# A Survey about Network Forensics Tools

Amor Lazzez,
Taif University
Kingdom of Saudi Arabia
e-mails: a.lazzez@tu.edu.sa ; a.lazzez@gmail.com

*Abstract*—**This paper gives an overview about the main tools and techniques available to ensure forensic investigations of network security attacks. Given that Web and Email services are the most common used network communication schemes, we mainly focus on the forensic investigation of Email and Web services attacks. Moreover, we present a set of forensics tools used for network traffic capture such as Snort, Pcap, TcpDump, and Ethereal. Besides, we present the major existing IP traceback schemes that have been designed to trace back to the origin of IP packets through the Internet. In addition to the survey of network forensics tools, the paper presents a generic framework proposed for network forensic analysis.**

***Keywords- network security attack, forensic investigation,***

## I. INTRODUCTION

With the phenomenal growth of the Internet, cyber attacks and crimes are happening every day and everywhere. When we face a cyber attack, we can detect it and take countermeasures. For instance, an intrusion detection system (IDS) can help detect attacks; we can update operating systems to close potential backdoors; we can install antivirus software to defend against many known viruses. Although, we can detect attacks and mitigate their damage, it is hard to find the real attackers or criminals. However, if we don't trace back to the attackers, they can always conceal themselves and launch new attacks. Therefore, it is very important to build the capability to trace and attribute attacks to the real cyber criminals, which may significantly reduce the attacks we face every day.

Traceback and attribution are performed during or after a cyber violation, to identify where an attack originated, how it propagated, and what computer(s) and person(s) are responsible. The goal of network forensics capabilities is to determine the path from a victimized network or system to the point of attack origination or the person who is responsible. In some cases, the computers launching an attack may themselves be compromised hosts or be controlled remotely. Attribution is the process of determining the identity of the source of a cyber attack. Types of attribution can include both digital identity (computer, user account, IP address, or enabling software) and physical identity (the actual person using the computer from which an attack originated).

Traceback in computer networks and especially in the Internet environment is considered so difficult to perform for many reasons. The first one is that today's Internet is stateless. For example, a backbone router only forwards the packets and does not care where they are from; a typical mail transfer agent simply relays emails to the next agent and never minds who the sender is. The second reason is that today's Internet is almost an unauthorized environment. An attacker can send millions of emails using another email address (Email Spoofing); Alain can make a VoIP call to Albert and pretend to be Brigitte; an attacker can change the source IP address in the packet header (IP spoofing) to that of a different machine and thus avoid traceback.

Even though these difficulties, and given the huge increase of cyber crimes over the Internet and computer networks, many techniques have been developed to conduct network forensics which deals with the capture, recording, and analysis of network events in order to discover evidential information about the source of security attacks in a court of law [1-3].

This paper aims to survey tools and techniques available to ensure forensic investigations of network security attacks. Given that Web and Email services are the most common used network communication schemes, we mainly focus on the forensic investigation of Email and Web services attacks. Moreover, we present a set of forensics tools used for network traffic capture (sniffers) such as tcpdump, windump, Snort, Ethereal, Sniffit, and dsniff. Besides, we present the major existing IP traceback schemes that have been designed to trace back to the origin of IP packets through the Internet. In addition to the survey of network forensics tools, the paper presents a generic framework proposed for network forensic analysis [1].

The remaining part of this paper is organized as follows. Section 2 defines network forensics, presents the principles of network forensics, and presents two different classifications of the network forensic systems. Section 3 explains how to perform the forensic investigation of Email attacks using certain freely available tools such as EmailTrackerPro [18] and SmartWhoIs [19]. The tools described in this Section could be used to trace the sender of an email. Section 4 describes how to conduct the forensic analysis of Web attacks using available tools like Web Historian [20] and Index.dat analyzer [21]. These tools help to reveal the browsing history of a person including the number of times a website has been visited in the past and the duration of each visit, the files that have been uploaded and downloaded from the visited website, the cookies setup as part of the visits and other critical information. Section 5 describes the use of packet sniffers like Ethereal [17] to explore the hidden information in the different headers of the TCP/IP protocol stack. These sniffers capture the packets exchanged in the Ethernet and allow the investigator to collect critical information from the packets. Section 6 describes the

use of IP traceback techniques to reliably determine the origin of a packet in the Internet, i.e., to help the forensic investigator to identify the true sources of the attacking IP packets [2, 3]. The IP traceback techniques allow a victim to identify the network paths traversed by the attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Section 7 presents a generic framework proposed for network forensic analysis [1]. Section 8 concludes the paper.

## II. NETWORK FORENSICS

Network forensics can be generally defined as a science of discovering and retrieving evidential information in a networked environment about a crime in such a way as to make it admissible in court. The concept of network forensics deals with the data found across a network connection mostly ingress and egress traffic from one host to another. Network forensics analyzes the traffic data logged through firewalls or intrusion detection systems or at network devices like routers. The goal is to traceback to the source of the attack so that the cybercriminals are prosecuted.

Network forensics is defined in [22] as "the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response or to recovery from these activities".

In [23], the author defined the network forensics as "the capture, recording, and analysis of network events in order to discover the source of security attacks." Network forensics involves monitoring network traffic and determining if there is an anomaly in the traffic and ascertaining whether it indicates an attack. If it is so then the nature of the attack is also determined. Network traffic is captured, preserved, analyzed and an incident response is invoked immediately.

The large number of security incidents affecting many organizations and the increase in sophistication of these cyber attacks are the main driving forces behind network forensics. During and after the attack, the attacker may take actions to try to avoid detection (changing system logs, installing a rootkit), which make attack traceback and attribution more difficult. Companies doing business on Internet cannot hide a security breach and are now expected to prove the state of their security as a compliance measure for regulatory purposes. Internet Service Providers (ISPs) are also being made responsible for what passes over their network. Hence, having the network forensics process in place will meet the requirements of all – users, organizations, and ISPs.

### A. *The Principles of Network Forensics*

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file for "MSW_USltr_format".

Different from intrusion detection, all the techniques used for the purpose of network forensics should satisfy both legal and technical requirements. For example, it is important to guarantee whether the developed network forensic solutions are practical and fast enough to be used in high-speed networks with heterogeneous network architecture and devices. More important, they need to satisfy general forensics principles such as the rules of evidence and the criteria for admissibility of novel scientific evidence (such as the Daubert criteria).[24-26].

The five rules are that evidence must be:

- Admissible. Must be able to be used in court or elsewhere.
- Authentic. Evidence relates to incident in relevant way.
- Complete. No tunnel vision, exculpatory evidence for alternative suspects.
- Reliable. No question about authenticity and veracity.
- Believable. Clear, easy to understand, and believable by a jury.

The evidence and the investigative network forensics techniques should satisfy the criteria for admissibility of novel scientific evidence [3]:

- Whether the theory or technique has been reliably tested
- Whether the theory or technique has been subject to peer review and publication
- What is the known or potential rate of error of the used method?
- Whether the theory or method has been generally accepted by the scientific community

### B. *Network Forensics vs. Network Security*

Network forensics is being researched for several years but it still seems a very young science as many issues are still not very clear. Network forensics is not another term for network security. Network security is an essential part in network forensics as data for forensic analysis can be collected from security products placed to detect and prevent intrusions.

Network security protects the system against attack while network forensics does not. Network security products look for possible harmful behaviors related with various attacks and monitor the network 24 hours a day. Network forensics is post mortem investigation of the attack in many cases. It is case restricted and is started after crime notification specifically addressing a particular attack.

Network forensics ensures that the attacker spends more time and energy to cover his tracks making the attack costly. Network criminals are also cautious to avoid prosecution for their illegal actions. This acts as a deterrent and reduces

network crime rate, thus improving security. Network forensics also can initiate investigation in real time provided resources are available to handle the traffic and analyze it.

### C. Network Forensics vs. Privacy

As it is mentioned above, network forensics deals with the capture, recording and analysis of network traffic in order to discover the source of a security incident. Forensic investigation may violate the privacy policies, but as long as only the data considered as suspicious and relevant to the case is investigated, the privacy may remain intact. Besides, the suspected perpetrator loses the right to privacy. Privacy considerations are outlined in the Guidelines for Evidence Collection and Archiving [RFC 3227]. In [27], the authors propose a forensic profiling system which accommodates real-time evidence collection as a network feature and uses a mechanism to keep the privacy intact.

### D. Classification of Network Forensic Tools

In [28], the author classifies the network forensic systems into two types: Catch-it-as-you-can tools and stop-look-and-listen tools.

- Catch-it-as-you-can Tools: All the packets passing through a particular traffic point are captured and written to storage. Analysis is subsequently done in batch mode. This approach requires large amounts of storage.
- Stop-look-and-listen Tools: Each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This requires a faster processor to match the pace of incoming traffic.

Both approaches require significant storage and the need for occasional erasing of old data to make room for new. The open source programs tcpdump and windump as well as a number of commercial programs can be used for data capture and analysis.

One concern with the "catch-it-as-you-can" approach is one of privacy since all packet information (including user data) is captured. Internet service providers (ISPs) are expressly forbidden by the Electronic Communications Privacy Act (ECPA) from eavesdropping or disclosing intercepted contents except with user permission, for limited operations monitoring, or under a court order. The U.S. FBI's Carnivore is a controversial example of a network forensics tool.

According to [4], network forensics tools may be classified into: host-based tools and network-wide tools:

- Host-based Forensics Tools: A host-based network forensics tool resides on a single host in the network and helps understand network activity by capturing and analyzing packets that arrive at that host. It usually provides a lot of information in the form of logs for the user to analyze. Tcpdump, Pcap and Snort, are some of the most used host-based network forensics tools.
- Network-wide Forensics Tools: Network-wide forensic tools consist of multiple monitors that can be installed at different points in the network and used for distributed network surveillance. Information required to perform certain network forensic activities such as IP traceback, attack reconstruction or e-mail tracing has to be collected from hosts in the same domain as the victim host, or from cooperating or hostile parts outside the victim's domain. Such network monitoring tools integrate data from the different monitors and provide a complete and comprehensive view of the network activity. Niksun NetDetector 2005 is one of the most popular network forensic tools with network-wide deployment.

## III. Web Forensics Investigation

The predominant web browsers in use today are Internet explorer and Firefox. Each of these browsers saves, in their own unique formats the web browsing history of each user who has an account on a machine. Internet explorer stores the browsing history of a user in the index.dat file and Firefox browser saves the web activity in a file named history.dat. These two files are hidden files. So, in order to view them, the browser should be setup to show both hidden files and system files. One cannot easily delete these two files in any regular way.

Web forensics deals with gathering critical information related to a crime by exploring the browsing history of a person, the number of times a website has been visited, the duration of each visit, the files that have been uploaded and downloaded from the visited website, the cookies setup as part of the visit and other critical information. Many tools have been proposed to ensure a forensic investigation of web attacks. In the following subsetions, we present both of the most common web forensic tools, to know Index.dat analyzer and Mandiant Web Historian.

### A. Index.dat Analyzer

The Index.dat analyzer [20] is a freeware web forensics tool used to view, examine and delete the contents of index.dat files. It can be used to simultaneously or individually view the browsing history, the cookies and the cache. The tool provides support to directly visit the website listed in the output of the analyzer and also to open the file uploaded to or downloaded from the website. The tool also provides critical information about a cookie like its key-value pair, the website address associated with the cookie, the date/time the cookie was first created and last accessed and etc. In addition to these two tools, there exist tools like Total Recall [12], which can be used to extract the list of favorite websites stored in the browser history.

### B. Mandiant Web Historian

Mandiant Web Historian [21] is a useful freeware utility which assists users in reviewing web site URLs that are stored in the history files of the most commonly used web browsers. The tool allows the forensic examiner to determine what, when, where, and how the intruders looked into the different sites. Web Historian can be used to parse a specific history file or recursively search through a given folder or drive and find all

the browser history files that the tool knows how to parse. Web Historian generates a single report (that can be saved in different file formats) containing the Internet activity from all of the browser history files it is able to locate.

## IV. EMAIL FORENSICS INVESTIGATION

Email is one of the most common used network communication services. As email usage increases, attackers and hackers began to use emails in committing crimes. In fact, Emails frequently contain malicious viruses, threats and spams that can result in the data interception, loss of data, and confidential information theft. Email forensic investigation refers to the study of the source and content of email as evidence, the identification of the actual sender and recipient of a message, the date/time it was sent, etc. Many tools have proposed for the forensics investigation of email attacks. In the following subsections, we present EmailTrackerPro, and SmartWhoIs; two email forensics tools which help to identify the sender of the message, trace the path traversed by the message and identify the phishing emails that try to obtain confidential information from the receiver.

### A. *EmailTrackerPro*

EmailTrackerPro [18] is a proprietary tool which helps identify the true source of emails to help track suspects, verify the sender of a message, trace and report email abusers. The trace analysis reports the sender's IP address, estimated location, network and domain information. EmailTrackerPro also helps uncover misdirection. EmailTrackerPro relies on the analysis of email header which contains the source email address, lists every point the email passed through on its journey, along with the date and time, and provides an audit trail of every machine the email has passed through. EmailTrackerPro relies on a location database to track emails to a country or region of the World, showing the information on a global map. EmailTrackerPro shows the email trace graphically and generates a summary report. The summary report provides an option to report the abuse of a particular email address to the administrators of the attacker and the victim networks and also contains some critical information that can be useful for forensic analysis and investigation. The report includes the geographic location of the IP address from which the email was sent, and if this cannot be found, the report at least includes the location of the attacker’s ISP. The report also includes the domain contact information of the network owner or the ISP, depending on the sender email address.

### B. *SmartWhoIs*

SmartWhois [19] is an open source software which allows you to look up all the available information about an IP address, hostname or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information. It helps you find answers to these important questions:

- Who is the owner of the domain?
- When the domain was registered and what is the owner's contact information?
- Who is the owner of the IP address block?

SmartWhois supports Internationalized Domain Names (IDNs), so you can query domain names that use non-English characters. It also fully supports IPv6 addresses. SmartWhoIs can be used along with eMailTrackerPro if the information provided by the latter is not complete.

## V. WEBMAIL ANALYSIS

Webmail poses a slight challenge to a forensic investigator because the emails are not conveniently archived and stored on an individual's hard drive. However, webmail will almost always leave traces on the system that accessed the webmail site. Most notable is that the web browser cache may contain messages that were read on the webmail system. However, many browsers are set by default to not cache SSL-encrypted pages (which most webmail sites are), rendering the technique of examining browser cache obsolete. There may, however, still be evidence that the browser accessed the webmail site. Unencrypted pages prior to the login page may be stored in cache, and unless the user is particularly savvy or paranoid, having saved cookies from the site is almost a given. Browser history is also likely to show evidence of the use of webmail. Bookmarks or "Internet Favorites" (in Internet Explorer) are also a good indication that a browser may be being used for webmail.

Although the content of the emails may not be immediately available, it is worthwhile to keep in mind that in a criminal case or civil case that goes to court, it may be possible to subpoena the webmail host for access to an account and relevant records.

## VI. PACKET SNIFFERS

A sniffer is software application that collects traffic flowing into and out of a computer attached to a network through a given interface [16]. Sniffers are used to collect information about different communications occurring over a network for different purposes; traffic monitoring, intrusion detection, and forensics investigation. Many tools have been proposed for traffic sniffing. The main are Ethereal, Snort, Pcap, and TcpDump.

### A. *Snort*

Snort [4] is a freeware network security tool which was initially developed for the Unix platform and has now been ported to the windows platform. Snort is a simple, command line tool used to show network traffic, detect network intrusion, perform protocol analysis, and ensure network troubleshooting. Snort has a small memory footprint and requires very little processing power. The tool can capture traffic flowing into and out of a computer network or it can put the network adaptor in promiscuous mode and listen to all network traffic.

### B. Pcap

Pcap [2, 4] is a packet capture tool used to collect traffic going through a network interface. Pcap was initially developed for network interfaces of a system running UNIX operating System. As an extension of Pcap, WinPcap [14] is a packet sniffing tool used to capture the packets flowing in and out of a network interface of a system running the Windows Operating System. WinPcap includes a network statistics engine and provides support for packet filtering. AirPcap [15] is an extension of Winpacp tool to collect packets going through a 8021.11 Wireless LAN interfaces of a windows system. AirPcap may capture the control frames (ACK, RTS, CTS), management frames (Beacon, Probe Requests and Responses, Authentication), and data frames.

### C. TcpDump

TcpDump [2, 4] is a command line tool used for network monitoring, protocol debugging, and data gathering. TcpDump displays the headers of packets going through a given network interface. TcpDump is available for use in multiple UNIX operating systems. WinDump is a version of TcpDump available for Windows operating systems. WinDump collects the traffic packets flowing into and from a network interface and may put the network interface in promiscuous mode which allows it to grab all the packets it sees, not just the ones destined for it.

### D. Ethereal

Ethereal [2,17] is a freeware widely used as a network packet sniffer and analyzer. In fact, it ensures a live capture of the network traffic, displays the information in the headers of all the protocols used in the transmission of the captured packets, and filters the network traffic depending on user needs. Ethereal classifies the captured packets according to the used protocol like TCP, UDP, ARP, etc., and displays detailed information relative to each captured packet such as the packet number in the captured file, the timestamp, the source IP address, the destination IP address, and the high-level protocol. Moreover, it shows the structure and a bit-level content of the different headers (starting from the framelevel) of each captured packet. Moreover, Ethereal provides options to save the capture file, export the results and also to search for packets based on a specific field or value in the current capture file or a saved capture file.

## VII. IP TRACEBACK TECHNIQUES

A network security attack involves a number of packets sent to a victim system. IP Traceback consists to identify the source of such attack packets. Let $P$: $h_1, h_2, \ldots, hi, h_{i+1}, \ldots, h_n$ denotes the connection path between hosts $h_1$ to $h_n$. Then, the IP traceback problem is defined as: Given the IP address of $h_n$, identify the actual IP addresses of hosts $h_{n-1}, \ldots, h_1$. If $h_1$ is the source and $h_n$ is the victim machine of a security attack, then $P$ is called the attack path [13].

The IP traceback problem is considered so hard to resolve for many reasons. The first reason is that an attack packet may be easily spoofed at different layers of the TCP/IP protocol stack which makes difficult the identification of its original application. In fact, an attack packet may be spoofed at the link layer by using a different MAC address than the original one, at the Internet layer by using a different source IP address, at the transport layer by using a different TCP/IP port, or at the application layer by using a different email address. The second reason is that the attack flow may be generated by a remotely controlled host or travel through a chain of compromised hosts, called stepping-stone, and acting as a conduit for the attacker's communication. Another reason is that the security functions practiced in existing networks may also prevent the capability to follow the reverse path. For example, if the attacker lies behind a firewall, then most of the traceback packets are filtered at the firewall and one may not be able to exactly reach the attacker.

Even though these difficulties, some IP traceback techniques have been proposed. In the following subsections, we review the major existing IP traceback schemes that have been designed to trace back to the origin of IP packets through the Internet. Existing IP traceback schemes may be categorized into four primary classes: Input Debugging, Controlled Flooding, ICMP Traceback, and Packet Marking [2, 3].

### A. Input Debugging

In [2], the authors proposed the input debugging scheme as an IP traceback technique. According to such scheme, after recognizing that it is being attacked, the victim develops an attack signature that describes a common feature contained in all the attack packets. The victim communicates this attack signature to the upstream router that sends it the attack packets. Based on this signature, the upstream router employs filters that prevent the attack packets from being forwarded through an egress port and determines which ingress port they arrived on. The process is then repeated recursively on the upstream routers, until the originating site is reached or the trace leaves the boundary of the network provider or the Internet Service Provider (ISP). From now on, the upstream ISP has to be contacted to repeat the procedure. The input debugging approach assumes that the attack is in progress and cannot be used "post-mortem". The main concern of this approach is the considerable management overhead at the ISP level to communicate and coordinate the traceback across domains.

### B. Controlled Flooding

As it is presented in [2], and according to the Controlled Flooding scheme, the victim uses a pre-generated map of the Internet topology to iteratively select hosts that could be coerced to flood each of the incoming links of the upstream router. Since the router buffer is shared by packets coming across all incoming links, it is possible that the attack packets have a higher probability of being dropped due to this flooding. By observing changes in the rate of packets received from the attacker, the victim infers the link through which the attack packet would have come to the upstream router. This basic testing procedure is then recursively applied on all the upstream routers until the source is reached. Though this method is both ingenious and pragmatic, using unsuspecting hosts to flood is

itself a denial-of-service attack. It would be a tremendous overhead to use flooding to detect distributed denial-of-service attacks when multiple upstream links may be contributing to the attack. The victim also needs to possess an accurate topology map to select the hosts that would flood the upstream routers. Like the input debugging scheme, the controlled flooding approach assumes that the attack is in progress and cannot be used "post-mortem".

### C. ICMP Traceback

In [12], the authors proposed an IP traceback scheme named iTrace relying on the use of ICMP messages for authenticated IP marking. According to iTrace, every router samples, with a low probability, the packets it is forwarding. For each sampled packet, the router copies the packet content into a special ICMP traceback message, adds its own IP address as well as the IP address of the previous and next-hop routers, and forwards the packet to the destination address. By combining the information obtained from the received ICMP traceback messages, the victim can then reconstruct the path back to the origin of the attacker.

This technique is more likely to be applicable for attacks that originate from a few sources and are of flooding-style attacks so that the receiver gets enough packets to reconstruct the attack path. To handle the situation of attackers sending their own ICMP traceback messages to mislead the destination, the iTrace scheme uses HMAC [10] and supports the use of X.509 Digital Certificates [11] for authenticating and evaluating ICMP traceback messages. The iTrace scheme suffers from two main concerns. The first concern is that ICMP traffic is increasingly getting filtered compared to normal traffic. The second concern is that if certain routers in the attack path are not enabled with iTrace, the destination would have to reconstruct several possible attack paths that have a sequence of participating routers, followed by one or more non-participating routers, and then followed by a sequence of participating routers.

### D. Packet Marking

In [9], the authors proposed a Probabilistic Packet Marking (PPM) scheme allowing the traceback of an attack flow. The baseline idea of PPM is that routers probabilistically write partial path information into the packets during forwarding. A marking field, large enough to hold a single router address, in the packet header is reserved. For IPv4, this would be a 32-bit field in the Options portion of the IP header. If the attack is made up of a sufficiently large number of packets and the route remains stable, the victim would receive at least one marked packet for every router in the attack path which makes it eventually able to the reconstruct the entire attack path. This allows victims to locate the approximate source of attack traffic without requiring outside assistance.

## VIII. A Generic Framework for Network Forensic Investigation

In [1], the authors propose a generic framework for network forensic investigation. The proposed framework aggregates many of the phases available in the already proposed digital forensic models [6-8] on which they built new phases specific to network forensics. As it is illustrated in figure 1, the proposed framework is composed of nine phases. In the following subsections, we present a detailed explanation for each of the considered phases:

### A. Preparation and Authorization

Network forensics is applicable only to environments where network security tools like intrusion detection systems, packet analyzers, and firewalls are deployed at various strategic points on the network. The staff handling these tools must be trained to ensure that maximum and quality evidence may be collected in order to facilitate the trace and attribution of network security attacks. Required authorizations to monitor the network traffic are obtained and a well defined security policy is in place so that privacy of individuals and the organization is not violated.

### B. Detection of Incident / Crime

The alerts generated by the deployed security tools, indicating a security attack or policy violation, are observed. Any observed anomalies will be analyzed. The presence and nature of the attack is determined from various parameters. A quick validation is done to assess and confirm the suspected attack. This will facilitate the important decision whether to continue the investigation or ignore the alert as false alarm. The confirmation of an incident yields two actions: incident response and network traces (evidences) gathering.

### C. Incident Response

The response to the detected security attack is initiated based on the information collected to validate and evaluate the incident. The response initiated depends on the type of attack and is guided by organization and legal policies. An action plan on how to prevent future attacks and recover from the existing damage is performed. At the same time, the decision whether to continue with the investigation and gather more information is also taken. This phase is applicable only to cases where an investigation is initiated while the attack is in progress and cannot be used after the crime notification.

### D. Collection of Network Traces

Networks traces are collected by the deployed network security tools (sensors). A well defined procedure using reliable hardware and software tools must be in place to collect maximum evidence causing minimum impact to the victim. The network must be monitored to identify future attacks. The integrity of captured data and logged network events must be ensured. Collection is the most difficult part as traffic data changes at a quick rate and it is not possible to generate the same trace at a later time. The amount of logged data will be enormous requiring huge memory space and system must be able to handle different formats appropriately.

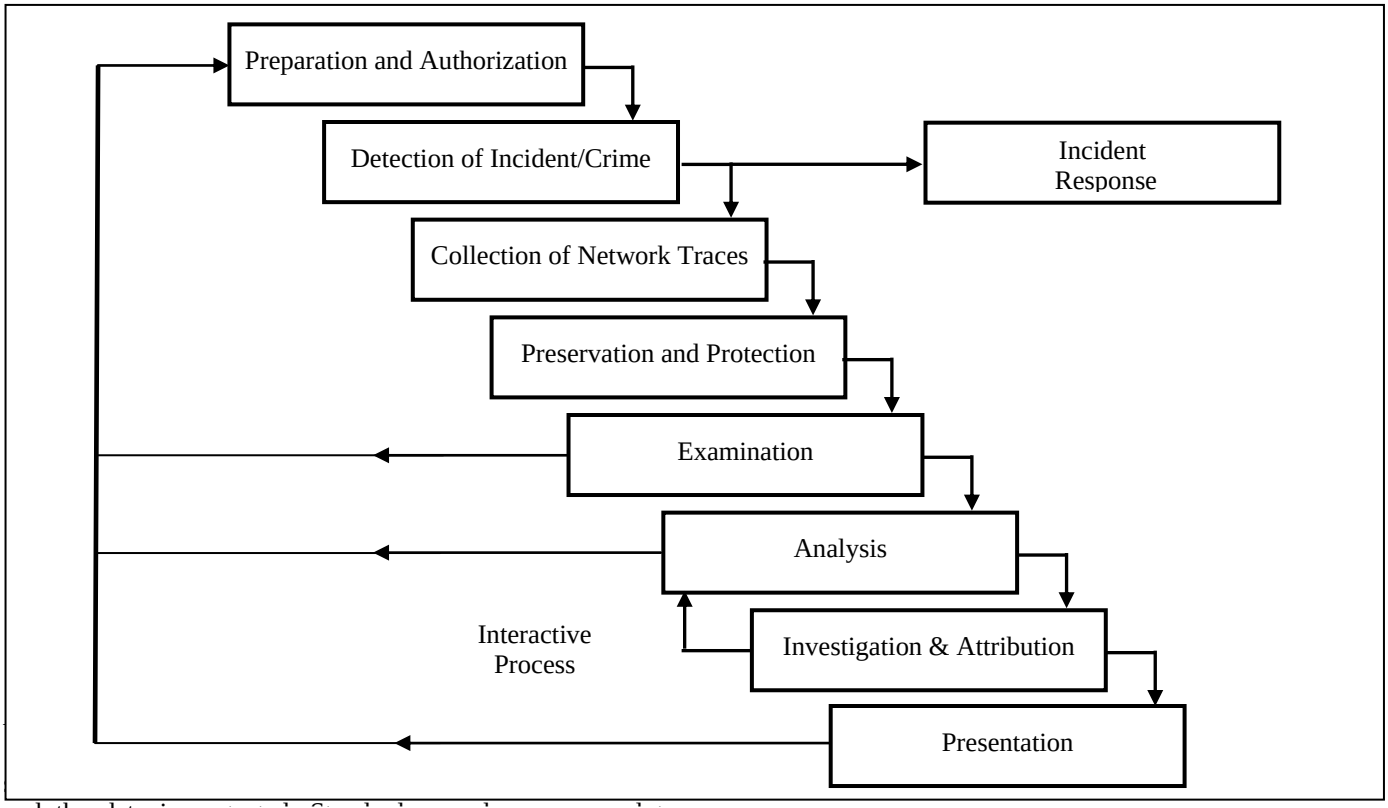


Figure 1: Generic Framework for Network Forensics

and the data is pr
ensure accuracy and
custody is strictly enforced so that there is no unauthorized use or tampering. Another copy of the data will be used for analysis and the original collected network traffic is preserved. This is done so that the investigation done may be proved again on the original preserved data to meet the legal requirements.

### *F. Examination*

The traces obtained from various security sensors are integrated and fused to form one large dataset on which analysis can be performed. Mapping and time lining of this data is also performed. This is done so that key information is not lost or mixed up. Data hidden or disguised by the attacker needs to be recovered. The collected data is classified and clustered into groups so that the volume of data to be stored may be reduced to manageable portions. It is easy to analyze large groups of organized data. Redundant information and unrelated data is removed and minimum representative attributes are identified so that the least information with the highest probable evidence needs analysis.

### *G. Analysis*

Collected evidences are methodically analyzed to extract specific indicators of the network intrusion. The extracted indicators are classified and correlated to deduce important observations using the existing attack patterns. Data mining and statistical approaches are used to search data and match attack models. Some of the important parameters are related to network connection establishment, protocol and operating system fingerprinting, packet fragmentation, installed software or rootkits, running rogue processes, etc. The attack patterns are put together and the attack is reconstructed and replayed to understand the intention and methodology of the attacker. The result of this phase is the validation of the suspicious activity.

### *H. Investigation and Attribution*

The information obtained from the analysis of the collected evidences is used to identify who, where, when, how and why of the incident. This will help in source traceback, reconstruction of the attack scenario and attribution to a source. The most difficult part of the network forensic analysis is establishing the identity of the attacker. Two simple strategies of the attacker to hide himself are IP spoofing and stepping stone attack. Researchers have proposed many IP traceback schemes to address the first attack and is still an open problem. Stepping stones are created by attackers to use compromised systems to launch their attacks. They can be detected using similarity and anomaly based approaches applied to packet

statistics. The approach of the investigation depends on the type of attack.

### *I. Presentation and Review*

The observations are presented in an understandable language while providing explanation of the various procedures used to arrive at the conclusion of the investigation process. The systematic documentation is also included to meet the requirements. The conclusions may also be presented using visualization so that they can be easily grasped. A detailed review of the incident is done and counter measures are recommended to prevent similar incidents in future. The results are documented to influence future investigations and network security policy.

## IX. CONCLUSION

In this paper we have presented an overview about the main tools and techniques available to ensure forensic analysis of network security attacks. Given that Web and Email services are the most common used network communication services, we mainly focused on the forensic investigation of Email and Web services attacks. In addition, we presented a set of forensics tools used for network traffic sniffing such as Snort, Pcap, TcpDump, and Ethereal. Moreover, the paper presented the major existing IP traceback schemes designed to trace back to the origin of an IP packet through the Internet. In addition to the survey of network forensics tools, the paper presented a generic framework proposed for network forensic analysis.

## REFERENCES

[1] Emmanuel S. Pilli, R.C. Joshi, and Rajdeep Niyogi, "A Generic Framework for Network Forensics", 2010 International Journal of Computer Applications (0975 – 8887), Volume 1 – No. 11

[2] Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore, "Tools and Techniques for Network Forensics", International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,April 2009

[3] Yong Guan, "Network forensics", chapter 20, Computer and Information Security Handbook, Publisher: Morgan Kaufmann, Pub. Date: May 22, 2009, Print ISBN-10: 0-12-374354-0, Web ISBN-10: 0080921949

[4] Sriranjani Sitaraman, Subbarayan Venkatesan, "Computer and Network Forensics", chapter III, Digital crime and Forensic Investigation in Cyberspace Book, Edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos, 2006, ISBN-10: 1591408725.

[5] Thomas M. Chen, Chris Davis, "An Overview of Electronic Attacks", chapter 1, Digital crime and Forensic Investigation in Cyberspace Book, Edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos, 2006, ISBN-10: 1591408725.

[6] Baryamureeba, V. and Tushabe, F. 2004. The enhanced digital investigation process model. In Proceedings of the 4th Digital Forensic Research Workshop, USA, 2004.

[7] Casey, E. and Palmer, G. 2004. The investigative process. in Casey, E. ed. Digital evidence and computer crime, Elsevier Academic Press, 2004.

[8] Ciardhuáin, S.Ó. 2004. An extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3 (1), 2004.

[9] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," IEEE/ACM Transactions on Networking, Vol. 9, No. 3, pp. 226–237, June 2001.

[10] US Department of Commerce, Federal Information Processing Standards, Publication 198, The Keyed-Hash Message Authentication Code (HMAC), March 6 2002.

[11] C. Adams, Internet X. 509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, Available at http://www.ietf.org/

[12] S. Bellovin, M. Leech and T. Taylor, ICMP Traceback Messages, Internet Draft, February 2003.

[13] S. Mitropoulos, D. Pastos and C. Douligers, "Network Forensics: Towards a Classification of Traceback Mechanisms," *Proceedings of the Workshop on Security and Privacy for Emerging Areas in Communication Networks*, pp. 9 – 16, Sep 2005.

[14] Riverbed Technology. "WinPcap: The industry-standard windows packet capture library" Internet: http://www.winpcap.org, Dec. 22nd 2012.

[15] Riverbed Technology. "AirPcap: 802.11 Wireless Packet Capture Device" Internet: http://www.riverbed.com/us/products/cascade/wireshark_enhancements/airpcap.php, Dec. 22nd 2012.

[16] S. Ansari, S. Rajeev and H. Chandrasekhar, "Packet Sniffing: A Brief Introduction," *IEEE Potentials*, Vol. 21, No. 5, pp. 17 – 19, Dec 2002/Jan 2003.

[17] OLEX: Open Logic Exchange. "Ethereal - Network Protocol Analyzer" Internet:http://olex.openlogic.com/packages/ethereal, Dec. 22nd 2012.

[18] Visualware. "eMailTrackerPro: Email tracing and spam filtering" Internet: http://www.emailtrackerpro.com, Dec. 22nd 2012.

[19] Tamos. "SmatWhois" Internet: http://www.tamos.com/products/smartwhois/, Dec. 22nd 2012.

[20] Mandiant. "Web Historian" Internet: http://www.mandiant.com/resources/download/web-historian, Dec. 22nd 2012.

[21] Softonic International."Index.dat analyzer" Internet: http://index-dat-analyzer.en.softonic.com/ , Dec. 22nd 2012.

[22] Palmer, G. 2001. A Road Map for Digital Forensic Research, 1st Digital Forensic Research Workshop, (New York, 2001), 15-30.

[23] M. Ranum, Internet: http://www.ranum.com/security, Dec. 22nd 2012.

[24] [24].G. Palmer, "A road map for digital forensic research," Digital Forensic Research Workshop (DFRWS), Final Report, Aug. 2001.

[25] C. M. Whitcomb, "An historical perspective of digital evidence: A forensic scientist's view," IJDE, 2002.

[26] S. Mocas, "Building theoretical underpinnings for digital forensics research," Digital Investigation, Vol. 1, pp. 61–68, 2004.

[27] Pallavi Kahai, Kamesh Namuduri, Ravi Pendse, "Tracing Cyber Crimes with a Privacy-Enabled Forensic Profiling System", chapter VII, Digital crime and Forensic Investigation in Cyberspace Book, Edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos, 2006, ISBN-10: 1591408725.

[28] Garfinkel Simson, "Network Forensics: Tapping the Internet", Internet: http://www.oreillynet.com/pub/a/network/2002/04/26/nettap.html?page=1, Dec. 22nd 2012