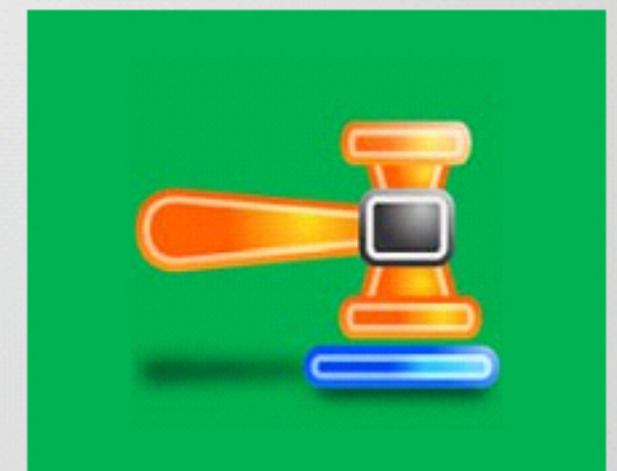
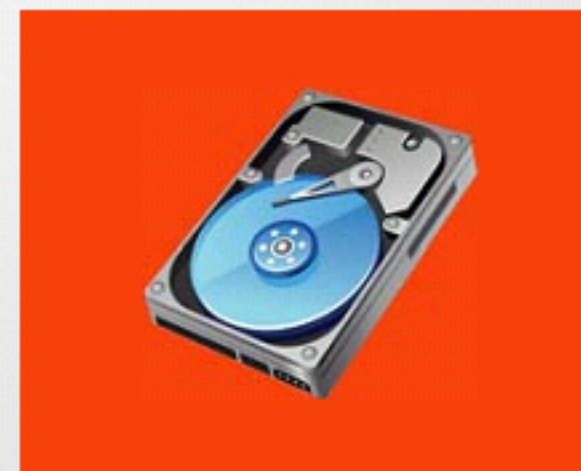


# Network Forensics

## Module 07

Designed by **Cyber Crime Investigators**. Presented by Professionals.





# Module Objectives



After successfully completing this module, you will be able to:

- 1 Understand the importance of network forensics
- 2 Discuss the fundamental logging concepts
- 3 Summarize the event correlation concepts
- 4 Understand network forensic readiness and list the network forensics steps
- 5 Examine the Router, Firewall, IDS, DHCP and ODBC logs
- 6 Examine the network traffic
- 7 Document the evidence gathered on a network
- 8 Perform evidence reconstruction for investigation





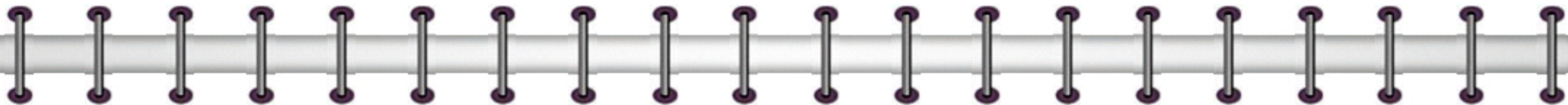
Jessica was missing from her home for a week. She left a note for her father mentioning that she was going to meet her school friend. A few weeks later Jessica's dead body was found near a dumping yard.

Investigators were called in to investigate Jessica's death. A **preliminary investigation of Jessica's computer and logs revealed some facts that helped the cops trace the killer.**



# Network Forensics

- Network forensics is the capturing, recording, and **analysis of network event** in order to discover the source of security incidents
- Capturing network traffic over a network is simple in theory, but relatively **complex** in practice; because of the large amount of data that flows through a network and the complex nature of the Internet protocols
- **Recording network traffic** involves a lot of resources, which makes it unfeasible to record all the data flowing through the network
- Further, an investigator needs to back up these recorded data to free up recording media and **preserve the data for future analysis**



## Network forensics can reveal the following information:

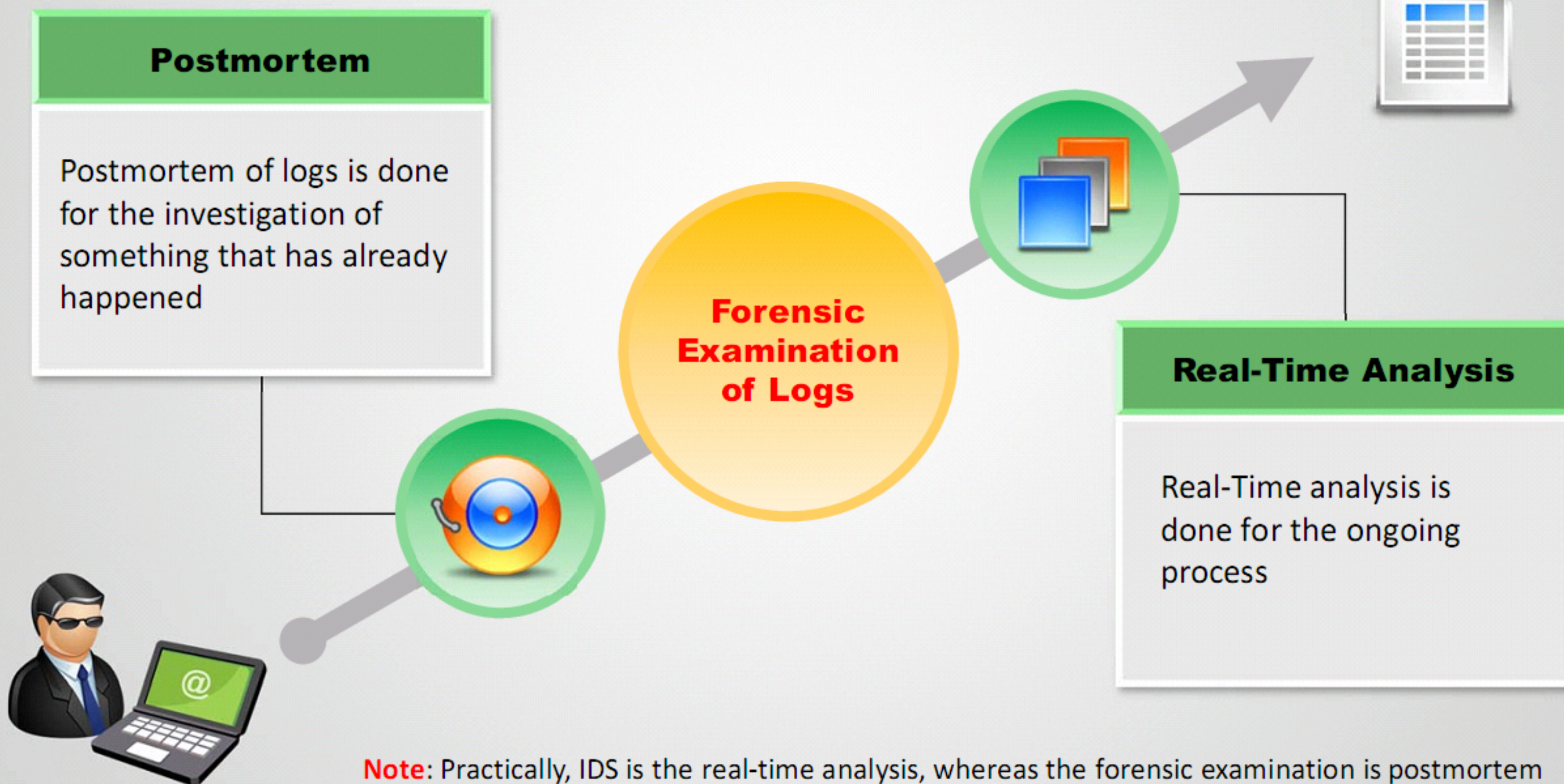
- Source of security incidents
- The path of intrusion
- The Intrusion techniques an attacker used
- Traces and evidence





# Postmortem and Real-Time Analysis

Forensic examination of logs is divided into two categories :





## Network Vulnerabilities

### Internal Network Vulnerabilities

These vulnerabilities occur due to the **overextension of bandwidth** and **bottlenecks**



### External Network Vulnerabilities

These vulnerabilities occur due to the threats such as **DoS/DDoS attacks** and **network data interception**





## Most common attacks launched against networks:

- Eavesdropping
- Data Modification
- IP Address Spoofing
- Denial of Service Attack
- Man-in-the-Middle Attack
- Packet Sniffing
- Enumeration
- Session Hijacking
- Buffer Overflow
- Email Infection
- Malware attacks
- Password-based attacks
- Router Attacks



## Attacks specific to wireless networks:

- Rogue Access Point Attack
- Client Mis-association
- Misconfigured Access Point Attack
- Unauthorized Association
- Ad Hoc Connection Attack
- HoneySpot Access Point Attack
- AP MAC Spoofing
- Jamming Signal Attack





# Where to Look for Evidence

- Logs collected in the **network devices** and **applications** can be used as evidence for investigating network security incidents

Functions	Layers	Protocols	Network Devices and Applications
Handles high-level protocols, issues of representation, encoding, and dialog control	Application layer	File Transfer (TFTP, FTP, NFS), Email (SMTP), Network Management (SNMP), Name Management (DNS)	Servers/Desktops, Anti-virus, Business Applications, Databases
Provides a logical connection between the endpoints and provides transport	Transport layer	Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)	Firewall, IDS/IPS
Selects the best path through the network for data flow	Internet layer	Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP)	Firewall, IDS/IPS, VPN
Defines how to transmit an IP datagram to the other devices	Network Access layer	Ethernet, Fast Ethernet, SLIP, PPP, FDDI, ATM, Frame Relay, SMDS, ARP, Proxy ARP, RARP	Routers and Switches



# Log Files as Evidence

1

Log files are the primary records of **user's activity** on **a system** or **a network**

2

Investigators use these logs to **recover** any services **altered** and **discover** the source of **illicit activities**

3

The basic problem with **logs** is that they can be **altered easily**. An attacker can easily insert false entries into log files

4

Computer records are not normally **admissible** as **evidence**; they must meet certain **criteria** to be admitted at all

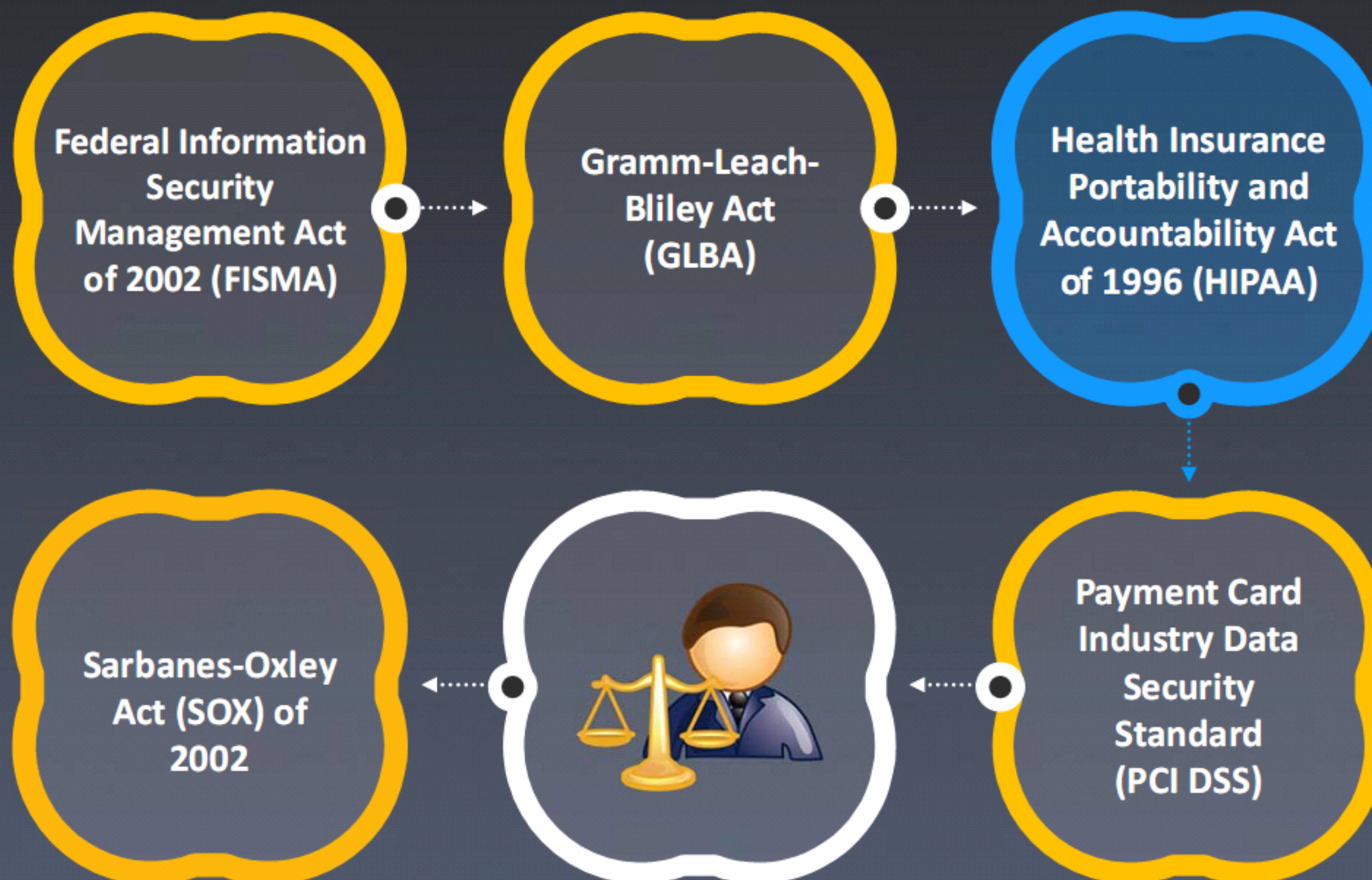
5

The prosecution must present appropriate testimony to show that **logs** are **accurate**, **reliable**, and **fully intact**



# Laws and Regulations

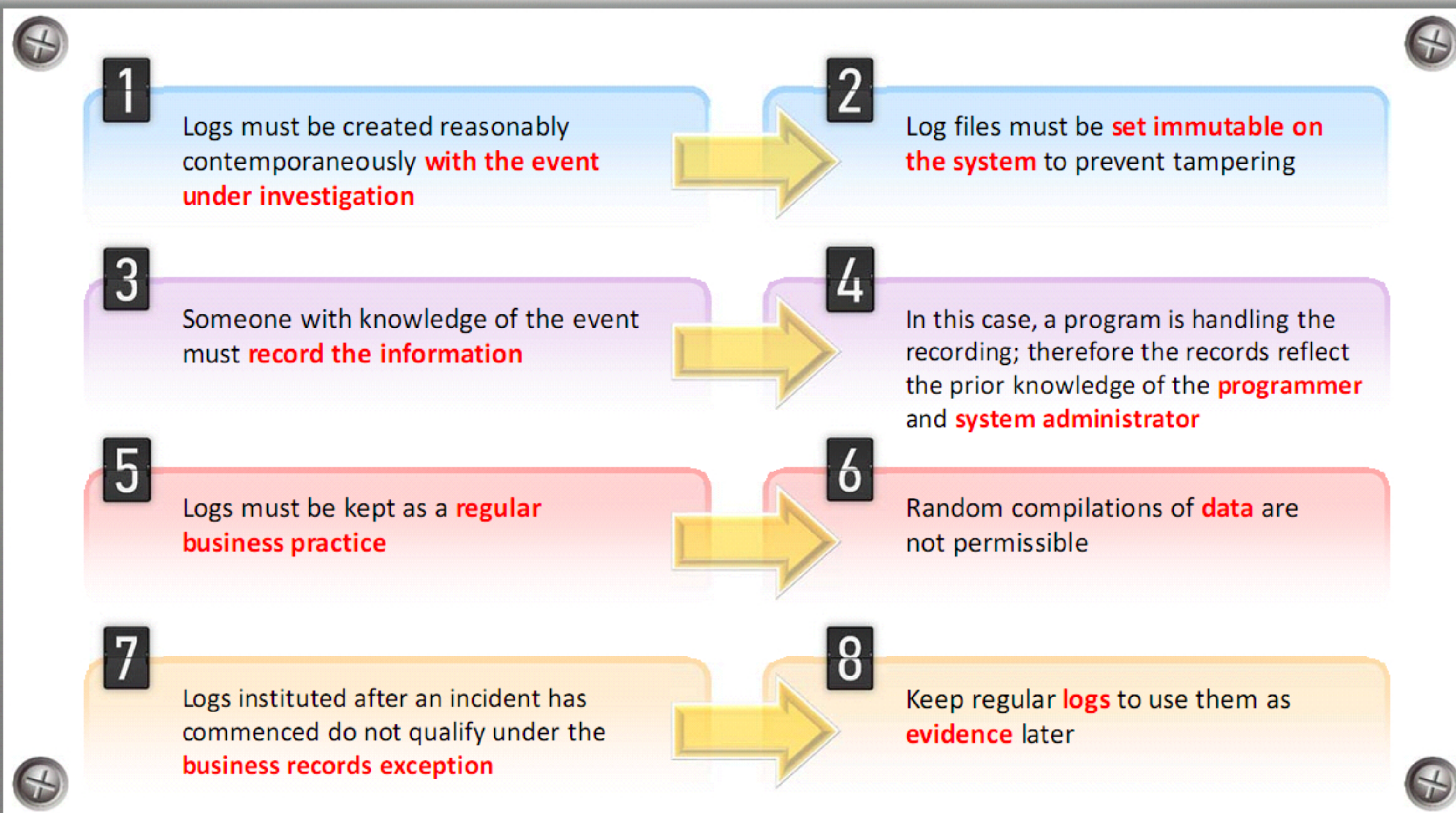
The following regulations, standards, and guidelines define organizations' needs for **log management**:





# Legality of using Logs

Some of the legal issues involved with creating and using logs that organizations and investigators must keep in mind:





# Legality of using Logs (Cont'd)



A “custodian or other qualified witness” must testify to the **accuracy** and **integrity** of the logs. This process is known as authentication

The custodian need not be the programmer who wrote the **logging software**; however, he or she must be able to offer **testimony** on what sort of system is used, where the relevant software came from, how and when the records are produced.



A custodian or other qualified witness must also offer testimony as to the **reliability** and integrity of the **hardware** and **software platform** used, including the logging software

A record of failures or of **security breaches** on the machine creating the logs will tend to impeach the evidence



If an investigator claims that a machine has been penetrated, **log entries** from after that point are inherently suspect



# Legality of using Logs (Cont'd)

1

In a civil lawsuit against alleged hackers, anything in an **organization's own records** that would tend to exculpate the perpetrators can be used against the organization



2

An organization's own **logging and monitoring software** must be made available to the court so that the defense has an opportunity to examine the credibility of the records



3

If an organization can show that the relevant programs are **trade secrets**, the organization may be allowed to keep them secret or to disclose them to the defense only under a confidentiality order



4

The **original copies** of any files are preferred. A printout of a disk or tape record is considered to be an original copy, unless and until judges and jurors come equipped with computers that have **USB or SCSI interfaces**





# Records of Regularly Conducted Activity as Evidence

“A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or a statute permitting certification, unless the source of information or the method of circumstances of preparation indicate lack of trustworthiness.”

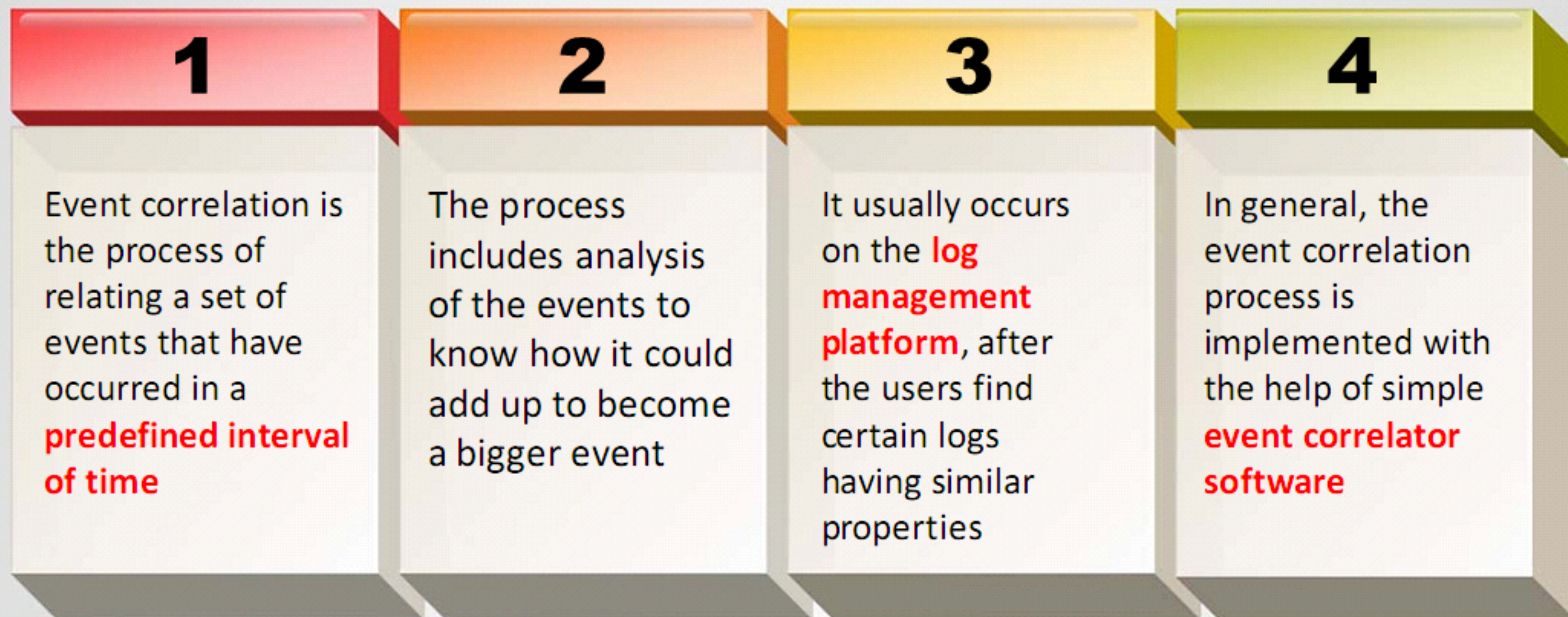
*Rule 803, Federal Rules of Evidence*

110101010000  
000010101001

10100101001010



# Event Correlation



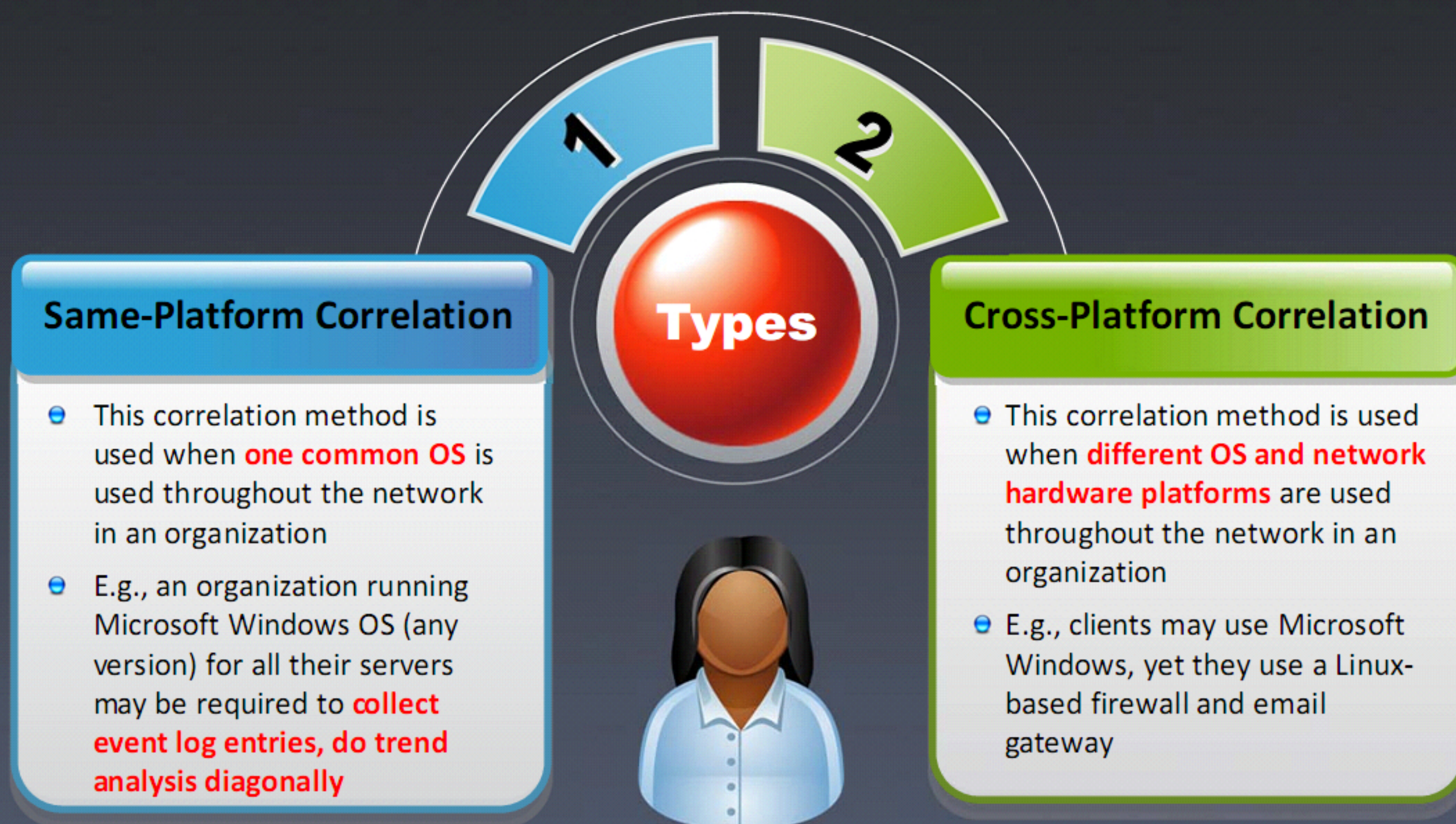
## Steps in event correlation

- Event aggregation
- Event masking
- Event filtering
- Root cause analysis





# Types of Event Correlation





# Prerequisites of Event Correlation

## Transmission of Data

- Transmitting data from one security device to another until it **reaches a consolidation point in the automated system**
- To have a secure transmission and to reduce the risk of exposure during data transmission, the data has to be **encrypted and authenticated**

## Normalization

- After the data is gathered, it must be **formatted** again from different log formats to a single or polymorphic log that can be easily inserted into the database



## Data Reduction

- After collecting the data, repeated data must be **removed** so that the data can be correlated more efficiently
- Removing unnecessary data can be done by **compressing the data, deleting repeated data, filtering** or combining similar events into a single event and sending that to the correlation engine



# Event Correlation Approaches



## Graph-Based Approach

This approach constructs a **graph** with each node as a system component and each edge as a dependency among two components

## Neural Network-Based Approach

This approach uses a **neural network** to detect the anomalies in the event stream, root causes of fault events, etc.



## Codebook-Based Approach

This approach uses **codebook** to store a set of events and correlate them



## Rule-Based Approach

In this approach, events are correlated according to a **set of rules** as follows: condition -> action





# Event Correlation Approaches (Cont'd)

## Field-Based Approach

- A basic approach where specific events are compared with **single or multiple fields** in the normalized data



## Automated Field Correlation

- This method **checks and compares** all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields



## Packet Parameter /Payload Correlation for Network Management

- This approach is used for correlating particular packets with other packets
- This approach can **make a list of possible new attacks** by comparing packets with attack signatures





# Event Correlation Approaches (Cont'd)

## Profile/Fingerprint -Based Approach

- A series of data sets can be gathered from **forensic event data** such as, isolated OS fingerprints, isolated port scans, finger information, and banner snatching to compare link attack data to other attacker profiles
- This information is used to identify whether any system is a **relay** or a **formerly compromised host**, and/or to detect the same hacker from different locations

## Vulnerability-Based Approach

- This approach is used to map **IDS events** that target a particular vulnerable host with the help of a vulnerability scanner
- This approach is also used to deduce an attack on a **particular host** in advance, and it prioritizes attack data so that you can respond to trouble spots quickly

## Open-Port-Based Correlation

- This approach determines the **rate of successful attacks** by comparing it with the list of open ports available on the host and that are being attacked



# Event Correlation Approaches (Cont'd)

## Bayesian Correlation

- This approach is an advanced correlation method that **assumes and predicts what an attacker** can do next after the attack by studying the statistics and probability, and uses only two variables



## Time (Clock Time) or Role-based Approach

- This approach is used to monitor **the computers' and computer users' behavior** and provide an alert if something anomalous is found



## Route Correlation

- This approach is used to **extract the attack route information** and use that information to single out other attack data

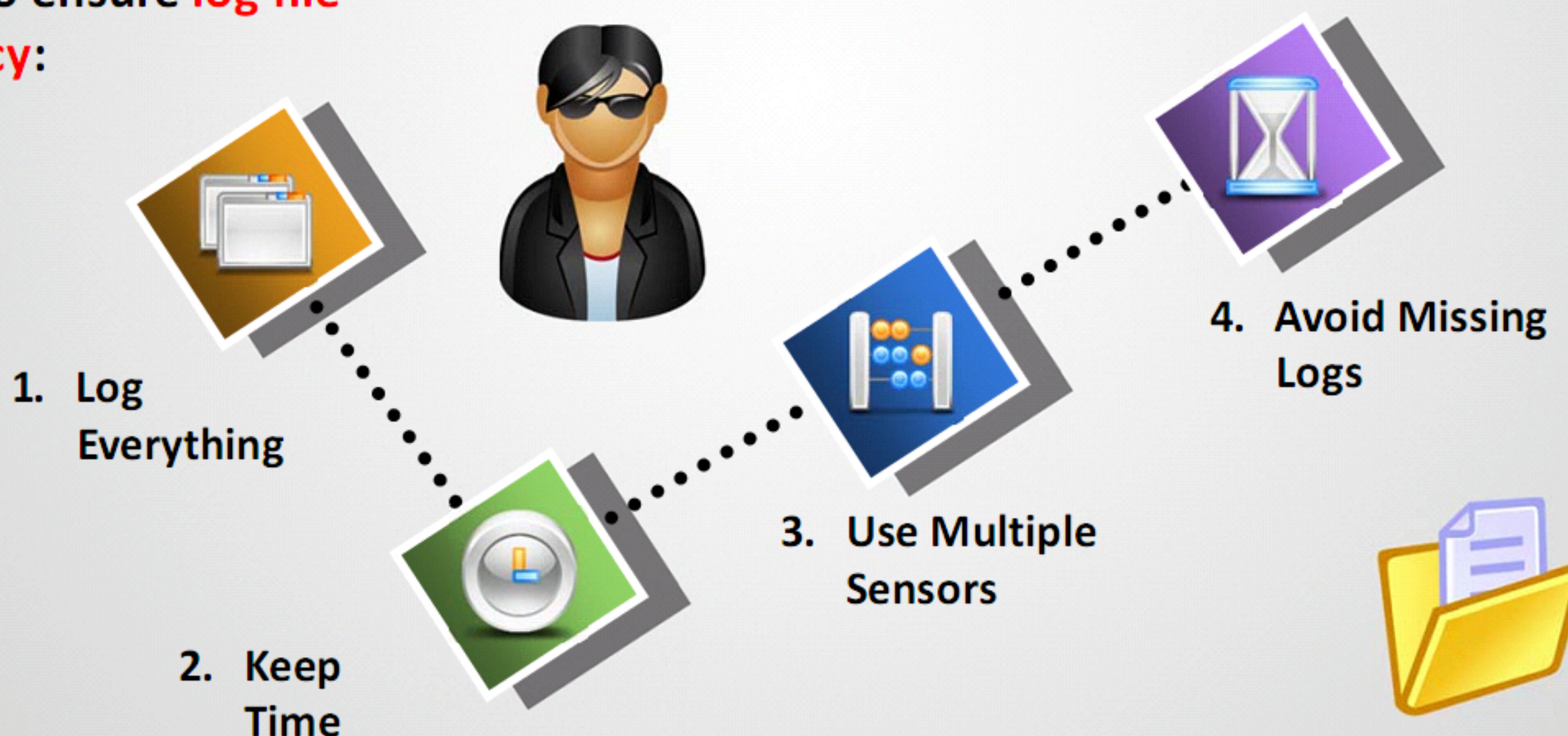




# Ensuring Log File **Accuracy**

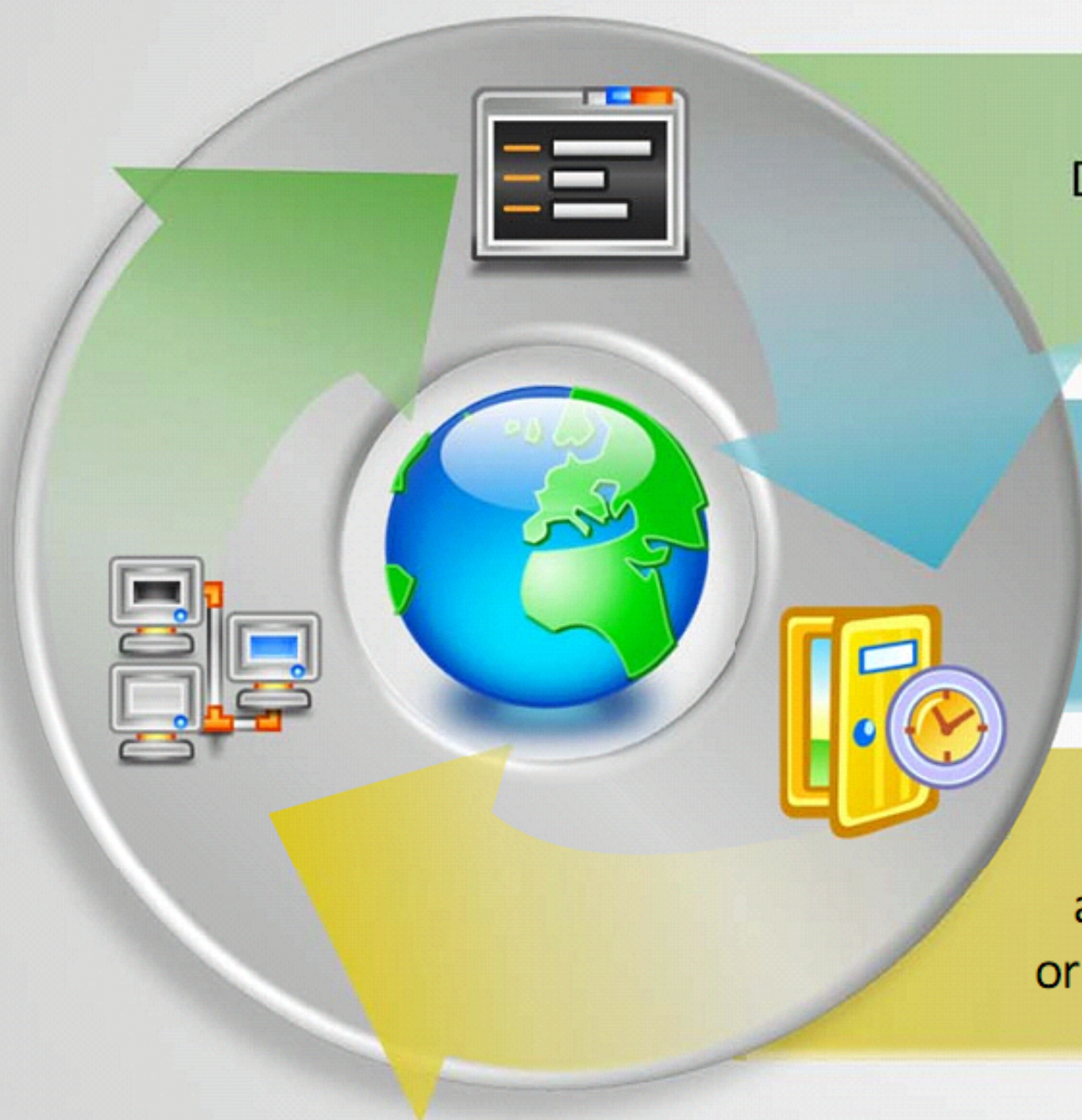
- ❌ The reliability of log files directly depends on their **accuracy**
- ❌ Accuracy means to **present the log files of investigated system** or server before the court in the same state as available
- ❌ Modification to the logs can impact the **validity of the entire log** and subject it to suspicion

## Steps to ensure **log file accuracy**:





# Log Everything



Do not consider any field in log files as less important, as every field can **play a major role as evidence**

Network administrators should always **configure the server logs settings** to record every field available

**E.g.:** Configure IIS logs to record web user information about the Web in order to gather clues about the attack origin either a logged-in user or external system

Consider a defendant who claims a hacker had attacked his system and installed a back-door proxy server on his computer. The attacker then used the back-door proxy to attack other systems. In such a case, how does an investigator prove that the traffic came from a specific user's Web browser or that it was a proxied attack from someone else?



- With the Windows time service, a network administrator can **synchronize standalone servers** to an external time source
- If you use a domain, the **Time Service** will automatically be synchronized to the **domain controller**



- A network administrator can synchronize a standalone server to an external time source by setting certain registry entries:
  - **Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
  - **Setting:** Type
  - **Type:** REG\_SZ
  - **Value:** NTP
  - **Key:** HKLM\SYSTEM\CurrentControlSet | Services\W32Time\Parameters\
  - **Setting:** NtpServer
  - **Type:** REG\_SZ
  - **Value:** ntp.xsecurity.com

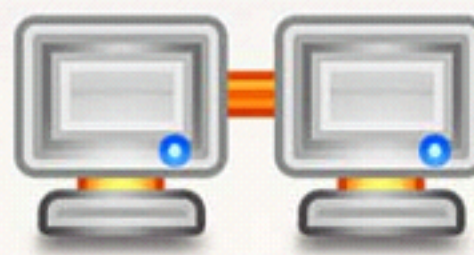


# Why Synchronize Computer Times?



When an administrator is investigating intrusion and security events that involve multiple computers, it is essential to synchronize the computers' clocks

1



If computers' clocks are not synchronized, it becomes almost impossible to accurately **correlate actions** that are logged on different computers

2



If the clocks on these computers are not accurate, it also becomes difficult to correlate logged activities with outside actions

3



# What is **Network Time Protocol** (NTP)?

- It is an Internet standard protocol (built on top of TCP/IP) used to **synchronize the clocks of client computers**
- NTP sends time requests to known servers and obtains **server time stamps**. Using those stamps, it adjusts the client's time

## Features of NTP:

- It is fault tolerant and dynamically auto-configuring
- It synchronizes accuracy up to one millisecond
- It can be used to synchronize all computers in a network
- It uses UTC time
- It is available for every type of computer





# Using Multiple Sensors



- Employ multiple sensors (firewall, IDS, etc.) to **record logs**. This helps to **prove the log credibility** if two separate devices record the same information

- Also, combining logs from different devices can **strengthen the value** of each

**E.g.:** Logs from Firewall, IDS, IPS may be helpful to prove that a system with a particular IP address has accessed a specific server at a particular point of time



# Avoiding Missing Logs

- When a web server is **offline or powered off**, log files are not created



- When a log file is missing, it is difficult to know if the server was actually offline or powered off, or if the **log file was deleted**



- If the record of hits shows that the server was online and active at the time that **log file data is missing**, the administrator knows that the missing log file might have been deleted



- To combat this problem, an administrator can **schedule a few hits to the server** using a scheduling tool and then keep a log of the outcomes of these hits to determine when the server was active



# Implement Log Management

- Log management is the **process of dealing** with large amounts of **system generated logs and records**

- It includes all the **processes and techniques** used to collect, aggregate, analyze, and report the computer-generated log messages

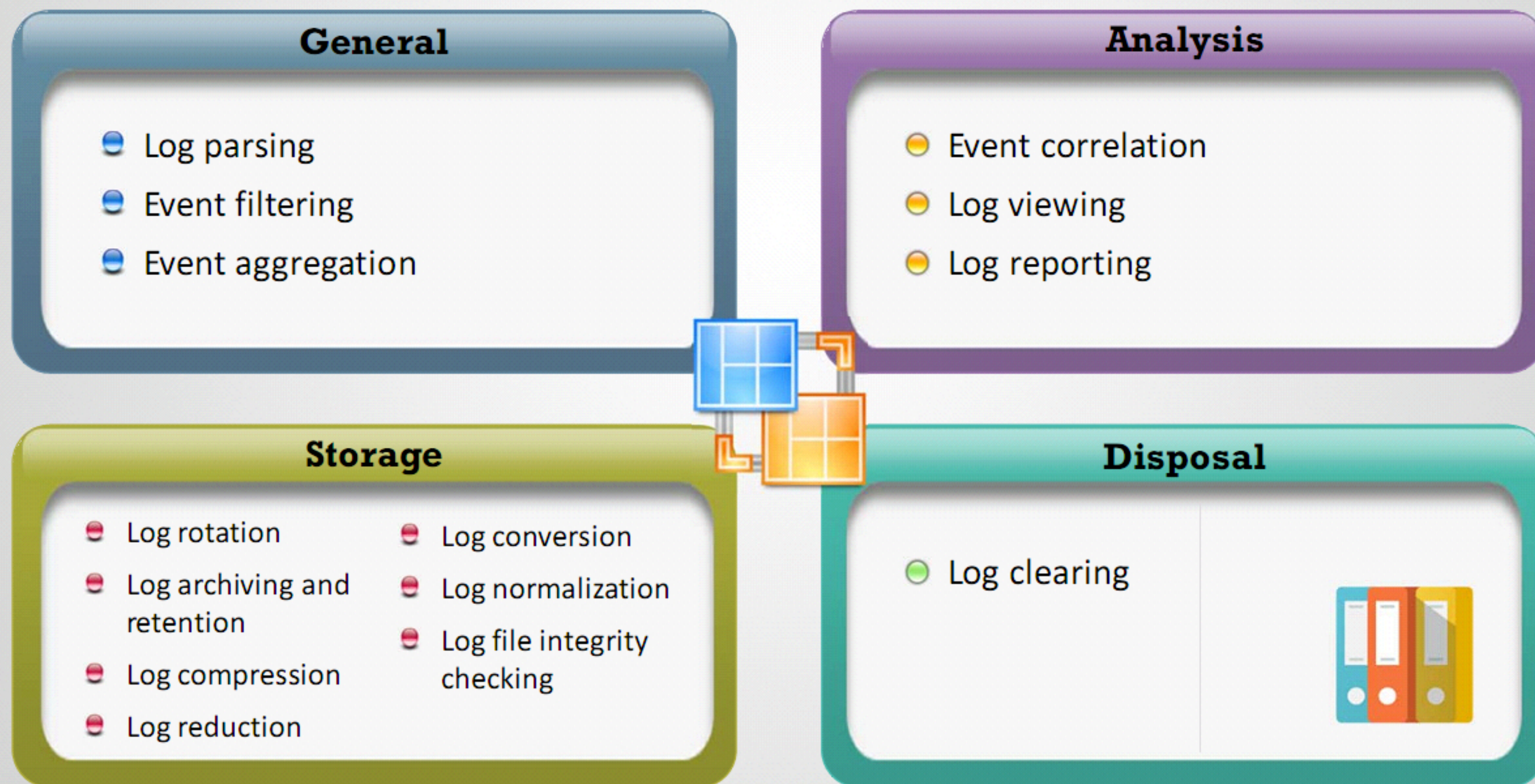
- Log management infrastructure consists of the hardware, software, networks, and media used to **generate, transmit, store, analyze, and dispose of log data**

- Log management **infrastructure** typically comprises the following three tiers:
  - Log generation
  - Log analysis and storage
  - Log monitoring



# Functions of Log Management Infrastructure

- Common log management infrastructure functions include:





# Challenges in Log Management



- Potential problems with the gathering of logs because of their **variety and dominant occurrence**



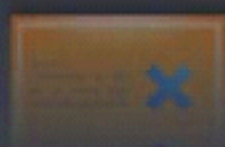
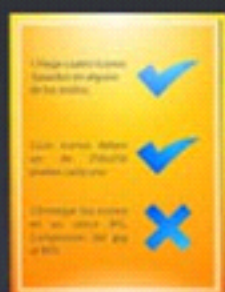
- Compromise of confidentiality, integrity, and availability of the logs is often **intentional or accidental**



- People performing log analysis have **no formal training** and often deprived of proper support



# Meeting the Challenges in Log Management



1

## Requirements

Define **requirements and goals** for performing log management across the organization

## Approach

Generate **policies and procedures** for log management to ensure a **consistent method**

2

4

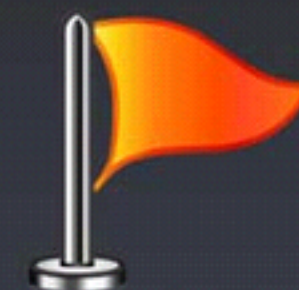
## Training

Provide the necessary training to all staff regarding their **log management responsibilities**

## Security

Create and maintain **infrastructure** for **secure log management**

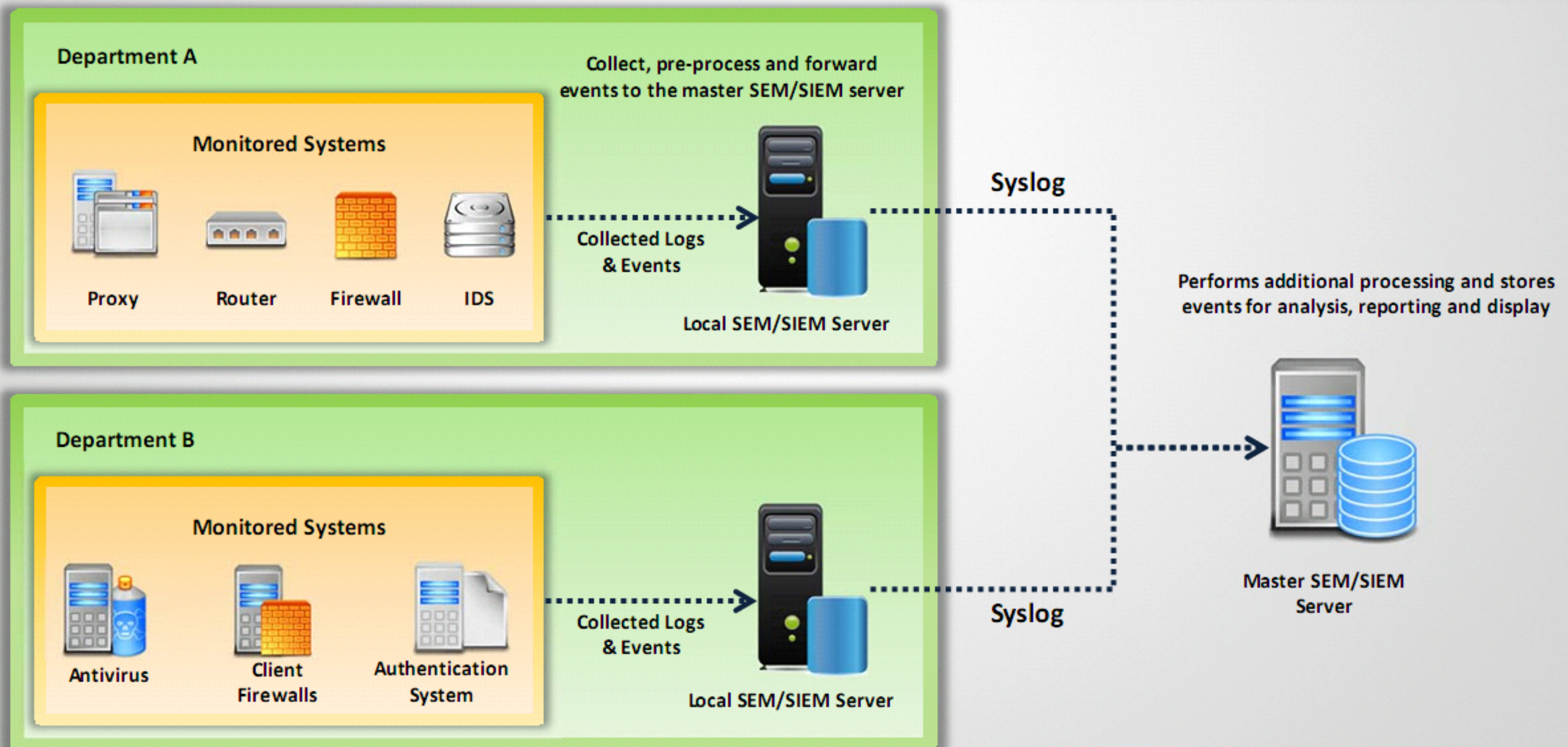
3





# Centralized Logging

- Centralized logging is defined as gathering the **computer system logs** for a group of systems in a centralized location
- It is used to efficiently monitor computer system logs with the frequency required to detect **security violations and unusual activity**





Syslog is a standard, network devices use to **forward log messages** to a server across an IP network

The term syslog refers to both the **syslog protocol** and the **application** or library sending syslog messages

Syslog sender sends log messages to the syslog receiver, also known as **syslogd**, syslog daemon or syslog server

Syslog uses either **TCP** or **UDP** to transfer log messages in a **cleartext format**



# IIS Centralized Binary Logging

- Centralized binary logging is a process in which many websites write **binary and unformatted log data** to a single log file
- An administrator needs to use a parsing tool to view and analyze the data. The files have the extension .ibl, which stands for the Internet binary log
- It is a server property, so all websites on that server **write log data** to the central log file
- It decreases the amount of system resources that are consumed during logging, therefore increasing performance and scalability

## Fields that are included in the centralized binary log file format:

- |                     |                     |                     |
|---------------------|---------------------|---------------------|
| • Date              | • Server IP address | • Server IP address |
| • Time              | • Server port       | • Server port       |
| • Client IP address | • Method            | • Method            |
| • User name         | • URI stem          | • URI stem          |
| • Site ID           | • URI query         | • URI query         |
| • Server name       | • Protocol status   | • Protocol status   |



# Ensure System's Integrity

Always **stay up-to-date** on service packs and hotfixes to assure that the system's files are valid



Audit all changes to binary files in **Windows System directory**



If an intruder is able to **modify system files** that record log files, then the log files are not valid as evidence





# Control Access to Logs



1

- In order to prove the credibility of logs, an investigator or network administrator needs to ensure that any **access to those files is audited**

2

- The investigator or administrator can use **NTFS permissions** to secure and audit the log files

3

- Web server needs to be **able to write to log files** when the logs are open, but no one else should have access to write to these files

4

- Once a log file is closed, no one should have access to modify the **contents of the file**



# Ensure Log File **Authenticity**



An investigator can prove that log files are authentic if he or she can prove that the **files have not been altered** since they were originally recorded



- Log files are generally simple text files that are easy to alter. The date and time stamps on these files are also easy to modify. Hence, they **cannot be considered authentic in their default state.**
- If a server has been compromised, the investigator should **move the logs off the server**



The logs should be **moved to a master server** and then moved offline to secondary storage media such as a DVD or portable disk





# Use Signatures, Encryption, and Checksums

- The only way to ensure the log file accuracy is to sign and encrypt the log using **PGP** or some other **public-key encryption scheme**
- File signatures are helpful because if a single file is corrupted, it does not invalidate the rest of the logs
- Tools such as **Fsum** can be used to generate **MD5 hashes** for the files
- Store the signatures and hashes with the logs, but also store a secure copy in a separate location

```
Administrator: Command Prompt

C:\Users\Admin\Desktop\fsum>fsum.exe

SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2007. All rights reserved.

Usage: fsum.exe <OPTIONS>... <FILE>...

Options:

  -c or --check      - check sums against given list
  -d<directory>     - set working directory
  -jf               - print only failed lines while checking
  -jm               - use MD5 format
  -js               - use SFV format
  -jnc              - suppress comments
  -r                - recurse subdirectories
  -s or --status     - don't output anything, status code shows success
  -w or --warn       - warn about improperly formatted checksum lines

  -md2              - include MD2 algorithm
  -md4              - include MD4 algorithm
  -md5              - include MD5 algorithm
  -sha1             - include SHA-1 algorithm
  -sha256           - include SHA-2( 256 ) algorithm
  -sha384           - include SHA-2( 384 ) algorithm
  -sha512           - include SHA-2( 512 ) algorithm
  -rmd              - include RIPEMD-160 algorithm
  -tiger            - include TIGER algorithm
  -panama           - include PANAMA algorithm
  -adler            - include ADLER32 algorithm
  -crc32            - include CRC32 algorithm
  -edonkey          - include EDONKEY algorithm

C:\Users\Admin\Desktop\fsum>fsum.exe -md5 Test.docx

SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2007. All rights reserved.

; SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337 <www.slavasoft.com>
;
; Generated on 05/11/16 at 15:31:15
;
3bdca7c407daa3e6cfbab0647944c09a *Test.docx

C:\Users\Admin\Desktop\fsum>
```



# Work with Copies

1

As with all forensic investigations, an investigator should **never work with the original files** when analyzing log files

2

The investigator should **create copies** before performing any postprocessing or log file analysis

3

If the original files are unaltered, the investigator can prove more **easily** that they are authentic and in their original form

4

When using log files as evidence in court, an investigator is required to **present the original files in their original form**



# Maintain Chain of Custody

As with all forensic evidence, the chain of custody must be maintained for log files



An investigator can prove that the log file has not been altered or modified since its capture; if he/she maintains the chain of custody

This can be done with either technical or nontechnical methods, such as MD5 authentication



When an investigator or a network administrator moves log files from a server, and after that to an offline device, he or she should keep track of where the log file went and what other devices it passed through





# Condensing Log File

1

Log files can be sorted by using a **syslog**, but the output of the syslog contains a large log file

2

It is difficult for the forensic team to look for the **important log entry**



3

Log entries need to be **filtered as per the requirement**



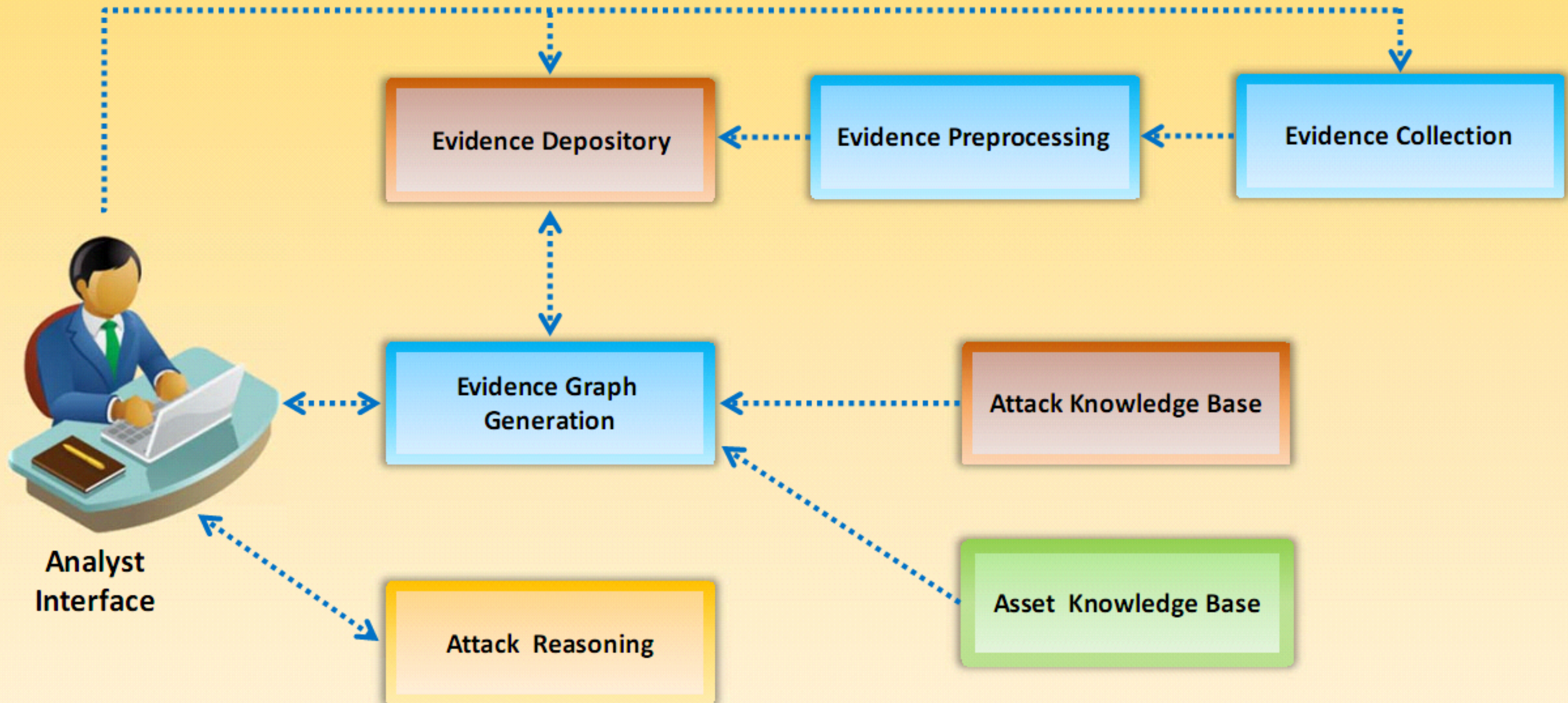
4

Tools that can be used:

- **Swatch**  
(<https://sourceforge.net/projects/swatch>)
- **Logcheck** (<http://logcheck.org>)



# Network Forensics Analysis Mechanism





# Log Capturing and Analysis

## Tools: GFI EventsManager

- GFI EventsManager enables to **manage event log data** for system reliability, security, availability, and compliance
- It **enables increased uptime** by collecting, normalizing, analyzing, categorizing and consolidating log data from multiple sources across the network

The screenshot displays the GFI EventsManager 2013 application window. The interface includes a menu bar (File, Configure, Help), a toolbar (Status, Configuration, Events Browser, Reporting, General), and a sidebar with a tree view of event sources. The main pane shows a filtered list of 34 security events. The 'Event description' pane on the right provides details for a selected event.

**Filter: Security Events (34 events)**

Type	Importance	Event ID	Date	Time	Rule Name	Log Format
Success Audit	Low	4624	2016/05/13	11:38:28	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	11:38:28	Logon attempt ...	Windows
Success Audit	Low	4624	2016/05/13	11:35:38	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	11:35:38	Logon attempt ...	Windows
Success Audit	Low	4624	2016/05/13	11:35:37	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	11:35:37	Logon attempt ...	Windows
Success Audit	Low	4634	2016/05/13	11:35:07	User Logoff	Windows
Success Audit	Low	4634	2016/05/13	11:35:07	User Logoff	Windows
Success Audit	Low	4624	2016/05/13	11:35:07	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	11:35:07	Logon attempt ...	Windows
Success Audit	High	4717	2016/05/13	11:15:35	User right assign...	Windows
Success Audit	Low	4634	2016/05/13	11:15:31	User Logoff	Windows
Success Audit	Low	4624	2016/05/13	11:15:31	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	11:13:50	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	11:13:45	Successful Log...	Windows
Success Audit	Low	4634	2016/05/13	11:00:31	User Logoff	Windows
Success Audit	Low	4634	2016/05/13	11:00:31	User Logoff	Windows
Success Audit	Low	4624	2016/05/13	11:00:31	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	11:00:31	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	11:00:31	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	11:00:31	Logon attempt ...	Windows
Success Audit	Low	4624	2016/05/13	10:58:14	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	10:58:14	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	10:49:21	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	10:48:36	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	10:35:47	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	10:28:52	Logon attempt ...	Windows
Success Audit	Low	4624	2016/05/13	10:04:55	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	09:54:58	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	09:54:44	Logon attempt ...	Windows
Success Audit	Low	4624	2016/05/13	09:54:44	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	09:52:01	Successful Log...	Windows
Success Audit	Low	4624	2016/05/13	09:52:01	Successful Log...	Windows
Success Audit	Medium	4648	2016/05/13	09:52:01	Logon attempt ...	Windows

**Event description**

Medium: Logon attempt using explicit credentials used to impersonate Administrators - during work hours

Date: 2016/05/13  
Time: 09:52:01  
Importance: Medium  
Rule Name: Logon attempt using explicit credentials used to impersonate Administrators - during work hours  
Monitored machine: RD-006  
Log Format: Windows  
Log Name: Security  
Event ID: 4648  
In Work Hours: Yes  
IsAdmin: Yes

A logon was attempted using explicit credentials.

Subject: Security ID: NT AUTHORITY  
Account Name: RD-006\$  
Account Domain: WORKGROUP  
Logon ID: 0x3E7  
Logon GUID: 00000000-0000-0000-0000-000000000000

Account whose Credentials were used:  
Account Name: Admin  
Account Domain: RD-006  
Logon GUID: 00000000-0000-0000-0000-000000000000

Target Server:  
Target Server Name: localhost  
Additional Information: localhost

Process Information:  
Process ID: 772  
Process Name: C:\Windows\System32\svchost.exe

Network Information:  
Network Address: 127.0.0.1  
Port: 0

This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.

Online information:  
<http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventId=4648>

Loading view finished. Click here for details.

Database: C:\Program Files (x86)\GFI\Database Server 2.1\Databases\esrmstg - Security Events - 34 event(s)



# Log Capturing and Analysis

## Tools: EventLog Analyzer

- EventLog Analyzer allows organizations to **automate the process of managing machine generated logs** by collecting, analyzing, correlating, searching, reporting, and archiving from one central location

The screenshot shows the ManageEngine EventLog Analyzer web interface. The top navigation bar includes links for Home, Reports, Compliance, Search, Alerts, Correlation, Settings, and Log Me. The main content area displays a 'Custom Report' for host 'WIN-CQCMK62867E'. Below the host name, there is a table titled 'Important Events' with columns for Process, Facility, Error, Warning, Information, Success, and Failure. The table lists various system events, including 'NET Runtime', 'Adobe Reader', 'Apache Service', 'ApexSQLMonitorService', 'Application Error', 'Application Hang', 'ASP.NET 4.0.30319.0', and 'Customer Experience Improvement'.

The screenshot shows a detailed view of a specific event in the ManageEngine EventLog Analyzer. The event is titled 'Application [ Microsoft-Windows-User Profiles Service ]'s Information events'. The event details are as follows:

Host	Event ID	Source	Message	Time
WIN-CQCMK62867E	1531	Microsoft-Windows-User Profiles Service	The User Profile Service has started successfully	09 May 2016, 10:47
WIN-CQCMK62867E	1532	Microsoft-Windows-User Profiles Service	The User Profile Service has stopped	09 May 2016, 10:46
WIN-CQCMK62867E	1530	Microsoft-Windows-User Profiles Service	Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards. No user action is required. DETAIL - 2 user registry handles leaked from \Registry\User\S-1-5-80-3263513310-3392720605-179883954-6-683002060-3227631582: Process 4172 (\Device\HarddiskVolume2\Windows\System32\conhost.exe) has opened key \REGISTRY\USER\S-1-5-80-3263513310-3392720605-179883954-6-683002060-3227631582\Control Panel\International Process 3160 (\Device\HarddiskVolume2\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\fdhost.exe) has opened key \REGISTRY\USER\S-1-5-80-3263513310-3392720605-179883954-6-683002060-3227631582\Control Panel\International	09 May 2016, 10:46
WIN-CQCMK62867E	1530	Microsoft-Windows-User Profiles Service	Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards. No user action is required. DETAIL - 3 user registry handles leaked from \Registry\User\S-1-5-21-2380688692-3007623415-286098518-6-500_Classes: Process 1348 (\Device\HarddiskVolume2\ProgramData\ApexSQL\ApexSQLAudit\Bin\2015.4.1254.0\ApexSQLAuditProcessor.Distributed.Console.exe) has opened key \REGISTRY\USER\S-1-5-21-2380688692-3007623415-286098518-6-500_CLASSES Process 1348 (\Device\HarddiskVolume2\ProgramData\ApexSQL\ApexSQLAudit\Bin\2015.4.1254.0\ApexSQLAuditProcessor.Distributed.Console.exe) has opened key \REGISTRY\USER\S-1-5-21-2380688692-3007623415-286098518-6-500_CLASSES	09 May 2016, 10:45

<https://www.manageengine.com>



# Log Capturing and Analysis Tools (Cont'd)



**Kibana**

<https://www.elastic.co>



**OSSEC**

<http://ossec.github.io>



**Syslog-ng**

<https://syslog-ng.org>



**Ipswitch Log Management**

<https://www.ipswitch.com>



**RSYSLOG**

<http://www.rsyslog.com>



**Veriato Server Manager**

<http://www.veriato.com>



**Firewall Analyzer**

<https://www.manageengine.com>



**Log Management Utility**

<http://www.biz.konicaminolta.com>



**Simple Event Correlator (SEC)**

<https://simple-evcorr.github.io>



**Snare**

<https://www.intersectalliance.com>



# Log Capturing and Analysis Tools (Cont'd)



**Splunk Enterprise**

<http://www.splunk.com>



**Logscape**

<http://logscape.com>



**Loggly**

<https://www.loggly.com>



**ArcSight ESM**

<http://www8.hp.com>



**vRealize Log Insight**

<http://www.vmware.com>



**XpoLog Log Management**

<http://www.xpolog.com>



**Sumo Logic**

<https://www.sumologic.com>



**LogRhythm**

<https://www.logrhythm.com>



**TIBCO LogLogic**

<http://www.tibco.com>



**Sawmill**

<https://www.sawmill.net>



# Log Capturing and Analysis Tools (Cont'd)



## McAfee Enterprise Log Manager

<http://www.mcafee.com>



## Event Log Explorer

<http://www.eventlogxp.com>



## Log & Event Manager

<http://www.solarwinds.com>



## WebLog Expert

<https://www.weblogexpert.com>



## Papertrail

<https://papertrailapp.com>



## ELM Enterprise Manager

<http://tntsoftware.com>



## EventReporter

<http://www.eventreporter.com>



## EventSentry

<http://www.eventsentry.com>



## Kiwi Log Viewer

<http://www.kiwisyslog.com>



## LogMeister

<http://www.logmeister.com>



# Log Capturing and Analysis Tools (Cont'd)



**InTrust**

<http://software.dell.com>



**MyEventViewer**

<http://www.nirsoft.net>



**Alert Logic Log Manager**

<https://www.alertlogic.com>



**WinAgents EventLog Translation Service**

<http://www.winagents.com>



**Sentinel Log Manager**

<https://www.netiq.com>



**EventTracker Enterprise**

<http://www.eventtracker.com>



**Tripwire Log Center**

<http://www.tripwire.com>



**Logstash**

<http://www.netwrix.com>



**AlienVault Unified Security Management**

<https://www.alienvault.com>



**SecurityCenter CV**

<https://www.tenable.com>



# Log Capturing and Analysis Tools (Cont'd)



## The Elastic Stack

<https://www.elastic.co>



## Logseene

<https://www.sematext.com>



## CorreLog

<https://correlog.com>



## SaaS Log Management

<http://www.cloudaccess.com>



## Assuria Log Manager

<http://www.assuria.com>



## ApexSQL Log

<http://www.apexsql.com>



## BlackStratus LOGStorm

<http://www.blackstratus.com>



## FortiSIEM

<https://www.fortinet.com>



## PowerBroker Event Vault

<https://www.beyondtrust.com>



## Graylog

<https://www.graylog.org>



# Analyzing Router Logs

- Routers **store network connectivity logs** with details such as date, time, source and destination IPs and Ports used
- This information can **help investigators in verifying the timestamps of an attack** and correlate various events to find the source and destination IP
- Routers **have many standards for storing the log** details of a network

The incoming log details are as follows:

1. Date and time
2. Source IP address
3. Source-port
4. Destination IP address
5. Destination-port

```
Router Logs - Notepad
File Edit Format View Help
1/27/2016 20:21:31 TCP from 151.197.xxx.xxx:3573 to xxx.xxx.xxx.xxx:445
1/27/2016 20:21:50 TCP from 151.197.xxx.xxx:3473 to xxx.xxx.xxx.xxx:2745
1/27/2016 20:21:58 TCP from 68.162.xxx.xxx:3267 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:00 TCP from 151.197.xxx.xxx:3273 to xxx.xxx.xxx.xxx:2745
1/27/2016 20:22:01 TCP from 68.162.xxx.xxx:3147 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:14 TCP from 151.197.xxx.xxx:2806 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:16 TCP from 151.197.xxx.xxx:3657 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:17 TCP from 151.197.xxx.xxx:3013 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:19 TCP from 151.197.xxx.xxx:3104 to xxx.xxx.xxx.xxx:445
```

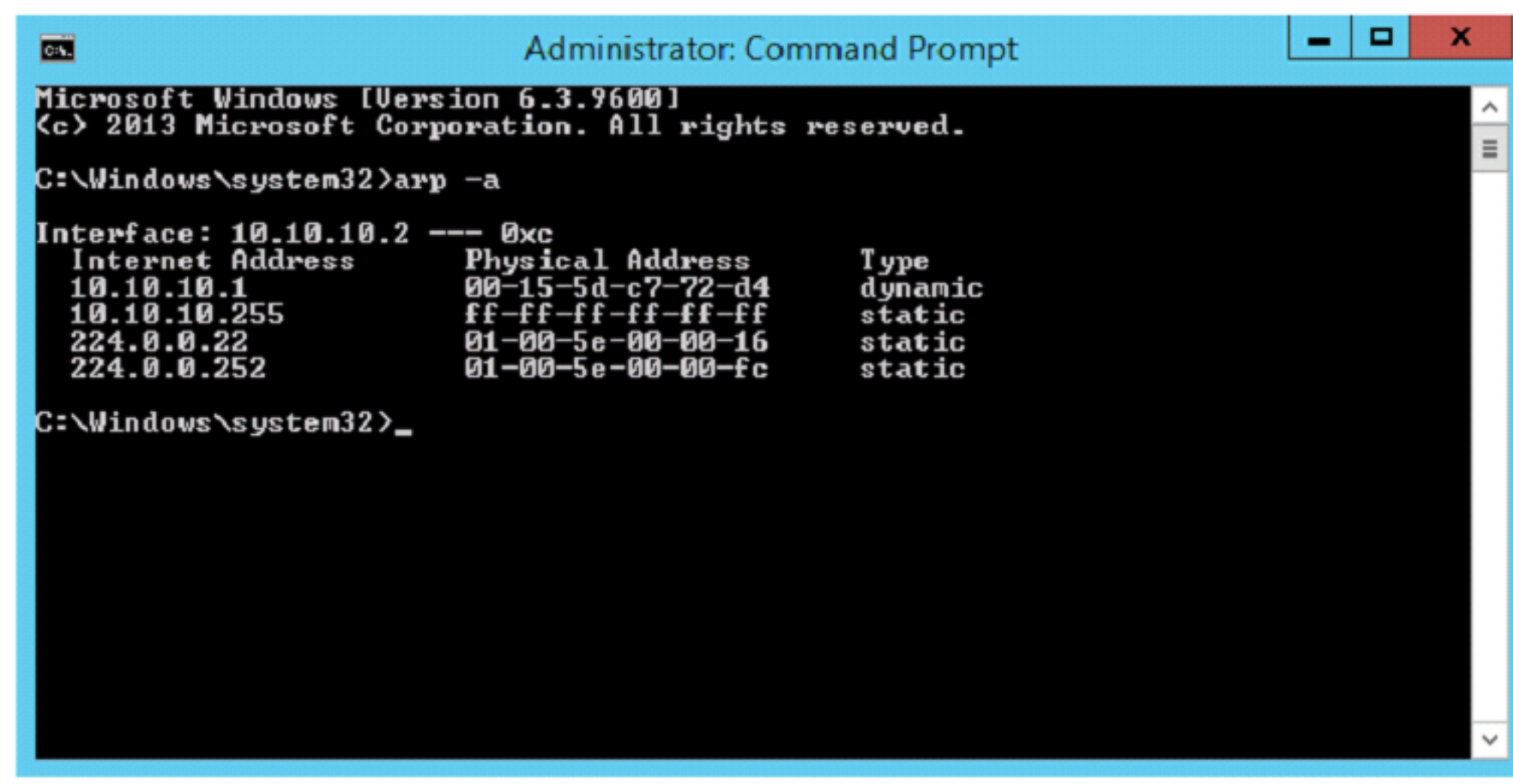


# Evidence Gathering from ARP Table

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**

An investigator can view the ARP table in Windows by issuing the command **arp -a**

The ARP table maintained on the router is of crucial importance, as it can provide information about the MAC address of all the hosts that were involved in recent communications



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -a

Interface: 10.10.10.2 --- 0xc
Internet Address      Physical Address      Type
10.10.10.1            00-15-5d-c7-72-d4    dynamic
10.10.10.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static

C:\Windows\system32>
```



# Analyzing Router Logs (Cont'd)

The outgoing log details are as follows:

1. Date
2. Time
3. Source IP address
4. Source-port
5. URL accessed
6. URL IP address
7. Port Used

```
Router Logs - Notepad
File Edit Format View Help
1 10/27/2004 20:19:21 TCP from 192.168.1.100:1037 4 to springmount-services.com
(108.167.161.72):80
10/27/2004 20:20:18 TCP from 192.168.1.100:1037 4 to www.agarbot.ovh
(104.31.88.182):80
10/27/2004 20:23:51 TCP from 192.168.1.100:1040 3 to supportcenter.verizon.net 5
(206.46.187.54):80
10/27/2004 20:23:52 TCP from 192.168.1.100:1041 to toshibadirect.com
(216.23.181.216):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1048 to crs.akamai.com
(65.161.97.137):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1049 to statse.webtrends.live.com
(63.236.111.50):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1051 to tracking.rangeonlinemedia.com
(66.179.100.233):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1052 to statse.webtrends.live.com
63.236.111.50:80 6 7
```



# Analyzing Router Logs: Cisco

- Cisco routers run on specific operating system, the **Cisco IOS**
- The OS has a built in security manager that **defines policies regarding basic logging parameters**
- The router **complies with syslog standards** to define severity levels using numeric code

Level	System	Description
Emergency	0	System unusable messages
Alert	1	Immediate action required messages
Critical	2	Critical condition messages
Error	3	Error condition messages
Warning	4	Warning condition messages
Notification	5	Normal but significant messages
Information	6	Informational messages
Debugging	7	Debugging messages



# Analyzing Router Logs: Cisco (Cont'd)

Cisco IOS helps users to classify logs using certain predefined identifiers such as:

Mnemonic	Severity	Description
%SEC-6-IPACCESSLOGDP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGNP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGP	6	A packet matching the log criteria for the given access list has been detected (TCP or UDP)
%SEC-6-IPACCESSLOGRL	6	Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available.
%SEC-6-IPACCESSLOGRP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGS	6	A packet matching the log criteria for the given access list was detected.
%SEC-4-TOOMANY	4	The system was not able to process the packet because there was not enough room for all of the desired IP header options. The packet has been discarded.
%IPV6-6-ACCESSLOGP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGDP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGNP	6	A packet matching the log criteria for the given access list was detected.



# Analyzing Router Logs: Cisco (Cont'd)

## ■ The Cisco router log details are as follows:

1. Event ID
2. Date
3. Time
4. Identifier
5. Protocol applied
6. Source IP address
7. Destination IP address



```
Cisco Router Logs - Notepad
File Edit Format View Help
002416 Feb 22 2016 11:51:07.149 EDT: %SEC-6-IPACCESSLOGP: list 185 denied
tcp 172.16.1.14(7331) -> 192.168.2.1(418), 1 packet [0x279C8521]
002417: Feb 22 2016 11:51:08.153 EDT: %SEC-6-IPACCESSLOGP: list 185 denied
tcp 172.16.1.14(7331) -> 192.168.2.1(428), 1 packet [0x279C8521]
002418: Feb 22 2016 11:51:09.153 EDT: %SEC-6-IPACCESSLOGP: list 185 denied
tcp 172.16.1.49(36426) -> 192.168.2.1(438), 1 packet [0x279C8521]
```



# Analyzing Router Logs: **Juniper**

Juniper networking devices run on the company's proprietary **Junos operating system**

The router stores logs in the **default messages file**

In M-, MX-, and T-series routers, the log files are present in **/var/log/ location**

In J-series routers, the log file location is **/cf/var/log/**

Command to view the logs: **user@my-device** > show log messages

The OS complies with **syslog severity level standards**



# Analyzing Router Logs: Juniper (Cont'd)

Juniper router logs include the following details:

1. Router name and ID
2. Status
3. Message
4. Date and Time



```
Junos log - Notepad
File Edit Format View Help
Nov 7 15:24:36 my-device smartd[4239]: atastandbyarmset: ioctl:
Inappropriate ioctl for device
Nov 7 15:24:36 my-device smartd[4239]: standby_request: Error:
atastandbyarmset(TRUE): Inappropriate ioctl for device
Nov 7 15:31:01 my-device xntpd[4364]: kernel time sync enabled 2001
Nov 7 16:07:10 my-device mib2d[4365]: SNMP_TRAP_LINK_DOWN: ifIndex 195,
ifAdminStatus up(1)
```



# Analyzing Firewall Logs

1



Firewalls are the **first entry points to a network** and store details of all the data packets moving in and out of a network

2



The network **firewall logs collect network traffic data** such as request source and destination, ports used, time and date, priority, etc.

3



These details will help investigators **correlate the data with other suspicious files** to find the source and other targets of an attack

4



Network firewalls come with management software that allow users to **monitor the logs**, control security settings and perform other maintenance tasks over the firewall

5



Investigators need to analyze the logs carefully based on the **timings and suspicious IP addresses**

6



Check for the **application generated requests**, DNS queries, suspicious IP addresses and URLs



# Analyzing Firewall Logs: Cisco

- Cisco Firewall uses mnemonics as identifiers to represent severity of any event

Mnemonic	Severity	Description
4000nn	4	IPS:number string from IP_address to IP_address on interface interface_name
106001	2	Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
106002	2	protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
106006	2	Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name
106007	2	Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response   Query}
106010	3	Deny inbound protocol src interface_name:dest_address/dest_port dst
106012	3	Deny IP from IP_address to IP_address, IP options hex
106013	3	Dropping echo request from IP_address to PAT address IP_address
106014	3	Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
106015	6	Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
106016	2	Deny IP spoof from (IP_address) to IP_address on interface interface_name.
106017	2	Deny IP due to Land Attack from IP_address to IP_address
106018	2	ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
106020	2	Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
106021	1	Deny protocol reverse path check from source_address to dest_address on interface interface_name
106022	1	Deny protocol connection spoof from source_address to dest_address on interface interface_name
106023	4	Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID
106100	4	access-list acl_ID {permitted   denied   est-allowed} protocol interface_name/source_address(source_port) -> interface_name/dest_address(dest_port) hit-cnt number ({first hit   number-second interval})
710003	3	{TCP   UDP} access denied by ACL from source_IP/source_port to interface_name:dest_IP/service



# Analyzing Firewall Logs: Cisco (Cont'd)

Cisco firewall logs include the following details:

1. Date and Time
2. Mnemonic message
3. Firewall Action
4. Source IP address and port
5. Destination IP address and port
6. Type of request














```
Feb 24 2016 09:14:54: %ASA-6-106100: access-list OUTSIDE denied tcp outside/192.168.208.63 (38807) -> inside/192.168.150.77(80) hit-cnt 1 first hit [0x22e8ac21, 0x0]
Feb 24 2016 09:16:14: %ASA-6-106015: Deny TCP (no connection) from 192.168.150.65/2278 to 64.101.128.83/80 flags RST on interface inside
Feb 24 2016 09:16:41: %ASA-4-106023: Deny icmp src outside:192.168.208.63 dst inside:192.168.150.77 (type 8, code 0) by access-group "OUTSIDE" [0xd3f63b90, 0x0]
Feb 24 2016 09:16:41: %ASA-6-106100: access-list OUTSIDE denied tcp outside/192.168.208.63 (38664) -> inside/192.168.150.77(80) hit-cnt 1 first hit [0x22e8ac21, 0x0]
Feb 24 2016 09:16:43: %ASA-4-106023: Deny icmp src outside:192.168.208.63 dst inside:192.168.150.77 (type 8, code 0) by access-group "OUTSIDE" [0xd3f63b90, 0x0]
Feb 24 2016 09:16:43: %ASA-6-106100: access-list OUTSIDE denied tcp outside/192.168.208.63 (38665) -> inside/192.168.150.77(80) hit-cnt 1 first hit [0x22e8ac21, 0x0]
Feb 24 2016 09:17:32: %ASA-1-106021: Deny ICMP reverse path check from 192.168.150.60 to 192.168.2.1 on interface outside
```



# Analyzing Firewall Logs:

## Checkpoint

- Checkpoint Firewall logs **can be viewed through a Check Point Log viewer** that uses icons and colors in the log table to represent different security events and their severity
- Red** represents the **connection attempts blocked by firewall** in accordance with the security policy or user-defined rules
- Orange** signifies **traffic detected** as suspicious, but accepted by the firewall
- Green** color is for the **traffic accepted by the firewall**
- Icons used in checkpoint logs include:

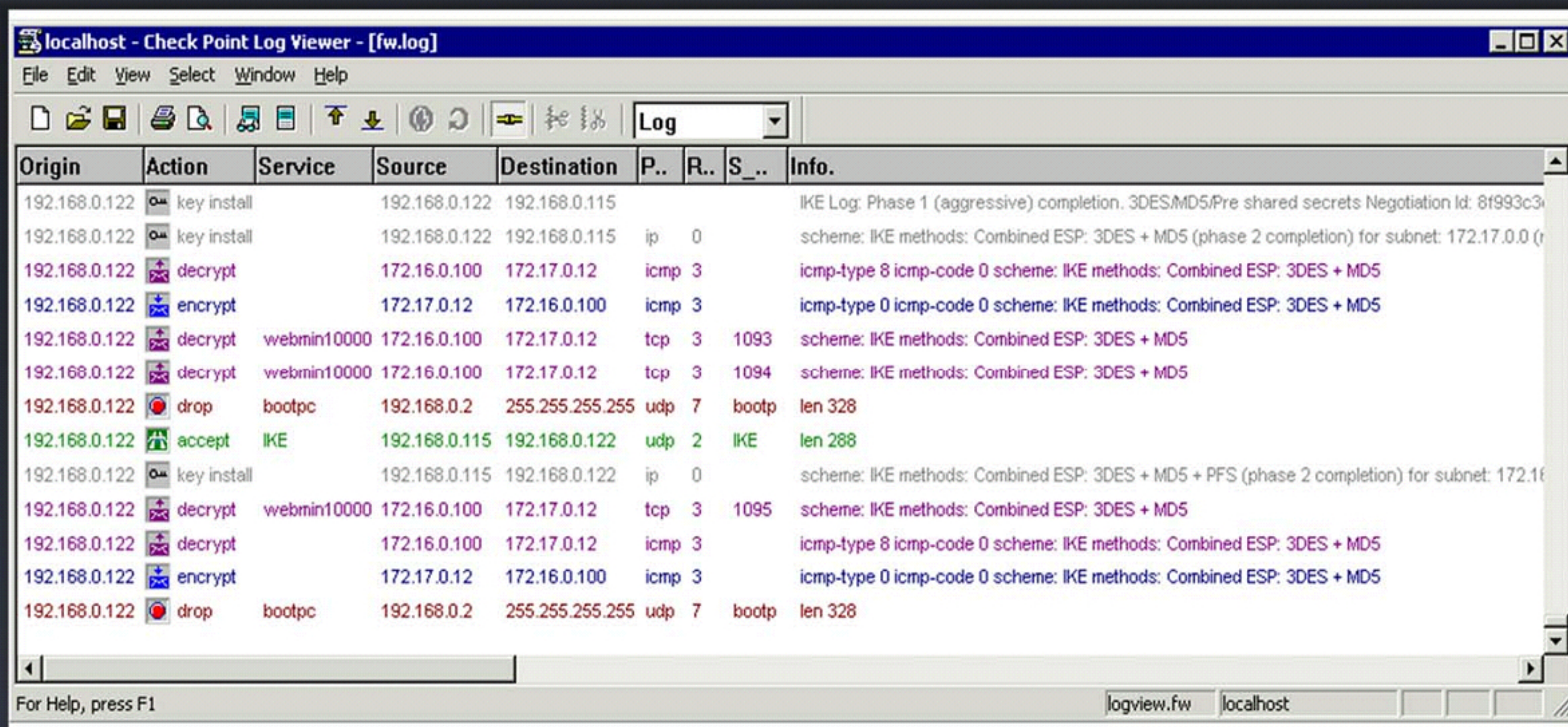
Action	Icon	Description
Connection Accepted		The firewall accepted a connection
Connection Decrypted		The firewall decrypted a connection
Connection Dropped		The firewall dropped a connection
Connection Encrypted		The firewall encrypted a connection
Connection Rejected		The firewall rejected a connection
Connection Monitored		A security event was monitored; however, it was not blocked, due to the current configuration
URL Allowed		The firewall allowed a URL
URL Filtered		The firewall blocked a URL
Virus Detected		A virus was detected in an email
Potential Spam Stamped		An email was marked as potential spam
Potential Spam Detected		An email was rejected as potential spam
Mail Allowed		A non-spam email was logged
Blocked by VStream Antivirus		VStream Antivirus blocked a connection



# Analyzing Firewall Logs: Checkpoint (Cont'd)

01

Checkpoint firewall log when viewed through Check Point Log viewer displays the result as follows



The screenshot shows the 'localhost - Check Point Log Viewer - [fw.log]' window. It features a menu bar (File, Edit, View, Select, Window, Help) and a toolbar with various icons. A dropdown menu is set to 'Log'. The main area displays a table of log entries with columns: Origin, Action, Service, Source, Destination, P., R., S., and Info. The entries include IKE phase 1 completion, ICMP exchanges, webmin10000 decryption, and bootpc drops. The status bar at the bottom indicates 'For Help, press F1' and shows the active file 'logview.fw' on 'localhost'.

Origin	Action	Service	Source	Destination	P..	R..	S_..	Info.
192.168.0.122	key install		192.168.0.122	192.168.0.115				IKE Log: Phase 1 (aggressive) completion. 3DES/MD5/Pre shared secrets Negotiation Id: 8f993c3...
192.168.0.122	key install		192.168.0.122	192.168.0.115	ip	0		scheme: IKE methods: Combined ESP: 3DES + MD5 (phase 2 completion) for subnet: 172.17.0.0 (r...
192.168.0.122	decrypt		172.16.0.100	172.17.0.12	icmp	3		icmp-type 8 icmp-code 0 scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	encrypt		172.17.0.12	172.16.0.100	icmp	3		icmp-type 0 icmp-code 0 scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	decrypt	webmin10000	172.16.0.100	172.17.0.12	tcp	3	1093	scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	decrypt	webmin10000	172.16.0.100	172.17.0.12	tcp	3	1094	scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	drop	bootpc	192.168.0.2	255.255.255.255	udp	7	bootp	len 328
192.168.0.122	accept	IKE	192.168.0.115	192.168.0.122	udp	2	IKE	len 288
192.168.0.122	key install		192.168.0.115	192.168.0.122	ip	0		scheme: IKE methods: Combined ESP: 3DES + MD5 + PFS (phase 2 completion) for subnet: 172.16...
192.168.0.122	decrypt	webmin10000	172.16.0.100	172.17.0.12	tcp	3	1095	scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	decrypt		172.16.0.100	172.17.0.12	icmp	3		icmp-type 8 icmp-code 0 scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	encrypt		172.17.0.12	172.16.0.100	icmp	3		icmp-type 0 icmp-code 0 scheme: IKE methods: Combined ESP: 3DES + MD5
192.168.0.122	drop	bootpc	192.168.0.2	255.255.255.255	udp	7	bootp	len 328



# Analyzing IDS Logs

- IDS Logs provide information helpful in finding **suspicious packet** types, determining the probes, generating new attack signatures and measuring attack statistics
- Most common **IDS devices** include **Juniper** and **Checkpoint**
- General indicators** of intrusion:

Requests targeted towards known vulnerabilities



Repeated unusual network activity

Failure to comply with protocols and syntaxes



Address anomalies in traffic

Unexpected elements such as date, time, system resources, etc.



Occurrence of mistyped command



# Analyzing IDS Logs: Juniper

- Juniper IDS comes with in-built Network and Security Manager (NSM), which stores event logs
- Users need the NSM log viewer to view and analyze the logs
- Juniper IDS stores logs with the information mentioned in the table



Column	Description
Log ID	Unique ID for the log entry, derived by combining the date and log number.
Time Received	Date and time that the management system received the log entry.
Alert	NSM-defined alert for this type of log entry. Configure alerts in policy rules.
User Flag	To set a flag, right-click the log row, select Flag, and then select one of the following flags from high, medium, low, closed, false positive, assigned, investigate, follow-up, pending
Src Addr	Source IP address of the packet that generated the log entry.
Dst Addr	Destination IP address of the packet that generated the log entry.
Action	Action the security device performed on the packet/connection that generated this log entry: <ul style="list-style-type: none"><li>•Accepted–Did not block the packet.</li><li>•Closed Client–Closed the connection and sent an RST packet to the client, but did neither to the server.</li><li>•Closed Server–Closed the connection and sent an RST packet to the server, but did neither to the client.</li><li>•Closed–Closed the connection and sent an RST packet to both the client and the server.</li><li>•Dropped–Dropped the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination.</li><li>•Dropped Packet–Dropped a matching packet before it could reach its destination but did not close the connection.</li><li>•Ignored–Matched the attack, did not take action, and ignored the remainder of the connection.</li></ul>
Protocol	Protocol that the packet that generated the log entry used.
Dst Port	Destination port of the packet that generated the log entry.



# Analyzing IDS Logs: Juniper (Cont'd)

Rule #	Security policy rule that generated the log entry.
Nat Src Addr	NAT source address of the packet that generated the log entry.
Nat Dst Addr	NAT destination address of the packet that generated the log entry.
Details	Miscellaneous string associated with log entry.
Category	<p>Type of log entry:</p> <ul style="list-style-type: none"><li>•Admin</li><li>•Alarm—The device generates event alarms for any security event that has a predefined severity level of emergency, critical, or alert. Additionally, the device generates traffic alarm log entries when it detects network traffic that exceeds the specified alarm threshold in a rule (the traffic alarm log entry describes the security event that triggered the alarm).</li><li>•Config—A configuration change occurred on the device.</li><li>•Custom—A match with a custom attack object was detected.</li><li>•Implicit—An implicit rule was matched.</li><li>•Info—General system information.</li><li>•Predefined—A match with a predefined attack object was detected.</li><li>•Profiler—Traffic matches a Profiler alert setting.</li><li>•Screen—Not applicable for IDP Series devices. Generated by ScreenOS firewall devices.</li><li>•Self—The device generated this log for a non-traffic related reason.</li><li>•Sensor.</li><li>•Traffic—Traffic matches a rule you have configured for harmless traffic.</li><li>•URL Filtering—Not applicable for IDP Series devices. Generated by ScreenOS firewall devices.</li><li>•User.</li></ul>
Subcategory	Category-specific type of log entry (examples are "Reboot" or message ID).



# Analyzing IDS Logs: Juniper (Cont'd)

Severity	Severity rating associated (if any) with this type of log entry: <ul style="list-style-type: none"><li>•Not Set (the device could not determine a severity for this log entry)</li><li>•Info</li><li>•Device_warning_log</li><li>•Minor and Major</li><li>•Device_critical_log</li><li>•Emergency</li><li>•Error</li><li>•Notice</li><li>•Informational</li><li>•Debug</li></ul>
Device	Device that generated this log entry.
Comment	User-defined comment about the log entry.
Application Name	Application associated with the current log.
Bytes In	For sessions, specifies the number of inbound bytes.
Bytes Out	For sessions, specifies the number of outbound bytes.
Bytes Total	For sessions, specifies the combined number of inbound and outbound bytes.
Dev Domain Ver	Domain version that generated this log entry.
Device Domain	Domain for the device that generated this log entry.



# Analyzing IDS Logs: Juniper (Cont'd)

Device family	Family of the device that generated this log entry.
Dst Intf	Name of the outbound interface of the packet that generated this log entry.
Dst Zone	Destination zone associated with a traffic log entry.
Elapsed Secs	For sessions, specifies how long the session lasted.
Has Packet Data	Indicates whether the log entry has associated packet data.
NAT Dst Port	The NAT destination port of the packet that generated the log entry.
NAT Src Port	The NAT source port of the packet that generated the log entry.
Packets In	For sessions, specifies the number of inbound packets.
Packets Out	For sessions, specifies the number of outbound packets.
Packets Total	For sessions, specifies the combined number of inbound and outbound packets.
Policy	Security policy that generated the log entry.
Roles	Role group associated with this log entry.
Rule Domain	The domain of the rule that generated the log entry.



# Analyzing IDS Logs: Juniper (Cont'd)

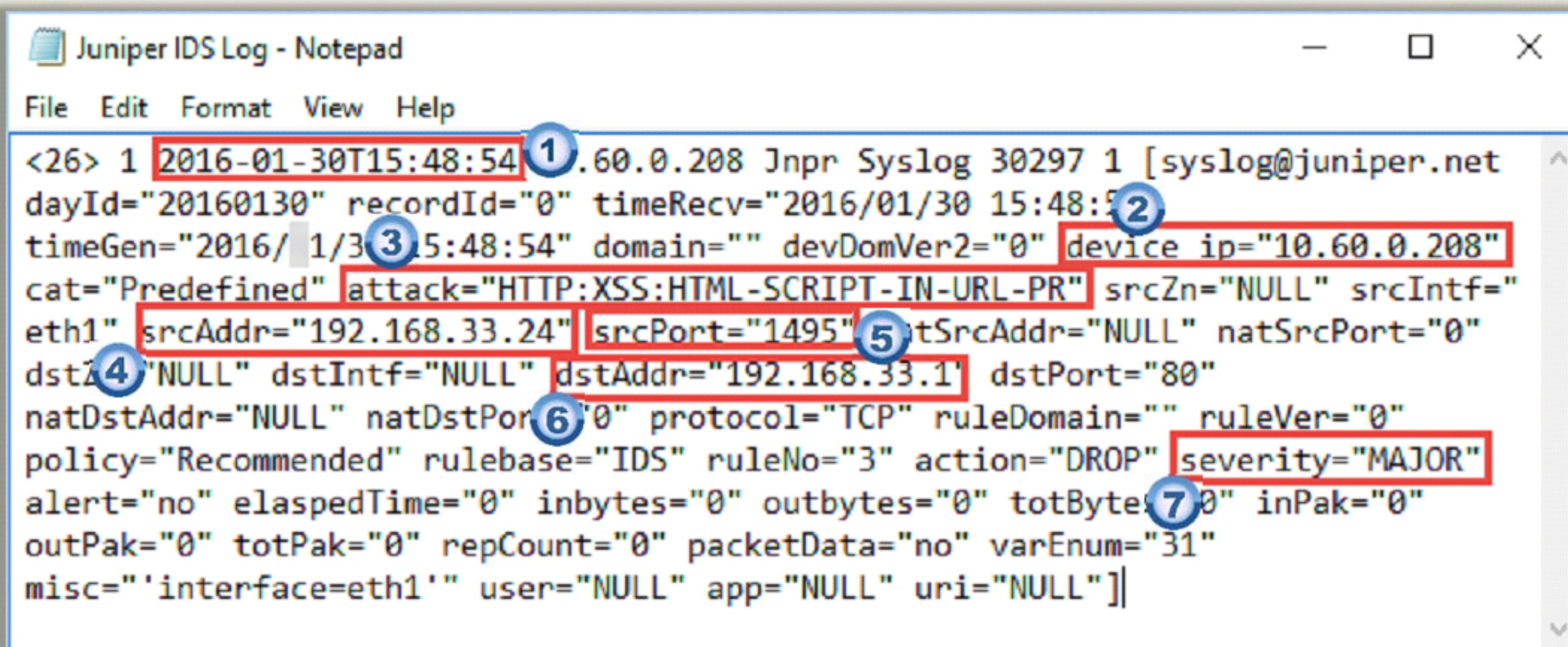
Rule Domain Ver	The domain version of the rule that generated the log entry.
Rulebase	Security policy rulebase that generated the log entry.
Src Intf	Name of the inbound interface of the packet that generated this log entry.
Src Port	Source port of the packet that generated the log entry.
Src Zone	Source zone associated with a traffic log entry.
Time Generated	Date and time the device generated the log entry.
User	User associated with this log entry.



# Analyzing IDS Logs: Juniper (Cont'd)

Details provided by the IDS in logs include:

1. Date and Time
2. Device IP address
3. Attack type
4. Source Address
5. Source Port
6. Destination Address
7. Severity of the attack

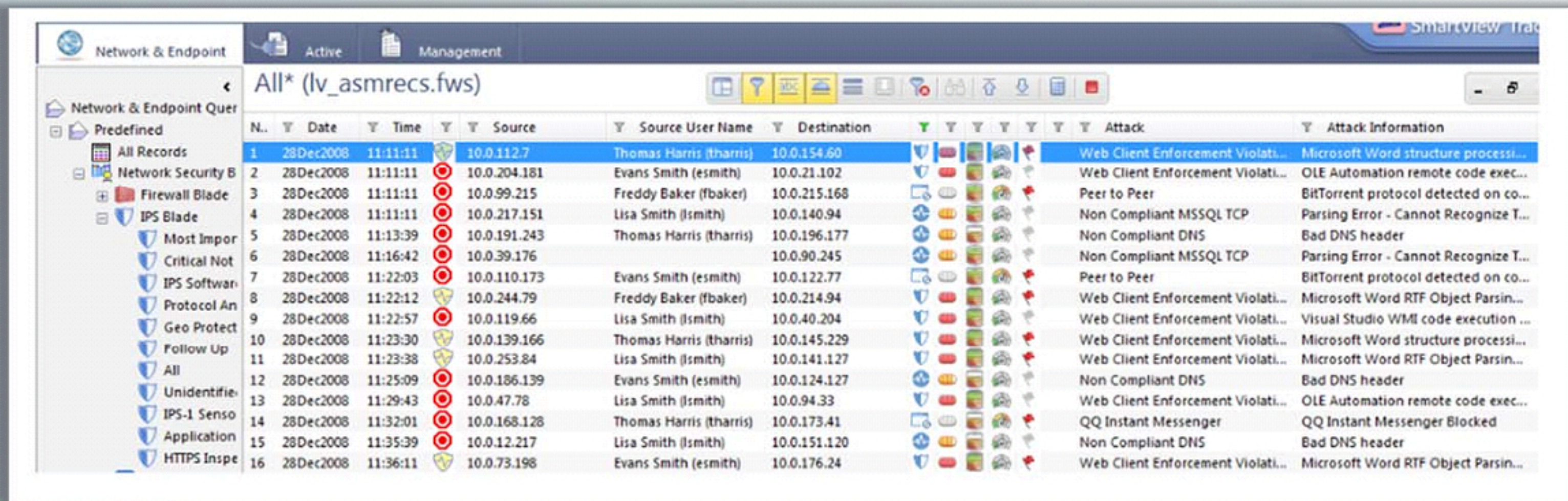


```
<26> 1 2016-01-30T15:48:54 10.60.0.208 Jnpr Syslog 30297 1 [syslog@juniper.net
dayId="20160130" recordId="0" timeRecv="2016/01/30 15:48:54"
timeGen="2016/01/30 15:48:54" domain="" devDomVer2="0" device ip="10.60.0.208"
cat="Predefined" attack="HTTP:XSS:HTML-SCRIPT-IN-URL-PR" srcZn="NULL" srcIntf="
eth1" srcAddr="192.168.33.24" srcPort="1495" dstSrcAddr="NULL" natSrcPort="0"
dst 4 "NULL" dstIntf="NULL" dstAddr="192.168.33.1" dstPort="80"
natDstAddr="NULL" natDstPort 6 "0" protocol="TCP" ruleDomain="" ruleVer="0"
policy="Recommended" rulebase="IDS" ruleNo="3" action="DROP" severity="MAJOR"
alert="no" elapsedTime="0" inbytes="0" outbytes="0" totBytes 7 "0" inPak="0"
outPak="0" totPak="0" repCount="0" packetData="no" varEnum="31"
misc="'interface=eth1' user="NULL" app="NULL" uri="NULL"]
```



# Analyzing IDS Logs: Checkpoint

- Checkpoint IPS has an **in-built software** for managing the device
- Users can view and analyze the logs using this software
- Steps to view and access logs in **checkpoint IDS**:
  - Go to SmartDashboard, click **SmartConsole** → select **SmartView Tracker**
  - Select the **Network & Endpoint** tab, expand **Predefined** → **Network Security Blades** → **IPS Blade**
  - Double-click **All** to view the complete **log information**

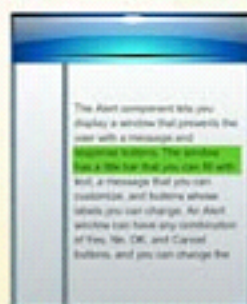


N.	Date	Time	Source	Source User Name	Destination	Attack	Attack Information
1	28Dec2008	11:11:11	10.0.112.7	Thomas Harris (tharris)	10.0.154.60	Web Client Enforcement Violati...	Microsoft Word structure processi...
2	28Dec2008	11:11:11	10.0.204.181	Evans Smith (esmith)	10.0.21.102	Web Client Enforcement Violati...	OLE Automation remote code exec...
3	28Dec2008	11:11:11	10.0.99.215	Freddy Baker (fbaker)	10.0.215.168	Peer to Peer	BitTorrent protocol detected on co...
4	28Dec2008	11:11:11	10.0.217.151	Lisa Smith (lsmith)	10.0.140.94	Non Compliant MSSQL TCP	Parsing Error - Cannot Recognize T...
5	28Dec2008	11:13:39	10.0.191.243	Thomas Harris (tharris)	10.0.196.177	Non Compliant DNS	Bad DNS header
6	28Dec2008	11:16:42	10.0.39.176		10.0.90.245	Non Compliant MSSQL TCP	Parsing Error - Cannot Recognize T...
7	28Dec2008	11:22:03	10.0.110.173	Evans Smith (esmith)	10.0.122.77	Peer to Peer	BitTorrent protocol detected on co...
8	28Dec2008	11:22:12	10.0.244.79	Freddy Baker (fbaker)	10.0.214.94	Web Client Enforcement Violati...	Microsoft Word RTF Object Parsin...
9	28Dec2008	11:22:57	10.0.119.66	Lisa Smith (lsmith)	10.0.40.204	Web Client Enforcement Violati...	Visual Studio WMI code execution ...
10	28Dec2008	11:23:30	10.0.139.166	Thomas Harris (tharris)	10.0.145.229	Web Client Enforcement Violati...	Microsoft Word structure processi...
11	28Dec2008	11:23:38	10.0.253.84	Lisa Smith (lsmith)	10.0.141.127	Web Client Enforcement Violati...	Microsoft Word RTF Object Parsin...
12	28Dec2008	11:25:09	10.0.186.139	Evans Smith (esmith)	10.0.124.127	Non Compliant DNS	Bad DNS header
13	28Dec2008	11:29:43	10.0.47.78	Lisa Smith (lsmith)	10.0.94.33	Web Client Enforcement Violati...	OLE Automation remote code exec...
14	28Dec2008	11:32:01	10.0.168.128	Thomas Harris (tharris)	10.0.173.41	QQ Instant Messenger	QQ Instant Messenger Blocked
15	28Dec2008	11:35:39	10.0.12.217	Lisa Smith (lsmith)	10.0.151.120	Non Compliant DNS	Bad DNS header
16	28Dec2008	11:36:11	10.0.73.198	Evans Smith (esmith)	10.0.176.24	Web Client Enforcement Violati...	Microsoft Word RTF Object Parsin...



# Analyzing IDS Logs: Checkpoint (Cont'd)

- Checkpoint IPS also provides details of each log
- To view the details of any log, go to the SmartView Tracker records list and double-click on the event



**Record Details**

Previous Next Copy Details

**Microsoft Outlook URI Vulnerability (MS08-015)**  
Web Client Enforcement Violation

Confidence Level: High  
Severity: Critical

Log Info	
Product	IPS Software Blade
Date	28Dec2008
Time	12:41:13
Number	1
Type	Log
Origin	R70

Traffic	
Source	10.0.15.232
Destination	10.0.216.39
Service	http (80)
Protocol	TCP tcp
Interface	eth0
Source Port	2112

General Event Information	
Action	Drop
Protection Name	Microsoft Outlook URI Vulnerability (MS08-015)
Attack	Web Client Enforcement Violation
Attack Information	Microsoft Outlook URI vulnerability detected (MS08-015)
CVE List	---
Severity	Critical
Confidence Level	High
Performance Impact	Low
Protection Type	Signature
Follow Up	Not Followed
<a href="#">Open Protection...</a> <a href="#">Add Exception...</a> <a href="#">Go To Advisory...</a>	

Policy	
Policy Name	---
Policy Date	---
Policy Management	---
IPS Profile	---

Attack Information	
Resource	---
Reject ID	---
Reason	---
<a href="#">More</a>	



# Analyzing Honeyypot Logs

01

Honeyypots are the devices that pretend to contain very useful information in order to lure attackers and find their whereabouts and techniques

02

Kippo is one of the most commonly used honeyypots

03

Logs stored in Kippo contain the following information:

1. Timestamp
2. Type of session
3. Session ID and Source IP address
4. Message with other details

```
Kippo honeypot Log - Notepad
File Edit Format View Help
2016-02-08 14:33:27+0100 [SSHChannel session (0)] SSHService ssh-
connection on HoneyPotTransport,0,192.168.122.1] request env: '\x00\
\x00\x00\x04LANG\x00\x00\x00\npl PL.utf8'
2016-02-08 14:33:27+0100 [SSHChannel session (0)] on SSHService ssh-
connection on HoneyPotTransport,0,192.168.122.1] getting shell
2016-02-08 14:33:27+0100 [SSHChannel session (0)] on SSHService ssh-
connection on HoneyPotTransport,0,192.168.122.1] Opening TTY log:
/var/log/kippo/log/tty/20160108-143327-9152.log
2016-02-08 14:33:33+0100 [SSHChannel session (0)] SSHService ssh-
connection on HoneyPotTransport,0,192.168.122.1] /etc/motd resolved
into /etc/motd
```



# DHCP Logging

The DHCP logs are saved in the **C:\Windows\System32\dhcp** folder on **DHCP servers**

## DHCP server log file format

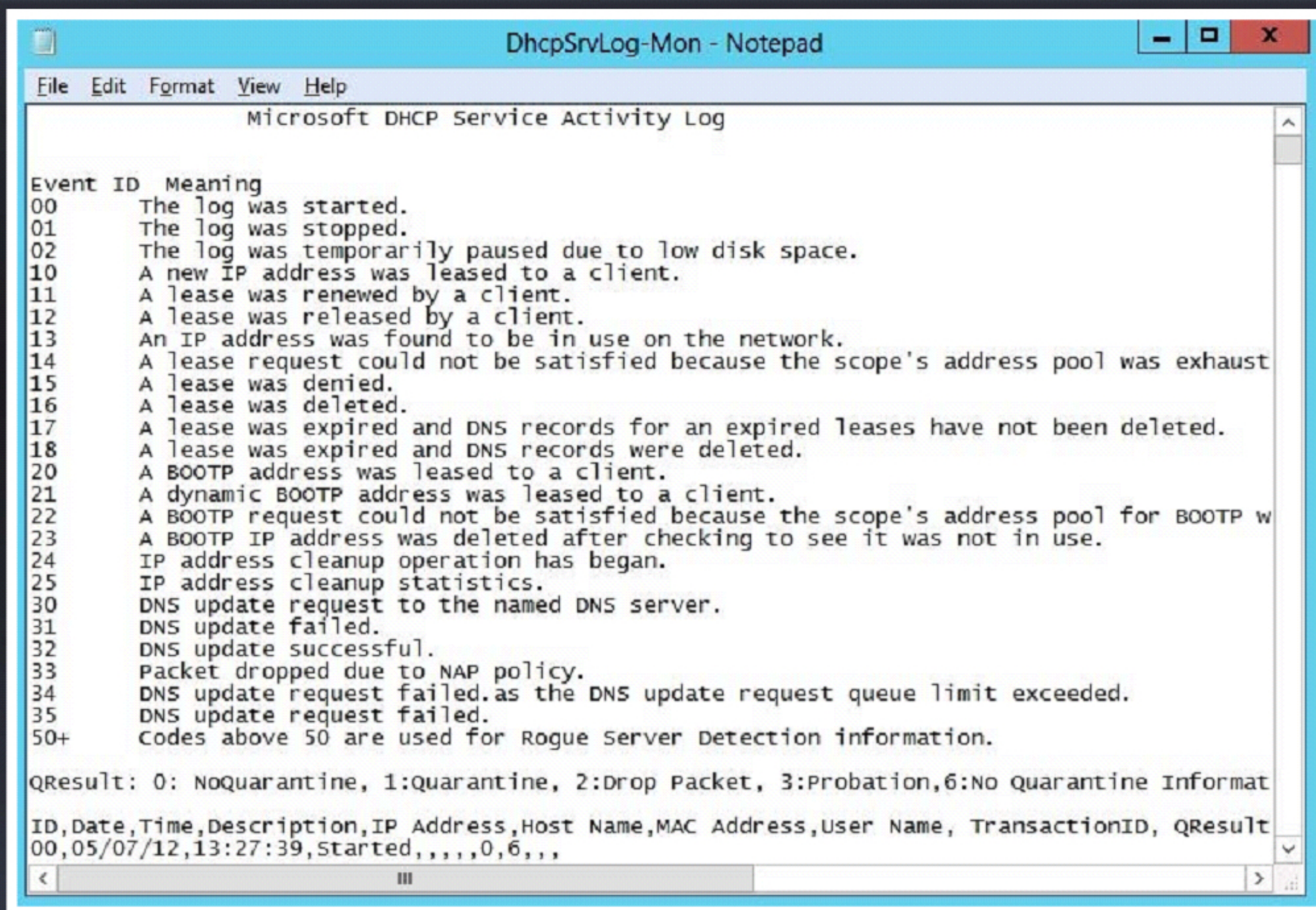
ID, Date, Time, Description, IP Address, Host Name, MAC Address



Field	Description
ID	A DHCP Event ID code
Date	The date on which this entry was logged on the DHCP server
Time	The time at which this entry was logged on the DHCP server
Description	A description of this DHCP server event
IP Address	The IP address of the DHCP client
Host Name	The host name of the DHCP client
MAC Address	The media access control (MAC) address used by the network adapter hardware of the client



# Sample DHCP Audit Log File



```
DhcpSrvLog-Mon - Notepad
File Edit Format View Help
Microsoft DHCP Service Activity Log

Event ID Meaning
00 The log was started.
01 The log was stopped.
02 The log was temporarily paused due to low disk space.
10 A new IP address was leased to a client.
11 A lease was renewed by a client.
12 A lease was released by a client.
13 An IP address was found to be in use on the network.
14 A lease request could not be satisfied because the scope's address pool was exhaust
15 A lease was denied.
16 A lease was deleted.
17 A lease was expired and DNS records for an expired leases have not been deleted.
18 A lease was expired and DNS records were deleted.
20 A BOOTP address was leased to a client.
21 A dynamic BOOTP address was leased to a client.
22 A BOOTP request could not be satisfied because the scope's address pool for BOOTP w
23 A BOOTP IP address was deleted after checking to see it was not in use.
24 IP address cleanup operation has began.
25 IP address cleanup statistics.
30 DNS update request to the named DNS server.
31 DNS update failed.
32 DNS update successful.
33 Packet dropped due to NAP policy.
34 DNS update request failed.as the DNS update request queue limit exceeded.
35 DNS update request failed.
50+ Codes above 50 are used for Rogue Server Detection information.

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation,6:No Quarantine Informat
ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name, TransactionID, QResult
00,05/07/12,13:27:39,Started,,,,,0,6,,,
```



# Evidence Gathering at the Data-Link Layer: **DHCP Database**

The **DHCP database** provides a means for determining the **MAC address** associated with the computer in custody

This database helps DHCP to conclude the MAC address in case DHCP is unable to maintain a **permanent log** of requests

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

The database can be queried by providing the time duration during which the given **IP address** accessed the server



# ODBC Logging

Open Database Connectivity (ODBC) logging **records a set of data fields in an ODBC-compliant database** like Microsoft Access or Microsoft SQL Server

With ODBS logging, the administrator must specify both the database to be logged, and **set up the database to receive the data**

Some of logged information includes the user's **IP address**, user name, request date and time, **HTTP status code**, bytes received, bytes sent, action carried out, and the **target file**

When ODBC logging is enabled, IIS disables the **HTTP.sys kernel-mode cache**. This is the reason, implementing ODBC logging can degrade overall server performance

Field Name	SQL Server Field Type	MS Access Field Type
ClientHost	varchar(255)	text(255)
Username	varchar(255)	text(255)
LogTime	date time	date time
Service	varchar(255)	text(255)
Machine	varchar(255)	text(255)
ServerIP	varchar(50)	text(50)
ProcessingTime	int	int
BytesRecvd	int	int
BytesSent	int	int
ServiceStatus	int	int
Win32Status	int	int
Operation	varchar(255)	text(255)
Target	varchar(255)	text(255)
Parameters	varchar(255)	text(255)



# Why Investigate **Network Traffic**?

Some of the reasons investigators analyze network traffic:

1

- To locate **suspicious network traffic**

2

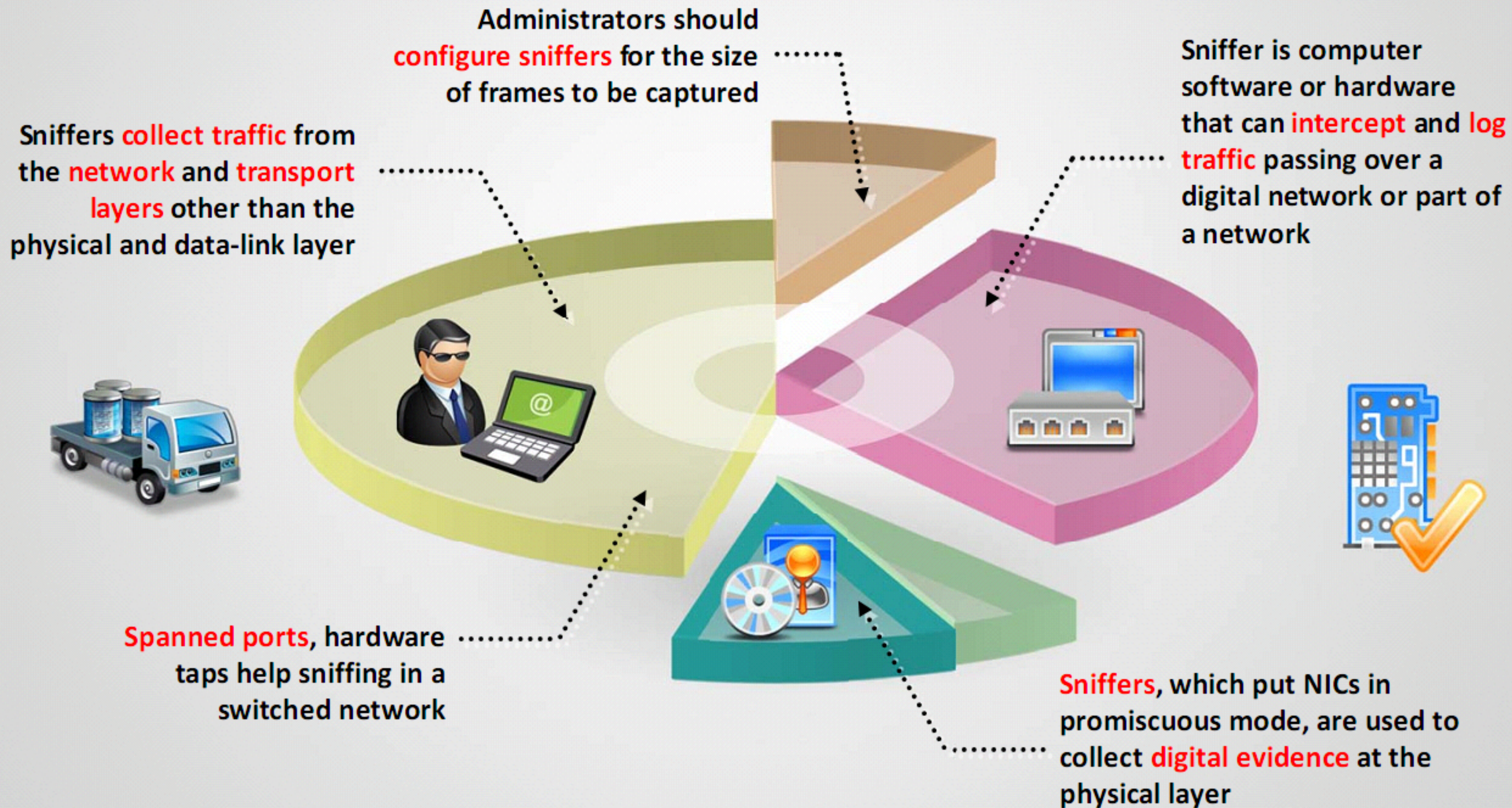
- To **know which network is generating the troublesome traffic** and where the traffic is being transmitted to or received from

3

- To **identify network problems**



# Evidence Gathering via Sniffing





# Sniffing Tool: **Wireshark**

It lets you **capture and interactively browse the traffic** running on a computer network

01

Wireshark uses **Winpcap** to capture packets, therefore, it can only capture the packets on the networks supported by Winpcap

02

It **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks

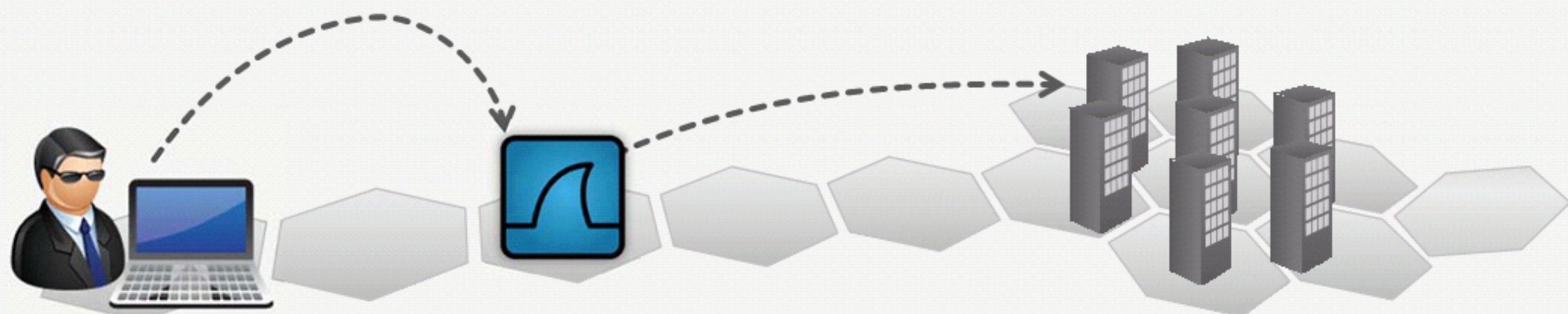
03

Captured files can be programmatically edited via **command-line**

04

A **set of filters** for customized data display can be refined using a display filter

05



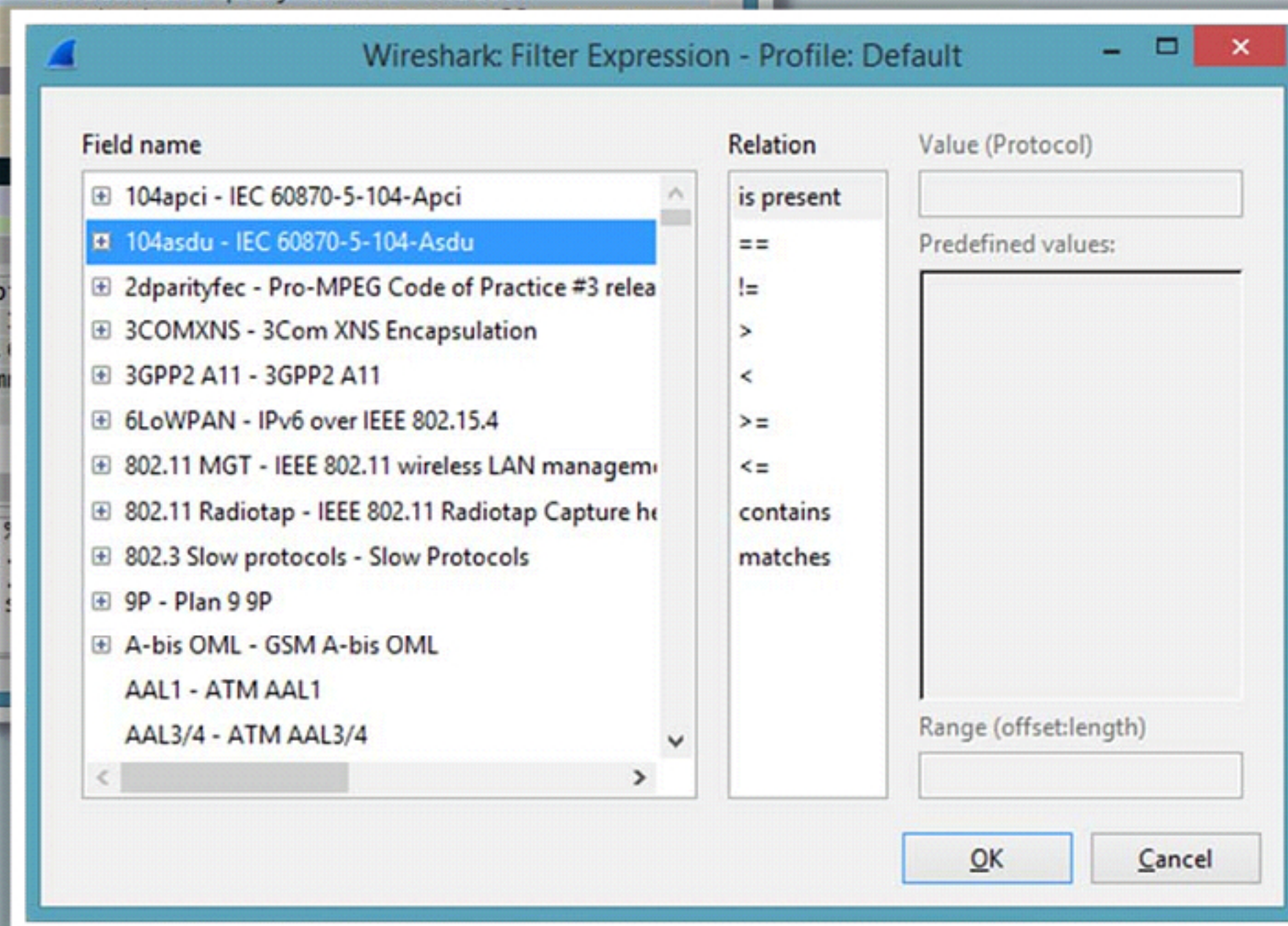
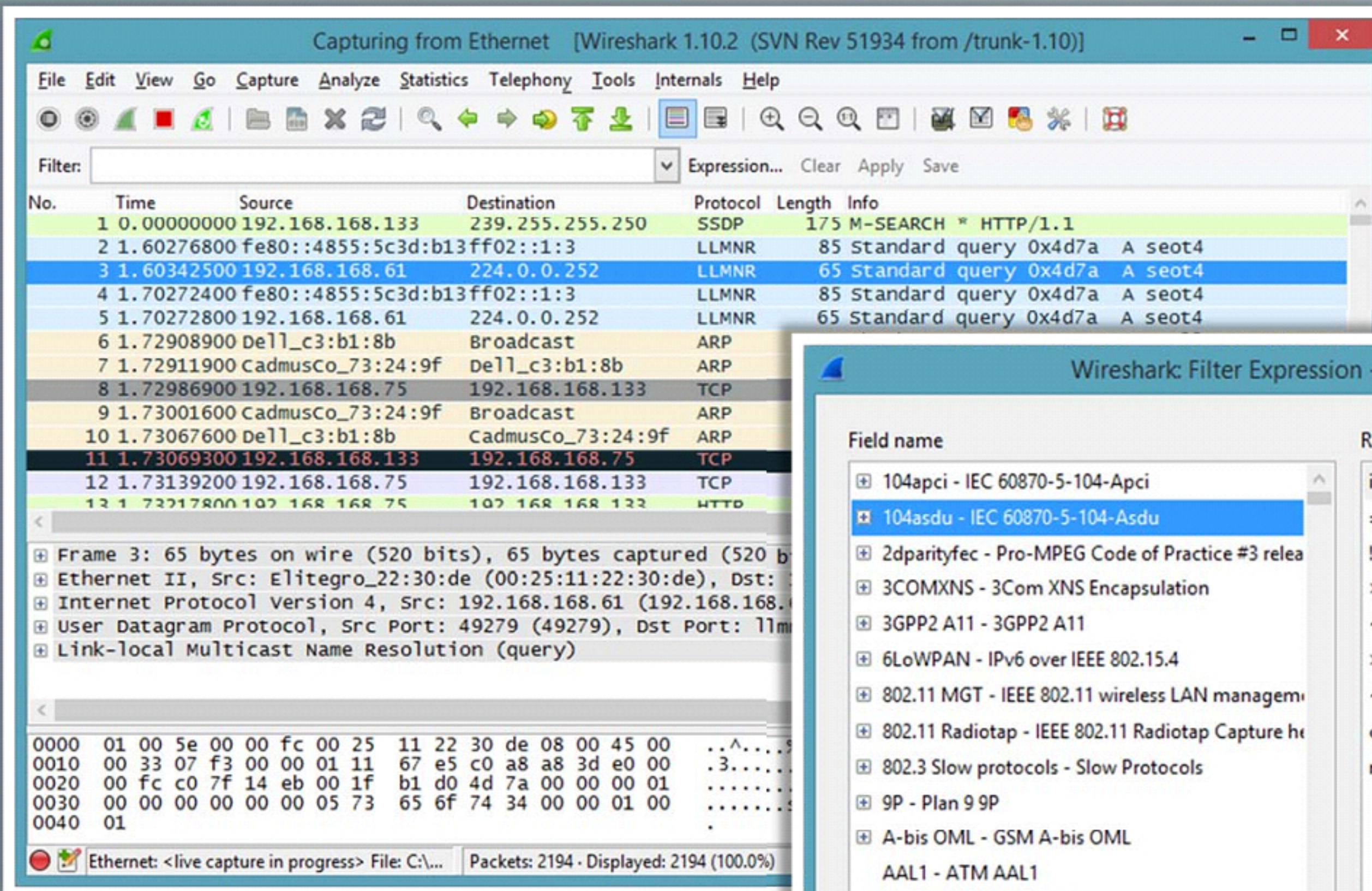
Network Administrator

Wireshark Tool

Network



# Sniffing Tool: Wireshark (Cont'd)



<http://www.wireshark.org>



# Display Filters in Wireshark

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

1

## Display Filtering by Protocol

E.g.: Type the protocol in the filter box;  
arp, http, tcp, udp, dns, ip



2

## Monitoring the Specific Ports

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

3

## Filtering by Multiple IP Addresses

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

4

## Filtering by IP Address

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

5

## 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`



# Additional Wireshark Filters

01

```
tcp.flags.reset==1
```

Displays all TCP resets



02

```
udp contains 33:27:58
```

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



03

```
http.request
```

Displays all HTTP GET requests



04

```
tcp.analysis.retransmission
```

Displays all retransmissions in the trace



05

```
tcp contains traffic
```

Displays all TCP packets that contain the word 'traffic'



06

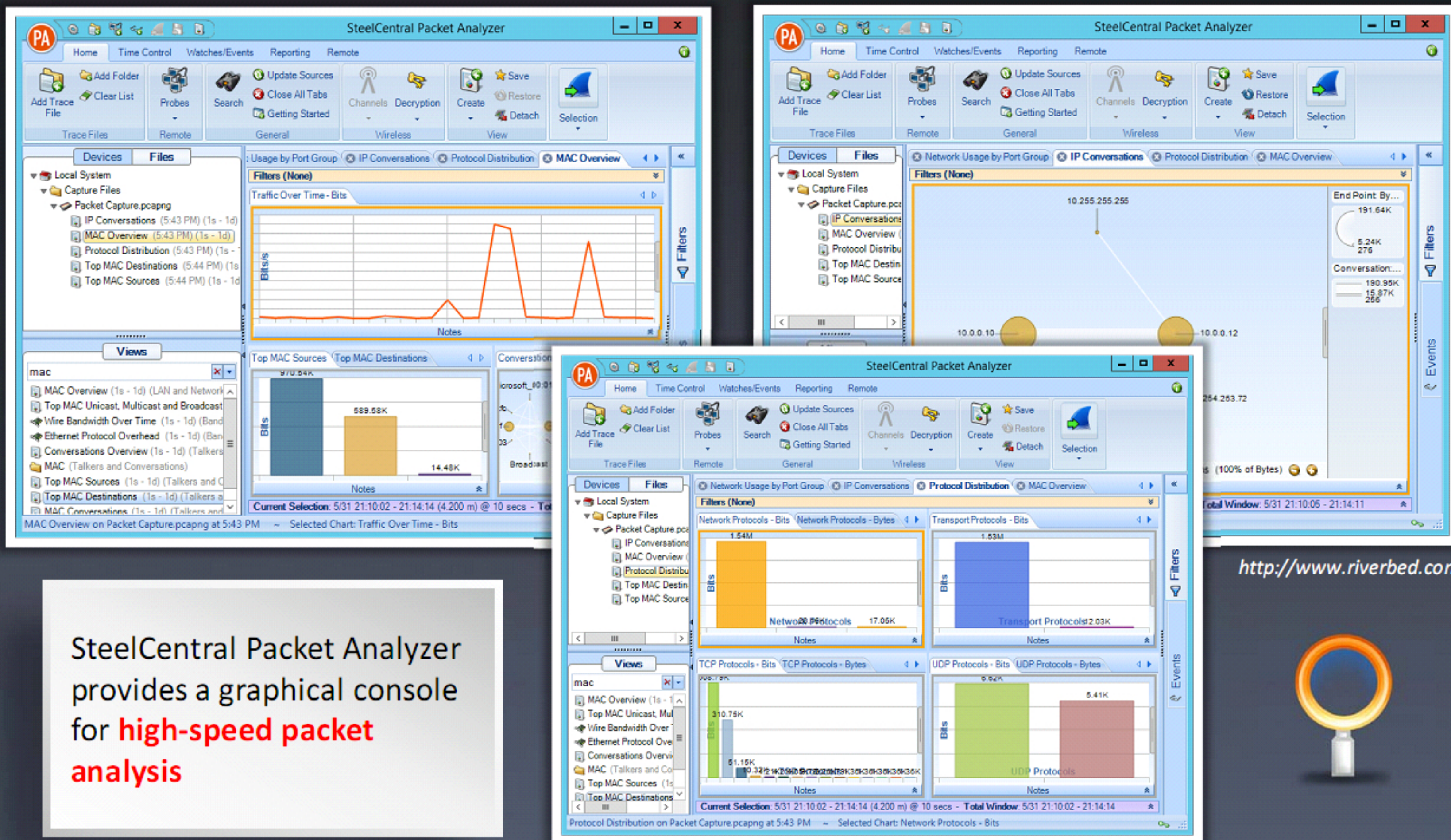
```
!(arp or icmp or dns)
```

Masks out arp, icmp, dns, or other protocols and allows you to view traffic of you interest





# Sniffing Tool: SteelCentral Packet Analyzer



SteelCentral Packet Analyzer provides a graphical console for **high-speed packet analysis**

<http://www.riverbed.com>





# Sniffing Tool: **Tcpdump/Windump**

TCPdump is a **command line interface packet sniffer** which runs on Linux and Windows



## TCPDump

Runs on Linux and UNIX systems

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -i eth0  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decoding  
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes  
05:17:26.804527 IP 192.168.0.134.netbios-ns > 192.168.0.255.netbios-ns:  
  NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST  
05:17:26.898597 IP 192.168.0.33.mdns > 224.0.0.251.mdns: 0 AAAA (QU)? ECC-iMac.local. (32)  
05:17:26.898601 IP6 fe80::3e07:54ff:fe57:9367.mdns > ff02::fb.mdns: 0 AAAA (QU)? ECC-iMac.local. (32)  
05:17:26.899415 IP 192.168.0.27.mdns > 224.0.0.251.mdns: 0*- [0q] 0/0/0 (12)  
05:17:26.899417 IP6 fe80::1828:de86:7fe2:77dc.mdns > ff02::fb.mdns: 0*- [0q] 0/0/0 (12)  
05:17:27.049655 ARP, Request who-has 192.168.0.8 tell kali, length 28  
05:17:27.070314 IP 192.168.0.33.mdns > 224.0.0.251.mdns: 0*- [0q] 1/0/2 (Cache flush) AAAA fe80::3e07:54ff:fe57:9367 (90)  
05:17:47.061653 ARP, Request who-has 192.168.0.8 tell kali, length 28  
05:18:06.879551 IP 192.168.0.189.netbios-ns > 192.168.0.255.netbios-ns:  
  NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST  
05:18:27.097654 ARP, Request who-has 192.168.0.8 tell kali, length 28  
05:18:36.865858 ARP, Request who-has 192.168.0.8 tell kali, length 28  
05:18:46.876451 ARP, Request who-has 192.168.0.8 tell kali, length 28
```

<http://www.tcpdump.org>

## WinDump

Runs on Windows systems

```
C:\Users\C\Desktop\WinDump\WinDump.exe  
C:\Users\C\Desktop\WinDump\WinDump.exe: listening on \Device\NPF_{C641A8-B883-...}A>  
15:10:35.004005 IP admin.137 > 192.168.168.255.137: UDP, length 46  
15:10:35.372362 IP6 WIN-F2JBJQ69T55.546 > ff02::1:2.547: dhcp6 soli  
15:10:35.669372 IP6 admin.50347 > ff02::1:3.5355: UDP, length 46  
15:10:35.669718 IP admin.50347 > 224.0.0.252.5355: UDP, length 46  
15:10:35.854857 IP6 admin.137 > ff02::1:3.5355: UDP, length 23  
15:10:35.855677 IP6 admin.63168 > 224.0.0.252.5355: UDP, length 23  
15:10:35.954878 IP6 admin.61220 > ff02::1:3.5355: UDP, length 23  
15:10:35.955385 IP6 admin.63168 > 224.0.0.252.5355: UDP, length 23  
15:10:36.082704 IP6 admin.50347 > ff02::1:3.5355: UDP, length 46  
15:10:36.083064 IP admin.50347 > 224.0.0.252.5355: UDP, length 46  
15:10:36.154879 IP6 admin.137 > 192.168.168.255.137: UDP, length 46  
15:10:36.459859 IP6 admin.137 > 192.168.168.255.137: UDP, length 50  
15:10:36.494136 IP admin.137 > 192.168.168.255.137: UDP, length 50  
15:10:36.494641 IP6 admin.64799 > ff02::1:3.5355: UDP, length 45  
15:10:36.494898 IP admin.64799 > 224.0.0.252.5355: UDP, length 45  
15:10:36.495848 IP6 admin.137 > admin.137: UDP, length 175  
15:10:36.496685 IP6 admin.5355 > admin.64799: UDP, length 94  
15:10:36.496743 IP admin. > : ICMP admin udp port 64799 unreth 130  
15:10:36.497512 IP6 admin.49395 > ff02::1:3.5355: UDP, length 90  
15:10:36.497750 IP admin.49395 > 224.0.0.252.5355: UDP, length 90  
15:10:36.904606 IP6 admin.137 > 192.168.168.255.137: UDP, length 90  
15:10:36.908276 IP6 admin.49395 > ff02::1:3.5355: UDP, length 90  
15:10:36.908503 IP admin.49395 > 224.0.0.252.5355: UDP, length 90  
15:10:37.210104 IP6 admin. > 192.168.168.255.137: UDP, length 90  
15:10:37.252106 IP
```

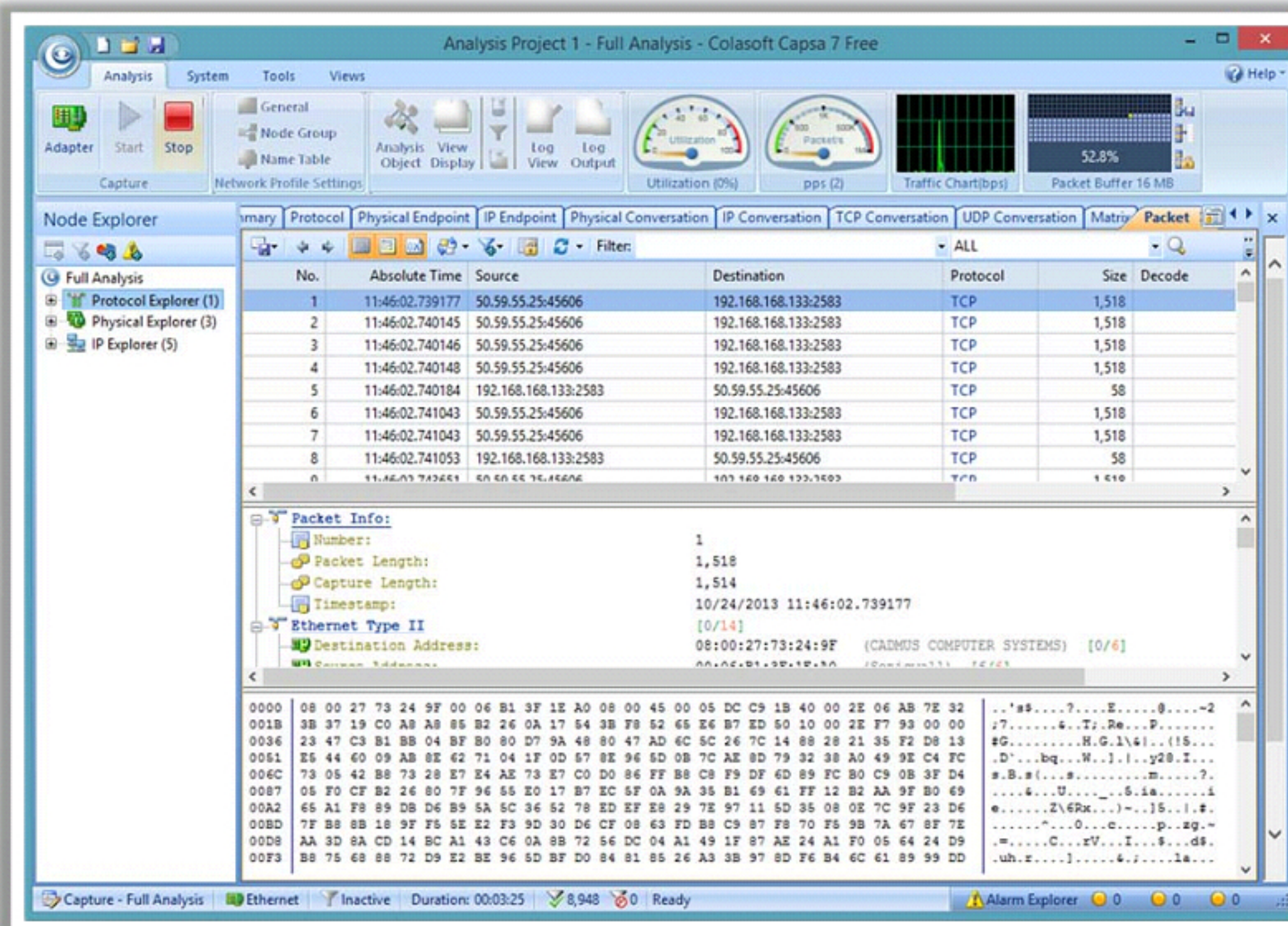
<http://www.winpcap.org>



# Packet Sniffing Tool: 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 graphical way

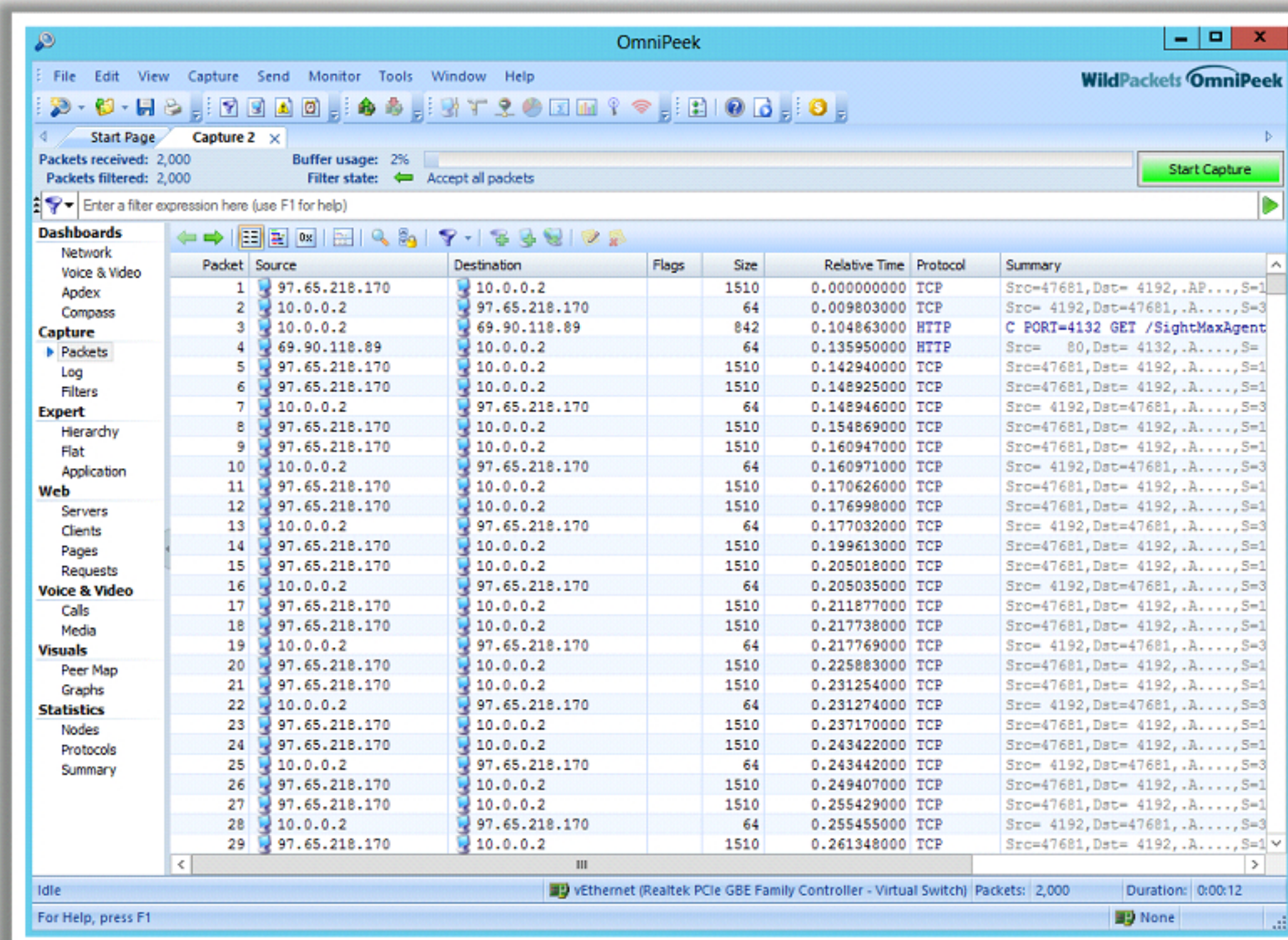


<http://www.colasoft.com>



# Network Packet Analyzer: OmniPeek Network Analyzer

- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the **locations of all the public IP addresses of captured packets**
- This feature is a great way to monitor the network in real time, and track that **traffic**

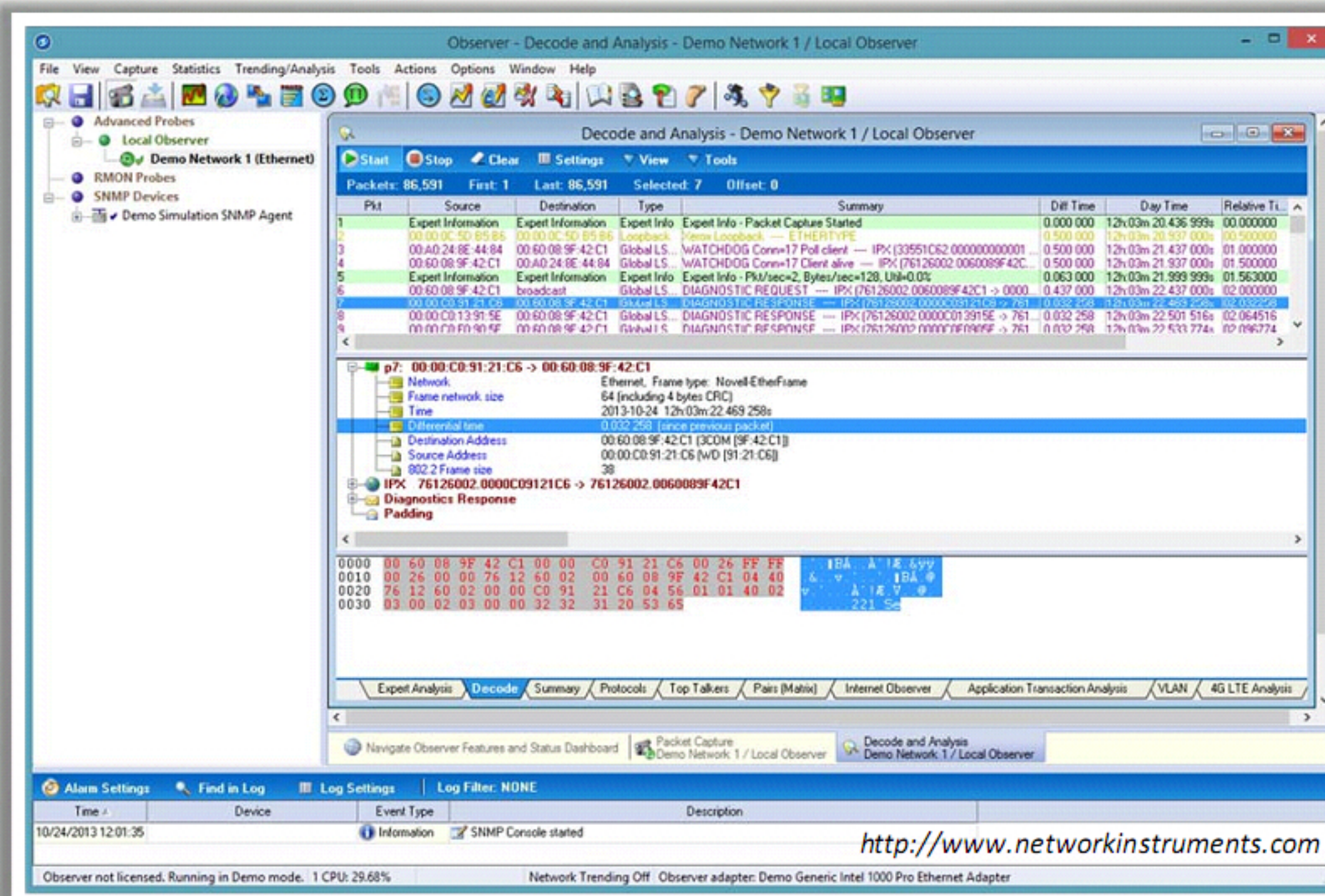


<http://www.wildpackets.com>



# Network Packet Analyzer: Observer

Observer provides a comprehensive drill-down into network traffic and provides **back-in-time analysis**, reporting, trending, alarms, application tools, and **route monitoring capabilities**



<http://www.networkinstruments.com>



# TCP/IP Packet Crafter: Colasoft Packet Builder

Colasoft Packet Builder allows user to select one from the provided templates: **Ethernet Packet**, **ARP Packet**, **IP Packet**, **TCP Packet** and **UDP Packet**, and **change the parameters** in the decoder editor, hexadecimal editor, or ASCII editor to create a packet

Colasoft Packet Builder

File Edit Send Help

Import Export Add Insert Copy Paste Delete Move Up Move Down Checksum Send Send All Adapter About

Decode Editor Packet No. 1

Packet Info:

- Packet Number: 000001
- Packet Length: 64
- Captured Length: 60
- Delta Time: 0.100000 Second

Ethernet Type II [0/14]

- Destination Address: FF:FF:FF:FF:FF:FF
- Source Address: 00:00:00:00:00:00
- Protocol: 0x0806

ARP - Address Resolution Protocol [14/28]

- Hardware type: 1
- Protocol Type: 0x0800
- Hardware Address Length: 6
- Protocol Address Length: 4
- Type: 1
- Source Physics: 00:00:00:00:00:00

Packet List

No.	Delta Time	Source	Destination
1	0.100000	00:00:00:00:00:00	FF:FF:FF:FF:FF:FF
2	0.100000	0.0.0.0	0.0.0.0
3	0.100000	0.0.0.0:0	0.0.0.0:0
4	0.100000	0.0.0.0:0	0.0.0.0:0

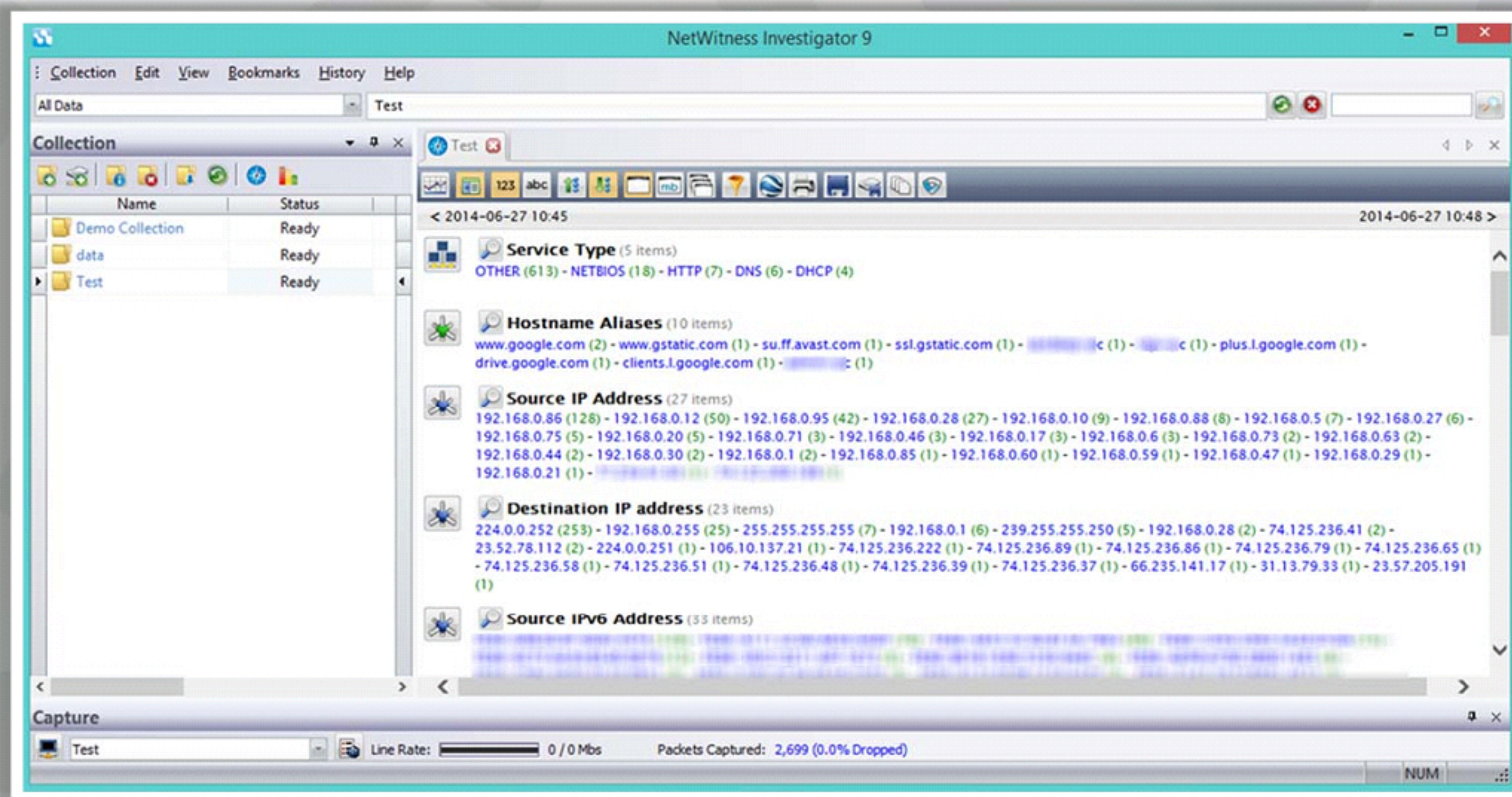
Hex Editor Total 60 bytes

Address	Hex	ASCII
0000	FF FF FF FF FF 00 00 00 00 00 00	.....
000C	08 06 00 01 08 00 06 04 00 01 00 00	.....
0018	00 00 00 00 00 00 00 00 00 00 00 00	.....
0024	00 00 00 00 00 00 00 00 00 00 00 00	.....
0030	00 00 00 00 00 00 00 00 00 00 00 00	.....



# Network Packet Analyzer: RSA NetWitness Investigator

RSA NetWitness Investigator captures live traffic and process packet files from virtually any existing network collection devices



<http://www.emc.com>



# Additional Sniffing Tools



## Ace Password Sniffer

<http://www.efeotech.com>



## EffeTech HTTP Sniffer

<http://www.efeotech.com>



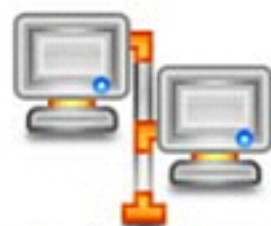
## IPgrab

<http://ipgrab.sourceforge.net>



## ntopng

<http://www.ntop.org>



## Big Mother

<http://www.tupsoft.com>



## Ettercap

<http://ettercap.sourceforge.net>



## EtherDetect Packet Sniffer

<http://www.etherdetect.com>



## SmartSniff

<http://www.nirsoft.net>



## dsniff

<https://www.monkey.org>



## EtherApe

<http://etherape.sourceforge.net>



# Additional Sniffing Tools (Cont'd)



## Network Probe

<http://www.objectplanet.com>



## CommView

<http://www.tamos.com>



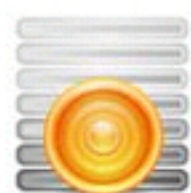
## WebSiteSniffer

<http://www.nirsoft.net>



## NetResident

<http://www.tamos.com>



## ICQ Sniffer

<http://www.etherboss.com>



## Kismet

<http://www.kismetwireless.net>



## MaaTec Network Analyzer

<http://www.maatec.com>



## AIM Sniffer

<http://www.fffetech.com>



## Alchemy Eye

<http://www.alchemy-lab.com>



## NetworkMiner

<http://www.netresec.com>



# Gathering Evidence from an IDS

An administrator can configure an IDS to **capture network traffic when an alert is generated**

However, this **data is not a sufficient source of evidence** because integrity checks cannot be performed on the log files

In a network investigation, preserving digital evidence is difficult, as data is **displayed on-screen for a few seconds**

Investigators can **record examination results** from networking devices such as routers, switches, and firewalls through a serial cable and software such as the Windows HyperTerminal program or a script on UNIX

If the amount of information to be captured is large, an investigator can **record the on-screen event** using a video camera or a related software program

The **disadvantage** of this method is that there is **no integrity check**, making it difficult to authenticate the information



# Documenting the Evidence Gathered on a Network



Documenting the evidence gathered on a network is easy if the **network logs** are small, as a **printout** can be taken and attested



Documenting **digital evidence** on a network becomes more complex when the evidence is gathered from systems located **remotely**, because of the unavailability of **date** and **time stamps** of the related files



If the evidence resides on a **remote computer**, detailed information about collection and location should be **documented**. The investigator should specify the **server** containing the data to avoid confusion



For documentation and integrity of the document, it is advisable to follow a **standard methodology**



To support the **chain of custody**, the investigator should print out **screenshots** of important items and attach a record of actions taken during the **collection process**



# Evidence Reconstruction for Investigation

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

- Evidence is not static and 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**
- Once the evidence is gathered, it can be used to **reconstruct the crime** to produce a clearer picture of the crime and identify the missing links in the picture

## Fundamentals of reconstruction for investigating a crime:

### Temporal analysis

---

It produces a sequential event trail, which sheds light on important factors such as what happened and who was involved

### Relational analysis

---

It correlates the actions of suspect and victim

### Functional analysis

---

It provides a description of the possible conditions of a crime. It testifies to the events responsible for a crime in relation to their functionalities



# Module Summary

- ☐ Network forensics is the capturing, recording, and analyzing network traffic and event logs to discover the source of security attacks
- ☐ Network Addressing Schemes are of two types, LAN Addressing and Internetwork Addressing
- ☐ Log files are the primary recorders of a user's activity on a system and of network activities
- ☐ The accuracy of log files determines their credibility. Any modification to the logs causes the validity of the entire log file being presented to be suspect.
- ☐ Routers store network connectivity logs with details such as date, time, source and destination IPs and Ports used that help investigators in verifying the timestamps of an attack and correlate various events to find the source and destination IP
- ☐ Investigators analyze network traffic to locate suspicious traffic, find the network generating the troublesome traffic, and identify network problems
- ☐ Documenting the evidence gathered on a network is easy if the network logs are small, as a printout can be taken and attested
- ☐ Gathering evidence on a network is cumbersome for the following reasons since the evidence is not static and not concentrated at a single point on the network