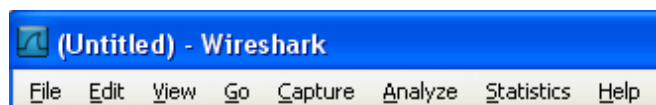


Wireshark_tutorial

1. Meniuri



Cele opt meniuri din partea superioara a platformei sunt pentru configurarea Wireshark:

- "File" Deschide si salveaza captura.
- "Edit" Gaseste si marcheaza pachete. Configureaza preferintele.
- "View" Configurarea vizualizarii platformei Wireshark.
- "Go" Navigheaza in datele capturii.
- "Capture" Seteaza filtrele capturii si o porneste/.
- "Analyze" Seteaza optiunile de analizare.
- "Statistics" Vizualizarea statisticilor Wireshark.
- "Help" Gasesti suport local sau online.

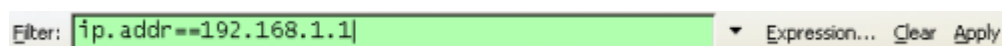
2. Scurtaturi



Scurtaturile folosite se afla chiar sub meniuri.

Informatiile pot fi obtinute cand se muta indicatorul mous-ului peste icoane.

3. Afisarea filtrelor



Pentru afisarea filtrelor se cauta in log-ul capturii.

Obs : A nu se confunda filtrele de captura cu cele de afisare. Detalii complete : verifica tutorialul filtrelor Wireshark.

4. Panoul cu lista de pachete

Time	Source	Destination	Port	Protocol	Info
4.371799	192.168.1.2	84.16.81.23	80	HTTP	GET /image/bu_logo.jpg HTTP/1.1
4.384927	84.16.81.23	192.168.1.2	3296	HTTP	HTTP/1.1 304 Not Modified
4.397701	84.16.81.23	192.168.1.2	3293	HTTP	HTTP/1.1 304 Not Modified
4.419743	192.168.1.2	84.16.81.23	80	HTTP	GET /image/carre.gif HTTP/1.1
4.419911	192.168.1.2	84.16.81.23	80	HTTP	GET /image/carre_bianc.gif HTTP/1.1
4.444310	84.16.81.23	192.168.1.2	3296	HTTP	HTTP/1.1 304 Not Modified
4.444744	192.168.1.2	84.16.81.23	80	HTTP	GET /lookxp/lookxoback.gif HTTP/1.1
4.457367	84.16.81.23	192.168.1.2	3293	HTTP	HTTP/1.1 304 Not Modified
4.474045	84.16.81.23	192.168.1.2	3296	TCP	[TCP segment of a reassembled PDU]
4.477516	84.16.81.23	192.168.1.2	3296	TCP	[TCP segment of a reassembled PDU]
185.	Cisco-L1_2a:fb:9b	3Com_9b:47:f7		ARP	who has 192.168.1.2? Tell 192.168.1.1
185.	3Com_9b:47:f7	cisco-L1_2a:fb:9b		ARP	192.168.1.2 is at 00:04:75:9b:47:f7

- Panoul cu lista de pachete afiseaza toate pachetele capstrate. Poti afla informatii ca sursa si destinatia adreselor MAC/IP, numarul portului TCP/UDP, protocolul sau continutul pachetelor.
- Daca un pachet OSI strat 2 este capturat vei vedea adresa MAC in coloana dedicata sursei si destinatiei, si bine inteles, nimic in coloana dedicata portului.
- Daca un pachet OSI strat 3 sau mai mare este capturat se va vedea adresa IP in coloana dedicata sursei si destinatiei. Coloana dedicata portului va avea continut numai daca pachetul este de strat 4 sau mai mare.

- Se pot adauga/sterge coloane sau schimba culori dupa cum urmeaza: Edit menu -> Preferences

5. Panoul cu detaliile despre pachete

Time	Source	Destination	Port	Protocol	Info
19.3	192.168.1.2	84.16.81.23	80	HTTP	GET /wifreshark_use.php HTTP/1.1
19.3	192.168.1.2	84.16.81.23	80	HTTP	GET /menu.js HTTP/1.1
19.4	84.16.81.23	192.168.1.2	1600	HTTP	HTTP/1.1 304 Not Modified
19.4	192.168.1.2	84.16.81.23	80	HTTP	GET /lookxp.css HTTP/1.1
19.4	84.16.81.23	192.168.1.2	1601	HTTP	HTTP/1.1 304 Not Modified

Selected Packet

OSI Layer 2 Ethernet II, Src: 3Com_9b:47:f7 (00:04:75:9b:47:f7), Dst: Cisco-L1_2a:fb:9b (00:18:39:2a:fb:9b)

OSI Layer 3 Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 84.16.81.23 (84.16.81.23)

OSI Layer 4 Transmission Control Protocol, Src Port: 1601 (1601), Dst Port: http (80), Seq: 1, Ack: 1, Len: 719

OSI Layer 7 Hypertext Transfer Protocol

- Panoul cu informatii despre pachet va oferi informatii mai multe despre pachetul selectat din panoul cu lista de pachete.
- Informatiile afisate pe fiecare strat OSI pot fi expandate si pliate. In captura de ecran care urmeaza sunt informatii despre HTTP expandate.
- Panoul cu informatii despre pachet va oferi informatii mai multe despre pachetul selectat din panoul cu lista de pachete.
- Informatiile afisate pe fiecare strat OSI pot fi expandate si pliate. In captura de ecran care urmeaza sunt informatii despre HTTP expandate.

```

# Frame 152 (773 bytes on wire, 773 bytes captured)
# Ethernet II, Src: 3Com_9b:47:f7 (00:04:75:9b:47:f7), Dst: Cisco-L1_2a:fb:9b (00:18:39:2a:fb:9b)
# Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 84.16.81.23 (84.16.81.23)
# Transmission Control Protocol, Src Port: 1601 (1601), Dst Port: http (80), Seq: 1, Ack: 1, Len: 719
# Hypertext Transfer Protocol
# GET /lookxp.css HTTP/1.1
Accept: */*
Referer: http://www.openmaniak.com/wifreshark_use.php/v/n
Accept-Language: fr-ch/v/n
Accept-Encoding: gzip, deflate/v/n
If-Modified-Since: Tue, 27 Nov 2007 18:01:18 GMT/v/n
If-None-Match: "2002c3-2590-474c5c8e"/v/n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727)/v/n
Host: www.openmaniak.com/v/n
Connection: keep-alive/v/n
Cookie: __utmz=196743026.110707899.1188047094.1196949320.1196949300.96; __utms=196743026.1196949300.96.17.utmcc
/v/n

```

6. Panoul de analiza

```

# Frame 152 (773 bytes on wire, 773 bytes captured)
# Ethernet II, Src: 3Com_9b:47:f7 (00:04:75:9b:47:f7), Dst: Cisco-L1_2a:fb:9b (00:18:39:2a:fb:9b)
# Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 84.16.81.23 (84.16.81.23)
# Transmission Control Protocol, Src Port: 1601 (1601), Dst Port: http (80), Seq: 1, Ack: 1, Len: 719
Source port: 1601 (1601)
Destination port: http (80)
0010 02 f7 82 ae 40 00 80 06 0e 81 c0 a8 01 02 54 10 .....T.
0020 51 17 06 41 00 38 69 66 8c 75 94 d2 db f6 50 18 Q..A...f..U...P.
0030 ff ff 69 bb 00 00 47 45 54 20 2f 6c 6f 6f 6b 78 ..1...GE T /lookx
0040 70 2e 63 73 73 20 48 54 54 50 2f 31 2e 31 0d 0a p.CSS HT TP/1.1.
0050 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 32 65 66 Accept: */*..Ref

```

- Panoul de analiza care se mai numeste "panoul pachetelor biti" in Wireshark, afiseaza aceleasi informatii furnizate si de panoul cu detalii despre pachete dar in modul hexazecimal.
- In exemplul care urmeaza s-a selectat portul TCP 80 in panoul cu detalii despre pachete si echivalentul lui in hexazecimal a aparut automat in panoul de analiza 0050.

7. Diverse

Network interface	Capture state	Capture file	Capture size	P	D	M
3Com EtherLink PCI (Microsoft's Packet Scheduler)	<live capture in progress>	File: C:\DOCUMENTS\1\admin\LOCALS~1\Temp\ether\000a01768 9677 KB		P: 34239	D: 3481	M: 0

In josul platformei pot fi gasite urmatoarele informatii:

- Placa de retea folosita in captura.
- Daca captura este pornita sau oprita.
- Unde sunt stocate datele capturii pe harddisk.
- marimea capturii.
- numarul pachetelor. (P)
- numarul pachetelor afisate. (D) (pachetele care se potriveau cu filtrul de afisare)
- numarul pachetelor marcate. (M)

- **Obs :** Este extrem de usoara instalarea si lansarea in executie a Wireshark-ului in vederea analizarii retelei.

O problema foarte comuna apare cand se lanseaza Wireshark cu setarile initiale; va aparea pe ecran o sumedenie de informatii in care, este posibil, sa nu existe si informatia dorita.

- **Filtrul de captura** este folosit pentru a limita marimea de date capturate pentru a preveni generarea de loguri foarte mari.
- **Filtrul de afisare** este mult mai puternic (si complex); permite sa cauti exact datele pe care le doresti.

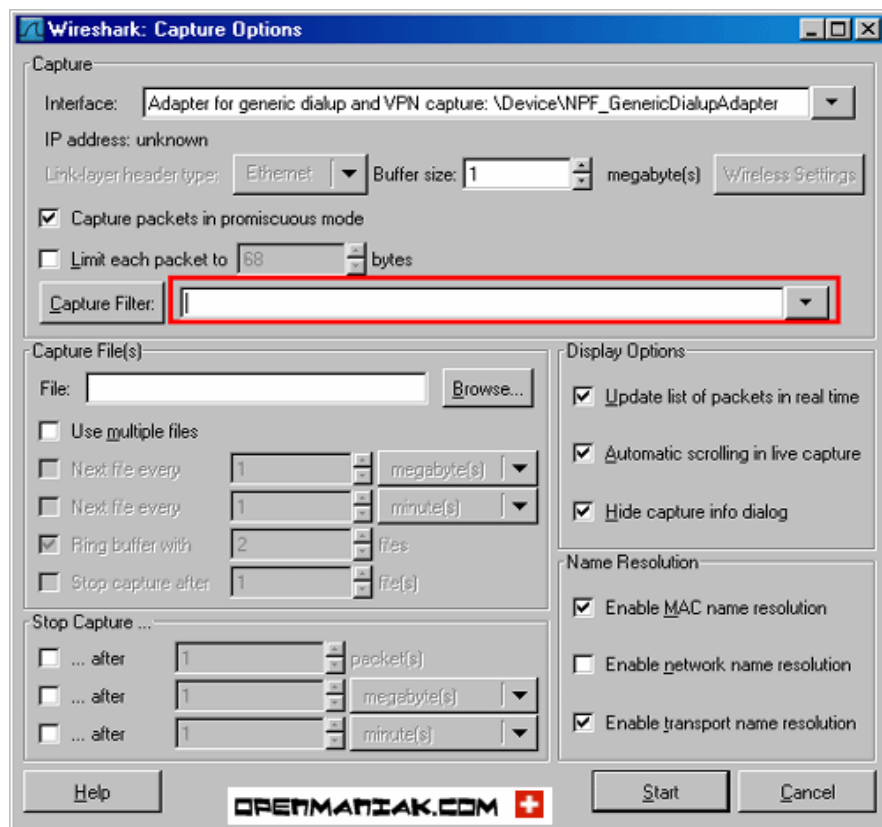
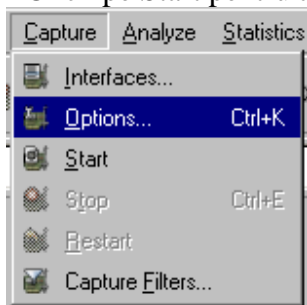
Sintaxa celor doua tipuri de filtre este complet diferita.

1. FILTRELE DE CAPTURA

Sintaxa filtrelor de captura este asemanatoare cu cea folosita de biblioteca Libpcap(Linux) sau Winpcap(Windows), TCPdump. Filtrul de captura trebuie setat inainte de a porni captura, in cazul filtrelor de afisare nu este nevoie acestea putand fi setate si in timpul capturii.

Pasii pentru a configura filtrele de captura sunt:

- select capture -> options.
- Completeaza campul "capture filter" sau click pe butonul "capture filter" pentru a oferi numele filtrului tau care va fi folosit pentru capturile urmatoare.
- Click pe Start pentru a captura date.



Syntax:	Protocol	Directie	Host(uri)	Valoare	Operatii logice	Alte expresii
Example:	tcp	dst	10.1.1.1	80	and	tcp dst 10.2.2.2 3128

- **Protocol:**

Valori: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

Daca nu este specificat nici un protocol toate acestea vor fi folosite.

- **Directie:**

Valori: src, dst, src and dst, src or dst

Daca nu este specificata nici o sursa sau destinatie sunt aplicate cuvintele "src or dst" .

De exemplu, "host 10.2.2.2" este echivalent cu "src or dst host 10.2.2.2". <BR

- **Host(uri):**

Valori: net, port, host, portrange.

Daca nici un host(uri) nu este specificat va fi folosit cuvantul "host" .

De exemplu, "src 10.1.1.1" este echivalent cu "src host 10.1.1.1".

- **Operatii logice:**

Valori: not, and, or.

Negatie ("not") are cea mai mare precedenta. Alternarea ("or") si concatenarea ("and") au o precedenta egala si asociata de la stanga la dreapta.

De exemplu,

"not tcp port 3128 and tcp port 23" este echivalent cu "(not tcp port 3128) and tcp port 23".

"not tcp port 3128 and tcp port 23" NU este echivalent cu "not (tcp port 3128 and tcp port 23)".

Exemple:

tcp dst port 3128

Afiseaza pachetele cu destinatia TCP portul 3128.

ip src host 10.1.1.1

Afiseaza pachetele cu IP-ul sursei egal cu 10.1.1.1.

host 10.1.2.3

Afiseaza pachetele cu IP-ul sursei sau destinatiei egal cu 10.1.1.1.

src portrange 2000-2500

Afiseaza pachetele cu sursa UDP sau TCP si cu portul din rangul 2000-2500.

not icmp

Afiseaza orice in afara de pachetele icmp. (icmp este de obicei folosit de unele ping)

src host 10.7.2.12 and not dst net 10.200.0.0/16

Afiseaza pachetele cu adresa IP a sursei egala cu 10.7.2.12 si in acelasi timp care nu sunt egale cu adresa IP 10.200.0.0/16.

(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000 and dst net 10.0.0.0/8

Afiseaza pachetele cu adresa IP a sursei 10.4.1.12 sau sursa retelei 10.6.0.0/16, acest rezultat este concatenat cu pachetele care au destinatia TCP si rangul portului intre 200 la 1000 precum si IP-ul retelei 10.0.0.0/8.

Obs:

semnul backslash "\" este folosit cand un cuvant este folosit drept valoare.

"ether proto \ip" (este echivalent cu "ip").

Acesta va avea ca tinta protocoalele IP.

"ip proto \icmp" (este echivalent cu "icmp").

Acesta va avea ca tinta pachetele icmp care sunt folosite de obicei de utilitarul ping.

Cuvintele "multicast" si "broadcast" pot fi de asemenea folosite dupa "ip" sau "ether".

"no broadcast" este folositor cand vrei sa excludi cererile broadcast.

2. FILTRELE DE AFISARE:

Filtrele de afisare sunt folosite pentru cautarea in datele capturate cu un filtru de captura.

Capabilitatile lui de cautare si mai extinse nu fac necesara restartarea capturii cand doresti sa schimbi filtrul.

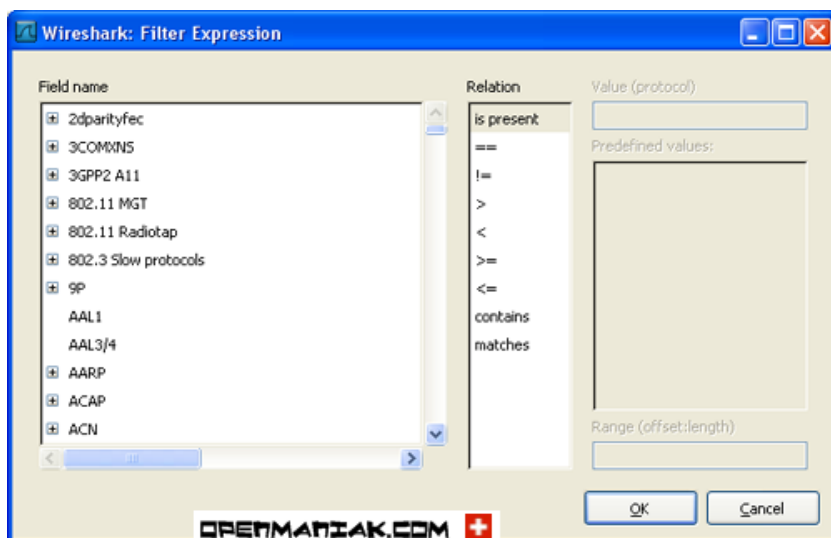
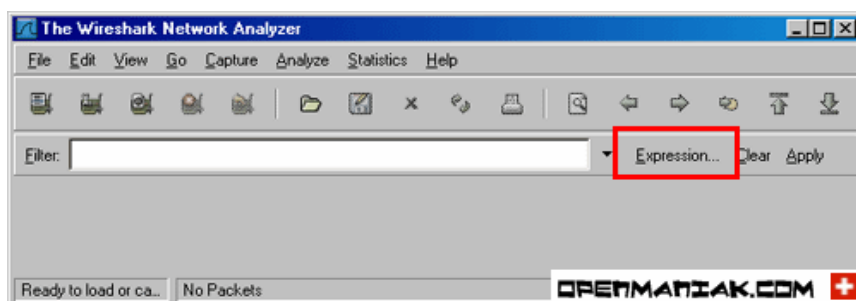
Syntax:	Protocol	.	Sir 1	.	Sir 2	Operator de comparare	Valoare	Operatii logice	Alte expresii
Example:	ftp		passive		ip	==	10.2.3.4	xor	icmp.type

- **Protocol:**

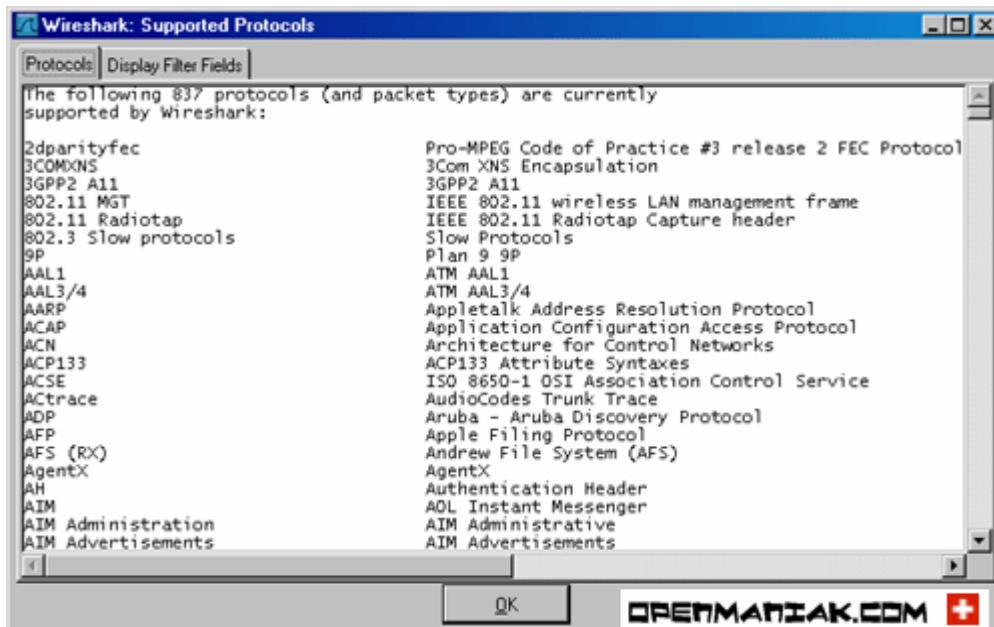
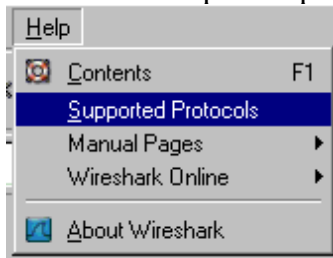
Un numar mare de protocoale, localizate intre straturile doi si sapte ale modelului OSI, sunt disponibile.

Le poti vedea cand apesi pe butonul "Expression..." din ecranul principal.

Cateva exemple ar fi: IP,TCP,DNS,SSH



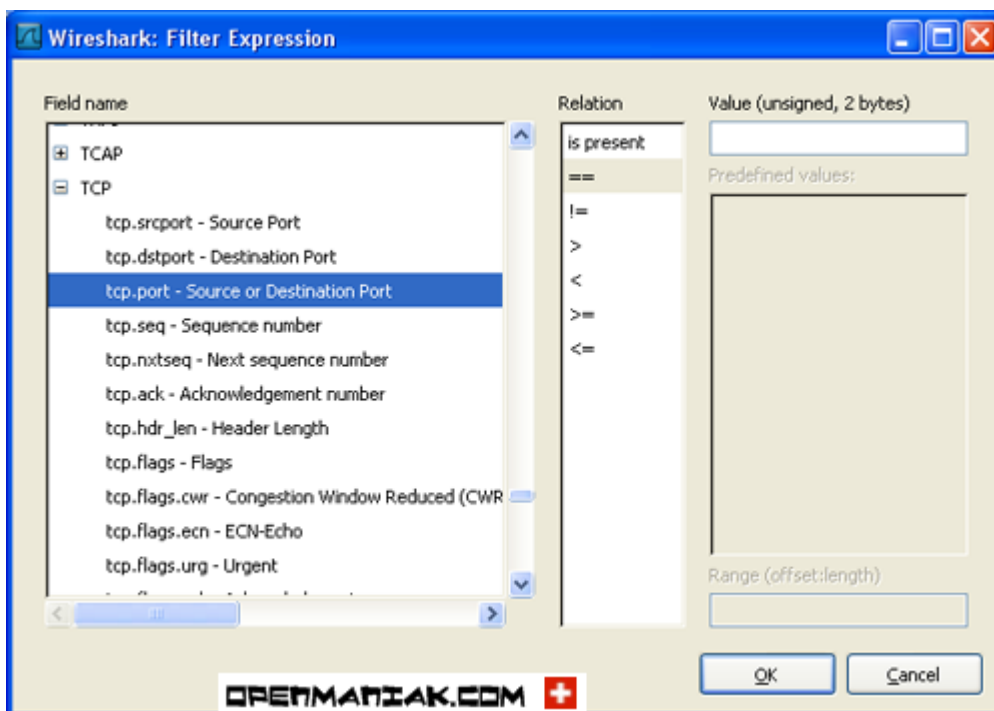
Protocoalele suportate precum si o mica descriere poate fi consultata dupa cum este indicat mai jos:



- Sir1, Sir2 (Optiuni suplimentare):

Categorii sub protocol in protocol.

Pentru a le gasi, uita-te dupa un protocol si apasa click pe caracterul "+".



- **Operatori de comparare::**

Sunt disponibili sase operatori:

Formatul englezesc:	formatul asemanator cu Ct:	Semnificatie:
eq	==	Egal
ne	!=	Diferit
gt	>	Mai mare ca
lt	<	Mai mic ca
ge	>=	Mai mare sau egal
le	<=	Mai mic sau egal

- **Operatii logice::**

Formatul englezesc:	formatul asemanator cu Ct:	Semnificatie:
and	&&	SI logic
or		SAU logic
xor	^^	XOR logic
not	!	NU logic

Expresia logica "XOR" este folosita pentru o alternare exclusiva. Cand este folosita intre doua conditii intr-un filtru, rezultatul va fi afisat pe ecran doar daca una din cele doua conditii este adevarata nu ca la expresia "OR".

Sa luam un exemplu cu urmatorul filtru de afisare:

"tcp.dstport 80 xor tcp.dstport 1025"

Doar pachetele cu destinatia TCP si portul 80 sau TCP si portul sursa 1025(dar nu amandoua!) vor fi afisate pe ecran ca rezultate.

Exemplu:

snmp || dns || icmp Afiseaza traficul SNMP sau DNS sau ICMP.

ip.addr == 10.1.1.1

Afiseaza pachetele cu adresa IP a sursrsei sau destinatiei egala cu 10.1.1.1.

ip.src != 10.1.2.3 or ip.dst != 10.4.5.6

Afiseaza pachetele cu IP-ul sursei diferit de 10.1.2.3 sau cu IP-ul destinatiei diferit de 10.4.5.6

Cu alte cuvinte, pachetele afisate vor avea:

Adresa IP a sursei: orice dar 10.1.2.3 , IP-ul destinatiei: orice

si

IP-ul sursei:orice,IP-ul destinatiei:orice dar 10.4.5.6

ip.src != 10.1.2.3 and ip.dst != 10.4.5.6

Afiseaza pachetele cu IP-ul sursei diferit de 10.1.2.3 si in acelasi timp cu IP-ul destinatiei diferit de 10.4.5.6

Cu alte cuvinte, pachetele afisate vor avea:

Adresa IP a sursei: orice dar 10.1.2.3 si IP-ul destinatiei: orice dar 10.3.4.5.6

tcp.port == 25 Afiseaza pachetele sursei TCP sau portul de destinatie 25.

tcp.dstport == 25 Afiseaza pachetele cu destinatia TCP si portul 25.

tcp.flags Afiseaza pachetele TCP care au steaguri.

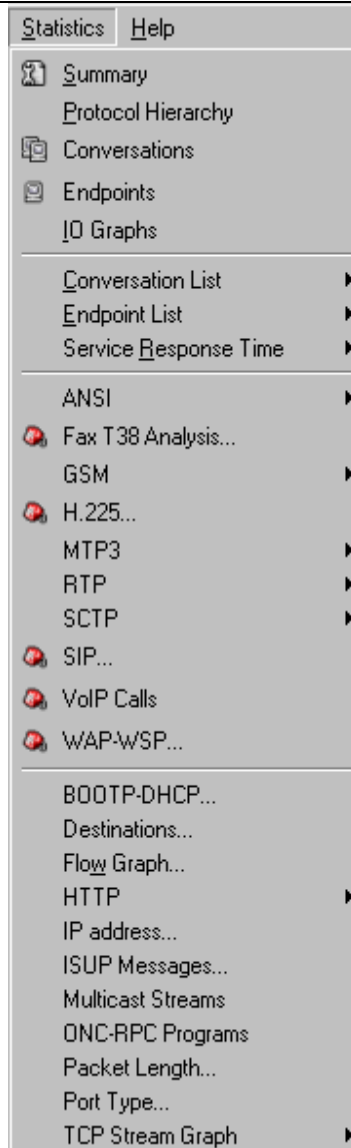
tcp.flags.syn == 0x02 Afiseaza pachetele TCP cu steagul SYN.

Daca sintaxa filtrului este corecta va fi subliniata cu verde, altfel, daca exista vre-o eroare va fi subliniata cu rosu.

Filter: <code>tcp.port == 100 </code>	Sintaxa corecta
Filter: <code>tcp.port = 100 </code>	Sintaxa gresita

- **Wireshark vine cu o multime de statistici cu care pot fi consultate apasand pe campul "statistics" din partea superioara a ecranului.**

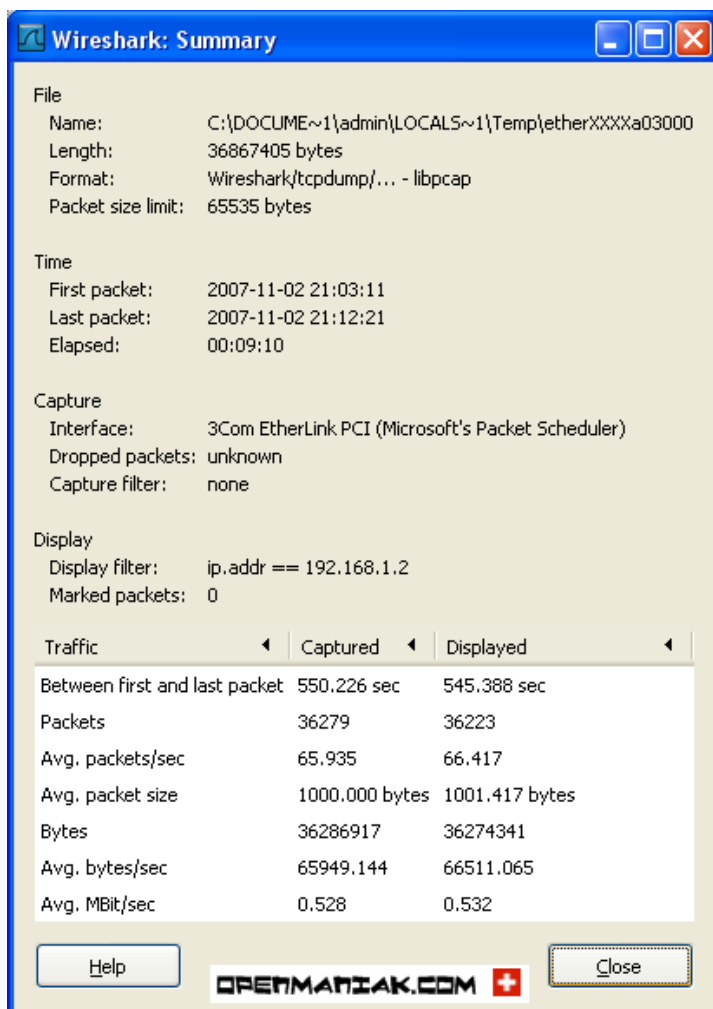
In dreapta sunt prezentate cateva exemple de statistici:



- **Summary**

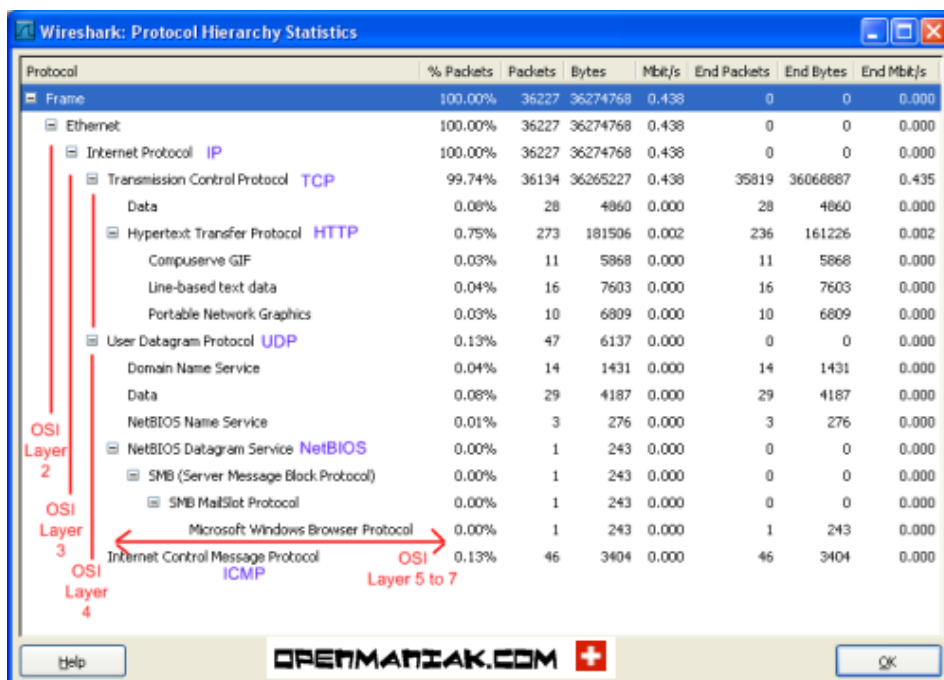
Informatiile globale, de baza care sunt disponibile in fereastra sunt:

- Proprietatile fisierului de captura.
- Timpul de captura.
- Informatii despre filtrul de captura.
- Informatii despre filtrul de afisare.



- **Protocol Hierarchy**

Ierarhia protocolului afiseaza o disecare pe straturi OSI a datelor afisate.

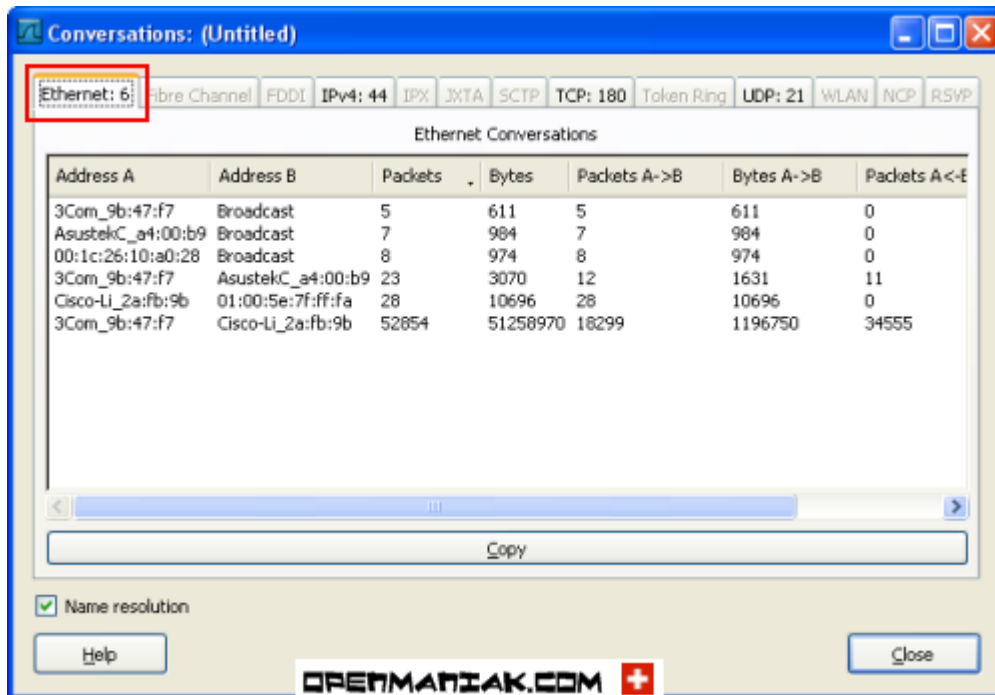


- **Conversations**

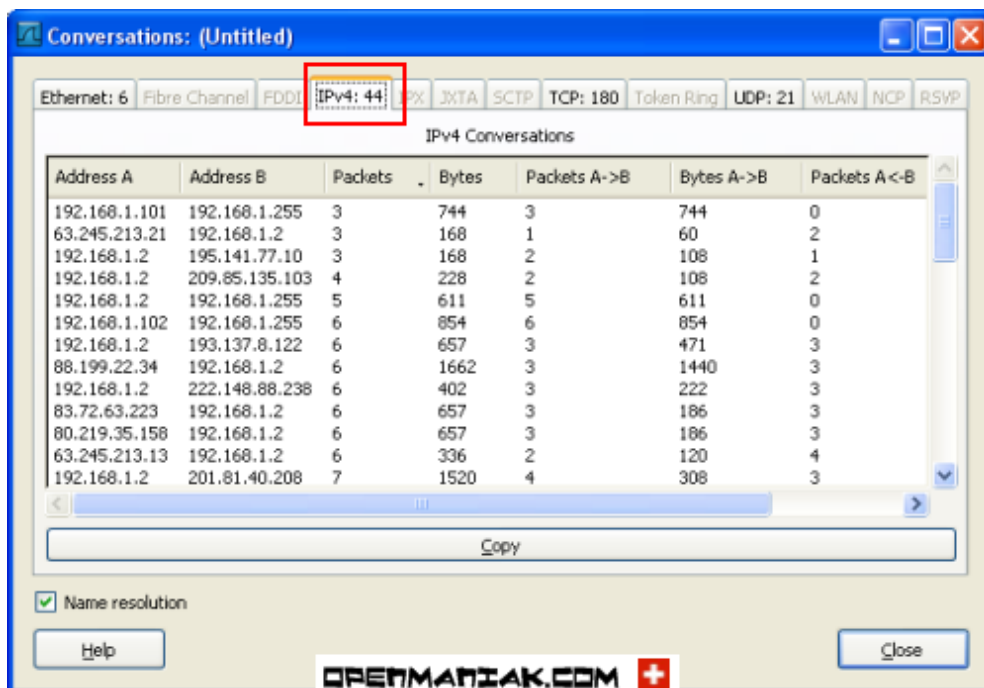
Daca se foloseste suita de aplicatii sau protocoale TCP/IP , ar trebui sa gasesti patru tab-uri active pentru

conversatiile Ethernet, IP, TCP si UDP. O "conversatie" reprezinta traficul dintre doua host-uri. Numarul din tab care precedeaza protocolul indica numarul conversatiilor. De exemplu: "Ethernet:6".

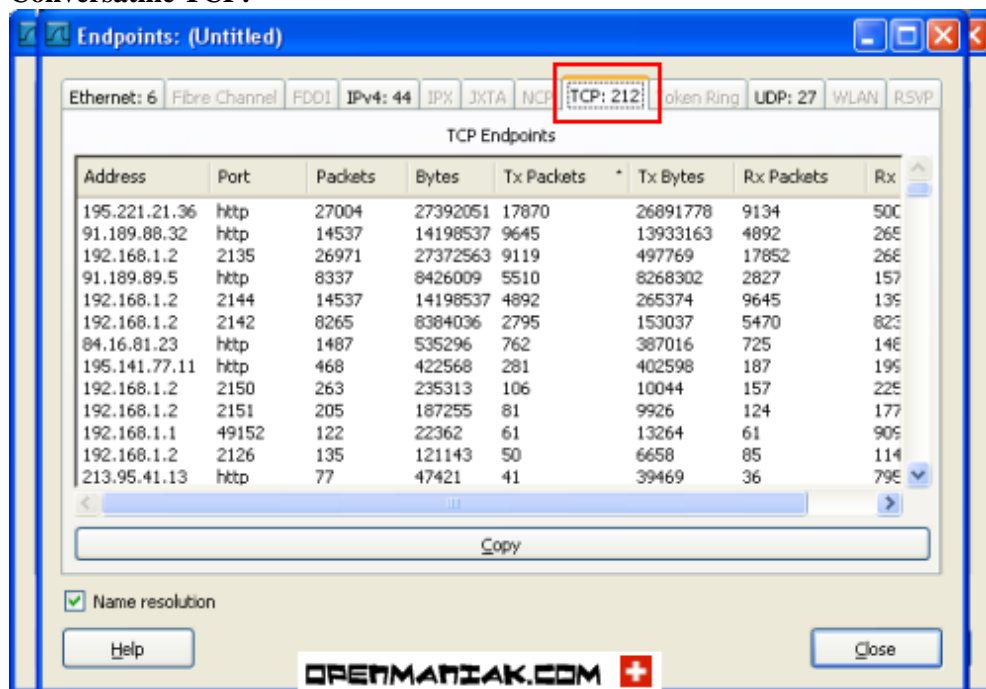
- Conversatiile Ethernet:



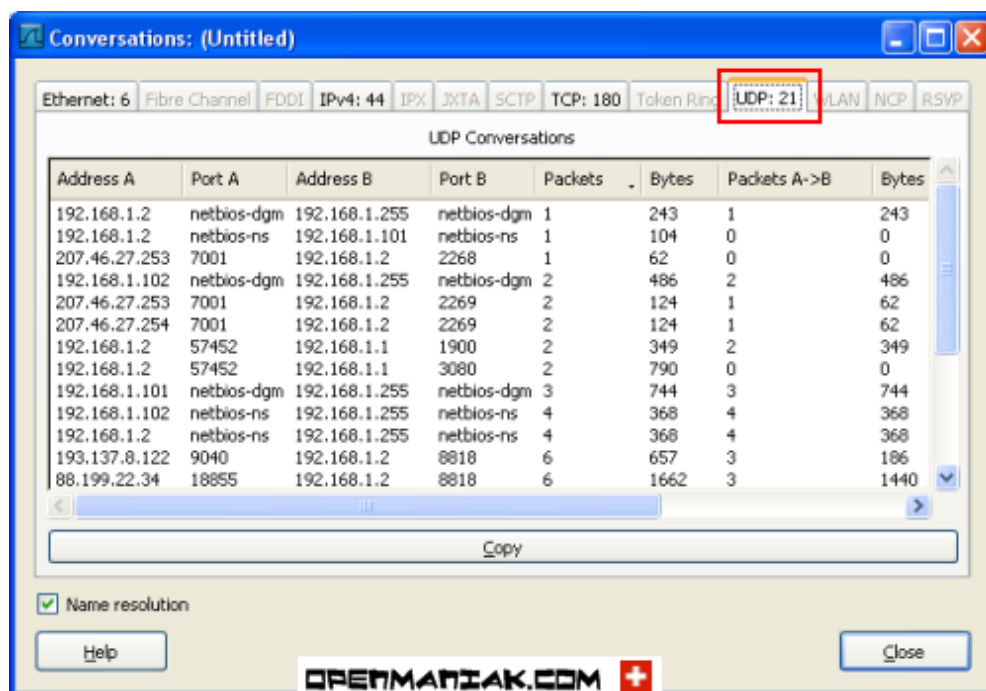
- Conversatiile IP:



Conversatiile TCP:



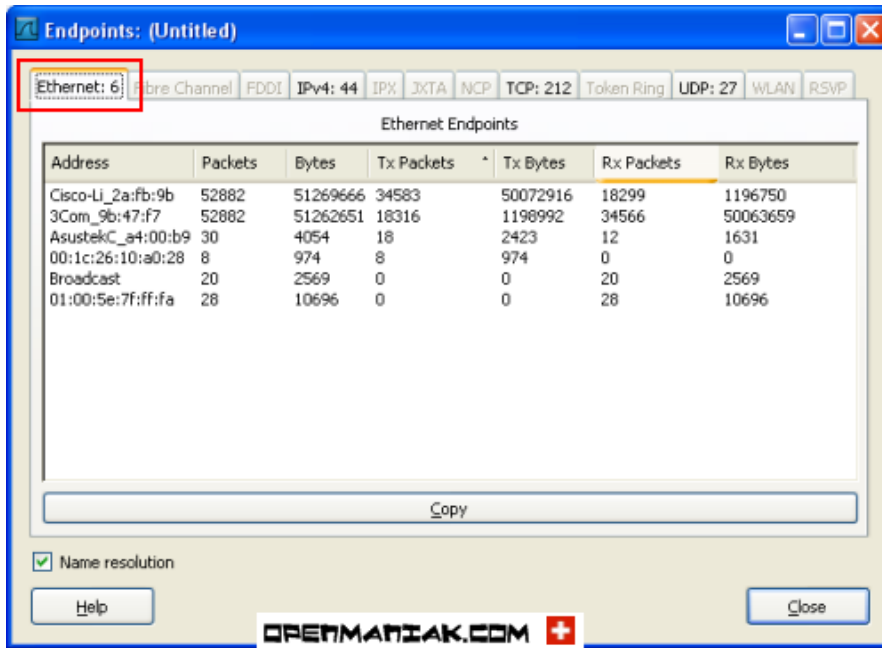
Conversatiile UDP:



- **Endpoints**

Punctele de sfarsit vin cu statistice despre date primite si transmise de pe o masina per. Numarul care preceda protocolul indica numarul de puncte de sfarsit. De exemplu: "Ethernet:6".

- **Punctele de sfarsit Ethernet:**



Endpoints: (Untitled)

Ethernet: 6 | Fibre Channel | FDDI | **IPv4: 44** | IPX | JXTA | NCP | TCP: 212 | Token Ring | UDP: 27 | WLAN | RSVP

Ethernet Endpoints

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Cisco-Li_2a:fb:9b	52882	51269666	34583	50072916	18299	1196750
3Com_9b:47:f7	52882	51262651	18316	1198992	34566	50063659
AsustekC_a4:00:b9	30	4054	18	2423	12	1631
00:1c:26:10:a0:28	8	974	8	974	0	0
Broadcast	20	2569	0	0	20	2569
01:00:5e:7f:ff:fa	28	10696	0	0	28	10696

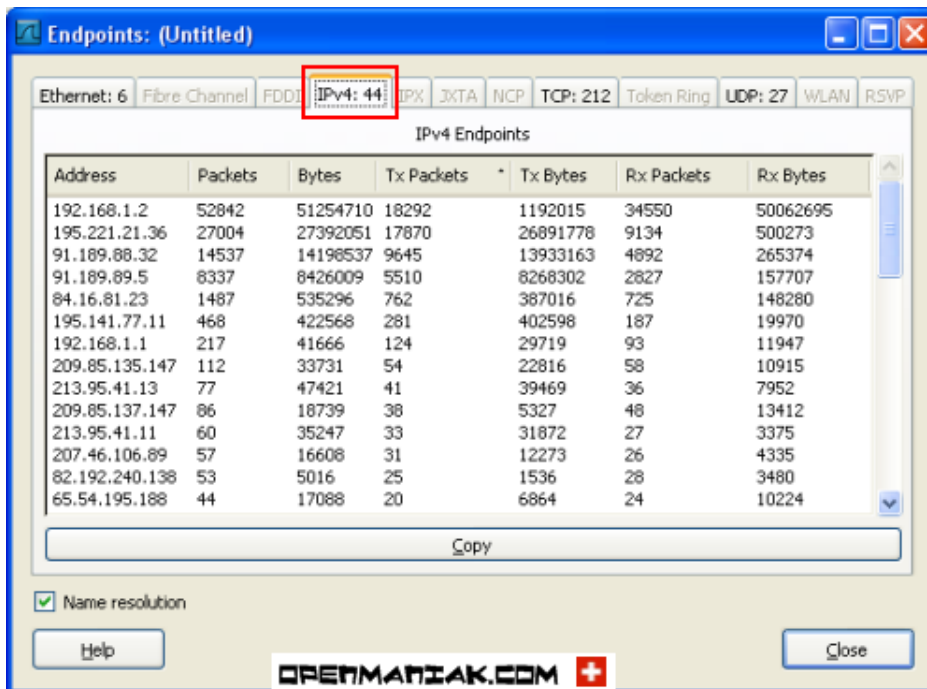
Copy

☒ Name resolution

Help Close

OPENMANIAK.COM

- **Punctele de sfarsit IP:**



Endpoints: (Untitled)

Ethernet: 6 | Fibre Channel | FDDI | **IPv4: 44** | IPX | JXTA | NCP | TCP: 212 | Token Ring | UDP: 27 | WLAN | RSVP

IPv4 Endpoints

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.1.2	52842	51254710	18292	1192015	34550	50062695
195.221.21.36	27004	27392051	17870	26891778	9134	500273
91.189.88.32	14537	14198537	9645	13933163	4892	265374
91.189.89.5	8337	8426009	5510	8268302	2827	157707
84.16.81.23	1487	535296	762	387016	725	148280
195.141.77.11	468	422568	281	402598	187	19970
192.168.1.1	217	41666	124	29719	93	11947
209.85.135.147	112	33731	54	22816	58	10915
213.95.41.13	77	47421	41	39469	36	7952
209.85.137.147	86	18739	38	5327	48	13412
213.95.41.11	60	35247	33	31872	27	3375
207.46.106.89	57	16608	31	12273	26	4335
82.192.240.138	53	5016	25	1536	28	3480
65.54.195.188	44	17088	20	6864	24	10224

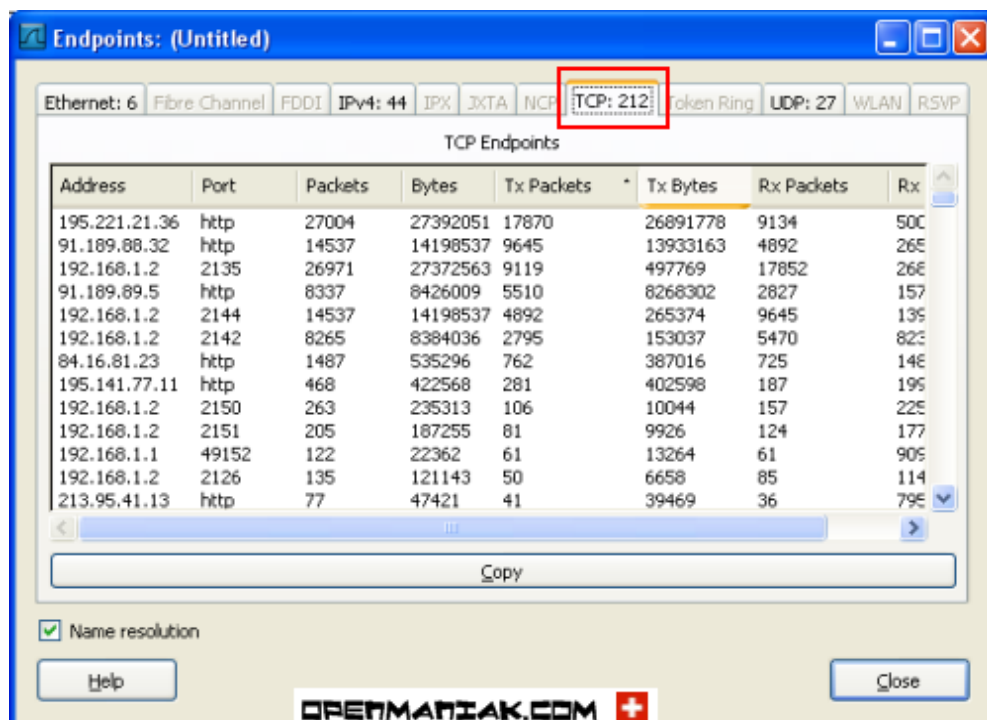
Copy

☒ Name resolution

Help Close

OPENMANIAK.COM

- **Punctele de sfarsit TCP:**



Endpoints: (Untitled)

Ethernet: 6 Fibre Channel FDDI IPv4: 44 IPX JXTA NCP **TCP: 212** Token Ring UDP: 27 WLAN RSVP

TCP Endpoints

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx
195.221.21.36	http	27004	27392051	17870	26891778	9134	500
91.189.88.32	http	14537	14198537	9645	13933163	4892	265
192.168.1.2	2135	26971	27372563	9119	497769	17852	265
91.189.89.5	http	8337	8426009	5510	8268302	2827	157
192.168.1.2	2144	14537	14198537	4892	265374	9645	135
192.168.1.2	2142	8265	8384036	2795	153037	5470	823
84.16.81.23	http	1487	535296	762	387016	725	148
195.141.77.11	http	468	422568	281	402598	187	195
192.168.1.2	2150	263	235313	106	10044	157	225
192.168.1.2	2151	205	187255	81	9926	124	177
192.168.1.1	49152	122	22362	61	13264	61	905
192.168.1.2	2126	135	121143	50	6658	85	114
213.95.41.13	http	77	47421	41	39469	36	795

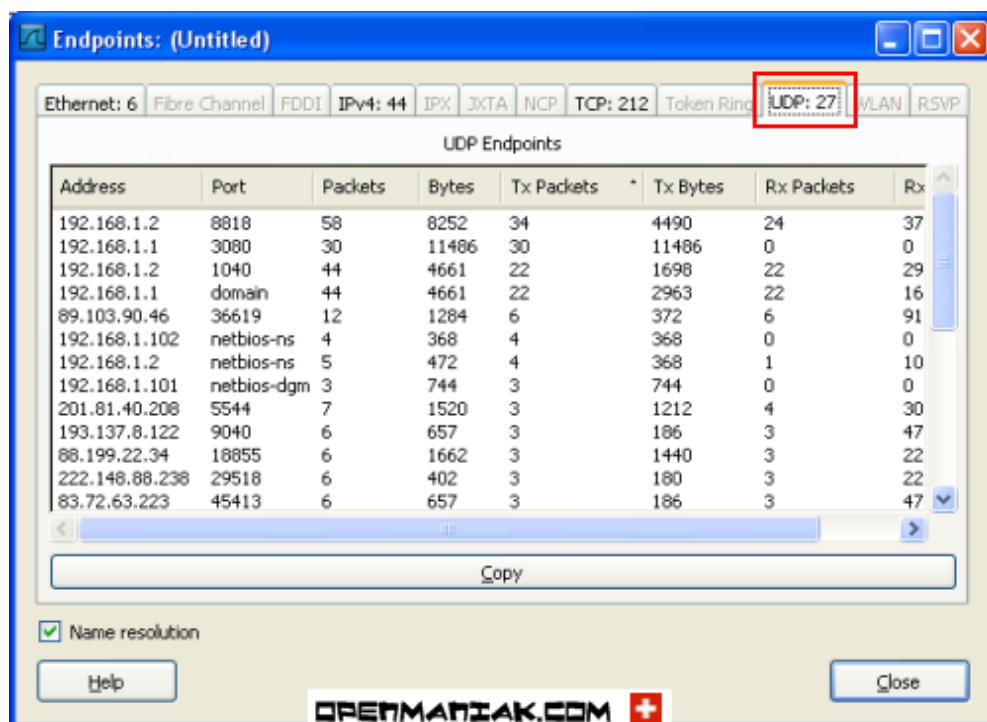
Copy

☒ Name resolution

Help Close

OPENMANIAK.COM

- **Punctele de sfarsit UDP :**



Endpoints: (Untitled)

Ethernet: 6 Fibre Channel FDDI IPv4: 44 IPX JXTA NCP TCP: 212 Token Ring **UDP: 27** WLAN RSVP

UDP Endpoints

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx
192.168.1.2	8818	58	8252	34	4490	24	37
192.168.1.1	3080	30	11486	30	11486	0	0
192.168.1.2	1040	44	4661	22	1698	22	29
192.168.1.1	domain	44	4661	22	2963	22	16
89.103.90.46	36619	12	1284	6	372	6	91
192.168.1.102	netbios-ns	4	368	4	368	0	0
192.168.1.2	netbios-ns	5	472	4	368	1	10
192.168.1.101	netbios-dgm	3	744	3	744	0	0
201.81.40.208	5544	7	1520	3	1212	4	30
193.137.8.122	9040	6	657	3	186	3	47
88.199.22.34	18855	6	1662	3	1440	3	22
222.148.88.238	29518	6	402	3	180	3	22
83.72.63.223	45413	6	657	3	186	3	47

Copy

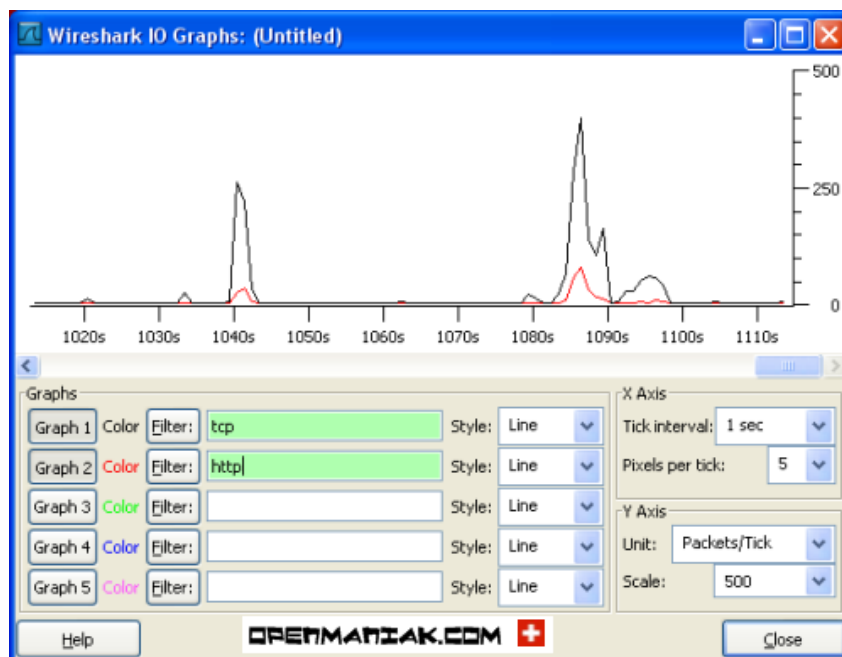
☒ Name resolution

Help Close

OPENMANIAK.COM

- **IO Graphs**

Grafice simple pot fi obtinute in sectiunea "IO graphs"; Grafice multiple pot fi adaugate in aceiasi fereastra la afisarea filtrelor de baza per. In exemplul de mai jos s-a realizat un grafic care depinde de filtrul de afisare "tcp" si "http".



- **Conversation List**

"Conversation List" vine cu aceleasi informatii date si de sectiunea "Conversations".

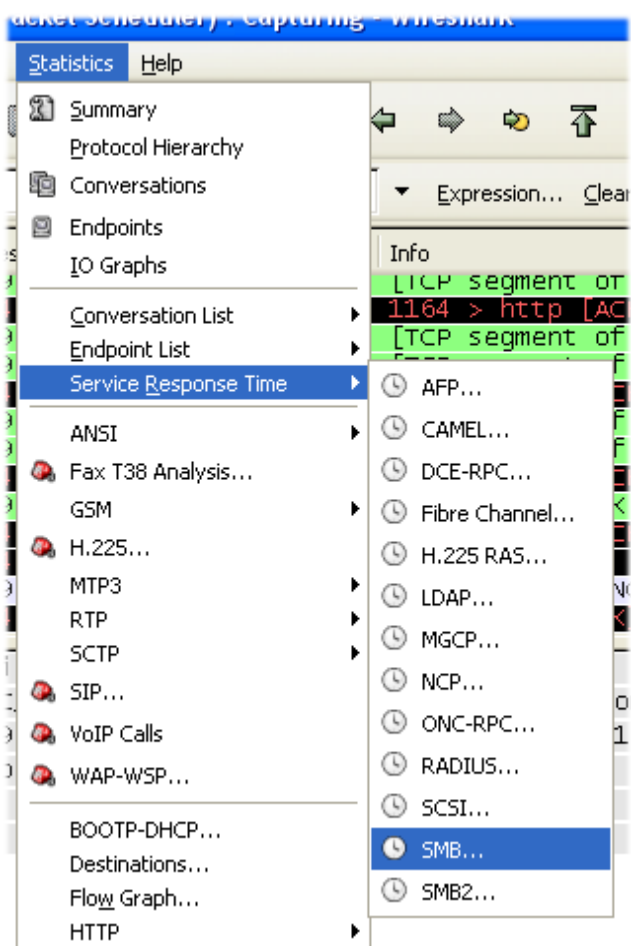
- **Endpoint List**

Sectiunea "Endpoint list" vine cu aceleasi informatii date si de sectiunea "Endpoints".

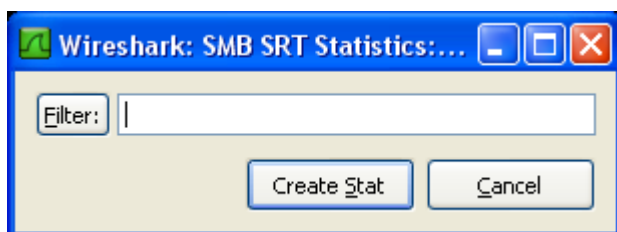
- **Service Response Time**

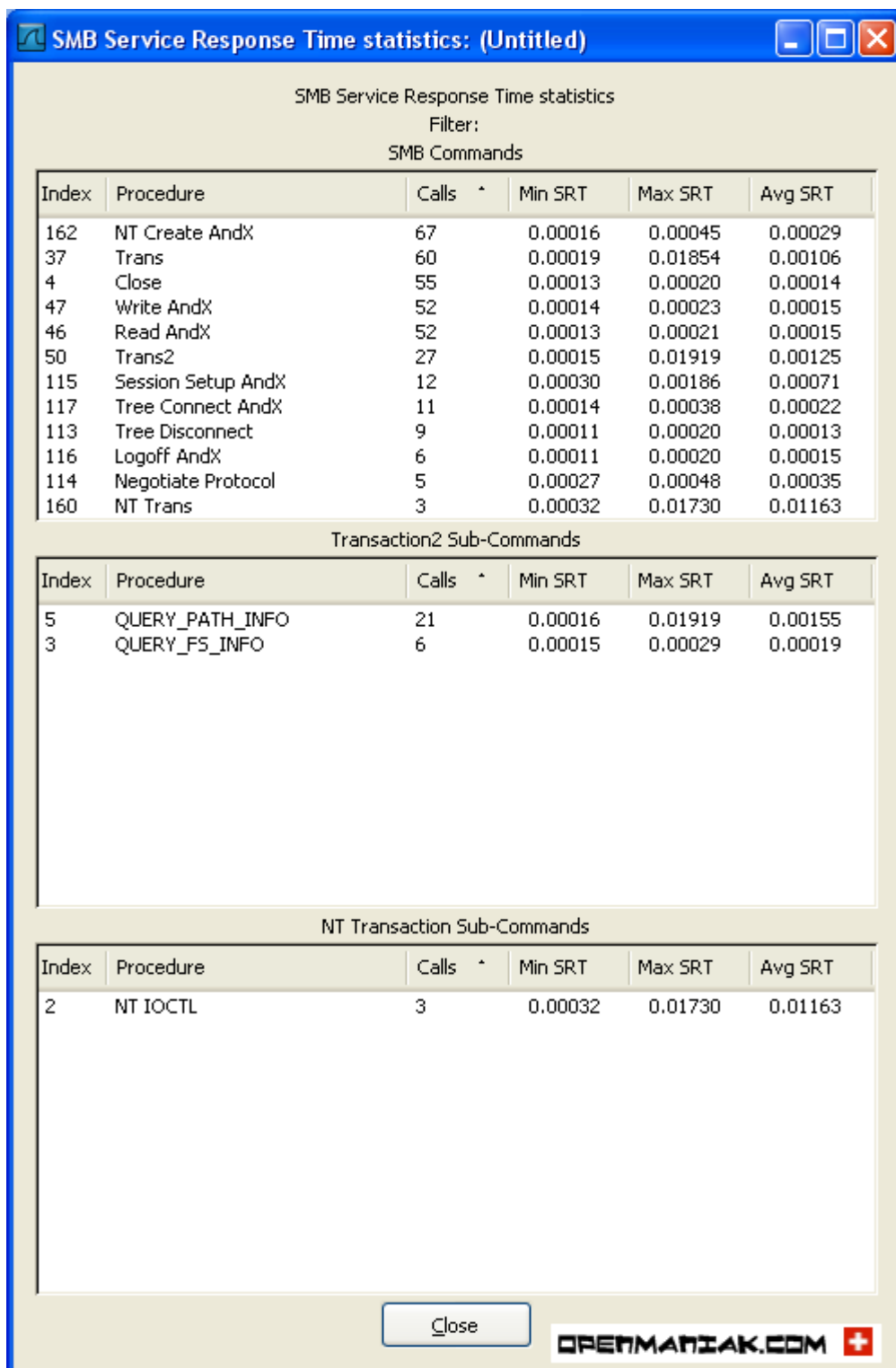
13 protocole sunt disponibile pentru o inspectie in profunzime.

In exemplul nostru vom alege SMB (Server Message Block) care ruleaza deasupra protocolului NetBIOS (vezi captura cu ierarhia protocoalelor) si este folosit de obicei de fisierele partajate intru-un mediu de retea local Microsoft Windows.



Wireshark afiseaza filtrul din campul smb. In exemplul nostru nu vom avea filtru de afisare.

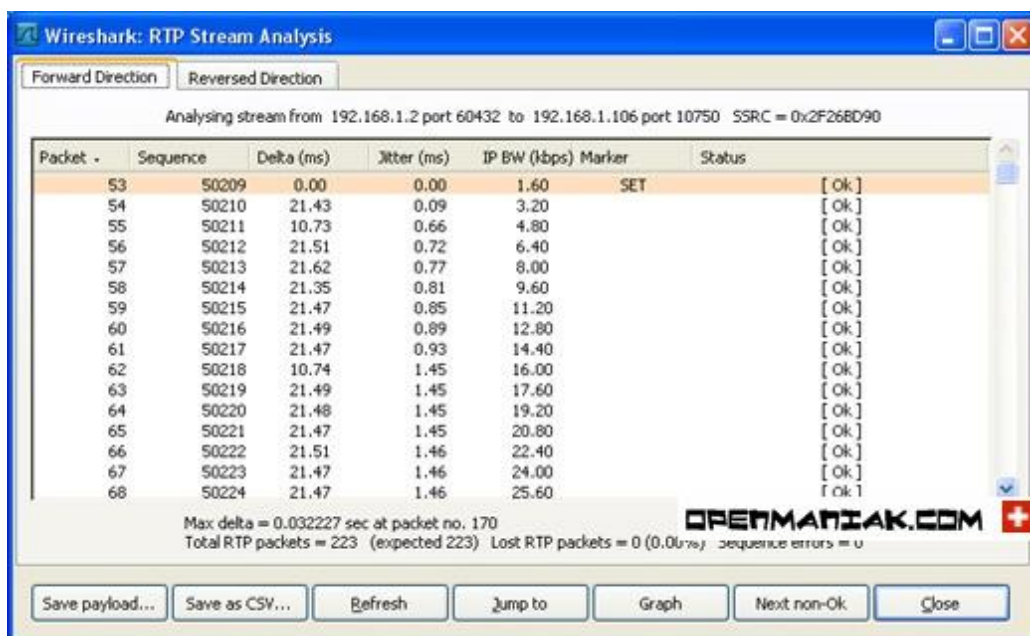
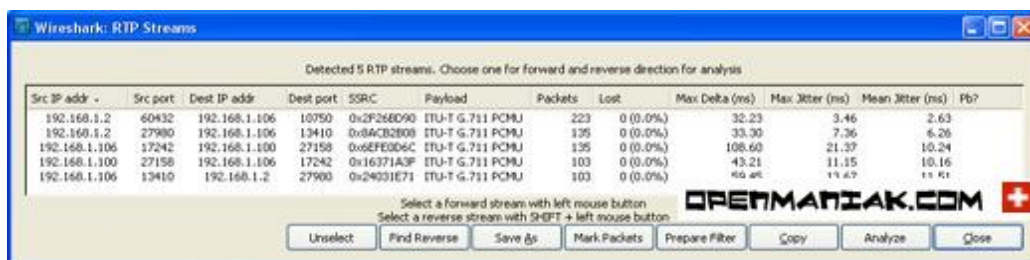




- **RTP**

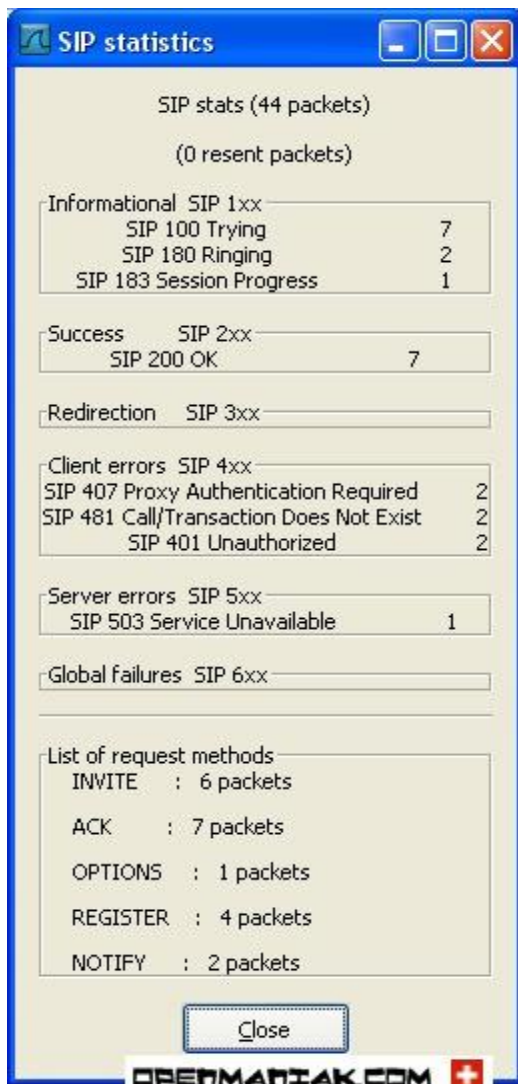
RTP (Real-time Transport Protocol, RFC 3550) este un protocol care transporta voce si video intr-o retea de tip IP. Ruleaza deasupra User Datagram Protocol. (UDP) Este frecvent folosit impreuna cu SIP or H.323 care vine cu sarcinile de semnalizare.

- **Show all streams**



• SIP

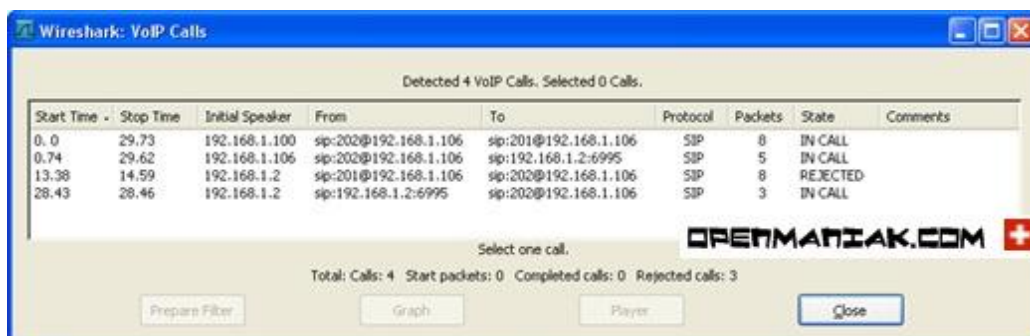
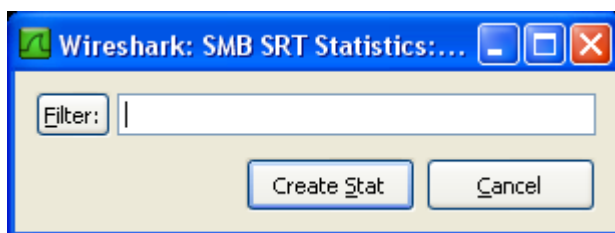
SIP (Session Initiation Protocol, RFC 3261) este un protocol de semnalizare pentru stabilirea de sesiuni VoIP sau video. Functioneaza de obicei cu protocolul RTP care este folosit pentru a transmite date in format multimedia.



• VoIP Calls

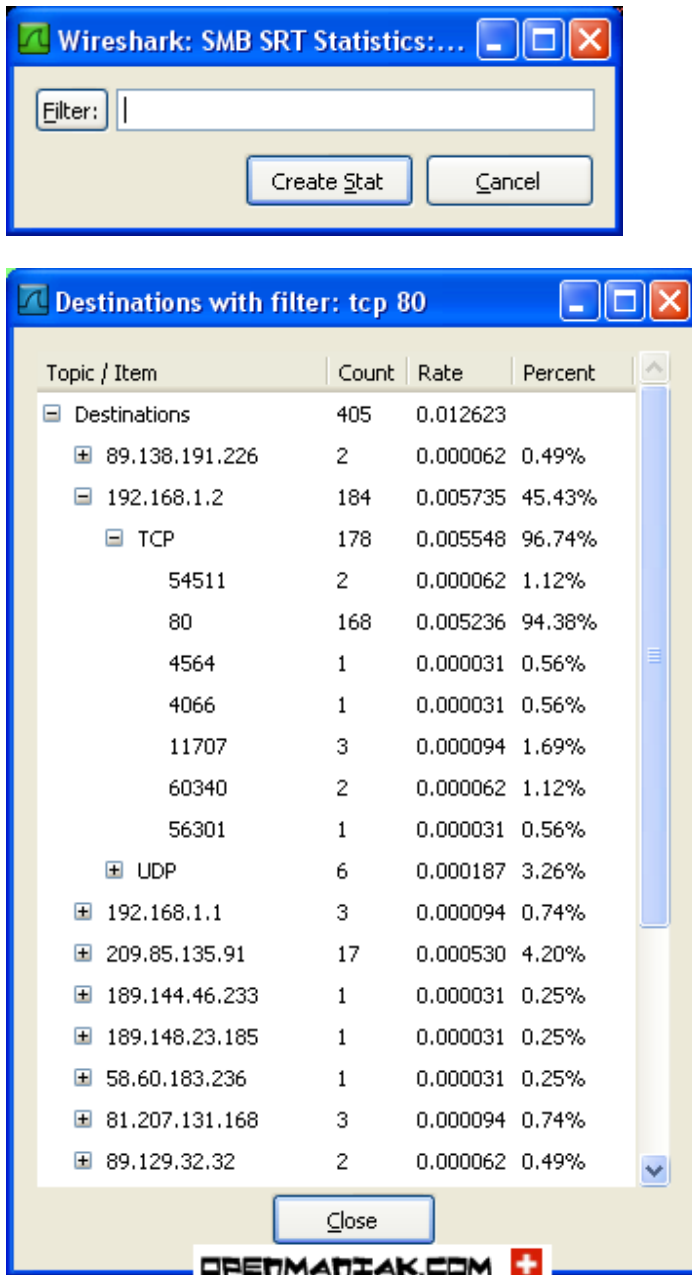
VoIP (Voice over IP) foloseste in general doua tipuri de protocoale:

- protocoale de semnalizare ca SIP sau H.323
- protocoale de transport ca RTP



Destinations

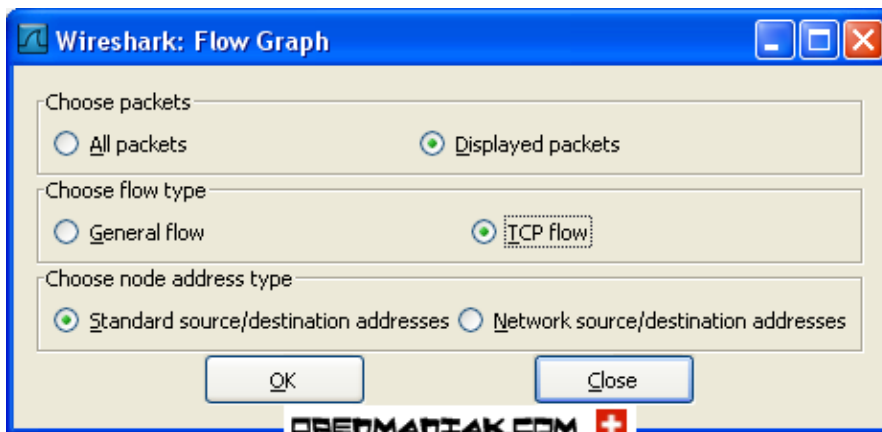
Sectinea "Destinations" arata toate destinatiile IP ale pachetelor de pe retea.



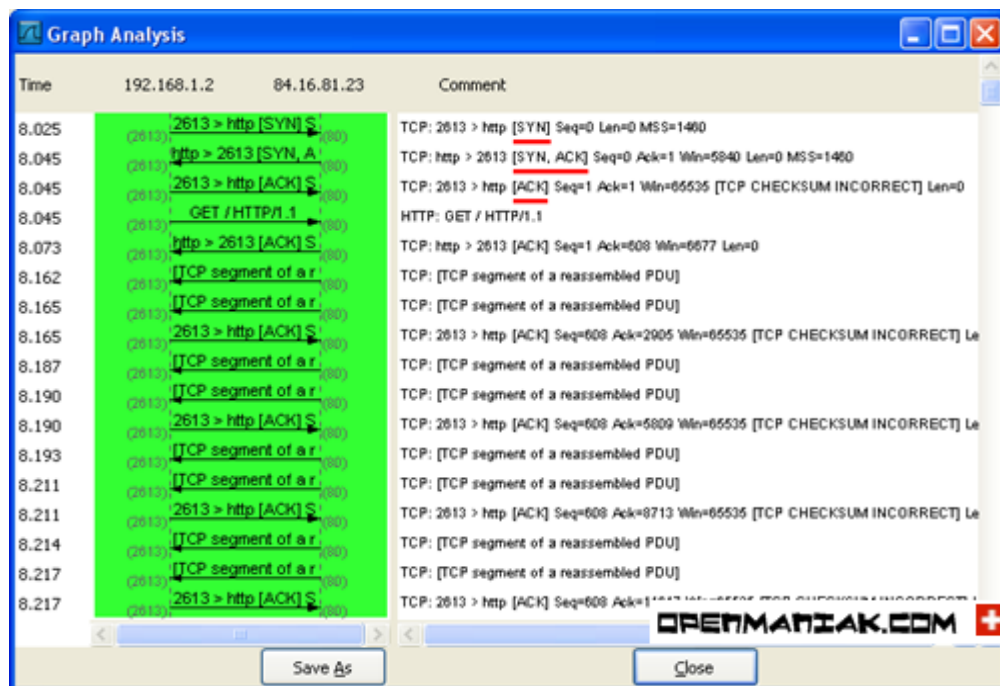
- **Flow Graph**

Sectiunea "Flow Graph" section vine cu o analiza secventiala a conexiunilor TCP.

In exemplul nostru am creat un filtru de afisare care are catinta doar traficul catre website-ul openmaniak.com.



Primele trei linii afiseaza conexiunile TCP stabilite cu secventele "SYN", "SYN ACK" si "ACK".



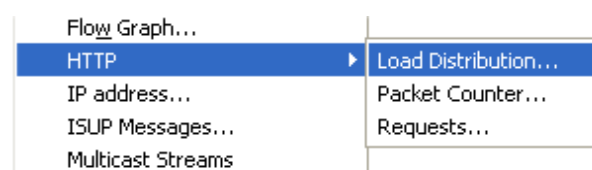
• HTTP

HTTP (Hypertext Transfer Protocol) este un protocol de comunicatie clien-serveris folosit pentru a transfera fisiere HTML. Un client HTTP , de cele mai multe ori un navigator web, trimete o cerere HTTP catre un server prin bine cunoscutul camp "URL", folosit pentru a localiza fisierul. Serverul web va rintoarce un raspuns HTTP si va pune la dispozitie pagina web dorita de client.

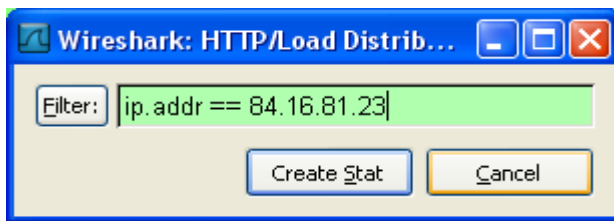
Radacina sub-sectiuniilor disponibil sub "HTTP":

- Load Distribution
- Packet Counter
- Requests

• Load distribution:



In exemplul nostru, s-a creat un filtru de afisare care va avea ca tinta doar traficul catre site-ul openmaniak.com.

A screenshot of the 'HTTP/Load Distribution with filter: ip.addr == 84....' window. It displays a table with three columns: 'Topic / Item', 'Count', 'Rate', and 'Percent'. The table contains data for HTTP requests by server, server address, and HTTP host, filtered for the IP address 84.16.81.23. A 'Close' button is located at the bottom right.

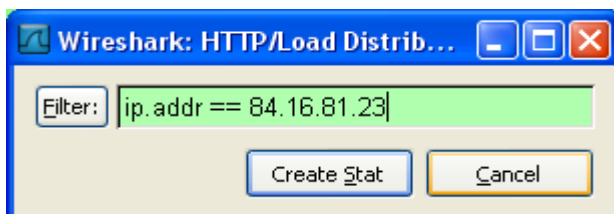
Topic / Item	Count	Rate	Percent
HTTP Requests by Server	31	0.003412	
HTTP Requests by Server Address	31	0.003412	100.00%
84.16.81.23	25	0.002752	80.65%
www.openmaniak.com	25	0.002752	100.00%
192.168.1.2	6	0.000660	19.35%
www.openmaniak.com	6	0.000660	100.00%
HTTP Requests by HTTP Host	31	0.003412	100.00%
www.openmaniak.com	31	0.003412	100.00%
84.16.81.23	25	0.002752	80.65%
192.168.1.2	6	0.000660	19.35%
HTTP Responses by Server Address	0	0.000000	

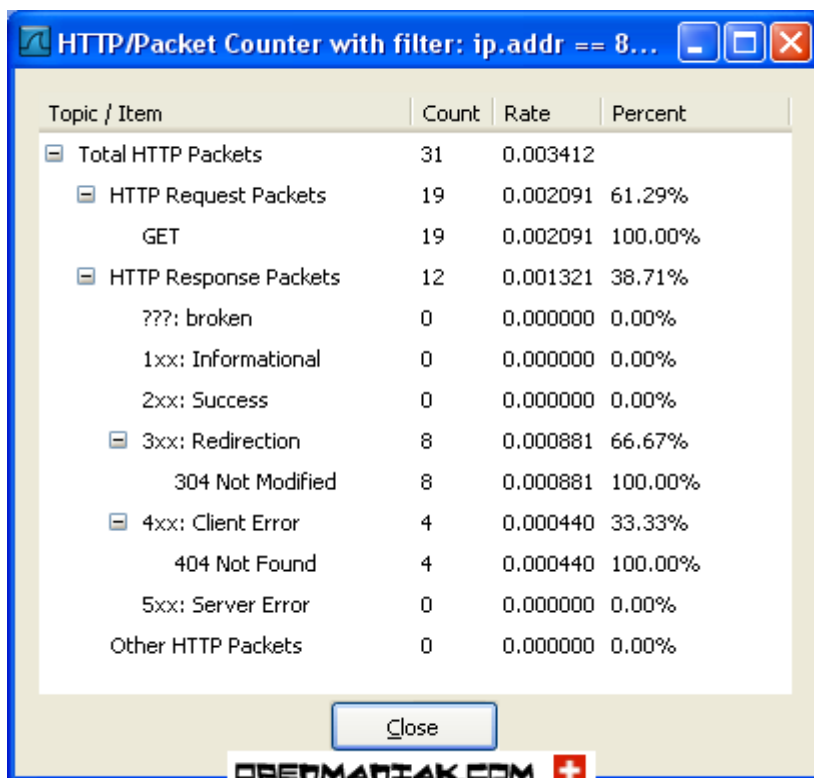
- **Packet Counter:**

Afiseaza cererile si raspunsurile HTTP.



In exemplu nostru, s-a creat un filtru de afisare care va avea ca tinta doar traficul catre website-ul openmaniak.com.





HTTP/Packet Counter with filter: ip.addr == 8...

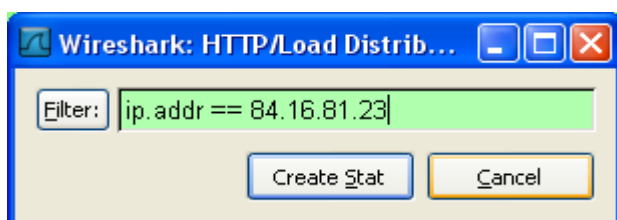
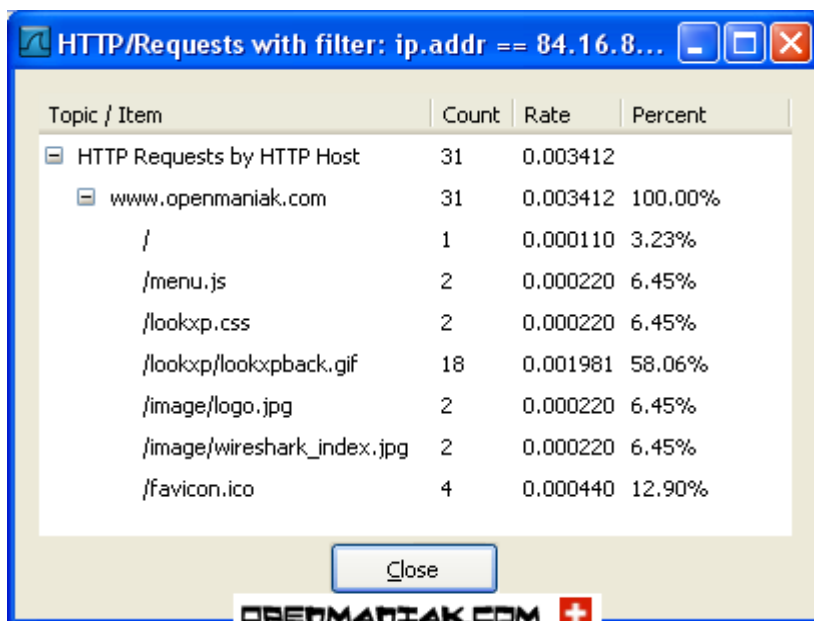
Topic / Item	Count	Rate	Percent
Total HTTP Packets	31	0.003412	
HTTP Request Packets	19	0.002091	61.29%
GET	19	0.002091	100.00%
HTTP Response Packets	12	0.001321	38.71%
???: broken	0	0.000000	0.00%
1xx: Informational	0	0.000000	0.00%
2xx: Success	0	0.000000	0.00%
3xx: Redirection	8	0.000881	66.67%
304 Not Modified	8	0.000881	100.00%
4xx: Client Error	4	0.000440	33.33%
404 Not Found	4	0.000440	100.00%
5xx: Server Error	0	0.000000	0.00%
Other HTTP Packets	0	0.000000	0.00%

Close

OPENMANIAK.COM

- **Requests:**

Afiseaza fisierele consultate de pe serverul web.

HTTP/Requests with filter: ip.addr == 84.16.81.23

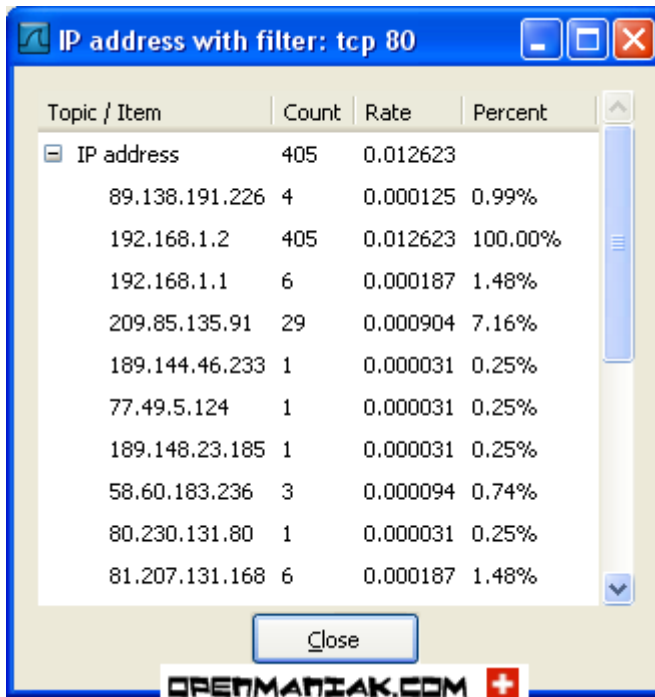
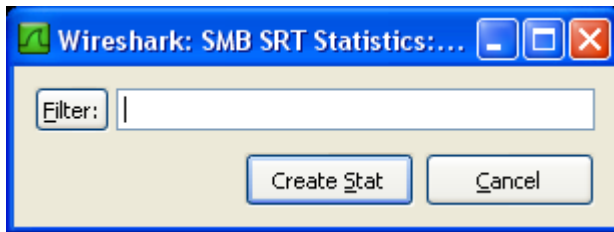
Topic / Item	Count	Rate	Percent
HTTP Requests by HTTP Host	31	0.003412	
www.openmaniak.com	31	0.003412	100.00%
/	1	0.000110	3.23%
/menu.js	2	0.000220	6.45%
/lookxp.css	2	0.000220	6.45%
/lookxp/lookxpback.gif	18	0.001981	58.06%
/image/logo.jpg	2	0.000220	6.45%
/image/wireshark_index.jpg	2	0.000220	6.45%
/favicon.ico	4	0.000440	12.90%

Close

OPENMANIAK.COM

- **IP address**

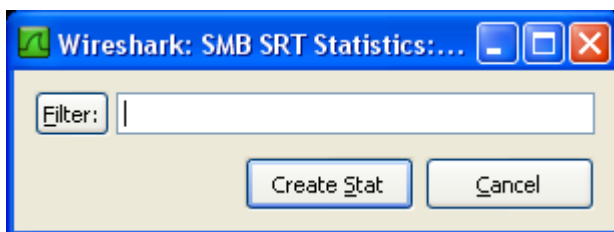
Afiseaza sursa si destinatia IP a pachetelor de pe retea.

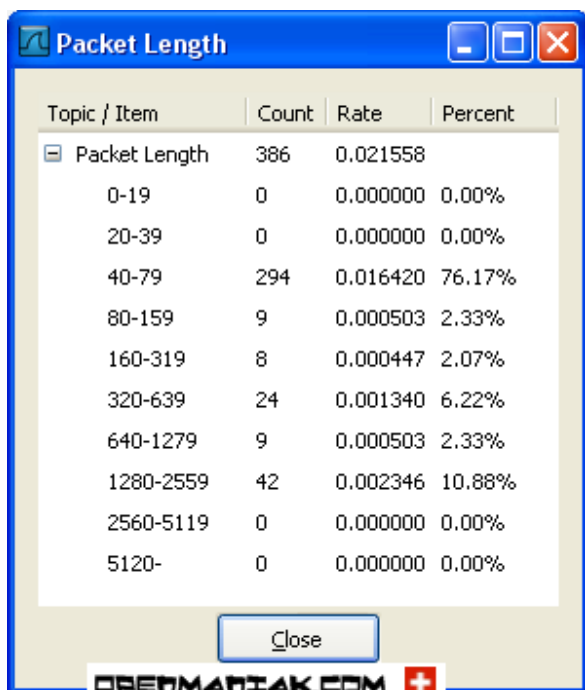


A screenshot of the 'IP address with filter: tcp 80' statistics window. It displays a table with columns for 'Topic / Item', 'Count', 'Rate', and 'Percent'. The table lists various IP addresses and their corresponding counts, rates, and percentages. A 'Close' button is located at the bottom right of the window. A watermark 'OPENMANIAK.COM' with a red plus icon is visible at the bottom of the image.

Topic / Item	Count	Rate	Percent
IP address	405	0.012623	
89.138.191.226	4	0.000125	0.99%
192.168.1.2	405	0.012623	100.00%
192.168.1.1	6	0.000187	1.48%
209.85.135.91	29	0.000904	7.16%
189.144.46.233	1	0.000031	0.25%
77.49.5.124	1	0.000031	0.25%
189.148.23.185	1	0.000031	0.25%
58.60.183.236	3	0.000094	0.74%
80.230.131.80	1	0.000031	0.25%
81.207.131.168	6	0.000187	1.48%

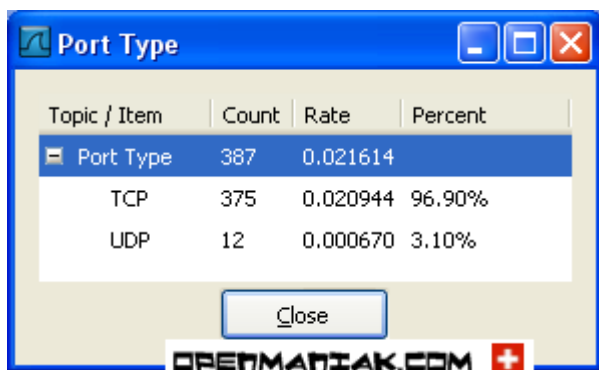
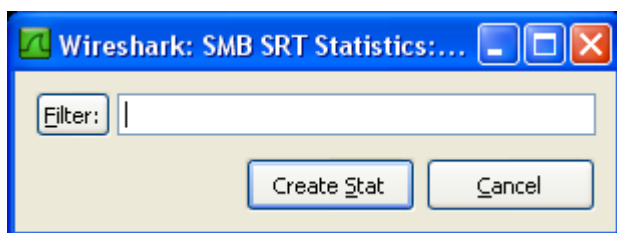
- Packet Length





• Port Type

Afiseaza informatii despre porturile TCP sau UDP.



Ethereal

Ethereal dispune de o interfata grafica compusa din 5 componente.

- **Bara de meniuri** – cele mai importante sunt *File* (care permite salvarea/incarcarea unei capturi) si *Capture*, care declanseaza operatiunea de captura.
- **Specificare filtru de afisare** – permite introducerea unei expresii care filtreaza pachetele care vor fi afisate.
- **Lista pachetelor capturate** - informatii despre pachetele capturate (numar de ordine atribuit de Ethereal, data capturii, adresa sursa, adresa destinatie, tipul protocolului, informatii specifice protocolului).
- **Detalii despre pachetul selectat** – informatii despre pachetul selectat din lista de pachete. Include detalii despre frame-ul Ethernet si datagrama IP.

- **Continutul pachetului in Hexa si ASCII**

Bara de meniuri

Specificare filtru de afisare

Lista pachetelor capturate

Detalii despre pachetul selectat

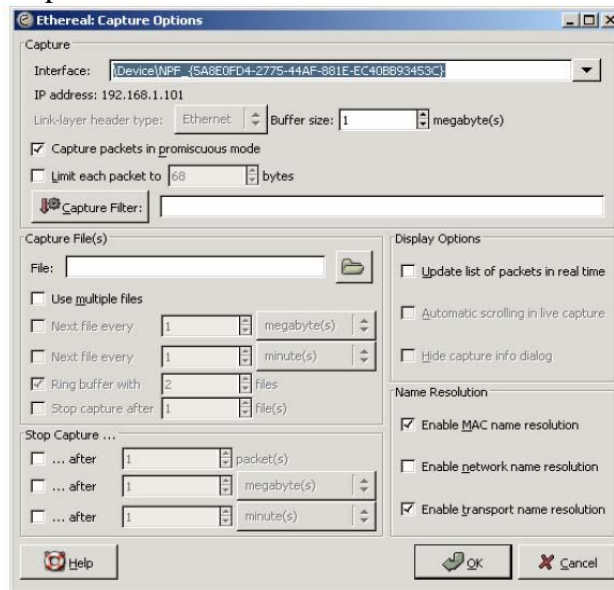
Continutul pachetului in Hexa si ASCII

The screenshot shows the Wireshark interface with the following components:

- Bara de meniuri:** File, Edit, View, Go, Capture, Analyze, Statistics, Help.
- Specificare filtru de afisare:** A filter bar with a dropdown menu and buttons for 'Expression...', 'Clear', and 'Apply'.
- Lista pachetelor capturate:** A table with columns: No., Time, Source, Destination, Protocol, and Info. It lists various network packets including DNS, TCP, and HTTP.
- Detalii despre pachetul selectat:** A detailed view of the selected packet (No. 6, Time 0.000000). It shows the Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol layers.
- Continutul pachetului in Hexa si ASCII:** A pane at the bottom showing the raw data of the selected packet in hexadecimal and ASCII format.

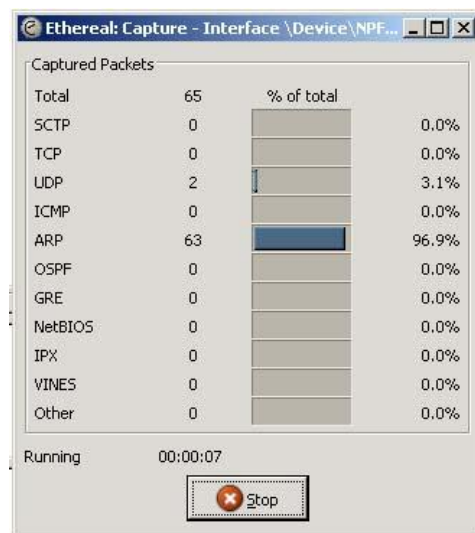
Ethereal GUI

Pentru a declansa captura, trebuie apelata comanda *Capture – Start*, care va afisa o fereastră unde pot fi definite optiunile de captura.



Optiuni de captura

- Printre optiunile de captura, se numara interfata care va fi utilizata, fisierul in care va fi salvata captura, durata capturii, etc. Optional se poate defini si un filtru pentru a captura numai anumite pachete. Expresiile de filtrare a capturii sunt diferite de expresiile de filtrare a listei de pachete capturate.
- Dupa declansarea operatiuni de capturare a pachetelor, va apare o fereastră care afiseaza numarul si tipul pachetelor capturate si in plus contine butonul *Stop* care opreste captura.



Fereastra de captura