**What is Network Forensics?**

Network forensics is capture, recording and analysis of network packets in order to determine the source of network security attacks. The major goal of network forensics is to collect evidence. It tries to analyze network traffic data, which is collected from different sites and different network equipment, such as firewalls and IDS. In addition, it monitors on the network to detect attacks and analyze the nature of attackers. Network forensics is also the process of detecting intrusion patterns, focusing on attacker activity.

### A generic Network forensic examination includes the following steps:

Identification, preservation, collection, examination, analysis, presentation and Incident Response.

### The following is a brief overview of each step:

**Identification**: recognizing and determining an incident based on network indicators. This step is significant since it has an impact in the following steps.

**Preservation**: securing and isolating the state of physical and logical evidences from being altered, such as, for example, protection from electromagnetic damage or interference.

**Collection**: Recording the physical scene and duplicating digital evidence using standardized methods and procedures.

**Examination**: in-depth systematic search of evidence relating to the network attack. This focuses on identifying and discovering potential evidence and building detailed documentation for analysis.

**Analysis**: determine significance, reconstruct packets of network traffic data and draw conclusions based on evidence found.

**Presentation**: summarize and provide explanation of drawn conclusions.

**Incident Response:** The response to attack or intrusion detected is initiated based on the information gathered to validate and assess the incident.

Here are my 5 tips if you are looking to monitor network traffic.

## 1.    Choose the right data source

Whatever your motive for monitoring network traffic, you have two main data sources to choose from:

(1) Flow data can be acquired from layer 3 devices like routers

(2) Packet data can be sourced from [SPAN, mirror ports or via TAPs](https://www.netfort.com/blog/top-5-alternatives-for-span-or-mirror-ports/)

Flow data is fine if you are looking for traffic volumes and mapping the journey of a network packet from its origin to its destination. This level of information can help detect unauthorized WAN traffic, the utilization of network resources and network performance. However, flow-based tools for monitoring network traffic lack the detailed data to perform true root cause analysis.

## Pick the correct points on the network to monitor

Naturally with agent-based software, you have to install software on each device you want to monitor. This is not only an expensive way of monitoring network traffic but it creates a significant maintenance overhead for IT teams. Even with agent-free software, a common mistake many people make when deploying tools to monitor network traffic is that they try and monitor too many data sources at the start. There is no need to monitor every network point. Instead you need to pick points where data converges. Examples of this would be Internet gateways, Ethernet ports on WAN routers or VLANs associated with critical servers.

## Sometimes real-time data is not enough

The ability to monitor network traffic in real-time is sufficient to achieve many objectives of network traffic monitoring, but sometimes real-time data is not enough. Historical data is just as important if you want to analyze past events, identify trends or compare current network activity to maybe a week previous. For these objectives it is best to use tools for monitoring network traffic with deep packet inspection.

Some tools for monitoring network traffic choose to age data. This means the further back you go historically, the less detail you can get. While this can save on disk space, it is not an ideal solution if you are trying to determine how an intruder managed to overcome your defenses to plant malware on the network. Without accurate and complete data relating to the event, you can be left looking for answers that no longer exist.

## Associate the data with usernames

Traditional network traffic monitoring tools usually report on activity using IP or MAC addresses. While this is useful information, it can be problematic in DHCP environments if you are trying to find a problematic device. One piece of information that can bring together network activity and devices is usernames. Username association will let you know who is doing what on the network.

## Check the flows and packet payloads for suspicious content

Many networks have [intrusion detection systems](https://www.netfort.com/languardian/solutions/network-security-monitoring/) at the network edge but very few networks have this type of technology monitoring traffic inside the network. All it takes is for one rogue mobile or [IoT](https://en.wikipedia.org/wiki/Internet_of_things) device for a network to be compromised

**Log Analysis** is an important part of Forensics. While analyzing an incident, it is very important to be clear in your goal. Collect the logs according to your needs. There may be various types of logs, which might not be useful for the incident under analysis. So, it is very important to understand the goal and collect appropriate logs.

Some logs which should be collected are listed below:

#### For Windows Operating System

* Save the application logs from the event viewer.
* Save the security logs from the event viewer.
* Save the system logs from the event viewer.

#### For Linux Operating System

* /var/log/message: For general message and system related stuff
* /var/log/auth.log: Authenication logs
* /var/log/kern.log: Kernel logs
* /var/log/boot.log : System boot log
* /var/log/utmp or /var/log/wtmp : Login records file

#### Other logs can be collected depending on the incident under analysis

* In case of a network hack, collect logs of all the network devices lying in the route of the hacked device and the perimeter router (ISP router). Firewall rulebase may also be required in this case.
* In case it is an unauthorized access, save the web server logs, application server logs, application logs, router or switch logs, firewall logs, database logs, IDS logs etc. This case we have to ensure that where-ever an authorization is present, we collect the log.
* Incase of a Trojan / Virus / Worm attack, save the antivirus logs apart from the event logs (pertaining to the antivirus).

Also, there are certain things that should be avoided, such as:

* Rebooting/formatting the infected system before obtaining the logs.
* Cleaning/modifying/carrying out any activity on the infected machine, until the forensic analysis is completed.
* Deleting/modifying any type of logs. This might destroy the evidence, present there.
* Carrying out any activity that might modify the logs.
* Hiding anything from Incident Response team.

**Network Forensics Tools**

### NIKSUN

NIKSUN NetDetector is a full-featured appliance for network security monitoring built on NIKSUN’S award-winning NikOS architecture. It is the only security monitoring appliance that integrates signature-based IDS functionality with statistical anomaly detection, analytics and deep forensics with full-application reconstruction and packet level decodes. Recognized as the industry’s best security monitoring and forensics appliance to safeguard against increasingly sophisticated cyber-attacks.

### NETSCOUT

Netscout Arbor Spectrum addresses these challenges by serving as a force multiplier for the security team, regardless of their size and expertise levels. Not only does it provide unprecedented visibility into network activity and quickly surface high-priority issues, it enables security teams to detect and investigate incidents in a far more efficient and complete fashion.

### LOGRYTHM

LogRhythm Network Monitor When attackers compromise the perimeter or are operating from within, you need to know. Evidence of intruders and insider threats lies within network communications. Detect network-based threats with real-time network monitoring and big data analytics

### SAVVIUS

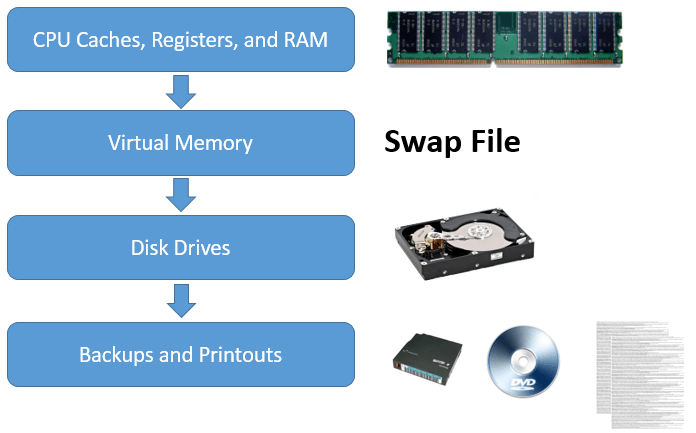
Savvius vigil automates the collection of network traffic needed for security investigations, both reducing the likelihood of a breach, minimizing their impact. Even breaches not discovered for months can be effectively investigated using Vigil. Savvius Vigil, which integrates with all leading IDS/IPS systems, includes Omnipeek, award-winning network forensics software.

### PACKETSLED

PacketSled automates incident response by fusing business context, AI, entity enrichment and detection with network visibility.  Used for real-time analysis and response, PacketSled’s platform leverages continuous stream monitoring and retrospection to provide network forensics and security analytics

## Order of Volatility

In forensics, order of volatility refers to the order in which you should collect evidence. Highly volatile data is easily lost, such as data in memory when you turn off a computer. Less volatile data, such as printouts, is relatively permanent and the least volatile. The following graphic shows the order of volatility from most volatile to least volatile.



### The IETF and the Order of Volatility

The Internet Engineering Task Force (IETF) released a document titled, Guidelines for Evidence Collection and Archiving. It is also known as [RFC 3227](https://tools.ietf.org/html/rfc3227#section-2.1). This document explains that the collection of evidence should start with the most volatile item and end with the least volatile item. So, according to the IETF, the Order of Volatility is as follows:

1. Registers, Cache
2. Routing Table, ARP Cache, Process Table, Kernel Statistics, Memory
3. Temporary File Systems
4. Disk
5. Remote Logging and Monitoring Data that is Relevant to the System in Question
6. Physical Configuration, Network Topology
7. Archival Media

### Registers, Cache

The contents of CPU cache and registers are extremely volatile, since they are changing all of the time. Literally, nanoseconds make the difference here. An examiner needs to get to the cache and register immediately and extract that evidence before it is lost.

### Routing Table, ARP Cache, Process Table, Kernel Statistics, Memory

Some of these items, like the routing table and the process table, have data located on network devices. In other words, that data can change quickly while the system is in operation, so evidence must be gathered quickly. Also, kernel statistics are moving back and forth between cache and main memory, which make them highly volatile. Finally, the information located on random access memory (RAM) can be lost if there is a power spike or if power goes out. Clearly, that information must be obtained quickly.

### Temporary File Systems

Even though the contents of temporary file systems have the potential to become an important part of future legal proceedings, the volatility concern is not as high here. Temporary file systems usually stick around for awhile.

### Disk

Even though we think that the data we place on a disk will be around forever, that is not always the case (see the SSD Forensic Analysis post from June 21). However, the likelihood that data on a disk cannot be extracted is very low.

### Remote Logging and Monitoring Data that is Relevant to the System in Question

The potential for remote logging and monitoring data to change is much higher than data on a hard drive, but the information is not as vital. So, even though the volatility of the data is higher here, we still want that hard drive data first.

### Physical Configuration, Network Topology, and Archival Media

Here we have items that are either not that vital in terms of the data or are not at all volatile. The physical configuration and network topology is information that could help an investigation, but is likely not going to have a tremendous impact. Finally, archived data is usually going to be located on a DVD or tape, so it isn’t going anywhere anytime soon. It is great digital evidence to gather, but it is not volatile.