) 2 E His	anialic actalling in live capture
	e capture info dialog
P Ring boffer with 2 . files. Name	Resolution
Stop capture after 1 Diffé(6)	
Stop Capture	ible MAC name resolution
🗖 after 1 🗘 packet(a) 🗖 En	able getwork name resolution
🗖 after 1 🗐 megabyte(s) 🗢	
T after 1 🔅 mmute(u) 🗘 🕅 En	
BHelp	able gransport name resolution

-. **Interface** : This field specifies the interface you want to capture on. You can only capture on one interface, and you can only capture on interfaces that Ethereal has found on the system.

While the capture is running, the following dialog box is shown:

Ethereal	Capture	from Intel(
Captured Packets					
Total	14	% of total			
SCTP	0		0.0%		
TCP	3		21.4%		
UDP	1	1	7.1%		
ICMP	0		0.0%		
ARP	4		28.6%		
OSPF	0		0.0%		
GRE	0		0.0%		
NetBIOS	0		0.0%		
IPX	0		0.0%		
VINES	0		0.0%		
Other	6		42.9%		
Running	00:00:13				
C Stop					

This dialog box will inform you about the number of captured packets and the time since the capture was started.



6	⇒ 🖬 ×	0 8 G) 命 命 😳 圣 否	0,0,0,	10 D B	* 2	0
Eilter	1			- + Expressio	in. S <u>C</u> lear	¥ Apply	
No	Time	Source	Destination	Protocol Info			
7 8	4.000176 6.000370 8.000400 8.008095	Dat 85 Dat 85 Dat 85 210 48	Spanning-tree-(for spanning-tree-(for	STP Conf STP Conf BROWSER Doma	Root = 327 Root = 327 Root = 327 In/Workgroup has 21	789/00:d	0:cb:0a:ab:0 0:cb:0a:ab:0
10 11 12 13 14	9.390813 9.956488 10.000493 10.390462 10.950499	214 1 214 1 214 1 214 1 214 1 214 1	Broadcast Spanning-tree-(for Broadcast Uroadcast Uroadcast	ARP who STP Conf ARP who	has 21 , Root has 21 has 21	87 10 77	Tell 210. Dicb:Oatabit Tell 210. Tell 210.

5. Saving captured packets

You can save captured packets simply by using the Save As... menu item from the File menu under Ethereal.

Ethereal: Save Capture File As		
Name:		
Save in folder: 🗁 Temp		[•]
₽ Browse for other folders		
Packet Range		
	Captured	Displayed
All packets	135	135
C Selected packet only	1	1
C Marked packets only	0	0
O From first to last marked packet	0	0
C Specify a packet gange:	. 0	0
File type: libpcap (tcpdump, Ethereal, o	etc.)	•
	Save	X Cancel
	Tour Sauce	A Concer