LECTURE 7:
INTRUSION DETECTION TECHNIQUES AND NETWORK FORENSICS

Part 2: Investigating Network Traffics

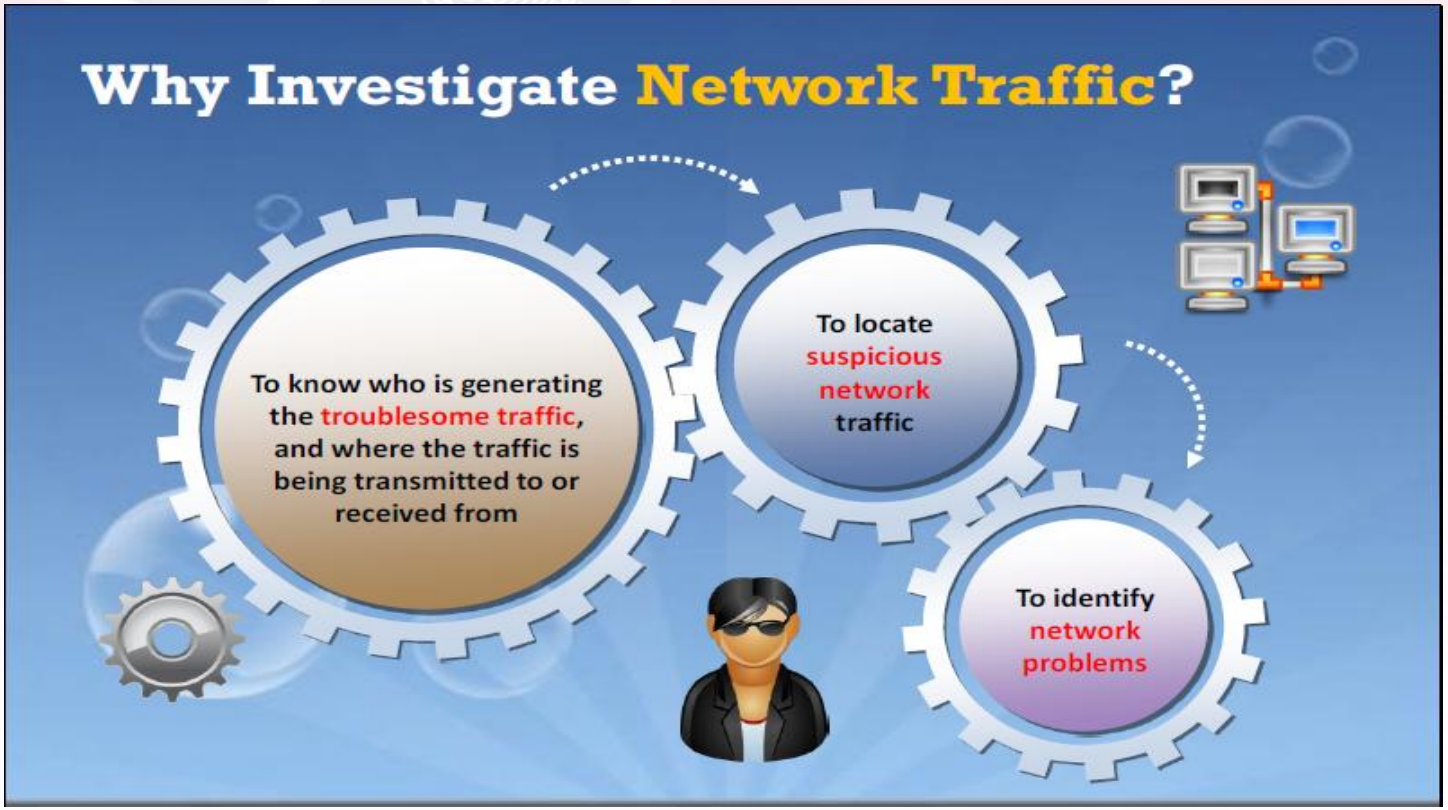
References:
Guide to Computer Forensics and Investigations
Certified Ethical Hacker and Forensic Investigations

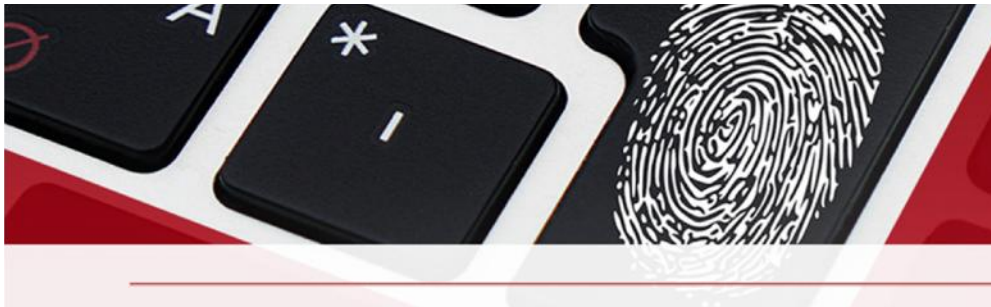
Objectives

- Understanding the network protocols
- Identifying the sources of evidence on a network
- Understanding the Physical and data-link layer of the OSI model
- Gathering evidence at the physical and data link layer
- Understanding Network and transport layer of the OSI model
- Gathering evidence at the network and transport layer
- Collecting evidence and documenting on a network
- Gathering evidence on a network
- Documenting the gathered evidence on a network
- Evidence reconstruction for investigation
- Identifying network forensic tools

Introduction

source: CHFI





Network Addressing Schemes

source: CHFI

There are **two types** of network addressing schemes:

LAN Addressing	Each node in LAN has a MAC address that is factory-programmed into its NIC.
	Data packets are addressed to either one of the nodes or all of the nodes.
Internetwork Addressing	Internetwork is a collection of LANs and/or other networks that are connected with routers.
	Each network has a unique address and each node on the network has a unique address, so an address is network address/node address combination.
	IP is responsible for network layer addressing in the TCP/IP protocol.

Overview of Network Protocols

source: CHFI

	Data Unit	Layer	Function	Protocols
Host Layer	Data	Application	Network process to application	HTTP, SMTP, NNTP, TELNET, FTP, NMP, TFTP
		Presentation	Data representation and encryption	
		Session	Interhost communication	
	Segments	Transport	End-to-end connections and reliability	UDP, TCP
Media Layer	Packets	Network	Path determination and logical addressing (IP)	ARP, RARP, ICMP,IGMP, IP
	Frames	Data Link	Physical addressing (MAC & LLC)	PPP, SLIP
	Bits	Physical	Media, signal and binary transmission	

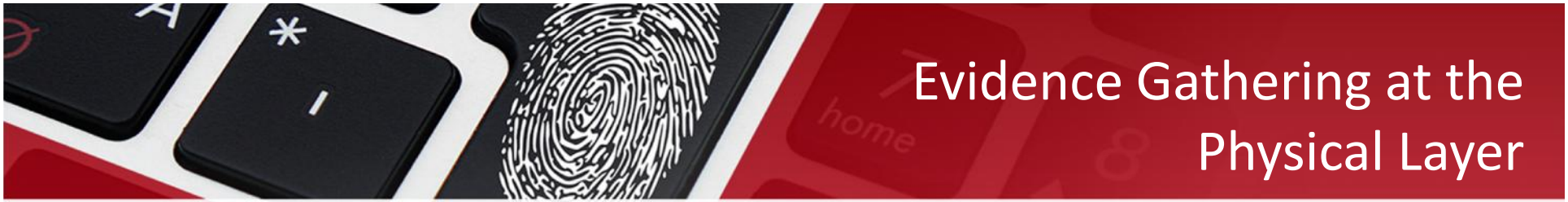
Overview of Physical and Data-link Layer of the OSI Model

Physical layer:

- It helps in transmitting data bits over a physical channel.
- It has a set of predefined rules that physical devices and interfaces on a network have to follow for data transmission to take place.

Data-link layer:

- It controls error in transmission by adding a trailer to the end of the data frame.

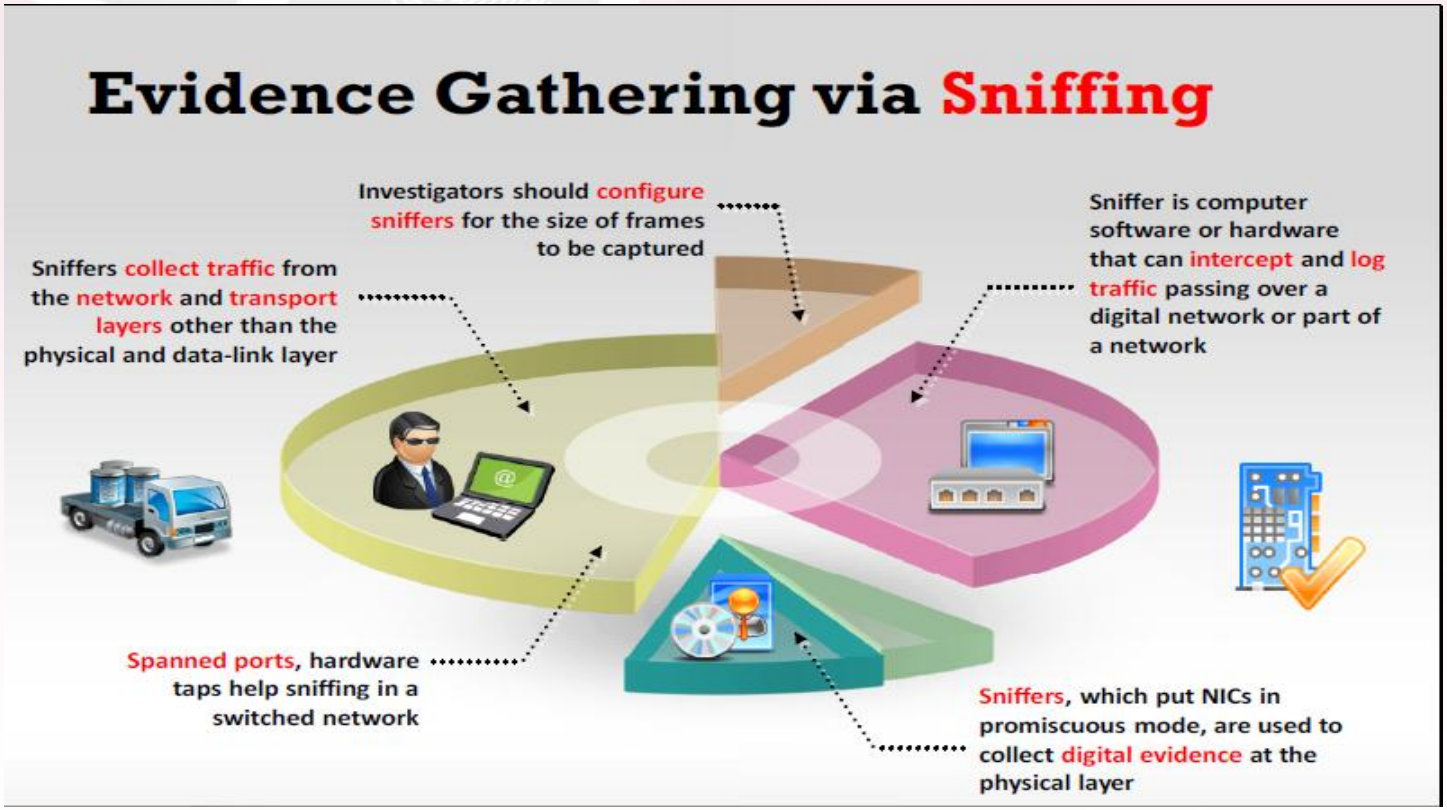


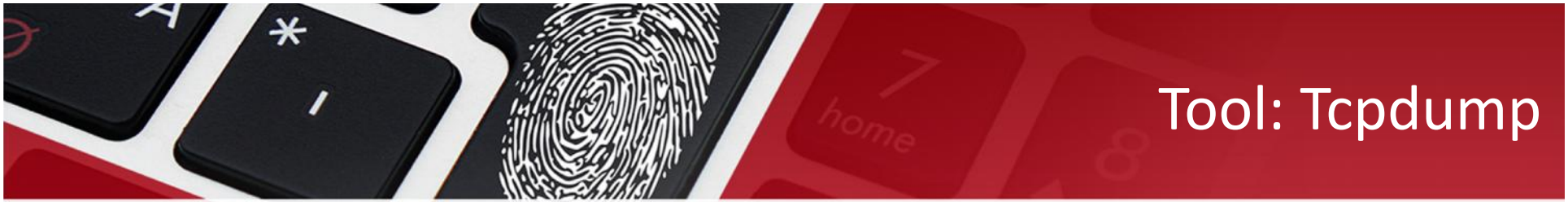
Evidence Gathering at the Physical Layer

- Sniffer is computer software or hardware that can intercept and log traffic passing over a digital network or part of a network.
- Sniffers, which put NICs in promiscuous mode, are used to collect digital evidence at the physical layer.
- SPANned ports, hardware taps help sniffing in a switched network.
- Sniffers collect traffic from the network and transport layers other than the physical and data-link layer.
- Investigators should configure sniffers for the size of frames to be captured.

Evidence Gathering: Sniffing

source: CHFI





Tool: Tcpdump

Tcpdump allows to sniff network packets and make statistical analysis of these dumps.

It operates by putting the network card into promiscuous mode.

It may be used to measure the response time, packet loss percentages, and view TCP/UDP connection establishment and termination.

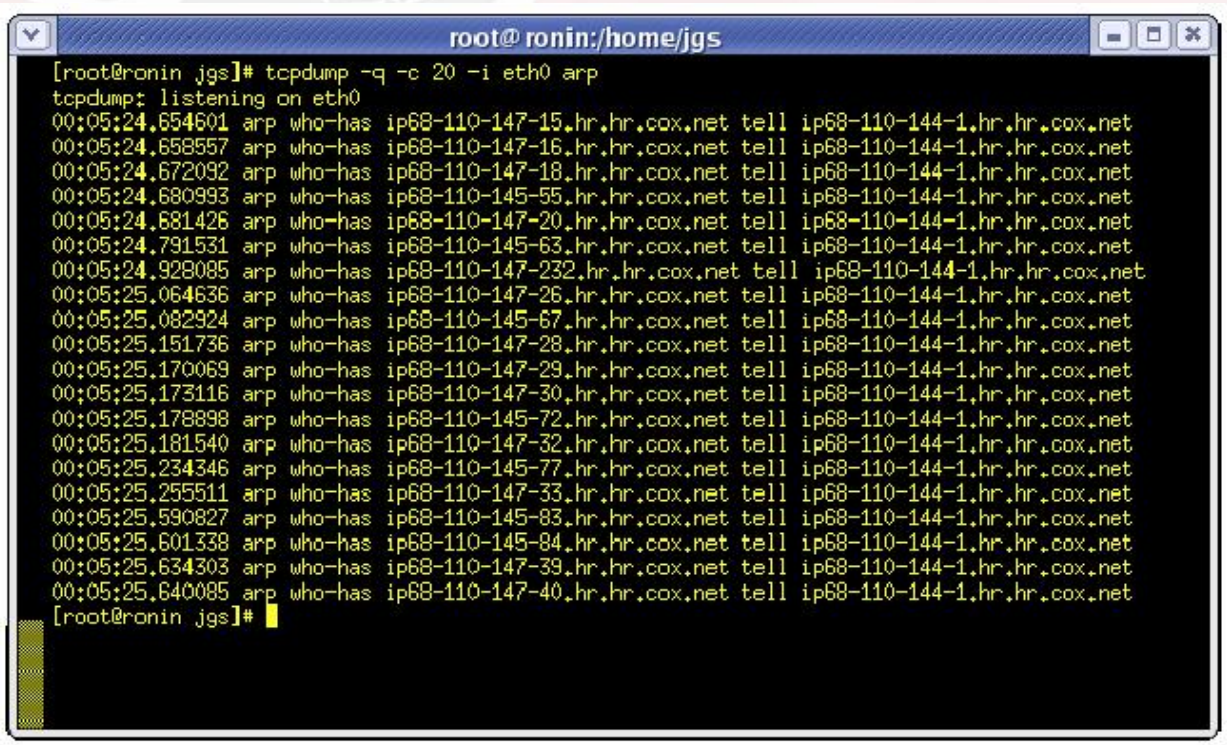
Tcpdump report consists of:

- Captured packet count.
- Received packet count.
- "dropped by kernel" packets count.

It supports following platforms:

- Sun OS 3.x or 4.x Solaris HP-UX IRIX Linux Ultrix and Digital UNIX BSD

Tcpdump: Screenshot



Tool: WinDump

WinDump is a version of tcpdump for Windows platform.

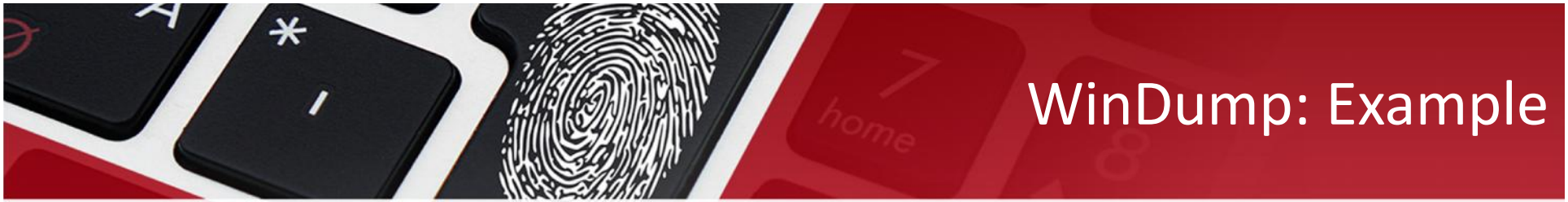
Command for saving the captured data packets using Windump as a sniffer:

- *C:\Windump –w filename.dmp*

The packets are stored in the C drive with the filename. The packets can be analyzed by using a notepad.

- *C:\Windump –w filename.dmp –s 65535*

The above command can be used to specify the size of the Ethernet packet to be captured.



WinDump: Example

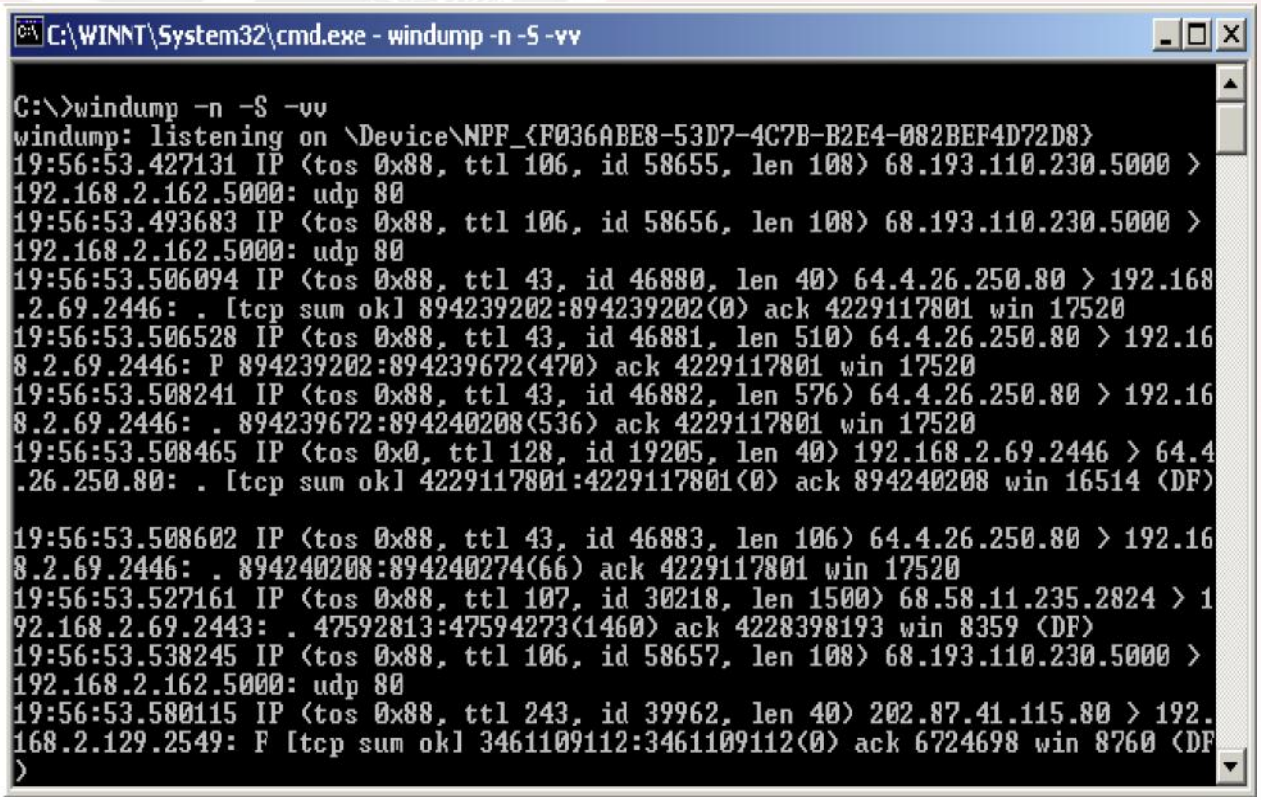
- Given below is the output obtained from WinDump:

```
20:50:00.037087 IP (tos 0x0, ttl 128, id 2572, len 46) 192.168.2.24.1036 >
64.12.24.42.5190: P [tcp sum ok] 157351:157357(6) ack 2475757024 win 8767 (DF)
```

The above entry can be deciphered as:

Timestamp → 20:50:00.037087
IP [protocol header] → tos 0x0, ttl 128, id 2572, len 46
source IP:port → 192.168.2.24.1036
destination IP:port → 64.12.24.42.5190:
P [push flag] [tcp sum ok] → 157351:157357
[sequence numbers] (6) [bytes of data]
acknowledgement and sequence number → ack 2475757024
window size (DF) [don’t fragment set] → win 8767

WinDump: Screenshot



Tool: NetIntercept

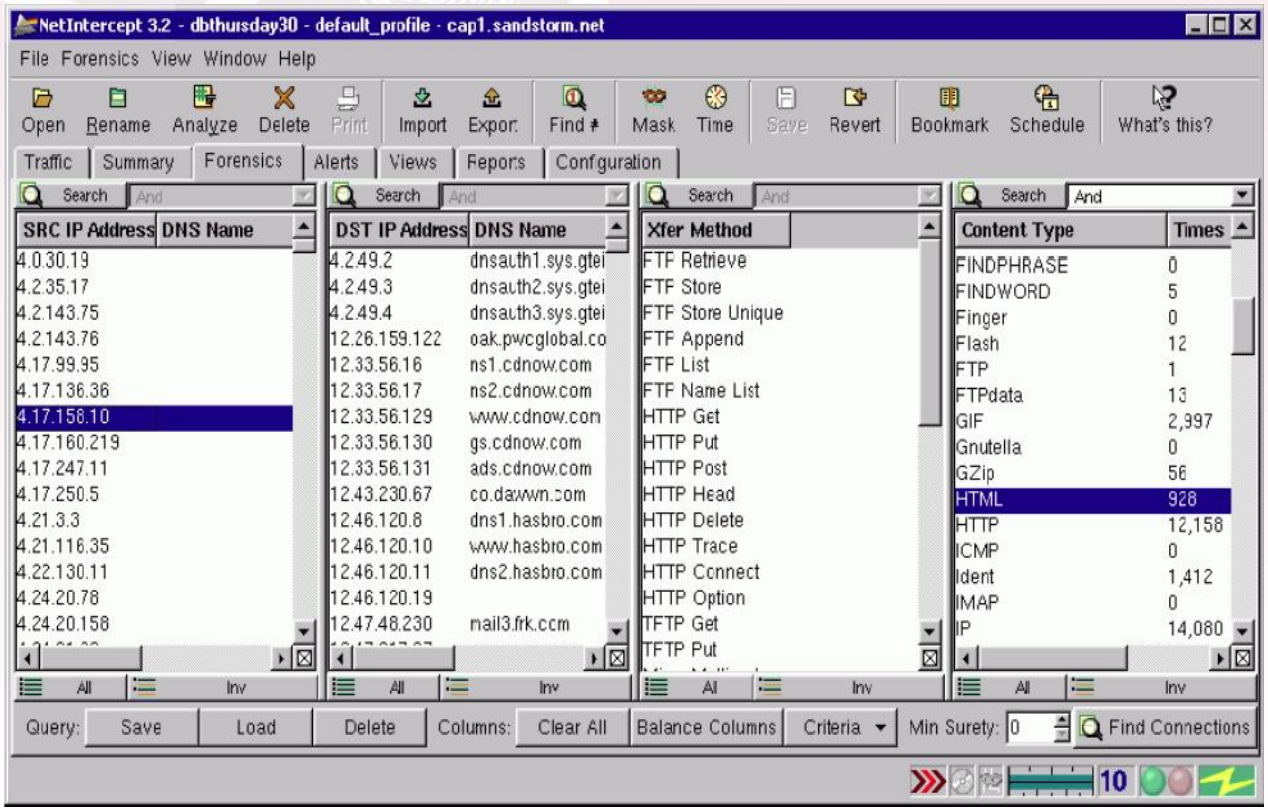
source: http://www.sandstorm.net

NetIntercept captures and archives network traffic, so you can analyze problems as soon as they're detected.

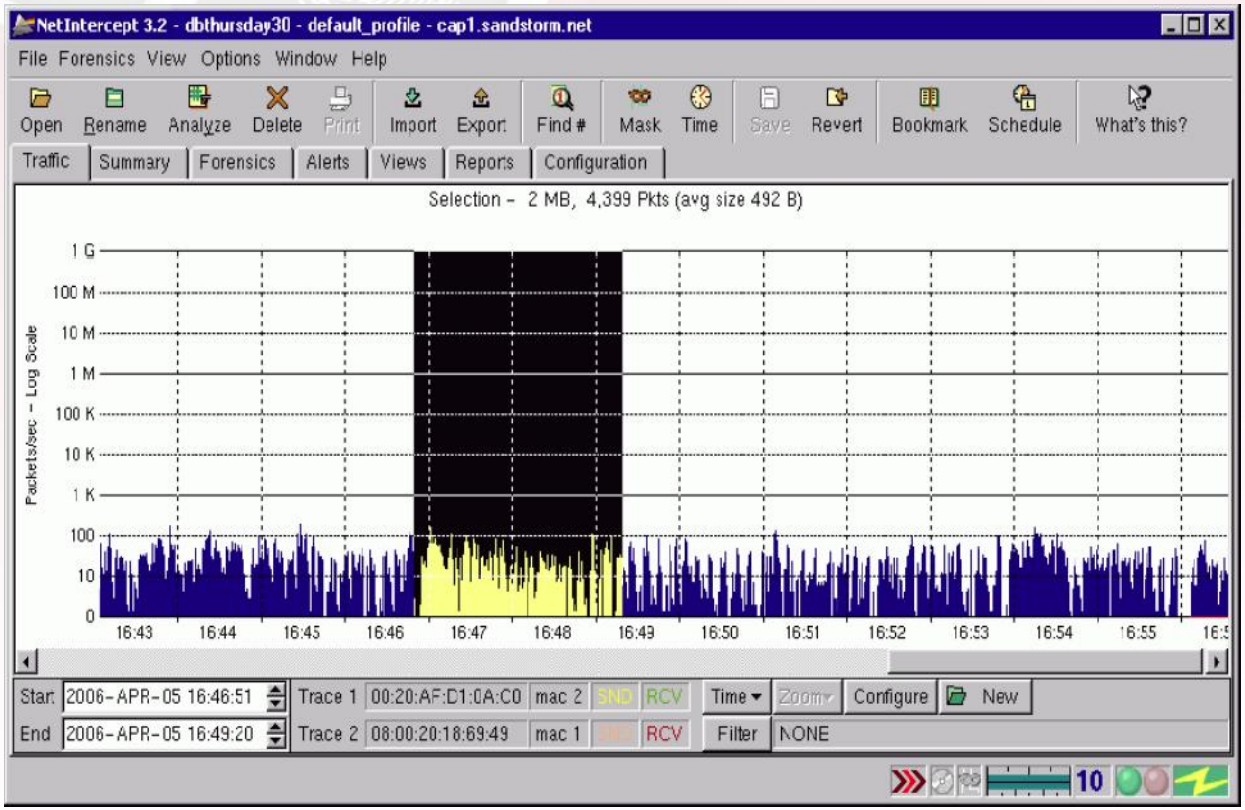
NetIntercept correlates user sessions and reconstructs files transmitted or received over the network, giving you immediate evidence of misbehavior.

Using NetIntercept, you can discover the security breaches, the points of regulatory non-compliance, and the network problems, and shift your focus from finding problems to fixing them.

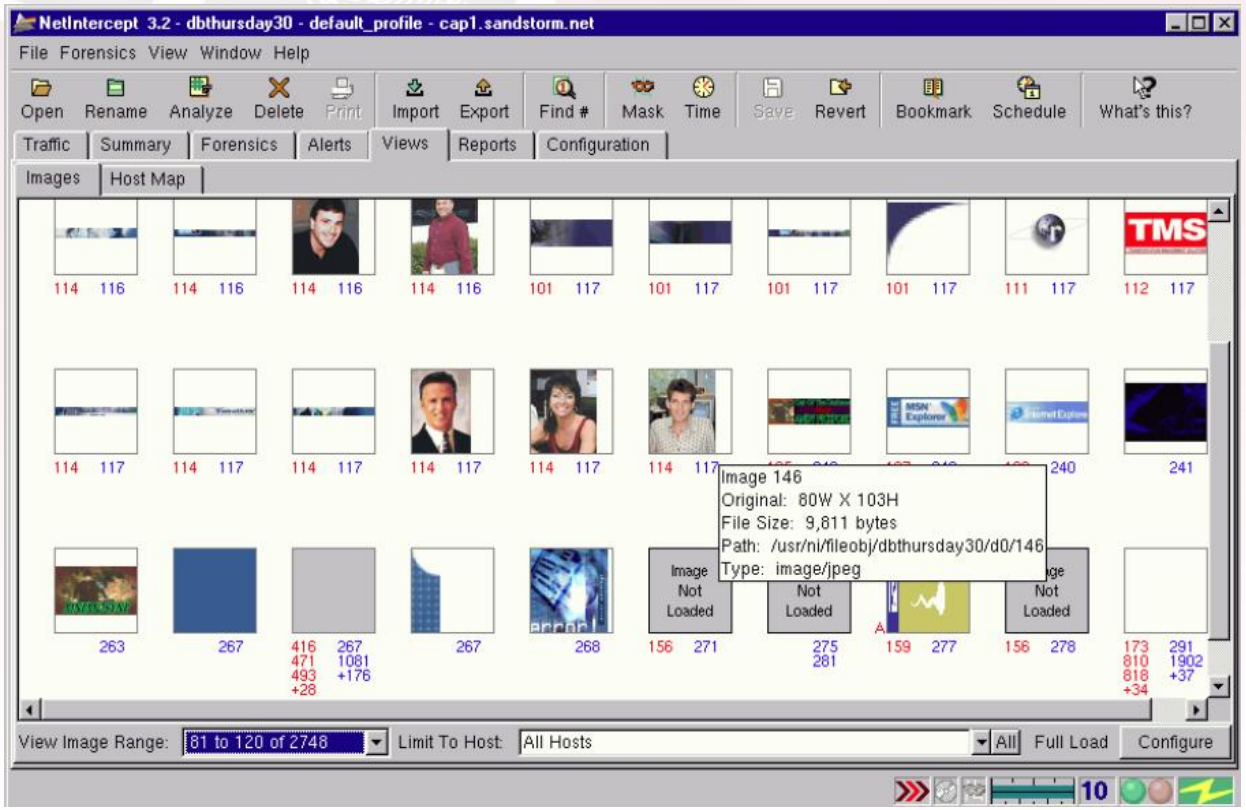
NetIntercept: Screenshots



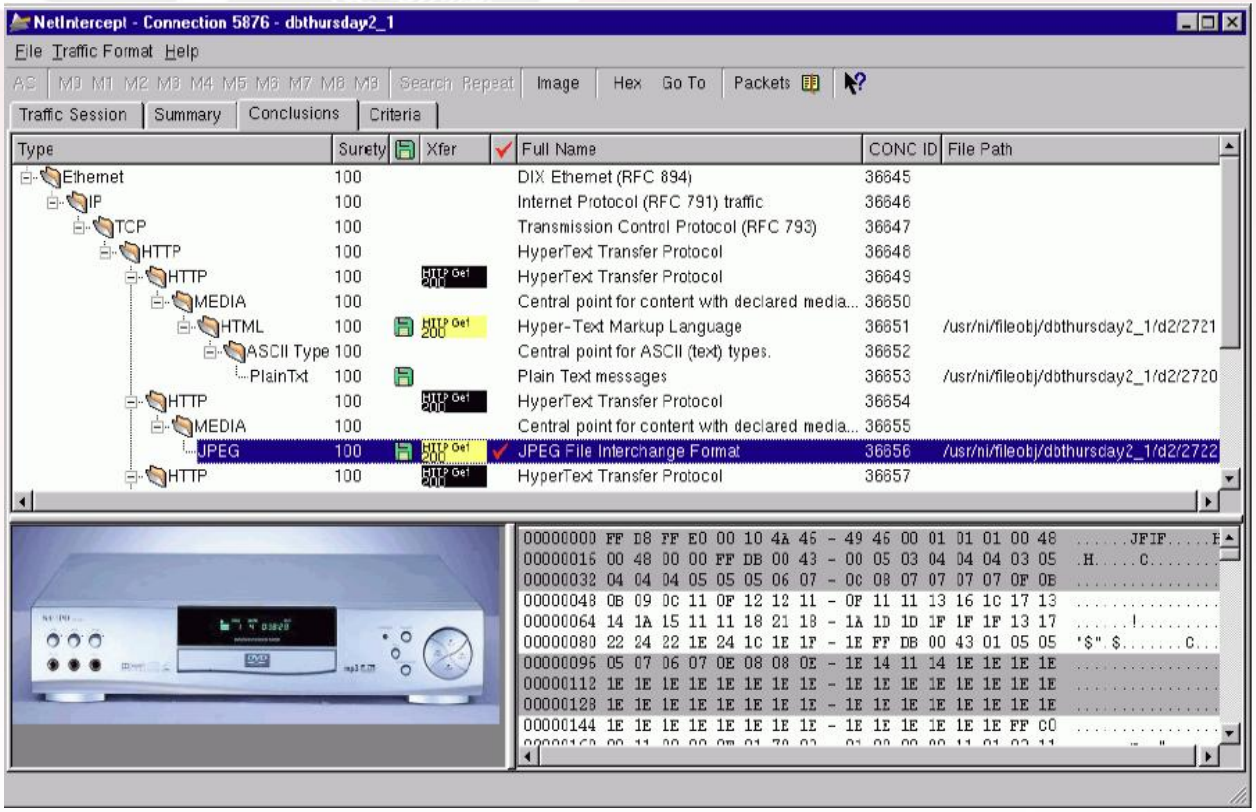
NetIntercept: Screenshots



NetIntercept: Screenshots



NetIntercept: Screenshots



Tool: Ethereal (Wireshark)

Wireshark

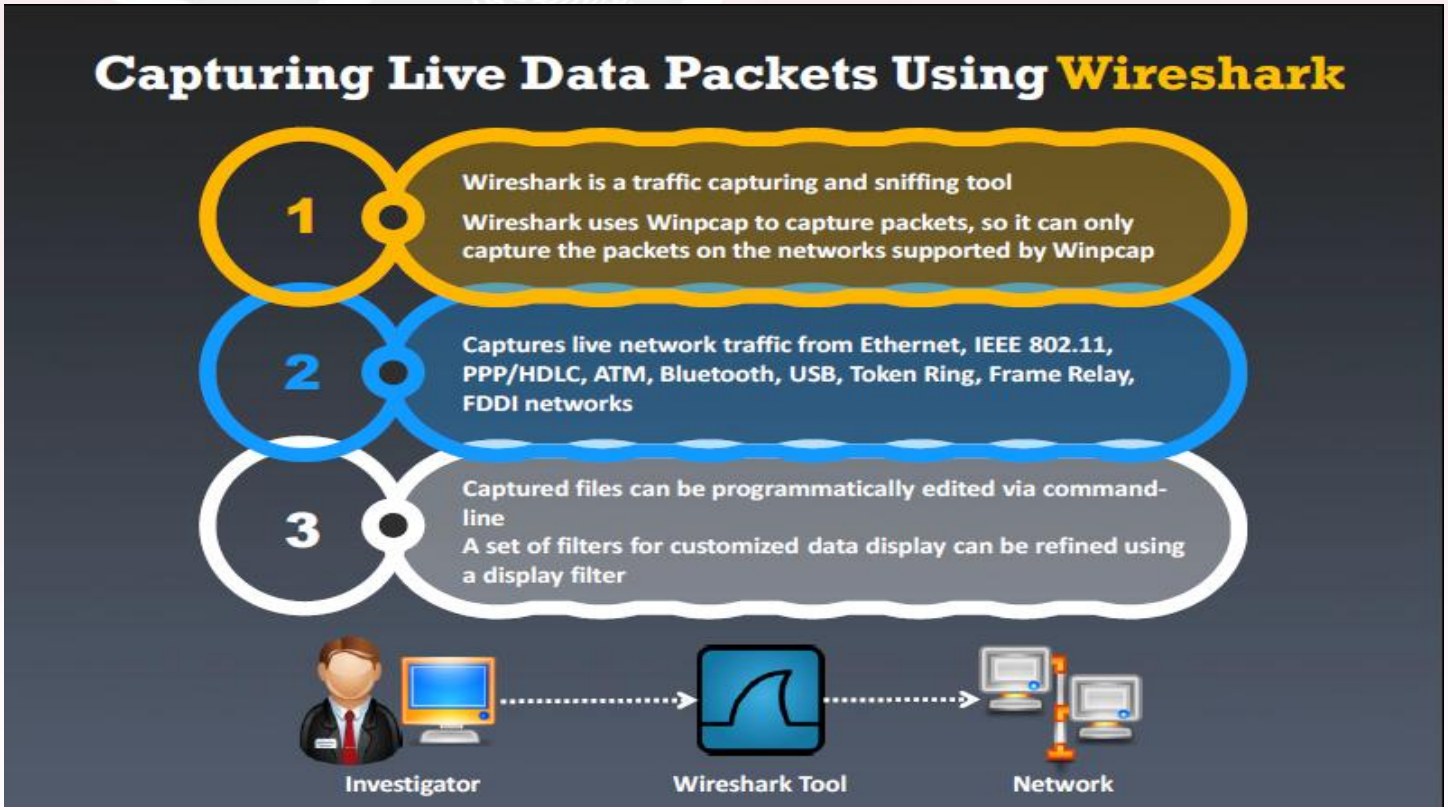
Ethereal (Wireshark) is a network protocol analyzer for UNIX and Windows.

It allows the user to examine data from a live network or from a capture file on a disk.

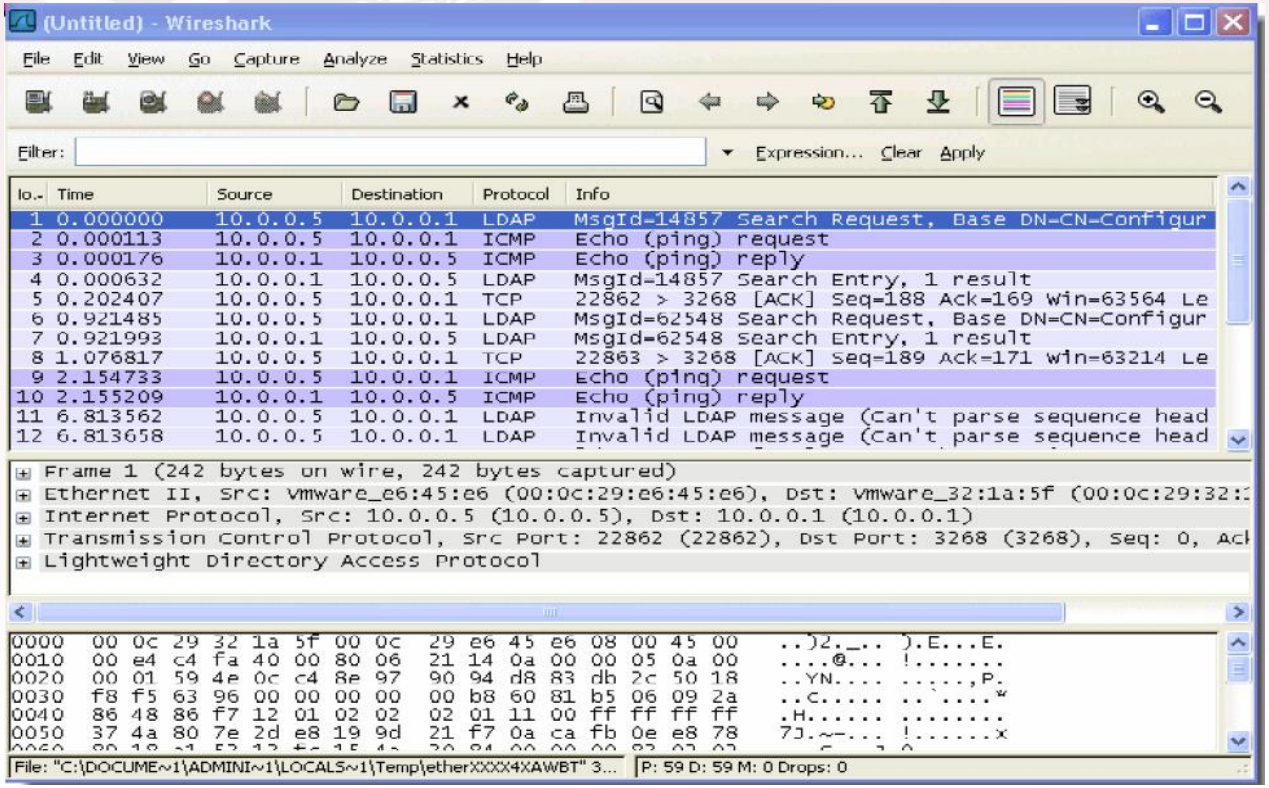
The user can interactively browse the captured data, viewing the summary and detailed information of each packet captured.

Tool: Wireshark

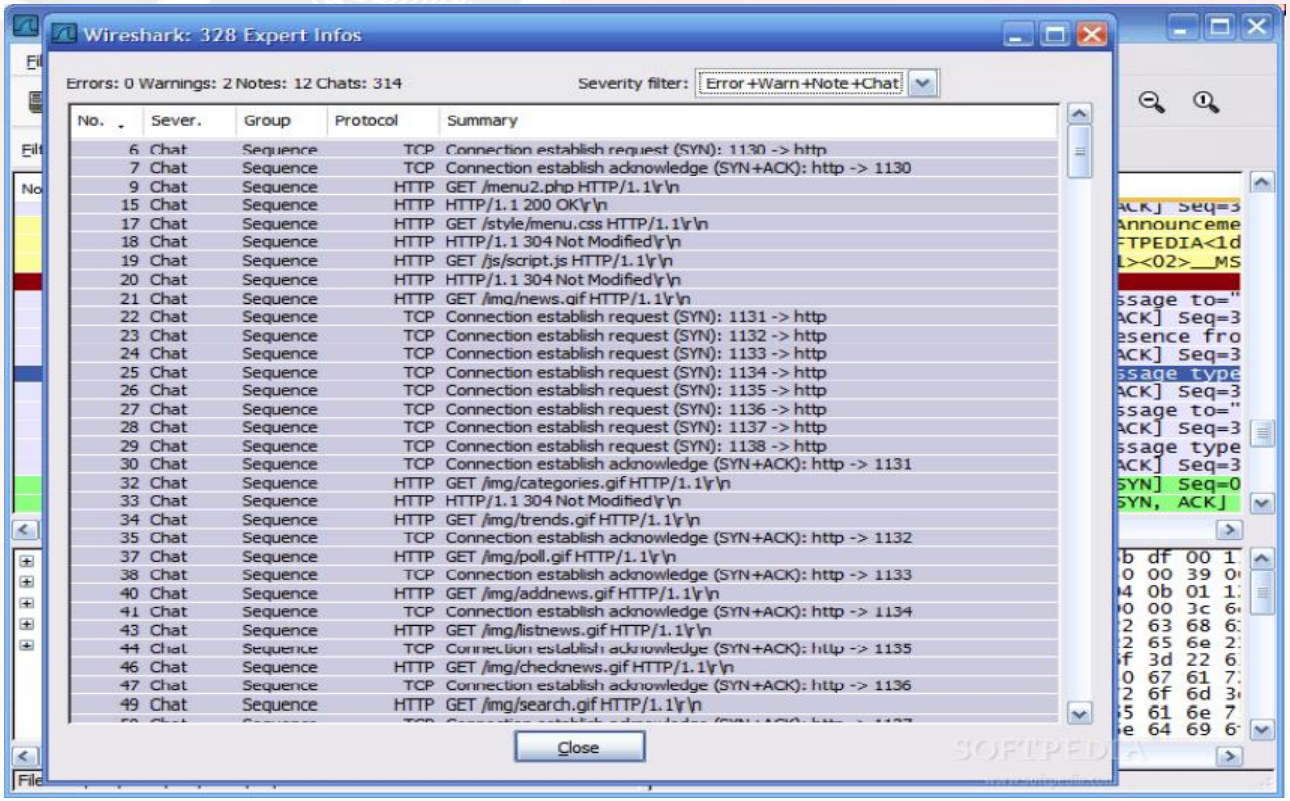
source: CHFI



Wireshark: Screenshots

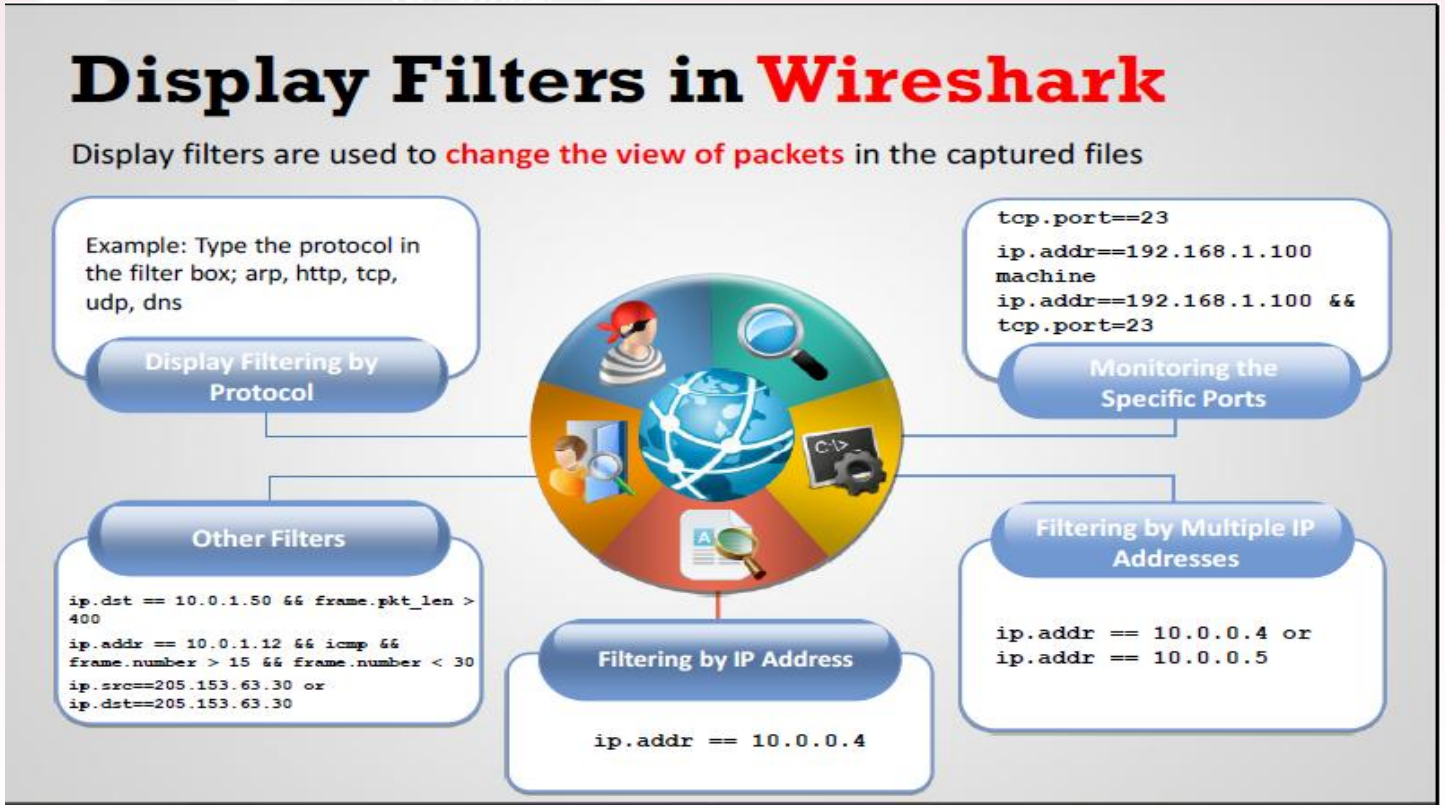


Wireshark: Screenshots



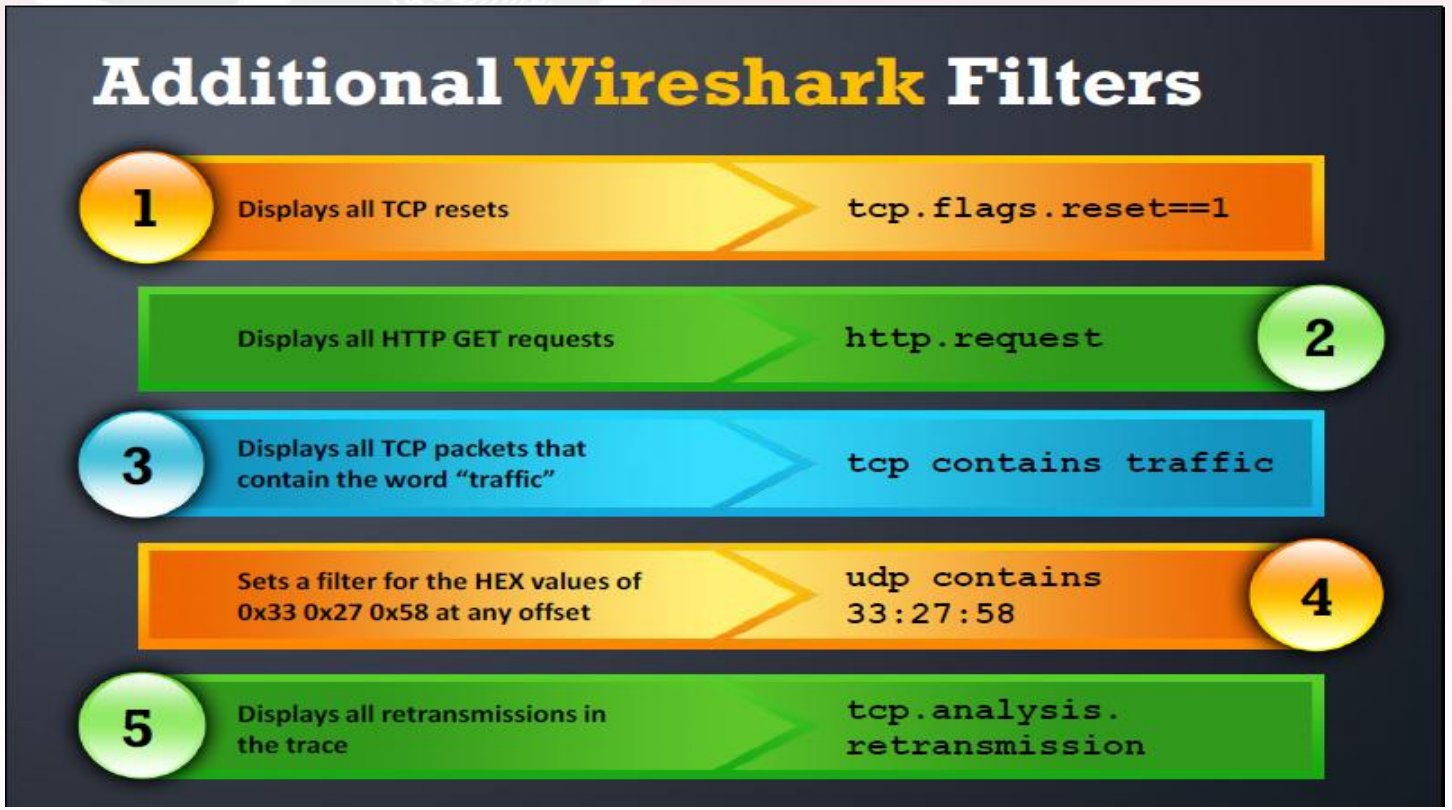
Tool: Wireshark

source: CHFI



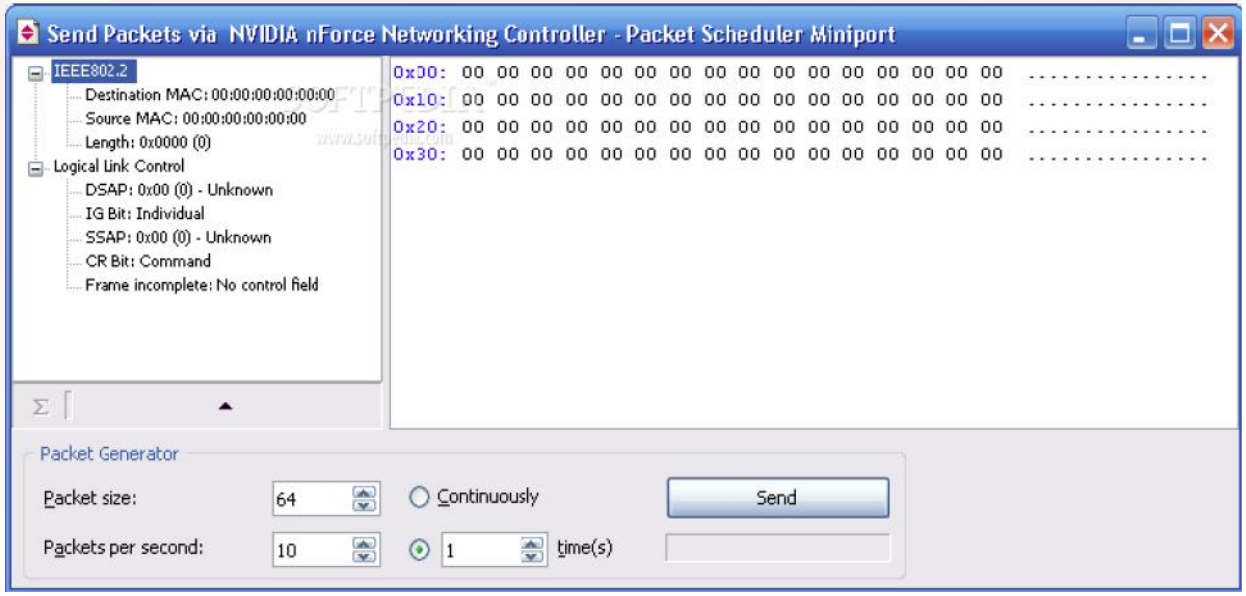
Tool: Wireshark

source: CHFI

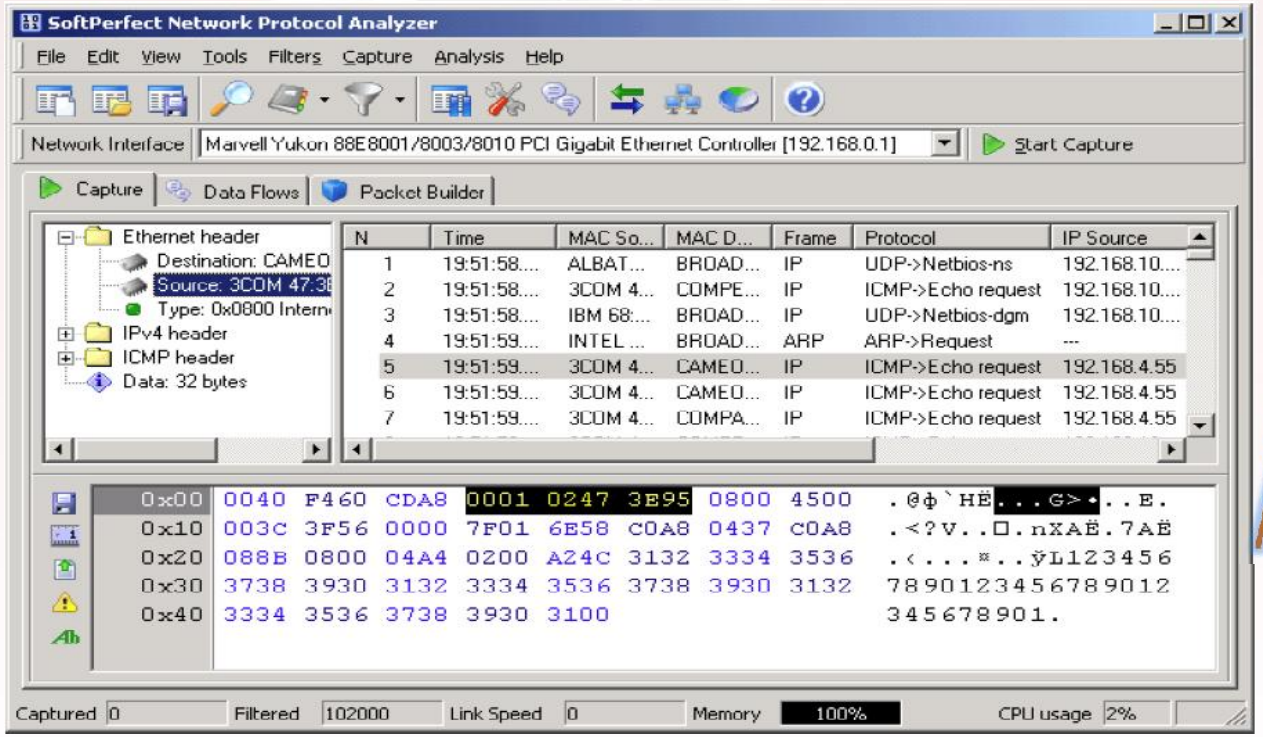


Tool: CommView

CommView - monitor network activity capable of capturing and analyzing packets on any Ethernet network.



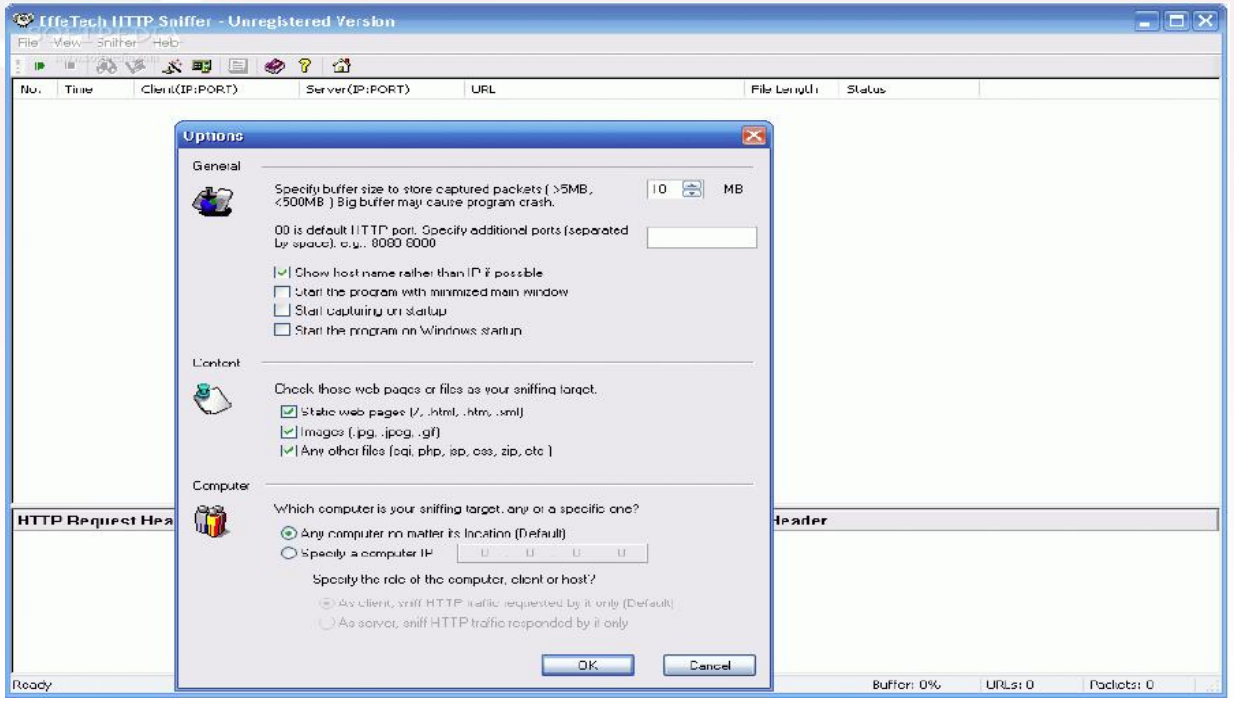
Tool: Softperfect Network Sniffer



Softperfect Network Sniffer - A network protocol analyzer or sniffer.

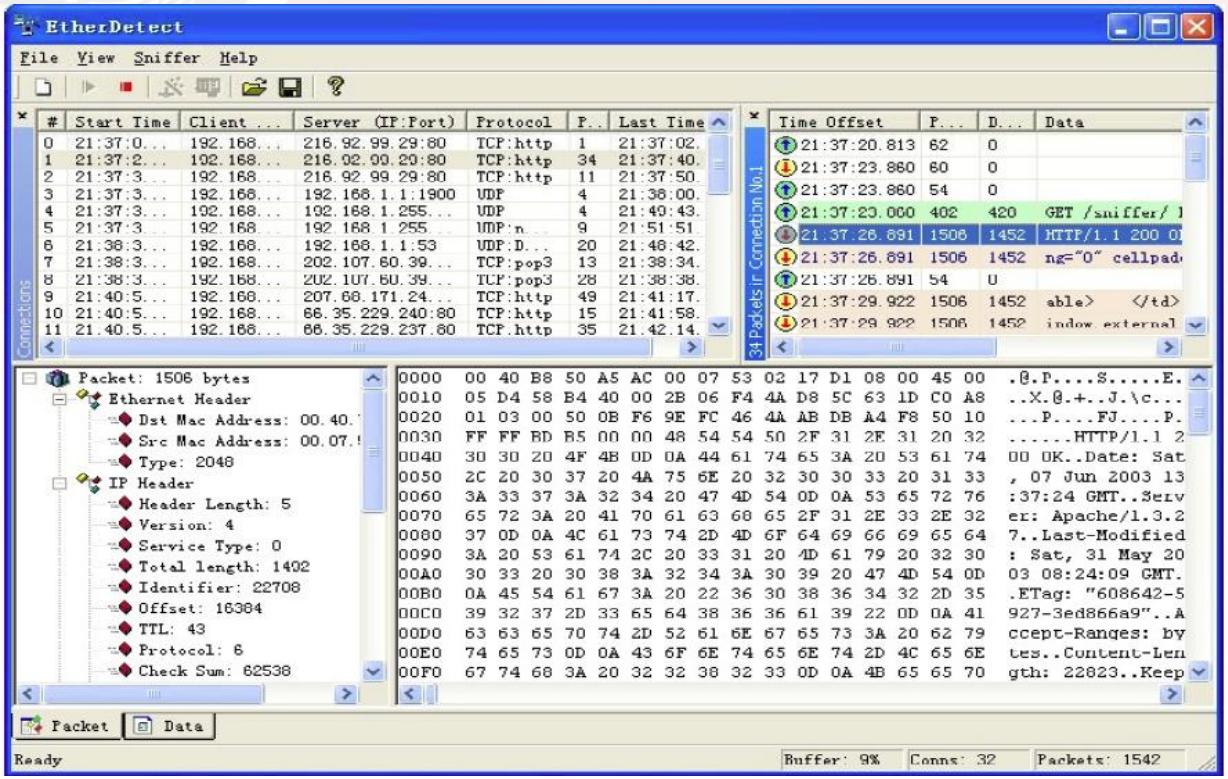
Tool: HTTP Sniffer

HttpDetect (EffeTech HTTP Sniffer) - HTTP sniffer, packet analyzer, content rebuilder, and http traffic monitor.



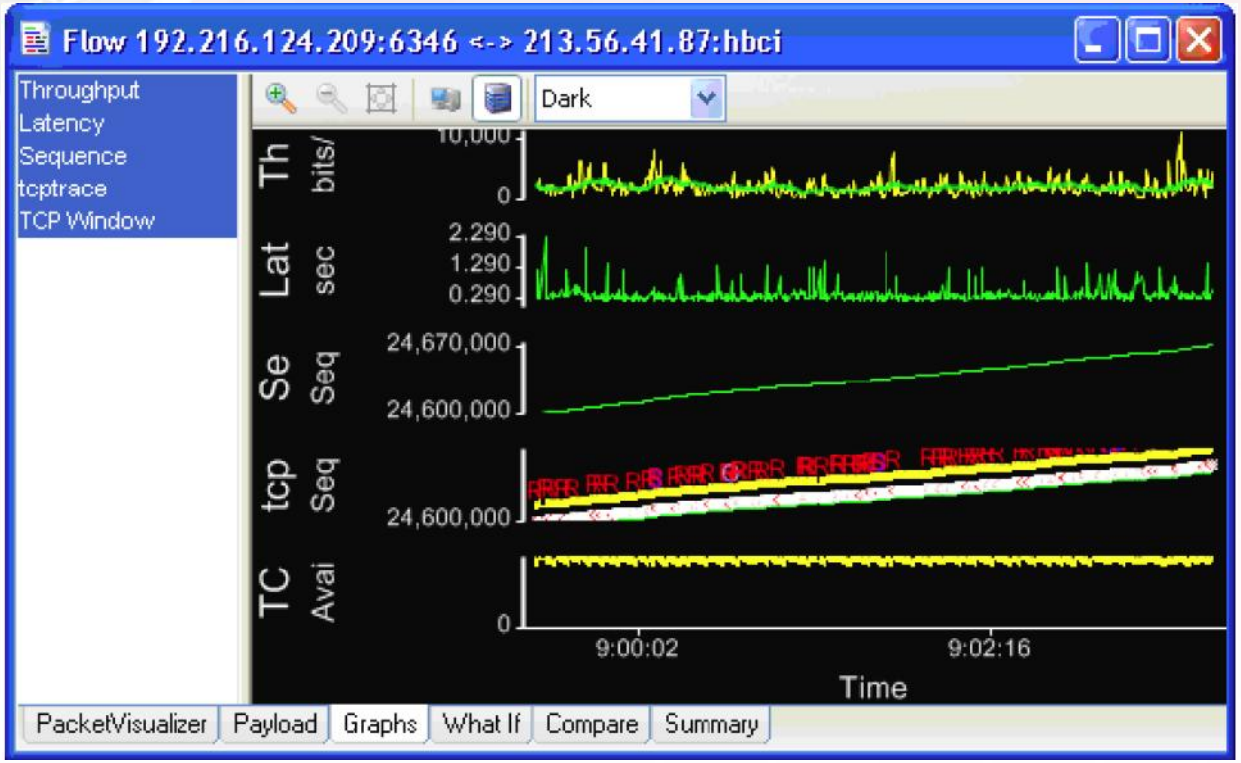
Tool: EtherDetect Packet Sniffer

EtherDetect Packet Sniffer - Connection oriented packet sniffer and protocol analyzer.

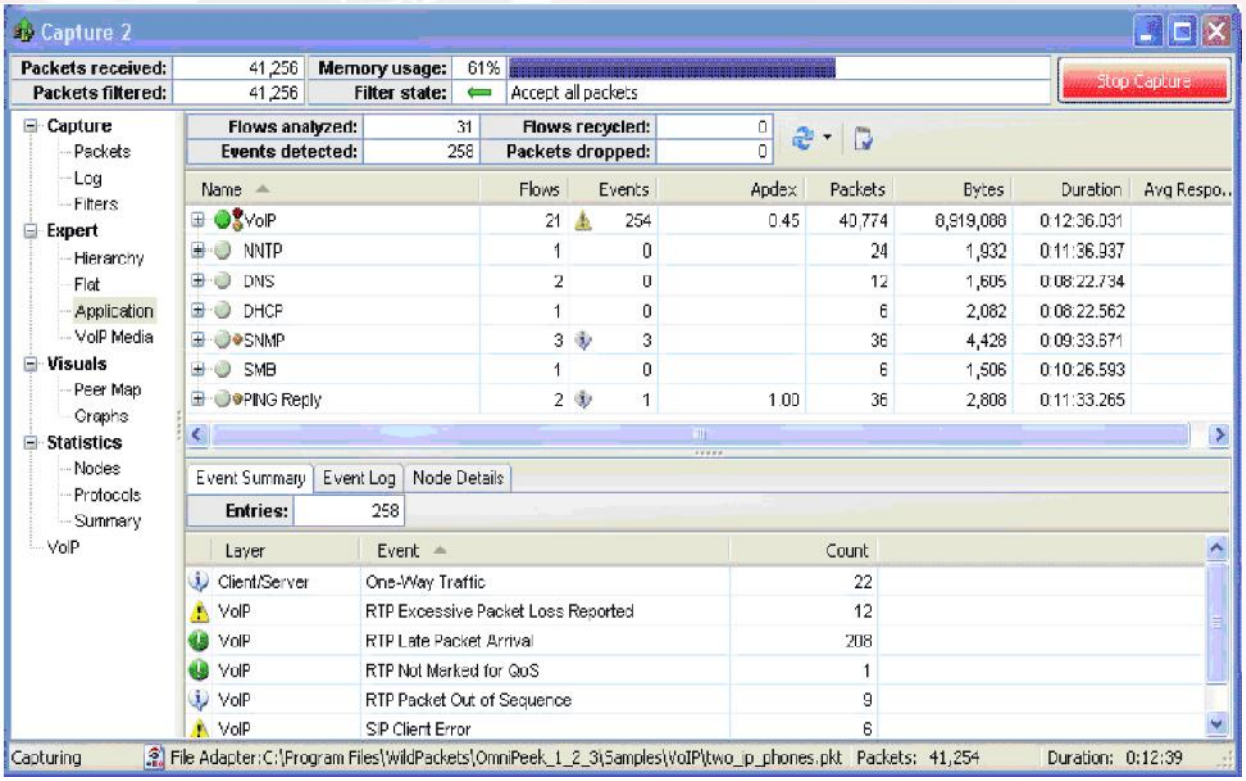


Tool: OmniPeek

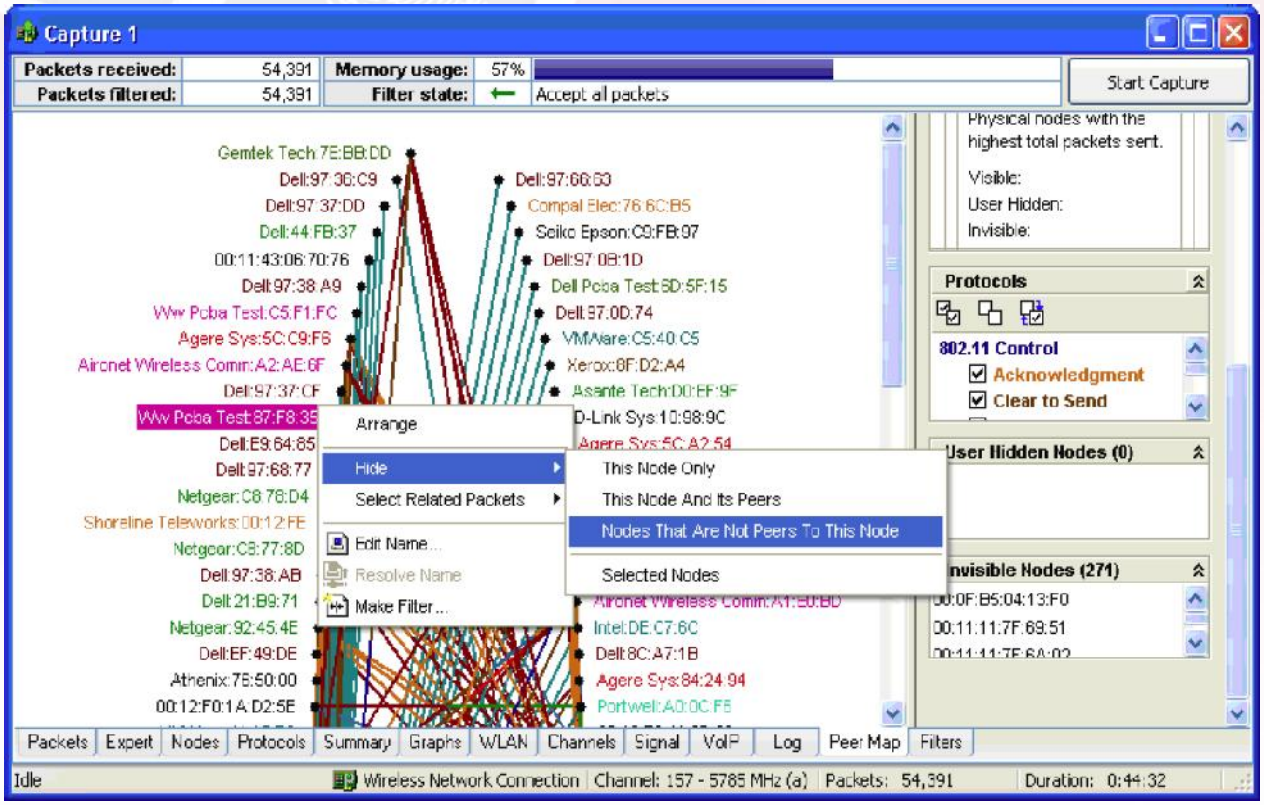
OmniPeek Workgroup is a full-featured, stand-alone network forensic analysis tool.
(http://www.wildpackets.com)



OmniPeek: Screenshots



OmniPeek: Screenshots



Tool: Iris Network Traffic Analyzer

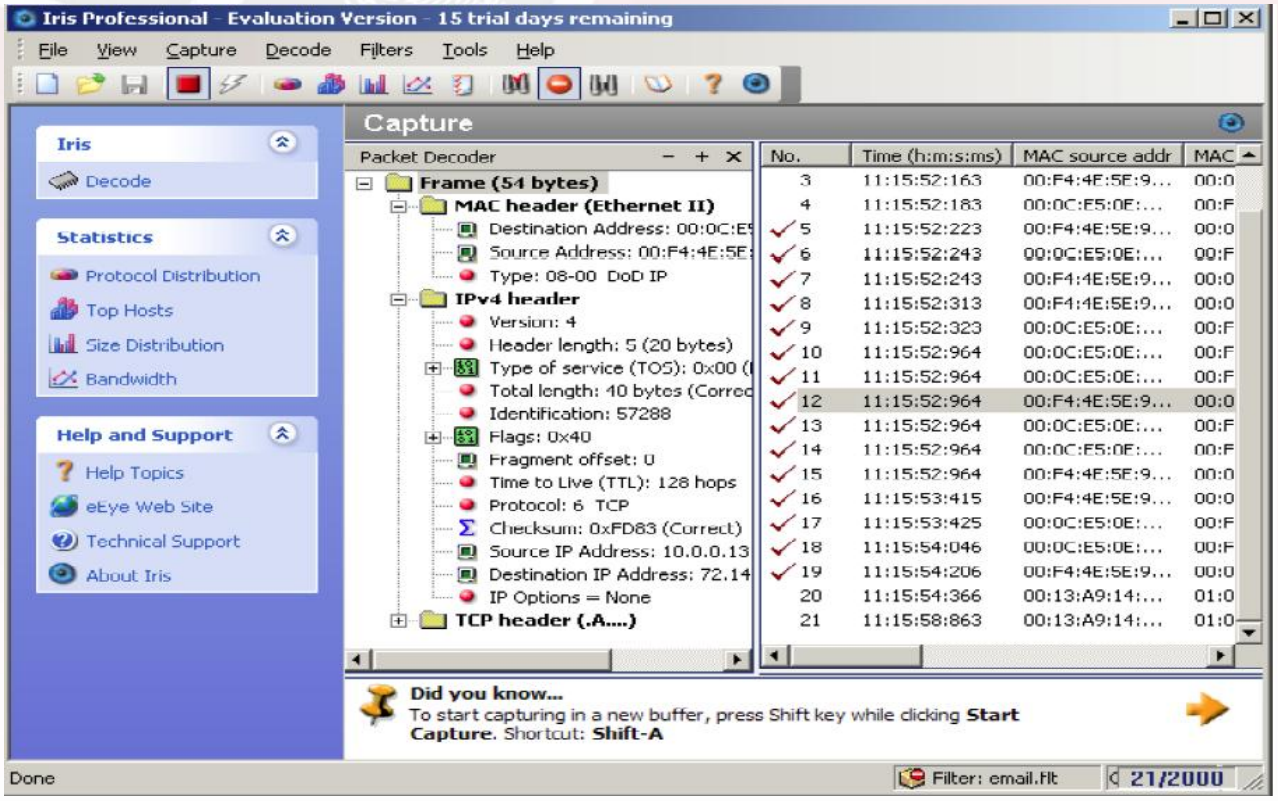
The Iris Network Traffic Analyzer is a vulnerability forensics solution used for network traffic analysis and reporting.

Iris captures network traffic and can automatically reassemble it to its native format.

Features of Iris Network Traffic Analyzer:

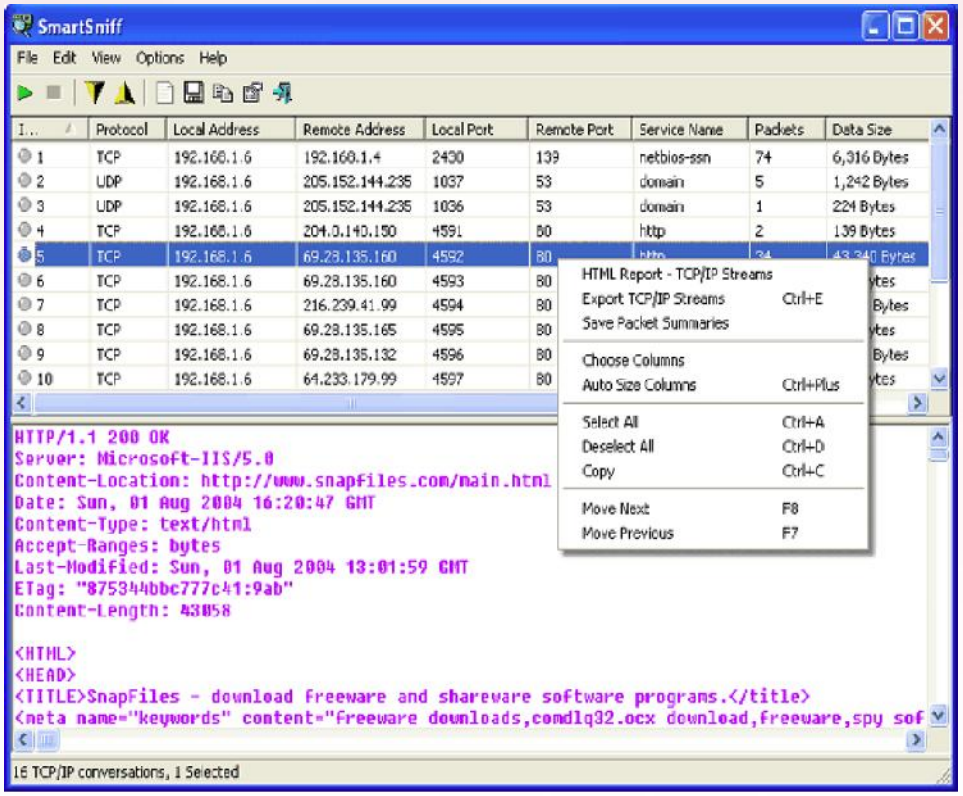
- Protocol Decoding
- Continuous Traffic Capture
- Create Custom Filters
- Complete Packet Reconstruction
- Powerful Sniffing and Spoofing Engine
- Screen Traffic by Key Criteria or Time Frame
- Alerting Capabilities
- Reconstruct TCP Sessions
- Packet Manipulation/Forging
- Log Foreign Connection Attempts
- Comprehensive Reporting
- Monitor Web-Based Email and Instant Messenger Services

Iris Network Traffic Analyzer : Screenshots



Tool: SmartSniff

- SmartSniff is a TCP/IP packet capture program that allows you to inspect network traffic that passes through your network adapter.
- It is a valuable tool to check what packets your computer is sending to the outside world.

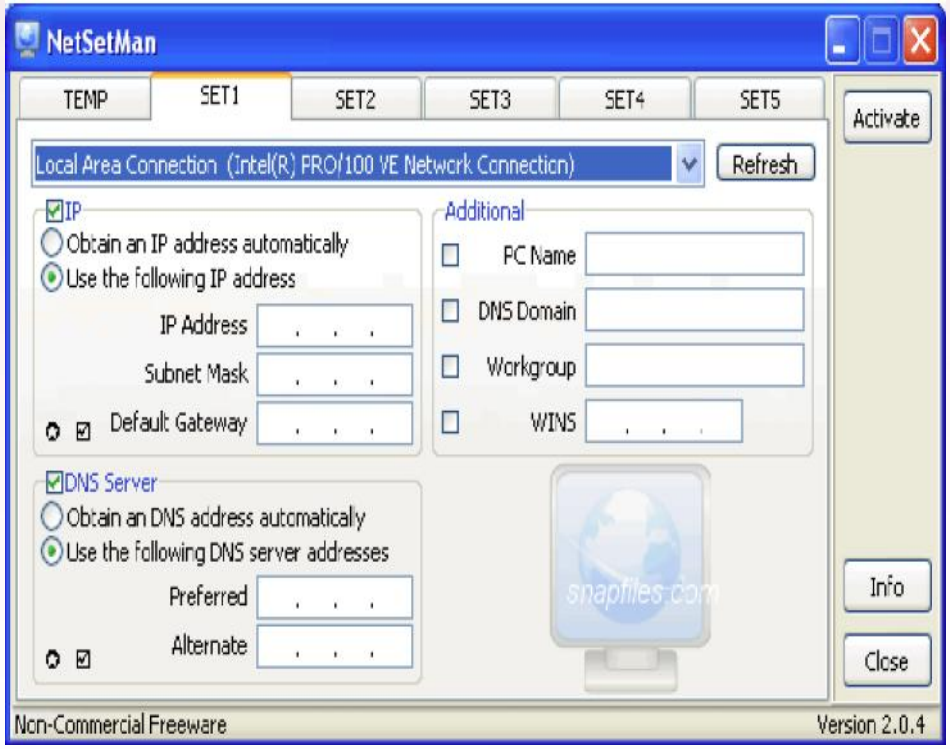


Tool: NetSetMan

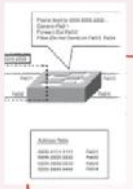
NetSetMan allows you to quickly switch between pre-configured network settings.

It is ideal for ethical hackers that have to connect to different networks all the time and need to update their network settings each time.

It allows you to create 6 profiles including IP address settings, Subnet Mask, Default Gateway, and DNS servers.



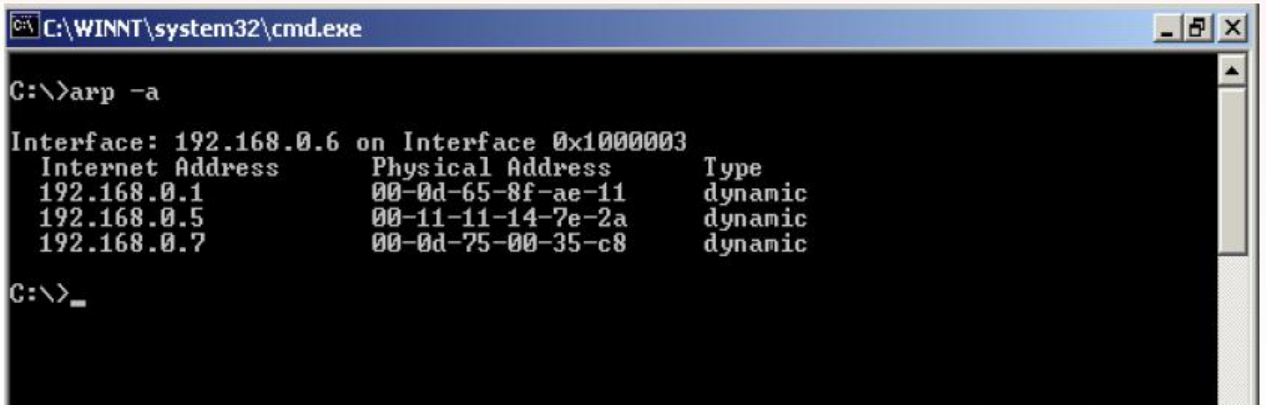
Evidence Gathering at the Data-link Layer



The MAC address , a part of the data-link layer, is associated with the hardware of a computer.

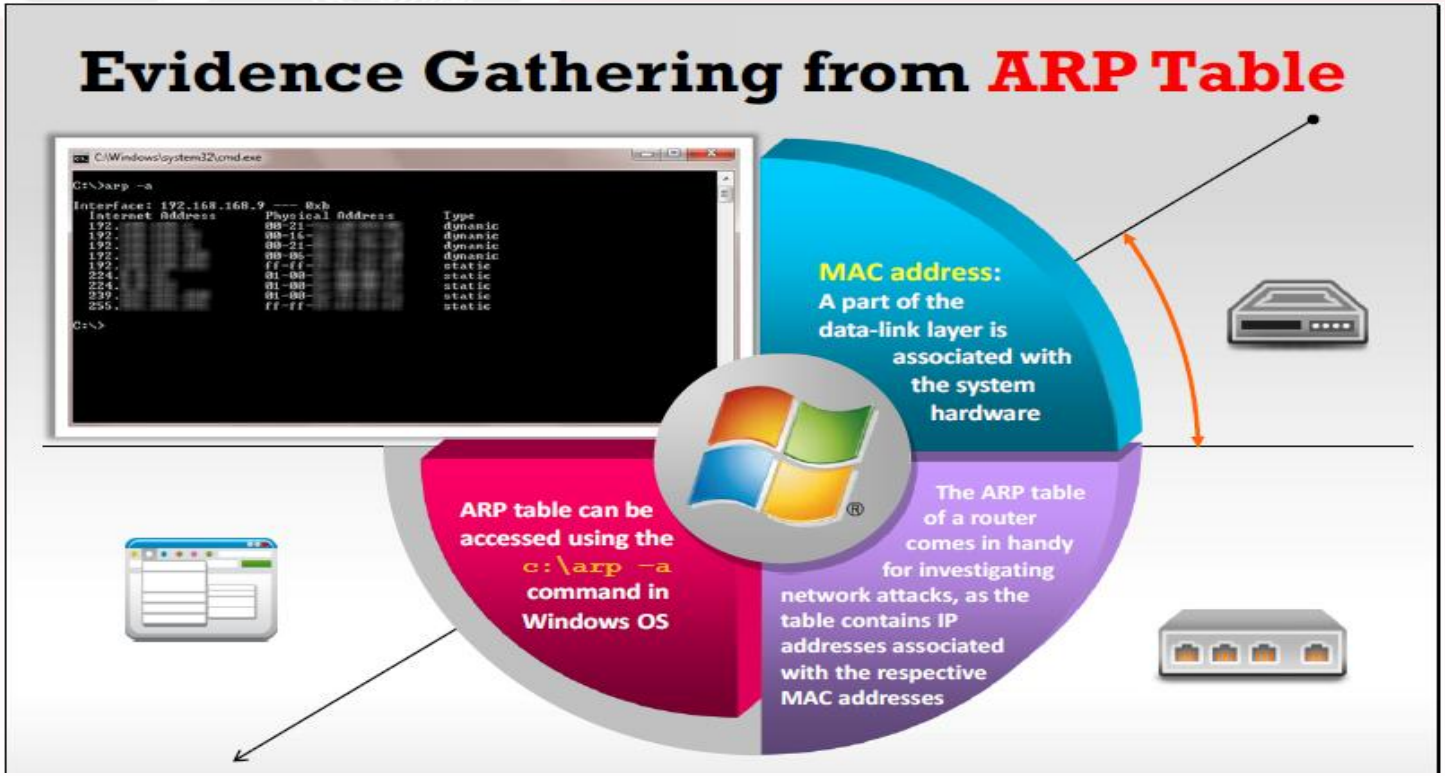
The ARP table of a router comes handy for investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.

ARP table can be seen using the given command in Windows OS
c:\arp -a



Evidence Gathering at the Data-link Layer: ARP Table

source: CHFI



Evidence Gathering at the Data-link Layer: DHCP Database

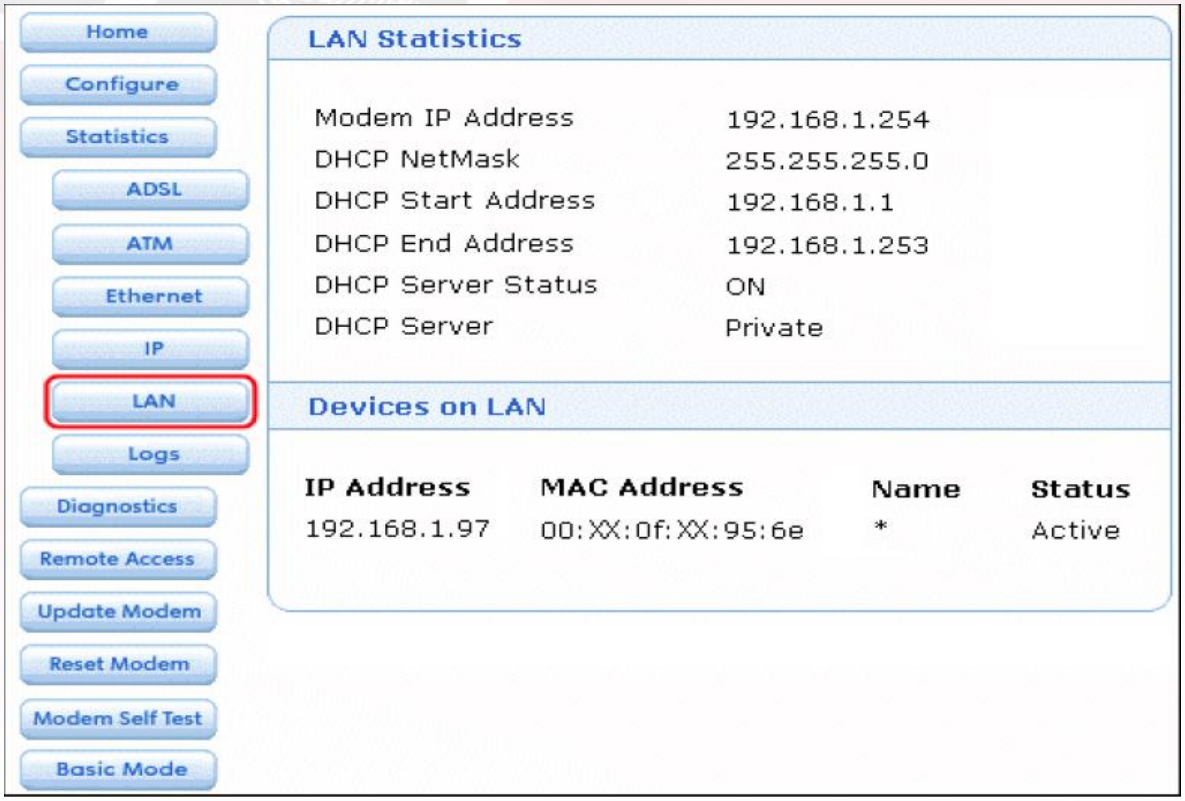
The DHCP database also provides as a means for determining the MAC addresses associated with the computer in custody.

The DHCP server maintains a list of recent queries, along with the MAC address and IP address.

Documentation of ARP table is done by the following:

- Photographing the computer screen.
- Screenshot of the table is taken and saved on the disk.
- The HyperTerminal logging facility is used.

Tool: DHCP Log



Evidence Gathering at the Data-link Layer: DHCP Database

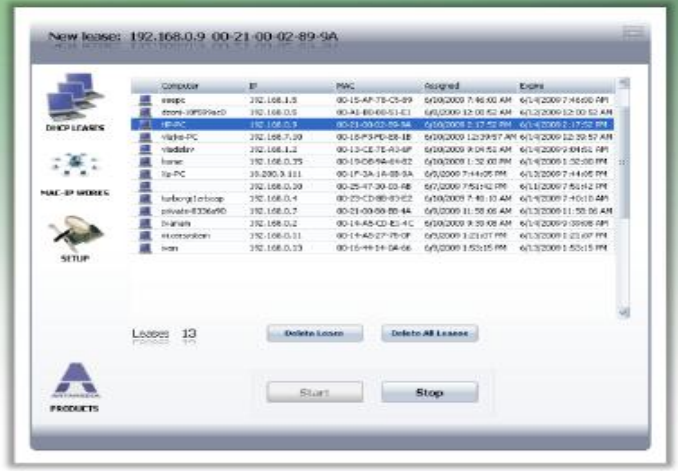
source: CHFI

Evidence Gathering at the Data-Link Layer: DHCP Database

- The DHCP database determines the **MAC addresses** associated with the computer in custody
- The DHCP server **maintains a list of recent queries** along with the MAC address and IP address

Documentation of the ARP table is done by:

- **Photographing** the computer screen
- Taking the **screenshot** of the table and saving it on a disk
- Using the **HyperTerminal logging** facility



Overview of Network and Transport Layer of the OSI Model

Network layer:

- It is responsible for sending information from the source to a destined address across various links.
- It adds logical addresses of the sender and receiver to the header of the data packet.

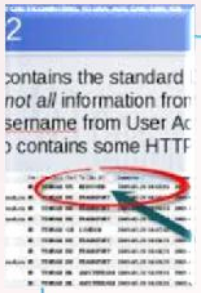
Transport layer:

- The transport layer ensures that the whole message sent by the source has reached its destination and is in order.
- It oversees the error control and flow control in between the transmission.

Evidence Gathering at the Network and Transport Layer

Authentication logs:

- Shows accounts related to a particular event.
- The IP address of the authenticated user gets stored in this log file.



Application logs:

- Application logging is meant for the storage of auditing information, which includes information produced by application activity.
- Web server logs help identify the system which was used as a means to commit the crime.
- Only administrator has the privilege to access these log files.

Operating System logs:

- It maintains log of events such as errors, system reboot, shutdown, security policy changes, user, and group management.
- But before enabling logging bear in mind: what to log otherwise, it can result in over-collection of data, making it difficult to trace the critical event.

Network device logs:

- Network devices such as router and firewalls are configured to send a copy of their logs to remote server, as the memory for these devices is low.
- The logs from network devices can be used as evidence for particular investigation on that network.

Gathering Evidence on a Network

Evidence on a Network

- IDS can be configured to capture network traffic when an alert is generated.
- Examination results of networking devices such as routers and firewalls, can be recorded through a serial cable using a Windows HyperTerminal program or by Script on UNIX.
- If the amount of information to be captured is huge, then record the onscreen event using a video camera or a relative software program.

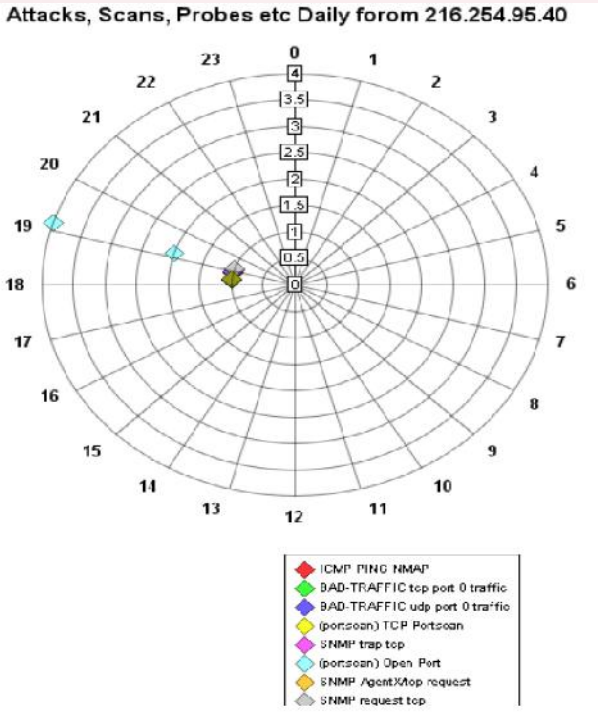
Gathering Evidence on a Network: Snort Intrusion Detection System

Snort is a versatile, lightweight, and very useful intrusion detection system.

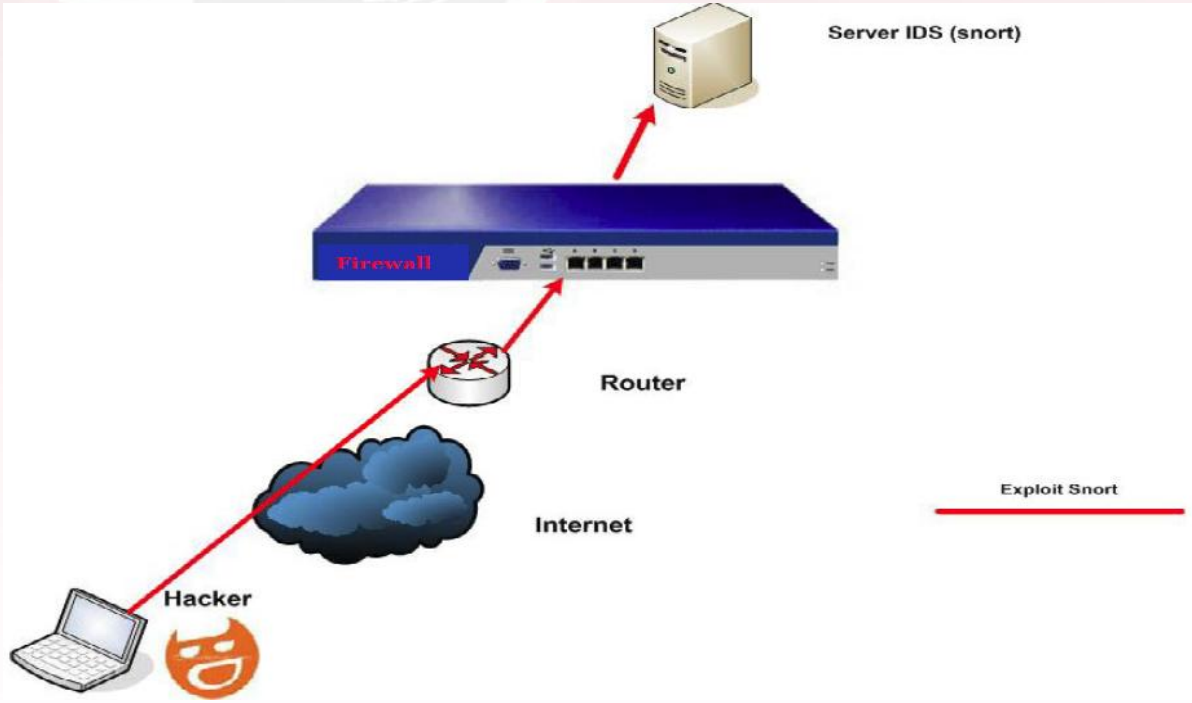
Snort logs packets in either tcpdump binary format or in Snort's decoded ASCII format to logging directories that are named based on the IP address of the foreign host.

Plug-ins allow the detection and reporting subsystems to be extended.

Available plug-ins include database logging, small fragment detection, portscan detection, and HTTP URI normalization.

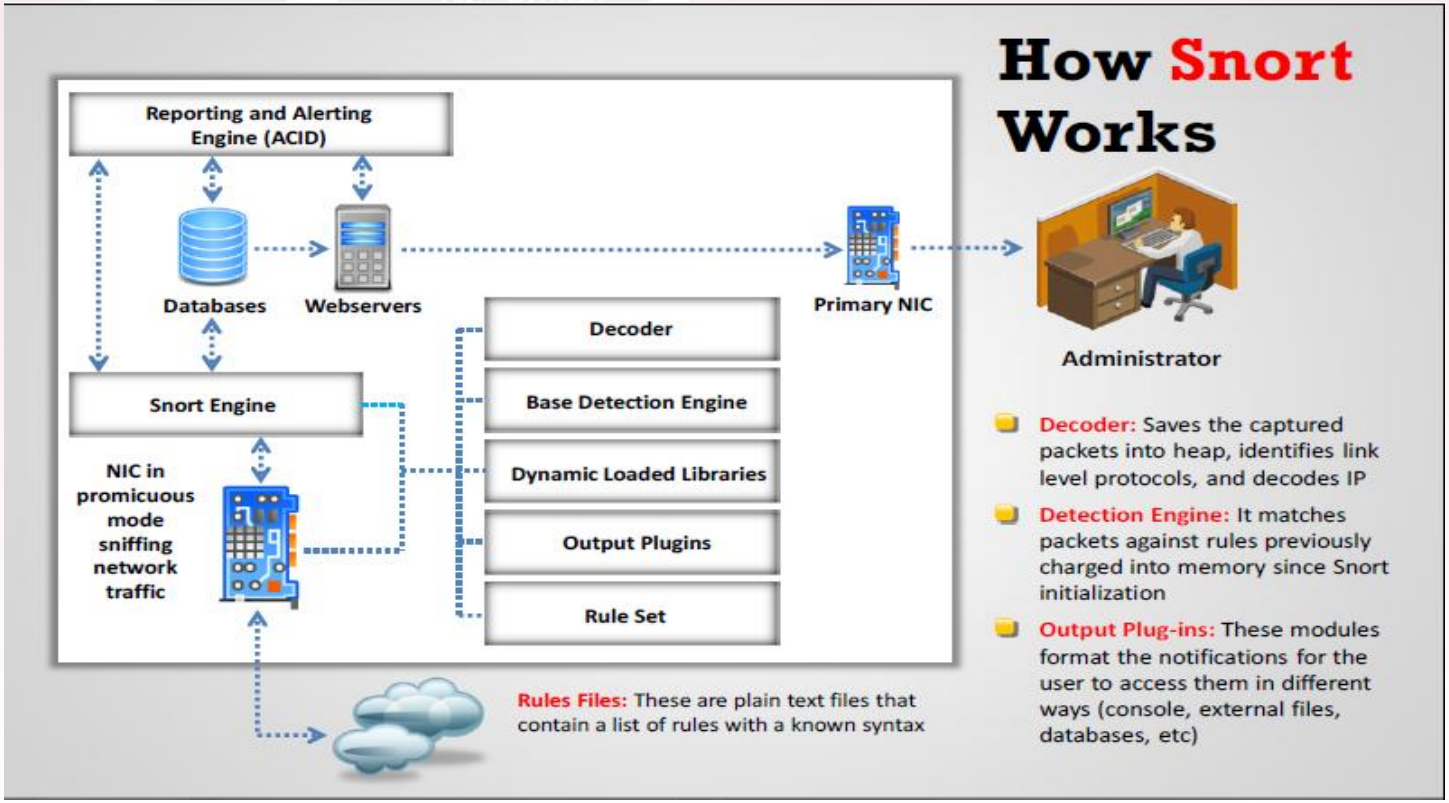


Gathering Evidence on a Network: Snort IDS Placement



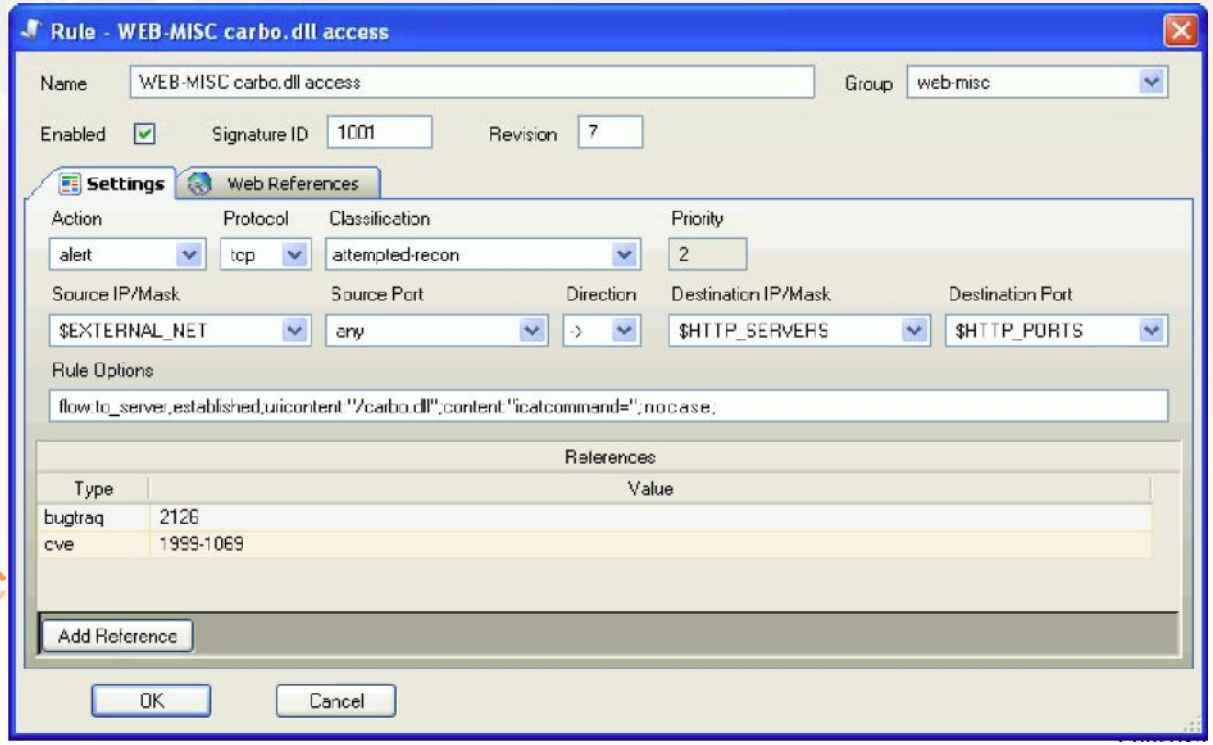
Gathering Evidence on a Network: Snort

source: CHFI



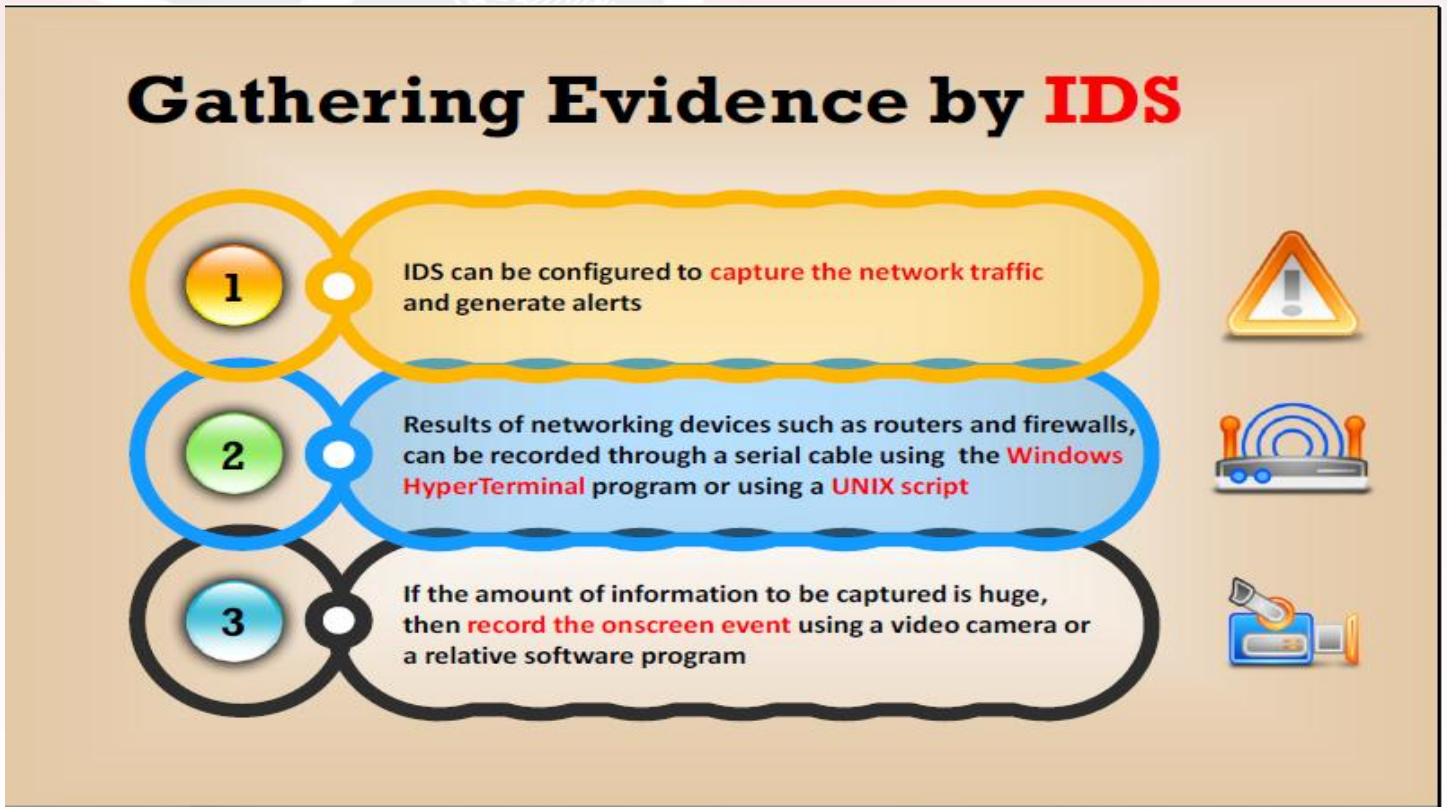
Gathering Evidence on a Network: IDS Policy Manager

IDS Policy Manager has been the de facto standard for managing Snort rules on Windows. You can create Snort rules graphically.

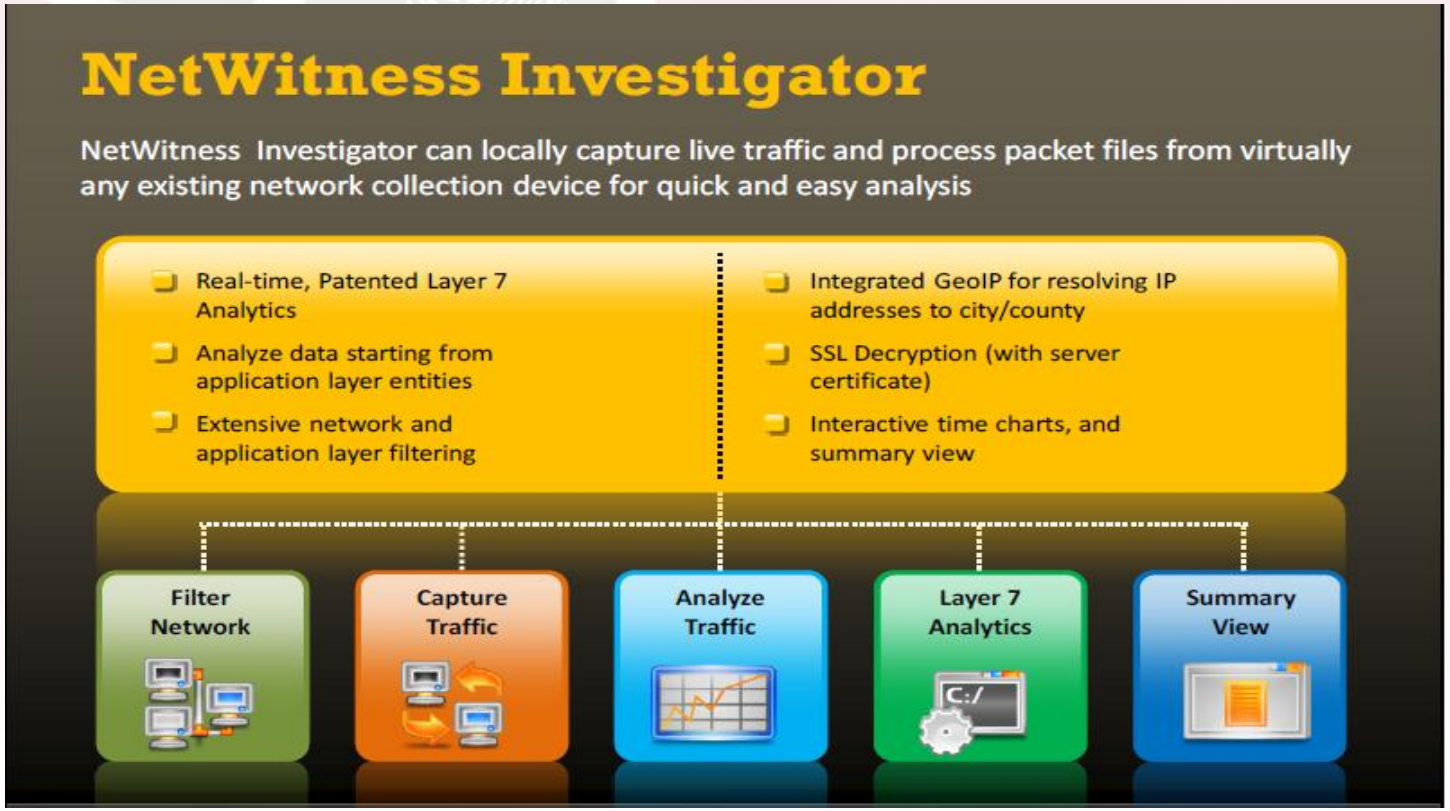


Gathering Evidence on a Network: IDS

source: CHFI



Tool: NetWitness



Documenting the Evidence Gathered on a Network

If the network logs are small, you can take a print-out and test.

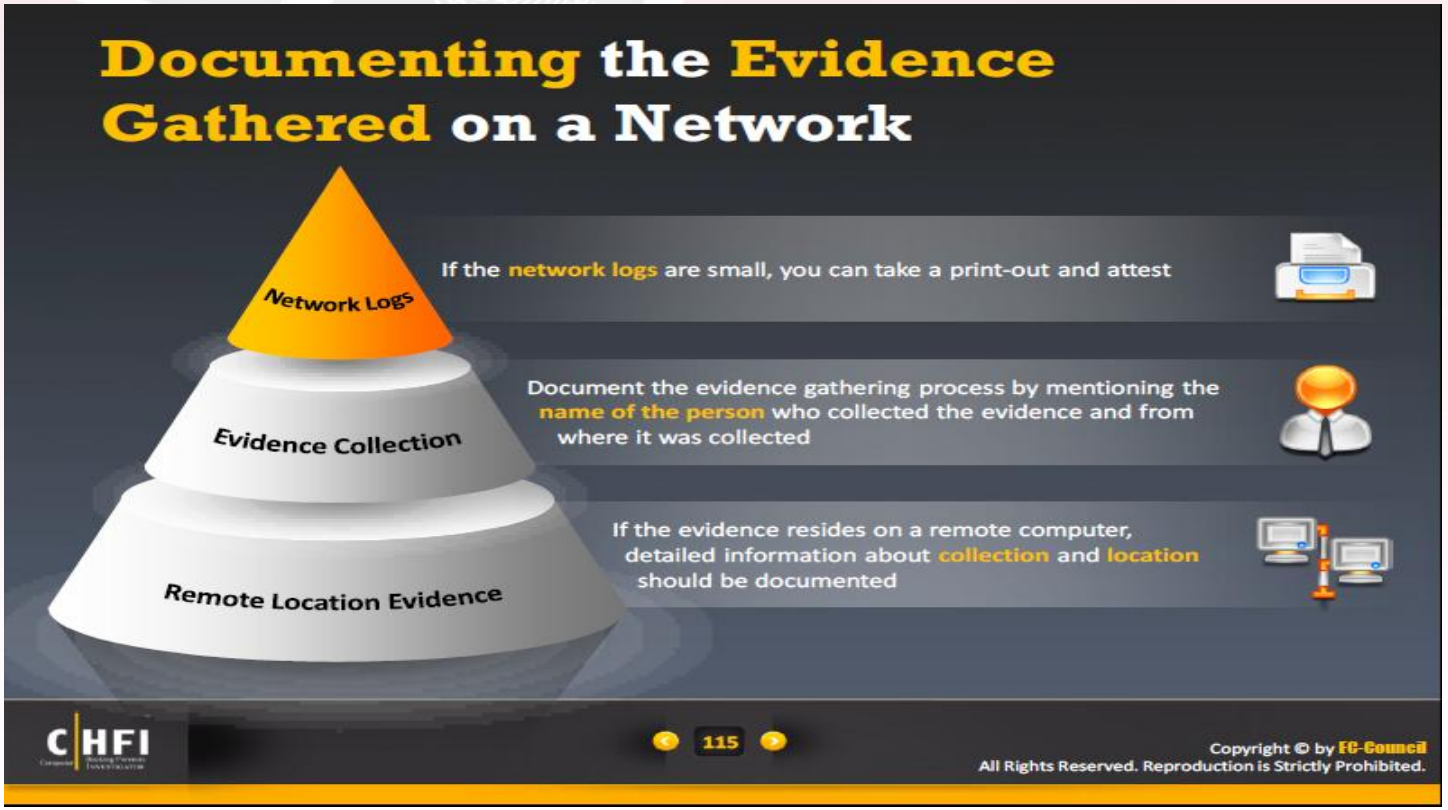
Document the evidence gathering process by mentioning the name of the person who collected the evidence, from where it was collected.

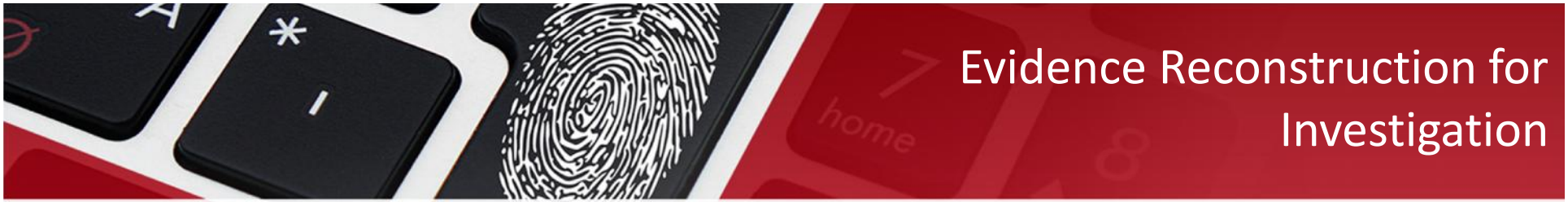
- The procedure used to collect evidence and the reason for collecting evidence.

The process of documenting digital evidence on a network becomes more complex when the evidence is gathered from systems which are on remote locations.

Documenting the Evidence Gathered on a Network

source: CHFI





Evidence Reconstruction for Investigation

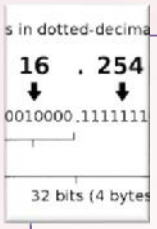
Gathering evidence trails on a network is very cumbersome for the following reasons:

- Evidence is not static and is not concentrated at a single point on the network.
- The variety of hardware and software found on the network makes the evidence gathering process more difficult.

Three fundamentals of reconstruction for investigating crime are:

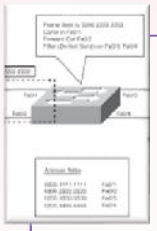
- Temporal analysis; helps to identify time and sequence of events.
- Relational analysis; helps to identify the link between suspect and the victim with respect to the crime.
- Functional analysis; helps to identify events that triggered the crime.

Summary



There are two types of network addressing schemes: LAN Addressing and Internetwork Addressing.

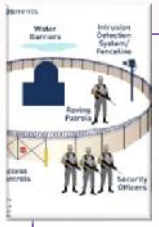
Sniffer is computer software or hardware that can intercept and log traffic passing over a digital network or part of a network.



The ARP table of a router comes handy for investigating network attacks as the table contains IP addresses associated with the respective MAC addresses.

The DHCP server maintains a list of recent queries along with the MAC address and IP address.

Application logging is meant for the storage of auditing information, which includes information produced by application activity.



IDS can be configured to capture network traffic when an alert is generated.