COMP8677-1-CS-2019S
NETWORKING AND DATA SECURITY
ESSAY: NETWORK FORENSICS- FOUNDATIONS, TERMINOLOGY AND EXAMPLES

University of Windsor

Professor:
Dr. Robert Kent

Submitted By,
Chandra Sekhar Chunduru – 104918812
Date: June 15, 2019

Network Forensics-Foundations, Terminology and Examples

Chandra Sekhar Chunduru (104918812)
Department of Computer Science
(Master of Applied Computing)
University of Windsor
Windsor, Canada
chundurc@uwindsor.ca

***Abstract*-- Network forensics is emerging as a new discipline that primarily focuses on monitoring, capturing, recording, and analysis of network traffic. It provides a path to find out the cybercriminals through analysis and traceback of collected network evidence. It is the use of scientifically proved techniques to collect and analyse the traffic flow such as network packets and events for investigative purposes. It is an enhancement to the traditional security models used in organizations to prevent data loss and prevent external attacks. The network forensics tools and approaches are expensive and time taking. However, network forensics deals with velocity and veracity of data. It supports organizations to investigate external and internal attacks. It is also important for every organization to have strict laws to protect data integrity. This paper is structured as follows: It starts with the framework and process models. Secondly, the differences between the computer and network forensics. In the later section, the various tools and techniques are presented. The challenges, applications are addressed in the final section.**

***Keywords*—Framework, Forensic Models, Computer Forensics, Tools, Techniques, Challenges, Applications**

I. INTRODUCTION

In today's rapidly growing world with many technological advancements, internet is the most essential means for faster communication between the users or machines, faster transaction speeds but it is unfortunately the major victim for the cybercrimes. The field of forensic science is very broad in which digital forensics plays a vital role. The term forensic is derived from the Latin word "forensic" in mid-17th century which means in open court or public. Forensic science is a detailed analysis of past events which involves scientific technologies that are helpful to generate precise information and disclose the event details happened at the crime scene. Once a crime is committed, the investigators will visit the site and analyse the crime scene. The witness is identified and taken into official custody for investigation and once this step is completed the perpetrator is arrested. The final step is to take notes about the scene. It may not be the eyewitness the key source of information at all the time. A Forensic Scientist is a person who performs these activities, collects the evidences and preserve them for future analysis. The following role of forensic science during the crime investigations are related to computer and network. Network forensics is introduced to carry on the investigation activities specially over the internet. It needs special infrastructure to analyse the network packets and devices. It is of a great importance for today's organizations which is discussed below. On one hand, it helps us to know the details ensuring similar future attacks are prevented. Additionally, network forensics is essential for investigating insiders' abuses which constitute second costliest type of attack within organizations [1 n/w for: notions n challenges].

This paper is structured as follows. First, the importance and terminology involved in network forensics is presented in section II and section III. Then, the difference between computer and network forensics is discussed along with the framework in section IV. In section V, the types, tools and techniques are comprehended. Then, in section VI, challenges in related to network forensics are highlighted. In section VII and section VIII, main applications and conclusion are mentioned.

II. IMPORTANCE OF NETWORK FORENSICS

In this 21st century, there is significant rise in the number of cybercrime incidents especially over the networks. According to the survey conducted in Canada in the year 2017, the statistics on the impact of cybercrime over Canadian businesses in 23 sectors were calculated. Out of these 68% of the business have network security, 74% of the business have E-mail security and 45% have Web Security. However, majority of them faced issues such as additional repairs or recovery costs, preventing the employees from doing their tasks [1]. These statistical analysis of network related data can be very useful to the organization in the long run to extract interesting insights for further research in organizations. The primary objective of network forensics is to replay the attack and understand the tools and techniques used by the intruder while attacking the devices. So, we can extract the meaningful information from each of the network devices.

III.TERMINOLOGY

Network Forensics is the subset of digital forensics which mainly focusses on the intrusion activities in the internet. As per **National Institute of Standards and Technology (NIST)**, it is considered as the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. It involves

many activities like capturing the packets, filtering them based on certain criteria and finally analyzing them to find the valid source as an evidence to be accepted in the court of law. There are many tools and techniques available to collect and analyze the network packet data. In this paper the terms, process framework and the various techniques related to network forensics with challenges involved are discussed.

IV. DIFFERENCE BETWEEN COMPUTER AND NETWORK FORENSICS

As the data is constantly emerging and most of it is unstructured, there should be a solution to organize the data while retaining its integrity. The connection between the data and forensic science is very unusual. The data in the computer forensics is static (data at rest) and generally preserved once there is a loss of power while in network forensics it is commonly believed notion that the data is constantly changing over time. In the former one, the process involved in identifying the evidence is stored locally i.e. in the file system while on the other hand in network forensics it is hard to find out as it is stored at various locations which cannot be easily determined. Unlike other are of digital forensics, the network forensics involves the analysis of logs. It needs some arrangements to be made ahead to analyse the network flow without storing a copy of the data. For example, consider an instance of not having a CCTV footage at the crime scene, then our total process of solving the issue will depend on the circumstantial evidence. In its presence, the entire crime scene can be reconstructed, and it becomes easier for the investigator to extract crucial information to solve the case and finally identify the criminal. In a nutshell, there are many different branches in digital forensics with each area having their own importance, applications, tools and techniques [2].

A GENERIC PROCESS FRAMEWORK FOR NETWORK FORENSICS

1.The Need for Framework:

A Generic framework for network forensic analysis is needed as this field is slowly emerging as an independent discipline. The previous digital forensics methodologies developed dealt with data stored locally on disks and file systems. In the initial times, the computer forensic investigator had the access to specialized tools which the attacker lacked but the network forensic investigator is having access to the same tools as the intruder. The difference between both lies in the ethics and purpose of the attack. This field has emerged in response to the illegal attacks to discover and identify the properties of the source of these attacks. The figure 1 shows the framework which contains a database to store all the packets obtained from the network traffic monitor. The conclusion database will obtain the results based on the user input analysis and finally will generate reports. Therefore, a special framework to address the need of network analysis is mandatory as it is self-reliant when referred to the computer forensics [3].

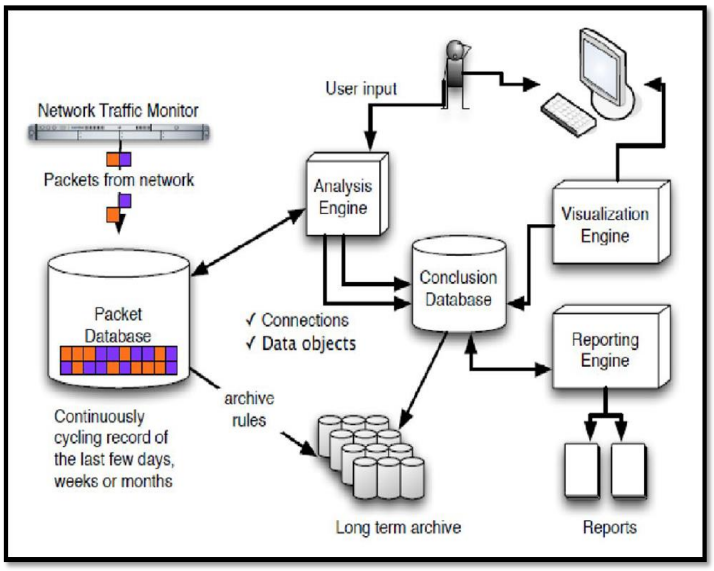

Figure 1 Generic Process Framework [21]

2.Process Flow Involved in Framework Model

The process model developed for network forensics is generic as it is organized into many steps which are combined into phases. The phases are common to the digital forensics model, but the function of each phase is designed especially for the network forensics. In total it comprises of nine phases as shown in the figure 3. Each phase with the function needed to be performed is explained in this section.

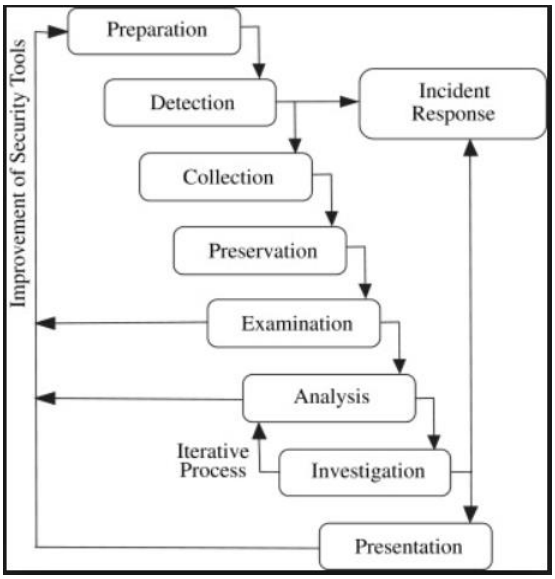

Figure 2 Network Forensics process model [21]

2.1 Preparation and Authorization:

This step involves identifying the environment in which the various strategic tools such as packet analyzers, firewalls

used in various parts of the network. The primary objective of this phase is to obtain the necessary authorization and legal warrants to guarantee the privacy and integrity of the data. The security policy is laid out to ensure the required authorizations and to monitor the network traffic so that the privacy of individuals and the organization is not violated. The behaviour and strategies used by the attackers are learnt.

2.2 Detection of Incident / Crime:
The security tools used generate alerts, which indicates the security policy violation or breach. In this phase such anomalies are analyzed depending on various parameters. A quick validation is performed to take the necessary decision whether to investigate further or ignore the alert as false alarm. The confirmation of an attack will lead to two outcomes– incident response and collection of data. The necessary precautions should be employed to alteration of the evidence obtained.

2.3 Incident Response:
The response to incident is initiated based on type of attack identified with adhering to all the organizational and legal policies. A plan of action is developed to sustain from such incidents in the future. Additionally, the decision whether to continue with the investigation and gather more information is also taken. This phase is only performed during the attacks [3].

2.4 Collection of Network Traces:
This step is very crucial and considered to be the most difficult to be performed. It required many reliable tools and strong procedures as it is difficult to generate the same trace logs at a later point of time. The primary reason for this cause is that data is dynamic and volatile, and it is not stored anywhere to obtain the previously found log trace. The amount of log data collected is very huge and required special storage to handle different data formats.

2.5 Protection and Preservation:
This step addresses the need of data for future use by storing them on a secondary storage for backup purpose. A hash function for all the traced data is calculated due to which the data is protected. The procedures defined ensures the veracity of the data. A strict law is enforced so that there is no unauthorized use or tampering.

2.6 Examination:
This phase is an extension to the previous phase. It ensures that no crucial information is lost or mixed with any other data. If there is any altered data by the attacker then such data is identified and the high volume of information is reduced in steps to identify the most relevant evidence.

2.7 Analysis:
The evidence found is searched systematically to find out the hints on which important observations are made. The attacking patterns are derived from the statistical analysis and on using some data mining algorithms. Some of the important parameters are related to network connection establishment, DNS queries, packet fragmentation, protocol and operating system fingerprinting, running rogue processes, installed software or rootkits. Then finally, all the patterns obtained are combined to rebuild and replay the attack to understand the instincts and methods used by the hacker. The output phase from this phase is the accord of such unusual attack.

2.8 Investigation and Attribution:
The information obtained from the evidence traces is used to identify who, what, where, when, how and why of the incident. This obtained information acts as the source to traceback, reconstruct the attack scenario and attribution. The toughest part of the network forensic analysis is identifying the attacker. The commonly used strategies by the attacker are IP spoofing (hiding) and stepping stone attack. Researchers have initiated many IP traceback schemes to reduce the number of first type of attack but still the problem persists. The approach to carry on the investigation is totally dependent on the nature of the attack.

2.9 Presentation and Review:
It is the final stage of the model which involves documentation and illustration of steps followed until this step in a comprehensible and clear format. Every piece of information presented should be confined with the legislation and policies along with the future recommendations to prevent such attacks from occurring.

V. NETWORK FORENSICS ANALYSIS

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation. Network investigation deals with volatile and dynamic data.

5.1 Network Forensics Analysis Tools:
The tools that allow administrators to monitor the networks, gather all information about anomalous traffic, assist in network crime investigation and help in generating a suitable incident response. These tools are called as the Network Forensics Analysis Tools (NFATs). NFATs are used to analyze the collected and aggregated data from various security tools. These provide IP security, detect inside and outside attack in the system, carry out risk analysis, data recovery, anomaly detection, prediction of future attacks and detect attack patterns etc.

There are several tools and the selection among them to analyze a specific attack depends on the available attack data sources like network trace, OS logs, application, log, binaries etc., and the objectives of the analysis (e.g., extract attack intelligence, redesign firewall rules, redesign security policy, collect digital evidence). The following are some of the tools

we could use to analyze a network:

5.1.1 NetIntercept
NetIntercept captures whole packets and reassembles up to 999,999 TCP connections at once, reconstructing files that were sent over your network and creating a database of its findings. It recognizes over 100 types of network protocols and file types, including web traffic, multimedia, email, and IM.

5.1.2 NetDetector
NetDetector is a full-featured appliance for network security surveillance, signature-based anomaly detection, analytics and forensics. It complements existing network security tools, such as firewalls, intrusion detection/prevention systems and switches/routers, to help provide comprehensive defense of hosted intellectual property, mission-critical network services and infrastructure.

5.1.3 IRIS
IRIS Network Monitoring Tools are the perfect combination of powerful features and network-friendly resource consumption. In other words, IRIS makes it possible to get thorough, detailed data from your network at any time, without compromising on the levels of service you expect.

5.1.4 SilentRunner
SilentRunner is a network discovery and analysis tool designed to safeguard a company's information assets. identifies security risks and network vulnerabilities and alerts management to potential loss of data. It is the only security system that enables a rapid response to protect a company's assets by quickly correlating complex network events and displaying readily understood graphics. When combined with firewalls and intrusion detection systems, SilentRunner effectively completes the total network security suite [4].

5.1.5 Netwitness
The RSA Netwitness Platform provides real-time visibility into all network traffic in the cloud and across virtual infrastructure—eliminating blind spots. To make it easier for analysts to rapidly detect legitimate, high-risk threats in all this network data, RSA Netwitness Network parses network data at capture time into various sessions of metadata and enriches it with threat intelligence and contextual information about your business [5].

5.1.6 Network Miner
Network Miner is a Network Forensic Analysis Tool for Windows. Network Miner can be used as a passive network sniffer/packet capturing tool to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network [6].

5.1.7 PyFlag
PyFlag is a general purpose, open source, forensic package which merges disk forensics, memory forensics and network forensics. It is a web-based, database-backed forensic and log analysis GUI and Computer forensics framework written in Python which stores disk images in numerous file formats, including raw, sgzip, AFF, and EnCase format.

5.1.8 SiLK
SiLK, the System for Internet-Level Knowledge, is a collection of traffic analysis tools developed by the CERT Network Situational Awareness Team (CERT NetSA) to facilitate security analysis of large networks. The SiLK tool suite supports the efficient collection, storage, and analysis of network flow data, enabling network security analysts to rapidly query large historical traffic data sets. SiLK is ideally suited for analyzing traffic on the backbone or border of a large, distributed enterprise or mid-sized ISP [7].

5.2 Network Forensics Techniques:
Network forensic techniques help in tracking different types of cyber attack by monitoring and inspecting network traffic. However, with the high speed and large sizes of current networks, and the sophisticated philosophy of attackers, copying normal behaviour and/or erasing traces to avoid detection, investigating such crimes demands intelligent network forensic techniques. This paper suggests a real-time collaborative network Forensic scheme (RCNF) that can monitor and investigate cyber intrusions. The scheme includes three components of capturing and storing network data, selecting important network features using chi-square method and investigating abnormal events using a new technique called correntropy-variation. We provide a case study using the UNSW-NB15 dataset for evaluating the scheme, showing its high performance in terms of accuracy and false alarm rate compared with three recent state-of-the-art mechanisms [8]. The following are different techniques proposed for network forensics in various research articles.

5.2.1 Email Forensics:
Emails are one of the most common medium of communication in this digital era. They are now being used for all sorts of communication, including provision of confidentiality, authentication, non-repudiation and data integrity. Emails are more vulnerable to be intercepted and might be used by hackers to learn of secret communication. Spam emails are a major source of focus within the Internet community. Email forensics refers to studying the source and content of electronic mail as evidence, identifying the actual sender and recipient of a message, date/time it was sent. Emails frequently contain links and codes of malicious viruses, threats and scams that can result in the loss of data, confidential information and even identity theft. The following are various tools that are used to identify the point of origin of the message, trace the path travelled by the message and to identify various phishing mails that try to obtain the confidential information of the users.

5.2.1.1 eMailTrackerPro:

It is a tool used in analyzing the headers of various email messages that are received, to disclose the original sender's location. It will trace the route in which the message has arrived using the email header. A basic trace will be shown on the main Graphical User Interface and a summary report can be obtained. The output report includes the geographic location of the IP address from where the email was sent and the domain contact information.

5.2.1.2 SmartWhois:

It is a network information utility that allows you to lookup all the available information about an IP address, hostname or domain, including address of the network provider and administrator. It is capable of caching query results, which reduces the time needed to query an address. In some cases, one can use SmartWhois along with eMailTrackerPro if the information provided by anyone of them is not clear.

5.2.2 Web Forensics:

The investigation of criminal activity that has occurred on the web is referred to as Web Forensics. It deals with the analysis of various contents, patterns and transmission paths of web pages including the browser history, web server scripts and header messages. This deals with the gathering of all the important information related to a particular crime and inspect the browser history of a person and get the plots of various factors such as the number times a web page has been visited, the duration of each visit, the files that have been uploaded and downloaded from that site, cookies that are setup and some other critical information [9].

a. Mandiant Web Historian:

It is a tool that allows users to extract, view and analyze different URLs on the histories of all the browsers available on the computer. This tool helps in determining what, where, when and how the hackers explored various sites. It parses a specific history file or find all the browser history files that the tool knows and generates a report that contains the internet activity from all the browser history files it can locate.

b. Index.dat Analyzer:

It is a tool that is used to view, examine and delete the contents of its files that are called as index.dat files.Index.dat files are some hidden files on a computer that contain all tracks of online activity when one uses the internet on the system. They maintain data of where you have been on the internet, what sites you have visited, list of all URLs, files and documents that are recently accessed. This tool provides support to directly visit the listed website and find files that are uploaded and downloaded from it. In addition to these two tools, there exist tools like Total Recall, which can be used to extract the list of favourite websites stored in the browser history.

5.2.3 Packet Sniffers:

Packet sniffers or protocol analyzers are tools that are commonly used by network technicians to diagnose network-related problems. Packet sniffers can also be used by hackers for less than small purposes such as spying on network user traffic and collecting passwords. Packet sniffers come in a couple of different forms. Some which are used by network technicians are single-purpose dedicated hardware solutions while other ones are software applications that run on standard consumer-grade computers, utilizing the network hardware provided on the host computer to perform packet capture and injection tasks.

Packet sniffers work by intercepting and logging network traffic that they can 'see' via the wired or wireless network interface that the packet sniffing software has access to on its host computer. The information gathered from a Packet Sniffer will significantly help a Network Administrator troubleshoot and fix network errors in a smaller span of time by understanding what is going over the wire as well as source/destinations.

The following are some of the packet sniffing tools that are available in the market:

- SolarWinds Packet Analysis Bundle
- WireShark
- PRTG Network Monitor
- Steel Central Packet Analyzer
- Tcpdump
- Kismet
- Fiddler
- EtherApe
- Packet Capture

Hackers can use sniffers to spy on unencrypted data in the packets to see what information is being exchanged between two systems. They can also capture information such as passwords and authentication tokens. Hackers can also capture packets for later playback in replay, man-in-the-middle, and packet injection attacks that some systems may be vulnerable to [10].

VI. CHALLENGES IN NETWORK FORENSICS ANALYSIS

An essential aim for a forensic investigator is to see how a criminal offense was undertaken – to spot the actors concerned, how the crime unfolded and to develop a chronology of the incident. The tools are developed particularly for the investigators. the knowledge provided by the tools should be at a really abstract level discarding the technical intricacies. Once an attack has been detected, the quantity of knowledge concerned makes rhetorical analysis a tough task [11]. The complexness downside in Network forensics is that the info nonheritable is usually at rock bottom level i.e. in a very raw format, that is commonly too tough for humans to know. The number downside in Network Forensics is that the amount of knowledge to be analyzed are

often substantial [11]. A key challenge in network forensics is to initial make sure that the network is forensically prepared. For an undefeated network investigation, the network itself should be equipped with AN infrastructure to totally support this investigation [14], [13], [15], [16], [17]. The infrastructure ought to make sure that the required data exists for a full investigation. Planning a network forensic infrastructure is commonly a difficult task as a result of the various potentialities in this design space. The subsequent could be a transient description of a number of these challenges:

1. Data sources: A typical network has many attainable sources of knowledge which has raw network packets, logs of network devices and services. Though it's fascinating to gather information from all the possibles sources, this option isn't forever possible, particularly for big networks. Therefore, a very important call is to pick a set of information sources which provides sensible coverage of the network and makes the gathering processes sensible.

2. Data granularity: A connected issue while choosing data sources is to determine on what proportion details ought to be unbroken. for example, once aggregation network packets, one could collect whole packets, packets' headers, association data (IP addresses, port numbers), etc. just like the higher than item, keeping in-depth information details isn't sensible in massive networks.

3. Data integrity: it's essential to confirm the integrity of the collected data. The end result of the forensics method will be adversely affected if the collected information is altered either deliberately or accidentally. Therefore, measures have to enforced to confirm information integrity throughout and once data assortment and analysis.

4. Data as Legal Evidence: exploitation the collected data internally at intervals a company is kind of completely different from presenting the info in a very court of law. Within the latter case, the collected information has got to pass tight legal procedures to qualify as proof in an exceeding court of law. They need to pass an acceptableness test; a screening method by the court [12], [18].

5. Privacy Issues: Collected information is predicted to incorporate sensitive data like personal emails and files. Therefore, the right handling of that information is crucial. The information has got to be protected by access management measures, so only licensed personnel to possess access.

6. Data Analysis: a serious challenge is analyzing the collected data so as to supply helpful data that can be utilized in a decision-making method. Such an analysis method is absolutely difficult because of the complexness of a typical network setting and also the quantity and variety of knowledge concerned. Innovative tools are required to assist human investigators to research the info. These tools could apply techniques from completely different fields like data processing [19], and knowledge visual image [20].

VII. APPLICATIONS OF NETWORK FORENSICS

The use of network forensics is not restricted to a single domain. As this field is functionally dependent on the internet, it has a purpose to serve where the use of the internet plays a vital role. The most common sectors that are more reliant on networks are hospitality, educational, private and government organizations. By using the different forensic tools available, the network traffic and active logs can be inspected. These tools not only help the researchers to save their crucial time but also facilitates in proposing new techniques and develop more advanced tools in the future. Overall, Network Forensics has rapidly emerged as a discipline with a wide variety of applications.

VIII. CONCLUSION

Nowadays with the increased dependence on electronic devices, there is a huge amount of data which must be stored, monitored and controlled at regular time intervals. For instance, the organizations collecting personal data need to enforce strict security policies to ensure the privacy and integrity of the data. In such instances, network forensics plays a vital role. Although it is emerging as a new discipline, it always requires constant enhancement to meet the future technological needs to develop more advanced models and tools. There are many challenges to overcome in developing a framework for network forensics models which needs to be the primary focus for research interest in the future.

REFERENCES

[1] "Cyber Security and Cybercrime in Canada, 2017", *Www150.statcan.gc.ca*, 2019. [Online]. Available: https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm. [Accessed: 14- Jun- 2019].

[2] "{{metadataController.pageTitle}}", *Subscription.packtpub.com*, 2019. [Online]. Available: https://subscription.packtpub.com/book/networking_and_servers/9781782174905/1/ch01lvl1sec12/differentiating-between-computer-forensics-and-network-forensics. [Accessed: 14- Jun- 2019].

[3] *Ijcaonline.org*, 2019. [Online]. Available: https://www.ijcaonline.org/journal/number11/pxc387408.pdf. [Accessed: 14- Jun- 2019].

[4] *News.hitb.org*, 2019. [Online]. Available: https://news.hitb.org/content/raytheons-silentrunner-computer-forensic-software-receives-patent. [Accessed: 14- Jun- 2019].

[5] N. Response and V. President Infosys, "Network Threat Detection and Response", *RSA.com*, 2019. [Online]. Available: https://www.rsa.com/en-us/products/threat-detection-response/network-security-network-monitoring. [Accessed: 14- Jun- 2019].

[6] "NetworkMiner - The NSM and Network Forensics Analysis Tool ⛏", *Netresec*, 2019. [Online]. Available: https://www.netresec.com/?page=networkminer. [Accessed: 14- Jun- 2019].

[7] "SiLK", *Tools.netsa.cert.org*, 2019. [Online]. Available: https://tools.netsa.cert.org/silk/. [Accessed: 14- Jun- 2019].

[8] 2019. [Online]. Available: https://www.researchgate.net/publication/320944549_RCNF_Real-time_Collaborative_Network_Forensic_Scheme_for_Evidence_Analysis. [Accessed: 14- Jun- 2019].
[9] "Internet forensics Definition from PC Magazine Encyclopedia", *Pcmag.com*, 2019. [Online]. Available: https://www.pcmag.com/encyclopedia/term/59910/internet-forensics. [Accessed: 14- Jun- 2019].
[10] "What Are Packet Sniffers and How Do They Work?", *Lifewire*, 2019. [Online]. Available: https://www.lifewire.com/what-is-a-packet-sniffer-2487312. [Accessed: 14- Jun- 2019].
[11] *Pdfs.semanticscholar.org*, 2019. [Online]. Available: https://pdfs.semanticscholar.org/3d85/6c75456afc1689c464656ed12df2f0916375.pdf. [Accessed: 15- Jun- 2019].
[12] P. Sommer, "downloads", Pmsommer.com, 2019. [Online]. Available: http://www.pmsommer.com/page7.html. [Accessed: 15- Jun- 2019].
[13] Dfrws.org, 2019. [Online]. Available: http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf. [Accessed: 15- Jun- 2019].
[14] Ncjrs.gov, 2019. [Online]. Available: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. [Accessed: 15- Jun- 2019].
[15] 2019. [Online]. Available: https://www.researchgate.net/publication/222400826_A_hierarchical_objectives-based_framework_for_the_digital_investigations_process. [Accessed: 15- Jun- 2019].
[16] R. Montasari, "An ad hoc detailed review of digital forensic investigation process models", 2019.
[17] P. . S. Kapse, "Survey on Different Phases of Digital Forensics Investigation Models", 2019.
[18] "RFC 3227 - Guidelines for Evidence Collection and Archiving", Datatracker.ietf.org, 2019. [Online]. Available: https://datatracker.ietf.org/doc/rfc3227/. [Accessed: 15- Jun- 2019].
[19] "Tan, Steinbach & Kumar, Introduction to Data Mining | Pearson", Pearson.com, 2019. [Online]. Available: https://www.pearson.com/us/higher-education/program/Tan-Introduction-to-Data-Mining/PGM93748.html. [Accessed: 15- Jun- 2019].
[20] Www2.cs.arizona.edu, 2019. [Online]. Available: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic13-final/slides.pdf. [Accessed: 15- Jun- 2019].
[21] *Etd.repository.ugm.ac.id*, 2019. [Online]. Available: http://etd.repository.ugm.ac.id/downloadfile/69906/potongan/S3-2014-276445-bibliography.pdf. [Accessed: 15- Jun- 2019].