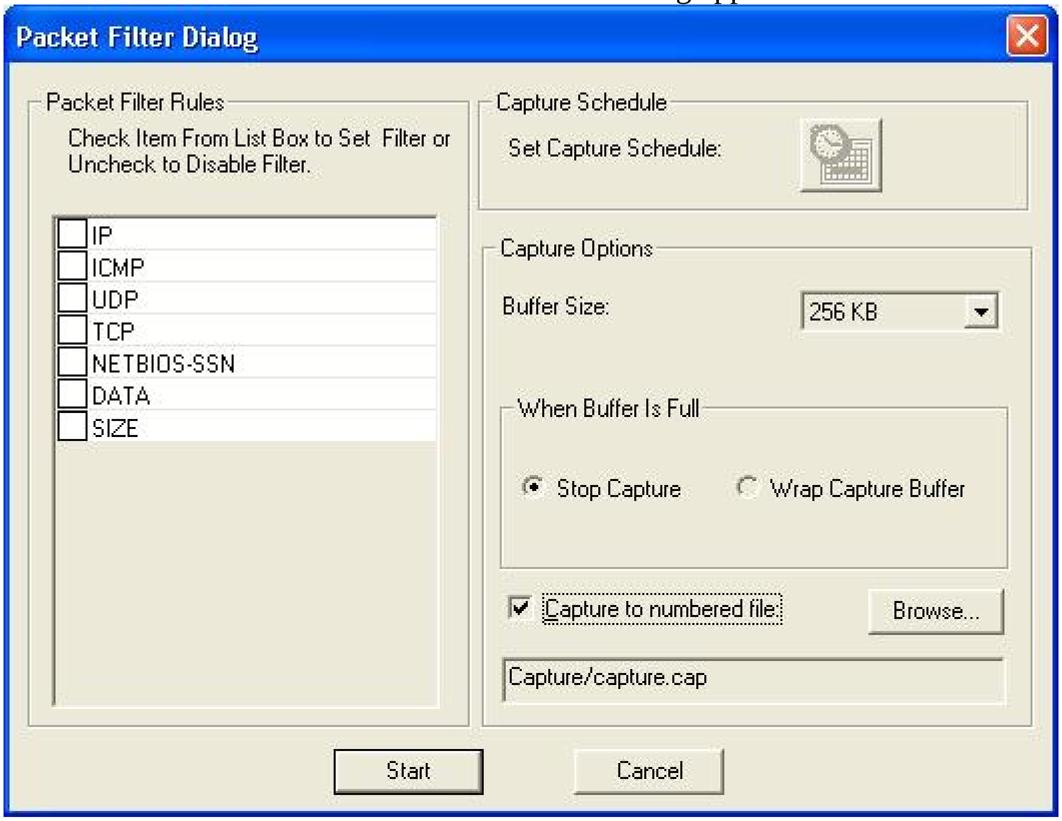
http://www.nsauditor.com

Nsasoft llc.

Packet Filter

Packet Filter is a tool that provides a real-time network packet filtering and analyzing. It allows to filter packets by all IP, ICMP, TCP, UDP, NETBIOS-SSN packet header fields. Before using the tool you should select the Interface you want to use.
After the interface is selected the Packet Filter Dialog appears in the screen.



Packet Filter Dialog

Packet Filter Rules

Check Item From List Box to Set Filter or Uncheck to Disable Filter.

- □ IP
- □ ICMP
- □ UDP
- □ TCP
- □ NETBIOS-SSN
- □ DATA
- □ SIZE

Capture Schedule

Set Capture Schedule:

Capture Options

Buffer Size: 256 KB

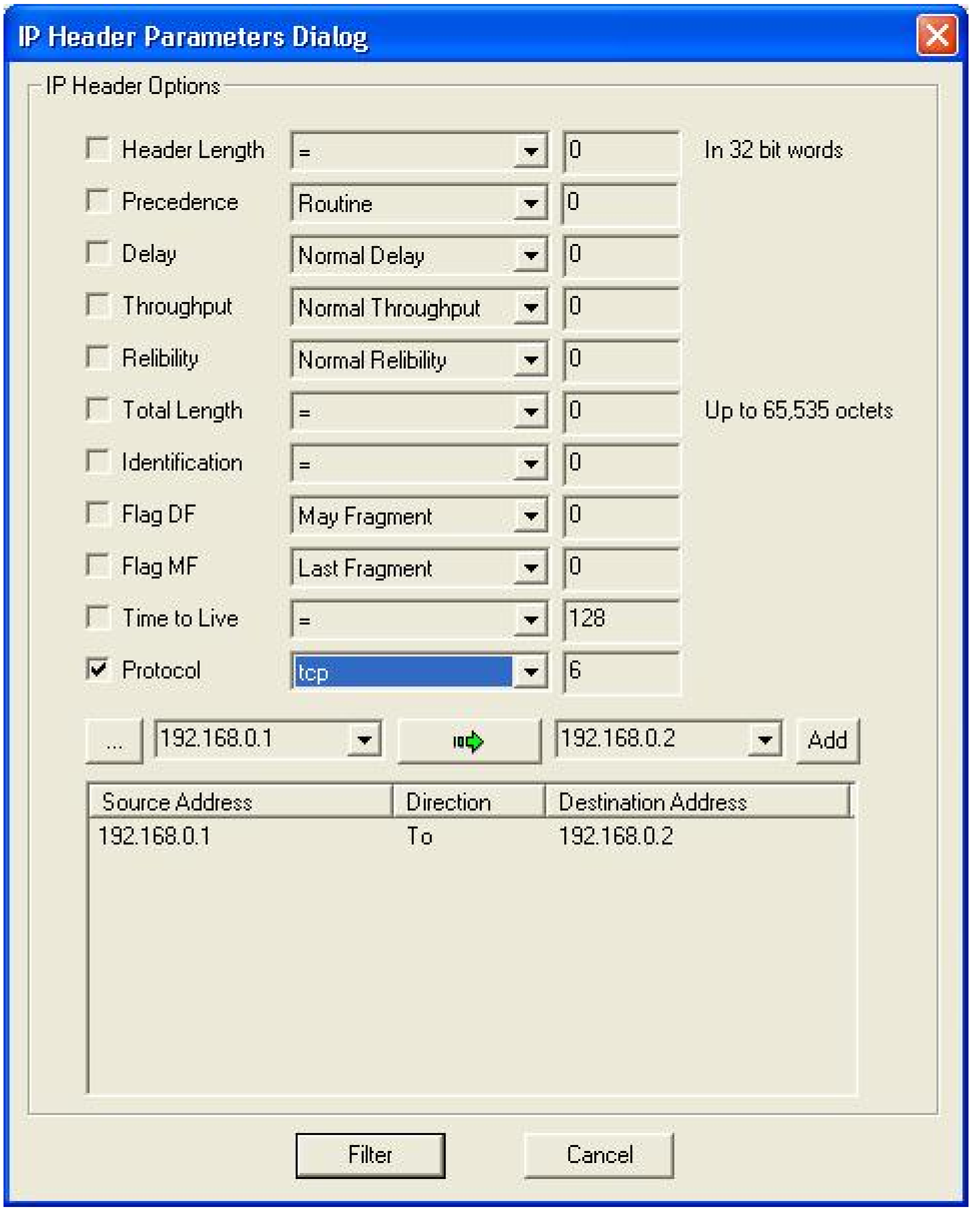
When Buffer Is Full

● Stop Capture ○ Wrap Capture Buffer

☑ Capture to numbered file:

Capture/capture.cap

This dialog allows to select the packet header to use for filtering. You can enable (disable) the following options: **IP**, **ICMP**, **UDP**, **TCP**, **NETBIOS-SSN**, **DATA**, **SIZE**.
Clicking on the check **IP** shows the **IP Header Parameters** dialog.
This dialog allows to enable (disable) and set values of IP header fields including **Header Length**, **Precedence**, **Delay**, **Throughput**, **Reliability**, **Total Length**, **Identification**, **Flag DF**, **Flag MF**, **Time to Live**, **Protocol**.
To add the source and destination addresses in the list click on the **Add** button**.**
To start filtering click on the **Filter** button .



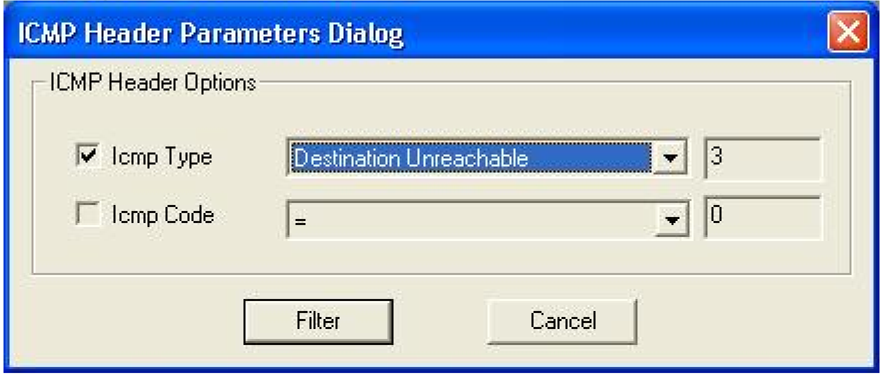
IP Header Options

□	Header Length	=	0	In 32 bit words
□	Precedence	Routine	0	
□	Delay	Normal Delay	0	
□	Throughput	Normal Throughput	0	
□	Relibility	Normal Relibility	0	
□	Total Length	=	0	Up to 65,535 octets
□	Identification	=	0	
□	Flag DF	May Fragment	0	
□	Flag MF	Last Fragment	0	
□	Time to Live	=	128	
☑	Protocol	tcp	6	

192.168.0.1 → 192.168.0.2

Source Address	Direction	Destination Address
192.168.0.1	To	192.168.0.2

Clicking on the check **ICMP** shows the **ICMP Header Parameters** dialog.



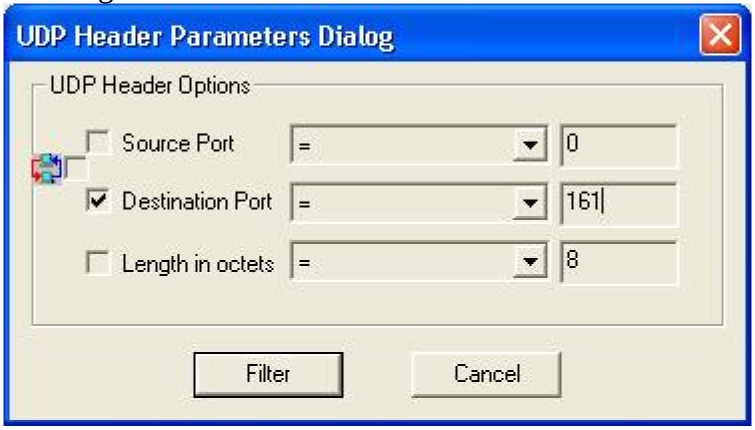
ICMP Header Options

☑	Icmp Type	Destination Unreachable	3
□	Icmp Code	=	0

This dialog allows to enable (disable) and set values to ICMP header fields including

ICMP Type and **ICMP Code**. To start filtering click on the **Filter** button.

Clicking on the check **UDP** shows the **UDP Header Parameters** dialog.



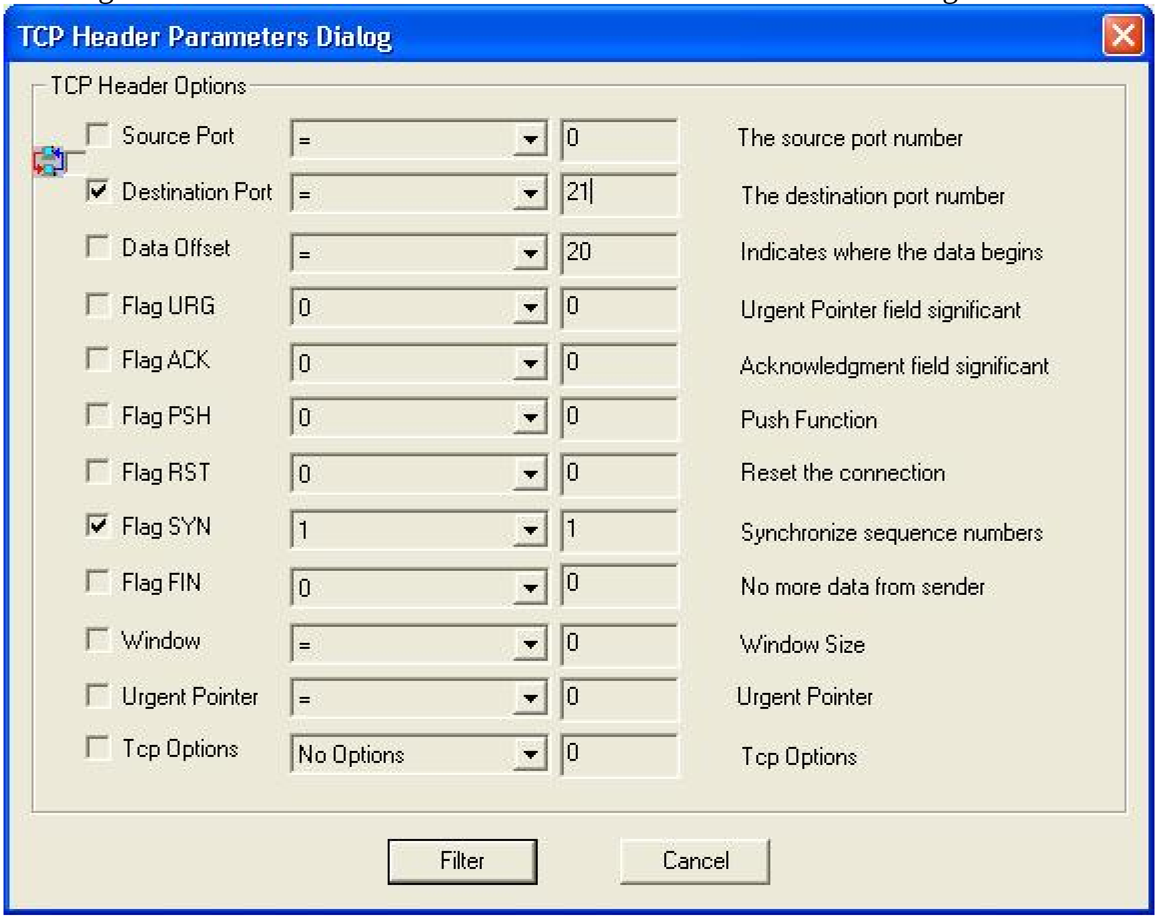
UDP Header Parameters Dialog

UDP Header Options

□ Source Port	=	0
☑ Destination Port	=	161
□ Length in octets	=	8

This dialog allows to enable (disable) and set values to UDP header fields including **Source Port, Destination Port**, **Length in octets.**
To start filtering click on the **Filter** button.

Clicking on the check **TCP** shows the **TCP Header Parameters** dialog.



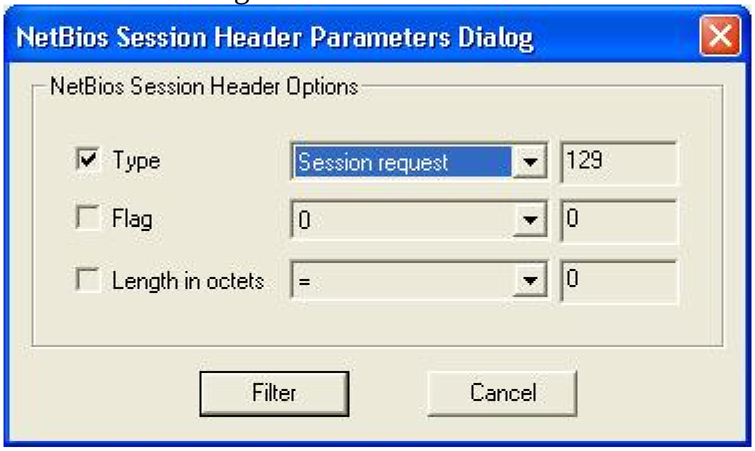
TCP Header Parameters Dialog

TCP Header Options

□ Source Port	=	0	The source port number
☑ Destination Port	=	21	The destination port number
□ Data Offset	=	20	Indicates where the data begins
□ Flag URG	0	0	Urgent Pointer field significant
□ Flag ACK	0	0	Acknowledgment field significant
□ Flag PSH	0	0	Push Function
□ Flag RST	0	0	Reset the connection
☑ Flag SYN	1	1	Synchronize sequence numbers
□ Flag FIN	0	0	No more data from sender
□ Window	=	0	Window Size
□ Urgent Pointer	=	0	Urgent Pointer
□ Tcp Options	No Options	0	Tcp Options

This dialog allows to enable (disable) and set values to TCP header fields including **Source Port, Destination Port**, **Data Offset, Flag URG, Flag ACK, Flag PSH, Flag RST, Flag SYN, Flag FYN, Window, Urgent Pointer, TCP Options.**
To start filtering click on the **Filter** button.

Clicking on the check **NET-BIOS SSN** shows the **NetBios Session Header Parameters** dialog.



NetBios Session Header Parameters Dialog

NetBios Session Header Options

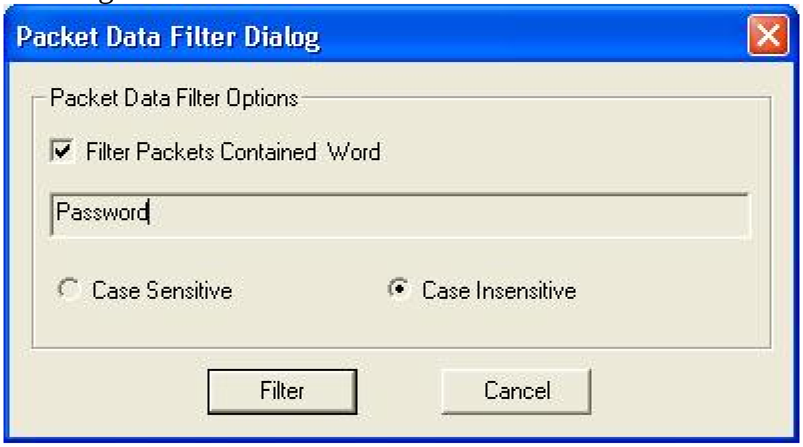
☑ Type Session request 129

□ Flag 0 0

□ Length in octets = 0

This dialog allows to enable (disable) and set values to NetBios Session header fields including **Type, Flag, Length in octets.**
To start filtering click on the **Filter** button.

Clicking on the check **DATA** shows the **Packet Data Filter** dialog.



Packet Data Filter Dialog

Packet Data Filter Options

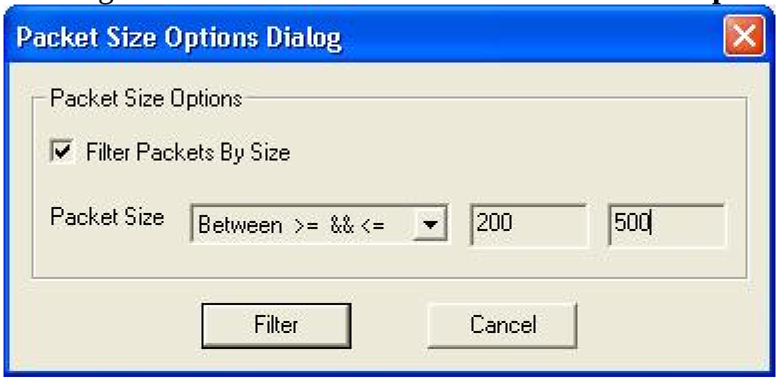
☑ Filter Packets Contained Word

Password

○ Case Sensitive ● Case Insensitive

This dialog allows to filter packets that contain the word specified in the editbox. To use this option enable the check **Filter Packets Contained Word** and enter the necessary word. You can use **Case Sensitive** or **Case Insensitive** search.
To start filtering click on the **Filter** button.

Clicking on the check **SIZE** shows the **Packet Size Options** dialog.



Packet Size Options Dialog

Packet Size Options

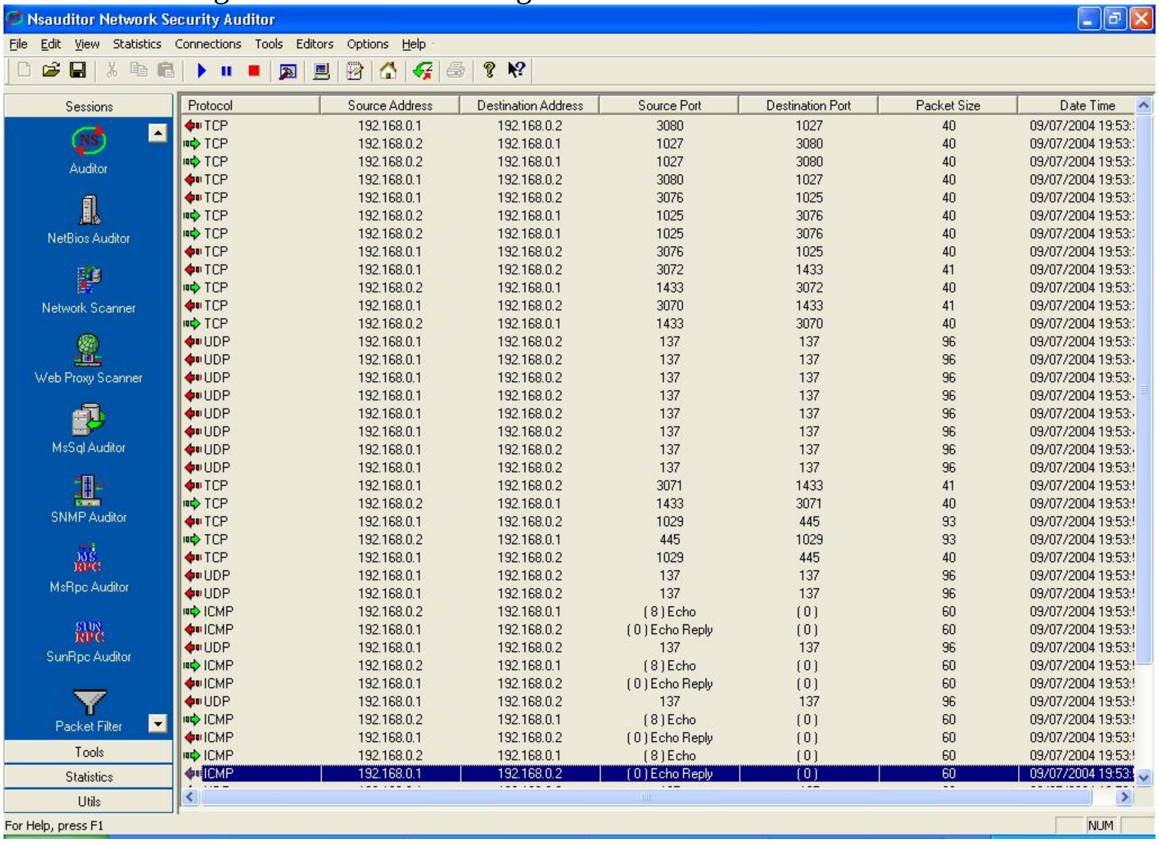
☑ Filter Packets By Size

Packet Size: Between >= && <= | 200 | 500

This dialog allows to **Filter Packets By Size** specified in the **Packet Size** field.
To start filtering click on the **Filter** button.

The option **Set Capture Schedule** will be available in later versions.
You can select the capture **Buffer Size** from the list. The minimal buffer size is 32KB and the maximal buffer size is 8MB.
To stop capturing when buffer is full select **Stop Capture.** And to wrap capture buffer select **Wrap Capture Buffer.**
To capture the data to numbered files enable the option Capture to numbered file.
Clicking on the **Browse** button allows you to change the selected file.
Click on the **Start** button to start filtering process.

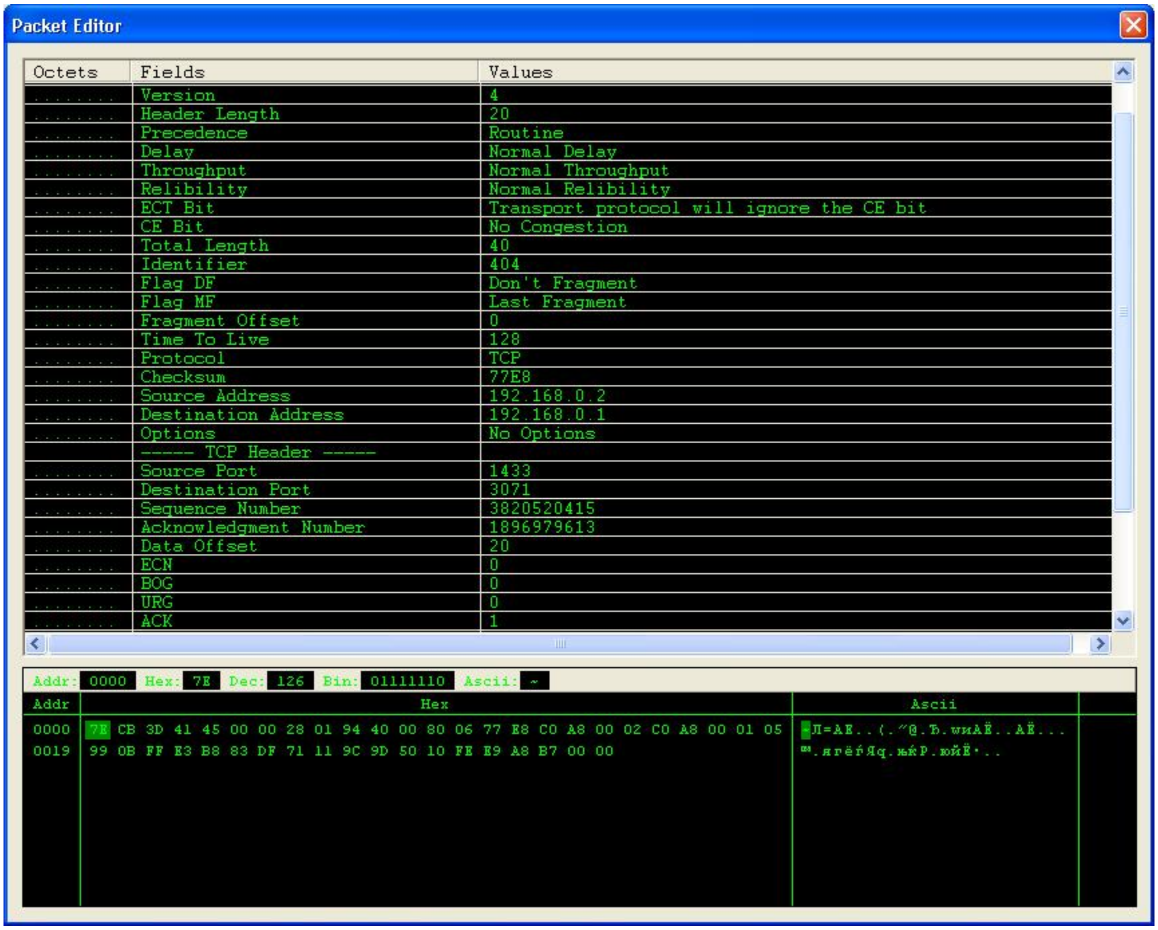
After the filtering is started the following view will be available:



Protocol	Source Address	Destination Address	Source Port	Destination Port	Packet Size	Date Time
TCP	192.168.0.1	192.168.0.2	3080	1027	40	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1027	3080	40	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1027	3080	40	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	3080	1027	40	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	3076	1025	40	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1025	3076	40	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1025	3076	40	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	3076	1025	40	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	3072	1433	41	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1433	3072	40	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	3070	1433	41	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1433	3070	40	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	3071	1433	41	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	1433	3071	40	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	1029	445	93	09/07/2004 19:53:
TCP	192.168.0.2	192.168.0.1	445	1029	93	09/07/2004 19:53:
TCP	192.168.0.1	192.168.0.2	1029	445	40	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
ICMP	192.168.0.2	192.168.0.1	(8) Echo	(0)	60	09/07/2004 19:53:
ICMP	192.168.0.1	192.168.0.2	(0) Echo Reply	(0)	60	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
ICMP	192.168.0.2	192.168.0.1	(8) Echo	(0)	60	09/07/2004 19:53:
ICMP	192.168.0.1	192.168.0.2	(0) Echo Reply	(0)	60	09/07/2004 19:53:
UDP	192.168.0.1	192.168.0.2	137	137	96	09/07/2004 19:53:
ICMP	192.168.0.2	192.168.0.1	(8) Echo	(0)	60	09/07/2004 19:53:
ICMP	192.168.0.1	192.168.0.2	(0) Echo Reply	(0)	60	09/07/2004 19:53:
ICMP	192.168.0.2	192.168.0.1	(8) Echo	(0)	60	09/07/2004 19:53:
ICMP	192.168.0.1	192.168.0.2	(0) Echo Reply	(0)	60	09/07/2004 19:53:

This view shows all the filtered packets with the following parameters: **Protocol, Source Address, Destination Address, Source Port, Destination Port, Packet Size, Date Time.**

Double-clicking on the row will open the packet editor which allows you to edit the packet header fields and data.



Packet Editor

Octets	Fields	Values
....	Version	4
....	Header Length	20
....	Precedence	Routine
....	Delay	Normal Delay
....	Throughput	Normal Throughput
....	Relibility	Normal Relibility
....	ECT Bit	Transport protocol will ignore the CE bit
....	CE Bit	No Congestion
....	Total Length	40
....	Identifier	404
....	Flag DF	Don't Fragment
....	Flag MF	Last Fragment
....	Fragment Offset	0
....	Time To Live	128
....	Protocol	TCP
....	Checksum	77E8
....	Source Address	192.168.0.2
....	Destination Address	192.168.0.1
....	Options	No Options
	----- TCP Header -----	
....	Source Port	1433
....	Destination Port	3071
....	Sequence Number	3820520415
....	Acknowledgment Number	1896979613
....	Data Offset	20
....	ECN	0
....	BOG	0
....	URG	0
....	ACK	1

Addr: 0000 Hex: 7E Dec: 126 Bin: 01111110 Ascii: ~

```
Addr                                 Hex                                             Ascii
0000  7E CB 3D 41 45 00 00 28 01 94 40 00 80 06 77 E8 C0 A8 00 02 C0 A8 00 01 05  ~Л=AE..(.″@.Ђ.wиAЁ..AЁ...
0019  99 0B FF E3 B8 83 DF 71 11 9C 9D 50 10 FE E9 A8 B7 00 00                    ™.яrёѓЯq.њќP.юйЁ·..
```