VirginiaTech
Invent the Future

Networking Tools

ECE 4564 - Network Application Design

Dr. William O. Plymale

ece
BRADLEY DEPARTMENT
of ELECTRICAL & COMPUTER ENGINEERING

Topics

- Unix Network Commands
- Network Tools
- Python Network Code

Unix Network Commands

- ping
- netstat
- nslookup
- dig
- traceroute
- vnstat
- nmap
- nload
- tcpdump

Linux Howto's

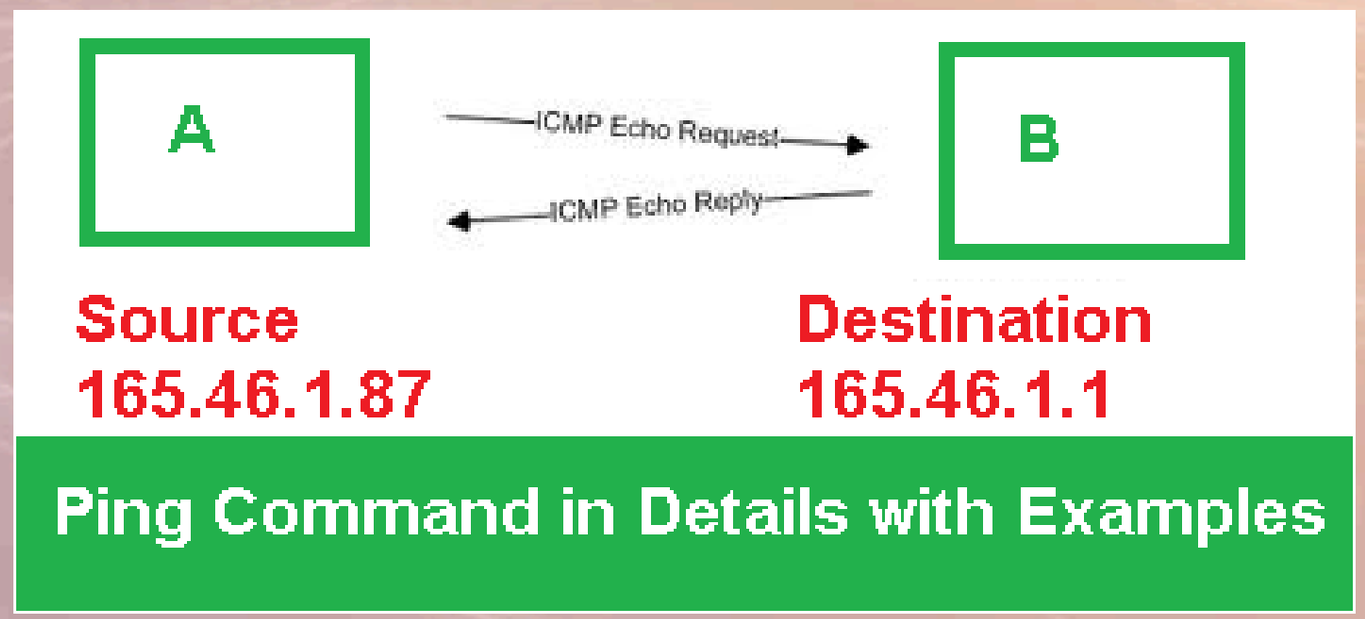
Tecmint

Linux Network Config and Troubleshooting

ping

Ping is a computer network administration utility used

- To test the reachability of a host on an Internet Protocol (IP) network
- To measure the round-trip time for messages sent from the originating host to a destination computer
- Name comes from active sonar terminology which sends a pulse of sound and listens for the echo to detect objects underwater



netstat

netstat (network statistics) is a command-line tool that

- displays network connections (both incoming and outgoing)
- routing tables
- network interfaces
- network protocol statistics

http://www.tecmint.com/20-netstat-commands-for-linux-network-management/

DNS is

- The “Domain Name System”
- What Internet users use to reference anything by name on the Internet
- The mechanism by which Internet software translates names to attributes such as addresses

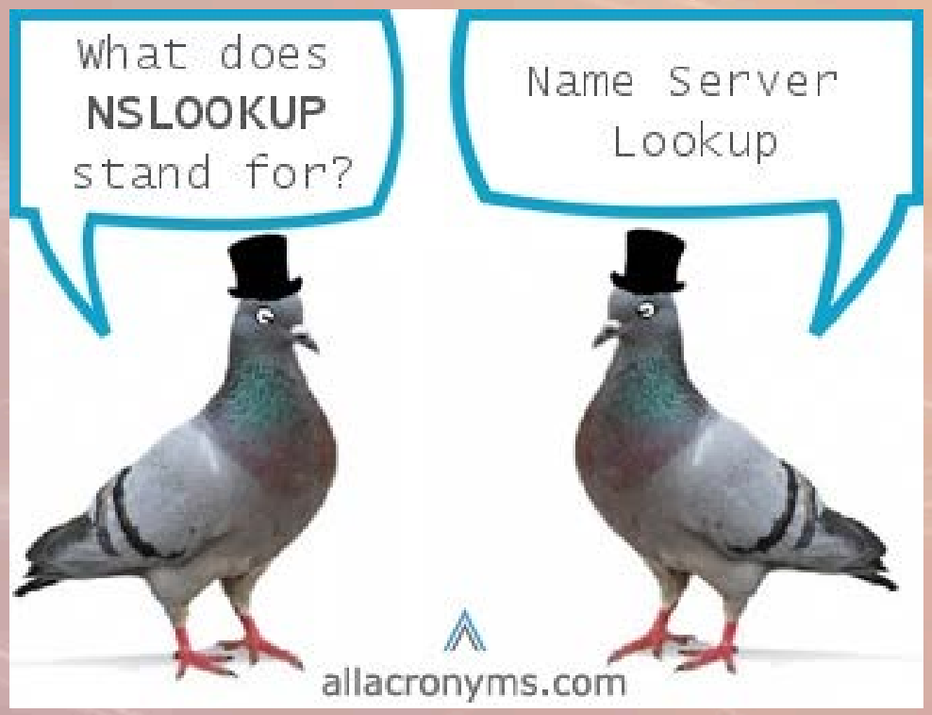
DNS as a Lookup Mechanism

- Users generally prefer names to numbers
- Computers prefer numbers to names
- DNS provides the mapping between the two
  - I have “x”, give me “y”

nslookup

nslookup is a network administration utility used

- to query DNS (Domain Name System) about
  - IP address mapping
  - domain name
  - DNS related record (RR).
- It is also used to test and troubleshoot problems related to DNS.



http://www.tecmint.com/8-linux-nslookup-commands-to-troubleshoot-dns-domain-name-server/

dig

dig (Domain Information Groper) is a network administration command-line tool for

- querying Domain Name System (DNS) name servers.
- for verifying and troubleshooting DNS problems
- to perform DNS lookups
- dig is part of the BIND domain name server software suite.
- dig command replaces older tool such as nslookup

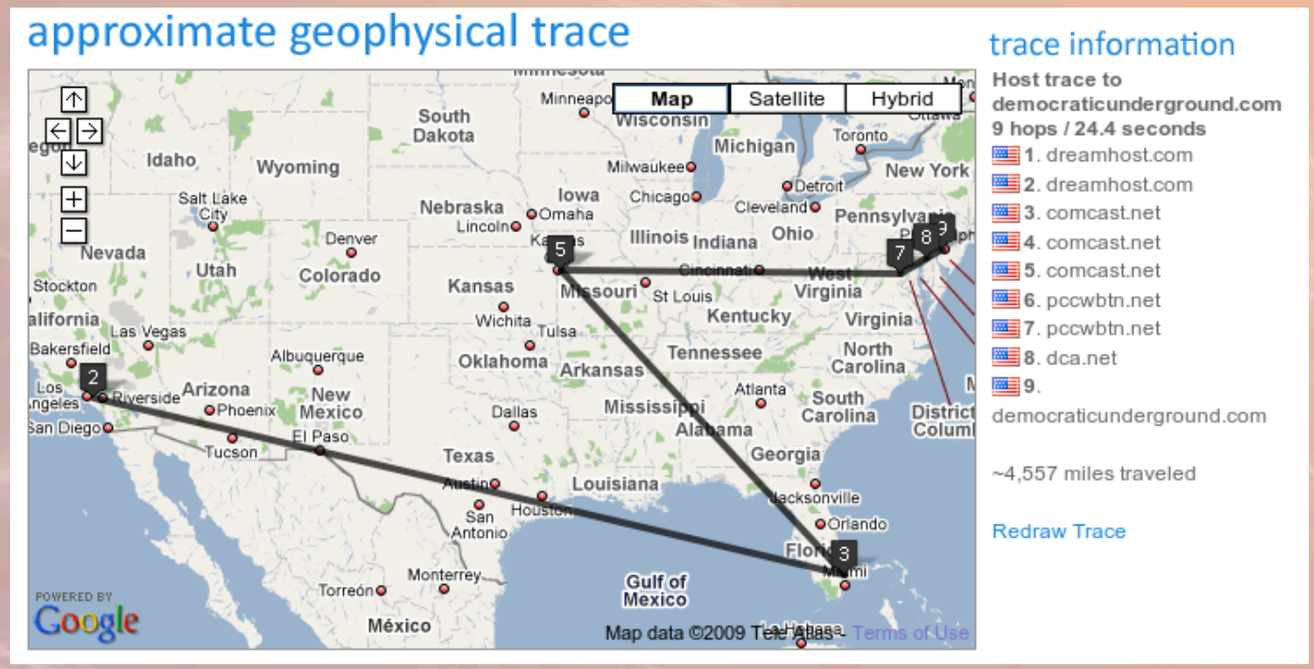
http://www.tecmint.com/10-linux-dig-domain-information-groper-commands-to-query-dns/

traceroute

traceroute is a computer network diagnostic tool for

- displaying the route (path) between two hosts
- measuring transit delays of packets across an Internet Protocol (IP) network.

The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path)



vnStat

vnstat is a console-based network traffic monitor.

It keeps a log of hourly, daily and monthly network traffic for the selected interface(s).

It isn't a packet sniffer.

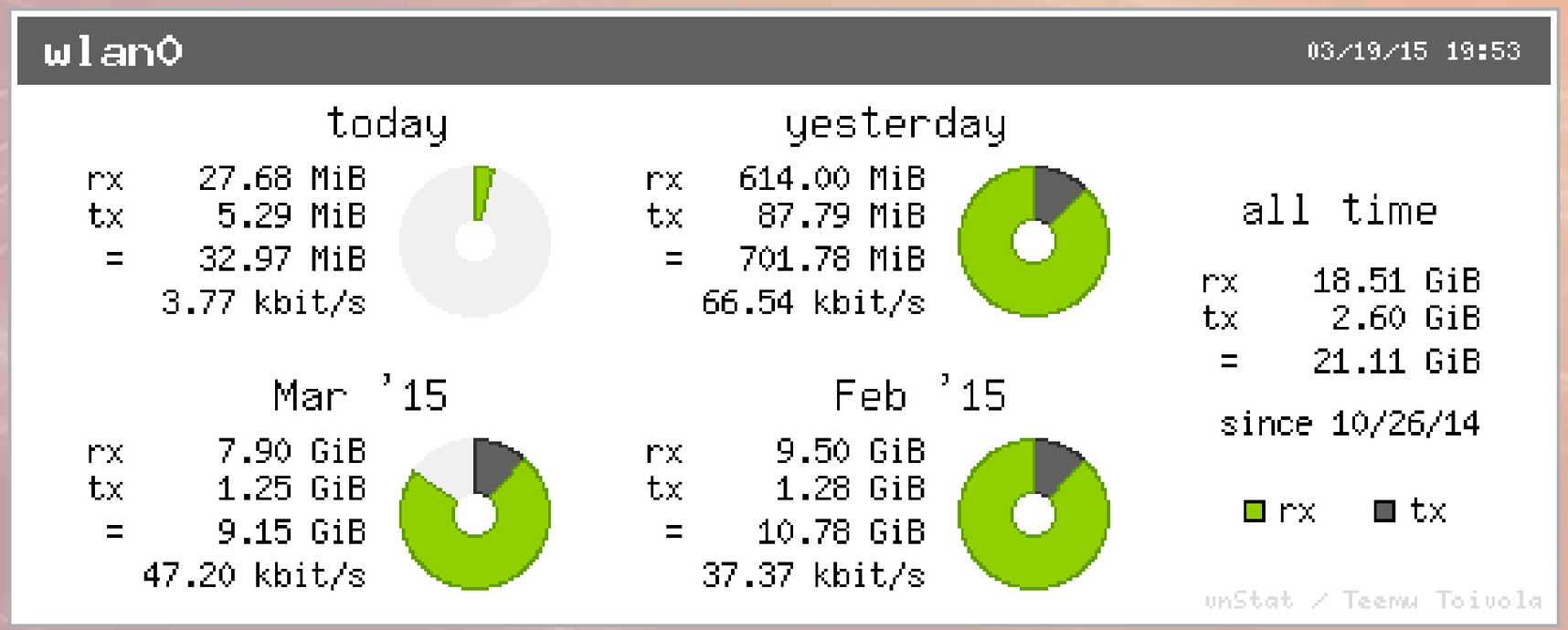
The traffic information is analyzed from the proc and sys filesystems.

vnstat can be used even without root permissions on most systems.

https://www.howtoforge.com/tutorial/vnstat-network-monitoring-ubuntu/

vnStati

- vnStati is used to produce graphical images representing the network traffic as graphs.
-
- It takes the required information to create graphs from vnStat and stores it in the specified location.

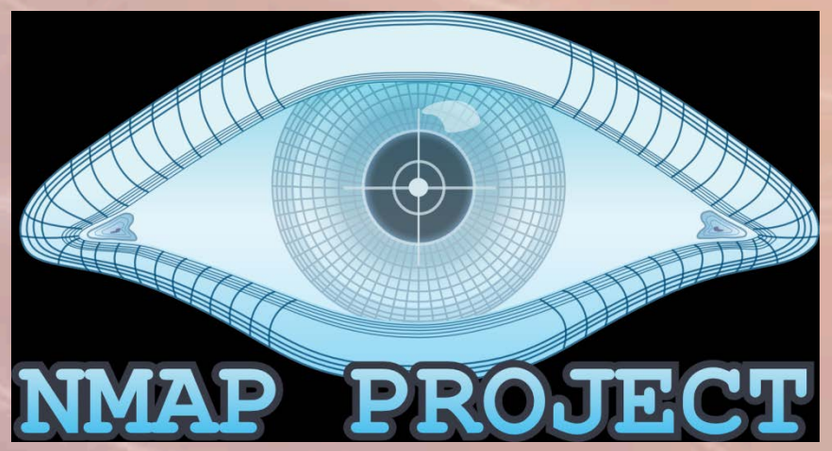


nmap

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

Useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics



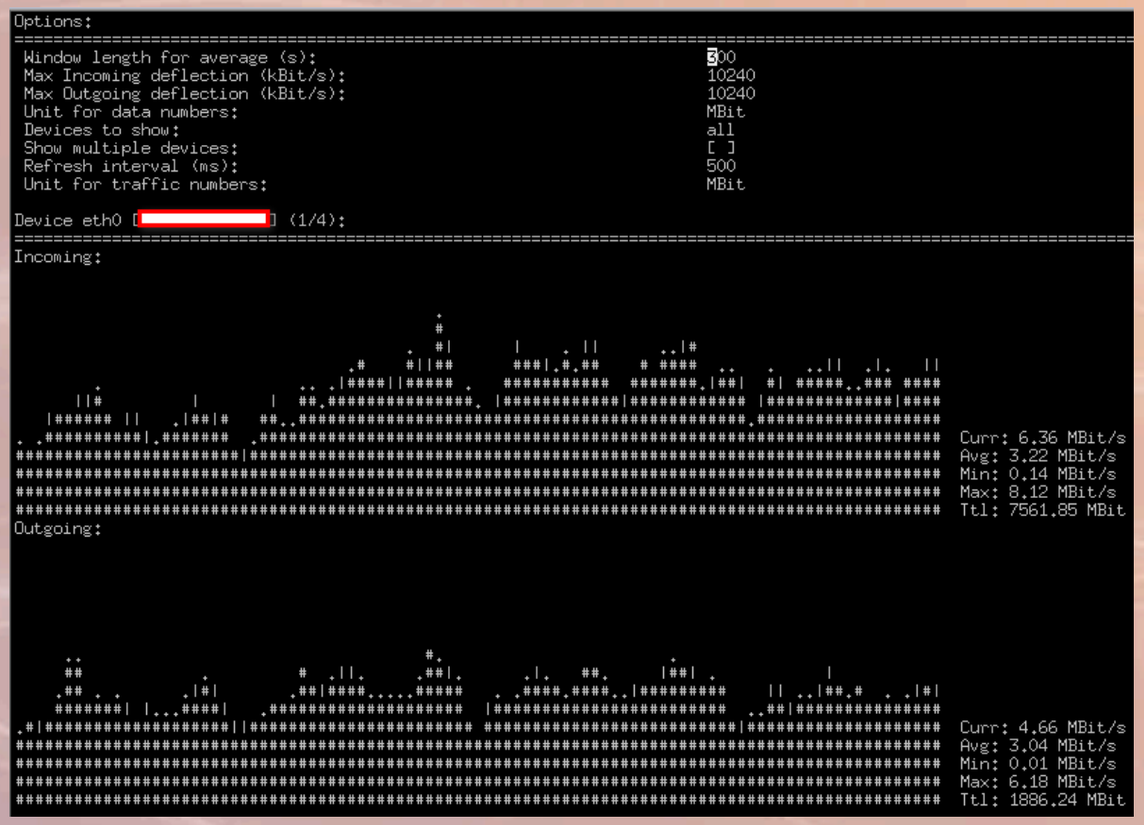
http://nmap.org/

nload

nload is a console application which monitors network traffic and bandwidth usage in real time.

It visualizes the in- and outgoing traffic using two graphs

provides additional info like total amount of transferred data and min/max network usage.



http://linux.die.net/man/1/nload

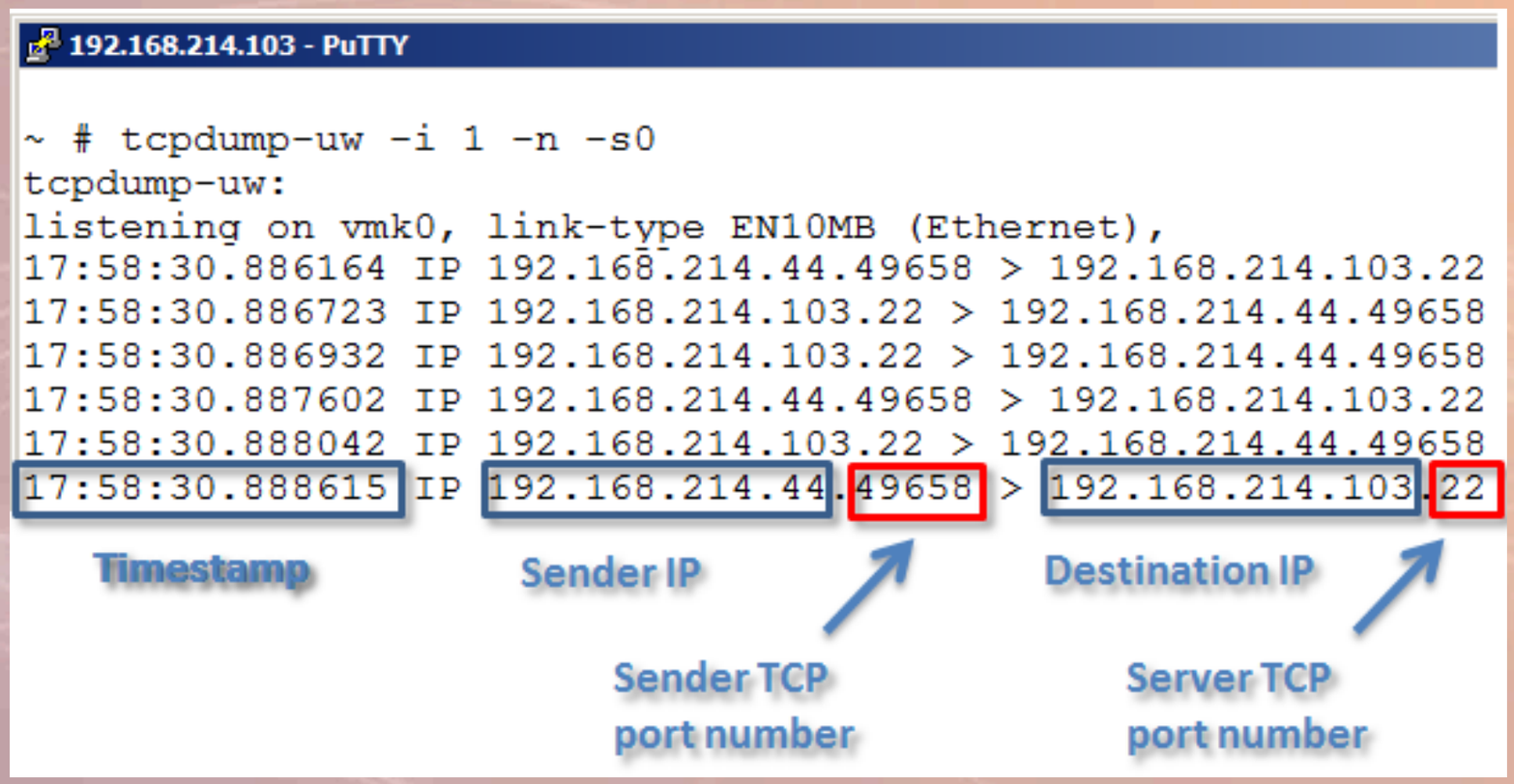
netdata

A Real-Time Performance Monitoring Tool for Linux Systems

http://www.tecmint.com/netdata-real-time-linux-performance-network-monitoring-tool/

tcpdump

- tcpdump is a common packet analyzer that runs under the command line.
- It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.



tcpdump

pcap file

tcpdump -s 0 port ftp or ssh -i eth0 -w mycap.pcap

In above command

-s 0 will set the capture byte to its maximum i.e. 65535, after this capture file will not truncate.

-i eth0 is using to give Ethernet interface, which you to capture. Default is eth0, if you not use this option.

port ftp or ssh is the filter, which will capture only ftp and ssh packets. You can remove this to capture all packets.

-w mypcap.pcap will create that pcap file, which will be opened using wireshark.

Unix Network Tools

- Wireshark
- Capsa
- Microsoft Network Monitor

Top 20 Free Network Monitoring and Analysis Tools for Sys Admins

Wireshark

Wireshark is a free and open-source packet/protocol analyzer.

https://www.wireshark.org/

It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Wireshark is cross-platform, running on GNU/Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

There is a terminal-based (non-GUI) version called TShark.

Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark

Wireshark is software that "understands" the structure (encapsulation) of different networking protocols.

It can parse and display the fields, along with their meanings as specified by different networking protocols.

Wireshark uses *pcap* to capture packets, so it can only capture packets on the types of networks that *pcap* supports.

Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.

Wireshark

Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.

Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

Data display can be refined using a display filter.

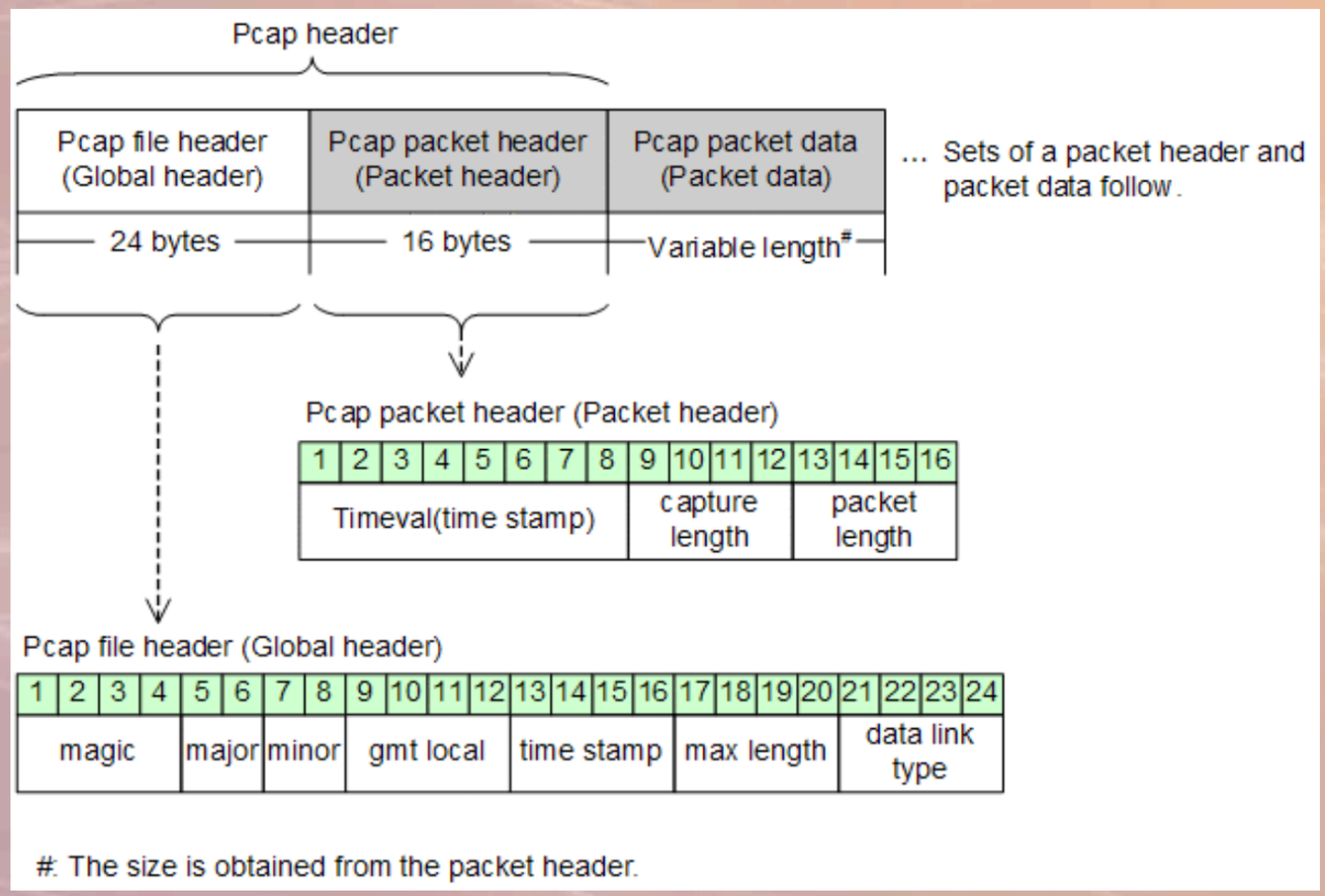
Plug-ins can be created for dissecting new protocols.

Wireshark is perhaps one of the best open source packet analyzers available today for UNIX and Windows.

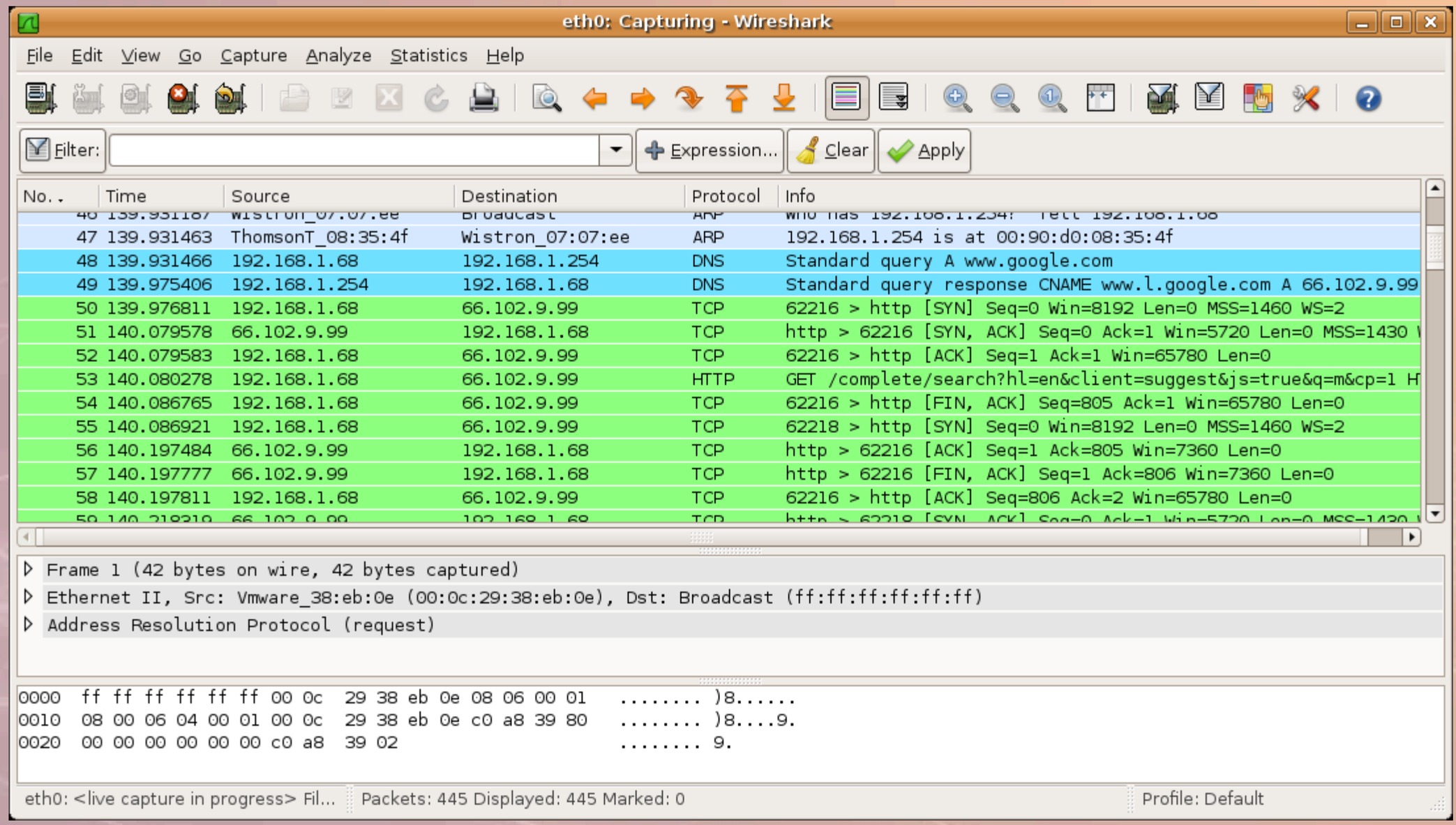
pcap

pcap (packet capture) consists of an application programming interface (API) for capturing network traffic

Unix-like systems implement pcap in the libpcap library
Windows uses a port of libpcap known as WinPcap.

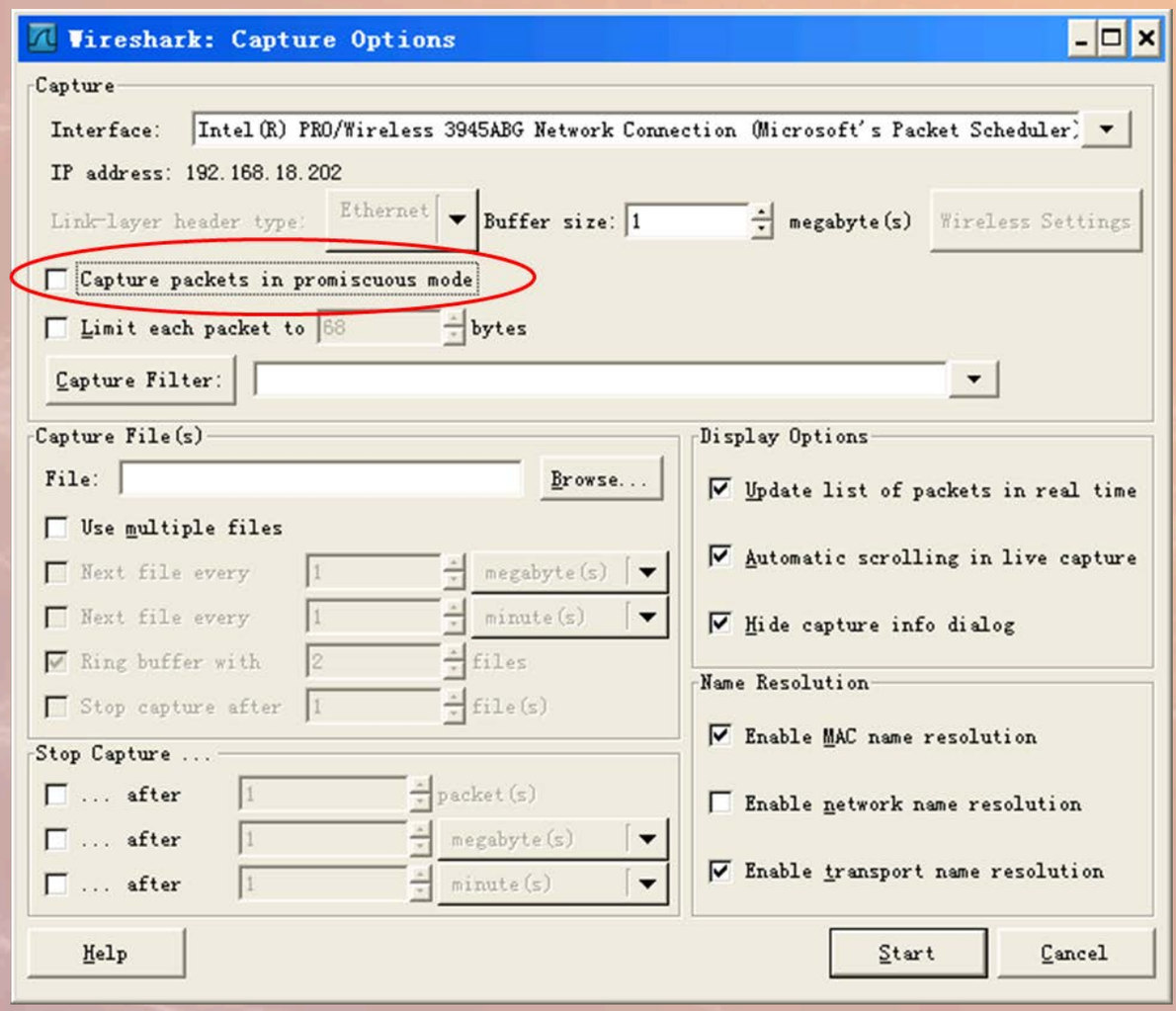


Wireshark


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
No. Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil...
Packets: 445 Displayed: 445 Marked: 0
Profile: Default

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).



Capsa

Capsa is the name for a family of packet analyzer developed by Colasoft.

Used by network administrators to monitor, troubleshoot and analyze wired & wireless networks.

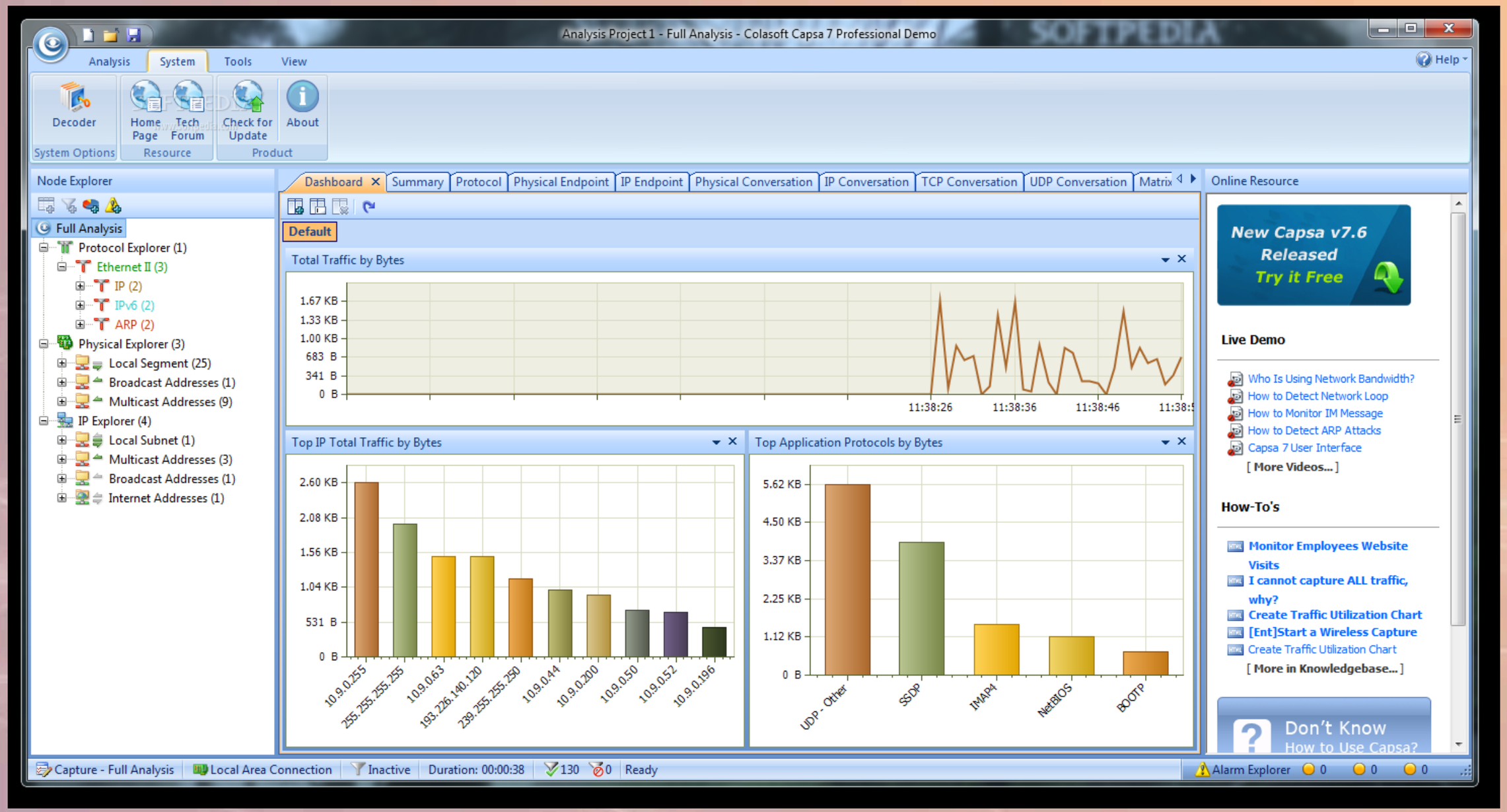
Currently, there are three editions available: Capsa Enterprise Edition, Capsa Professional Edition, and Capsa Free Edition.

http://www.colasoft.com/capsa-free/

Capsa Features

- Wired & wireless network real-time packet capturing
- Traffic & bandwidth monitoring
- Advanced protocol analysis
- Captures packets from a single or multiple network adapters
- Logs DNS, web browsing, Email, FTP & IM services

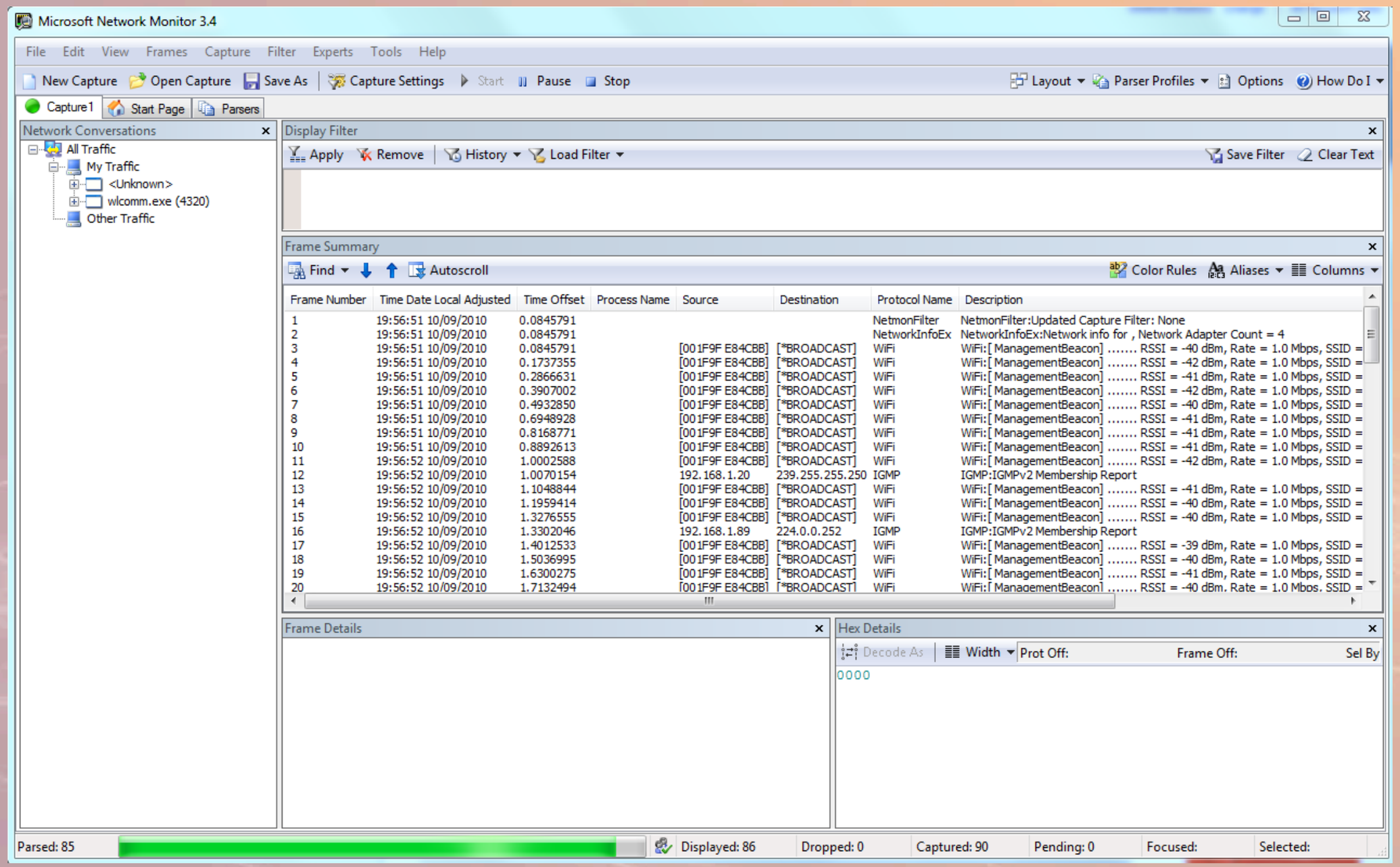
Capsa


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Professional Demo
Analysis
System
Tools
View
Help
Decoder
Home Page
Tech Forum
Check for Update
About
System Options
Resource
Product
Node Explorer
Full Analysis
Protocol Explorer (1)
Ethernet II (3)
IP (2)
IPv6 (2)
ARP (2)
Physical Explorer (3)
Local Segment (25)
Broadcast Addresses (1)
Multicast Addresses (9)
IP Explorer (4)
Local Subnet (1)
Multicast Addresses (3)
Broadcast Addresses (1)
Internet Addresses (1)
Dashboard
Summary
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Default
Total Traffic by Bytes
1.67 KB
1.33 KB
1.00 KB
683 B
341 B
0 B
11:38:26
11:38:36
11:38:46
Top IP Total Traffic by Bytes
2.60 KB
2.08 KB
1.56 KB
1.04 KB
531 B
0 B
10.9.0.255
255.255.255.255
10.9.0.63
193.226.140.120
239.255.255.250
10.9.0.44
10.9.0.200
10.9.0.50
10.9.0.52
10.9.0.196
Top Application Protocols by Bytes
5.62 KB
4.50 KB
3.37 KB
2.25 KB
1.12 KB
0 B
UDP - Other
SSDP
IMAP4
NetBIOS
BOOTP
Online Resource
New Capsa v7.6 Released
Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect Network Loop
How to Monitor IM Message
How to Detect ARP Attacks
Capsa 7 User Interface
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Don't Know
How to Use Capsa?
Capture - Full Analysis
Local Area Connection
Inactive
Duration: 00:00:38
130
0
Ready
Alarm Explorer
0
0
0

Microsoft Network Monitor

- Microsoft Network Monitor is a packet analyzer.
- It enables capturing, viewing, and analyzing network data and deciphering network protocols.
- It can be used to troubleshoot network problems and applications on the network.

Microsoft Network Monitor



Microsoft Message Analyzer

Microsoft Message Analyzer is a packet analyzer.

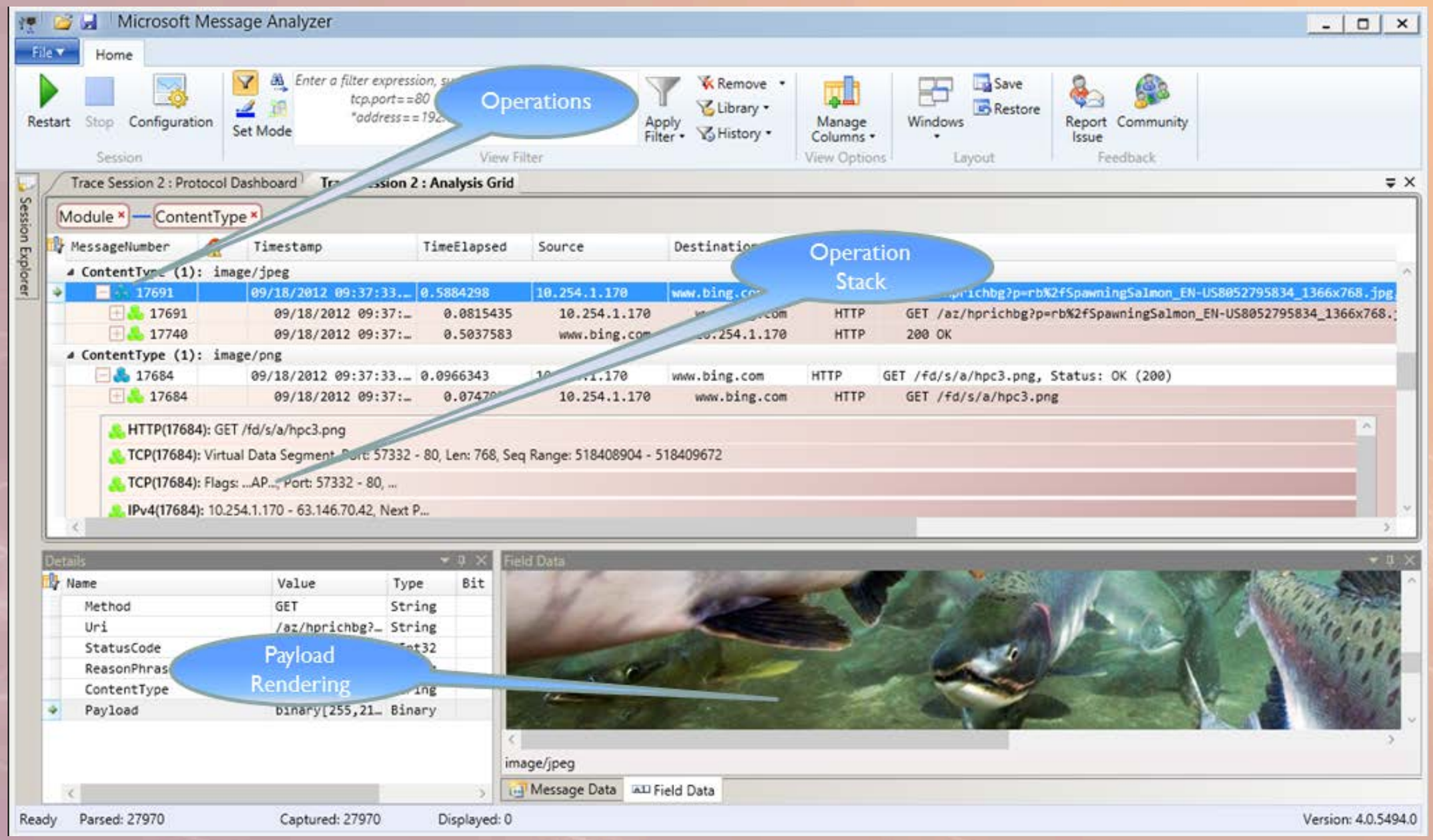
It enables you to capture, display, and analyze protocol messaging traffic.

To trace and assess system events and other messages from Windows components.

It enables capturing, viewing, and analyzing network data and deciphering network protocols.

It can be used to troubleshoot network problems and applications on the network..

Microsoft Message Analyzer

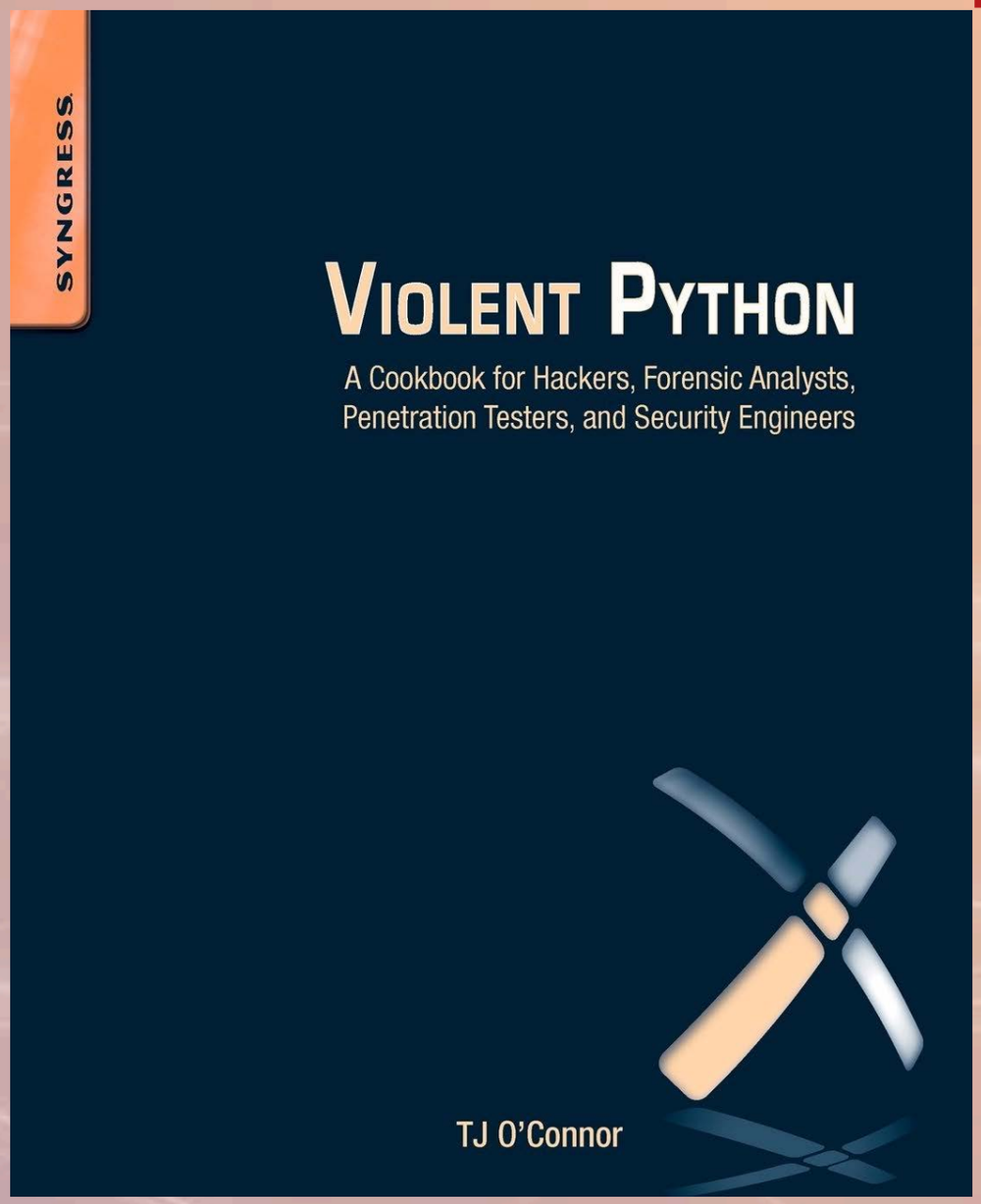


Python Network Apps

- Python GeoIP
- scapy

sudo apt-get install dnsutils

Python Network Apps



https://github.com/shadow-box/Violent-Python-Examples

GeoIP

A form of geolocation that uses the host's IP address to locate the host's geographic location.

Requires an API and MaxMind's GeoIP database to pinpoint a host's location to a city.

https://geoip2.readthedocs.io/en/latest/

GeoIP Databases

GeoLite2 databases are free IP geolocation databases comparable to, but less accurate than, MaxMind's GeoIP2 databases.

GeoLite2 databases are updated on the first Tuesday of each month.

IP geolocation is inherently imprecise. Locations are often near the center of the population.

http://dev.maxmind.com/geoip/geoip2/geolite2/

PyGeoIP

```
import geoip2.database
reader =
geoip2.database.Reader('/home/plymale/violent/GeoLite2-
City_20190409/GeoLite2-City.mmdb')

response = reader.city('128.101.101.101')

print(response.country.iso_code)
print(response.country.name)
print(response.subdivisions.most_specific.name)
print(response.city.name)
print(response.postal.code)
print(response.location.latitude)
print(response.location.longitude)

reader.close()
```

Scapy

Scapy is a powerful interactive packet manipulation program.

- able to forge or decode packets of a wide number of protocols
- send packets on the wire
- capture packets
- match requests and replies
- can handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery
- can also send invalid frames or inject your own 802.11 frames,

http://www.secdev.org/projects/scapy/

Scapy

"The Very Unofficial Dummies Guide to Scapy"

Adam Maxwell

Installation

1. Install Python 2.5+
2. Download and install Scapy

sudo apt-get install python-scapy

3. (Optional): Install additional software for special features.

apt-get install tcpdump graphviz imagemagick python-gnuplot python-crypto python-pyx

4. Run Scapy with root privileges.

https://theitgeekchronicles.files.wordpress.com/2012/05/scapyguide1.pdf

Scapy

Welcome to Scapy (2.2.0)

>>> send(IP(dst="127.0.0.1")/ICMP()/"HelloWorld")

Sent 1 packets.

>>>

send - this tells Scapy that you want to send a packet (just a single packet)

IP - the type of packet you want to create, in this case an IP packet

(dst="127.0.0.1") - the destination to send the packet to (in this case my router)

/ICMP() - you want to create an ICMP packet with the default values provided by Scapy

/"HelloWorld") - the payload to include in the ICMP packet (you don't have to provide this in order

for it to work.

Scapy

Scapy Basics

Scapy

"Packet Wizardry Ruling the Network with Python"
Rob Klein

Scan an entire C-Class network for all hosts running that have port 80 listening.

```
p=IP(dst="hackaholic.org/24")/TCP(dport=80, flags="S")
sr(p)

results = _[0]

for pout, pin in results:
...    if pin.flags == 2:
...        print pout.dst
```

Scapy

Created a packet which was sent to the /24-subnet that hackaholic.org is connected to and set the TCP header to destination port 80 and the SYN flag.

The SYN flag is used to initiate a connection.

A reply of SA (SYN/ACK) means the port is listening, a RA (RESET/ACK) means it is closed, and finally no response means the host is down or filters packets.

After constructing the packet, Scapy emits the packets.

The results are then dissected in the for-loop and the destination IP addresses of hosts that replied SA are listed.

Closing