Sniffer's
Network Packet Analyzer
Basics

Sniffer

- Network Analysis
  - Range of techniques that network engineers and designers employ to study the properties of networks, including connectivity, capacity and performance.
- Network packet analyzer
  - Tries to capture network packets and then display that packet data as detailed as possible.
    - Capture and decode

Sniffer Continued

- Intended purposes:
  - network administrators use them to **troubleshoot network problems**
  - network security engineers use them to **examine security problems**
  - developers use them to **debug protocol implementations**
  - people use them to **learn network protocol** internals
- You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

Popular Sniffer's

- EtherPeek (http://www.wildpackets.com/)
  - EtherPeek product family has been specifically designed to address the unique challenges of today's network environments
  - Designed to accelerate the troubleshooting of Ethernet-specific problems
  - EtherPeek features powerful problem detection and Ethernet-specific diagnostic capabilities

EtherPeek Continued

- Verisons
  - EtherPeek VX
    - WildPackets Expert VoIP Network Analyzer
      - is the ultimate solution for intelligent diagnosis of pre and post-deployment VoIP and Ethernet network issues within enterprises
  - EtherPeek NX
    - WildPackets' Expert Ethernet Network Analyzer
      - provides network engineers with the expert diagnostics they need to deploy, secure, and troubleshoot Ethernet networks
  - EtherPeek SE
    - WildPackets' Ethernet Protocol Analyzer
      - is an intuitive, powerful network and protocol analyzer for Ethernet networks

Ethereal (http://www.ethereal.com)

- Ethereal is a downloadable - network packet analyzer
- Some of the many features Ethereal provides:
  - Available for **UNIX** and **Windows**.
  - **Capture** live packet data from a network interface.
  - Display packets with **very detailed protocol information**.

Ethereal Features continued

- **Open and Save** packet data captured.
- **Import and Export** packet data from and to a lot of other capture programs.
- **Filter packets** on many criteria.
- **Search** for packets on many criteria.
- **Colorize** packet display based on filters.
- Create various **statistics.**

Ethereal Filters

- Rich set of display filters (40,855 as of version 0.10.14) that let you quickly drill down to the traffic
- Downloadable manual
  - Filters area
    - Each protocol page you will find a list of supported display filters for that protocol, along with data type and version information

Open captured files

- Input File Formats from different tools
  - libpcap, tcpdump and various other tools using tcpdump's capture format
  - Sun snoop and atmsnoop
  - Shomiti/Finisar *Surveyor* captures
  - Novell *LANalyzer* captures
  - Microsoft Network Monitor captures
  - AIX's iptrace captures
  - Cinco Networks NetXray captures
  - Network Associates Windows-based Sniffer and Sniffer Pro captures
  - Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures
  - AG Group/WildPackets EtherPeek/TokenPeek/AirOPeek/EtherHelp/Packet Grabber captures
  - RADCOM's WAN/LAN Analyzer captures
  - Network Instruments Observer version 9 captures

Terms, Concepts and Models

- Protocols
  - special set of rules that end points in a telecommunication connection use when they communicate.
- Transmission Control Protocol (TCP)
  - which uses a set of rules to exchange messages with other Internet points at the information packet level
- Internet Protocol (IP)
  - which uses a set of rules to send and receive messages at the Internet address level

Terms, Concepts and Models

- MAC or physical address
  - unique identifier attached to most forms of networking equipment.
- Internet Protocol Address (IP address)
  - unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard.

Open System Interconnection (OSI) Model

- OSI established in 1984
- describes how information from a software application in one computer moves through a network medium to a software application in another computer.

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

Issues

- Sniffer software
  - Computer system
    - should be connected to a hub or monitoring port on switch
    - Network card set correctly
    - Must be Authorized to capture packets
  - Network
    - Connection located where traffic of interest is best captured
      - Internet traffic close to gateway
      - Specific department – connected off one of their switches.

Screen Shots Ethereal

Interface

- Summary Line Area
  - Displays a one-line summary of the highest-layer protocol contained in the frame, time of capture, source and destination.
- Detail
  - Provides details on all the layers inside the frame.
- Hex
  - Displays the raw captured data in the hexadecimal format.

few packets.cap - Ethereal

File Edit View Capture Analyze Help

No.	Time	Delta	Source	Destination	Protocol	Info
13	14.817570	14.817570	192.168.0.10	192.168.0.2	TCP	1242 > 80 [SYN] Seq=1404510823 Ack=0 Win=655
14	14.817689	0.000119	192.168.0.2	192.168.0.10	TCP	80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404
15	14.818178	0.000489	192.168.0.10	192.168.0.2	TCP	1242 > 80 [ACK] Seq=1404510824 Ack=366161510
16	14.819035	0.000857	192.168.0.10	192.168.0.2	HTTP	GET / HTTP/1.1
17	14.975815	0.156780	192.168.0.2	192.168.0.10		
23	19.382555	4.406740	192.168.0.10	192.168.0.2		
24	19.382634	0.000079	192.168.0.2	192.168.0.10		
52	54.234482	34.851848	192.168.0.2	192.168.0.10		
53	54.235272	0.000790	192.168.0.10	192.168.0.2		

SUMMARY LINE Area

You can inspect the captured data in great detail, even while a capture session is in progress. Items in the packet list can be shown in any color you like.

```
▷ Frame 16 (464 bytes on wire, 464 bytes captured)
▷ Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
▷ Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
▷ Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.0.2\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
```

DETAIL area

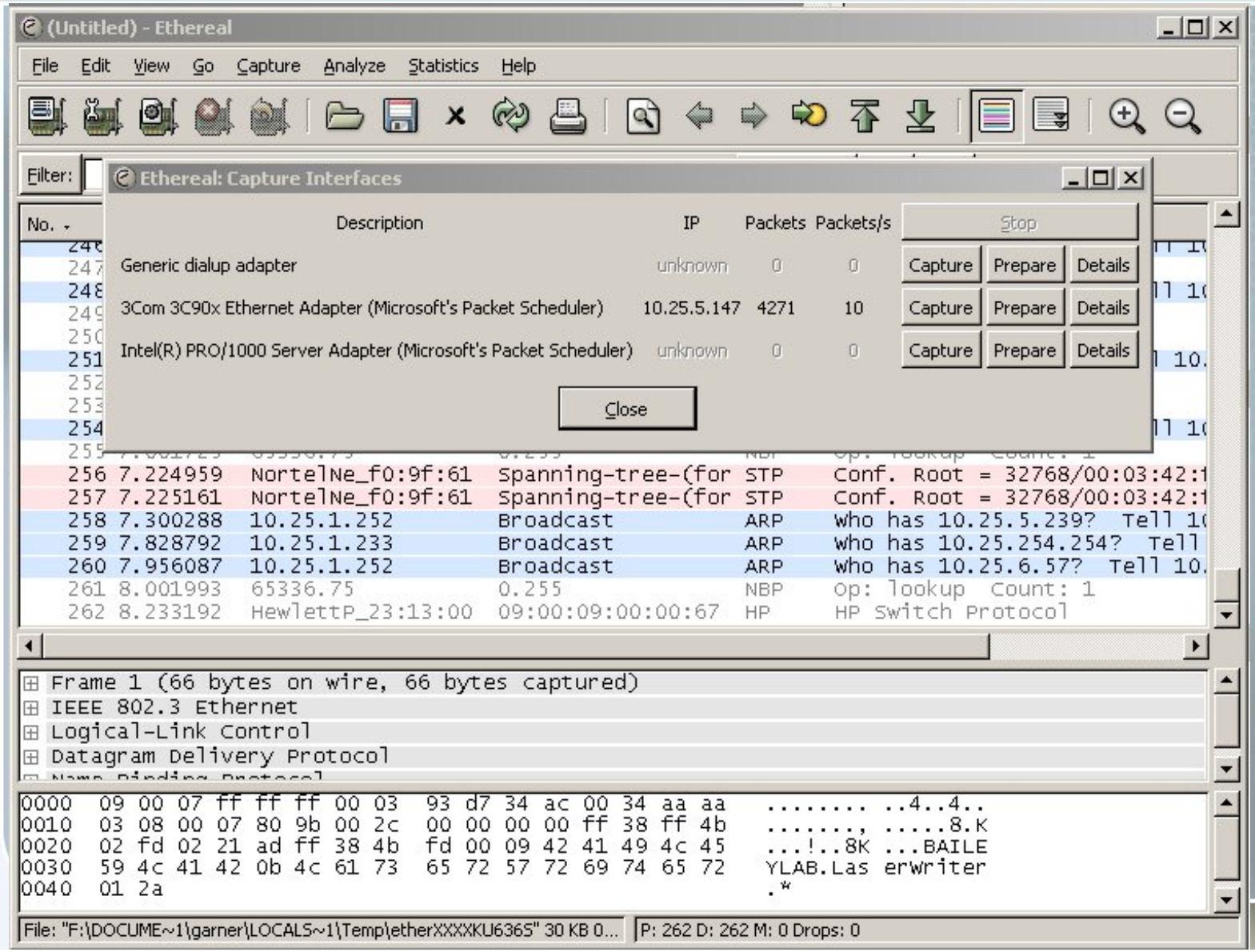
```
0000  00 0b 5d 20 cd 02 00 04  61 4a 1e 95 08 00 45 00   ..] .... aJ....E.
0010  01 c2 d1 6d 40 00 80 06  a6 6b c0 a8 00 0a c0 a8   ...m@... .k......
0020  00 02 04 da 00 50 53 b7  22 68 da 3f d0 01 50 18   .....PS. "h.?..P.
0030  ff ff 46 26 00 00 47 45  54 20 2f 20 48 54 54 50   ..F&..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 39 32 2e   /1.1..Ho st: 192.
```

HEX area

Filter: tcp | Expression... | Clear | Apply | File: few packets.cap 24 KB 00:0 | P: 104 D: 19 M: 0

Recent Capture

Ethereal Capture Tab



Google Search

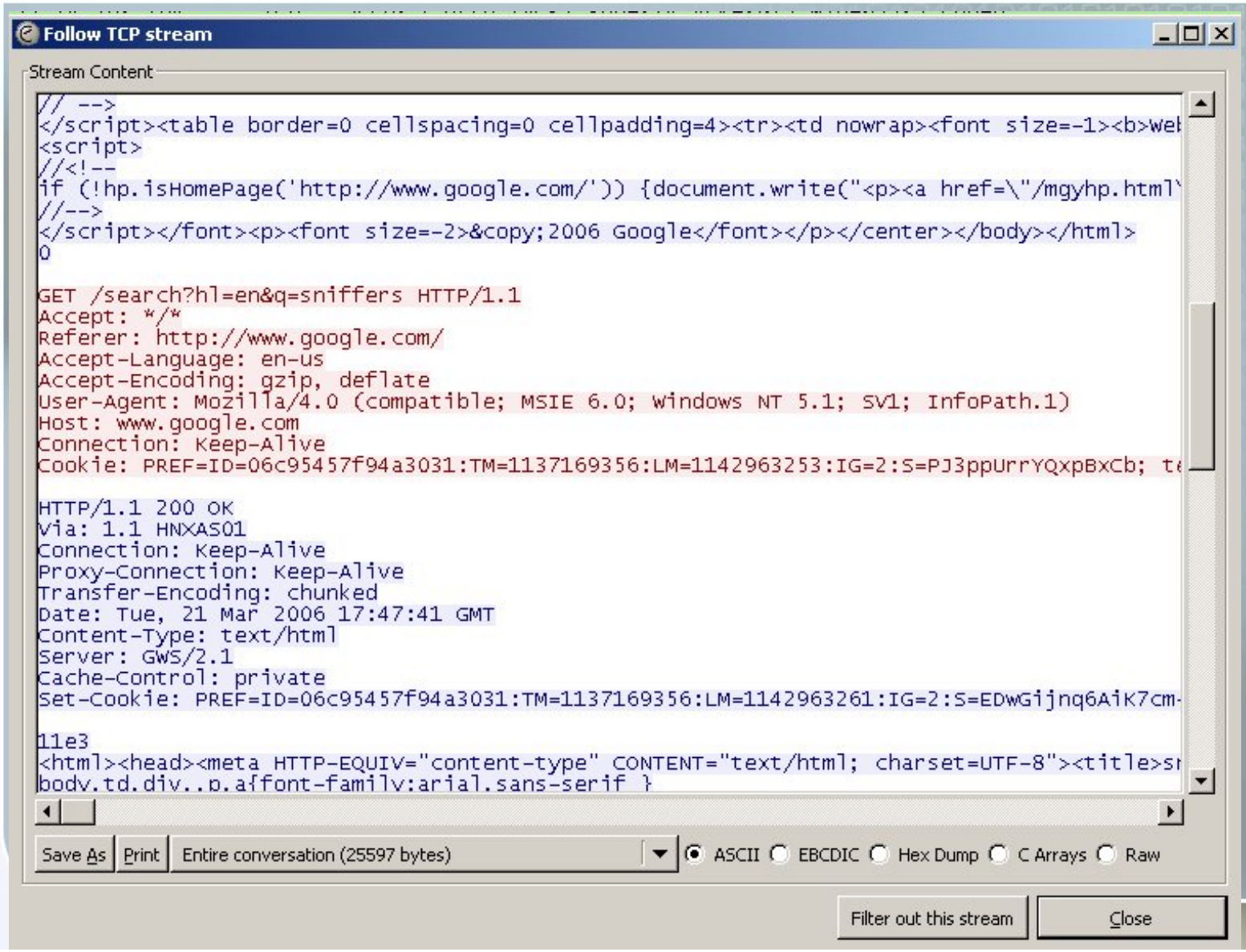
File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 10.25.5.147 and ip.addr eq 72.14.203.104) and (tcp.port eq 477 | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
295	9.528576	10.25.5.147	72.14.203.104	TCP	4779 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
298	9.531638	72.14.203.104	10.25.5.147	TCP	http > 4779 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460
299	9.531696	10.25.5.147	72.14.203.104	TCP	4779 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
300	9.532040	10.25.5.147	72.14.203.104	HTTP	GET / HTTP/1.1
323	9.617680	72.14.203.104	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
343	9.742180	10.25.5.147	72.14.203.104	TCP	4779 > http [ACK] Seq=314 Ack=1461 Win=65535 Len=0
344	9.742888	72.14.203.104	10.25.5.147	TCP	[TCP Previous segment lost] [TCP segment of a reassembled PDU
345	9.742932	10.25.5.147	72.14.203.104	TCP	[TCP Dup ACK 343#1] 4779 > http [ACK] Seq=314 Ack=1461 Win=6
547	12.052175	72.14.203.104	10.25.5.147	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
548	12.052266	10.25.5.147	72.14.203.104	TCP	4779 > http [ACK] Seq=314 Ack=3915 Win=65535 Len=0
774	18.212146	10.25.5.147	72.14.203.104	HTTP	GET /search?hl=en&q=sniffers HTTP/1.1
775	18.313399	72.14.203.104	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
776	18.313526	72.14.203.104	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
777	18.313566	10.25.5.147	72.14.203.104	TCP	4779 > http [ACK] Seq=683 Ack=6835 Win=65535 Len=0
778	18.315334	72.14.203.104	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
779	18.317344	72.14.203.104	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
780	18.317403	10.25.5.147	72.14.203.104	TCP	4779 > http [ACK] Seq=683 Ack=8881 Win=65535 Len=0
782	18.373594	72.14.203.104	10.25.5.147	TCP	[TCP segment of a reassembled PDU]

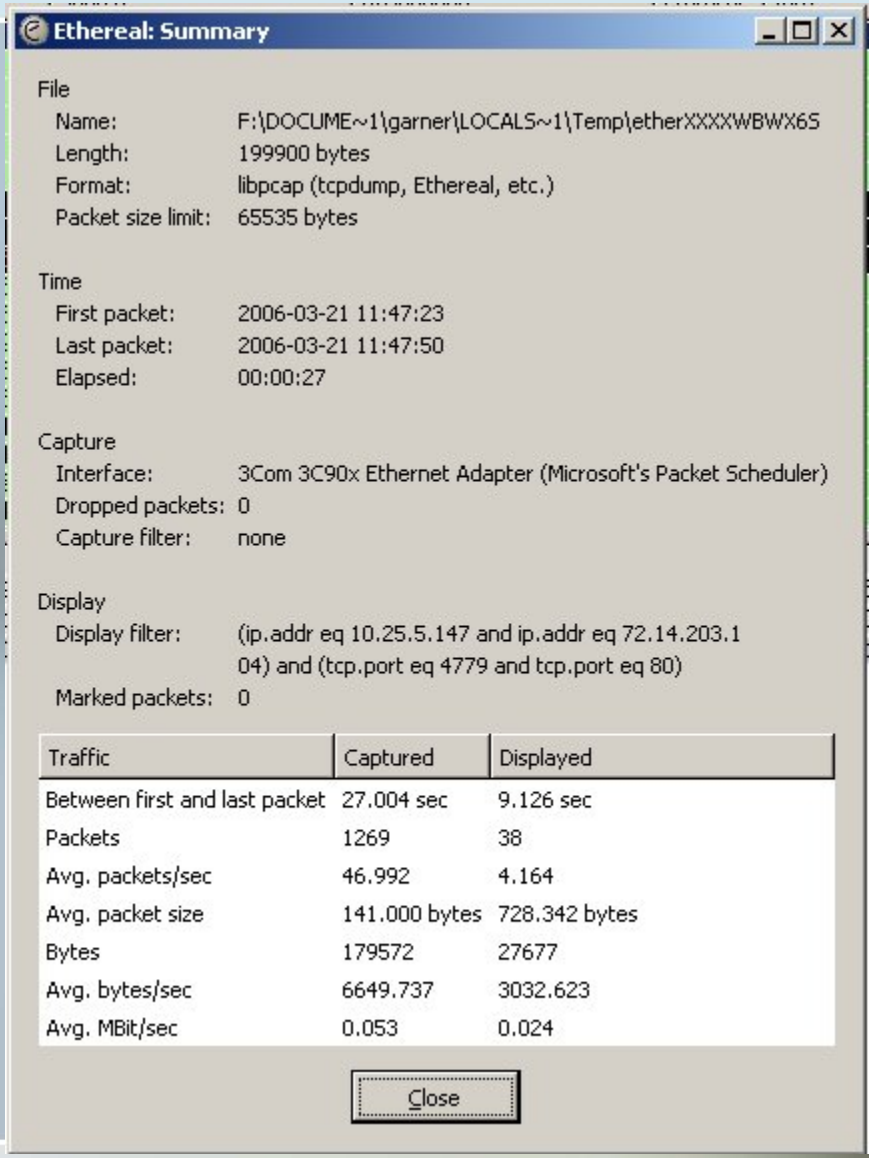
```
⊞ Frame 295 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 10.25.5.147 (00:60:08:c7:64:21), Dst: 10.25.254.254 (00:0f:20:98:76:3d)
⊞ Internet Protocol, Src: 10.25.5.147 (10.25.5.147), Dst: 72.14.203.104 (72.14.203.104)
⊞ Transmission Control Protocol, Src Port: 4779 (4779), Dst Port: http (80), Seq: 0, Ack: 0, Len: 0
```

Follow TCP stream (Google)



Summary

- 1269 Packets
- 27.004 seconds



Ethereal: Summary

File
Name: F:\DOCUME~1\garner\LOCALS~1\Temp\etherXXXXWBWX6S
Length: 199900 bytes
Format: libpcap (tcpdump, Ethereal, etc.)
Packet size limit: 65535 bytes

Time
First packet: 2006-03-21 11:47:23
Last packet: 2006-03-21 11:47:50
Elapsed: 00:00:27

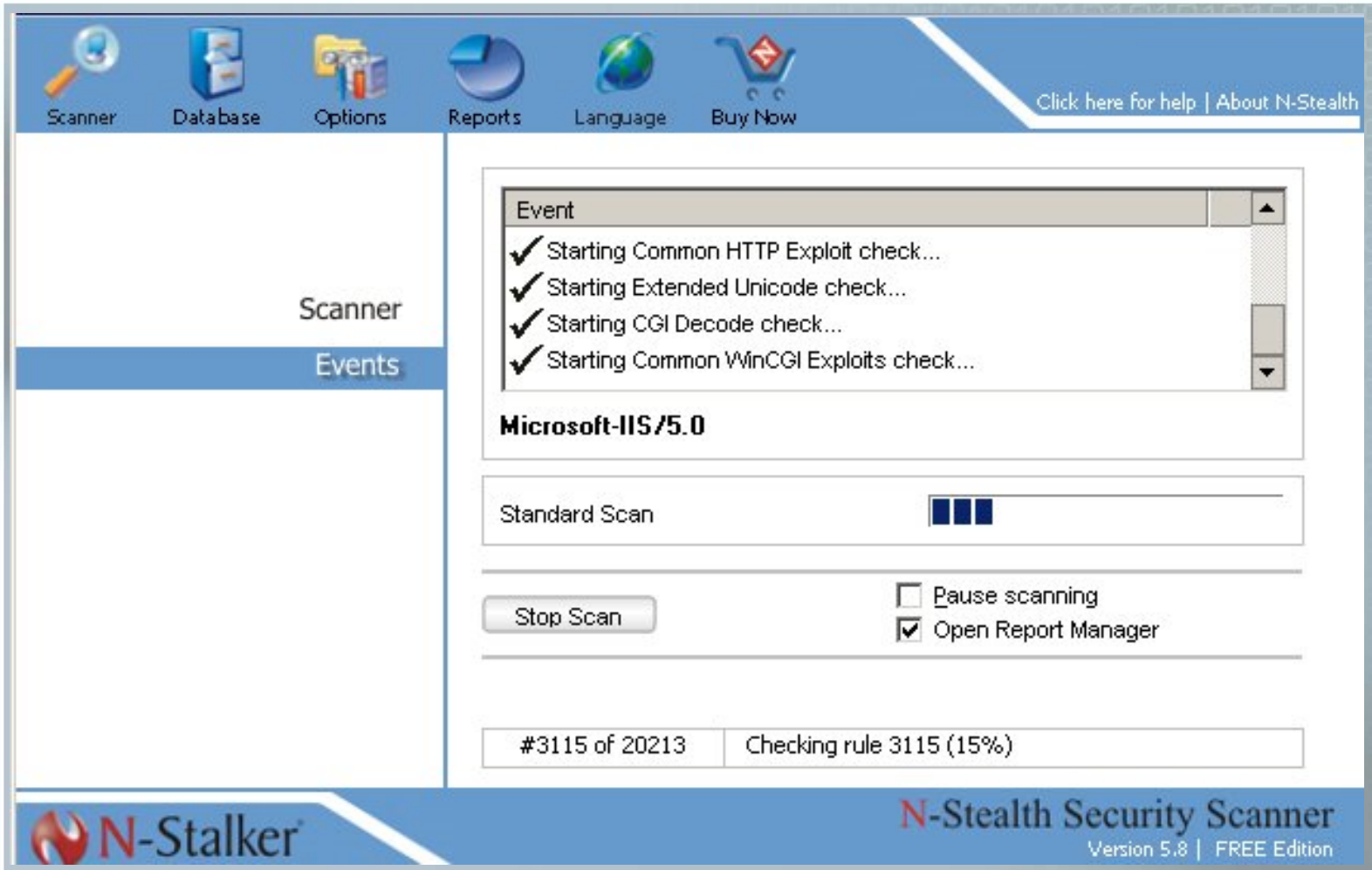
Capture
Interface: 3Com 3C90x Ethernet Adapter (Microsoft's Packet Scheduler)
Dropped packets: 0
Capture filter: none

Display
Display filter: (ip.addr eq 10.25.5.147 and ip.addr eq 72.14.203.104) and (tcp.port eq 4779 and tcp.port eq 80)
Marked packets: 0

Traffic	Captured	Displayed
Between first and last packet	27.004 sec	9.126 sec
Packets	1269	38
Avg. packets/sec	46.992	4.164
Avg. packet size	141.000 bytes	728.342 bytes
Bytes	179572	27677
Avg. bytes/sec	6649.737	3032.623
Avg. MBit/sec	0.053	0.024

Close

Tools at work



Tools capture

245	3.292154	10.25.5.147	10.25.1.223	TCP	4877 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
246	3.292347	10.25.1.223	10.25.5.147	TCP	http > 4877 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
247	3.292385	10.25.5.147	10.25.1.223	TCP	4877 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
248	3.293951	10.25.5.147	10.25.1.223	HTTP	GET / HTTP/1.0
249	3.295118	10.25.1.223	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
250	3.295232	10.25.1.223	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
251	3.295263	10.25.5.147	10.25.1.223	TCP	4877 > http [ACK] Seq=102 Ack=2921 Win=65535 Len=0
252	3.295640	10.25.1.223	10.25.5.147	HTTP	HTTP/1.1 401 Access Denied (text/html)
253	3.295674	10.25.5.147	10.25.1.223	TCP	4877 > http [ACK] Seq=102 Ack=4242 Win=64215 Len=0
254	3.297738	10.25.5.147	10.25.1.223	TCP	4878 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
255	3.297882	10.25.1.223	10.25.5.147	TCP	http > 4878 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
256	3.297911	10.25.5.147	10.25.1.223	TCP	4878 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
257	3.298087	10.25.5.147	10.25.1.223	HTTP	POST / HTTP/1.0
258	3.299093	10.25.1.252	Broadcast	ARP	Who has 10.25.6.203? Tell 10.25.1.252
259	3.327642	10.25.1.223	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
260	3.327747	10.25.1.223	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
261	3.327783	10.25.5.147	10.25.1.223	TCP	4878 > http [ACK] Seq=103 Ack=2921 Win=65535 Len=0
262	3.328132	10.25.1.223	10.25.5.147	HTTP	HTTP/1.1 405 Method not allowed (text/html)
263	3.328166	10.25.5.147	10.25.1.223	TCP	4878 > http [ACK] Seq=103 Ack=4105 Win=64352 Len=0
264	3.330147	10.25.5.147	10.25.1.223	TCP	4879 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
265	3.330298	10.25.1.223	10.25.5.147	TCP	http > 4879 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
266	3.330326	10.25.5.147	10.25.1.223	TCP	4879 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
267	3.330499	10.25.5.147	10.25.1.223	HTTP	HEAD / HTTP/1.0
268	3.331313	10.25.1.223	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
269	3.331395	10.25.1.223	10.25.5.147	TCP	http > 4879 [FIN, ACK] Seq=195 Ack=103 Win=65433 Len=0
270	3.331426	10.25.5.147	10.25.1.223	TCP	4879 > http [ACK] Seq=103 Ack=196 Win=65341 Len=0
271	3.333888	10.25.5.147	10.25.1.223	TCP	4880 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
272	3.334035	10.25.1.223	10.25.5.147	TCP	http > 4880 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
273	3.334063	10.25.5.147	10.25.1.223	TCP	4880 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
274	3.334234	10.25.5.147	10.25.1.223	HTTP	PROPFIND / HTTP/1.0
275	3.334939	10.25.1.223	10.25.5.147	TCP	[TCP segment of a reassembled PDU]
276	3.335151	10.25.1.223	10.25.5.147	HTTP	HTTP/1.1 411 Length Required (text/html)
277	3.335188	10.25.5.147	10.25.1.223	TCP	4880 > http [ACK] Seq=107 Ack=193 Win=65344 Len=0
278	3.336953	10.25.5.147	10.25.1.223	TCP	4881 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
279	3.337097	10.25.1.223	10.25.5.147	TCP	http > 4881 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
280	3.337125	10.25.5.147	10.25.1.223	TCP	4881 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
281	3.337300	10.25.5.147	10.25.1.223	HTTP	OPTIONS / HTTP/1.0
282	3.337996	10.25.1.223	10.25.5.147	HTTP	HTTP/1.1 200 OK
283	3.338055	10.25.1.223	10.25.5.147	TCP	http > 4881 [FIN, ACK] Seq=394 Ack=106 Win=65430 Len=0
284	3.338083	10.25.5.147	10.25.1.223	TCP	4881 > http [ACK] Seq=106 Ack=395 Win=65142 Len=0
285	3.342911	10.25.5.147	10.25.1.223	TCP	4882 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
286	3.343068	10.25.1.223	10.25.5.147	TCP	http > 4882 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

```
⊞ Frame 286 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: hnxas08.hendrix.local (00:09:5b:8f:56:70), Dst: 10.25.5.147 (00:60:08:c7:64:21)
⊞ Internet Protocol, Src: 10.25.1.223 (10.25.1.223), Dst: 10.25.5.147 (10.25.5.147)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 4882 (4882), Seq: 0, Ack: 1, Len: 0

0000  00 60 08 c7 64 21 00 09  5b 8f 56 70 08 00 45 00   .`..d!.. [.Vp..E.
0010  00 30 3e cc 40 00 80 06  a0 58 0a 19 01 df 0a 19   .0>.@... .X......
0020  05 93 00 50 13 12 52 b3  b4 3e be 7f 83 72 70 12   ...P..R. .>...rp.
0030  ff ff 0b 26 00 00 02 04  05 b4 01 01 04 02         ...&.... ......
```

Tools Scan/Capture

- 42,000 packets
- 39.003 seconds

Tools Protocol Hierarchy

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	42284	19124224	3.826	0	0	0.000
Ethernet	100.00%	42283	19124130	3.826	0	0	0.000
Logical-Link Control	3.32%	1405	152974	0.031	0	0	0.000
HP Extended Local-Link Control	3.03%	1283	145184	0.029	0	0	0.000
HP Switch Protocol	3.03%	1283	145184	0.029	1283	145184	0.029
Spanning Tree Protocol	0.09%	40	2400	0.000	40	2400	0.000
Datagram Delivery Protocol	0.06%	25	1650	0.000	0	0	0.000
Name Binding Protocol	0.06%	25	1650	0.000	25	1650	0.000
Nortel SONMP	0.09%	40	2464	0.000	40	2464	0.000
GARP VLAN Registration Protocol	0.01%	6	360	0.000	6	360	0.000
Cisco Discovery Protocol	0.00%	1	144	0.000	1	144	0.000
Data	0.00%	1	73	0.000	1	73	0.000
Dynamic Trunking Protocol	0.00%	2	120	0.000	2	120	0.000
Internetwork Packet eXchange	0.02%	7	579	0.000	0	0	0.000
Service Advertisement Protocol	0.02%	7	579	0.000	7	579	0.000
Address Resolution Protocol	0.54%	228	13656	0.003	228	13656	0.003
Internet Protocol	96.10%	40635	18956069	3.792	0	0	0.000
User Datagram Protocol	0.18%	77	12614	0.003	0	0	0.000
NetBIOS Name Service	0.02%	9	828	0.000	9	828	0.000
NetBIOS Datagram Service	0.05%	22	5300	0.001	0	0	0.000
SMB (Server Message Block Protocol)	0.05%	22	5300	0.001	0	0	0.000
SMB MailSlot Protocol	0.05%	22	5300	0.001	0	0	0.000
Microsoft Windows Browser Protocol	0.05%	22	5300	0.001	22	5300	0.001
Domain Name Service	0.08%	34	3251	0.001	34	3251	0.001
Hypertext Transfer Protocol	0.02%	8	2608	0.001	8	2608	0.001
Common Unix Printing System (CUPS) Browsing Protocol	0.01%	4	627	0.000	4	627	0.000
Internet Group Management Protocol	0.03%	11	660	0.000	11	660	0.000
Transmission Control Protocol	95.89%	40547	18942795	3.790	32476	13058018	2.612
Hypertext Transfer Protocol	19.08%	8067	5884065	1.177	4081	671655	0.134
Line-based text data	9.42%	3985	5212253	1.043	118	33850	0.007
Hypertext Transfer Protocol	0.01%	5	1572	0.000	5	1572	0.000
Media Type: message/http	0.00%	1	157	0.000	0	0	0.000
DCE RPC	0.01%	4	712	0.000	4	712	0.000

The Ethereal Network Analyzer

File Edit Capture Display Tools Help

No.	Len	Time	Source	Destination	Protocol	Info
1	77	0.000000	24.94.186.99	pow.zing.org	DNS (UDP)	Standard query
2	77	0.010000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
3	164	0.060000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
4	70	0.070000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
5	71	0.080000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
6	161	0.120000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
7	158	0.130000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
8	77	9.990904	24.94.186.99	pow.zing.org	DNS (UDP)	Standard query
9	77	9.990904	pow.zing.org	i.got.net	DNS (UDP)	Standard query
10	148	10.090904	i.got.net	pow.zing.org	DNS (UDP)	Standard query response
11	148	10.090904	pow.zing.org	24.94.186.99	DNS (UDP)	Standard query response

DNS lookup from the server's perspective. It's interesting to note that the server issued four queries to resolve the name, and the client re-sent its query before the server could respond.

```
⊟ DNS query
  ├ Transaction ID: 0x83c8
  ⊞ Flags: 0x0000 (Standard query)
  ├ Questions: 1
  ├ Answer RRs: 0
  ├ Authority RRs: 0
  ├ Additional RRs: 0
  ⊟ Queries
    ⊟ www.brunching.com: type A, class inet
      ├ Name: www.brunching.com
      ├ Type: Host address
      └ Class: inet
```

```
0000  00 50 73 2c 44 c1 08 00  20 2b 01 05 08 00 45 00   .Ps,D... .+....E.
0010  00 3f 4b e7 00 00 40 11  84 ac ce 39 24 5a cf 6f   .?K...@. ...9$Z.o
0020  e8 17 07 f4 00 35 00 2b  18 c0 83 c8 00 00 00 01   .....5.+ ........
0030  00 00 00 00 00 00 03 77  77 77 09 62 72 75 6e 63   .......w ww.brunc
0040  68 69 6e 67 03 63 6f 6d  00 00 01 00 01            hing.com .....
```

Filter: File: dns.pcap Drops: 0

www.pcap – Ethereal

File Edit Capture Display Tools Help

No.	Length	Time	Source	Destination	Protocol	Info
16	74	7.034102	10.1.1.85	www.brunching.com	TCP	1028 > www [SYN] Seq=426174114 Ack=
17	70	7.096750	www.brunching.com	10.1.1.85	TCP	www > 1028 [SYN, ACK] Seq=395957598
18	66	7.096850	10.1.1.85	www.brunching.com	TCP	1028 > www [ACK] Seq=426174115 Ack=
19	356	7.097373	10.1.1.85	www.brunching.com	HTTP	GET / HTTP/1.0
20	66	7.163414	www.brunching.com	10.1.1.85		
21	1434	7.433255	www.brunching.com	10.1.1.85		
22	66	7.433328	10.1.1.85	www.brunch		
24	1434	7.441772	www.brunching.com	10.1.1.85		
25	66	7.447430	10.1.1.85	www.brunch		
29	1434	7.518176	www.brunching.com	10.1.1.85		
30	96	7.518236	www.brunching.com	10.1.1.85		
31	66	7.537425	10.1.1.85	www.brunch		
88	1434	8.029938	www.brunching.com	10.1.1.85		
89	641	8.031954	www.brunching.com	10.1.1.85		
90	998	8.037775	www.brunching.com	10.1.1.85		
91	66	8.037891	10.1.1.85	www.brunch		

```
▷ Frame 31 (66 on wire, 66 captured)
▷ Ethernet II
▽ Internet Protocol
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00
    Total Length: 52
    Identification: 0x0063
  ▷ Flags: 0x04
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0xd51c (correct)
    Source: 10.1.1.85 (10.1.1.85)
    Destination: www.brunching.com (208.37.137.201
▽ Transmission Control Protocol, Src Port: 1028 (10
    Source port: 1028 (1028)
    Destination port: www (80)
    Sequence number: 426174405
    Acknowledgement number: 3959580121
    Header length: 32 bytes
  ▷ Flags: 0x0010 (ACK)
```

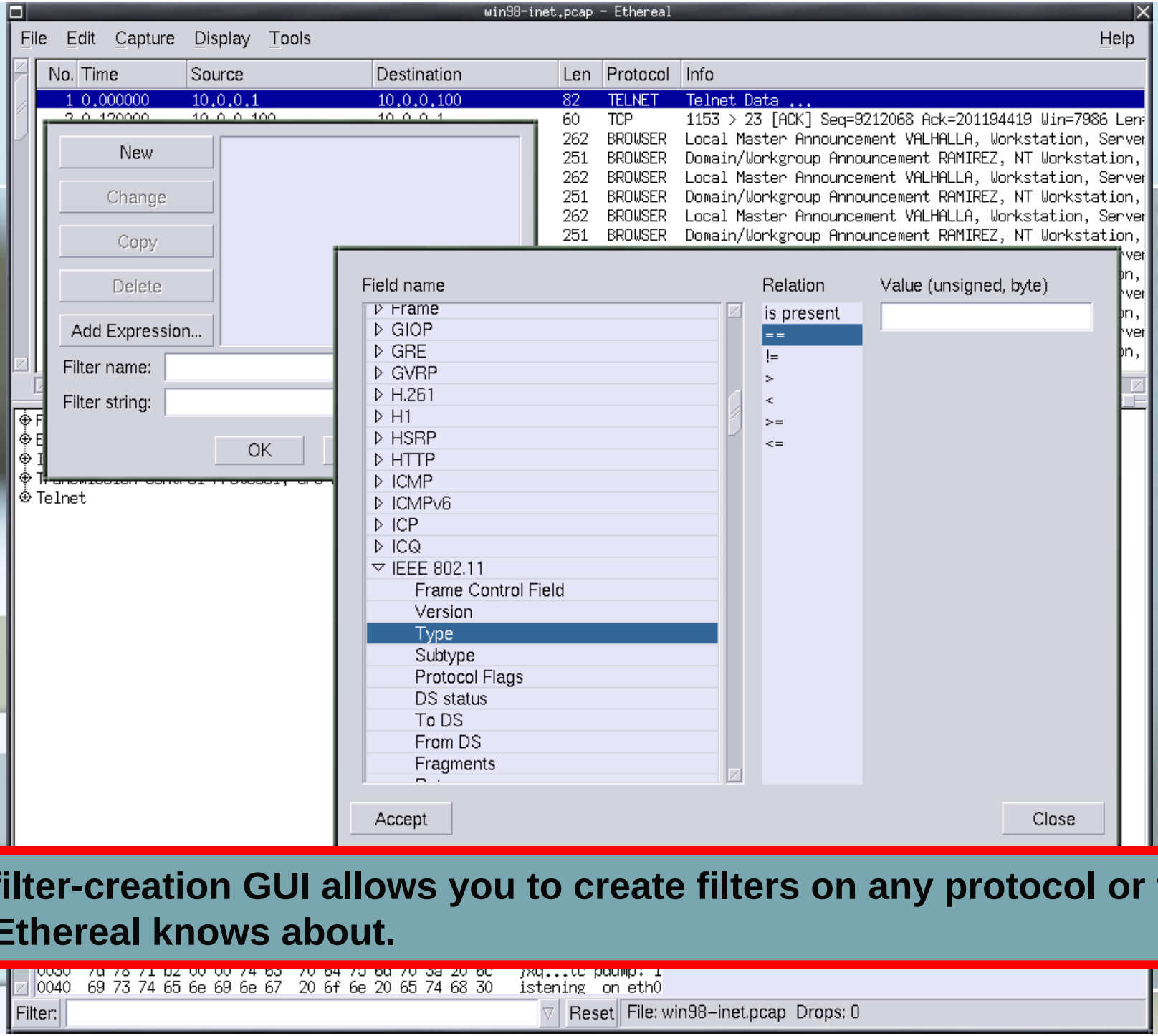
Contents of TCP stream

```
GET / HTTP/1.0
Connection: Keep-Alive
User-Agent: Mozilla/4.75 [en] (X11; U; Linux 2.2.17-crunch i686)
Host: www.brunching.com
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

HTTP/1.1 200 OK
Date: Fri, 27 Apr 2001 18:47:18 GMT
Server: Apache/1.3.12 (Unix)
Set-Cookie: Apache=nis132.kc.netisinc.com.24820988397239143; path=/; expires=Mon, 25-Apr-11 18:47:18 G
MT
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<META name="description" CONTENT="Comedy, pure and simple as a hammer
to the forebrain.">
<META name="keywords" CONTENT="comedy, humor, jokes, fun, satire, parody,
movie reviews, ratings, funny, joke">
<LINK REL=StyleSheet HREF="/style.css" TYPE="text/css" MEDIA=screen>
<TITLE>The Brunching Shuttlecocks — Comedy with a "Runch"</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#0000FF" VLINK="#800080" ALINK="#000080">
<CENTER>
<TABLE WIDTH="65%" BORDER=0>
<TR>
<TD>
<BR>
<!— Copyright (C) 1998, 1999 Engage Media Corporation. All Rights Reserved —>
<IFRAME WIDTH=468 HEIGHT=60 SRC='http://ad-adex3.flycast.com/server/iframe/TheBrunchingShuttlecocks/Ge
neralHumor/46502' SCROLLING='no' MARGINWIDTH=0 MARGINHEIGHT=0 FRAMEBORDER=0 VSPACE=0 HSPACE=0>
<A TARGET='_top' HREF='http://ad-adex3.flycast.com/server/click/TheBrunchingShuttlecocks/GeneralHumor/
46502'>
<IMG BORDER=0 WIDTH=468 HEIGHT=60 SRC='http://ad-adex3.flycast.com/server/img/TheBrunchingShuttlecocks
```

Follow TCP Stream" item under the "Analyze" menu allows you to inspect the ASCII contents of a TCP data stream in a separate window. This can be invaluable for tracking down HTTP, SMTP, and POP server problems.



The filter-creation GUI allows you to create filters on any protocol or field that Ethereal knows about.

Questions or Comments