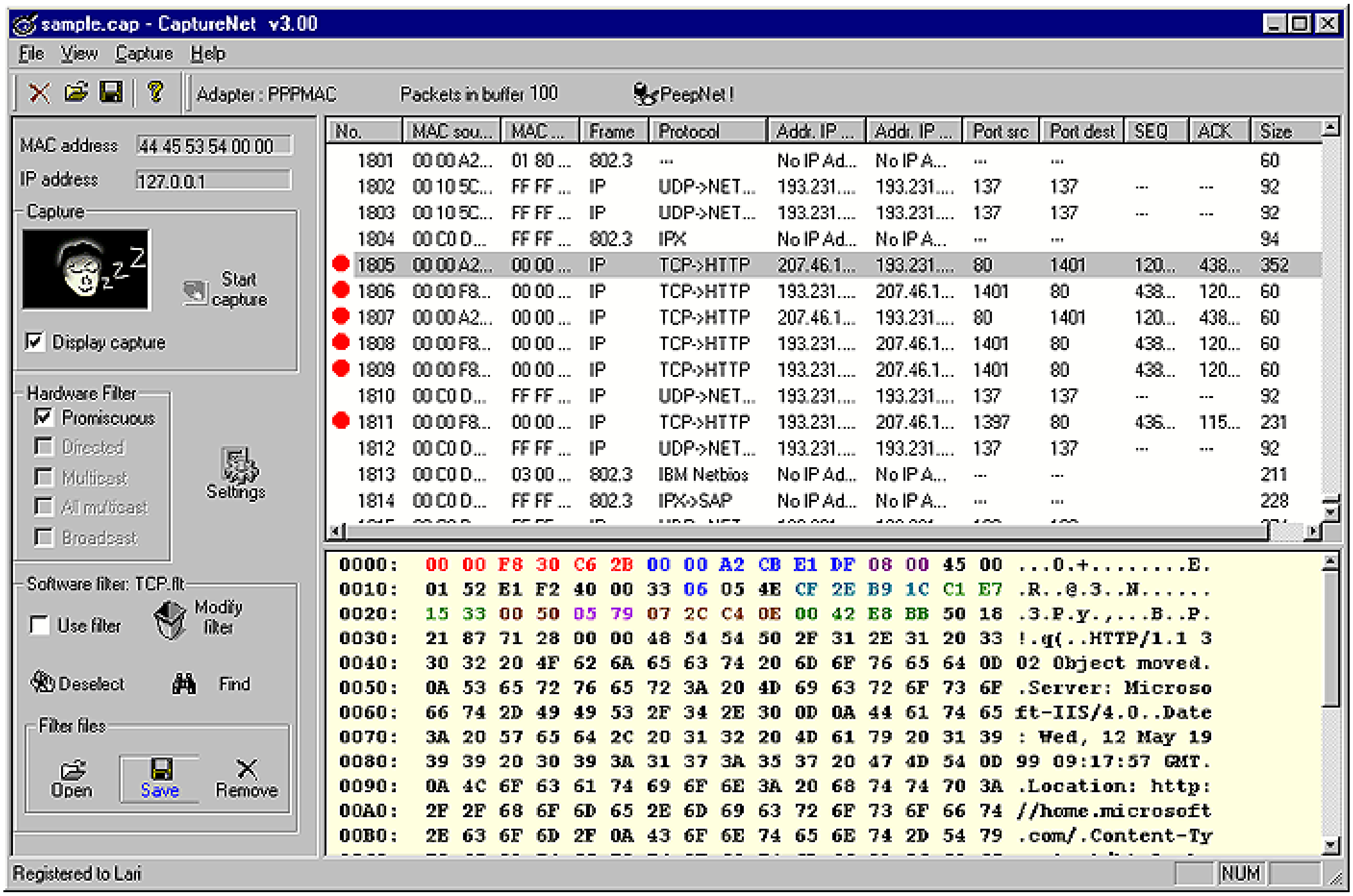
Main Interface



MAC address 44 45 53 54 00 00

IP address 127.0.0.1

☑ Display capture

☑ Promiscuous

□ Directed

□ Multicast

□ All multicast

□ Broadcast

□ Use filter

No.	MAC sou...	MAC ...	Frame	Protocol	Addr. IP ...	Addr. IP ...	Port src	Port dest	SEQ	ACK	Size
1801	00 00 A2...	01 80 ...	802.3	...	No IP Ad...	No IP A...	...	...			60
1802	00 10 5C...	FF FF ...	IP	UDP->NET...	193.231....	193.231....	137	137	---	---	92
1803	00 10 5C...	FF FF ...	IP	UDP->NET...	193.231....	193.231....	137	137	---	---	92
1804	00 C0 D...	FF FF ...	802.3	IPX	No IP Ad...	No IP A...	...	...			94
● 1805	00 00 A2...	00 00 ...	IP	TCP->HTTP	207.46.1...	193.231....	80	1401	120...	438...	352
● 1806	00 00 F8...	00 00 ...	IP	TCP->HTTP	193.231....	207.46.1...	1401	80	438...	120...	60
● 1807	00 00 A2...	00 00 ...	IP	TCP->HTTP	207.46.1...	193.231....	80	1401	120...	438...	60
● 1808	00 00 F8...	00 00 ...	IP	TCP->HTTP	193.231....	207.46.1...	1401	80	438...	120...	60
● 1809	00 00 F8...	00 00 ...	IP	TCP->HTTP	193.231....	207.46.1...	1401	80	438...	120...	60
1810	00 C0 D...	FF FF ...	IP	UDP->NET...	193.231....	193.231....	137	137	---	---	92
● 1811	00 00 F8...	00 00 ...	IP	TCP->HTTP	193.231....	207.46.1...	1397	80	436...	115...	231
1812	00 C0 D...	FF FF ...	IP	UDP->NET...	193.231....	193.231....	137	137	---	---	92
1813	00 C0 D...	03 00 ...	802.3	IBM Netbios	No IP Ad...	No IP A...	---	---			211
1814	00 C0 D...	FF FF ...	802.3	IPX->SAP	No IP Ad...	No IP A...	...	...			228

```
0000:  00 00 F8 30 C6 2B 00 00 A2 CB E1 DF 08 00 45 00  ...0.+........E.
0010:  01 52 E1 F2 40 00 33 06 05 4E CF 2E B9 1C C1 E7  .R..@.3..N......
0020:  15 33 00 50 05 79 07 2C C4 0E 00 42 E8 BB 50 18  .3.P.y.,...B..P.
0030:  21 87 71 28 00 00 48 54 54 50 2F 31 2E 31 20 33  !.q(..HTTP/1.1 3
0040:  30 32 20 4F 62 6A 65 63 74 20 6D 6F 76 65 64 0D  02 Object moved.
0050:  0A 53 65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F  .Server: Microso
0060:  66 74 2D 49 49 53 2F 34 2E 30 0D 0A 44 61 74 65  ft-IIS/4.0..Date
0070:  3A 20 57 65 64 2C 20 31 32 20 4D 61 79 20 31 39  : Wed, 12 May 19
0080:  39 39 20 30 39 3A 31 37 3A 35 37 20 47 4D 54 0D  99 09:17:57 GMT.
0090:  0A 4C 6F 63 61 74 69 6F 6E 3A 20 68 74 74 70 3A  .Location: http:
00A0:  2F 2F 68 6F 6D 65 2E 6D 69 63 72 6F 73 6F 66 74  //home.microsoft
00B0:  2E 63 6F 6D 2F 0A 43 6F 6E 74 65 6E 74 2D 54 79  .com/.Content-Ty
```

Command line arguments

Run CaptureNet with /? Argument to see a list of arguments

/? - Shows a list of arguments.

/autostart - Loads CaptureNet without showing the splash screen and starts capturing upon loading.

/f: <filter_file.flt> - Loads a software filter file (which has to be in the same directory as Capturenet)

What is CaptureNet

CaptureNet is a network sniffer for Windows 95/98/NT.

CaptureNet captures all network packets while PeepNet interprets them and tries to reconstruct the original sessions the packets belonged to, showing you, for example, the web page a user was watching.

CaptureNet:

- Can be used to store ALL network activity in timestamped files as evidence of possible criminal activities.
- It can capture all packets with or without software filters.
- It is able to save captured data to a file for later analyses.
- Recognizes main protocols used in an Ethernet network.
- Works with dial-up adapters too.
- It was designed to maintain its settings between uses.
- Offers the possibility to search through thousands of packets those matching a user-defined filter.

Inclusive

Check this radio button to **select** packets that fulfill the filter condition.

Exclusive

Check this radio button to **reject** packets that fulfill the filter condition.

Reset buffers

Clears the list of packets displayed in packets window and empties the internal buffers.

Number of received packets is set to 0.

Command is not available while capturing.

Open capture file

Open a previously saved capture file (*.cap). If “Display capture” is OFF it will be set to ON.

Display capture

Turn on and off the packets decoding and displaying

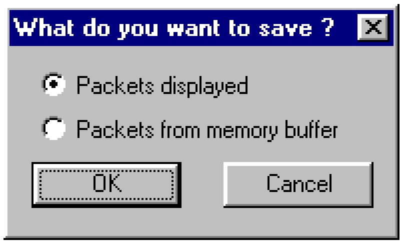
The processes of decoding and displaying captured packets consume more CPU time than a flow of hundreds of packets per second. On the other hand, when CaptureNet runs in background (minimized) there is no point in consuming CPU time with packets analyses.

Save packets

After a capturing session you can save the captured packets using this button.

A **What do you want to save dialog** will appear asking what do you want to save.

What do you want to save dialog



What do you want to save ?

● Packets displayed

○ Packets from memory buffer

Click on the radio button you want to learn about.

Saving displayed packets

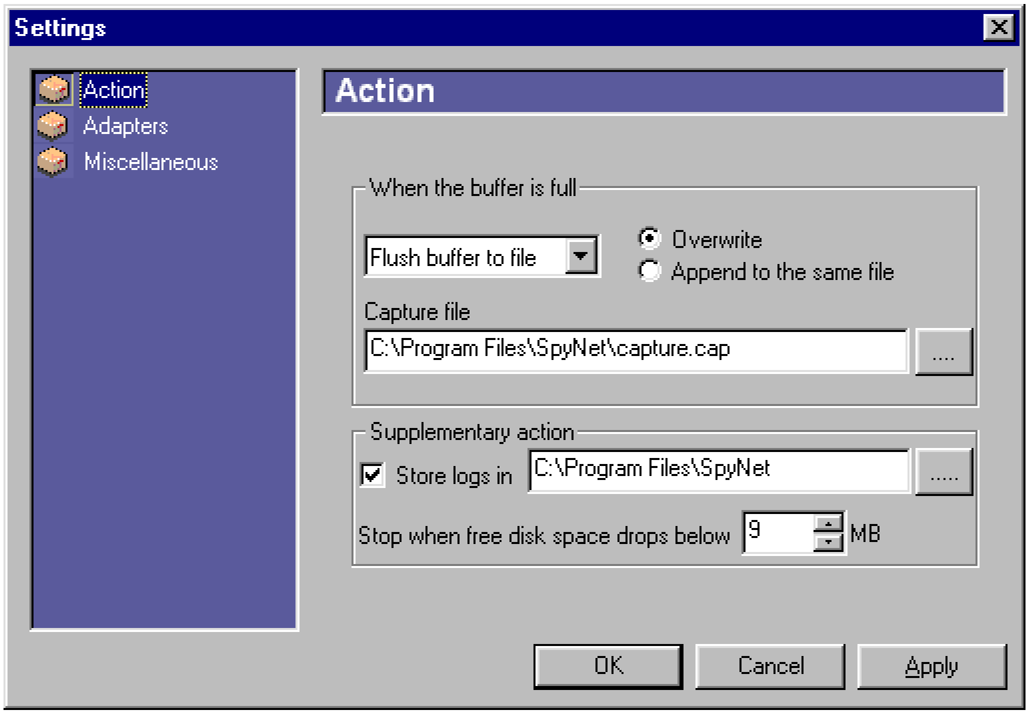
Select the **Displayed packets** radio button if you want to save only packets displayed in packets window. The number of displayed packets may differ from number of packets from memory buffer because while capturing it is possible to switch ON or OFF the process of displaying captured packets.

Saving packets from memory buffer

Regardless of being displayed or not, all received packets are found in memory buffer. If you have set the packets displaying OFF, use **Packets from memory buffer** option to save captured packets.

Memory buffer size can be adjusted from Miscellaneous tab.

Settings->Action Panel



When the buffer is full

Flush buffer to file

● Overwrite

○ Append to the same file

Capture file

C:\Program Files\SpyNet\capture.cap

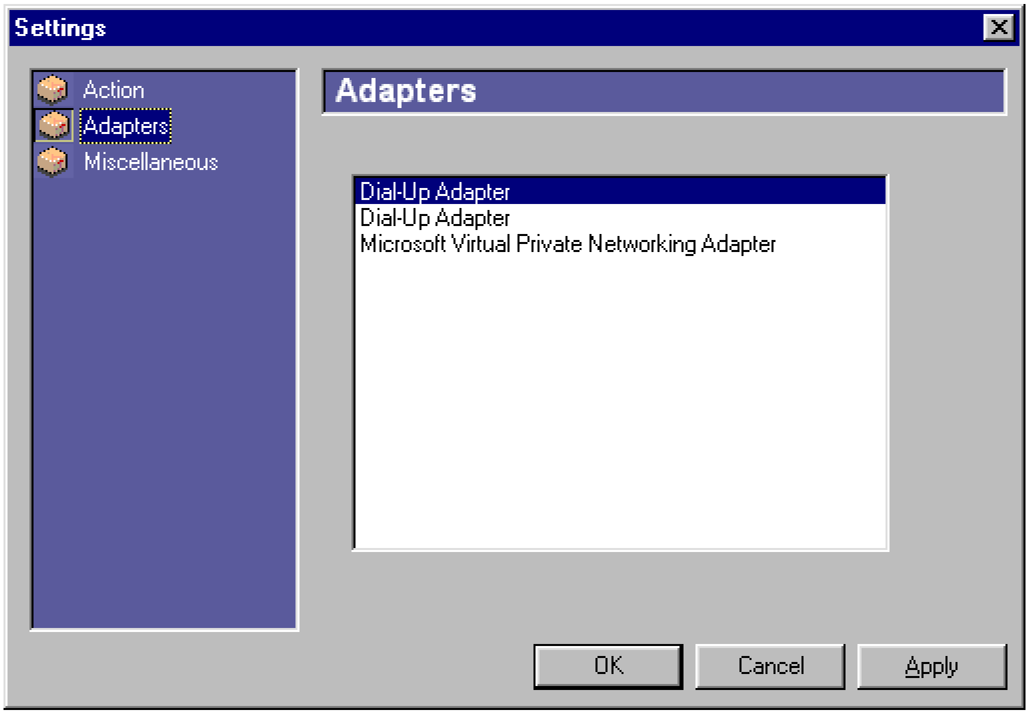
Supplementary action

☑ Store logs in C:\Program Files\SpyNet

Stop when free disk space drops below 9 MB

Click the element you want help for.

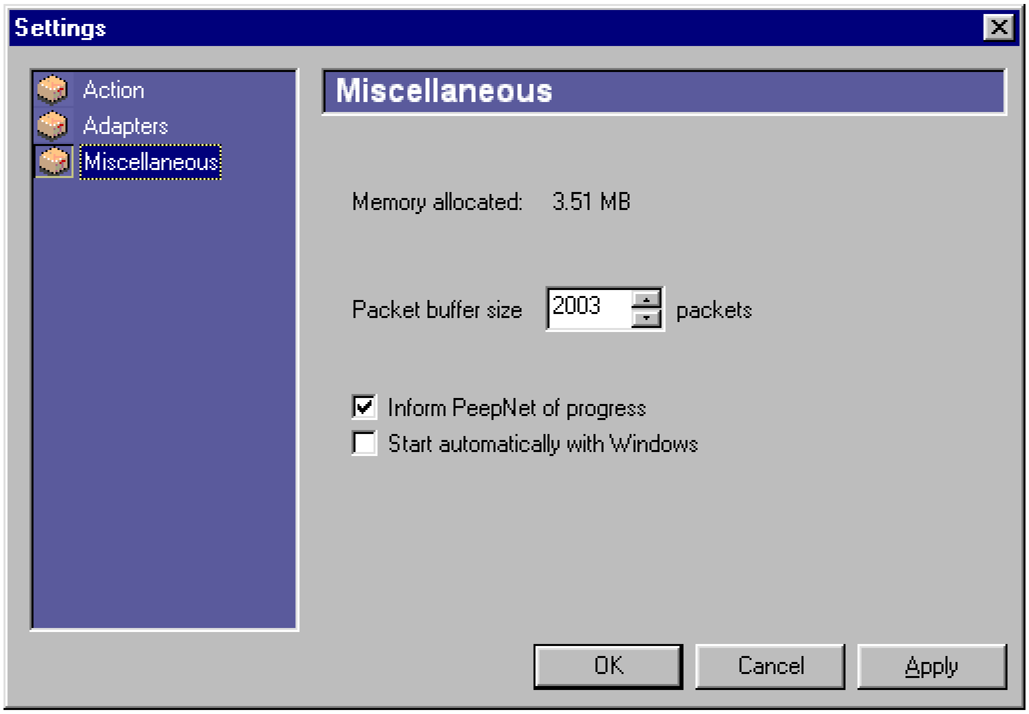
Settings->Adapter Panel



Dial-Up Adapter
Dial-Up Adapter
Microsoft Virtual Private Networking Adapter

Click the element you want help for.

Settings->Miscellaneous Panel



Memory allocated: 3.51 MB

Packet buffer size 2003 packets

☑ Inform PeepNet of progress

□ Start automatically with Windows

Click the element you want help for.

About dialog box

Display copyright information and registration status of this CaptureNet copy.

Adapter internal name

Display the internal name of the selected adapter.

Packets in buffer

Indicates how many packets are in the internal buffer. When saving memory buffer packets , there will be saved as much packets as indicated here.

Launch PeepNet

This will execute PeepNet program.

MAC address

Shows the Network Adapter hardware address. Every Ethernet card for example has a unique 48bits number.

IP addres

Shows this host IP address.

Start/Stop capture

Starts/ stops capturing process. The same result can be achieved by selecting the appropriate menu item.

Also when the program is minimized, this command is available by right clicking the systray icon.

Starts the capture (shortcut Ctrl-A).

Pressing again this button will stop the capture (Ctrl-Z).

Hardware filters

Hardware filters deals with the adapter’s hardware address.

The following hardware filters are available:

1. Promiscuous filter
2. Directed filter
3. Multicast filter
4. All Multicast filter
5. Broadcast filter

Promiscuous filter

Checking this filter tells CaptureNet to capture all packets.

Directed filter

Checking this filter tells CaptureNet to capture packets addressed to this Adapter.

Note: This not includes packets sent by this adapter.

Multicast filter

Checking this filter tells CaptureNet to capture multicast packets.

All Multicast filter

Checking this filter tells CaptureNet to capture all multicast packets.

Broadcast filter

Checking this filter tells CaptureNet to capture broadcast packets

Settings

There are 3 setting panels:

1. Action
2. Network adapter
3. Miscellaneous

Use filter

Check here to apply the defined filter to incoming packets or packets loaded from a capture file

Note: This check box will be disabled when the current filter is NULL. (i.e. all filter components are empty)

Only packets that will match whole filter will be captured. The filter is *inclusive* i.e. only those packets that will match all filter conditions will be captured and eventually displayed.

Animation

This animation indicates when CaptureNet is looking for packets (moving eyes) or idle (sleepy guy).

IP protocol field

This field is specific to IP datagrams and indicates the type of the encapsulated packet. In this case it is a TCP packet.

See here the structure of a few frame types.

Modify filter

The Filter menu provides four ways to selectively capture and display captured traffic on your LAN.   These filters may be used singly, in combination, or may be left unused.

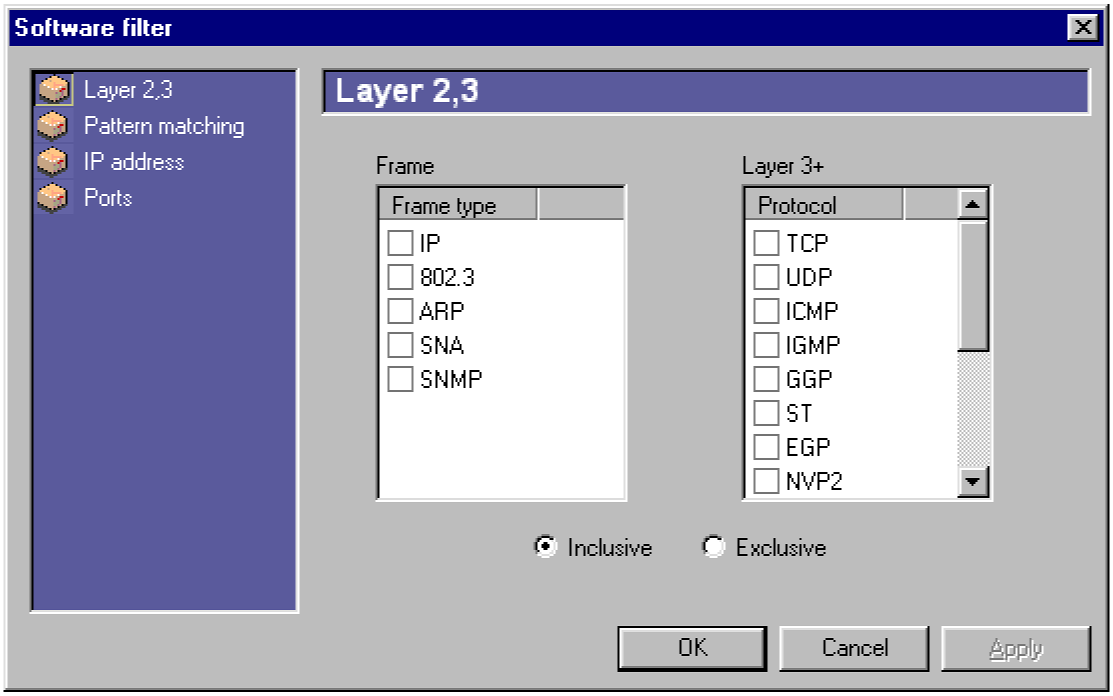
The analyzer offers four ways to filter traffic; by frame type, words to be found in packet, station address and ports –for TCP/UDP. This allows you to analyze traffic in various logical 'slices' on a busy LAN that contains packets that are not a part of the problem.

Four filters are available here to help you capturing only the desired packets:

1. Layer 2,3
2. Pattern matching
3. IP address
4. Port filter

Only packets that will match whole filter will be captured.

Layer 2,3 filter



Software filter

Layer 2,3

Frame

Frame type
□ IP
□ 802.3
□ ARP
□ SNA
□ SNMP

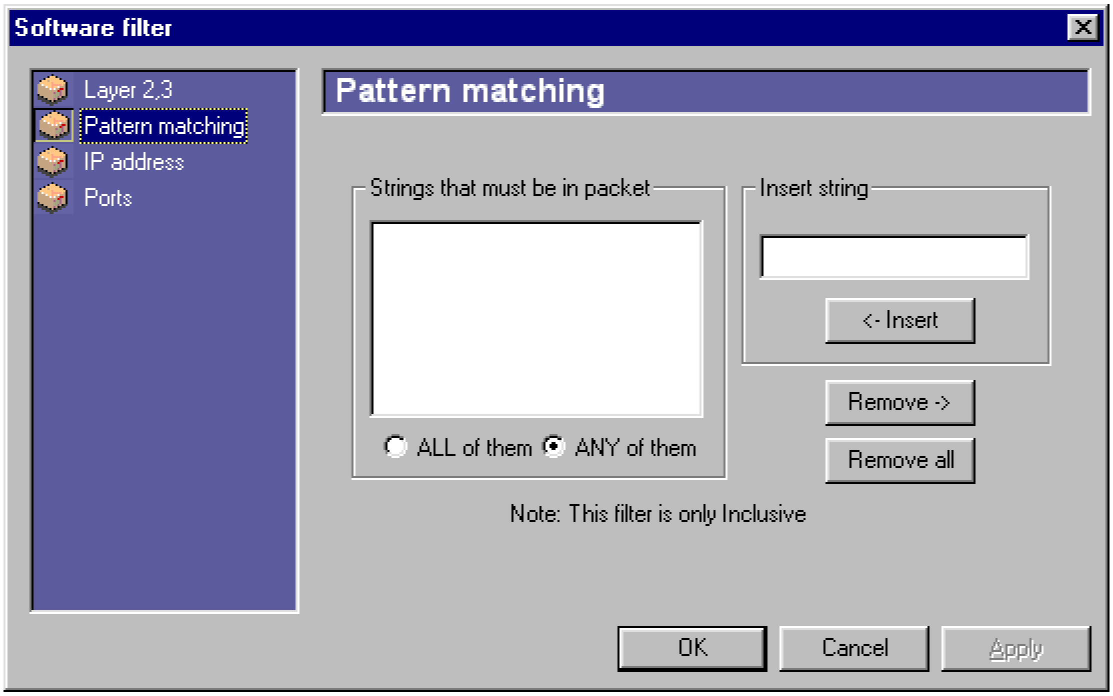
Layer 3+

Protocol
□ TCP
□ UDP
□ ICMP
□ IGMP
□ GGP
□ ST
□ EGP
□ NVP2

● Inclusive ○ Exclusive

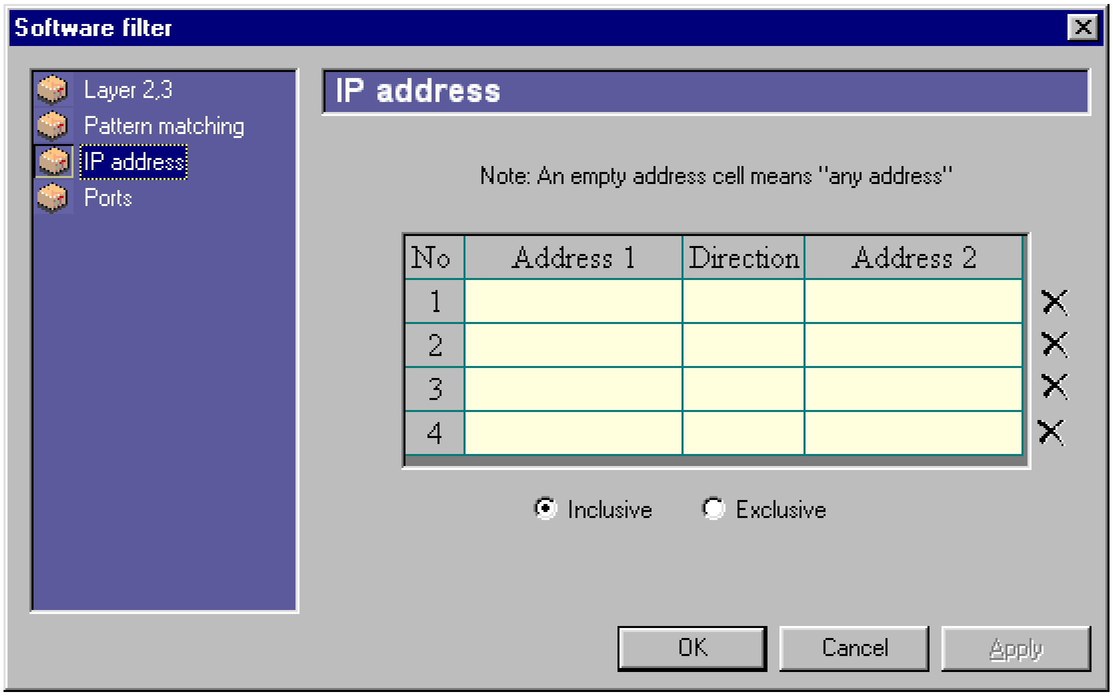
Only packets that match the packet types selected here will be captured.

Pattern matching filter



Only packets that match the packet types selected here will be captured.

IP address filter



IP address

Note: An empty address cell means "any address"

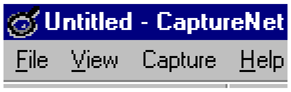
No	Address 1	Direction	Address 2
1			
2			
3			
4			

● Inclusive ○ Exclusive

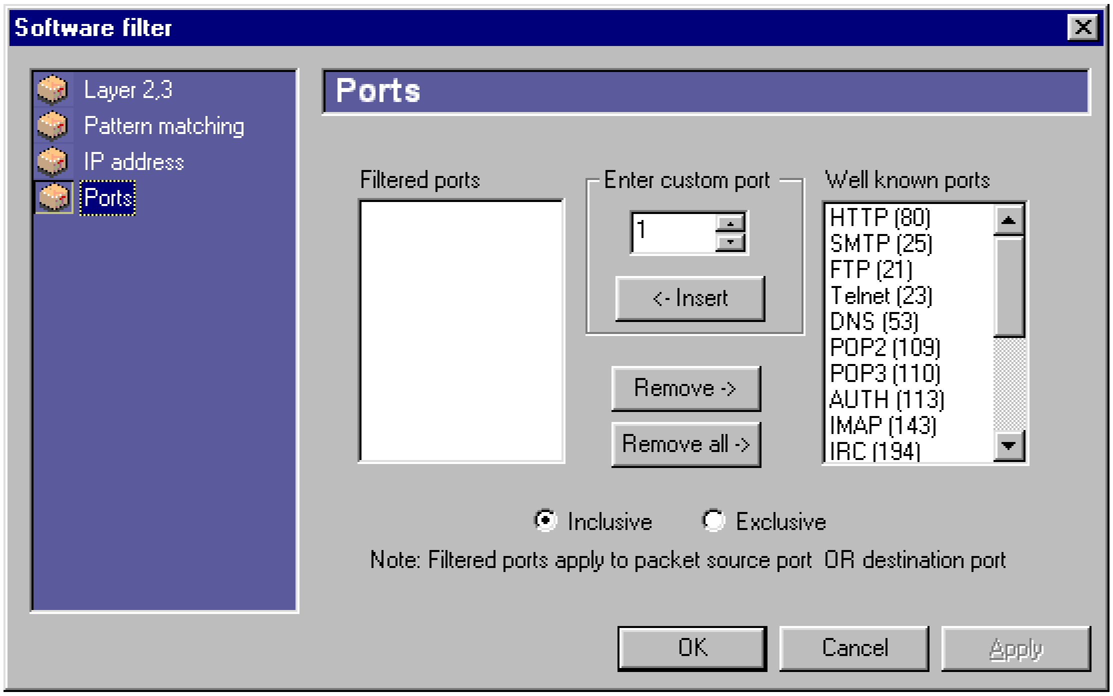
Just as Layer 2,3 filter make the analyzer capture those packets matching a specific protocol, Address Filters make the analyzer choose only packets sent (1) from a specified IP address; (2) to a specified IP address; (3) from one address to another address; or (4) bidirectional traffic between two addresses. If no address filters are defined, then address filtering is disabled. If you specify one or more address filters, then only those packets matching one or more of those filters will be accepted.

Only packets that match the packet types selected here will be captured.

Menu



Port filter



Enter custom port: 1

Well known ports: HTTP (80), SMTP (25), FTP (21), Telnet (23), DNS (53), POP2 (109), POP3 (110), AUTH (113), IMAP (143), IRC (194)

● Inclusive ○ Exclusive

Note: Filtered ports apply to packet source port OR destination port

Only packets that match the packet types selected here will be captured.

Unselect packets

This will remove the mark sign (●) from selected packets.

Find packets

Finds and selects packets matching the software filter.

If there are packets that match the current filter, they will be marked with a ● sign and a message on the status bar will tell you the number of selected packets.

The process of searching occurs only among packets displayed in the packet window. (not in the packets buffer.)

Open filter file

Opens a previously saved filter file. Upon opening, the Use filter will be set to ON.

Save filter file

Saves to disk the current software filter.

Remove filter

This clears all filter fields thus setting it to NULL. Also the Use filter check box will be set to OFF and will be disabled.

The filter file will not be deleted from disk.

Packets number

Here it is displayed the packet number.

Source MAC address

Here it is shown the MAC hardware address of the adapter that has sent this packet.

This field is enlarged (becoming visible) only at resolutions bigger than 800x600.

Destination MAC address

Here it is shown the MAC hardware address of the adapter that is the intended receiver of this packet.

This field is enlarged (becoming visible) only at resolutions bigger than 800x600.

Frame type

Frame types recognized by this version of CaptureNet are:

1.	IP	(08 00) 0x0008
2.	802.3	< 0x05DC
3.	ARP	(08 06) 0x0608
4.	SNA	(80 D5) 0xD580
5.	SNMP	

The **Type** field it is found at offset 0x0b (12) within the packet.

See here how data flows in a TCP/IP network.

Protocol type

This field shows both the protocol and service.

E.g.: TCP->HTTP means that the data is encapsulated in a TCP packet and represents a part of a HTTP session (generated for example while requesting a web page after clicking a link)

See here the structure of a few frame types.

Source IP address

This field shows the IP source address (of course if it is an IP packet).

See here the structure of a few frame types.

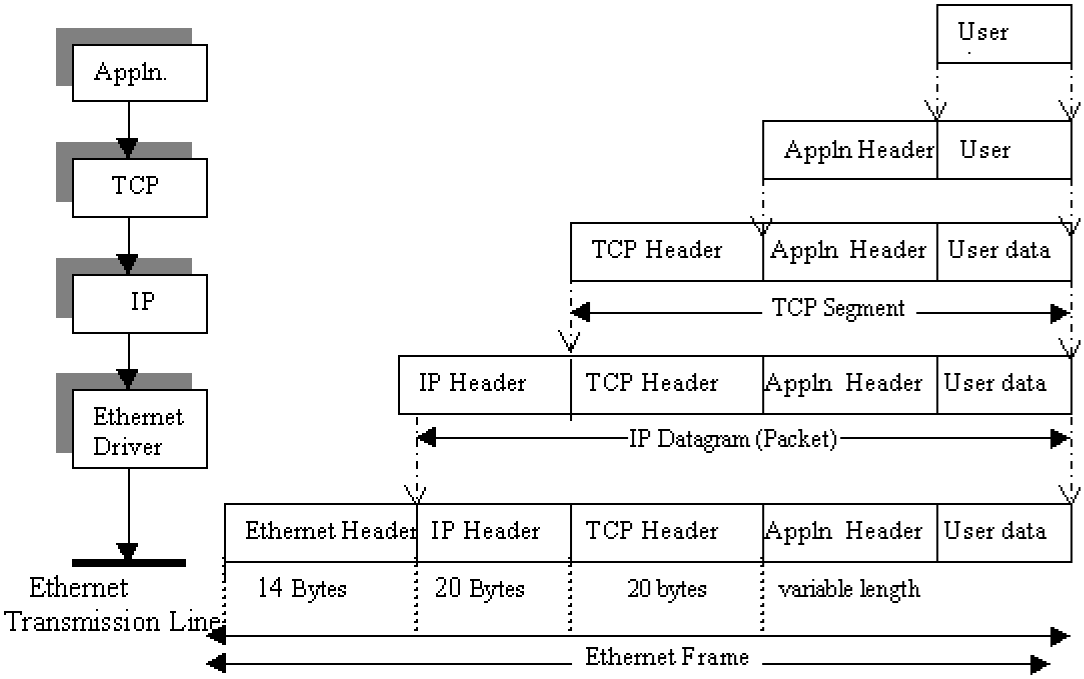
Destination IP address

This field shows the IP destination address (of course if it is an IP packet).

See here the structure of a few frame types.

Data flow in a TCP/IP network

To transmit data across a layered network we pass data from our application to a protocol on a protocol stack. After that protocol finishes with your data it passes the data to the next protocol on the stack. As the data passes through each layer, the protocols on the stack encapsulate the data for the next lower level in the stack. Encapsulation, therefore, is the process of storing your data in the format required by the lower level protocol in the stack.



See here the structure of a few frame types.

Source port

This field shows source port of packets (specific to TCP, UDP packets).

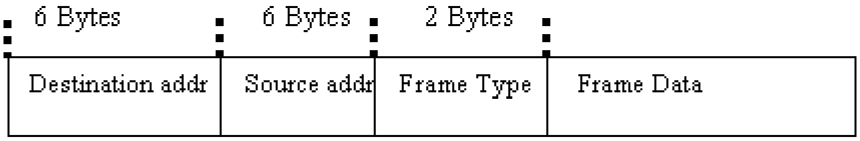
If this is for example 80, this means that a WEB server sent this packet.

See here the structure of a few frame types.

Frame structure

Few frame structures:

Here is the structure of Ethernet frame

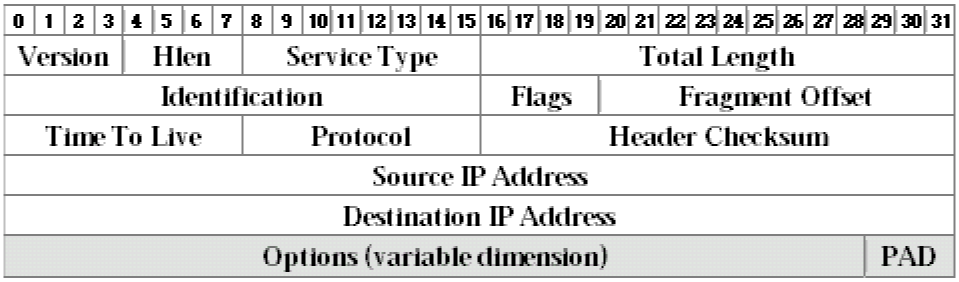


6 Bytes	6 Bytes	2 Bytes	
Destination addr	Source addr	Frame Type	Frame Data

Format of an Ethernet Data Frame.

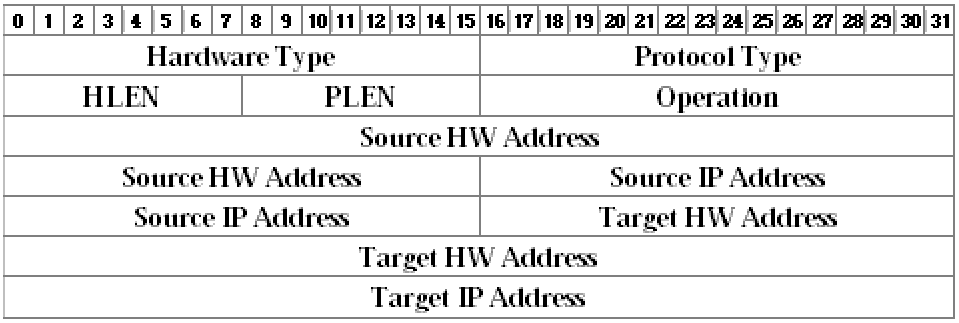
The DATA portion from an Ethernet frame could be one of those packets:

IP v4



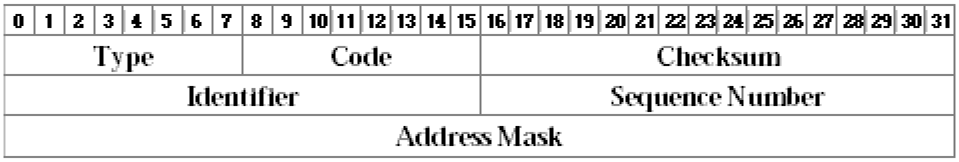
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				Hlen				Service Type								Total Length															
Identification																Flags				Fragment Offset											
Time To Live								Protocol								Header Checksum															
Source IP Address																															
Destination IP Address																															
Options (variable dimension)																													PAD		

ARP



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Hardware Type																Protocol Type															
HLEN								PLEN								Operation															
Source HW Address																															
Source HW Address																Source IP Address															
Source IP Address																Target HW Address															
Target HW Address																															
Target IP Address																															

ICMP



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type								Code								Checksum															
Identifier																Sequence Number															
Address Mask																															

Here is the TCP packet structure

<table>
<tr><td colspan="3"><b>Source Port (2 Bytes)</b></td><td colspan="2"><b>Destination Port (2 Bytes)</b></td></tr>
<tr><td colspan="5">Sequence Number (4 Bytes)</td></tr>
<tr><td colspan="5">Acknowledge Number (4 Bytes)</td></tr>
<tr><td>Hlen
(4 Bits)</td><td>Reserved
(6 Bits)</td><td>Code Bits
(6 Bits)</td><td colspan="2">Window
(2 Bytes)</td></tr>
<tr><td colspan="3">Checksum (2 Bytes)</td><td colspan="2">Urgent data (2 Bytes)</td></tr>
<tr><td colspan="4">Options (If Any-3 Bytes)</td><td>Padding (1 Byte)</td></tr>
<tr><td colspan="5">DATA</td></tr>
</table>

Destination port

This field shows destination port of packets (specific to TCP, UDP packets).

See here the structure of a few frame types.

Hexa viewer

Hexa representation of the packet’s data.

ASCII viewer

ASCII representation of the packet’s data.

Adapter list

Select from the names listed the adapter you want to monitor.

Memory allocation

Tells how much memory has been allocated for the internal buffers.

Buffer size

This is an important setting for the SpyNet operation. This setting tells CaptureNet for how many packets to reserve memory space at program start-up. Allocating memory for every packet at the time it arrives it is a very resource-consuming task. That's why the memory is allocated at program start-up and CaptureNet it has to be restarted if this setting is changed. I recommend a value of 1000 packets for running coupled with PeepNet (i.e. having PeepNet set to Run).

When this buffer is filled, depending on how the Action is set, PeepNet will start analyzing the captured data.

So, inserting here a very big value, it will let you wait quite a long time before seeing some results in PeepNet.

If running CaptureNet alone, a value of 3000 can be satisfactory.

Start automatically with Windows

Makes CaptureNet run automatically after Windows finishes it's loading.

Checking this will create a registry entry which will make load CaptureNet after Windows completes its loading. Clearing this, will remove this registry entry.

Note: When loaded from StartUp folder, CaptureNet will always start capturing.

To start automatically, use the /autostart parameter.

Inform PeepNet of progress

Check this and CaptureNet will inform PeepNet about current filling rate of packet buffer. The progress bar from PeepNet will show when the action of analyzing the packets will occur. Useful only when CaptureNet and PeepNet are running on the same host.

When buffer is full

When buffer is full (number of captured packets equals packet buffer size) there are three possibilities:

1. **Flush buffer to file** which can be done in two modes

   a). Overwrite

   -Capture file will be overwritten at each write

   b). Append

   -Capture file will grow with every buffer flushing (PeepNet will stop running)

   Note: Be warned that this file can become extremely large in a short time.

2. **Wrap memory buffer**

   There will be no disk operation. When the capture buffer it will be filled it will start from the beginning, overwriting old packets.

3. **Stop capture**

   Pretty self-explanatory.

Capture filename

Will be used by CaptureNet when will flush the capture buffer. PeepNet will monitor the same file. When running on the same computer with CaptureNet, PeepNet will automatically set this filename to the same value as CaptureNet

Choose capture file

Choose the path and filename of the capture file.

Store logs in

When checked, CaptureNet in both *append* and *overwrite* modes saves every capture log in the directory specified in following edit control. This option was introduced for archiving purposes. Log filename is stamped with a time string.

Logs directory

After writing capture file, CaptureNet can also automatically store the file in a separate directory for later analyses (for archiving purposes or even as evidence). The filename is composed from the filename taken from **Capture file edit box** and is completed with a timestamp in the following format:

If date is 08 August 1999 and the time is 14:57:51 the filename will be:

capture_Sun_Aug_08_14_57_51_1999.cap

Choose Logs directory

Displays a Browse Folders window letting you choose the supplementary logs directory.

Stop when free disk space drops below

Space that is guaranteed to remain free onto the disk partition where supplementary logs are created. When free space drops below this value, only this supplementary logging will be stopped. (i.e. CaptureNet will continue to write the main log file and PeepNet will operate normally.)

Frame

Select here what frame types do you want to filter.

E.g.: Selecting 802.3 will filter only packets with a **type** value smaller then 0x5DC

See here the structure of a few frame types.

Layer 3

Select the protocols you want to filter. Only selected protocols will be captured.

Note: Selecting from the right panel an IP encapsulated packet (for example TCP or UDP) will automatically select the IP frame.

Strings list

This list contains strings that must be in the packet data. The string comparison is case insensitive.

Use this filter to catch only packets with desired words in them. For instance you can insert the PASS string and will see the results.

All of them

All words from the **String list** must be in packet.

Any of them

The filter condition will be fulfilled if any word is present in the packet data.

Insert strings

Write here the word you want to insert in the words list and then press Insert button.

Remove button

Press this button to remove selected values from the filter list.

Remove All button

Press this button to remove all values from the filter list.

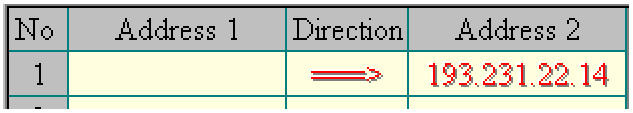
IP address filter

Use this filter to select only packets coming or leaving a particular host(s).

If an address cell is empty, it is considered to be **Any address**.

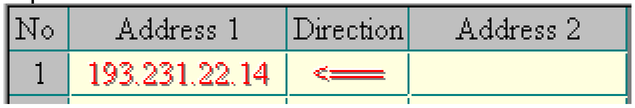
Up to four IP hosts addresses are permitted. Possible configurations are:

1. ---



No	Address 1	Direction	Address 2
1		==>	193.231.22.14

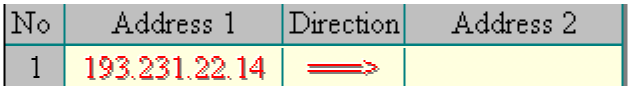
equivalent with



No	Address 1	Direction	Address 2
1	193.231.22.14	<==	

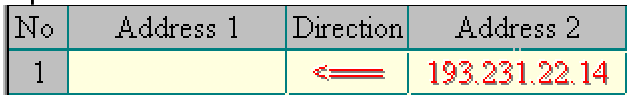
This means all IP packets addressed to host 193.231.22.14 will be captured.

2. ---



No	Address 1	Direction	Address 2
1	193.231.22.14	==>	

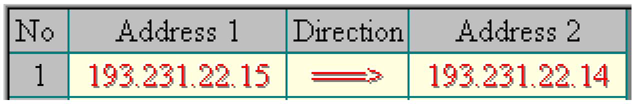
equivalent with



No	Address 1	Direction	Address 2
1		<==	193.231.22.14

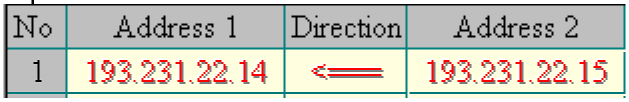
This means all IP packets leaving host 193.231.22.14 will be captured.

3. ---



No	Address 1	Direction	Address 2
1	193.231.22.15	==>	193.231.22.14

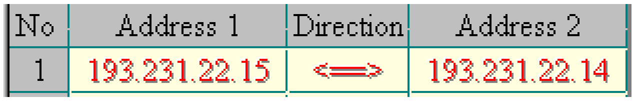
equivalent with



No	Address 1	Direction	Address 2
1	193.231.22.14	<==	193.231.22.15

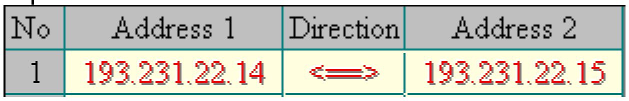
All packets coming from 193.231.22.15 addressed to 193.231.22.14 will be captured.

4. ---



No	Address 1	Direction	Address 2
1	193.231.22.15	<==>	193.231.22.14

equivalent with



No	Address 1	Direction	Address 2
1	193.231.22.14	<==>	193.231.22.15

This will catch the whole conversation between 193.231.22.15 and 193.231.22.14.

Clear filter

Click these buttons to remove the correspondent filter.

Filtered ports

This list contains those ports you select to be monitored. If this list is empty, ALL ports will be monitored.

When you want to remove ports from the list, select them with your mouse cursor and then click Remove button.

To remove a single value, just double-click on it.

Insert custom ports

Type in the number of the desired port and click Insert   button to insert it in the ports list.

Well known ports

This list contains few known port values. Double click on the desired value to insert it in the filtered ports list.

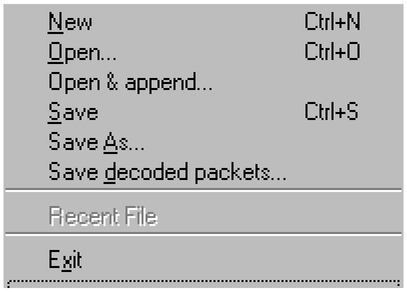
Save decoded packets

This option will create a file with decoded packets. For every **displayed** packet there will be an entry in file.

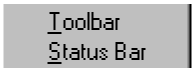
Something like this:

```
=====================================================================

No:                 136
MAC source address: 00 00 21 86 17 43
MAC dest address:   FF FF FF FF FF FF
Frame:              IP
Protocol:           UDP->NETBIOS-DGM
Source IP address:  193.231.21.71
Dest IP address:    193.231.21.255
Source port:        138
Destination port:   138
SEQ:                ---
ACK:                ---
Packet size:        251

Packet data:
0000:  FF FF FF FF FF FF 00 00 21 86 17 43 08 00 45 00 ........!..C..E.
0010:  00 ED CF 00 00 00 80 11 BB EA C1 E7 15 47 C1 E7 .............G..
0020:  15 FF 00 8A 00 8A 00 D9 42 A6 11 02 01 02 C1 E7 ........B.......
0030:  15 47 00 8A 00 C3 00 00 20 46 43 45 50 46 45 45 .G...... FCEPFEE
0040:  42 46 43 46 46 45 44 43 41 43 41 43 41 43 41 43 BFCFFEDCACACACAC
0050:  41 43 41 43 41 43 41 41 41 00 20 45 47 45 42 45 ACACACAAA. EGEBE
0060:  44 44 43 43 41 43 41 43 41 43 41 43 41 43 41 43 DDCCACACACACACAC
0070:  41 43 41 43 41 43 41 43 41 42 4F 00 FF 53 4D 42 ACACACACABO..SMB
0080:  25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %...............
0090:  00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 29 ...............)
00A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00B0:  00 00 00 29 00 56 00 03 00 01 00 01 00 02 00 3A ...).V.........:
00C0:  00 5C 4D 41 49 4C 53 4C 4F 54 5C 42 52 4F 57 53 .\MAILSLOT\BROWS
00D0:  45 00 0F 2A 40 77 1B 00 52 4F 54 41 52 55 43 00 E..*@w..ROTARUC.
00E0:  00 00 00 00 00 00 00 00 04 00 03 20 45 00 15 04 ........... E...
00F0:  55 AA 52 4F 54 41 52 55 20 43 00                U.ROTARU C.

=====================================================================
```

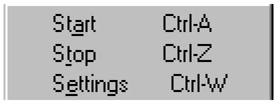
File Menu


New Ctrl+N
Open... Ctrl+O
Open & append...
Save Ctrl+S
Save As...
Save decoded packets...
Recent File
Exit

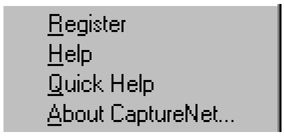
View Menu



Capture Menu



Help Menu



Toolbar

Display or hide toolbar**.**

Status bar

Display or hide status bar**.**

Open & append

This option can be used to load a capture file without loosing captured packets or to concatenate two or more capture files. (eventually supplementary logs).

The size of the concatenated files can be even bigger than the buffer size. The program will allocate all the memory it needs on run-time.

Save as...

Save with a different name/location.

Exit

Exits CaptureNet program.

Last recent used files

Use the numbers and filenames listed at the bottom of the File menu to open the last four documents you closed. Choose the number that corresponds with the document you want to open.

Sequence number

This field is specific to TCP packets.

A number indicating the current block's position in the overall message. This number is also used between two TCP implementations to provide the initial send sequence (ISS) number.

Acknowledgment number

This field is specific to TCP packets.

A number that indicates the next sequence number expected. In a backhanded manner, this also shows the sequence number of the last data received; it shows the last sequence number received plus 1.

Packet size

Size of the packet in bytes.

Registering SpyNet

Benefits of registration

1. Unlimited support by email
2. My very warm thanks.

Pricing

Description	Price
SpyNet (CaptureNet + PeepNet)	$79

Registering information:

Credit card

If you wish to pay by credit card use the following link

http://www.all-connect.com/ShareRegister/shr2/SpyNet.htm

Western Union

The easiest way I found so far is like this:

1. Bring money to any **Western Union** agent in your country (they are present in 156 countries) and fill out a short form for sending money to:

   Name: **Nicula Laurentiu Gabriel**
   Address: **Bd. Iuliu Maniu, No.14, Bl.13, Sc.C, Et.5, Ap.106**
   City: **Bucharest**
   Country: **Romania**

2. Pay a service fee
3. Get a receipt with a Money Transfer Control Number (MTCN);
4. **Inform me about this transfer.** You **MUST** put in this email the following information:
   1. **MTCN** given by Western Union.
   2. **Your complete name** you used in the Western Union form **(very important!!!).**

3. A *Company name* and/or a *person name* to whom you want the program to be registered;

As soon as I receive your email, I'll respond with an email with a serial number that can be entered (by using copy and paste mechanism) in corresponding fields from Register dialog.

Some Western Union agent's phones around the world:

Australia	1 800 501 500	Ireland	1 800 395 395
Austria	(0222) 8920380	Israel	1 800 213141
Belgium	0800 99090	Italy	167 220055
Canada	800 235 0000	Netherlands	0800 0566
Czech Republic	(02) 24009173	New Zeeland	(09) 270 0050
Denmark	800 10711	Russia	(095) 1198266
Germany	(0681) 9333328	Sweden	020 741742
Greece	(01) 927 1010	Switzerland	0512 223358
Hungary	(01) 267 4282	United Kingdom	0800 8333 833
Iceland	552 3752	Unites States	800 325 6000
India	(011) 331 1122		

Postal Mail

Wrap money in some nontransparent paper and send them using postal mail or DHL to:

Name: **Nicula Laurentiu Gabriel**
Address: **Bd. Iuliu Maniu, No.14, Bl.13, Sc.C, Et.5, Ap.106**
City: **Bucharest**
Country: **Romania**

Print command (File menu)

Use this command to print a document. This command presents a Print dialog box, where you may specify the range of pages to be printed, the number of copies, the destination printer, and other printer setup options.

Shortcuts

Toolbar: 🖨
Keys: CTRL+P

Print dialog box

The following options allow you to specify how the document should be printed:

Printer

This is the active printer and printer connection.   Choose the Setup option to change the printer and printer connection.

Setup

Displays a Print Setup dialog box, so   you can select a printer and printer connection.

Print Range

Specify the pages you want to print:

All	Prints the entire document.
Selection	Prints the currently selected text.
Pages	Prints the range of pages you specify in the From and To boxes.

Copies

Specify the number of copies you want to print for the above page range.

Collate Copies

Prints copies in page number order, instead of separated multiple copies of each page.

Print Quality

Select the quality of the printing.   Generally, lower quality printing takes less time to produce.

Print Progress Dialog

The Printing dialog box is shown during the time that <<YourApp>> is sending output to the printer.   The page number indicates the progress of the printing.

To abort printing, choose Cancel.

Print Preview command (File menu)

Use this command to display the active document as it would appear when printed. When you choose this command, the main window will be replaced with a print preview window in which one or two pages will be displayed in their printed format. The print preview toolbar offers you options to view either one or two pages at a time; move back and forth through the document; zoom in and out of pages; and initiate a print job.

Print Preview toolbar

The print preview toolbar offers you the following options:

Print
Bring up the print dialog box, to start a print job.

Next Page
Preview the next printed page.

Prev Page
Preview the previous printed page.

One Page / Two Page
Preview one or two printed pages at a time.

Zoom In
Take a closer look at the printed page.

Zoom Out
Take a larger look at the printed page.

Close
Return from print preview to the editing window.

Print Setup command (File menu)

Use this command to select a printer and a printer connection.   This command presents a Print Setup dialog box, where you specify the printer and its connection.

Print Setup dialog box

The following options allow you to select the destination printer and its connection.

Printer

Select the printer you want to use. Choose the Default Printer; or choose the Specific Printer option and select one of the current installed printers shown in the box. You install printers and configure ports using the Windows Control Panel.

Orientation

Choose Portrait or Landscape.

Paper Size

Select the size of paper that the document is to be printed on.

Paper Source

Some printers offer multiple trays for different paper sources. Specify the tray here.

Options

Displays a dialog box where you can make additional choices about printing, specific to the type of printer you have selected.

Network...

Choose this button to connect to a network location, assigning it a new drive letter.

Page Setup command (File menu)

<< Write application-specific help here. >>