

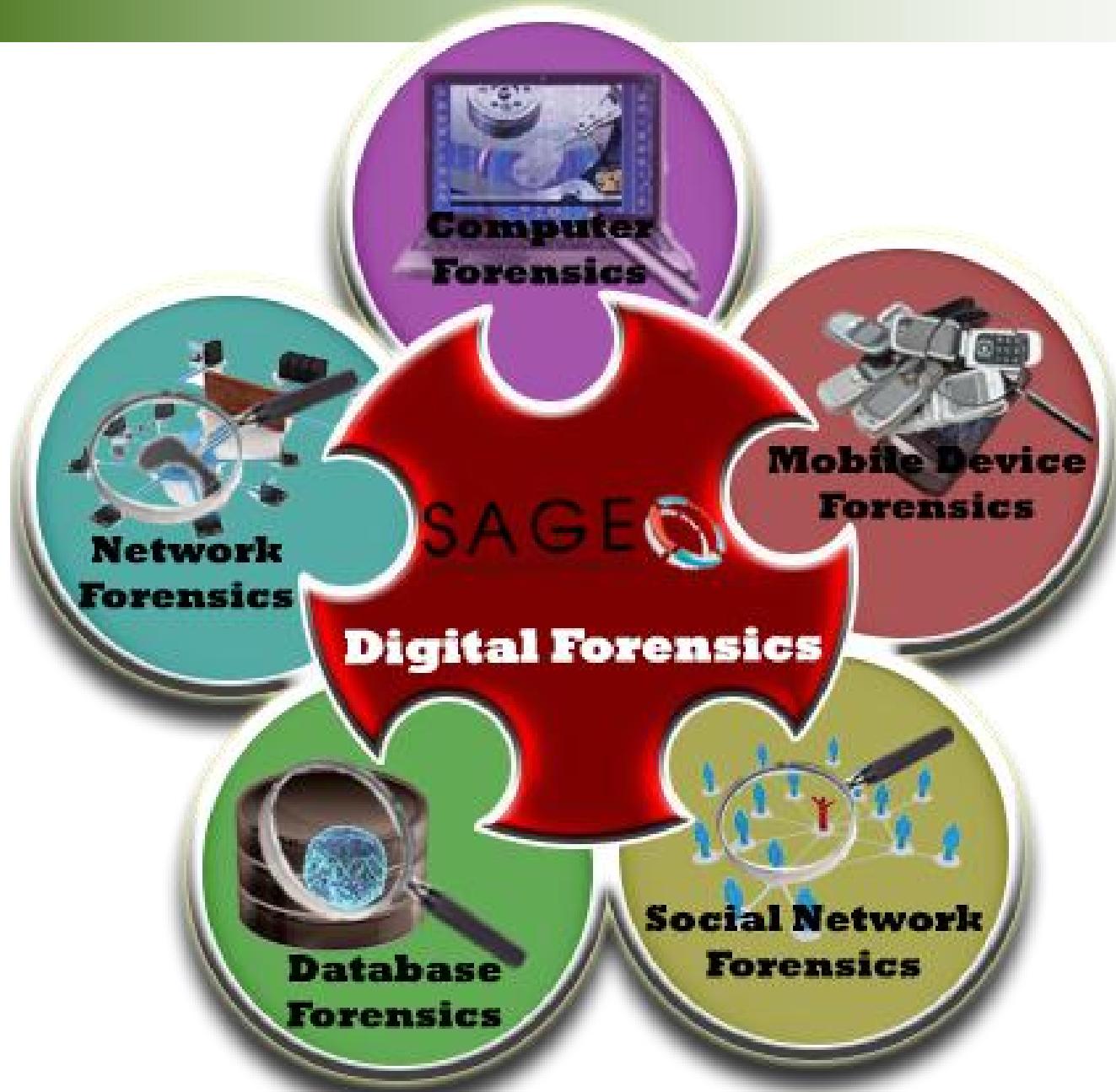
Digital Forensics

Pháp chứng Kỹ thuật số

#6: Network Forensics
Spring 2022



ThS. Lê Đức Thịnh
thinhld@uit.edu.vn



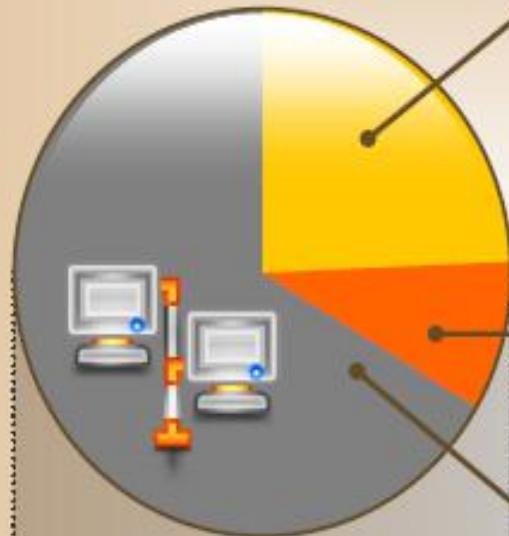


HỎI: Trong ngũ cảnh nào cần làm pháp chứng mạng?

Module Flow



Network Forensics



Network forensics is the process of identifying **criminal activity** and the people behind it

Network forensics can be defined as the **sniffing, recording, acquisition** and **analysis** of the network traffic and event logs in order to investigate a network security incident

It allows investigators to inspect **network traffic** and **logs** to identify and locate the attack system



Network forensics can reveal:

- ⌚ Source of security incidents and network attacks
- ⌚ Path of the attack
- ⌚ Intrusion techniques used by attackers



Các hướng điều tra Pháp chứng mạng

- **An toàn mạng:** khi giám sát một mạng máy tính có lưu lượng truy cập bất thường và xác định sự xâm nhập.
 - Kẻ tấn công có khả năng xóa tất cả các tập tin đăng nhập trên một máy chủ bị tấn công, do vậy bằng chứng dựa trên lưu lượng mạng có thể là bằng chứng duy nhất để phân tích pháp chứng.
- **Tội phạm trên mạng:** Trong trường hợp phân tích các gói tin thu được có thể bao gồm các nhiệm vụ như nối ghép tập tin chuyển giao, tìm kiếm cho các từ khóa và phân tích thông tin liên lạc như email hoặc các buổi trò chuyện.

Các câu hỏi cần phải trả lời

- Ai là kẻ xâm nhập và làm thế nào họ thâm nhập vào các biện pháp phòng ngừa an ninh hiện hành?
- Những gì thiệt hại đã xảy ra?
- Những kẻ xâm nhập sau khi rời khỏi hệ thống mạng đã để lại điều gì trên hệ thống như một tài khoản người dùng mới, một Trojan hoặc Worm hoặc phần mềm Bot?
- Chúng ta đã nắm bắt được đầy đủ dữ liệu để phân tích và mô phỏng lại cuộc tấn công và việc sửa chữa?

Pháp chứng mạng và giao thức mạng

- Người điều tra viên khi tiến hành điều tra trên Mạng cần hiểu biết rõ giao thức của Mạng mà mình đang điều tra.
- Các thông tin cần hiểu biết:
 - Cấu trúc các gói tin của các tầng giao thức
 - Các giao thức của bộ giao thức trong mạng
 - Các quy trình hoạt động
- Người điều tra viên cần sử dụng thành thạo các công cụ nhằm tìm được các bằng chứng số liên quan đến yêu cầu của mình.

Overview of Network Protocols

	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 and LLC)	PPP, SLIP
	Bits	Physical	Media, signal and binary transmission	

Network Addressing Schemes

There are two types of network addressing schemes

LAN Addressing

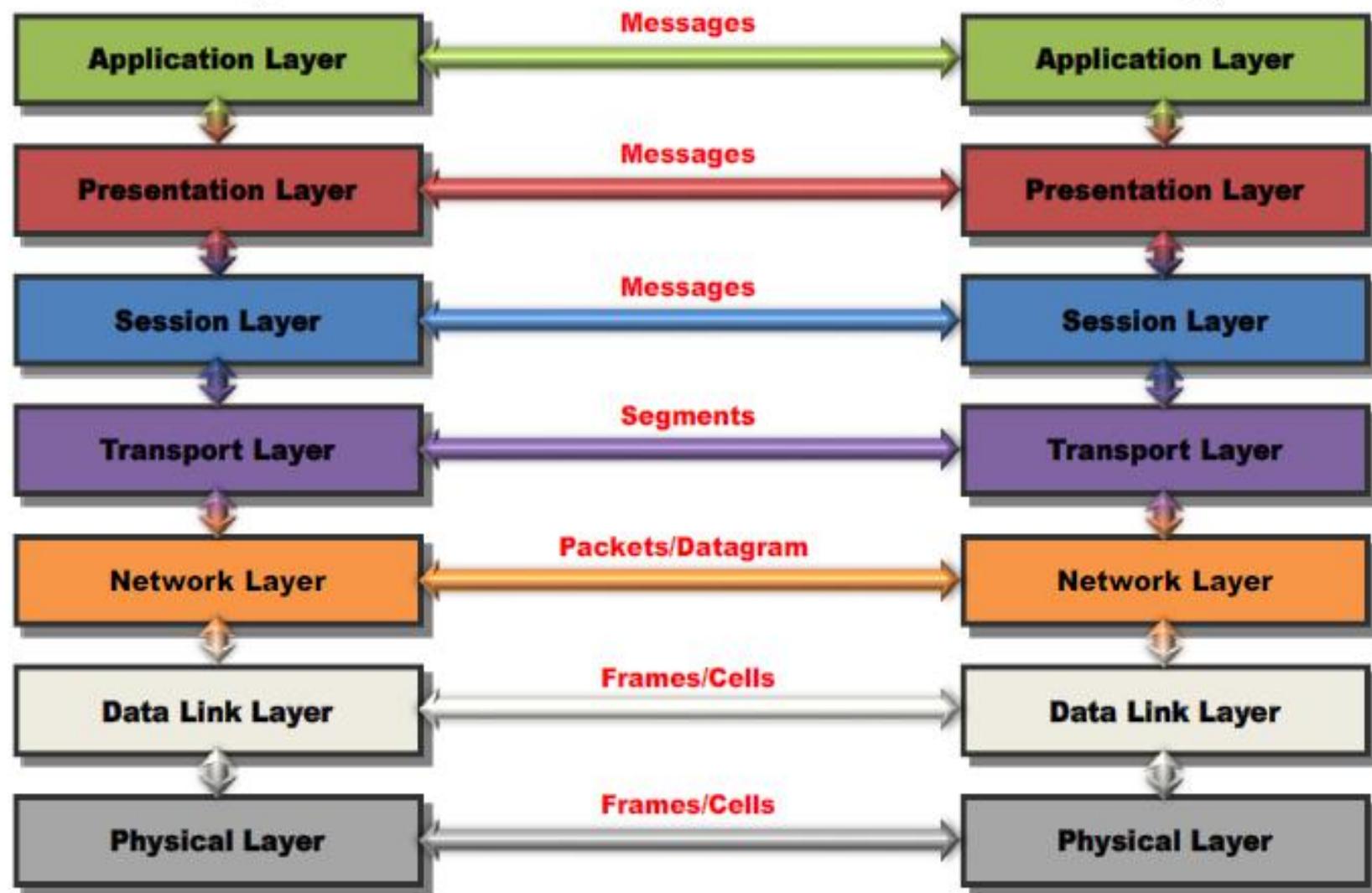
- Each node in LAN has a **MAC address** that is factory-programmed into its NIC
- Data packets are addressed to either one of the nodes or all of the nodes



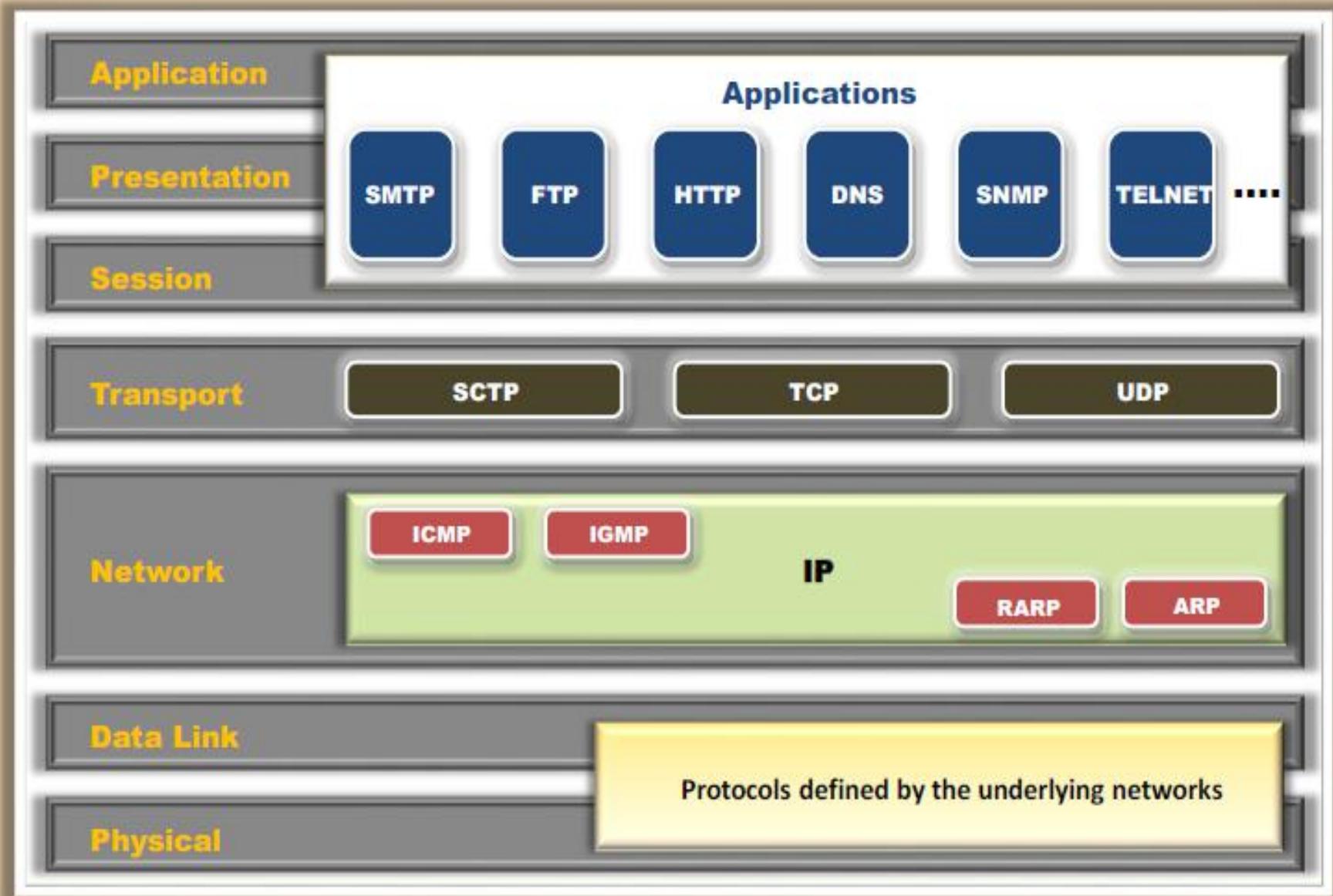
Internet Addressing

- Internet 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 **Internet address is a combination of network and node addresses**
- IP is responsible for network layer addressing in the **TCP/IP protocol**

OSI Reference Model



TCP/ IP Protocol





IP Address
Spoofing

Data
Modification
Attacks

Session
Sniffing

Packet
Sniffing

Port
Scanning



Man-in-the-
Middle Attack



Trojan Horse

Enumeration

Denial of
Service (DoS)

Buffer
Overflow



Email
Infection

Malware
Attacks

Virus and
Worms

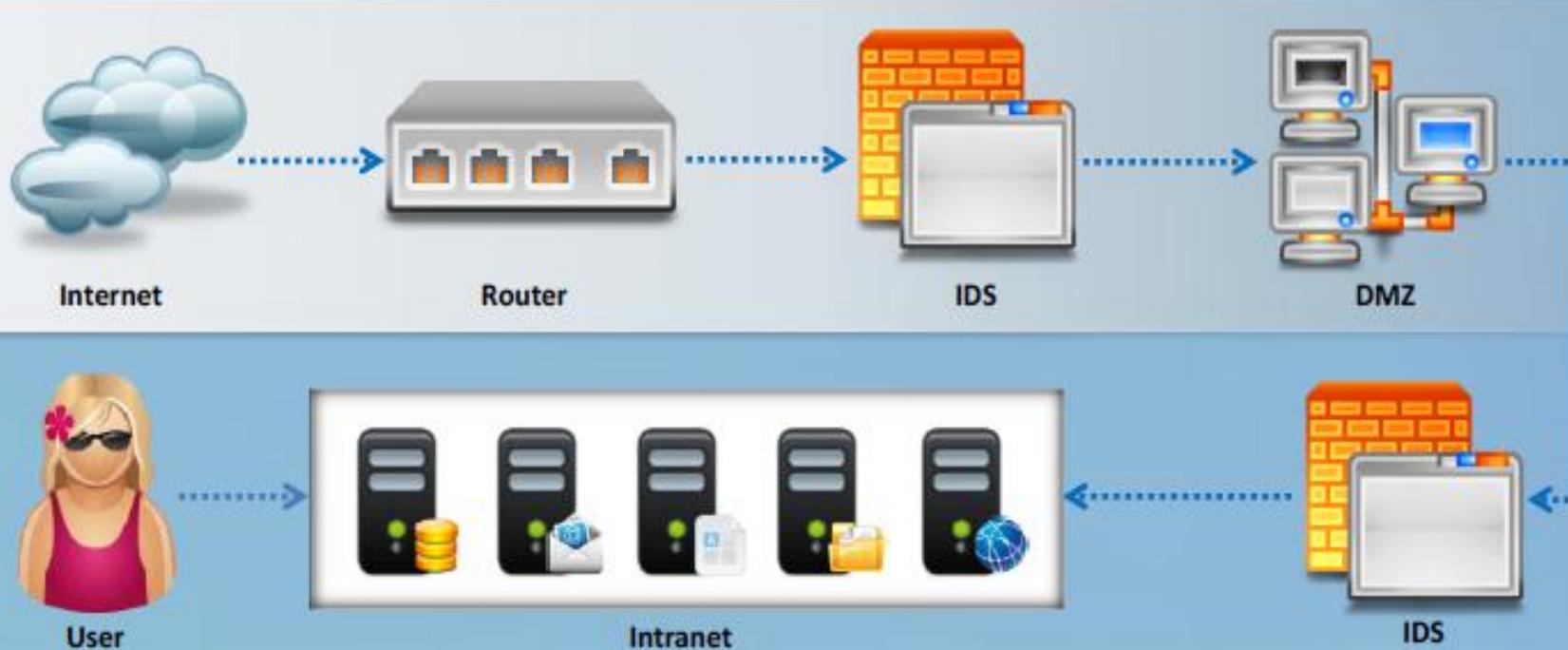


Types of Network Attacks



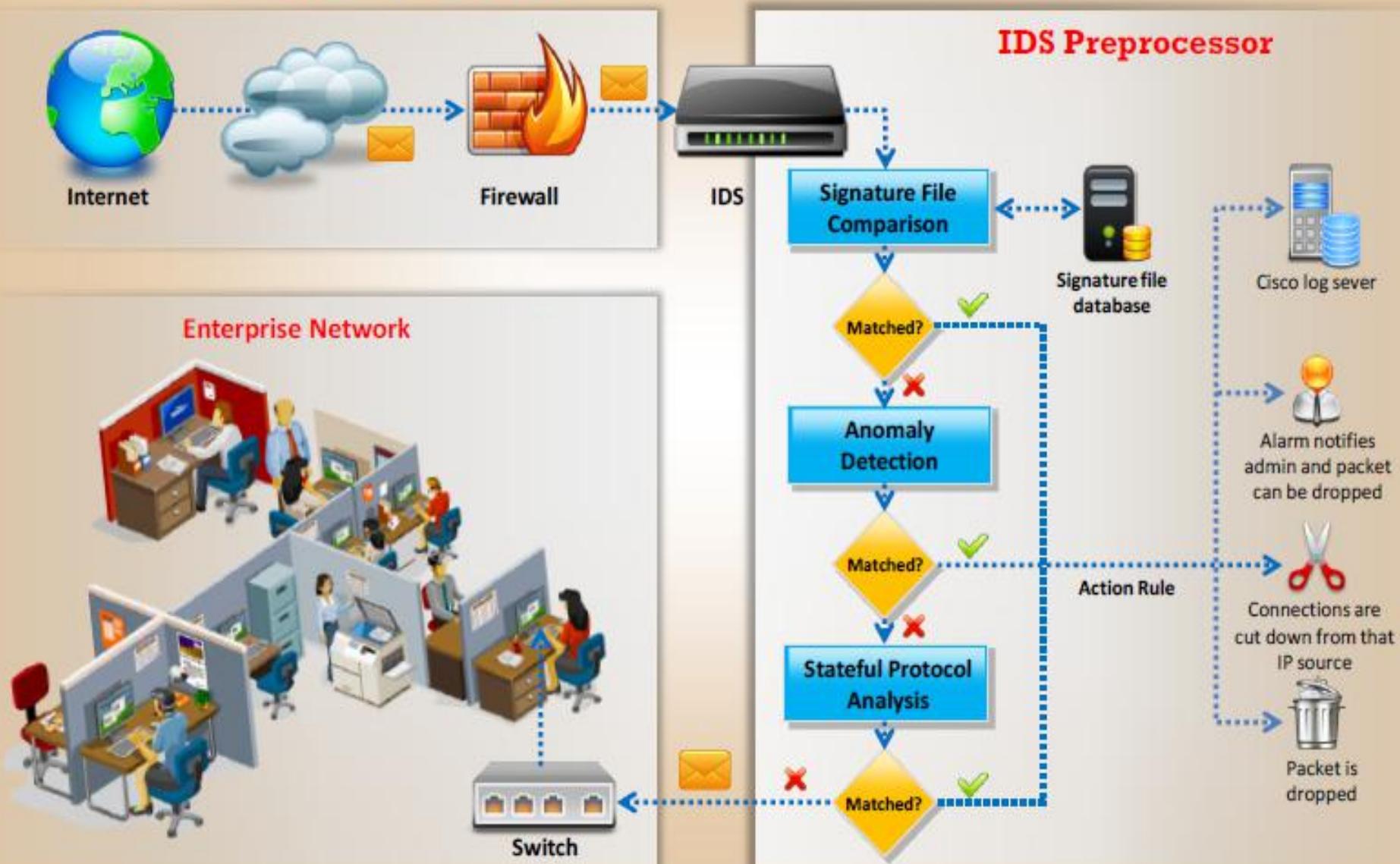
CÁC KỸ THUẬT GIÁM SÁT/ ĐIỀU TRA THÔNG THƯỜNG

Intrusion Detection Systems (IDS) and Their Placement



- An intrusion detection system (IDS) **gathers and analyzes information** from within a computer or a network to **identify** the possible violations of security policy, including unauthorized access, as well as misuse
- An IDS is also referred to as a "**packet-sniffer**," which intercepts packets traveling along various communication mediums and protocols, usually TCP/IP
- The packets are analyzed after they are **captured**
- An IDS evaluates a **suspected intrusion** once it has taken place and signals an alarm

How IDS Works



Types of Intrusion Detection Systems

Network-Based Intrusion Detection

- These mechanisms typically consist of a **black box** that is placed on the network in the promiscuous mode, listening for patterns indicative of an intrusion



Log File Monitoring

- These mechanisms are typically programs that **parse log files** after an event has already occurred, such as failed login attempts



Host-Based Intrusion Detection

- These mechanisms usually include **auditing for events** that occur on a specific host
- These are not as common, due to the overhead they incur by having to **monitor each system event**



File Integrity Checking

- These mechanisms check for **Trojan horses**, or **files** that have otherwise been modified, indicating an intruder has already been there, for example, Tripwire



General Indications of Intrusions



File System Intrusions

- ▀ The presence of new, unfamiliar files or programs
- ▀ Changes in file permissions
- ▀ Unexplained changes in the file's size
- ▀ Rogue files on the system that do not correspond to your master list of signed files
- ▀ Unfamiliar file names in directories
- ▀ Missing files



Network Intrusions

- ▀ Repeated probes of the available services on your machines
- ▀ Connections from unusual locations
- ▀ Repeated login attempts from remote hosts
- ▀ Arbitrary data in log files, indicating an attempt at creating either a Denial of Service, or a crash service

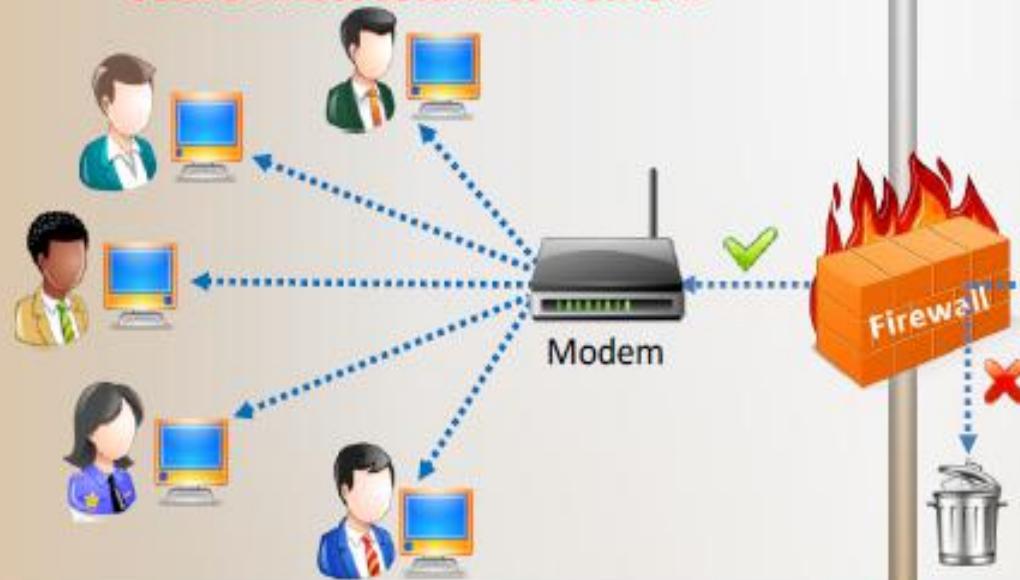


Firewall

- Firewall is hardware, software, or a combination of both designed **to prevent unauthorized access** to or from a private network
- It is placed at the **junction point, or gateway** between the two networks, which is usually a private network and a public network such as the **Internet**
- Firewall **examines all messages entering or leaving the intranet** and blocks those that do not meet the specified security criteria
- Firewalls may be concerned with the **type of traffic** or with the **source or destination addresses and ports**



Secure Private Local Area Network



Public Network



Internet

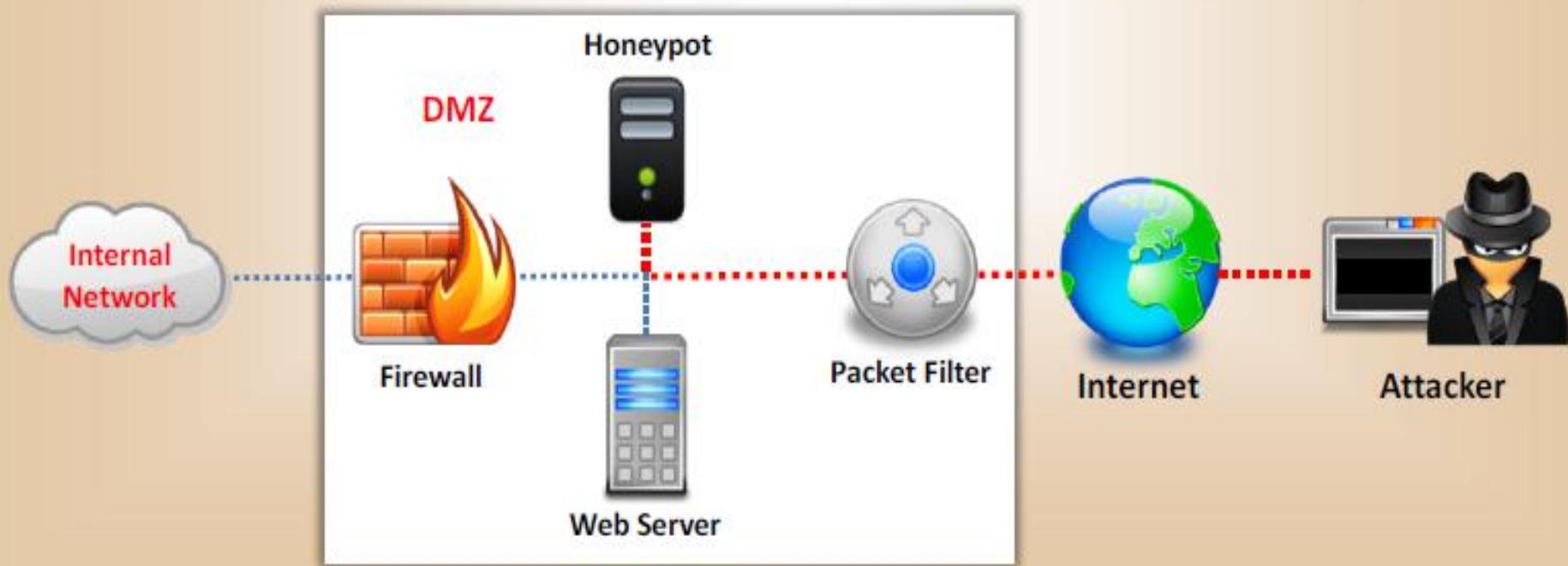
- ✓ = Specified traffic allowed
- ✗ = Restricted unknown traffic

Honeypot

Honeypot is an information system resource that is expressly **set up to attract and trap people** who attempt to penetrate an organization's network

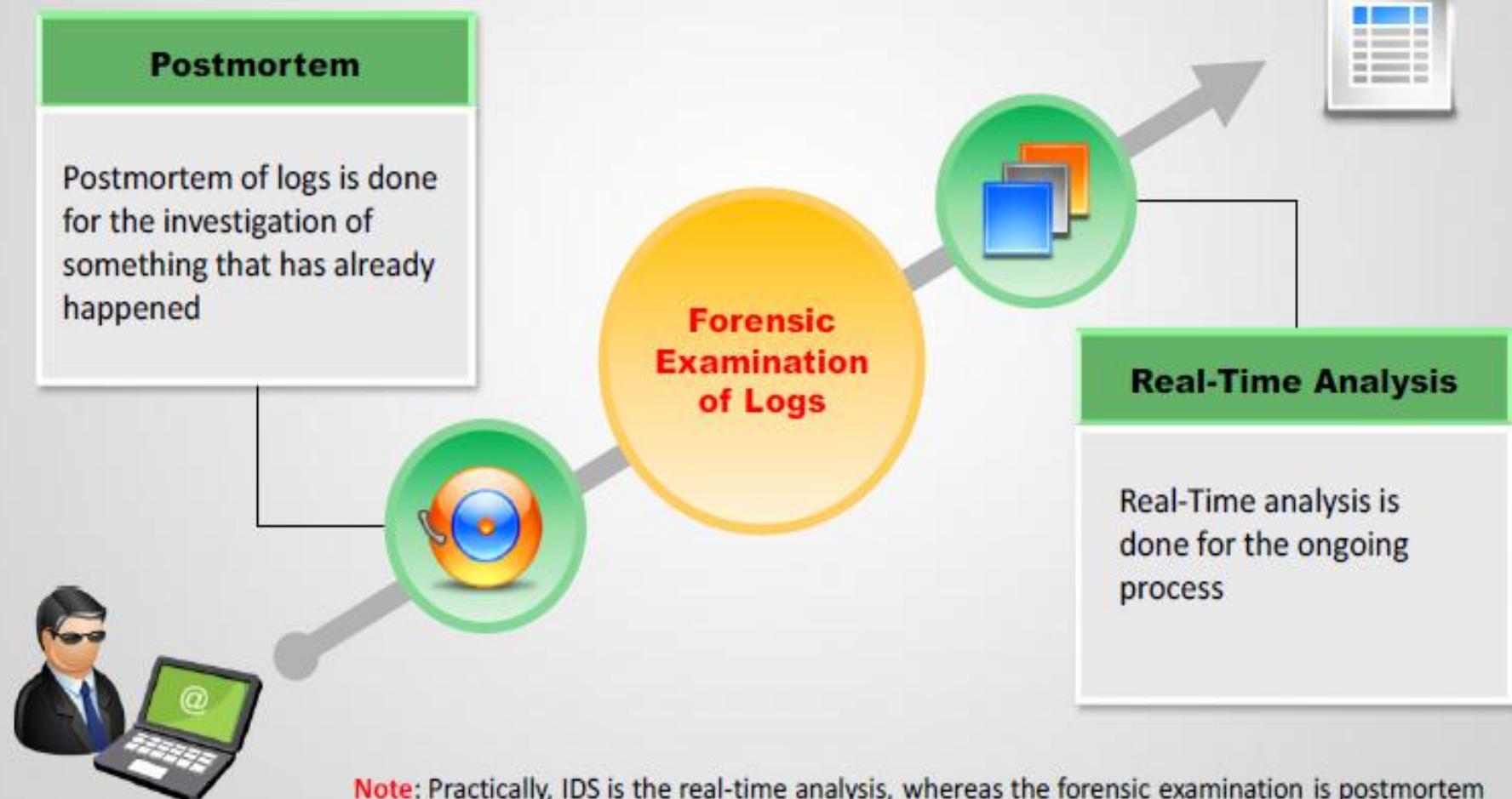
It has no authorized activity, does not have any production value and is **susceptible a probe, attack, or compromise**

A honeypot can be used to **log access attempts** to those ports including the attacker's keystrokes. This could send early warnings of a more concerted attack



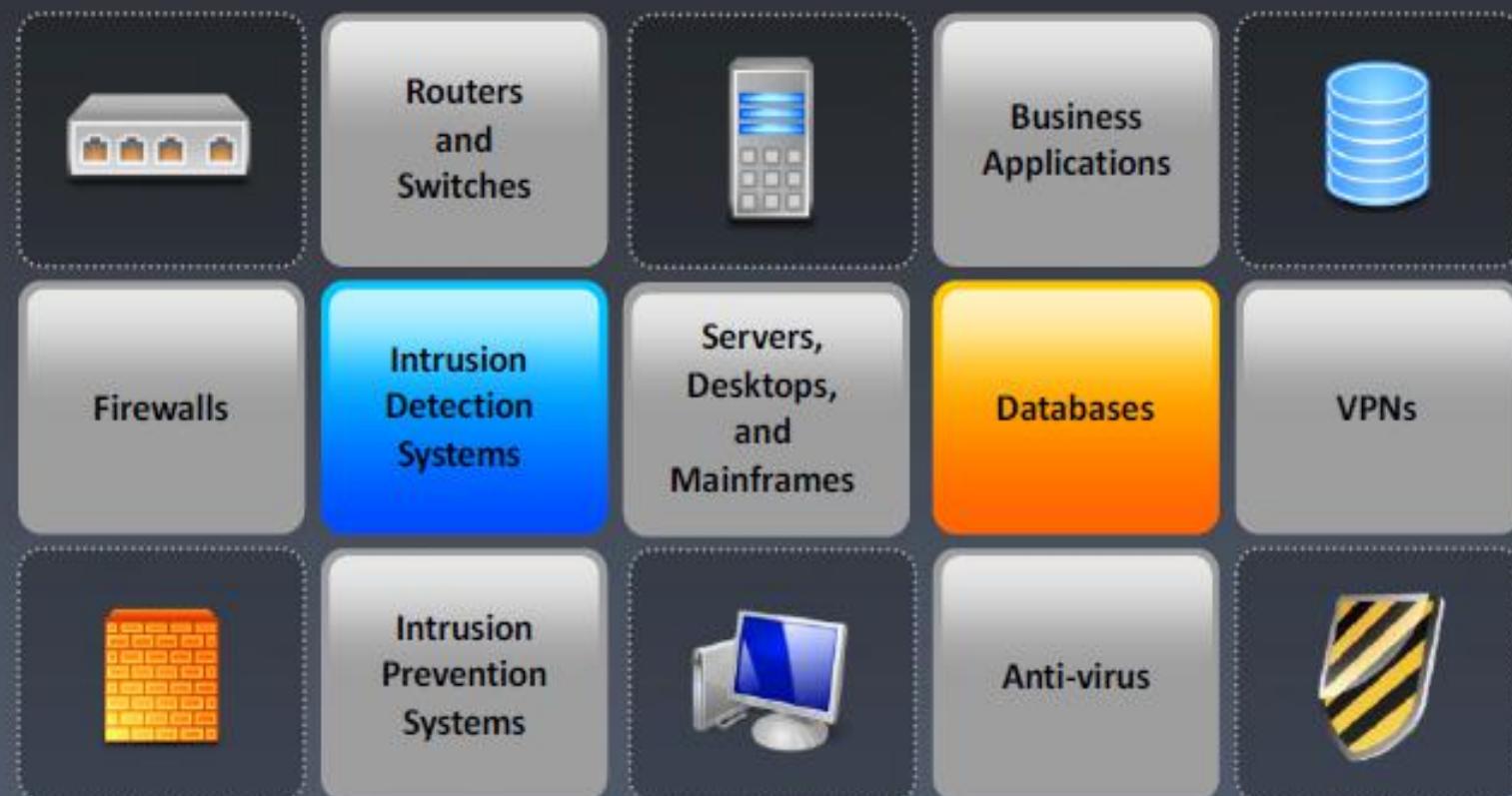
Postmortem and Real-Time Analysis

Forensic examination of logs are divided into two categories :



Where to Look for Evidence

- Use **Log capturing tools** to capture log files of various devices and applications
- Log files from the following devices and applications can be used as evidence for network security incidents:



Note: For complete coverage of log investigations, refer to the modules "Investigating Web Attacks" and "Windows Forensics"

Log Capturing Tool: ManageEngine EventLog Analyzer

ManageEngine EventLog Analyzer 6

Dashboard View: (Customize)

Date: Time Range: May, 2008

Reports: My Reports, Top N Reports, Compliance Reports, Trend Reports

IIS W3C Web Server Logs

Overview

	Critical	Error	Warning	Information	Total
Event Count	575	1,221	146	1,153	3,000

Hosts

Name	Critical	Error	Warning	Information	Total
app01host	575	1,221	146	1,153	3,000

Reports

Report	Total Events	Top Events
Browser Usage Report	1,963	
Cross Site Scripting Attempts	536	
File Type Report	1,963	
Filez Report	250	
HTTP Error Status Codes Report	1,837	
Malicious URLs Report	525	
OS Usage Report	1,963	
Page-URL Report	250	
SQL Injection Attempts	202	
User Events	0/0	

<http://www.manageengine.com>

- EventLog Analyzer is a web-based, real time **event log** and **application log** monitoring and management software
- It collects, analyzes, reports, and archives:
 - **Event Log** from distributed Windows hosts
 - **SysLog** from distributed Unix hosts, routers, switches, and other SysLog devices
 - **Application logs** from IIS Web server, IIS FTP server, MS SQL server, Oracle database server, DHCP Windows and DHCP Linux servers

Log Capturing Tool: ManageEngine Firewall Analyzer



■ ManageEngine Firewall Analyzer is a firewall log analysis tool for **security event management** that collects, analyzes, and archives logs from network perimeter security devices and generates reports



The screenshot shows the ManageEngine Firewall Analyzer 5 interface. At the top, there's a navigation bar with links for Home, Reports, Alerts, Settings, Ask ME, Support, and Search Here. Below the navigation bar is a dashboard section with several charts and graphs. One chart shows traffic overview by protocol (Web, Secure Shell, Mail, Unassigned, FTP, Name Service, Webex Protocols, File Sharing, SMTP, Database Application, KMP, Streaming, Telnet, Network Security, News, Services, Microsoft, Printer, Network Management, Routing) over time. Another chart shows security events by device (Datacenter, My Firewall). Below these are two tables: Traffic Statistics and Security Statistics, showing detailed traffic and event data for different devices and protocols.

Device Name	Protocol Group	Traffic IN (MB)	Traffic OUT (MB)	Total Traffic (MB)
MyFirewall	Web	44%	105559.6	134162.15
MyFirewall	Secure Shell	20%	32859.61	36816.97
MyFirewall	Mail	9%	15319.75	25337.9
MyFirewall	Unassigned	3%	8730.79	9938.69
MyFirewall	FTP	1%	1927.17	9163.08
MyFirewall	Others	1%	985.43	1600.93
MyFirewall	Total	100%	165382.34	217019.73
Datacenter	Web	76%	114122.57	130734.75
Datacenter	Mail	10%	15772.68	25872.52
Datacenter	Unassigned	7%	11210.01	12639.38

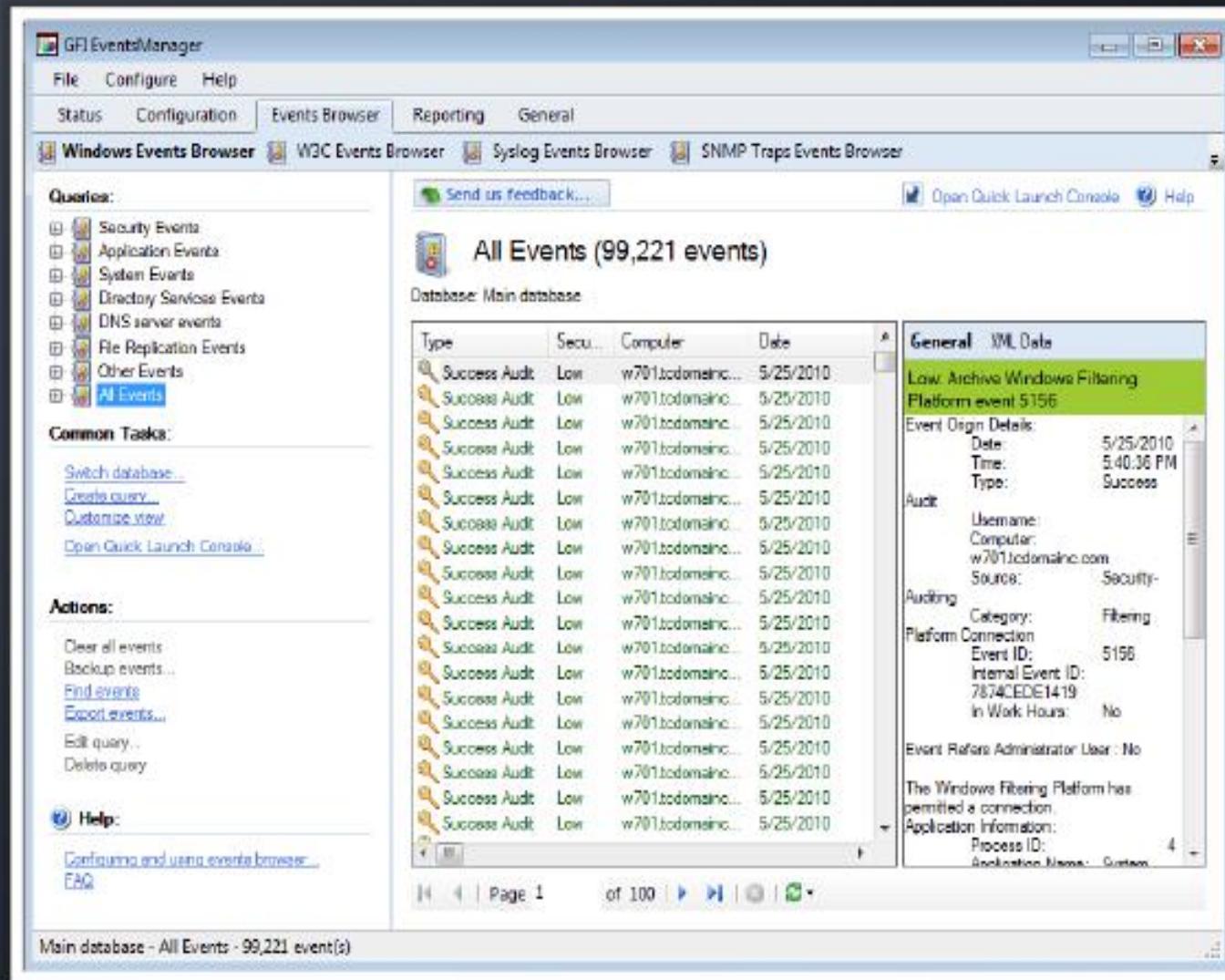
<http://www.manageengine.com>

Log Capturing Tool: GFI EventsManager

- GFI EventsManager automatically processes and archives logs, collecting the information you need to know about the most important events occurring in your network
- It supports a wide range of event types such as W3C, Windows events, Syslog, SQL Server and Oracle audit logs and SNMP traps generated by devices such as firewalls, routers and sensors



GFI EventsManager Screenshot



What is Syslog



Log Capturing Tool: Kiwi Syslog Server

Kiwi Syslog Server is a syslog server for Windows that receives logs and displays and forwards **syslog messages** from hosts such as **routers, switches, Unix hosts** and other **syslog-enabled devices**

1

View syslog data from anywhere on the network via **web access**

2

Filter messages and create advanced alerts with **Advanced Script Processing**

3

Log to any database with **ODBC** logging

4

View **syslog messages** in multiple windows simultaneously

5

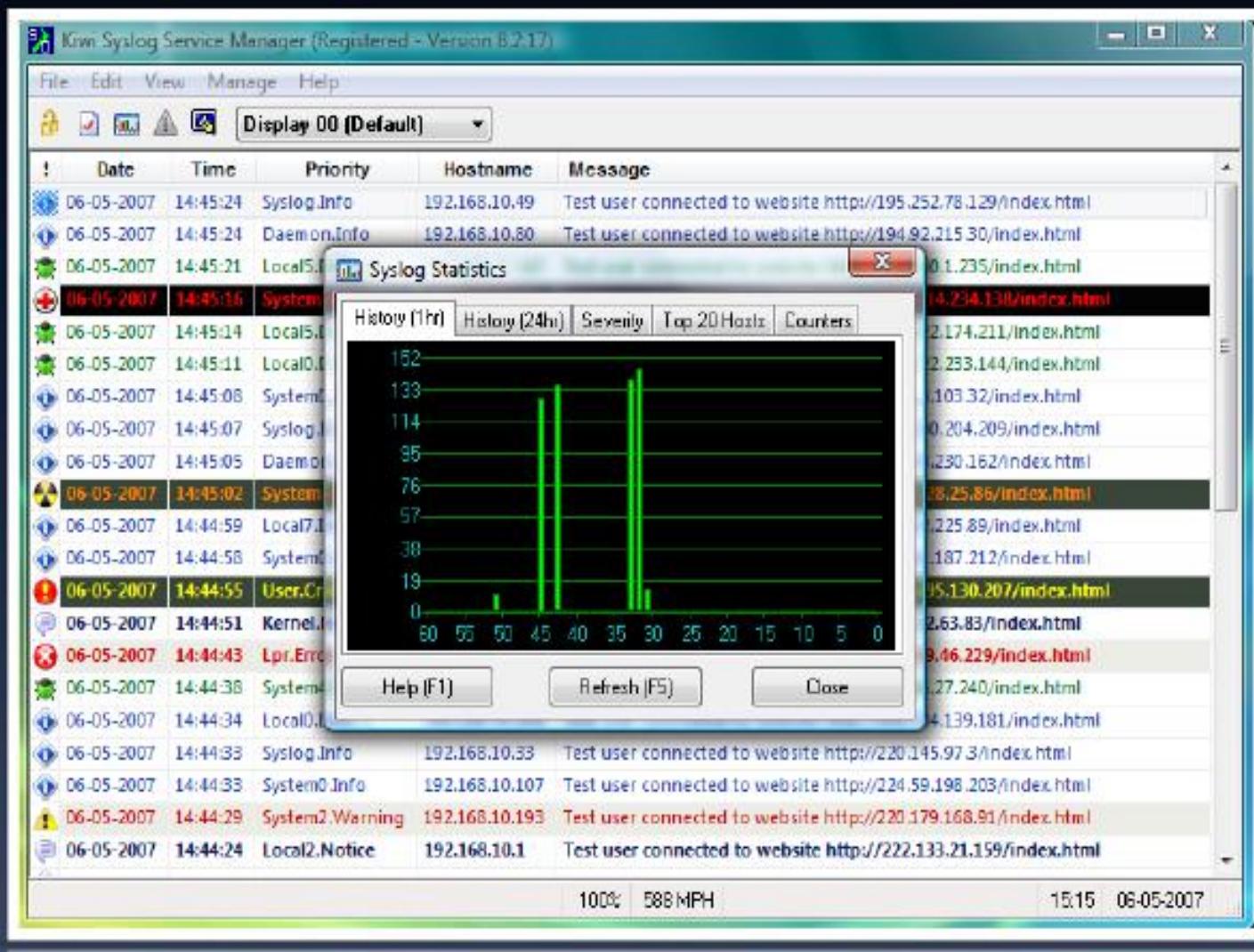
Automatically perform actions based on alerts such as **sending email, forwarding messages, triggering audible alarms, etc.**

6

Produce trend analysis graphs and email syslog **traffic statistics**



Kiwi Syslog Server Screenshot



<http://www.kiwisyslog.com>

100% 298 MPH

12:12 08-02-2005

Handling Logs as Evidence



Use Multiple Logs as Evidence

- Recording the same information in two different devices makes the evidence stronger
- Firewall logs, IDS logs, and TCPDump output can contain evidence of an Internet user connecting to a specific server at a given time

Avoid Missing Logs

- When no log files exist, there is no way of knowing if the **server got no hits** (say it was offline for a day) or if the log file was actually deleted
- Determine whether the server was **running and online** during the time for which log entries are not available by monitoring the server uptime records

Use Signatures, Encryption, and Checksums

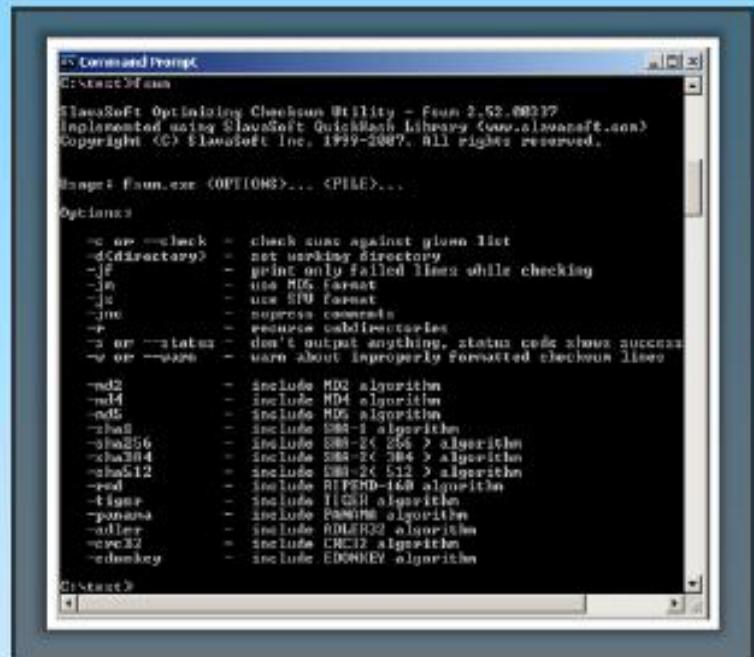
To ensure that the log file is not modified, **encrypt the log** by using the public-key encryption scheme

File signature makes the log file more secure

Use **Fsum tool, MD5** to generate the hash code

Store the **signature** and **hashes** with the log

Store a secure **copy** in a separate location



<http://www.slavasoft.com>



Work with Copies



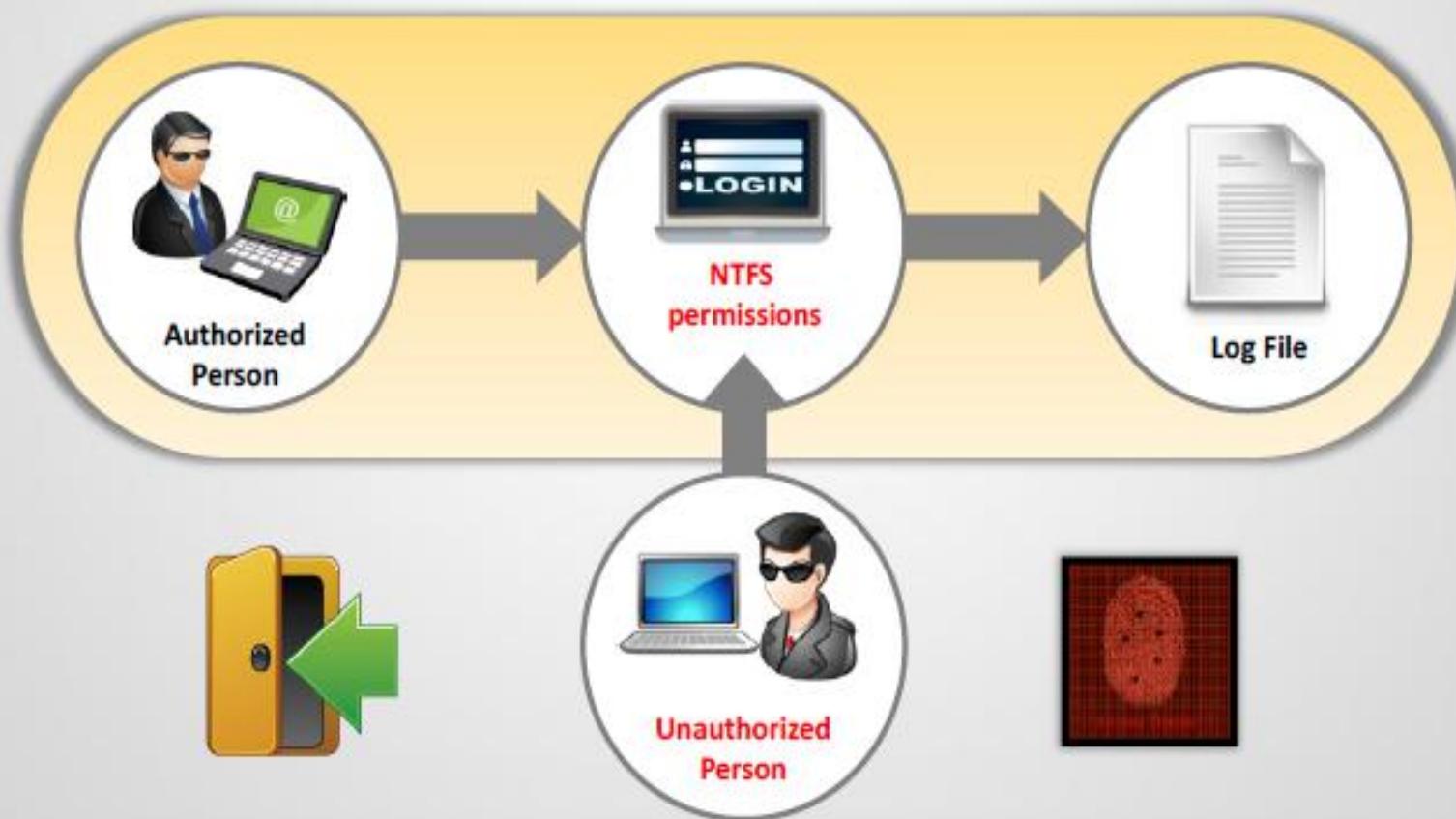
Do not use original log files for analysis; always work on copies

Ensure that the original logs are never touched to maintain the **authenticity** of the original log files

If you use log files as **court evidence**, you must present the original files in their original form

Access Control

- Once a log file is created, it is important to prevent the file from being accessed and to audit any authorized and unauthorized access
- If you properly secure and audit a log file using NTFS permissions, you will have documented evidence to establish its credibility



Chain of Custody

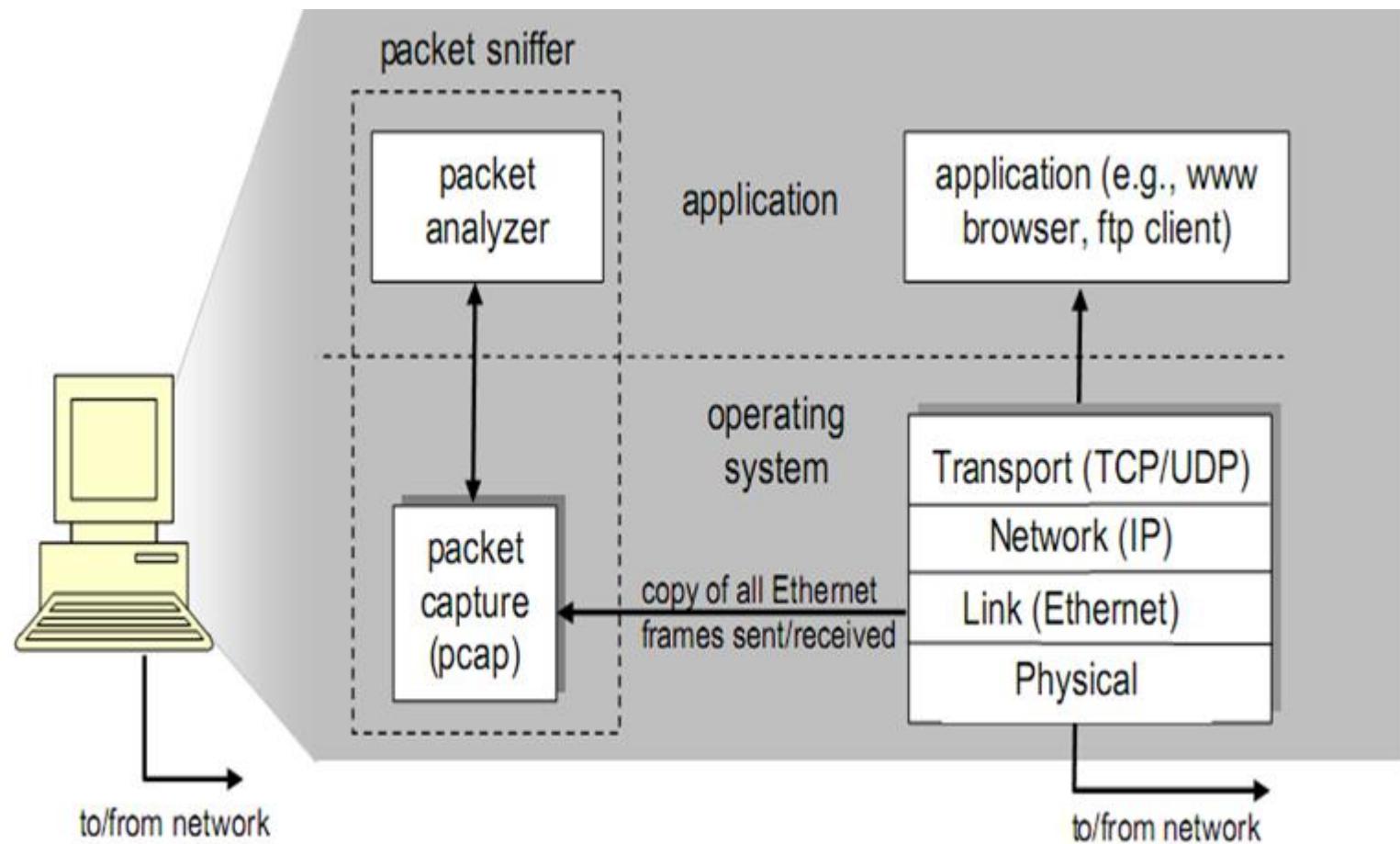
- As you move log files from the server and later to an offline device, you should keep track of **where the file goes**
- This can be done either through technical or non-technical methods such as **MD5 authentication**



Mạng TCP/IP

- Người điều tra viên cần hiểu yêu cầu mình muốn, các thông số nào mình cần biết.
- Xác định mục đích khi thu thập thông tin làm gì như: thu thập chứng cứ pháp lý, hoặc phát hiện xâm nhập.
- Xác định yêu cầu phân tích dữ liệu dựa trên các gói tin TCP/IP thu thập được.
- Các công cụ pháp chứng mạng như: Tcpdump/windump, Wireshark

TCP/IP Packet sniffer

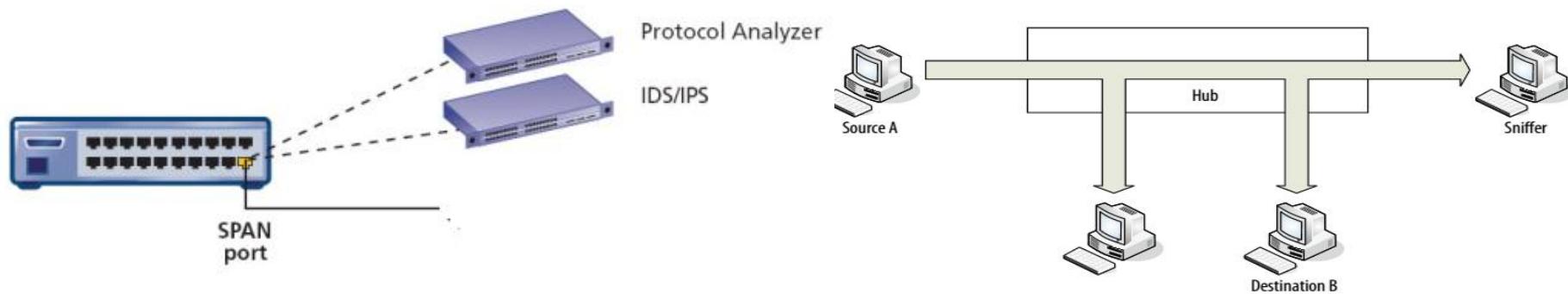




**Có những phương pháp nào
để kết nối sniffer mạng nội bộ?**

SPAN port?

- Switched Port Analyzer port
- Cho phép cấu hình để Switch tự động sao chép các gói tin qua lại giữa các cổng đến một cổng được gọi là cổng giám sát (SPAN port).
- Các phần mềm sniffer hay các hệ thống phân tích sẽ cần phải được kết nối với một SPAN port để có thể xem xét được lưu lượng qua Switch



Sniffer?

- Sniffer là một chương trình cho phép nghe các lưu lượng thông tin trên một hệ thống mạng.
- Tương tự như là thiết bị cho phép nghe lén trên đường dây điện thoại.
- Việc bắt gói tin bằng Sniffer là thụ động và thường sẽ không tạo ra bất kỳ lưu lượng mạng nào.

Phương thức sử dụng Sniffer?

- “**Catch-it-as-you-can**”: Tất cả các gói chuyển qua một điểm traffic nào đó đều được bắt lại và rồi ghi vào thiết bị lưu trữ để sau đó tiến hành phân tích.
 - Cách tiếp cận này yêu cầu một lượng lớn thiết bị lưu trữ, thường sử dụng các hệ thống RAID.
- “**Stop, look and listen**”: Mỗi gói tin được phân tích sơ bộ ngay trong bộ nhớ, chỉ một vài thông tin nào đó là được lưu trữ cho quá trình phân tích sau này.
 - Cách tiếp cận này yêu cầu thiết bị lưu trữ ít hơn nhưng lại cần các processor có tốc độ nhanh hơn để có thể xử lý hết các traffics đi vào.

Các công cụ Sniffer

- Sniffer đầu tiên là sản phẩm của Network Associates với tên là Sniffer Network Analyzer
- Có rất nhiều công cụ Sniffer được phát triển như:
 - tcpdump/windump: công cụ viết trên linux/windows
 - Wireshark (Ethereal): công cụ thông dụng và nhiều tính năng mạnh hỗ trợ việc phân tích.
 - Tshark: Đây là một công cụ khá hiệu quả khi phân tích các tập tin PCAP trên giao diện commandline (linux), tshark cung cấp đầy đủ các chức năng như bắt gói tin, đọc và phân tích gói tin, trích xuất dữ liệu...
 - Kismet: hiệu quả để Sniffer gói tin trên mạng Wireless.
 - Ettercap: hoạt động hiệu quả và bảo mật
 - NetStumbler: thực hiện Sniffer trên chuẩn 802.11
 - Ngrep: tính năng lọc tốt và thường dùng với tcpdump
 - KisMAC: thực hiện Sniffer trên hệ điều hành Mac OS X.

Phân tích gói tin

- Nghe các gói tin và phân tích giao thức, mô tả quá trình, khôi phục định dạng để hiểu rõ hơn điều gì đang diễn ra trên mạng.
 - Các luồng thông tin đang chạy trên mạng?
 - Các loại mã độc
 - Tấn công mật khẩu
 - Tấn công botnet
 - ...

Kỹ thuật phân tích gói tin

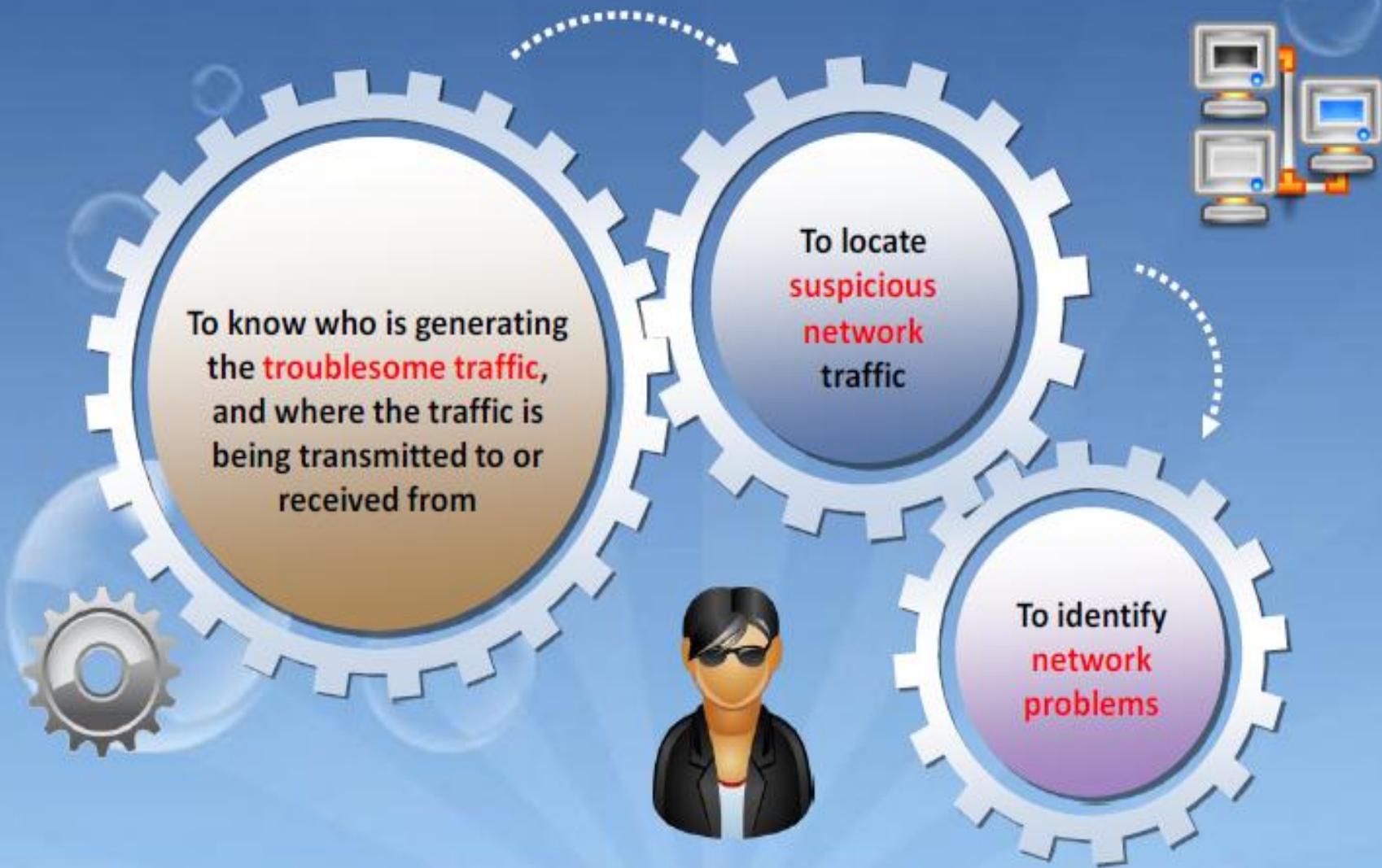
■ Có 3 kỹ thuật cơ bản:

- Pattern Matching (theo mô hình): xác định các gói tin liên quan bằng cách kết hợp các giá trị cụ thể trong các gói tin bắt được.
- Parsing Protocol Fields (phân tích các thành phần giao thức): rút trích ra nội dung của các giao thức trong các lĩnh vực.
- Packet Filtering (lọc gói tin): lọc các gói riêng biệt dựa trên giá trị của các thành phần trong siêu dữ liệu.

ĐIỀU TRA LƯU LƯỢNG MẠNG



Why Investigate Network Traffic?



Điều tra lưu lượng mạng

- Định danh và phân loại những loại tấn công như Dos, DDos, virus, worm, ... theo thời gian thực dựa vào những sự hành vi thay đổi bất thường trong mạng.



Evidence Gathering via Sniffing

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

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



Spanned ports, hardware taps help sniffing in a switched network

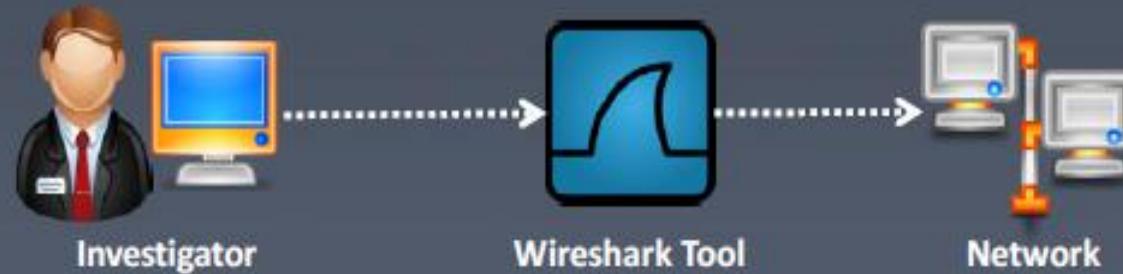


Sniffers, which put NICs in promiscuous mode, are used to collect digital evidence at the physical layer



Capturing Live Data Packets Using Wireshark

- 1 Wireshark is a traffic capturing and sniffing tool
Wireshark uses Winpcap to capture packets, so it can only capture the packets on the networks supported by Winpcap
 - 2 Captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks
 - 3 Captured files can be programmatically edited via command-line
A set of filters for customized data display can be refined using a display filter



Wireshark Screenshot

Capturing from Wi-Fi [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr == 192.168.1.104 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.104	173.194.72.154	TCP	54	57914 > http [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2	5.869943000	204.79.197.200	192.168.1.104	TCP	60	https > 57955 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	8.919798000	192.168.1.104	204.79.197.200	TCP	54	57954 > https [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
4	8.920123000	192.168.1.104	222.255.28.220	TCP	54	57951 > http [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
5	8.920248000	192.168.1.104	222.255.28.220	TCP	54	57952 > http [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
6	8.959224000	204.79.197.200	192.168.1.104	TCP	60	https > 57954 [FIN, ACK] Seq=1 Ack=2 Win=257 Len=0
7	8.959277000	192.168.1.104	204.79.197.200	TCP	54	57954 > https [ACK] Seq=2 Ack=2 Win=1020 Len=0
8	9.219594000	192.168.1.104	222.255.28.220	TCP	54	[TCP Retransmission] 57951 > http [FIN, ACK] Seq=1 Ack=1 Win=1024
9	9.219604000	192.168.1.104	222.255.28.220	TCP	54	[TCP Retransmission] 57952 > http [FIN, ACK] Seq=1 Ack=1 Win=1024
10	9.819547000	192.168.1.104	222.255.28.220	TCP	54	[TCP Retransmission] 57951 > http [FIN, ACK] Seq=1 Ack=1 Win=1024
11	9.819547000	192.168.1.104	222.255.28.220	TCP	54	[TCP Retransmission] 57952 > http [FIN, ACK] Seq=1 Ack=1 Win=1024
12	10.271796000	192.168.1.104	65.55.223.46	TCP	56	51135 > 33033 [PSH, ACK] Seq=1 Ack=1 Win=256 Len=2
13	10.606330000	65.55.223.46	192.168.1.104	TCP	60	33033 > 51135 [ACK] Seq=1 Ack=3 Win=83 Len=0
14	10.606487000	192.168.1.104	65.55.223.46	TCP	500	51135 > 33033 [PSH, ACK] Seq=3 Ack=1 Win=256 Len=446
15	10.896989000	65.55.223.46	192.168.1.104	TCP	60	33033 > 51135 [ACK] Seq=1 Ack=449 Win=83 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

Ethernet II, Src: LiteonTe_6b:a0:b8 (40:f0:2f:6b:a0:b8), Dst: Cisco-Li_95:7b:66 (00:1a:70:95:7b:66)

Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 173.194.72.154 (173.194.72.154)

Transmission Control Protocol, Src Port: 57914 (57914), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Hex	Dec	ASCII
0000	00 1a 70 95 7b 66 40 f0	. . p. { f @. / k . . . E .
0010	00 28 4b 97 40 00 80 06	(K . @ h . .
0020	48 9a e2 3a 00 50 d2 a6	H . . . P . . y P .
0030	00 00 3b dc 00 00	.. ; . .

Wi-Fi: <live capture in progress> File... Packets: 54647 · Displayed: 54289 (99.3%) Profile: Default

Digital Forensics

Display Filters in Wireshark

Display filters are used to **change the view of packets** in the captured files

Example: Type the protocol in the filter box; arp, http, tcp, udp, dns

Display Filtering by Protocol

Other Filters

```
ip.dst == 10.0.1.50 && frame.pkt_len > 400  
ip.addr == 10.0.1.12 && icmp &&  
frame.number > 15 && frame.number < 30  
ip.src==205.153.63.30 or  
ip.dst==205.153.63.30
```



```
tcp.port==23  
ip.addr==192.168.1.100  
machine  
ip.addr==192.168.1.100 &&  
tcp.port=23
```

Monitoring the Specific Ports

Filtering by Multiple IP Addresses

```
ip.addr == 10.0.0.4 or  
ip.addr == 10.0.0.5
```

```
ip.addr == 10.0.0.4
```

Additional Wireshark Filters

1

Displays all TCP resets

`tcp.flags.reset==1`

2

Displays all HTTP GET requests

`http.request`

3

Displays all TCP packets that contain the word “traffic”

`tcp contains traffic`

4

Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset

`udp contains 33:27:58`

5

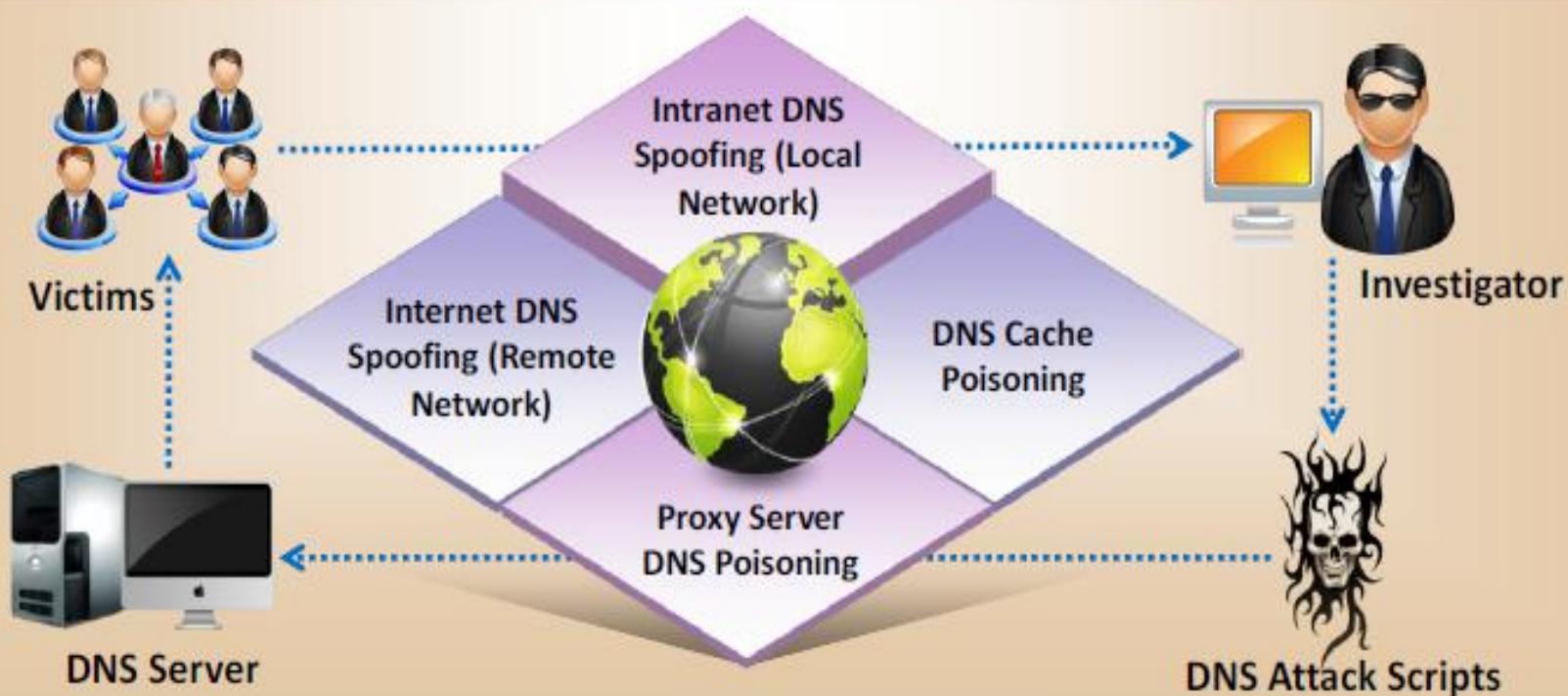
Displays all retransmissions in the trace

`tcp.analysis.retransmission`

Chi tiết: <https://gitlab.com/wireshark/wireshark/-/wikis/home>

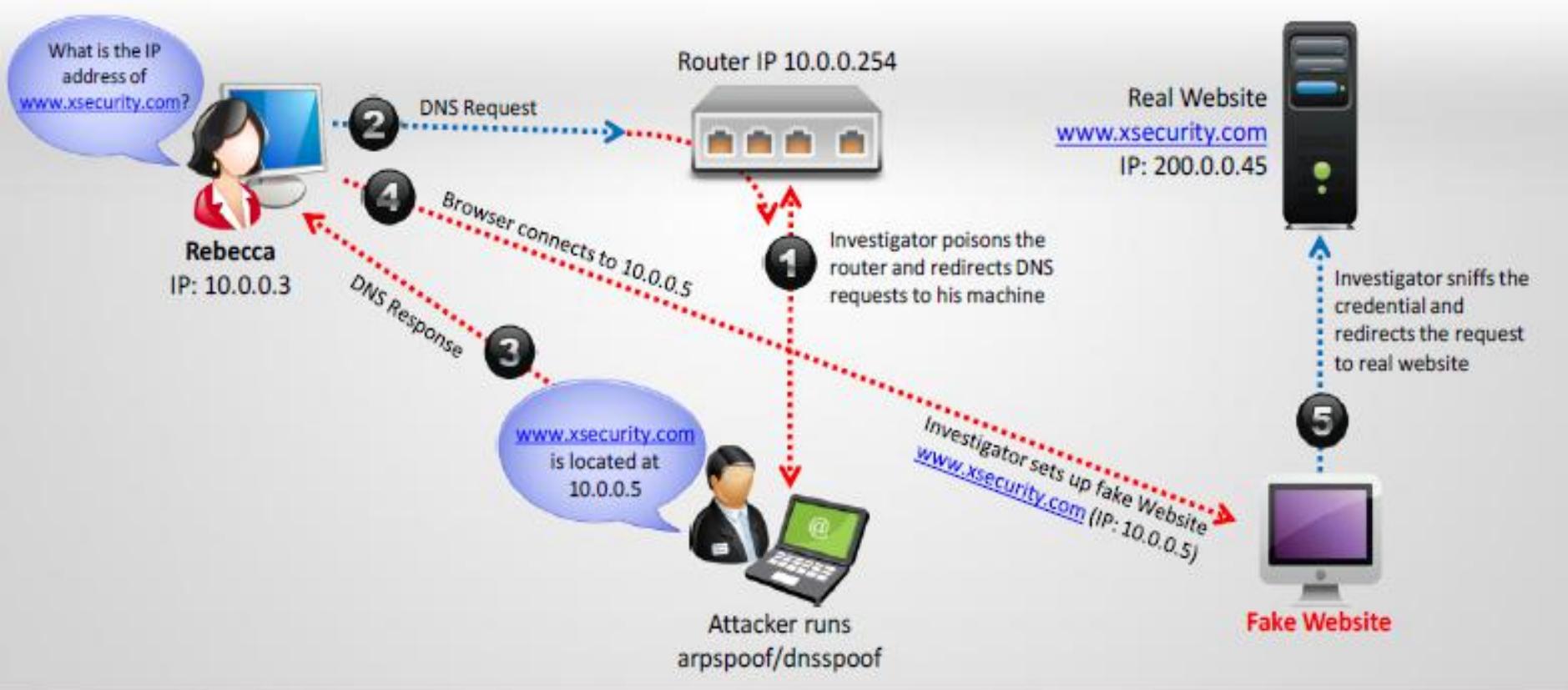
Acquiring Traffic Using DNS Poisoning Techniques

1. DNS poisoning is a technique that **tricks a DNS server** into believing that it has received authentic information when, in reality, it has not
2. It results in **substitution of a false Internet provider address** at the domain name service level where web addresses are converted into numeric Internet provider addresses
3. Perform DNS poisoning by setting up a fake website



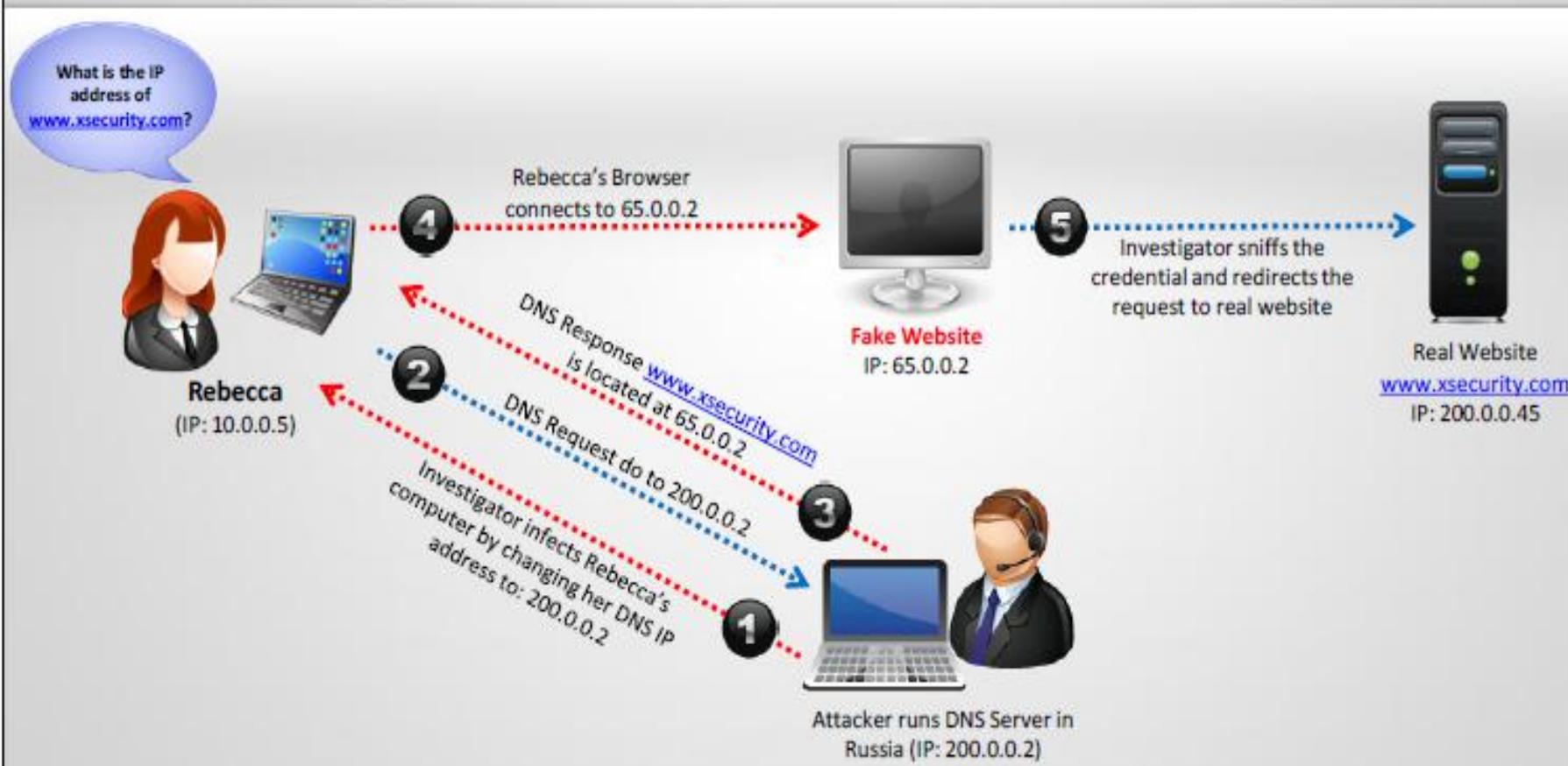
Intranet DNS Spoofing (Local Network)

- For this technique, you must be connected to the **local area network (LAN)** and be able to sniff packets
- It works well against **switches** with ARP poisoning the router



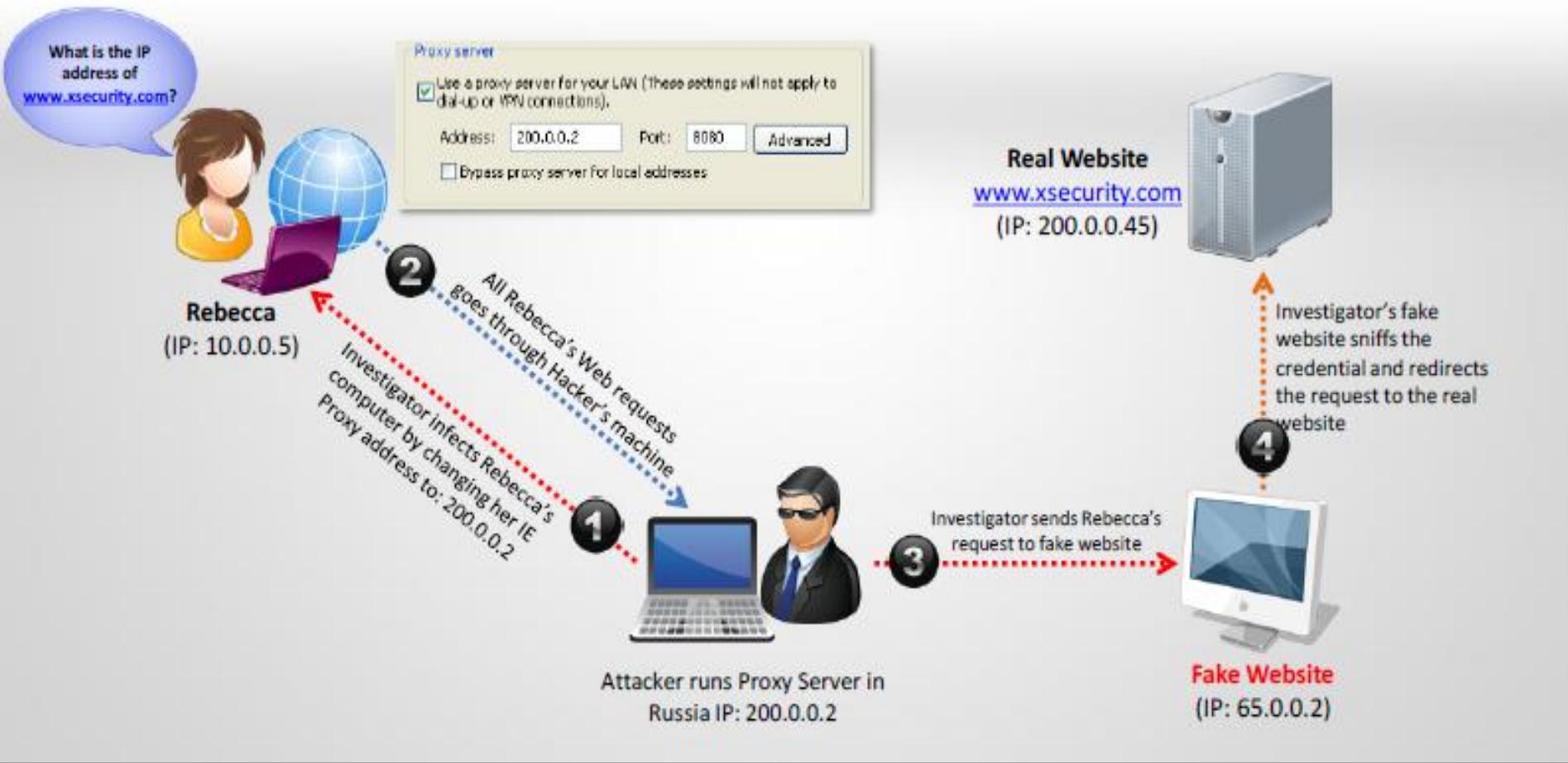
Intranet DNS Spoofing (Remote Network)

- In this example of Internet DNS spoofing, the investigator infects Rebecca's machine with a Trojan and changes her DNS IP address to that of the investigator



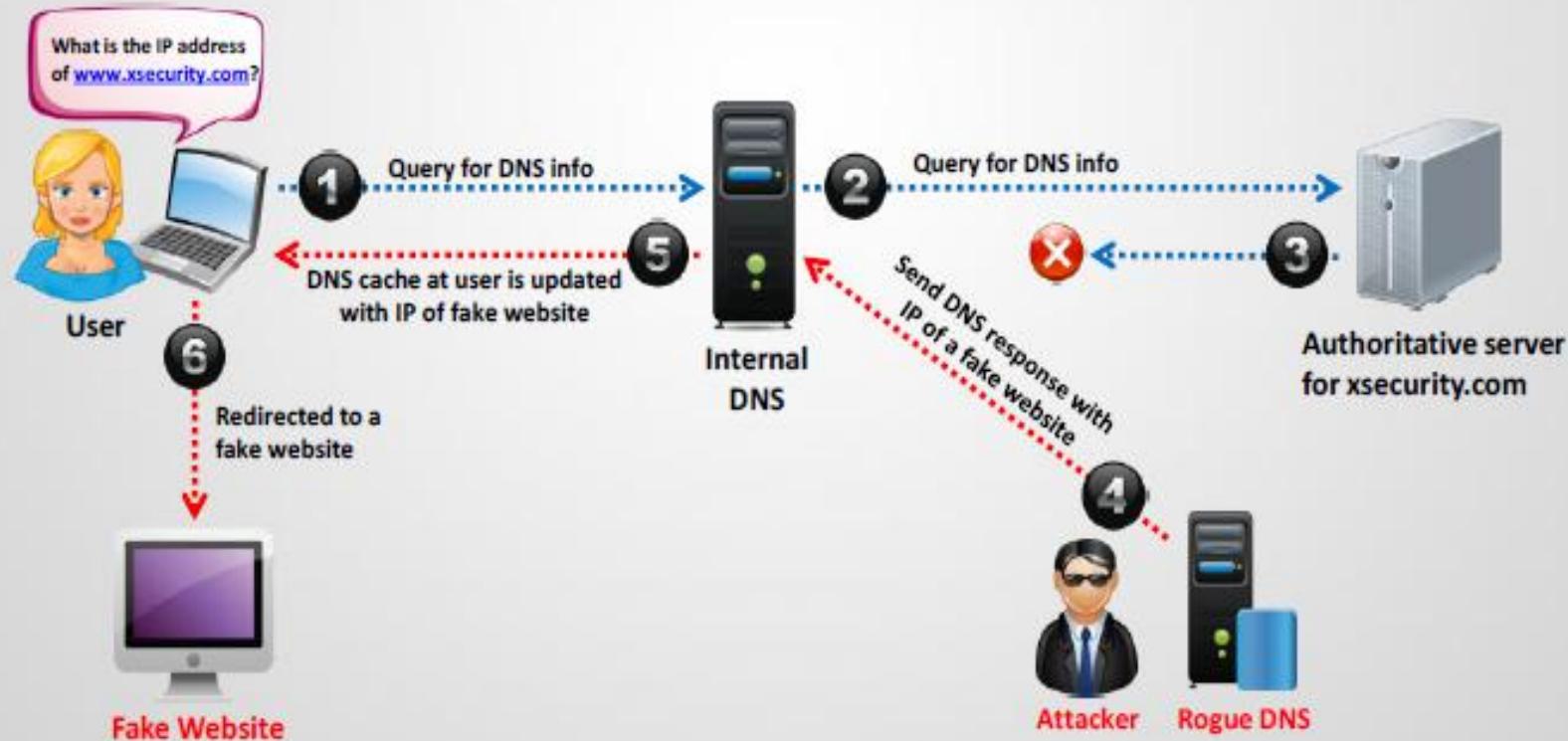
Proxy Server DNS Poisoning

- In this example, the investigator sends a Trojan to Rebecca's machine and changes her proxy server settings in Internet Explorer to those of the investigator



DNS Cache Poisoning

- DNS cache poisoning involves **changing or adding records** in the resolver cache of a DNS so that a DNS query for a domain returns an IP address of a fake website set by the investigator
- If the server cannot validate that DNS responses have come from an authoritative source, it will **cache the incorrect entries** locally and serve them to users who make the same request



Evidence Gathering from ARP Table

```
C:\Windows\system32\cmd.exe
C:\>arp -a
Interface: 192.168.168.9 --- 0xb
Internet Address      Physical Address          Type
192.168.168.1         00-21-64                dynamic
192.168.168.2         00-16-3f                dynamic
192.168.168.3         00-21-64                dynamic
192.168.168.4         00-06-3f                dynamic
192.168.168.224       ff-ff-ff                static
192.168.168.231       01-00-5c                static
192.168.168.239       01-00-5c                static
255.255.255.255       ff-ff-ff                static
C:\>
```

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



MAC address:
A part of the data-link layer is associated with the system hardware

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



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



A screenshot of a Windows application window titled "DHCP LEASES". The window displays a table of network leases. The columns are labeled "Computer", "IP", "MAC", "Rented", and "Expires". The table shows 13 entries. The entry for "IE-PC" is highlighted with a blue selection bar. The "Expires" column for "IE-PC" shows the date and time as "6/14/2009 2:17:52 PM".

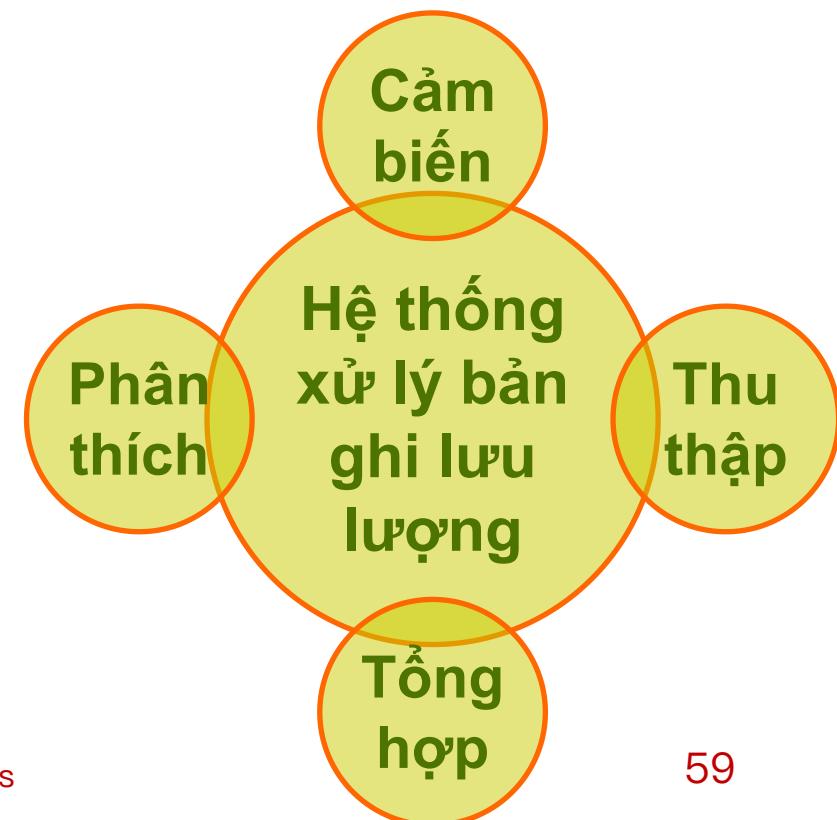
Computer	IP	MAC	Rented	Expires
sspc	192.168.1.5	00-15-AB-7B-C5-B9	6/10/2009 7:46:02 AM	6/14/2009 7:46:02 AM
com-10599a0d	192.168.0.5	00-41-80-60-51-C1	6/10/2009 12:01:52 AM	6/13/2009 12:00:52 AM
IE-PC	192.168.0.3	00-51-00-02-59-94	6/10/2009 2:17:52 PM	6/14/2009 2:17:52 PM
vista-PC	192.168.1.20	00-15-P3-PD-8B-1B	6/10/2009 1:29:57 AM	6/14/2009 1:29:57 AM
vladimir	192.168.1.12	00-13-CE-7E-A3-4F	6/10/2009 9:04:52 AM	6/14/2009 9:04:52 AM
home	192.168.0.35	00-19-08-94-61-82	6/10/2009 1:32:00 PM	6/14/2009 1:32:00 PM
ta-PC	192.168.1.111	00-1F-3A-1A-88-9A	6/10/2009 1:44:05 PM	6/13/2009 7:14:05 PM
laptop1	192.168.0.20	00-25-47-30-03-4B	6/7/2009 7:51:42 PM	6/14/2009 7:51:42 PM
private-8336a90	192.168.0.4	00-25-CD-80-81-E2	6/10/2009 7:40:10 AM	6/14/2009 7:40:10 AM
barans	192.168.0.7	00-21-00-00-00-44	6/10/2009 11:58:06 AM	6/13/2009 11:58:06 AM
Electronica	192.168.0.11	00-14-45-C0-E3-4C	6/10/2009 9:39:08 AM	6/14/2009 9:39:08 AM
ben	192.168.0.19	00-16-49-27-7B-0F	6/9/2009 1:23:07 PM	6/13/2009 1:23:07 PM

Leases 13

Aptarion
PRODUCTS

Thông tin lưu lượng mạng

- Một bản ghi lưu lượng bao gồm địa chỉ IP nguồn và đích, cổng nguồn và đích (nếu có), giao thức, ngày, giờ và số lượng dữ liệu truyền đi trong mỗi dòng.
- Bản ghi lưu lượng là một tập hợp thông tin về một dòng lưu lượng.
- Hệ thống xử lý bản ghi lưu lượng



Các cảm biến (Sensors)

- Ghi bằng thiết bị trên mạng: Một số thiết bị như CISCO Router, Switch, Firewall đã có hỗ trợ việc tạo ra và ghi dữ liệu mạng.
- Cài đặt thiết bị độc lập: Triển khai server ghi bằng phần mềm xử lý ở bất cứ nơi nào trên mạng mà có thể bắt thông tin lưu lượng.
- Giao thức trao đổi thông tin lưu lượng: NetFlow, IPFIX, sFlow

Lưu ý khi đặt cảm biến

- **Sự trùng lắp:** Làm tăng nguồn cần thiết để phân tích, và gây ra tắc nghẽn mạng trong quá trình tổng hợp.
- **Đồng bộ hóa thời gian:** Nếu thời gian trên một cảm biến không chính xác, rất khó để tương quan lưu lượng được xuất bởi thiết bị này với các thiết bị khác.
- **Lưu lượng ngoài so với bên trong:** Lưu lượng dữ liệu nội bộ có thể giúp xác định các máy trạm bị xâm nhập đang tìm cách lan truyền tới những mục tiêu mới, bao gồm cả bên trong và bên ngoài.

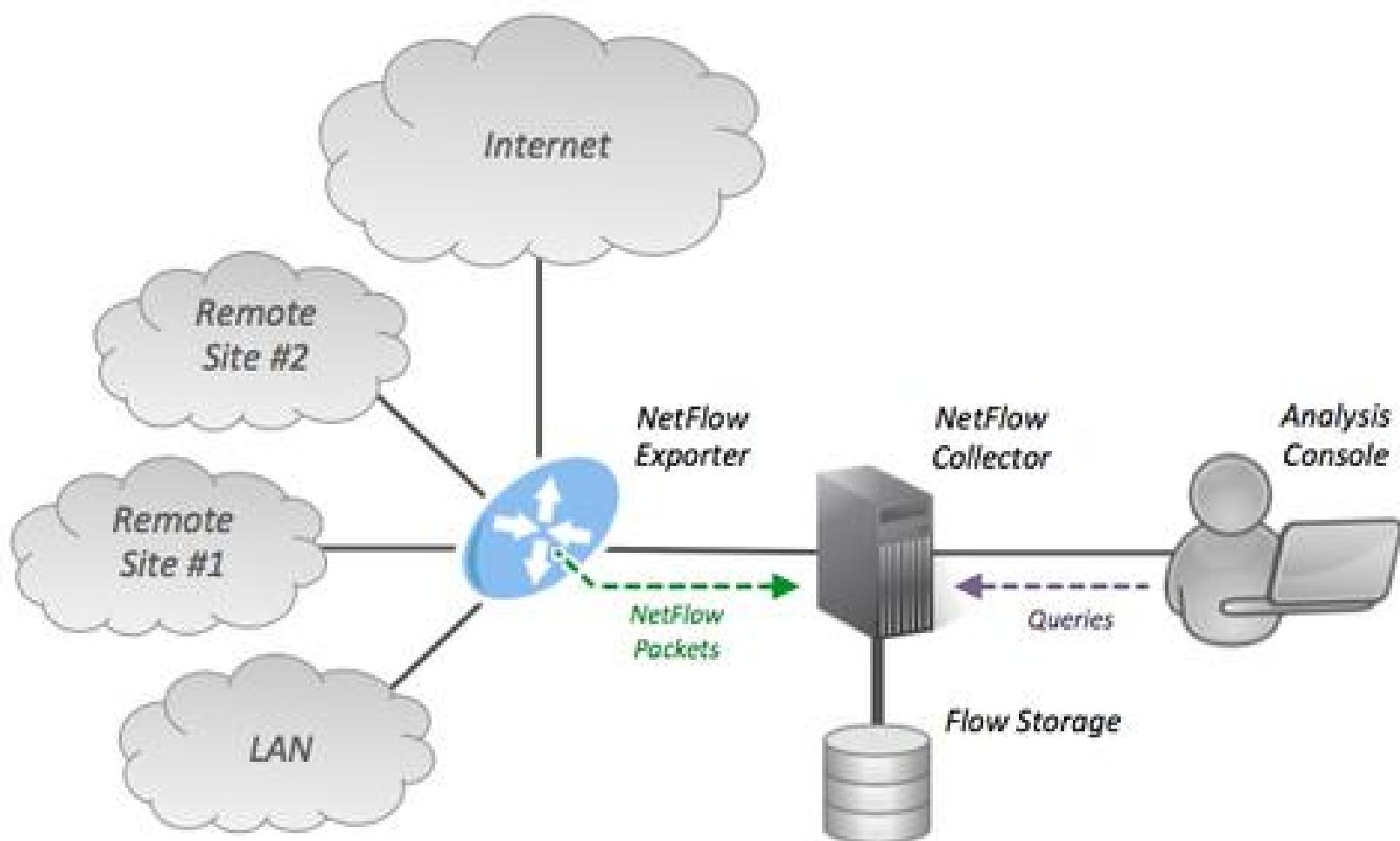
Lưu ý khi đặt cảm biến

- **Tài nguyên:** Xem lại các biểu đồ mạng một cách cẩn thận và chọn điểm nút thắt mà nó sẽ tối đa hóa khả năng thu thập, trong khi nó vẫn phù hợp với phạm vi ngân sách và khả năng để xử lý và phân tích.
- **Năng lực thiết bị:** Việc kích hoạt xử lý bản ghi lưu lượng và xuất chúng có thể ảnh hưởng đến hiệu suất của thiết bị mạng, đặc biệt là nếu nó được sử dụng quá mức.

NetFlow

- Là một giao thức giám sát lưu lượng mạng do Cisco phát triển.
- NetFlow là một giao thức thu thập “collecting”, tổng hợp “aggregating” và ghi lại “recording” dữ liệu luồng lưu lượng trong một mạng.
- Được nhúng trong phần mềm IOS của Cisco trên bộ định tuyến “router” và thiết bị chuyển mạch “switch” của công ty và đã được hỗ trợ trên hầu hết các thiết bị của Cisco kể từ phiên bản 11.1 của Phần mềm Cisco IOS Software. Nhiều nhà sản xuất phần cứng khác hỗ trợ NetFlow.

NetFlow



NetFlow

- Hầu hết tất cả các thiết bị của Cisco đều hỗ trợ NetFlow. (trừ Cisco 2900, 3500, 3660, 3750). Hơn nữa, NetFlow có sẵn cho nhiều bộ định tuyến và chuyển mạch của các nhà cung cấp khác.

Vendor + Type	Models	Supported NetFlow Versions
Alcatel-Lucent router	7750SR	v5, IPFIX
Juniper legacy router	M-series, T-series, MX-series with DPC	v5, v8, v9
Juniper router	MX-series, FPC5 for T4000	v5, IPFIX
Enterasys Switch	S-Serie, N-Serie	v5, v9
Flowmon Probe	1000, 2000, 4000, 6000, 10000, 20000, 40000, 80000, 100000	v5, v9, IPFIX
Nortel Switch	ERS5510, ERS5520, ERS5530, 8600	v5, v9, IPFIX
Huawei router	NE5000E, NE40E/X NE80E	v5, v9

Thành phần của NetFlow

■ Creating a flow (Tạo luồng):

- Luồng “flow” là cách nhóm một chuỗi các gói tin “packets” một chiều vào thành một gói tin lớn cụ thể.
- Mỗi packet khi chuyển qua router hoặc switch đều được kiểm tra bằng một tập các thuộc tính IP. Các thuộc tính này giúp định dạng và phân nhóm các packet vào các luồng khác nhau một cách rõ ràng.

■ IP Source:	IP nguồn
■ IP Destination:	IP đích
■ Source Port:	Cổng nguồn
■ Destination Port:	Cổng đích
■ Class of Service:	Loại dịch vụ
■ Layer 3 Protocol Type:	Loại giao thức 3 lớp
■ Interface:	Giao diện

Thành phần của NetFlow

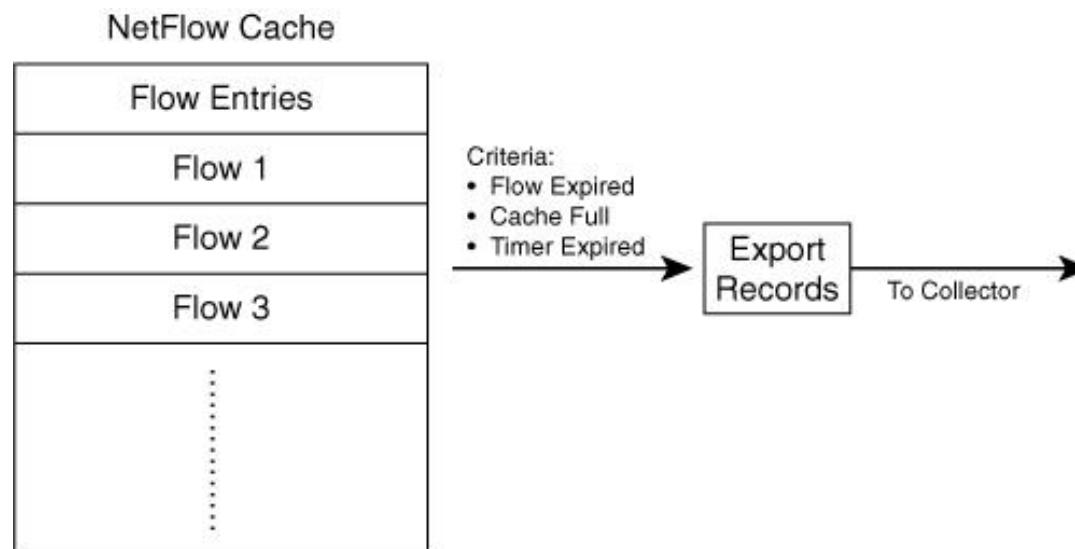
■ NetFlow cache (Bộ nhớ đệm NetFlow):

- Việc giám sát và nhóm mọi gói tin chuyển đi bởi thiết bị mạng sẽ tạo ra nhiều dữ liệu.
- Dữ liệu này được cô đọng thành một cơ sở dữ liệu trong thiết bị mạng được gọi là bộ đệm NetFlow Cache.
- Một bản ghi luồng “Flow record” được giữ cho mỗi luồng hoạt động.
- Dữ liệu hết hạn và sau đó được xuất từ bộ nhớ cache sang máy chủ thu thập NetFlow

Thành phần của NetFlow

■ NetFlow export:

- ❑ Các luồng được nhóm lại để xuất thành một khối dữ liệu gọi là “NetFlow Export datagram”. Mỗi khối dữ liệu Datagram bao gồm tối đa 30 luồng



Thành phần của NetFlow

- **NetFlow Record (bản ghi Netflow):**
 - Chứa thông tin của một luồng (flow)

Thành phần của NetFlow

■ NetFlow collector (Bộ thu thập dữ liệu Netflow):

- Là một máy chủ hoặc máy tính khác chạy phần mềm NetFlow Receiver Software, có nhiệm vụ thu thập và tổng hợp thông tin về luồng.
- NetFlow export được cấu hình để để gửi thông tin các luồng tới Collector. NetFlow cache tìm kiếm luồng đã kết thúc và gửi thông tin về luồng đó tới NetFlow collector server.
- Có khoảng từ 30-50 luồng được đóng gói và gửi dưới dạng UDP tới NetFlow collector server.

Thành phần của NetFlow

■ NetFlow MIB:

- Truy cập một số dữ liệu NetFlow qua SNMP bằng NetFlow MIB
- Mặc dù không được thiết kế để thay thế cho NetFlow export, nhưng nó cung cấp một cách để truy cập vào dữ liệu NetFlow thông qua một cơ chế khác.

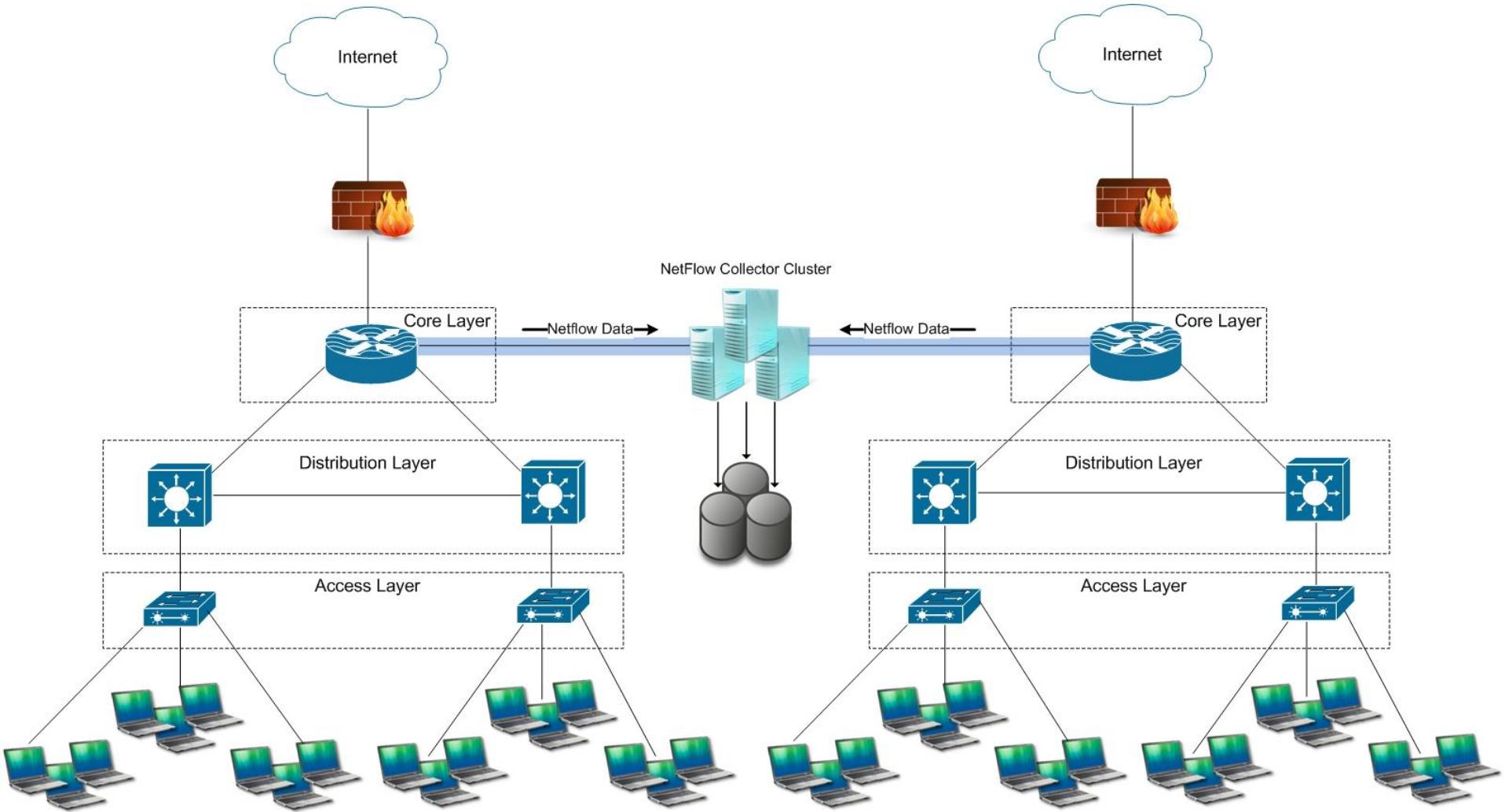
Thành phần của NetFlow

■ NetFlow Data:

□ Có nhiều loại lưu lượng “traffic categories” có thể được theo dõi bằng NetFlow. Ví dụ, cảm biến NetFlow V9 Sensor của PRTG cho phép theo dõi và phân loại nhiều loại lưu lượng theo mặc định:

- Chat
- Citrix
- FTP/P2P
- Infrastructure (DHCP, DNS, ICMP, SNMP)
- Mail
- NetBIOS
- Remote Control Protocols
- WWW
- Total Traffic

NetFlow Collectors



Ứng dụng NetFlow

- Giám sát mạng, người dùng và ứng dụng
“Network, user and application monitoring”
- Lập kế hoạch mạng (Network planning)
- Lập hóa đơn và báo cáo dựa trên mức sử dụng
“Usage-based billing and reporting”
- Báo cáo và lập hồ sơ ứng dụng “Application reporting and profiling”
- Phân tích bảo mật “Security analysis”

Giao thức sFlow

- sFlow được phát triển bởi InMon công bố bởi IETF RFC vào năm 2001 (<https://sflow.org>)
- **Thống kê lấy mẫu** gói tin và không hỗ trợ việc ghi lại và xử lý thông tin về các gói dữ liệu duy nhất, cân bằng tốt với các mạng rất lớn, với thông lượng cao.
- Tập trung vào thống kê nên phần bên dưới của gói tin không được lấy mẫu và không được ghi lại nên không thể phân tích.
- Hàng hỗ trợ: <https://sflow.org/products/network.php>

Giao thức sFlow

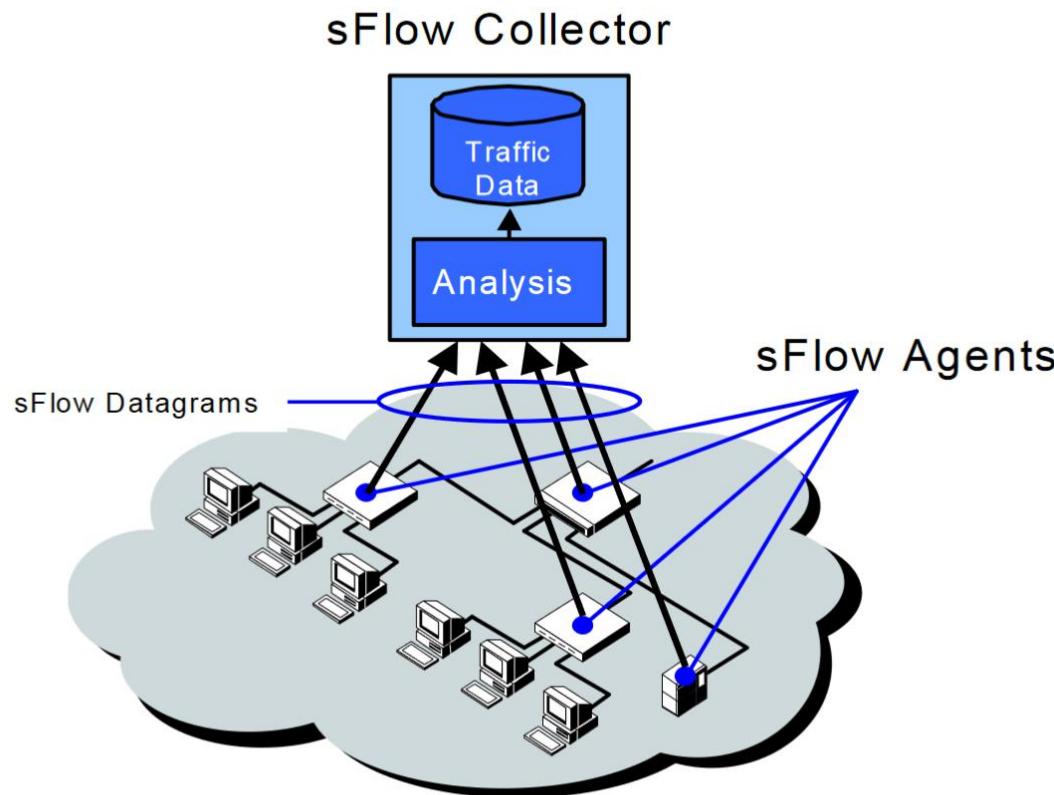


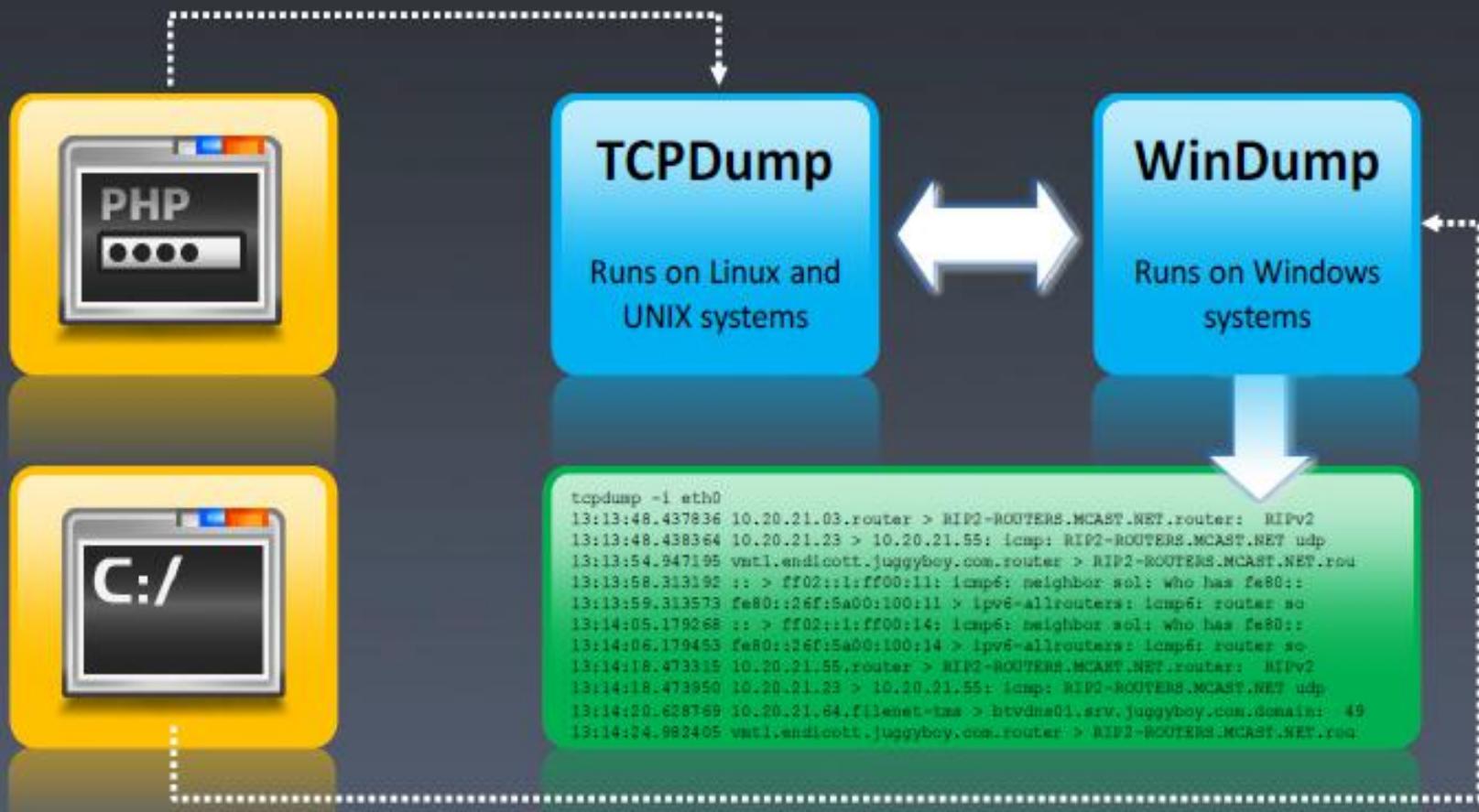
Figure 3 *sFlow Agents and Collector*



CÁC CÔNG CỤ ĐIỀU TRA

Tcpdump/Windump

TCPdump is a very powerful command line interface packet sniffer that runs on Linux and Windows



Cú pháp tcpdump

```
tcpdump [ -AdDefIKlLnNOpqRStuUvxX ] [ -B buffer_size ]  
[ -c count ]  
[ -C file_size ] [ -G rotate_seconds ] [ -F file ]  
[ -i interface ] [ -m module ] [ -M secret ]  
[ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]  
[ -W filecount ]  
[ -E spi@ipaddr algo:secret,... ]  
[ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]  
[ expression ]
```

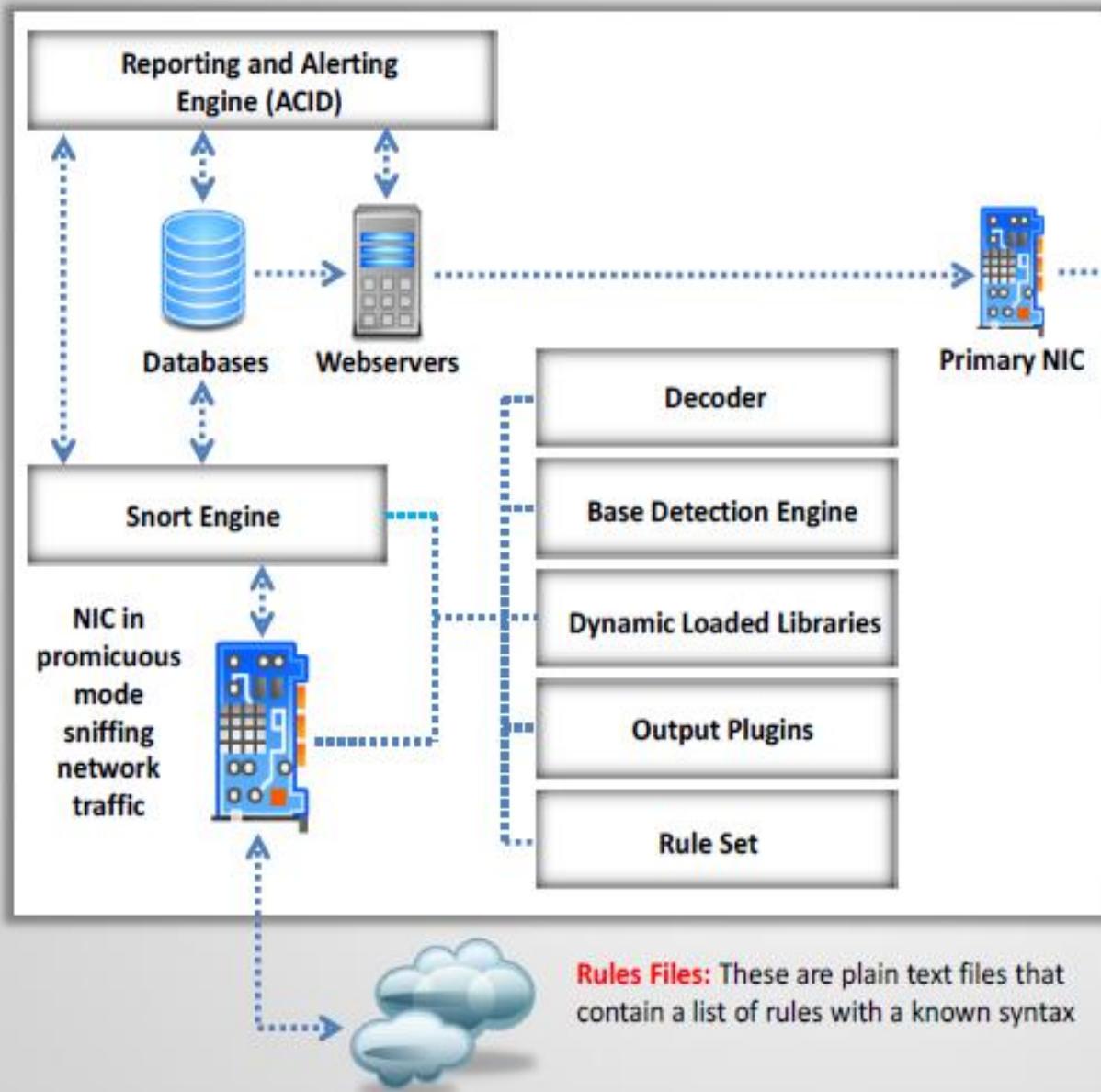
Intrusion Detection Tool: Snort

- Snort is an open source network intrusion detection system, capable of performing real-time **traffic analysis and packet logging on IP networks**
- It can perform **protocol analysis** and **content searching/matching**, and is used to detect a variety of **attacks and probes**, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts
- It uses a flexible **rules language** to describe traffic that it should collect or pass, as well as a **detection engine** that utilizes a modular plug-in architecture
- **Uses of Snort:**
 - Straight packet sniffer like tcpdump
 - Packet logger (useful for network traffic debugging, etc.)
 - Network intrusion prevention system

```
C:\ Command Prompt
Snort Commands
c:\Snort\bin>snort -c c:\Snort\etc\snort.conf -l c:\Snort\log -i 2
--- Initialization Complete ---
-> Snort! <-
Version 2.9.0.2-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 92)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright (C) 1998-2010 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 1.12 <Build 18>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSP Version 1.1 <Build 3>
Commencing packet processing (pid=5896)
85: Session exceeded configured max bytes to queue 1048576 using 1048979 bytes (client queue). 192.168.168.7 11616 --> 92.46.53.163 80 (0) : LwState 0x1 LwFlags 0x2003
*** Caught Int-Signal
Run time for packet processing was 5985.944000 seconds
Snort processed 11774 packets.
Snort ran for 0 days 1 hours 39 minutes 45 seconds
Pkts/hr: 11774
Pkts/min: 118
Pkts/sec: 1
85: Pruned session from cache that was using 1098947 bytes (purge whole cache).
192.168.168.7 11616 --> 92.46.53.163 80 (0) : LwState 0x1 LwFlags 0x22003
Packet I/O Totals:
Received: 147490
Analyzed: 11774 ( 7.983%)
Dropped: 135707 ( 92.011%)
Filtered: 0 ( 0.000%)
Outstanding: 135716 ( 92.017%)
Injected: 0
```

<http://www.snort.org>

How Snort Works



- **Decoder:** Saves the captured packets into heap, identifies link level protocols, and decodes IP
- **Detection Engine:** It matches packets against rules previously charged into memory since Snort initialization
- **Output Plug-ins:** These modules format the notifications for the user to access them in different ways (console, external files, databases, etc)

NetworkMiner

- NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows that is used as a **passive network sniffer/packet** capturing tool in order to detect operating systems, sessions, hostnames, open ports etc.
- It **extracts files and certificates** transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network



NetworkMiner Professional 1.0

File Tools Help

Select a network adapter in the list --

Case Panel

Filesize MD5
Blended ... 3e2d6cf...

Parameters (1343) | Keywords | Cleartext | Anomalies

Hosts (11%) | Frames (15%) | Rss (60) | **Images** | Messages | Credentials (6) | Sessions (63) | DNS (37)

Source ...	S. port	Destinat... D. port	Protocol	Filename	Extension	Size	
66.249...	TCP 80	192.168...	TCP 1111	HttpGetNormal	bnd.20...	html	6 B
66.249...	TCP 80	192.168...	TCP 1115	HttpGetNormal	index.ht...	javascript	163 B
66.249...	TCP 80	192.168...	TCP 1115	HttpGetNormal	bnd.80...	html	6 B
66.249...	TCP 80	192.168...	TCP 1119	HttpGetNormal	bnd.A5...	html	6 B
204.9.1...	TCP 80	192.168...	TCP 1120	HttpGetNormal	gattaca...	txt	9 B
63.245...	TCP 443	192.168...	TCP 1125	TlsCertificate	mozilla...	cer	774 B
66.249...	TCP 80	192.168...	TCP 1126	HttpGetNormal	bnd.2A...	html	6 B
66.249...	TCP 80	192.168...	TCP 1127	HttpGetNormal	bnd.70...	html	6 B
66.249...	TCP 80	192.168...	TCP 1116	HttpGetChunked	bnd.1E...	bd	189 B
66.249...	TCP 80	192.168...	TCP 1129	HttpGetNormal	index.ht...	javascript	163 B
66.249...	TCP 80	192.168...	TCP 1129	HttpGetNormal	bnd.9E...	html	6 B
66.249...	TCP 80	192.168...	TCP 1130	HttpGetNormal	bnd.60...	html	6 B
66.249...	TCP 80	192.168...	TCP 1131	HttpGetNormal	index.ht...	javascript	163 B
66.249...	TCP 80	192.168...	TCP 1131	HttpGetNormal	bnd.67...	html	6 B
66.249...	TCP 80	192.168...	TCP 1132	HttpGetNormal	bnd.80...	html	6 B
66.249...	TCP 80	192.168...	TCP 1128	HttpGetChunked	bnd.23...	bd	189 B

Live Sniffing Buffer Usage:

<http://www.netresec.com>

NetFlow Analyzer

- NetFlow Analyzer is a “web-based” bandwidth monitoring, network forensics and network traffic analysis tool
- It generates instant reports on network traffic and users using NetFlow from Cisco devices



<http://www.manageengine.com>

NetWitness Investigator

NetWitness Investigator can locally capture live traffic and process packet files from virtually any existing network collection device for quick and easy analysis

- ❑ Real-time, Patented Layer 7 Analytics
 - ❑ Analyze data starting from application layer entities
 - ❑ Extensive network and application layer filtering
-
- ❑ Integrated GeoIP for resolving IP addresses to city/county
 - ❑ SSL Decryption (with server certificate)
 - ❑ Interactive time charts, and summary view



Colasoft Capsa Network Analyzer

- Capsa network analyzer **captures all data transmitted over the network** and provides a wide range of analysis statistics in an intuitive and graphic way
- It identifies and analyzes more than **300 network protocols**, as well as **network applications** based on the protocols

The screenshot displays two windows of the Colasoft Capsa Network Analyzer interface.

Protocol Window: This window shows a hierarchical tree view of network protocols. The root node is 'Ethernet II'. Other nodes include 'IP', 'TCP', 'UDP', 'KMP', 'DHCP', 'Other', 'Loopback', 'PvD', 'ARP', 'Request', 'Ethernet SNAP', and 'Ethernet 802.3'. Each node has associated statistics: Bytes, Packets, Bits Per Sec., Packets/s, Bytes%, and Packets%. The 'IP' node is expanded, showing its sub-nodes: 'Private-use ..' and '10.0.0.0/8'. The '10.0.0.0/8' node is also expanded, listing specific IP addresses: '10.101.1..', '10.101.2..', '10.101.3..', '10.103.1..', '10.103.2..', '10.103.3..', '10.103.4..', and '10.103.5..'. Each IP address entry includes its own set of statistics.

IP Endpoint Window: This window shows a list of IP endpoints. The top section lists 'Private-use ..' and '10.0.0.0/8' with their respective statistics. Below this, a detailed list of IP addresses is provided, each with its own set of statistics. The list includes:

- 10.101.1..: 128.64 MB, 217,824, 8,040 MB, 99,104, 120,589 MB, 124,000
- 10.101.2..: 104,578 MB, 831,133, 37,826 MB, 413,536, 66,752 MB, 417,597
- 10.103.1..: 83,538 MB, 142,054, 78,037 MB, 80,743, 5,501 MB, 62,211
- 10.103.2..: 68,277 MB, 170,047, 61,548 MB, 99,549, 6,729 MB, 70,498
- 10.103.3..: 61,543 MB, 80,904, 57,892 MB, 45,440, 3,300 MB, 53,514
- 10.103.4..: 60,150 MB, 80,588, 5,393 MB, 29,410, 54,757 MB, 51,188
- 10.103.5..: 58,261 MB, 163,673, 20,258 MB, 78,685, 38,004 MB, 84,088

<http://www.colasoft.com>

Firewall Evasion Tool: Traffic IQ Professional

Traffic IQ Professional enables security professionals to **audit and validate the behavior of security devices** by generating the **standard application traffic or attack** traffic between two virtual machines

Traffic IQ Professional can be used to **assess, audit, and test the behavioral characteristics** of any non-proxy packet-filtering device including:

- Application layer firewalls
- Intrusion detection systems
- Intrusion prevention systems
- Routers and switches



The screenshot shows the Traffic IQ Professional software interface. The main window displays a table titled "Traffic Scan Lists" with columns for Internal IP Address, Internal Port, Traffic Type, External IP Address, External Port, Expected Result, Time Limit, and Repeats. A context menu is open over the last row of the table, showing options like Add, Modify, Delete, Select All, Swap, Change, Increment, Decrement, and Change Values, along with dropdown menus for Internal Port, External Port, Internal IP Address, and External IP Address. Below the table, there are sections for Adapter Status and Traffic Status, each showing a list of internal and external machines with their respective packet counts. At the bottom left, it says "Ready".

<http://www.blade-software.com>

Nfdump/NfSen

- Bộ công cụ Nfcapd, Nfdump, NfSen bao gồm các công cụ cho việc thu thập, hiển thị, và phân tích dữ liệu
- Nfcapd là daemon trong Linux được phát triển tích hợp với nfdump để bắt các gói tin NetFlow
- Nfdump đọc các file ghi Nfcapd và xử lý thông tin, nfdump cho phép mở rộng tùy biến các tập tin dữ liệu được lưu trữ trên đĩa.
- NfSen “Netflow Sensor”: cung cấp một giao diện web cho nfdump. Nó là một công cụ mã nguồn mở được viết bằng Perl và PHP, được thiết kế để chạy trên Linux và Unix.

Documenting the Evidence Gathered on a Network



If the **network logs** are small, you can take a print-out and attest



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



If the evidence resides on a remote computer, detailed information about **collection** and **location** should be documented



References

- CHFIv8 Slides: Module 16
- Pháp chứng kĩ thuật số, TS. Đàm Quang Hồng Hải



Q&A



Digital Forensics

Pháp chứng Kỹ thuật số

#6: Network Forensics