UNIVERSITY OF Southampton

Security Incidents: Network Analysis

By Dr. Nawfal Fadhel

Academic Centre of Excellence

Question

Have you ever investigated anything?

Case Study: Bind. Torture. Kill.

Dennis Rader: Respected citizen till he was found to be a serial killer.

- Murdered ten people in Kansas from 1974 to 1991
- He confessed in an anonymous letter to a newspaper
- He offered to send police a floppy disk after police bated him saying a floppy disk couldn't be traced.

Case Study: Bind. Torture. Kill.

- Metadata on the RTF file he sent contained
  - Dates
  - Title: "Christ Lutheran Church"
  - "Last Saved By:" Dennis
- Christ Lutheran Church Wichita website showed Dennis Rader as President of Congregation Council

Case Study :John Mcaffee

- Fugitive from Belize police
- Posed for a photo in Guatemala
- Published on the Internet with GPS location metadata

Case Study : Nurin Jazlin's Murder

- Background
  - Submitted to DF in 2007
  - DE:CCTV recording
  - The CCTV recorded a man driving a motorcycle,who then left a bag at a shops lot premise.It was discovered that the bag contained the body of the victim.

Computer Forensics

Forensics are about collecting evidence systematically to a court of law to prove or disprove a claim utilizing state of the art forensic procedure and tools.

McKemmish (1999):

"The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable"

There is:

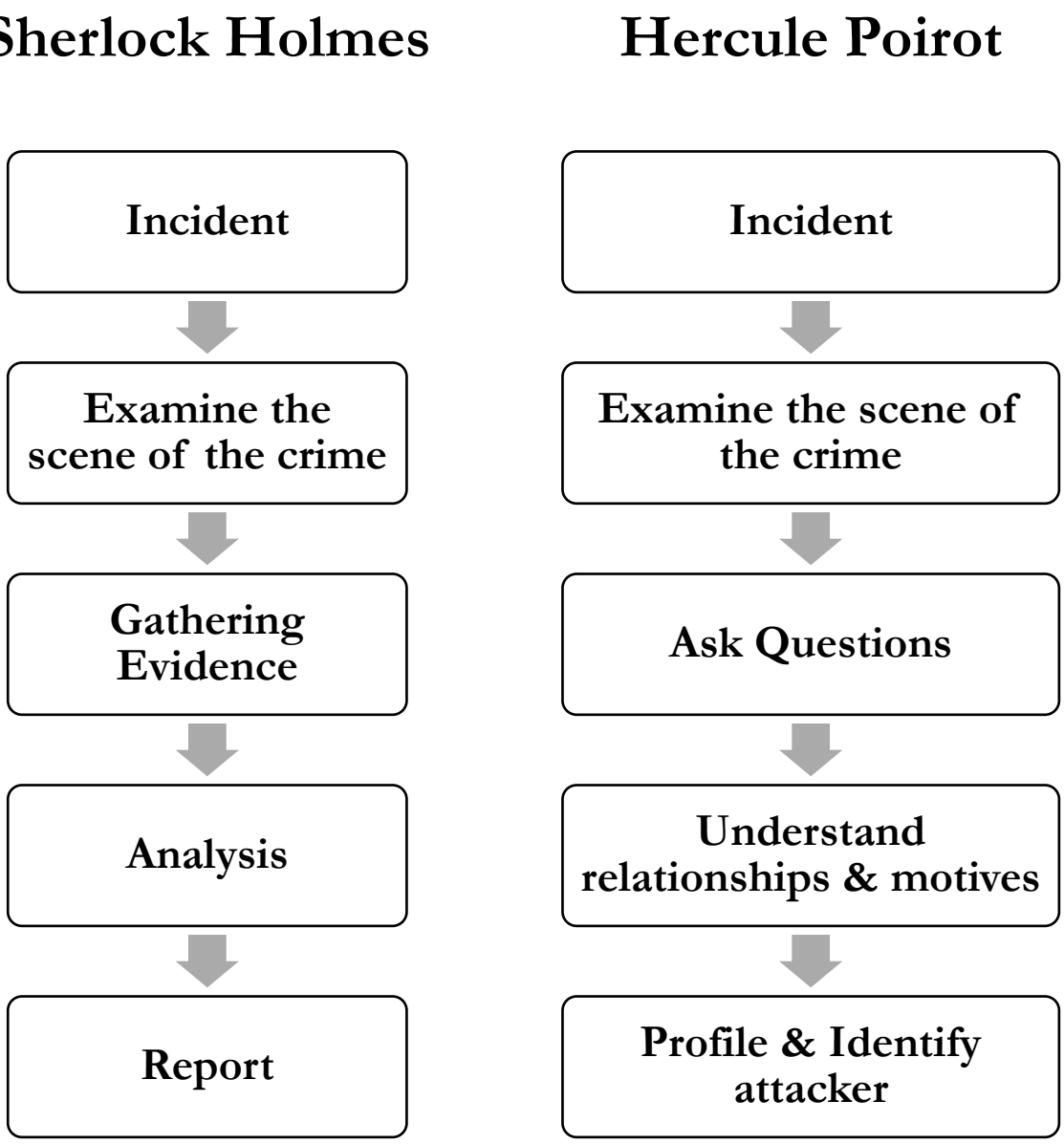
I. Computer forensics

II. Network forensics

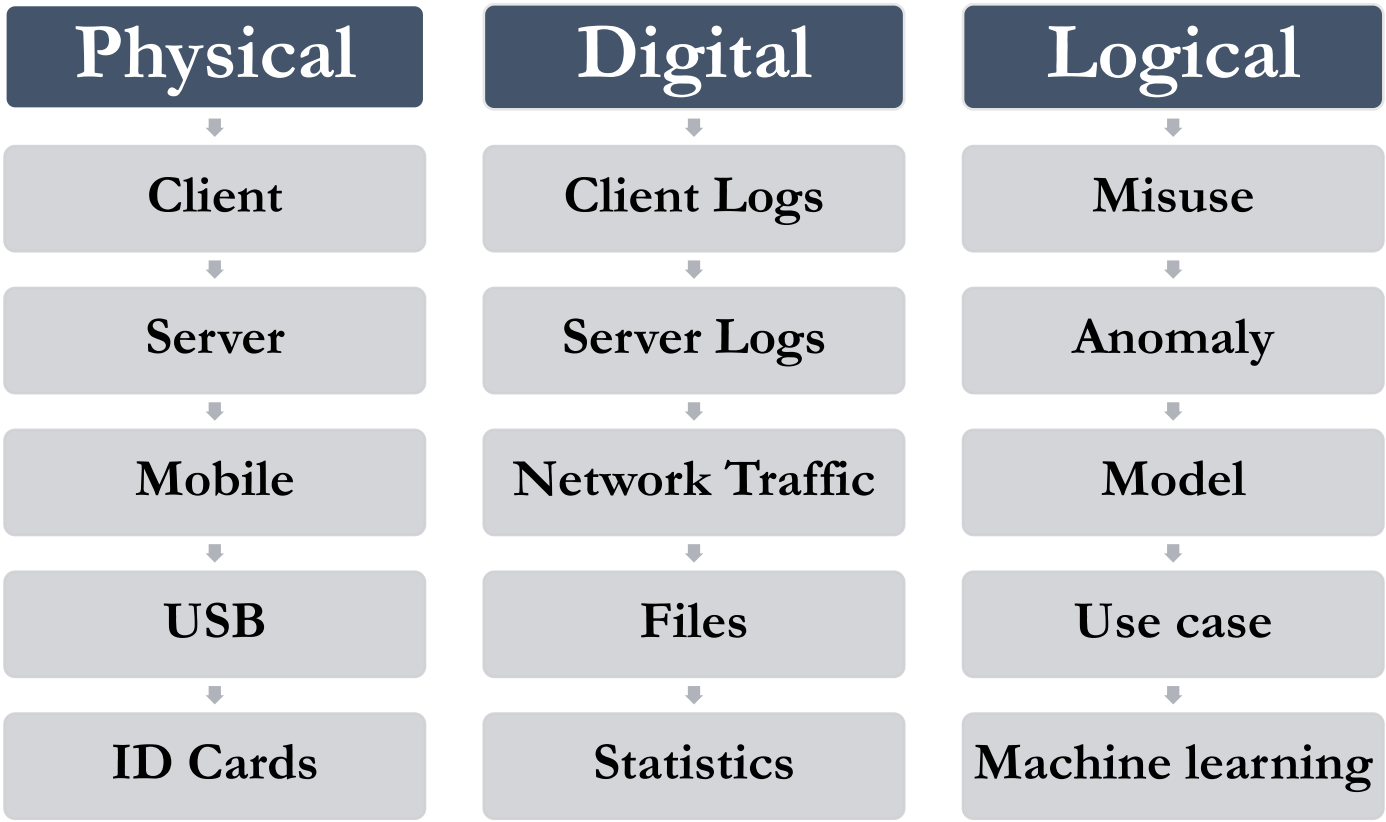
Investigations

I. Real-time forensics (Intrusion Detection Systems?)
II. Reconstructive - post-facto – forensics.
III. Predictive (Threat Analysis) – Out of scope

Investigators

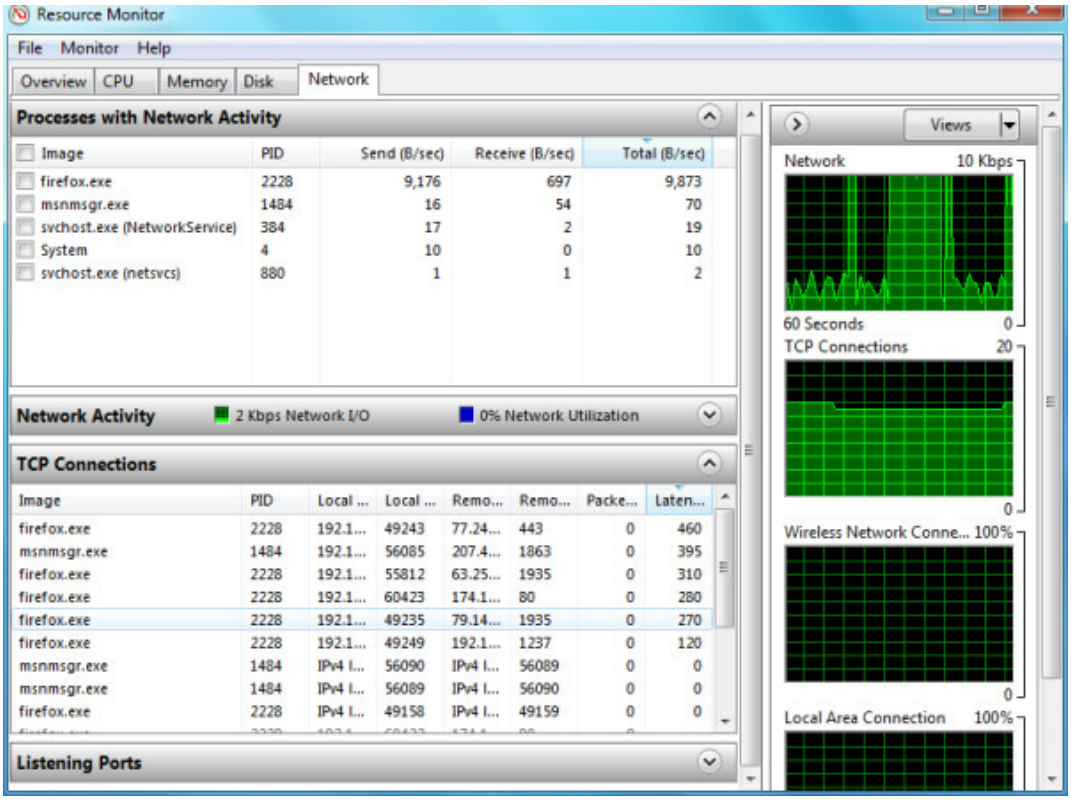


Evidence Types



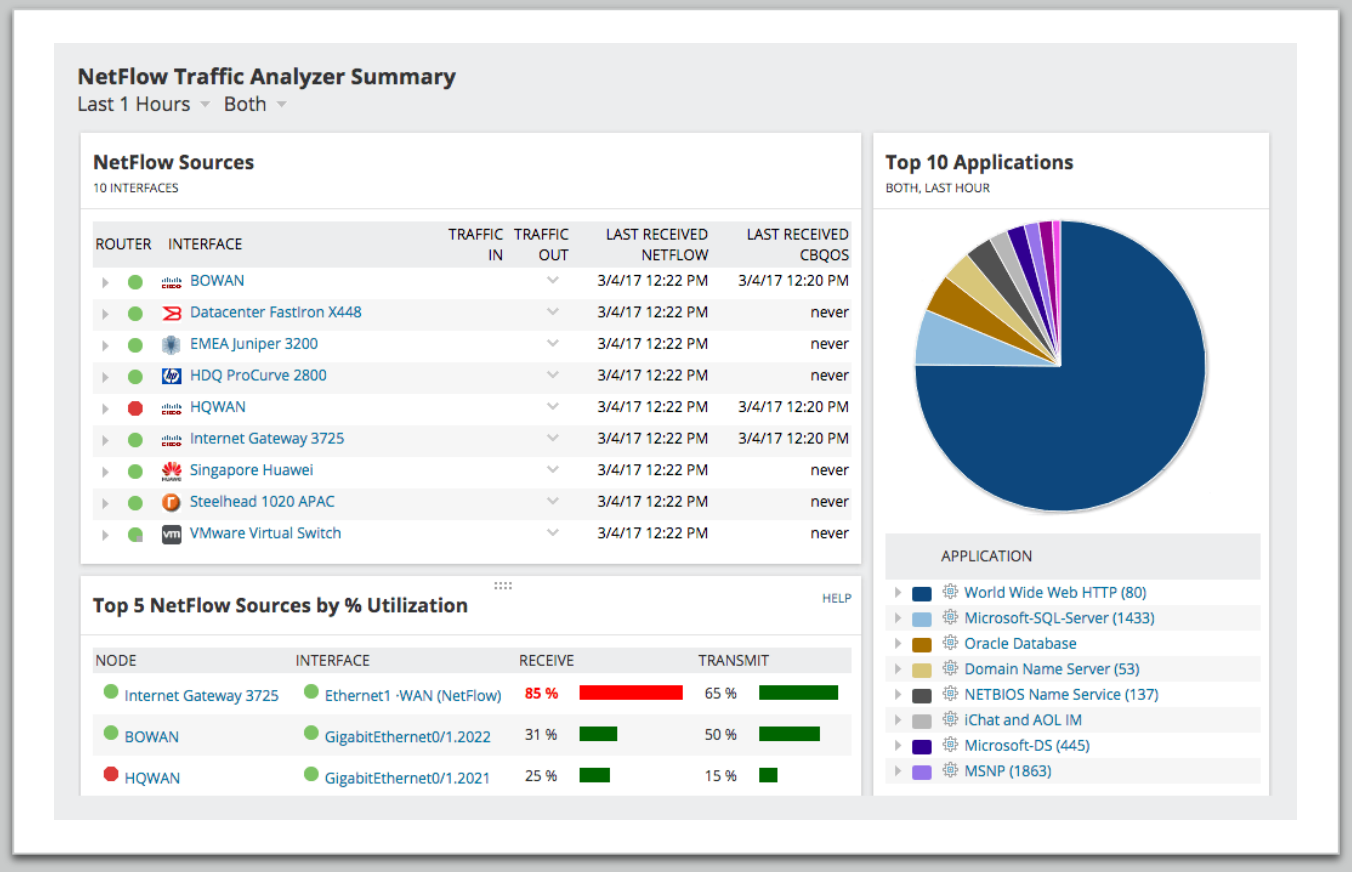
Data Sources - Network Traffic

Network traffic or data traffic is the amount of data at a given point of time that passes across a network. Network data is mostly encapsulated in network packets in computer networks that provide the network load.



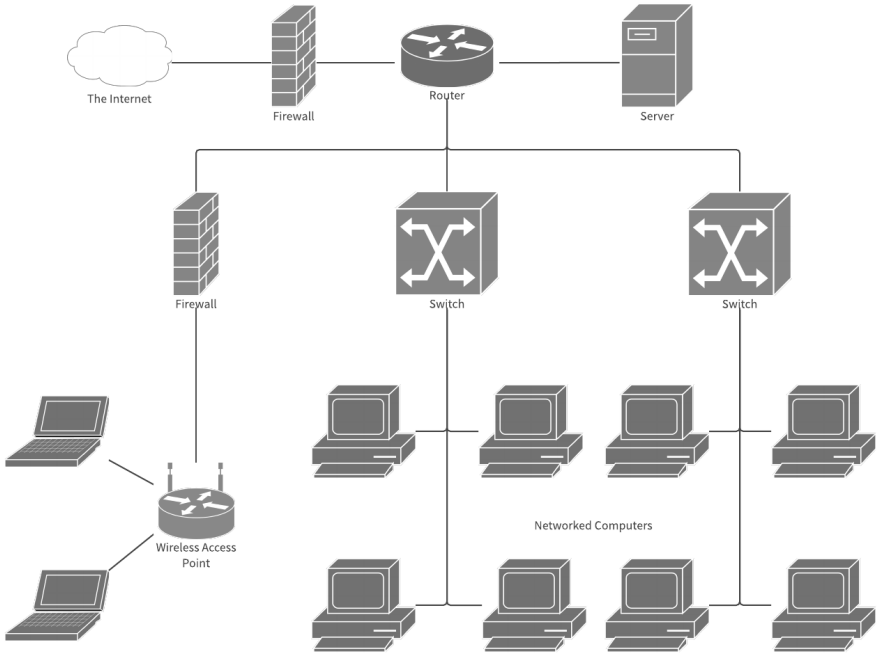
Data Sources - Network aggregates (Netflow)

NetFlow is a feature introduced on Cisco routers around 1996 that allows IP network traffic to be collected as it enters or exits an interface. By analysing NetFlow data, a network administrator may determine things like traffic source and destination, service class, and congestion causes.



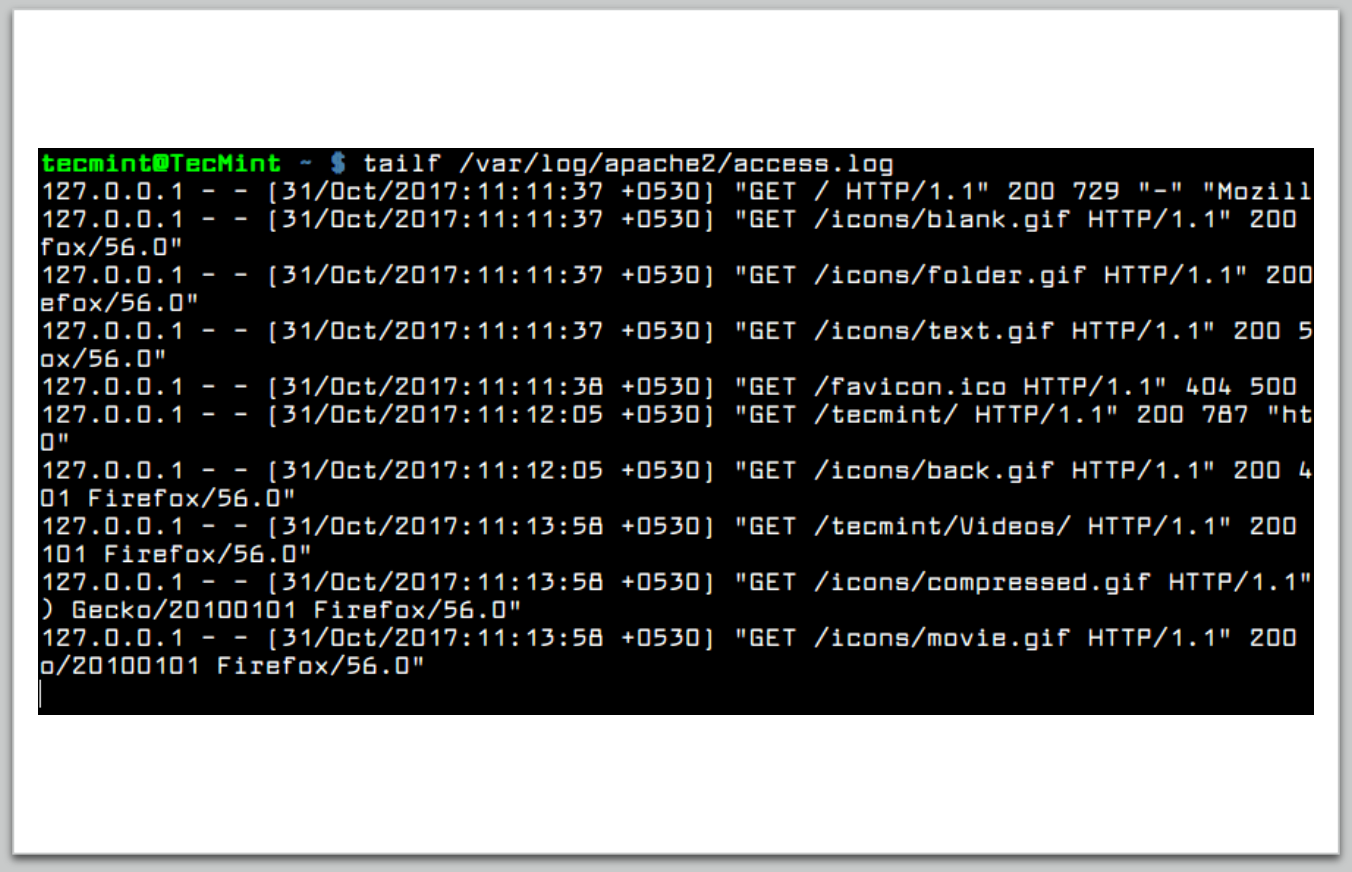
Data Sources - Network Infrastructure Information

Network infrastructure information: Network infrastructure is the hardware and software assets of a whole network allowing an enterprise network to connect, interact, run and maintain. This provides clients, systems, software, utilities and external networks / the internet with the contact route and services.



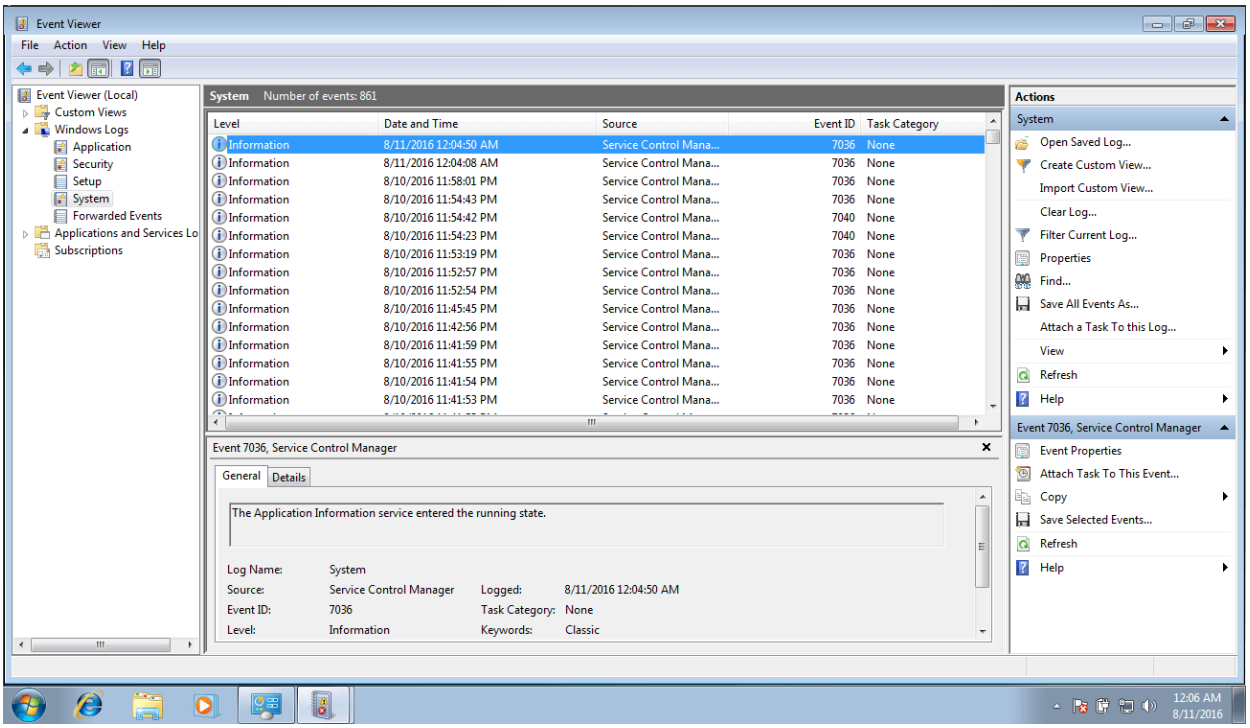
Data Sources - Application logs

Includes web server logs and files. Application log is a log file (or several files) created and maintained automatically by a server consisting of a list of the operations it performed.



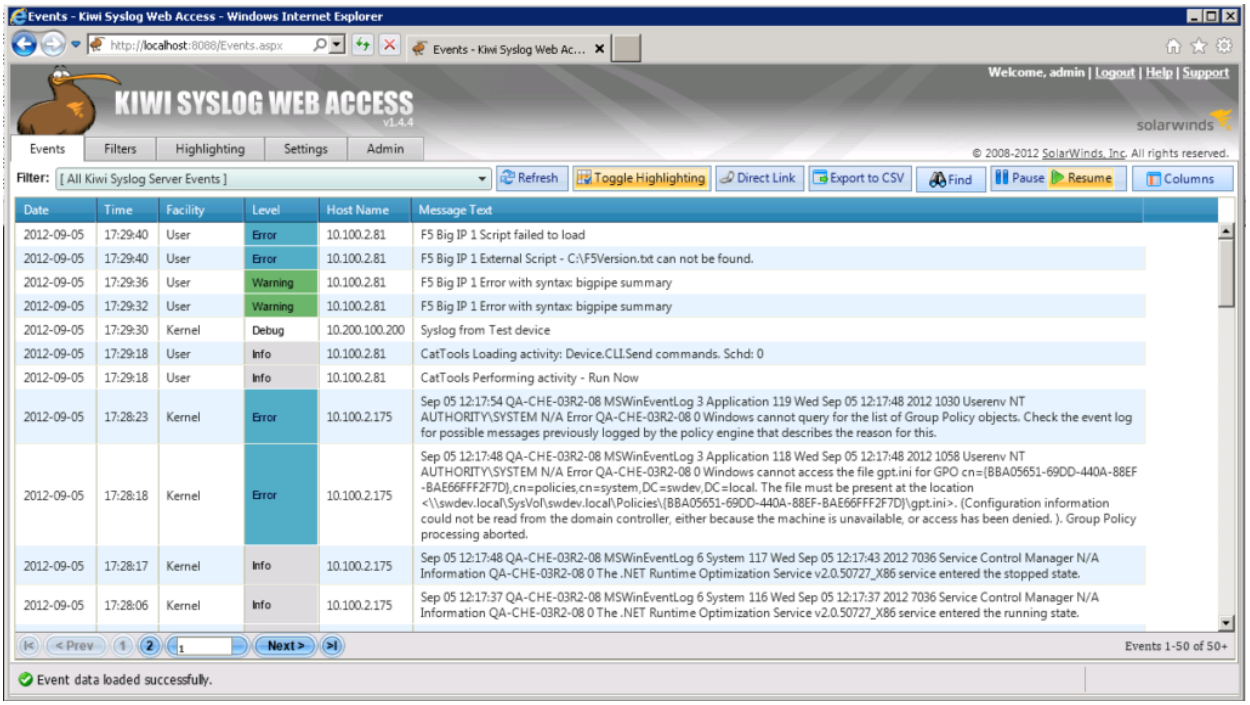
Data Sources - System and kernel logs

System or kernel logs provide a timeline of operating system, application and system events and are a valuable tool for troubleshooting problems. Essentially, the first thing that an administrator has to do when a problem is found is to review log files.



Data Sources - Syslog

Syslog is a way to send event messages to a logging server for network devices – usually referred to as a Syslog server. A wide range of tools supports the Syslog protocol and can be used to log different types of events.

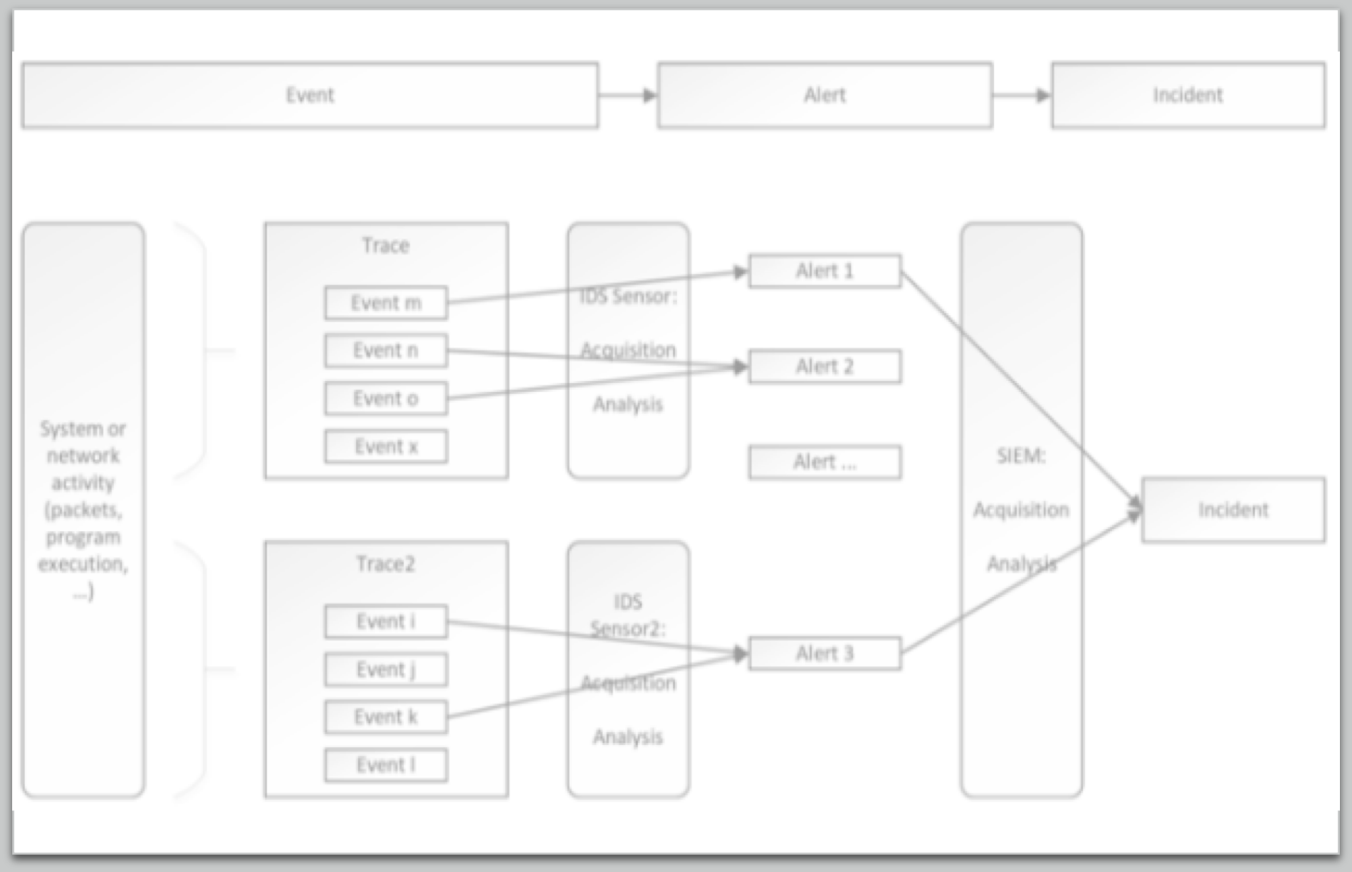


There are

- Registry Keys. Meta-data, pictures, video footage

Analysis Methods

Collected logs are analysed based on various techniques ai med at distinguishing ' normal ' incidents from those sugge sting attacks.



Analysis Methods – Misuse Detection

A Misuse Intrusion Detection System seeks evidence of known trace malicious events and alerts when they are found to inform the analyst about the specifics of the exploited vulnerability and its impact.

Detection of misuse leverages the vast array of information that characterises malicious code and the vulnerabilities exploited by this malicious code.

Software vulnerabilities are particularly relevant for this approach, especially in the (CVE), but identification of misuse has a wider scope.

Example: Antivirus

Analysis Methods – Anomaly Detection

Detection of anomalies is a fundamental tool for detecting cyber attacks because no knowledge of the attacks can be sufficiently comprehensive to provide coverage.

The key advantage of identifying anomalies is their free dom from CVE.

Example: Zero Day Exploit detection

Analysis Methods – Models

Detection of anomalies is based on the concept of a model to test existing trace observations.

The choice of an anomaly model is extremely important. In fact, many publications related to anomaly detection are made in thematic venues such as statistics, signal processing or information fusion, outside of the cybersecurity domain.

Example: IDS

Analysis Methods – Specification Vs Learning

An attack is considered an infringement of a system specification.

The key issue in this approach is to attain specification that can be recognised in the traces with consistency.

If the specifications are precise it more likely to enable the detection of perturbations.

- Supervised learning is used to create models when ground truth is available,
- Unsupervised learning to let models self organise.

Example: Formal Methods

Analysis Methods – Use Cases

From the begining, it requires developers to understand the behaviour of their systems and have sufficient business domain knowledge to understand why and how anomalies manifest themselves, and what their significance is with respect to cybersecurity. In other words TEST CASES

Example: Testing Frameworks

Analysis Methods – Blended

In practice, it is very hard to separate anomaly detection and misuse detection, as they are often intertwined in current sensors.

This approach organises both misuse and anomaly detection in order to leverage the strengths of both approaches and limit their drawbacks. It also leverages the specifications of the application protocol to understand not only the syntax of the trace but also its semantic, in order to propose a better diagnosis.

Summary - Evidence Collection Pattern