

Lecture-03

Network Tools and Protocol Analyzer



Muhammad Yousif

Lecturer

Department of Computer Science(CS)

Minhaj University

myousif.cs@mul.edu.pk



Topic

- **Trace root**
- ***whois***
- **Network Tools**
- **Packet Sniffers Tools**

Trace root

- **Traceroute** is a TCP/IP utility which allows the user to determine the route packets take to reach a particular host.
- Traceroute works by increasing the " **time to live(TTL)** " value of each successive packet sent. The first packet has a TTL value of one, the second two, and so on. When a packet passes through a host, the host decrements the TTL value by one and forwards the packet to the next host.
- When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender.
- The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

TraceRoute example

TraceRoute to 60.54.190.2 [54.60.in-addr.arpa]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	12	8	9	72.249.0.65	-
2	6	6	7	8.9.232.73	xe-5-3-0.edge3.dallas1.level3.net
3	7	7	11	4.68.19.133	ae-33-89.car3.dallas1.level3.net
4	17	46	20	4.68.63.162	-
5	9	12	12	66.198.2.37	if-5-0-0-31.core2.dtx-dallas.as6453.net
6	43	43	42	209.58.33.9	if-15-0-0-959.mcore5.laa-losangeles.as6453.net
7	42	42	42	209.58.33.22	if-10-0-0-999.mcore3.laa-losangeles.as6453.net
8	317	331	320	216.6.84.50	ix-13-0-0.mcore3.laa-losangeles.as6453.net
9	320	319	317	219.93.174.81	-
10	322	319	318	58.27.124.53	-
11	344	325	318	58.27.113.36	-
12	326	328	319	210.187.135.6	bat-odsy02-srp1-0.tm.net.my
13	323	327	329	203.106.206.194	-
14	325	324	322	58.27.100.78	-
15	Timed out	Timed out	Timed out		-
16	Timed out	325	332	60.54.190.1	54.60.in-addr.arpa
17	327	332	328	60.54.190.2	54.60.in-addr.arpa

Trace complete



What is whois?

- **WHOIS** is a query/response protocol which is widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet.
- The WHOIS system originated as a method that system administrators could use to look up information to contact other IP address or domain name administrators



Uses of Whois

- Supporting the security and stability of the Internet by providing contact points for network operators and administrators, including ISPs, and certified computer incident response teams.
- Allowing users to determine the availability of domain names.



Uses of Whois

- Contributing to user confidence in the Internet as a reliable and efficient means of information and communication and as an important tool for promoting digital inclusion, e-commerce and other legitimate uses by helping users identify persons or entities responsible for content and services online.
- Assisting businesses, other organizations and users in combating fraud, complying with relevant laws and safeguarding the interests of the public.



Links

- <http://webtools.live2support.com>
- <http://whois.domaintools.com>
- <http://www.traceroute.org>
- <http://network-tools.com>



Wireshark

Network Protocol Analyzer



Overview

■ Protocol Analysis

- Verify Correctness
- Analyze performance
- Better understanding of existing protocols
- Optimization and debugging of new protocols

■ Tools

- tcpdump & tshark
- Wireshark



Network Protocol Examples

- Defines the rules of exchange between a pair (or more) machines over a communication network
- HTTP (Hypertext Transfer Protocol)
 - Defines how web pages are fetched and sent across a network
- TCP (Transmission Control Protocol)
 - Provides reliable, in-order delivery of a stream of bytes



Protocol Analysis

- Verify correctness
- Debug/detect incorrect behavior
- Analyze performance
- Gain deeper understanding of existing protocols by “seeing” how they behave in actual use



What is Wireshark?

- Wireshark is a network packet/protocol analyzer.
 - A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- Wireshark is perhaps one of the best open source packet analyzers available today for **UNIX** and **Windows**.



What is Wireshark?

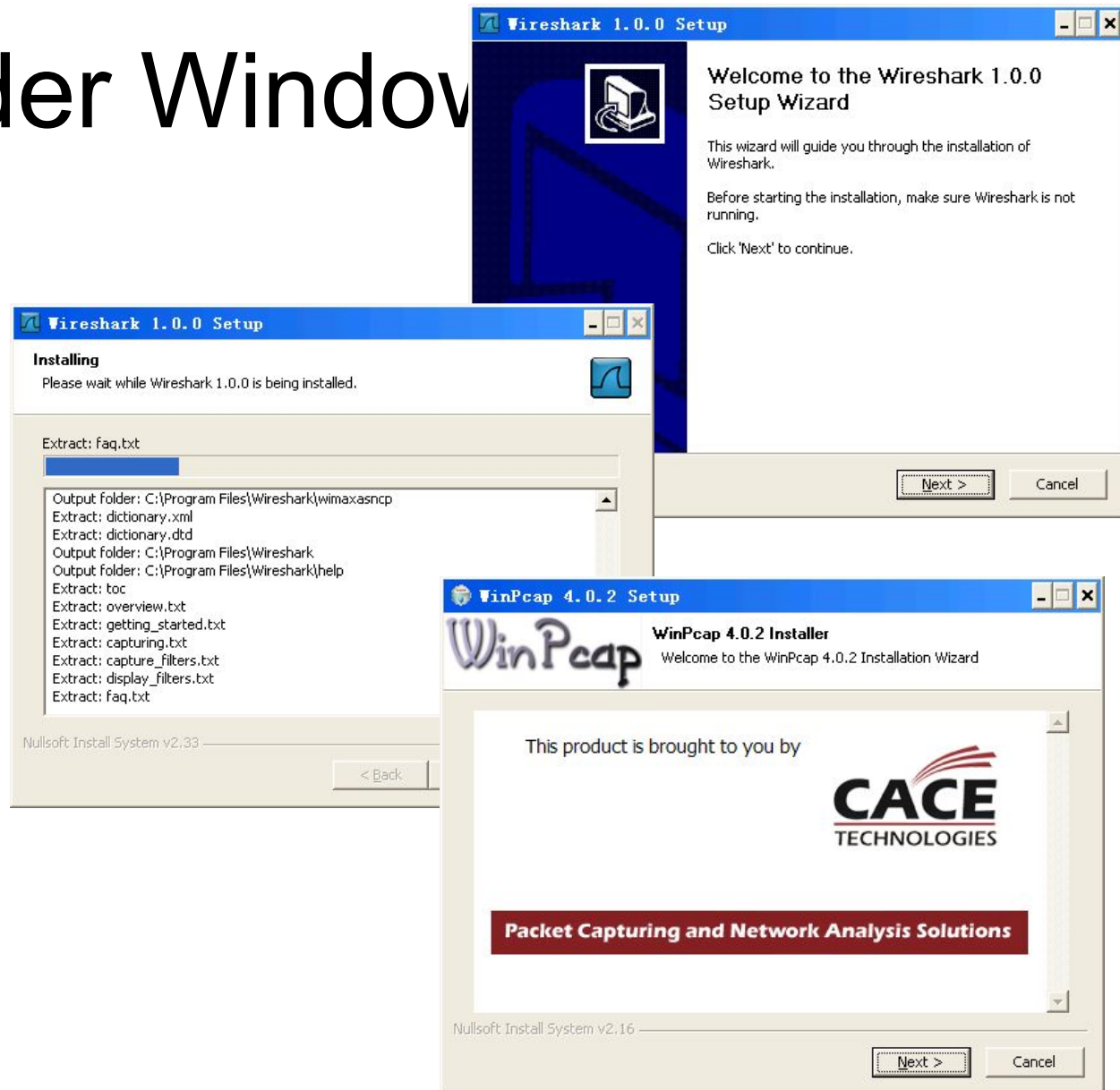
- Wireshark's wireless analysis features have grown to be a very powerful tool for troubleshooting and analyzing wireless networks.
- With Wireshark's display filters and powerful protocol dissector features, you can sift through large quantities of wireless traffic
- Without a doubt, Wireshark is a powerful assessment and analysis tool for wireless networks that should be a part of every auditor, engineer, and consultant toolkit.

Some intended purposes

- network administrators use it to **troubleshoot network problems**
- network security engineers use it to **examine security problems**
- developers use it to **debug protocol implementations**
- people use it to **learn network protocol internals**
- Wireshark isn't an intrusion detection system.
- Wireshark will not manipulate things on the network, it will only "measure" things from it.

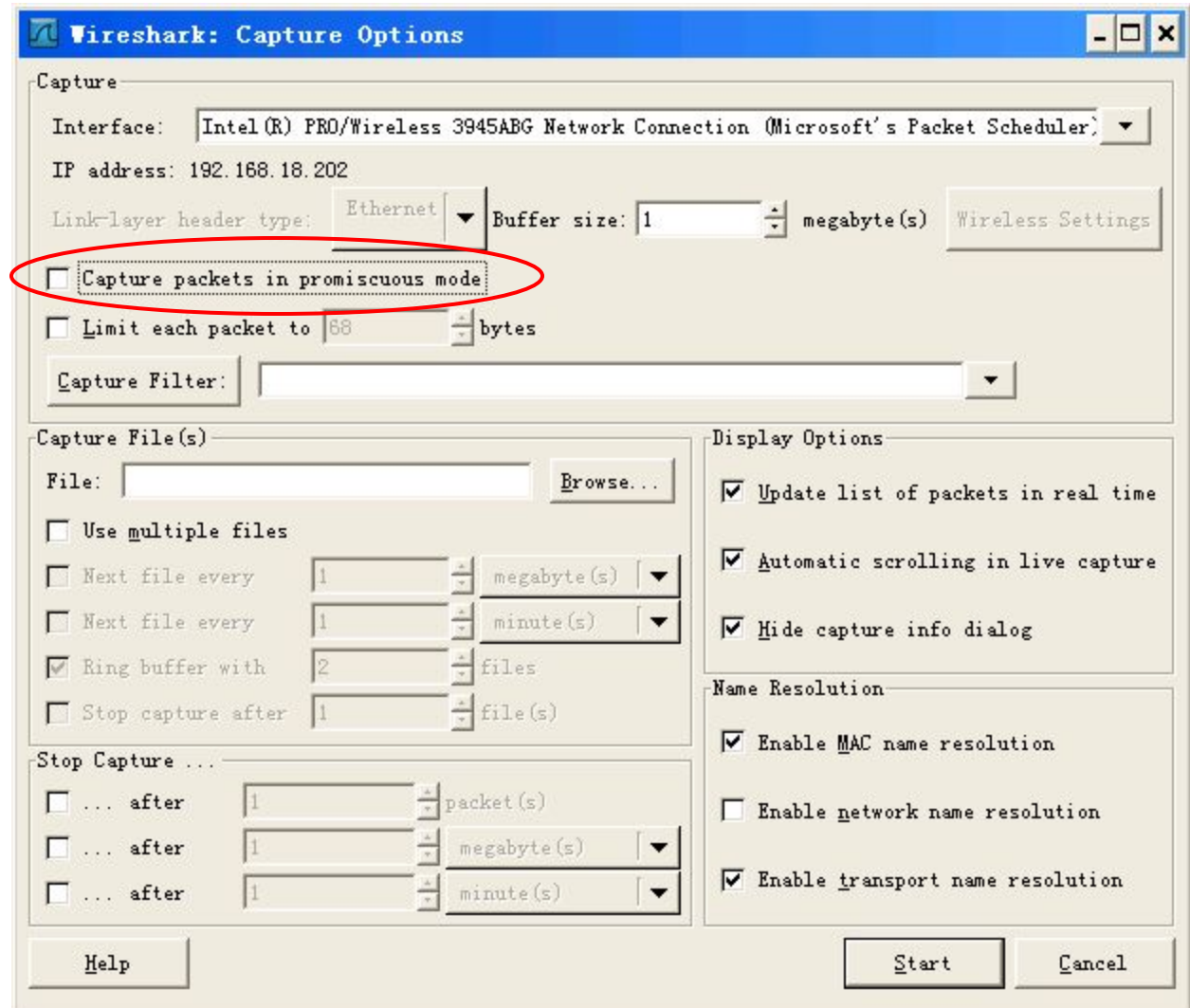
Install under Windows

- Download
- Install



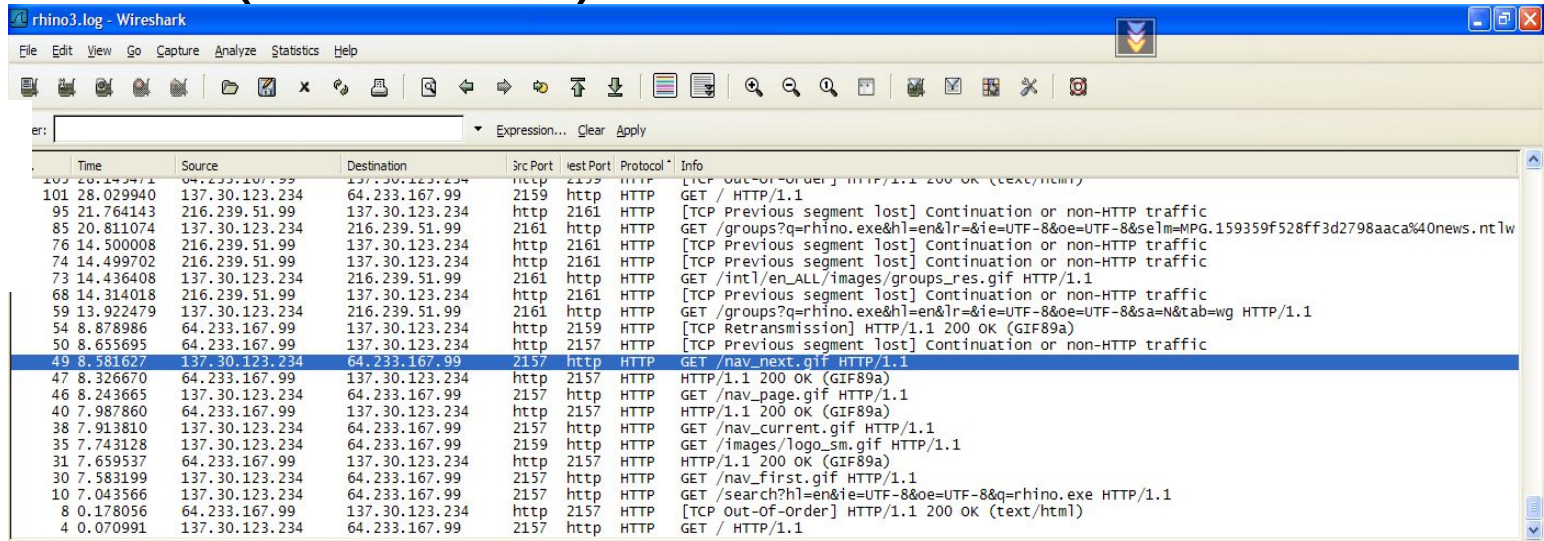
Configuration

This checkbox allows you to specify that Wireshark should put the interface in **promiscuous** mode when capturing. If you do not specify this, Wireshark will only capture the packets going to or from your computer (not all packets on your LAN segment).



Wireshark (Ethereal)

Packet
listing

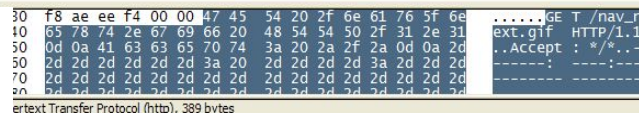


Time	Source	Destination	Src Port	Dest Port	Protocol	Info
101.28.029940	137.30.123.234	64.233.167.99	2159	http	HTTP	[TCP Out-of-Order] HTTP/1.1 200 OK (text/html)
95.21.764143	216.239.51.99	137.30.123.234	2161	HTTP	HTTP	GET / HTTP/1.1
85.20.811073	137.30.123.234	216.239.51.99	2161	HTTP	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
76.14.500008	216.239.51.99	137.30.123.234	2161	HTTP	HTTP	GET /groups?q=rhino.exe&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=MPG.159359f528ff3d2798aaca%40news.ntlw
74.14.499702	216.239.51.99	137.30.123.234	2161	HTTP	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
73.14.436408	137.30.123.234	216.239.51.99	2161	HTTP	HTTP	GET /intl/en_ALL/images/groups_res.gif HTTP/1.1
68.14.314018	216.239.51.99	137.30.123.234	2161	HTTP	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
59.13.922479	137.30.123.234	216.239.51.99	2161	HTTP	HTTP	GET /groups?q=rhino.exe&hl=en&lr=&ie=UTF-8&oe=UTF-8&sa=N&tab=wg HTTP/1.1
54.8.878986	64.233.167.99	137.30.123.234	2159	HTTP	HTTP	[TCP Retransmission] HTTP/1.1 200 OK (GIF89a)
50.8.655695	64.233.167.99	137.30.123.234	2157	HTTP	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
49.8.581627	137.30.123.234	64.233.167.99	2157	http	HTTP	GET /nav_next.gif HTTP/1.1
47.8.326670	64.233.167.99	137.30.123.234	2157	HTTP	HTTP	HTTP/1.1 200 OK (GIF89a)
46.8.243665	137.30.123.234	64.233.167.99	2157	HTTP	HTTP	GET /nav_page.gif HTTP/1.1
40.7.987860	64.233.167.99	137.30.123.234	2157	HTTP	HTTP	HTTP/1.1 200 OK (GIF89a)
38.7.913810	137.30.123.234	64.233.167.99	2157	http	HTTP	GET /nav_current.gif HTTP/1.1
35.7.743128	137.30.123.234	64.233.167.99	2159	http	HTTP	GET /images/logo_sm.gif HTTP/1.1
31.7.659537	64.233.167.99	137.30.123.234	2157	HTTP	HTTP	HTTP/1.1 200 OK (GIF89a)
30.7.583199	137.30.123.234	64.233.167.99	2157	http	HTTP	GET /nav_first.gif HTTP/1.1
10.7.043566	137.30.123.234	64.233.167.99	2157	HTTP	HTTP	GET /search?hl=en&ie=UTF-8&oe=UTF-8&q=rhino.exe HTTP/1.1
8.0.178056	64.233.167.99	137.30.123.234	2157	HTTP	HTTP	[TCP Out-of-Order] HTTP/1.1 200 OK (text/html)
4.0.070991	137.30.123.234	64.233.167.99	2157	http	HTTP	GET / HTTP/1.1

Detailed
packet
data at
various
protocol
levels

Frame 49 (443 bytes on wire, 443 bytes captured)
Ethernet II, Src: AppleCom.cc:57:92 (00:03:93:cc:57:92), Dst: Cisco_41:a8:40 (00:0d:ed:41:a8:40)
Internet Protocol, Src: 137.30.123.234 (137.30.123.234), Dst: 64.233.167.99 (64.233.167.99)
Transmission Control Protocol, Src Port: 2157 (2157), Dst Port: http (80), Seq: 2012, Ack: 20812, Len: 389
Source port: 2157 (2157)
Destination port: http (80)
Sequence number: 2012 (relative sequence number)
[Next sequence number: 2401 (relative sequence number)]
Acknowledgement number: 20812 (relative ack number)
Header length: 20 bytes
[X] Flags: 0x0018 (PSH, ACK)
Window size: 63662
Checksum: 0xeeef4 [incorrect, should be 0x28d3 (maybe caused by checksum offloading?)]
Hypertext Transfer Protocol
[X] GET /nav_next.gif HTTP/1.1\r\n
Accept: */*\r\n
-----\r\n
Accept-Language: en-us\r\n
-----\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; .NET CLR 1.1.4322)\r\n
Host: www.google.com\r\n
Connection: Keep-Alive\r\n
Cookie: PREF=ID=269e53562e69c3c5:TM=1082665356:LM=1083170916:TB=3:S=53_bmTAWajyv1FX0\r\n
\r\n

Raw data



```
30 f8 ae ee f4 00 00 47 45 54 20 2f 6e 61 76 5f 6e .....GE T /nav_n
40 65 78 74 2e 67 69 66 20 48 54 54 50 2f 31 2e 31 ext.gif HTTP/1.1
50 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 2d ..Accept: */*..
50 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
70 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
80 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
```

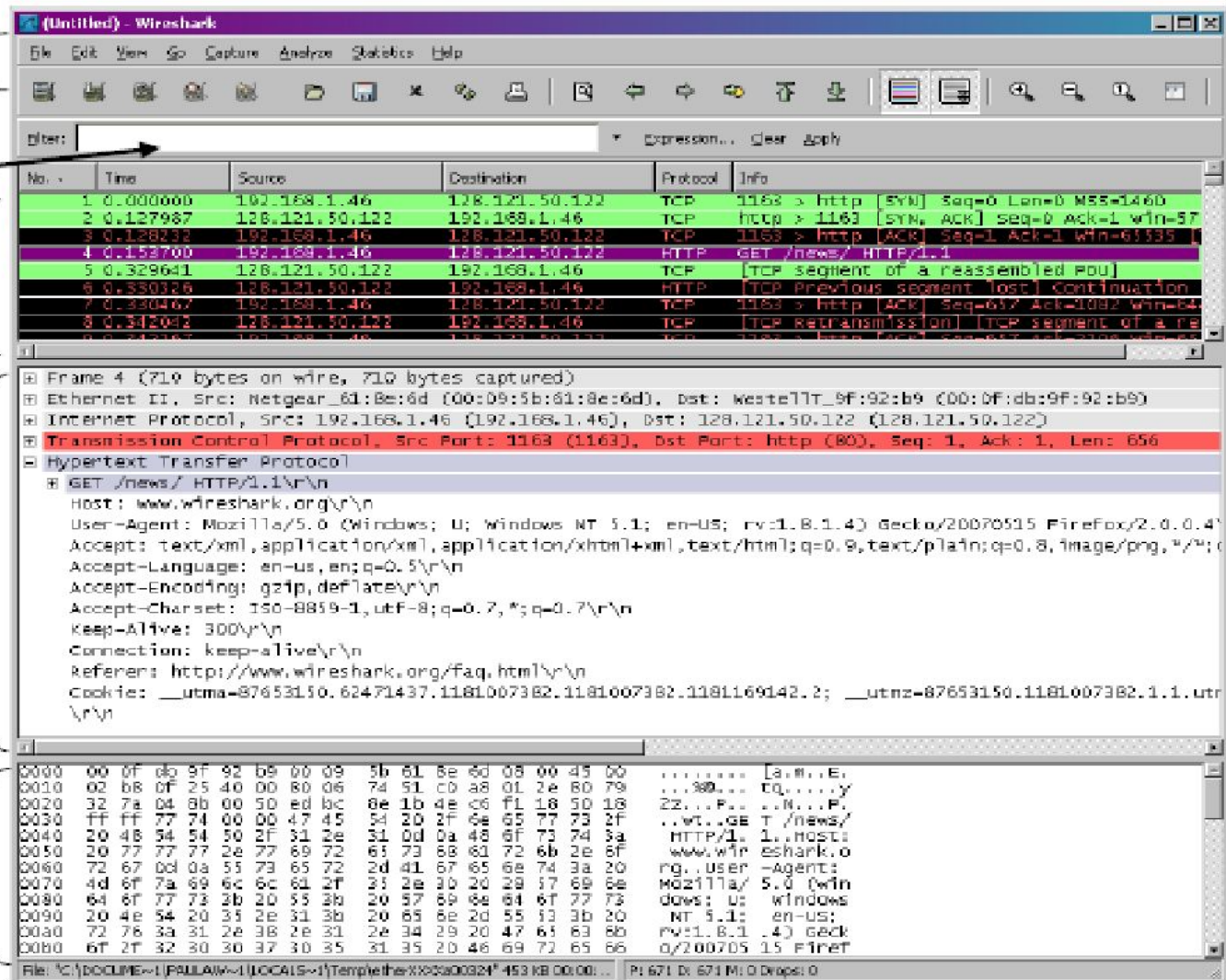
command
menus

display filter
specification

listing of
captured
packets

details of
selected
packet
header

packet content
in hexadecimal
and ASCII



Download

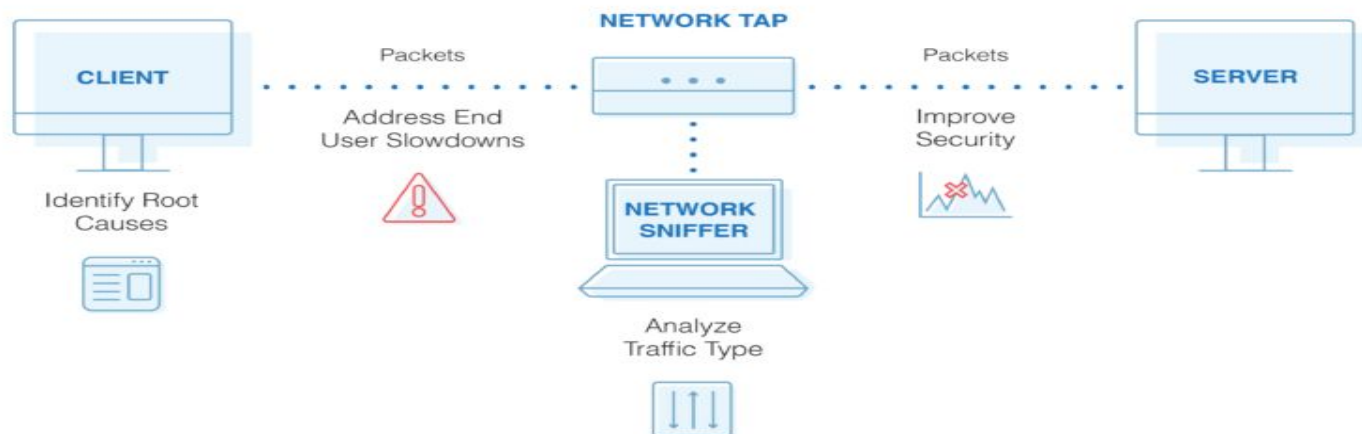
- You can download the software and document at <http://www.wireshark.org/>



Packet Sniffers Tools

- A packet sniffer can help you target new resources when expanding your network capacity, manage your bandwidth, increase efficiencies, ensure delivery of business services, enhance security, and improve end-user experience.

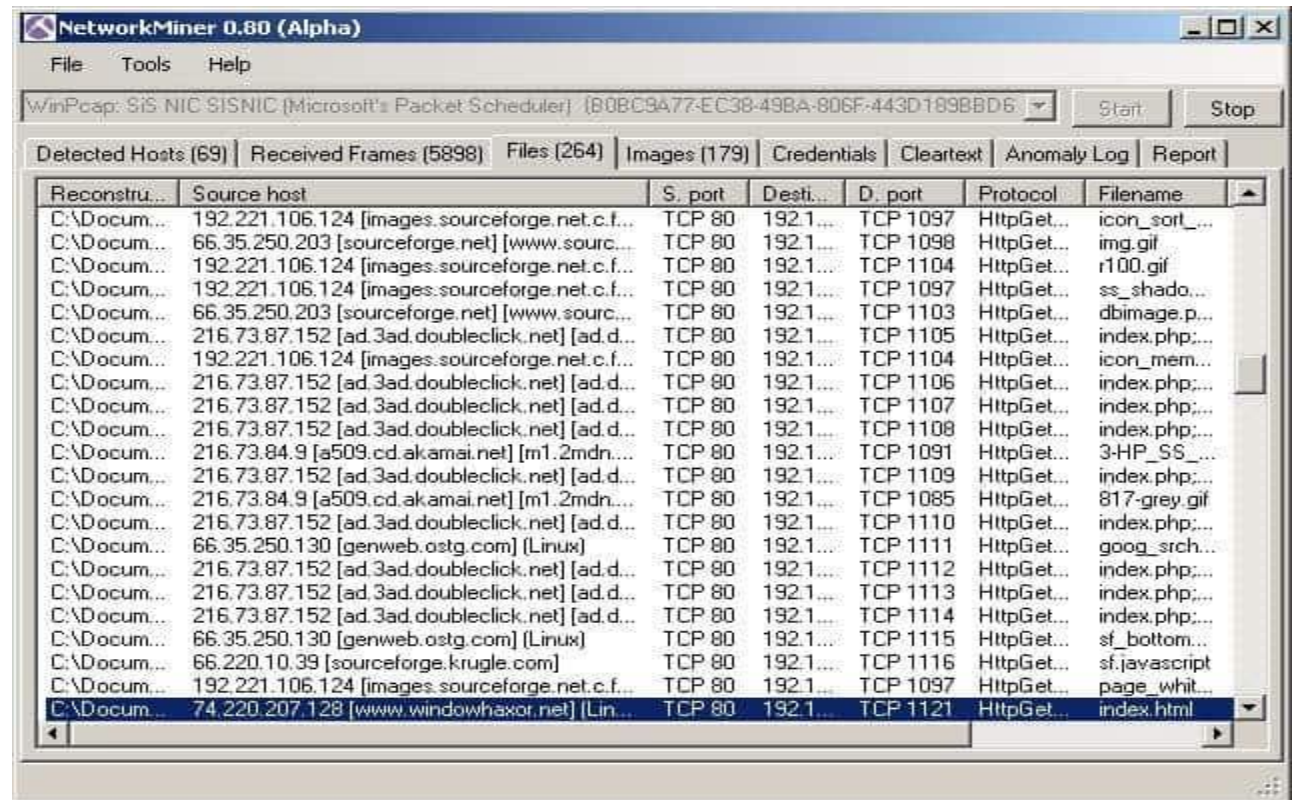
Benefits of Packet Sniffing



Packet Sniffers Tools

■ Network Miner

- Network Miner for Windows makes network analysis very simple and can detect the host-name as well as the OS and open ports of network hosts through packet sniffing.



Fiddler

- Fiddler is not technically made for packet sniffing but can be used either way. It can manipulate and log HTTP/HTTPS traffic.

The screenshot displays the Fiddler Web Debugger interface. The main window shows a list of intercepted HTTP requests. The selected request (number 5) is from fonts.googleapis.com, with a status of 200 and a content type of text/css. The right-hand pane shows the details of the selected request, including the Request Headers, Cache, Client, Cookies / Login, and Response body.

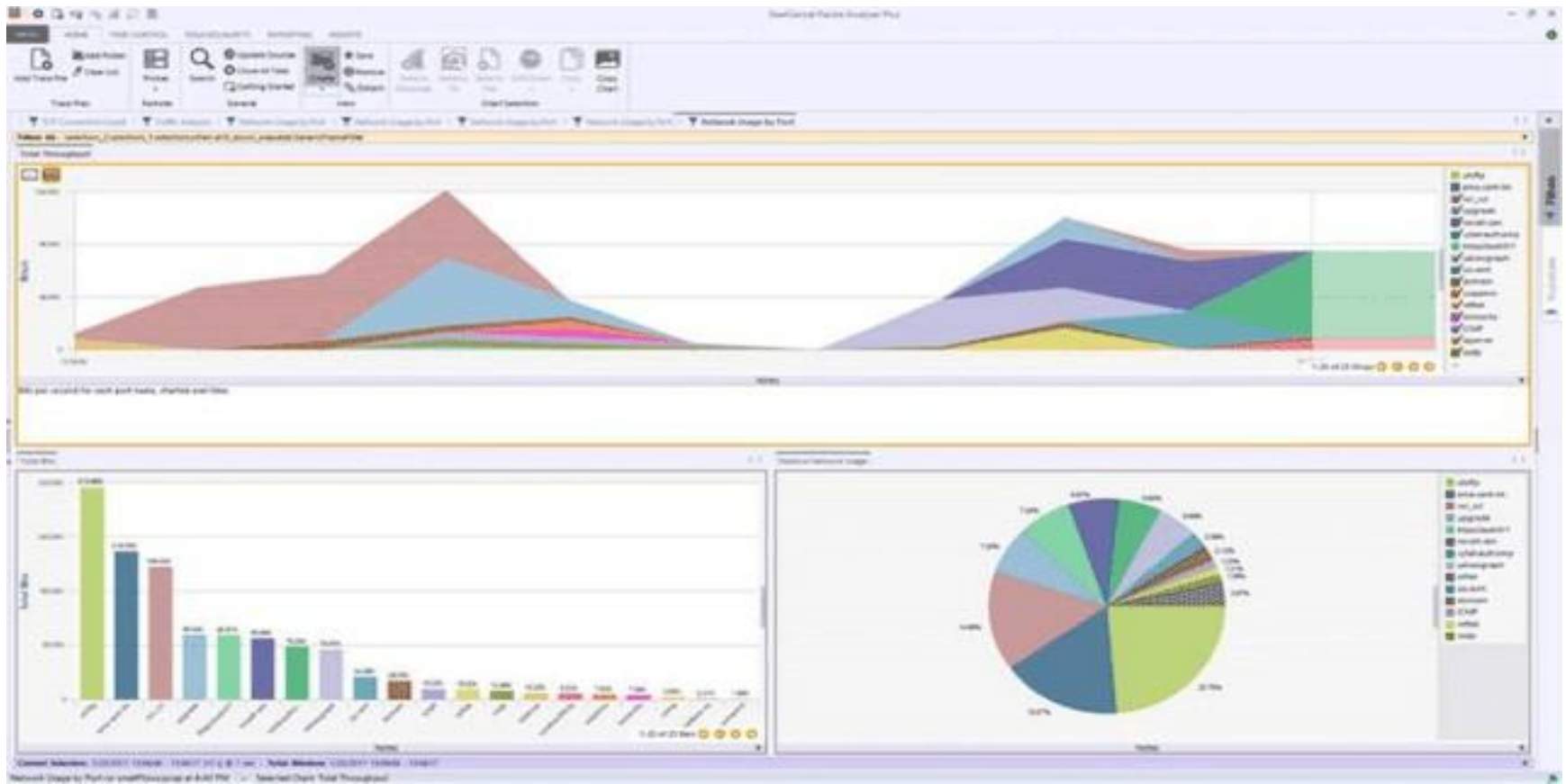
#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTP	fiddler2.com	/	6,987	no-cac...	text/html; c...	chrom
2	304	HTTP	fiddler2.com	/Telerik.Web.UI.WebReso...	0	public, ...		chrom
3	304	HTTP	fiddler2.com	/Sitefinity/WebsiteTempla...	0	private	text/css	chrom
4	304	HTTP	fiddler2.com	/Sitefinity/WebsiteTempla...	0	private	text/css	chrom
5	200	HTTP	fonts.googleapis.com	/css?family=Signika:400,3...	321	private...	text/css	chrom
6	304	HTTP	fiddler2.com	/Sitefinity/WebsiteTempla...	0	private	text/css	chrom
7	304	HTTP	fiddler2.com	/WebResource.axd?d=TG...	0	public; ...		chrom
8	304	HTTP	fiddler2.com	/ScriptResource.axd?d=q...	0	public; ...		chrom
9	304	HTTP	fiddler2.com	/ScriptResource.axd?d=H...	0	public; ...		chrom
10	304	HTTP	fiddler2.com	/Images/default-source/d...	0	private		chrom
11	304	HTTP	platform.twitter.com	/widgets.js	0	public, ...	application/...	chrom
12	200	HTTP	Tunnel to	apis.google.com:443	0			chrom
13	304	HTTP	www.google-analyt...	/ga.js	0	Expires...		chrom
14	304	HTTP	connect.facebook.net	/en_US/all.js	0	public, ...	application/...	chrom
15	304	HTTP	themes.googleuser...	/static/fonts/signika/v3/_...	0	Expires...		chrom
16	304	HTTP	themes.googleuser...	/static/fonts/signika/v3/ko...	0	Expires...		chrom
17	304	HTTP	themes.googleuser...	/static/fonts/signika/v3/F...	0	Expires...		chrom
18	304	HTTP	themes.googleuser...	/static/fonts/signika/v3/7...	0	Expires...		chrom
19	200	HTTP	Tunnel to	r.twimg.com:443	0			chrom
20	200	HTTP	www.google-analyt...	/__utm.gif?utmwv=5.4.2...	35	private...	image/gif	chrom
21	200	HTTP	p.twitter.com	/t.gif?_=1370471798674...	43	no-cache	image/gif	chrom
22	304	HTTP	cdn.api.twitter.com	/1/urls/count.json?url=htl...	0	must+...	application/...	chrom

Request Headers
GET / HTTP/1.1
Cache
Cache-Control: max-age=0
Client
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.
Cookies / Login
☒ Cookie
__utma=1.846454601.1370469291.1370469291.1370471791.2
__utmb=1.1.10.1370471791

Response body: 6,987 bytes.
☒ Chunked Transfer-Encoding
HTTP Compression

Steel Central Packet Analyzer

- Steel Central Packet Analyzer offers an interactive graphical user interface that helps you identify the root network problem using a wide selection of pre-defined analysis views.
- It provides packet sniffing down to the bit level through Packet Analyzer Plus' full integration with Wireshark.



Colasoft Capsa

- It is a Windows packet capture tool boasting free, standard, and enterprise editions.
- The free version is designed for Ethernet sniffing and can monitor 10 IP addresses and approximately 300 protocols.
- While the free version is fairly limited in scope, it offers some graphical analysis of the network traffic it captures and can even be used to set alerts.





Q&A

