

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.

Ethereal: Capture Options	
Capture	
Interface: Intel(R) PRO/100 VE Network Connection	m (Microsoft's Packet Scheduler) : V 💌
IP address: 210.221.197.10	
Link layer header typeEthernet C Buffer size, 1	- megabyte(s)
Capture packets in promiscuous mode	
Limit each packet to 68 🗄 bytes	
\$®⊆spture Filter	•
Capture File(s)	Display Options
File: Browse	Update list of packets in real time
Use multiple files	A DESCRIPTION AND ADDRESS OF ADDRESS
T First fie wary 1 megabyte(6)	Actomatic actolling in live capture
Next file every 1 execute(a)	F Hide capture into dialog
🕫 Ring buffer with 🛛 👔 files.	Name Resolution
C Stop capture after 1 🗘 file(6)	Hame Resolution.
Stop Capture	P Enable MAC name resolution
🗖 _ after [1 🗳 packet(a)	Enable network name resolution
🗆 after 🕴 🚺 megabyte(s) 😂	
E attac 1 A monthly A	R Enable transport 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 Pa	ckets				
Total	14	% of total			
SCTP	0		0.0%		
TCP	3		21.4%		
UDP	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		(@ E	9 4	中的生子	0.0	Q # D B X 0
E)Elter.					▼ + Expression. Sciear ¥ Apply		
No	Te	me	Source		Destination	Protocol	Info
- Fr D IE	4 1. 5 2. 6 4. 7 6. 9 8. 10 9. 11 9. 12 10 13 10 14 10 14 10 14 10 14 10	274609 000064 000176 000370 000400 0008095 390813 956488 0.000493 0.390462 0.950499 1. (60 by 02.3 Eth	210 Das Das Das Das 210 210 210 210 210 210 210 210 210 210	10 85 85 85 48 1 1 1 1 1 1 1 1 1 1	spanning-tree-(for spanning-tree-(for spanning-tree-(for spanning-tree-(for spanning-tree-(for groadcast spanning-tree-(for groadcast spanning-tree-(for groadcast uroadcast uroadcast es captured)	TCP STP STP STP BROWSER ARP ARP ARP ARP	Tisl > 1863 [ACK] Seq-5 Ack-8 Win- Conf. Root = 32789/00:d0:cb:0a:abi Conf. Root = 32789/00:d0:cb:0a:abi Conf. Root = 32789/00:d0:cb:0a:abi Domain/workgroup Announcement WORK Who has 21 Who has 21 Who has 21 Who has 21 T Tell 210. Who has 21 T Tell 210. T Tell 210. Who has 21 T Tell 210. T Tell 210. Who has 21 T Tell 210. T T Tell
sp	annir	ng Tree	Protocol				
0000	01 03 00	80 c2 0 00 00 0 00 80 1 00 0f 0	0 00 00 00 0 00 00 80 5 00 d0 ct	d0 cb 0a 15 00 d0 0a ab 85 a5 a5 a5	ab 85 00 26 42 42 cb 0a ab 85 00 00 80 01 00 00 14 00 a5 a5		

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				
O Selected packet only	1	1				
O Marked packets only	0	0				
O From first to last marked packet	0	0				
C Specify a packet range:	0	0				
File type: libpcap (topdump, Ethereal,	etc.)	0				
	Save	X Cancel				