An Anatomy for Recognizing Network Attack Intention

Anchit Bijalwan, Satenaw Sando, Muluneh Lemma

Abstract*: *Research in the field of Network forensics is tremendously expanding with the tendency to help in arbitrating, capturing and detaining the exponential growth of the cyber crimes. With this expansion, the field of Network forensics is still not clear and is uncertain. In this paper, we have presented the architecture of an analysis mechanism for network forensics. The work followed by generic process model for network forensics investigation is also presented and discussed in detail. Overall this paper presents an overview of the network forensics architecture, generic process models to help a user in the times of emergency by considering the incident and thus maintaining the privacy and security policies.

Index Terms*: *Network Forensics, Attack Intention, Traceback, Attribution, Incident response.

I. INTRODUCTION

Internet has experienced tremendous growth on conventional attacks in this decade which ravaging the confidentiality, integrity and availability of many services. These attacks target the user alongside the enterprises and the organizations too. This causes exploitation on the security related to the internet systems and its services e.g. web and cloud etc. These attacks causes economical lose to businesses and have a very bad impact on internet related buisness, security and the related infrastructure.

On 28 September 2018 will be known as black Friday. There were 50M accounts had been attacked by hackers. The breaches found after few days. Users had been affected when they re-login the account on the same day. Later on facebook revealed that the app which user were taking for a login, not looking as already being compromised by the attackers. These kinds of issue were being taken by the attackers several times in yesteryears. The attackers exploited the vulnerability to get the code of facebook which is related to one of the feature such ‘as view as’. This feature is designed to the user to see how their profile looks on other’s account. As and when the user will access this feature, the attacker will be able to steal the access token of your account and he will be able compromised your facebook account.

Distributed Denial of Services (DDOS) attacks are besetting today’s growing economy alongside the users capability towards producing more output. These DDOS attacks on social media such as twitter, facebook etc. are recent headlines. In July 2014, arbor network produces global DDOS attack data retrieved from its collection and illustrations, threatening and monitoring the infrastructure and its shows a flood in measuring and determining the initial half annual attacks in 2014 with over 100 attacks larger than 100 GB/sec were reported.

According to NSFOCUS, high volume and high rate DDOS attacks were increasing tremendously in the first half of 2014. Most of the attack hit industry and media by the DDoS attack traffic. On MAY 21 2014, the senior VP & general managerin security, Stuart Scholly at AKAMAI referred that distributed denial of services proliferators contingent rarely upon conventional botnet infection which was hinge on reflection and amplification techniques. According to them, instead of using the network of zombie computers, DDOS attackers abuse the internet protocols that are available on the servers as well as the devices. According to Ameen Pishdadi, founder of DDOS protecting leader GigeNET on Sep 23, 2014, the most popular attacks that were seen are DNS reflection and NTP. NTP attacks were very huge at the beginning of the year and were actually larger than the normal.

PLXsert on May 23, 2014 , has spotted 14 SNMP DDOS attacks undertaken targeting umpteen industries including hosting, consumer products, gaming and software-as-a-service (SaaS) as well as infrastructure as a service mostly in the US (49.9%) and China (18.49%). On Feb 11, 2014, according to a twitter post by Cloudfare CEO Matthew Prince, the full volume of the DDOS attack has exceeded 400 GB/sec which made this maximum distributed denial of service attack ever recorded till that time. This attack uses the NTP (network time protocol) reflection. It is exactly the same process as attacks taken that time for gaming sites.

DDOS attacks are quickly becoming the serious threats and the pain point for the industries. DDOS attacks are becoming more effective and causing the major disruption and sometimes brings down the organizations for the entire working days. If the organizations and enterprise wants to provide the uninterrupted service to their customers, they need to take this threat very seriously.

Through Network Forensics, we are able to analyze how the attack occurred, the duration of the attack and exploiting it, who was involved with the attack and the method used for the attack. Network Forensics implementation is like using a network time machine that allows you to go back to a particular time point and regenerate the series of events that showed at the time of a breach. Network Forensics is used as a tool for monitoring the activities, specifying the source of attacks and analysis and detecting them. Various Network Forensics tools can be used to capture the packets, analyze and investigate them. Network forensics is an extended phase of the network security. Network security protects the system against attacks while Network Forensics main focus is to record the evidence of the attack. Deep learning technique is also the best

Revised Manuscript Received on September 15, 2019

Anchit Bijalwan, Faculty of Electrical & Computer Engineering, Arba Minch University, Arba Minch, Ethiopia.

Satenaw Sando, Faculty of Electrical & Computer Engineering, Arba Minch University, Arba Minch, Ethiopia.

Muluneh Lemma, Dean Research, AMIT, Arba Minch University, Arba Minch, Ethiopia.

Retrieval Number: C4022098319/19©BEIESP
DOI:10.35940/ijrte.C4022.098319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

possible way for intrusion detection [1].

The aim of this work is to provide the detailed overview about the Network Forensics and to present the various aspects of it such as collection, detection, preservation, analysis, investigation etc. This paper is grouped as follows: Section I describes introduction, Section II gives the background study. It describe network forensics mechanism in section III, Section IV describes generic framework for network forensics investigation, and Section V shows the analysis for the network forensics, the Investigation in section VI and research challenges and research article is concluded in section VII.

II. BACKGROUND STUDY

Network forensics is the field of research that tremendously expands with the tendency to help in arbitrating, capturing and detaining the exponential growth of the cyber crimes. With this expansion, the field of Network forensics is still not clear and is uncertain. This section describes the definition, taxonomy and motivation for this upcoming field.

A. Definition

Network forensics is very important and emerging terminology now days when people are tormented with the different kind of network attack. Network Forensics is the science which starts after crime happens in the network. It helps to read the behavior of attackers and can helps to prevent the same kind of future attacks. Network forensics investigates all kind of attacks through the pattern comes from all egress and ingress traffic.

There are many definitions for the term Network forensics since its existence by Marcus J. Ranum in 2012 and all researchers have greatly gamut since then. Schwartz in 2010 coined Network forensics as “The reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices”. Though, Network forensics contains the utilization of scientifically and experimentally proven techniques to identify, collect, detect, acquire, corroborate, examine, analyze and present the document via using digital information from live network sessions.

Network forensics process can be done through collecting all the ingress & egress traffic from the various resources, devices like servers, firewall, honeypots and various browsers. These proactive and reactive processes investigate the attack intention and recover the clues from an intrusion. The ultimate goal of this field is gives law enforcement and security tightening perspective. It refers to find out the level of attack intrusion so that the network can be intact, secure, strengthen with the evidences.

Network Forensics is used as a tool for monitoring the activities, specifying the source of attacks and analysis and detecting them. Various Network Forensics tools can be used to capture the packets, analyze and investigate them. Network forensics is an extended phase of the network security. Network security protects the system against attacks while Network Forensics main focus is to record the evidence of the attack.

Network Forensics deals with the capturing, retaining and analyzing of the network traffic. Packet mining, packet forensics or Digital forensics terminology can be taken for network forensics. All are having the same concept with the objective to register each & every packet and the data that it contains which was moving throughout the network and storing them for some period of time. Network Forensics can be used as a powerful device to unlock the mysteries found within the network means capturing the digital evidence before any specific event takes place. A network forensics analyzer which was commonly called as a network recorder captures and stores all the traffic so that it can be retrieved later for further analysis.

Network Forensics focuses on two issues. Firstly, related to the security which involves detecting the traffic and identifying the intrusions. Secondly, it is related to the law enforcement which shows capture and analyzes the traffic and can include various tasks such as searching for the keywords, reassembling the transferred files. The tendency of network forensics is to make attackers busy on the network and involve them to spend much time and energy to trace the track and scenarios go more costly.

B. Texonomy of Network Forensics Tools

Garfinkel et al. [2] classified the Network forensics systems into catch-it-as-you-can terminology and stop-look-and-listen terminology. Catch-it-as-you-can term takes all the packets as much as possible which cross through a certain traffic point and store further. In these kinds of tools analysis is done in the batch mode. This type of process therefore, need huge amount of space. In Stop-look and listen term, each packet is analyzed in a minimum necessary way in memory. Some information is preserve for the future acquisition. Speed processor is needed to check the path of ingress traffic especially in this approach. Quite a bit space is needed to store for updating the new information from the old in both the approaches.

Sitaraman et al. [3] described the whole network as host based and network based. In Host based network collect and analyze the packet comes at specific host. It relies on a single host and helps to understand network activity.

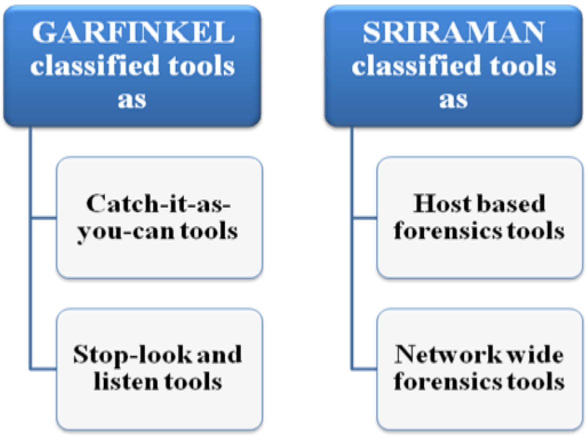
GARFINKEL classified tools as
Catch-it-as-you-can tools
Stop-look and listen tools
SRIRAMAN classified tools as
Host based forensics tools
Network wide forensics tools

Figure 1: Classification of Network Forensics tools

III. NETWORK FORENSICS MECHANISM

The different components of the network forensics analysis have been shown in Figure 2. It shows the various stages through which the clues will be evaluated.

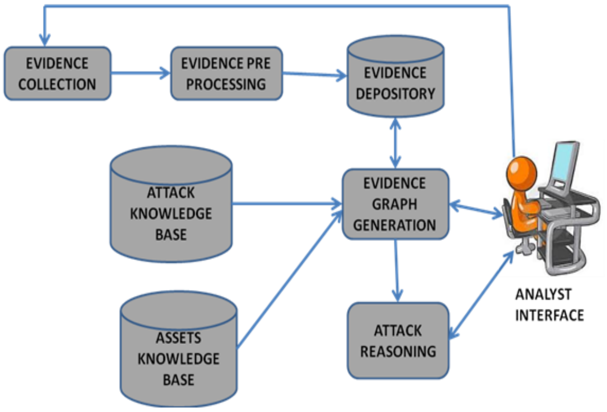

Fig 2: Network Forensics Analysis Design

The architecture of analysis mechanism for the network forensics is shown in Figure 2. The first module of this architecture is evidence collection module**.** The first module collects intrusion clues from many hosts and from the network and preserve for under investigation which further forward to the evidence preprocessing module that parses certain types of clues such as intrusion alerts into required structure and reduces the repetition in low level clues by aggregation. The second module is attack knowledge base module is a separate module that provides prior knowledge of known exploits. The second separate module is assets knowledge base that provides prior knowledge of the networks and hosts under investigation. The first and the second separate module merge and produce output send to the evidence graph manipulation module which generates and updates the evidence graph by retrieving intrusion defense in the repository. Further, automated reasoning will be performed in attack reasoning module. This reasoning will be based on evidence graph. It is followed by all the visualization of evidence graph and reasoning results is passed to the analyst in analyst interface module. The final analysis and the feedback use to send for both graph generation and attack reasoning module.

This architecture itself reveals that the identified source will be collected for further investigation. Here all the real time tools should be worked efficiently. This collected evidence sends for preprocessing. The entire preprocessed evidence further store in the depository. The attack knowledge base will ensure the entire alert to graph generation module. Asset knowledge base who gives the information about no of host under investigation, combine with attack knowledge base which further merge in graph generation module. The graph generator module also retrieves information from evidence depository and refurbished information sends to the depository. This graph generator module sends all revamp data to interface module. Graph generator module also forward the all investigated evidence to attack reasoning module. The analyst interface module gives their expertise comments with out of band information by “Edit the evidence graph directly” and another “Send queries to extract specific evidence”. The updated evidence graph finally sends to the attack reasoning module for improving the results.

Network forensics is the process of investigating the attack that describes how an incident happened and the involvement of the parties in this process. The network forensics investigation of the digital evidence has been employed as the post incident response for an activity but it’s definitely not an incident that complies with the organization’s terms and policies [5]. Therefore, there are various frameworks and techniques have been proposed in order to investigate the digital evidence. Pilli et al. [6] had shown ubiquitous research survey on network forensics and proposed a generic framework for the network forensics investigation [7]. This proposed framework describes many of the phases that already have been proposed in the various digital forensics models but some new phases have been added specifically [8],[9],[10]. The figure 3 presented below describes the proposed framework and the detailed description about those phases later. The attack intention and types can further analyze according to their malicious intent [11]. Process model and it is compared with other existing work in [12].

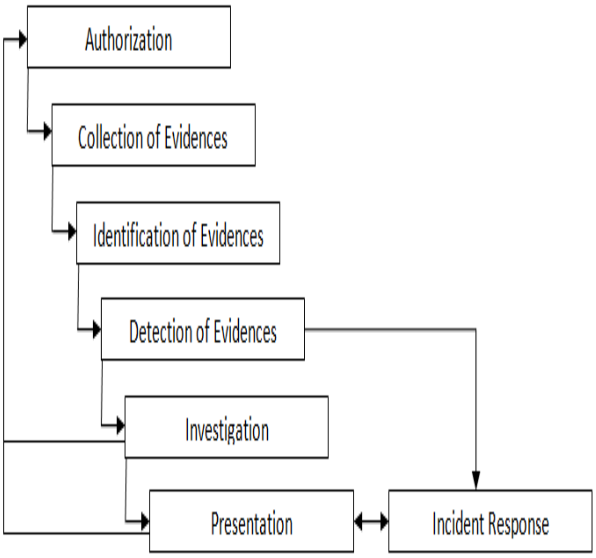

Fig 3: Generic Process Model for Network Forensic Investigation

A. Authorization

In this stage background is set towards the higher ground tasks. Various network security tools such as intrusion detection system or intrusion prevention system, firewalls and the packet analyzers are deployed at number of points on the network and also they require taking the access of the sensitive data on the network. Trained staff is required in order to handle these tools and ensures to collect the quality evidence to facilitate the acknowledgment of network security attacks. Required legal warrants and authorization must be obtained in order to ensure that the privacy of an individual and the organization is not violated.

B. Collection of Evidences

The various tools including software, hardware deployed to capture logs as much as can possible. The various sensors are also installed to reconnaissance the activities. Network evidences are collected by the various NFATs employed such as TCPdump, Wireshark, TCPflow, Snort, SiLK, PADS, and bro. As the incoming traffic changes very rapidly and also it is not possible to retrieve exactly same traces at the same time, so therefore it is critical to analyze at that point or stage. The network must be monitored and the integrity of the captured traces must be maintained as well to identify the future attacks. Sometimes the large amount of memory space requires keeping the logs intact. Logs are more in quantity so system must be able to handle it in proper manner.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

C. Identification of Evidences

Data collected in the previous stage is identified by the network forensics specialist for the further investigation. This stage also makes sure to preserve the copy of the network data so as to facilitate legal requirements and as soon as the process is repeated on the original data, results obtained after investigation are proved to be same. Without modifying original data, a copy of the data is analyzed and also a hash of data is preserved. Bijalwan et al. [13] showed the UDP flooding approach in their work through randomizer approach.

D. Detection of Crime

In case of eccentricity, alerts have been generated by the deployed security tools like TCPdump, wireshark, PADS, bro, snort etc. These tools help to detect the security breach and the privacy violation. These eccentricities are further analyzed for the various parameters in order to persuade the presence and the nature of the attack. To determine the attack or for further analysis a quick validation process has been take out. This process decides whether to continue or ignore the alert as false alarm. If the analysis goes on, then it performs two actions: collection of the clues and incident response of the clues. Network traffic is classified through SVM for multiclass classification [14].

E. Investigation

The data we get in the previous stage may consist of the reluctant data or referred as contradictory data. Therefore in this stage an examination is made and a mythological search is conducted so that no crucial information is lost. The data collected is classified and clustered into the groups to reduce the stored volume of data into manageable portions. Highest possible evidence and the data containing the least information are identified to remove the redundancy. After examination, these evidences are analyzed to identify network intrusions. Data mining and soft computing technique are used to search the data and correlate the attack patterns. To understand the nature and the workability of the attackers, the attack patterns are then put together. The attacks are further reconstructed and replayed. Few important parameters are related to network connection establishment are operating system fingerprinting, DNS queries, packet fragmentation, protocol. Validation of the suspicious activity is the final outcome of this phase. The information obtained from the previous stage is use to check who, where, when, how and why of the incident as it helps in the source traceback, attribution to a source and reconstruction of the attack scenario. The result of the previous phase further observes to see the way from where the attack emanates. It is observe from any intermediate systems and through communication pathways. The data for incident response and prosecution of the attacker are the final outcome of this phase. Attackers hide themselves using two simplest approaches: Stepping stone attack and the IP spoofing. Similar and anomaly based approaches are used to detect these attacks. The approach of the investigation depends on the type of the attack.

F. Presentation

In this phase, the process model in which observations are presented in a require format. It provides the explanation of the various procedures to reach at the conclusion of the investigation process. The conclusions are drawn from the visualizations so that they can be easily understood. Here the system documentation is also being done to meet the legal requirements. A detailed review of the incident is done and counter measures are recommended to prevent the similar incidents in the future. The entire case documentation is done for the future investigations and network security.

G. Incident Response

For detecting the security attack, the response is initiated depending upon the information to be collected for validating the incident. This response is predicated on the nature of the attack identified. It is governed by the organizational policy, legal and business constraints. For preventing the future attacks and to get rid from the attacks, an action plan is performed. The decision is also taken at the same time to proceed for investigation and traces collection. This phase is applicable where the attack is still in progress and investigation is already being initiated.

This is an anatomy of network forensics which works both in real-time and post attack scenarios. The real time network traffic is shown in first three phases. The authorization phase ensures all observing tools are well in place, the collection phase captures the network traces ensuring integrity of the data. The detection phase helps in the discovery of the attacks. Suitable incident response hinge upon the nature of the attacks finally. The last two phases are same for both real time and the post attacking scenarios.

Investigation phase and presentation phases exhibit the post attack investigation. the various sources and identifies the attack give input to this phase. Attack patterns are classified using various data mining, soft computing or statistical approaches in analysis phase. The traceback technique and the attribution and the final presentation phase results in the accomplishment of the attacker in investigation phase.

IV. NETWORK FORENSICS FRAMEWORK

The classification of the Network Forensics Framework (NFF's) is based on an exhaustive literature survey. By implementing the architectural framework of network forensics, we derive such classification which narrows down the scope and allows a comprehensive study of the area. NFF's are classified mainly into five categories as traceback NFF's, soft computing networks based framework,honeypot based framework, attack graphs based framework and formal method based frameworks. A full operational perspective of each NFF and the structural aspect and its implementation objectives are presented here in this section.

A. Distributed Device Based Frameworks

It is the famous framework which presents the local area network and internet. It is distributed in nature because the servers and the clients at different physical locations. These logs must be collected and analyzed. General architecture for the distributed framework is presented in the figure 4 below.

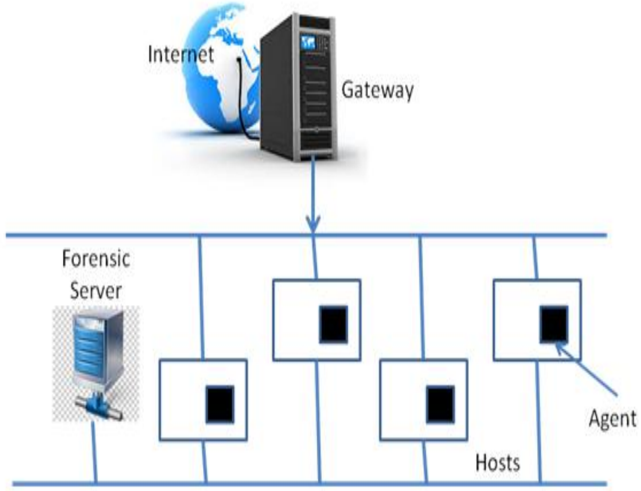

Fig 4: General Architecture for Distributed Framework

B. Soft Computing Based Frameworks

There are two main functions of this framework. The first component is to capture and analyze the data whereas the other component is to classify the data. For an effective and automated analysis system, Network Forensic Based Fuzzy logic and Expert System is used. Four important functions of this system are the fuzzification, acquisition, preprocessing and the knowledge base. The construction of knowledge base and the fuzzy inference engine mutually exchange the information. A general architecture of the fuzzy logic based frameworks is presented in the figure 5.

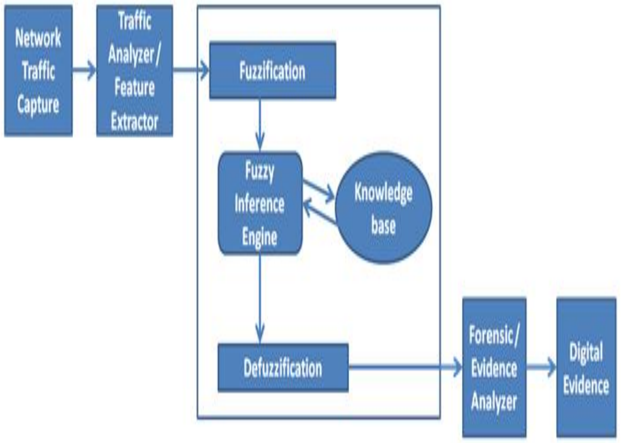

Fig 5: Fuzzy logic based Framework

C. Honeypot Based Frameworks

Honeypot frameworks are used to analyze the attack process methodology of the attacker and improve defense mechanisms. By using various tools this model integrates results of the data logged into a single system to reduce human intervention by exploiting computational intelligence. The tool used to integrate data logs is referred as Automated Network Forensic tool. For collecting the data, open source forensics tools are used and an isolated network of virtual machines is built into a honeynet. At one stage, some tools characterize information produced and at other stages it is then transformed using other tools. Identification and automation is done for the time consuming and error prone processes and data sets are first partitioned and then tested.

D. Attack Graph Based Frameworks

Wang and Daniels implemented a graph based approach towards network forensics analysis in 2008. This model facilitates automated reasoning and evidence presentation. This framework consists of the six important modules such as evidence collection, preprocessing, attack & assets knowledge, evidence graph, attack reasoning module. Attacks are analyzed combining with the results from both levels.

E. Formal Method Based Frameworks

In 2008, Rekhis developed a system for Digital Forensic in Networking (DigForNet) which is fruitful for analyzing the security incidents and explaining the number of way consider by the attackers. Further, DigForNet has taken formal reasoning tools (I-TLA and I-TLC). It also compatible for intrusion response teams to reexamine and reconsider all the attack scenarios. Identification of attack scenerios is also possible through Investigation-based Temporal Logic of Actions (I-TLA). Investigation-based Temporal Logic Model Checker (I-TLC) executes attack scenarios and also can easily show progress of the attack. These generated scenarios are used to identify the risk that can compromise the system, entities originating the attacks and to confirm the investigation different steps have been taken. These hypothetical steps can handle all these unknown attacks.

F. Formal Method Based Frameworks

Aggregation framework is developed to improve from the limitation of already present tools instead of developing a new tool for finding out the clues of forensic investigation.

G. Proposed Frameworks

For understanding Network attack, we will have to build and design network lab which refers in Figure 6, to deploy the network monitoring system. Effective network monitoring system needs continuous, comprehensive, concrete and convenient work for achieving the desired output or the target.

Continuous: To escape from the detection, network vulnerability changes their location very rapidly in the network. So we will have to keep continuously reconnaissance the network log and update the changes.

Comprise: The system should understand the propagation of the network vulnerability especially botnet and the technique used for propagation in the network.

Concrete: System requires providing concrete information as early as possible because vulnerability (botnet) constantly changes their place. So information of specific kind of botnet and its value also degrades quickly.

Convenient: The system should get this information within a time so that value cannot change.

However, it is a very requirement of individuals to have domain knowledge and its analysis. The system will collect information about various aspects of vulnerability including its flooding, i.e., denial of services, communication infrastructure, propagation technique, identities of compromise host and details of activities then participated in.

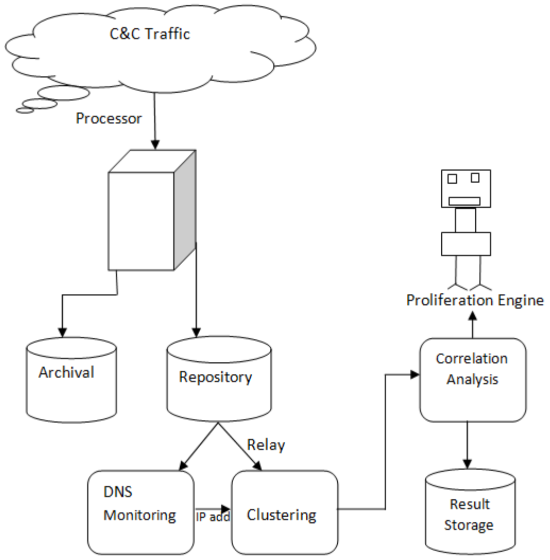

Fig 6: Proposed network Forensics Framework

V. NETWORK FORENSICS ANALYSIS

A. Network Forensics Scrutiny

Network forensics results in linking the diverse data sets have relevance to activities, habitually correlating the digital traces obtained in the different data sources such as web pages, logs, internet related group, online chat rooms [15]. Network forensics process can be developed in two ways: the first step is to susceptive use of conventional security devices like firewalls and intrusion detection system, analyzing the data and then investigating it. The other way is to eagerly trap the attacker by means of honeynets [16] or greynets [17], to observe the attack patterns and thus creating the observable profiles of attackers and their exploitation mechanisms.

In 1987, Denning et al. [18], proposed an intrusion detection model that lifted research contribution in same area by new researchers. After that in 1990, Ranum et al. [19], defines the capture, recording and analysis of the attacks occurred. In 2002, Reith et al. [20] proposed new model referred as an abstract digital forensic model which is predicated on the DFRW model. This model consist nine stages that becomes the key component of this model. These include identification, preservation, collection, examination, analysis, presentation and decision in this given model.

In 2006, McGrath et al. [21] interpreted network forensics after malicious data collection with the help of non intrusive network traffic record system. Mandia et al. [22] developed robust incident response methodology. His first phase i.e. Initial response exhibited the formulation of a response and sum up them for an incident. The collection and analysis phase comes under investigation phase which define in previous different models. In 2007, Frelling and Schwittay et al. [23] proposed the model in which computer forensic and incident response processes can be utilized with management oriented approach in the digital investigations.

In 2008, Abdullah, Mahmod and Ghani et al. [24], [25] identifies the five categories including framework, trustworthiness, data detection/acquisition and recovery. Casey and Palmer et al. [26] developed an investigative process model. It ensures the simplicity on previous tedious investigation process, evidence handling and minimizes chances of errors.

Umpteen authors contributed research in the field of network forensics and work done in an application of frequent sequence mining algorithm. The researcher Palomoa et al. [27] shown a novel theory approach for analyzing and visualizing network traffic data. It was predicated on growing hierarchical self organizing maps (GHSOM). This GHSOM was basically used to make cluster network traffic data and to present this in sequentially. Pilli et al. [4], showed a framework and layout for network forensics that exhibit different tools & techniques, their process models and different frameworks and their implementations. Zhong et al. [28], derived an apriori algorithm that is basically made for a kind of most sturdy mining Boolean association rule algorithm. The analysis of apriori algorithm on mentioned procedure can improve the efficiency of evidence.

There are also many other researchers, scholars and authors who have made research on the network forensics. They have presented their work using different tools and techniques. In 2002, Corey et al. [29], had described a network for monitoring the vulnerabilities. It is especially prepared to identify the configuration problem easily. The forensic analysis yields the convenient way to find out security vulnerability. This allows all the best possible scrutiny of security violations. Tools like tcpdump, gnutella and netintercept have been used for the forensic analysis. In 2008, Wang et al. [30] had developed a novel graph based approach towards the analysis for network forensics. This is the approach for developing a model related to evidence graph. This model ensures an automated reasoning and the presentation.

In 2012, Raftopoulos et al. [31], investigated through the correlation of information based on four security parameters. These four security parameters are namely IDS alerts, examination & vulnerabilities reports and unwanted filtered traffic through search engine to expedite manual forensics analysis of compromised systems. Tools like Nmap, NIC whois, nessus and open vas have been used. Techniques like C4.5 decision tree based algorithm, NIC whois querying, TCP/UDP port scanning have been used. Comparison among the tree augmented naïve bayes (TAN), Bayesian tree classifier (BTC) and support vector machine (SVM) have been done for the forensics investigation.

In 2014, Shulman et al. [32], had reviewed the strongest procedure preventing cache positioning attacks on DNSSEC. This mechanism enables a posteriori analysis for the purpose of forensics. Detection of the attacks are used with ANYCAST technology, DNS cache poisoning by MiTm (man in the middle) and cache poisoning by subverting hosting infrastructure. In 2013, Rasmi et al. [33], proposed an algorithm which is known as the similarity of attack intention (SAI) to check the similarity on cyber crime intention. It uses cosine similarity as a distance. In 2010, Pilli et al. [5], had presented a generic process model. He has shown various implementations for network forensics also. He also proposed a novel framework as well as the research gaps with complete discussion for the work in progress. He described many previous tool and techniques which is used to define a framework. In 2012, Milling et al. [34] showed all the relevant condition for various graph topologies. He distinguished between a random model of infection and a epidemic model. Ball algorithm, tree algorithm, erdos-renyi graph, mehlhorn 2-approximation algorithm have been used for the detection and analysis of the attacks.

In 2013, Huang et al. [35], showed their work into three categories to classify the network. These categories correlate law enforcement exalted person ensure the investigation related to the cyber crime. In 2013, Thapliyal et al. [36], outlines the process of botnet forensics analysis and its implementation. In 2014, Herrmann et al. [37], discusses about the opportunities and concerns that may result from using evidence gained by fingerprinting techniques in criminal investigations. In 2014, Scanlon and Kechadi et al. [38], compares and contrast some of the existing digital evidence formats or bags and analyses them for their compatibility with evidence gathered from a network source. Identification and investigation of various formats like digital evidence bag format, encase format, generic forensic zip, advanced forensic format, raw format, common digital evidence storage format and daubert testing have been done. In 2011, Pilli et al. [5], had shown the traceback technique that marks the address of the router and interface number from every entered egress packets on the network.

B. Network Forensics Analysis Tools (NFAT's)

Network forensics analysis tools (NFAT) provides an extended view of the data collection and also allows inspecting the traffic from the protocol stack. NFATs also allow the best possible analysis of security violations. It was determined that the firewalls and intrusion detection systems (IDSs) are the well developed tools for the network security. But NFATs mutually stimulates with firewalls and IDSs in two ways that it retains a long term record of the network traffic and allows the quick analysis of the inconvenient spots that are identified by these two tools [29]. While accessing the NFATs, it determines what traffic is of the interest and also analyzes that traffic promptly and efficiently. NFAT performs the three tasks very well: Capturing the network traffic, analyzing the network traffic according to the user's needs and system user discovering the convenient and provocative things about the analyzed traffic.

NFAT must maintain the complete record of the network traffic. For further analysis, a successful NFAT must be able to capture and storing the traffic from the fully sopped network. NFAT actually captures the traffic but under some circumstances, it uses the filter and might be able to eliminate the irrelevant traffic, mitigating the storage and the performance concerns at any cost. Greater the NFAT discarding the traffic, longer will be the interval in which it can extract the traffic and smaller will be the scope of the possible post hoc analysis. The user interface must simplify the traffic and the content examination by the forensics tool. This interface lets the operator precisely specifying the traffic which is of the interest and avoids viewing the traffic. Generally, network monitoring tools support the criteria for specifying the traffic such as IP addresses, end point media access control (MAC), TCP or UDP port numbers. NFAT systems can enhance this by granting selection procedure according to the user or file names, specific content types and so on. NFAT user interface must specify the selection criteria easy and definite. Some of the functions of NFAT are as follows:

- Recording and analysis of network traffic
- Anomaly detection
- Determination of hardware and network protocols in use
- Incident recovery
- Prediction of future attack targets
- IP protection
- Assessments of the risk
- Exploit attempt detection
- Data aggregation from umpteen sources such as firewalls, IDSs and sniffers
- Detection of employee misuse, abuse of company networks and computing resources.
- Network performance

There are three properties of network forensics and analysis tools that is gather evidence where the researcher will listen to the network. The second property is that there shouldn't alteration on the data as it is non- intrusive. The third property is replay features which ensures researcher for the evidence without any alteration.

It helps researchers or administration to monitor the ingress and egress traffic, firewalls, servers etc. and record the events [6]. Now there is a brief introduction about the NFATs in the table 1 and the classification is reflected in figure 7.

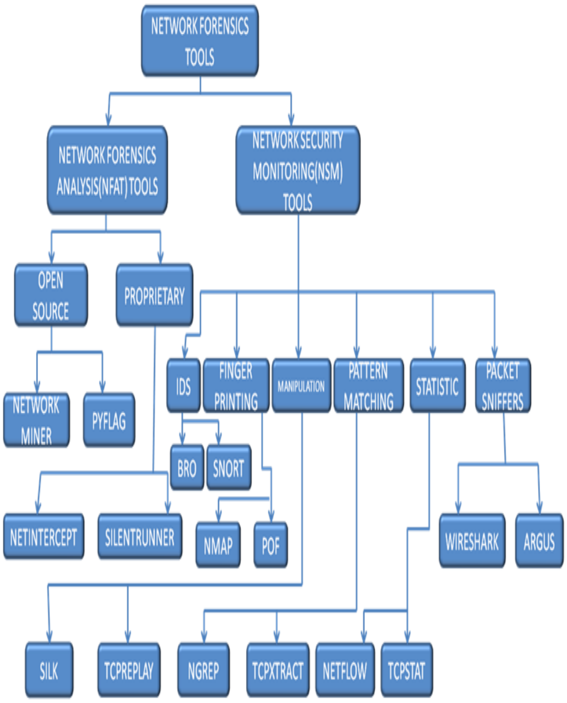

Fig 7: Network forensics tools classification

There are many network forensics analysis and tools exist commercially such as Visualroute, Encase, Silentrunner, NetIntercept, netflow, NetDetector. Many open source tools are such as Nmap, Wireshark,Tcpflow, TCPDump/ Libpcap/ WinDump, tcptrace, Snort, P0f, Tcpstat. Various commands are also available which are inbuilt in many modern operating systems and are very useful for network forensics: Nslookup, Traceroute, Netstat, Nbstat, Whois, Ping, Wget, and dig.

VI. NETWORK FORENSICS INVESTIGATION

Investigation is the process is taken by the all researcher after analyzing the facts.

Herein the researcher opt various network forensics methods to retrieve the source of crime and get the information how crime is happened and what methodology has been taken by the criminal to permeate the infection.

A. Network Forensics Technique

In this section we describe related technologies which show their connection to network forensics and their limitations. These techniques help us to detect the attacks which are explained below [39] [40] [41]. Figure 8 represents the classification of the network forensics technologies.

1. IP Traceback Techniques

The IP traceback techniques is a reverse technique to identify the source of attack. It ensures to reconnaissance the network path taken by the attack traffic. It doesn't need an interactive operational support from ISPs. Suppose that the way between victim and the attacker is represents by h1, h2, h3,….,hn, then to get the host for the IP traceback h1,h2,….,hn-1 given the IP address of the victim hn [42].

This strategy is basically apply for the masquerade attacks that can be retrieved though disparate layers. TCP/IP suit's second layer i.e. data link layer in which different MAC address could be used. Internet layer can be fitted with different IP address and in the transport layer; different TCP/IP port could be used. It showed that ip traceback is taken hard to sort out the problem.

Although there are many complexities to resolve the problem though, some IP traceback techniques have also been proposed. Here the author defined some important existing IP traceback techniques through internet that have especially been designed to trace back to the origin of IP packets through the internet. IP traceback techniques are categorized as: Link Input Debugging, controlled flodding, state testing, packet marking and ICMP traceback and payload attribution [43, 44].

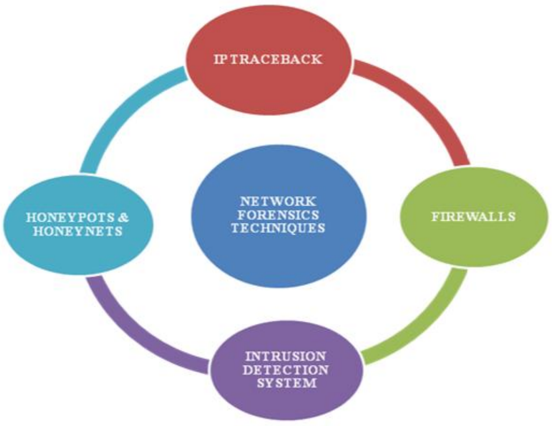

Fig 8: Network Forensics Techniques

- Link State Testing: The link state testing is the procedure will be being taken when the attack gets in process. It starts tracebacking from the source router near of vicitim's position. It ensures the upstream link that was taken a carry the attack traffic. Upstream router will have been determined the testing is necessary to take while the attack is in escalate position and consists of a traceback procedure from the router closest to the victim's place.
- Input Debugging: researcher has introduced the input debugging scheme in [43] for ip tracebacking technique. Here the researcher has defined the terminology for attack signature, procedures, its limitation
- Controlled Flooding: In controlled flooding technique, victim first try to find the map of internet topology then by iterative method victim would select the host launching the flood on each incoming links of upstream router [43]. This technique victim

Table 1: Network Forensics Tools

Tool	Description	Features	Advantages
SilentRunner	Silent Runner provides 3 dimensional network view to the user so that user can observe and monitor. It monitor all the packets enters in network and dives graphical view and it correlate the network traffic.	It captures all evidence from the services of the events for analyzing the traffic	Alert against detection of malicious traffic
NetIntercept	It is the network monitoring and analyzing tool. It is placed in firewall. It is the combination of hardware and software with complete system, placed into the firewall boarder. It is ability to store large data logs.	NetIntercept can not only decrypt the SSH-2 sessions and accept only secure far administration into the system, but also permits other tools to inspect and analyse its log files.	Capturing, analyzing and discovery
NetDetector	Net detector imports and exports the data in multiple (numerous) hetrogenious formats. Primarily NetDetector is a passive capturing, analyzing, and reporting on network traffic. It is supported with an intuitive management console and also have full standard based reporting tools.	GUI- popus, email or utilized by NetDetector as altering mechanism. NetDetector also enables the security administrator to run a complete forensics investigation by coupling with IDS	Support to network interface such as Ethernet, FDDI and protocols such as TCP/IP, Frame relay. Export data to HTTP, SCP and FTP.
TCPDump	TCPDump are network packet analyzer which support the network forensic analysis. This tool works on command line. After capturing the logs, it retain network traffic in different output formats.	It filters and collects data. It is able to read packets from network card, interface card, or an old saved packet life.	Intercept and display the communication of another user and computer

Ngrep	Ngrep is a low level network traffic debugging too in UNIX. It facilitates specifying hexadecimal expression or extended regular to match against data payload of packets.	For identifying and analyzing anomalous network communications it debugs the plaintext protocol interactions. It also stores, reads and reprocess pcap dump files at the time of finding a specific data patterns.	With HTTP basic authentication, FTP authentication, it can be utilized for more mundane plain text credential collection
Wireshark	It is an open source packet analyzer, which is extensively used as a tool for analyzing the network traffic. In the past it was famous as Ethereal. It captures and displays the packets in human readable format by utilizing real time. It is powerful software utilized for troubleshooting network issues that for free of cost.	It can capture the packets on only those networks, which are supported by Pcap, snoop, network sniffer. Microsoft network monitors are exception to this. It can capture the packets on these network as well.	Filter option, graphical front end is available
Driftnet	The images and audio stream in network traffic is capture by Driftnet. It is also known as a 'graphical tcpdump' for UNIX.	Driftnet is use to capture MPEG audio stream from the network and play it through a player such as mpg123. Images may be saved by clicking on them.	_
Network Miner	This tool is taken as a non active network sniffer or packet collecting source in order to detect sessions, open ports, hostnames, OS etc. without using of egress and ingress traffic on the network. It can be taken in another platform too.	The main purpose of this tools is to gather evidences for the forensic investigation. It collect the data from network traffic.	It is a network forensics analysis tool It can run both windows and Linux with wine.
Kismet	It is a packet sniffer intrusion detection system used for observing wireless suspicious activity.	It consists wireless Intrusion Detection system	This tool captures more packets. the sniffed packet's log traced and store in compatible file
NetStumbler	It facilitates detection of wireless LANs using the various WLAN standards and analyze the network traffic for the windows.	It is used to verify configurations, searching locations in a Wireless LAN	This tool find out the unauthorized access point
NetSleuth	This tool is use for network analysis. It analyze pcap files and fingerprint this tool is consist and develop for forensic investigation.	Silent port scanning Features provide the analysis of pcap file of attack which is still not detect in the network it monitor the whole network.	There is no requirement for the hardware or reconfiguration of networks.
Xplico	This forensic analysis tool also used for data extraction from traffic It can rebuild the stored contents with a packet sniffer.	It has the ability to process huge amounts of data and also manages pcap files of many Gbyte and Tbyte.	It can support the decoding of audio codec's and MSTRA.
PyFlag	It is a network forensics analysis tool and a web based and log analysis GUI framework. This tool is written in python.	It parses and extect pcap files and break this in low level protocols. It checks the data recursively.	It can search the files and build an index and contains the hash databases.
DeepNines	It is a network security monitoring tool for providing real time network defense for content and applications.	It filters and collects data. It extracts all applications.	_
Argus	It is a system and network monitoring application used for network forensics. it shows services of network's status along with server's status. It sends alert when there is any problem.	It extract graphs. It monitor the results of sql queries. It analyzes the log.	It provides rate limit multiple notifications to prevent paging floods.
Fenris	This tool is also used for debugging the code and network forensic analysis.	It filters and collects data.	It features a command line interface as well as a soft ICE-alike GUI and web frontend.
Flow-Tools	It is a software package used to collect, send, and process and generate reports from NetFlow data from Cisco and Juniper routers. This tool is used for deployment.	It analyzes the log and filters and collects the data.	-
EtherApe	It is a graphical monitor tool for storing the network traffic. After filtering the traffic this tool can read packets from a file.	Live Data can be captured	

Honeyd	It is open source software that allows a user to run and set up multiple virtual hosts on a computer network.	Honeyd provides mechanism for monitoring the traffic, detecting the threats.	-
Snort	It is extensively used tool for network intrusion detection, prevention and network forensic analysis. The role of Snort tool are analyze of protocol, match the content as well as search the content.	It is used to detect the attacks including CGI, buffer overflows, stealth port scans etc. It filters and collects data.	It generate real time traffic analysis.
NetWitness	It shows the different network forensic threat analysis, the protection from data leakage, compliance verification.	It provides the data stream, correlation Features.	_
Solera DS	It provide network forensics classification analysis.	It captures high speed data.	It improves the network security and optimizes network performance.
Bro	It is a network security and monitoring tool that collect all information transmitted as a part of TCP connections It process 'tcpdump' packet flows also.	It allows the analysis of the network traffic and also can reconstructs thousands of TCP connections at a time and saves the results in ordinary files, makes easy to analyze data.	_
TCPFlow	It collects and process netflow data on the command line. Various tools fall under it which is working with netflow format	It displays the netflow data and creates the statistics of the flow IP addresses, ports etc.	_
PADS	It is a security scanner used in computer network. It specifically sends crafted packets to the target host and analyzes the response.	host discovery, port scanning, version detection are the features of this tool.	It Checks the system security and identifying the network
NfDump	It is extensively used tool for network intrusion detection, prevention and network forensic analysis. The role of Snort tool are protocol analysis, content searching and content matching.	It is used to detect the attacks including CGI, buffer overflows, stealth port scans etc. It filters and collects data.	It generate real time traffic analysis.
TCPTrace	It shows the different network forensic threat analysis, the protection from data leakage, compliance verification.	It provides the data stream, correlation Features.	_
Nmap	It provide network forensics classification analysis.	It captures high speed data.	It improves the network security and optimizes network performance.

itself force host to launch flood.

- ICMP Traceback: In [45], the researchers showed an IP traceback by using a scheme called iTrace. It helps on those attacks which emanates from limited sources causes flooding. ICMP carries the information of nearby connected routers and send the information to the next destination. This HMAC [46] is basically used by iTrace scheme. It is also supported the use of X.509 Digital Certificates [47]. This authenticates and also evaluate messages are related to ICMP traceback.
- Packet Marking Techniques: The principle of this technique is that the path is taken as sample of one node in a single fraction of time. In [48], the authors contributed a Probabilistic Packet Marking (PPM) technique that allows the traceback for an attack flow. Basic idea behind this technique is that during forwarding, in packets should be mandatory written partial path information by routers probabilistically and there is a reserved field called marking which is adequate capacity to keep a single router address in the packet header.
- Payload Attribution: This technique needs the source id, destination id, appearance time when it reach on the network of all the packets that carries these payload. To extract information is very tedious as the size of the payload usually very large whereas the information of umpteen substrings requires to be placed. Most of the time the researcher do not have any information related to its header that refer packet of interest however it is observed the expected a part of the payload. Here, Hierarchical Bloom Filter works perfectly in a Payload attribution system. This filter has a low memory footprints and good processing speed with less false positive rate.

2. Intrusion Detection System

Intrusion detection systems (IDS) are applicable to find out any malicious programs or network attacks or intrusions in a system. It monitors various computing resources either a single host or an entire network and generates the alerts when an attack is detected. In Intrusion detection system both the network based as well as host based information are combined to develop the hybrid systems. There are two main approaches of IDS which is broadly classified as:

- *Signature based:* In this approach, to detect the malicious programs, the incoming packets are matched with the known patterns of attacks and if they matches the alerts are generated [49].
- *Anomaly Based:* This approach exhibits the ingress traffic which do not matches the normal or desired behavior is fabricated to be an intrusion. The basic idea is just detection not an investigation [21].

Sometimes IDS can give wrong alerts called as false negative and also false positive. False positive generates alert sometime when even attack hasn't happened. False negative refers to an unable to generate an alert even though an attack has happened or entered in the network. [50].

3. Firewalls

Firewall is basically manual defensive mechanism applied in the network. It is applied to give a defense to prevent an attacker from not to enter inside specifically a particular protection boundary. However, if the boundary is crossed by an attacker, there are the chances of an intrusion or an attack. Therefore, it is good if we implement defense wall i.e. defense in depth that gives the chain of firewalls [19]. For the network forensics system, this approach reduces the work load involved in the process as it prevents the attacks to penetrate through the network. The basic idea behind this technique is just the prevention [51].

4. Vulnerabilities Detection Techniques

There are several techniques which are as follows:

- Black-Box testing: The behavioral testing also referred as black-box testing. In this testing, the internal design is basically tested. Further, it is compared with the expected results. The tested design or implementation is also not aware to tester too. This can be non functional and functional too. However functional process is taken widely in black box testing.
- White-box testing: Code based testing also referred as white box testing. This analysis programmer also well known of internal structure. It can be done both manually as well as automatically. It can be followed with during code inspection and through reviews. WinRunnner, Quick test professional tools [51] is taken for the purpose of testing by the programmer.
- Double Guard Detecting Techniques: This technique is based on observation on network. This Double Guard detects the behavior of network through user session both front and back hand end of the web server. It identifies the source of attack through the alerts. [52].

5. Hidden Markov Models (HMM)

Attacks exploit web application vulnerabilities which are derived from the input validation. Hence to detect these attacks a new analysis is performed using Hidden Markov Model (HMM). It exhibits that web application related attacks can be detected effectively through this model whether the attack is known or unknown. It is used in Host based intrusion detection system. The availability of attacks inside the train set related problem can be addressed explicitly by hidden markov based model. [49].

6. Honeypots and Honeynets

Honeypots [53, 54] is a system on the internet that is deliberately setup to allure and trap user who try to attempt and pentrate other user's systems, mainly have two different types of honeypots i.e low interaction and high interaction. In high interaction available tools to deploy this and which are the most closer to the Neofelis architecture were ARGOS and honeypotX [55] respectively. Low interaction honeypot is a certain no of configured services to probe the system. Honeynet is basically a designing of network which is being made for reconnaissance. The attacker's characteristics can be trapped with the help of honeynet [53]. The architecture of honeynet divides on serial and parallel. Parallel architecture reduces the delay whereas serial architecture protects from the direct attacks. On the other hand honeywall capture all the ingress and egress data traffic including the data is also inside of honeypot system then it will monitor all.

A. Highly Efficient Technique for NF

Cybercrimes are increasing day by day with the increase in the usage of the internet. To prevent these crimes, there is a need for the good and efficient tools and techniques to investigate these crimes. To extract the network event of both the attacker and the victim, Payload attribution plays crucial role. These extract network event can be forwarded for the analysis of the incidents [56, 57, 58]. The new contribution may helps integrating into existing network monitor system.

The below given techniques are helpful for the small passage payload as the accuracy of attribution increases with increasing of the length.

- Bloom Filters: This technique is for the payload attribution. It will modify the data structure that allure string insertion and query without changes on structural design with attribution implementation methods. Bloom filters are taken in umpteen network and in many applications through supporting queries related to the space efficient probabilistic data structures [59].
- Rabin Fingerprinting: Rabin et al. [60], exhibited polynomial based fingerprint scheme for binary strings. These strings are basically contains short checksums. This scheme has found several applications [59].
- Winnowing: if we need the accuracy in detection of both partial and full copies between the docs, Winnowing [61] is an efficient fingerprinting algorithm. For an example each sequence of *x* consecutive characters in a docs, it is further compute its hash value. Next it stores it in an array. So, the initial sequence of an array is a hash of $a1a2 : : : ax$, the second item is a hash of $a2a3 : : : ax+1$, etc., where ak are the document's , for $k = 1; : : : ; n$. Next suppose that the window slide size is w through the array of hashes. Further it will be selected least hash within each window. If hashes are more with the minimum value, select rightmost one. The selected hashes show that fingerprints are better for document fingerprinting than the subset of Rabin fingerprints. This idea can be used to select boundaries for blocks in packet payloads.
- Attribution Systems: Various researches have been made to design and implement feasible traceback system to identify system which can directly generate malicious traffic. But, the procedure pull back the codes related to flodding, best case single level payload and the connection chain. Here the hash based technique especially for ip traceback is the Source Path Isolation Engine (SPIE**)** [62]. It creates network audit trails that produce packet's hash digest on the header of a packet header and a payload fragment. It further keeps them in router's Bloom filters.

Shanmugasundaram et al. [63] designed the Hierarchical Bloom Filter (HBF). It is a little compact hash based payload digest data structure. For distributed forensics network, a payload attribution system based on HBF is a key module [59]. The system achieves both low memory footprint and a reasonable processing speed at a least false positive rate. SPIE and HBF both are the digesting techniques, but SPIE is a packet digesting scheme while HBF is a payload digesting technique. An alternative approach to the payload attribution problem has been proposed called as the **Rolling Bloom Filter** (RBF) [64]. This technique aggregate all query results in linear form from the multiple Bloom filters. It uses Rabin-Karp string-matching algorithm for packet content fingerprints This technique is the best case performance of the HBF [64].

VII. RESEARCH CHALLENGES

For Network Forensics Analysis, various tools and techniques have been used; frameworks and implementations have been surveyed in the previous sections. But there are some limitations and specific research gaps associated with it which is defined below.

- Data Analysis: With the use of the various tools data captured from the different sources need to be analyzed properly and it should be organized to make the decisions and for implementations. So there is a need for the advanced tools to investigate.
- Data as Legal Evidence: The challenge is to preserve and archive the real data so as to use it in the court of law. Preserving the evidence carefully and secretly needs some advance procedures.
- Privacy: For the investigation procedures, a special care has to take place so that the private information of the user is not violated across the entire network.
- Data Integrity: Different techniques have been used to ensure data integrity. But the major challenge is to pay heed that the data is not forged or it shouldn’t be tampered by an attacker and maintaining the integrity so as not to affect the investigation process. This requires the use of advanced techniques.
- Data Granularity: After capturing the data, the challenge is that what data should needs to be retained and what needs to be eliminated.
- Data Capture: Data have been captured from various sources like entire network, audit log, authentication log using the available tools. But the main challenge is to decide which sources of the network are appropriate to capture the data to ensure whether it is short term basis or the long term basis.

The challenges obtained through research gaps after the exhaustive research survey on investigation of Botnet attack are following:

- **Collection:** collection is an important process of network forensics in which we collect all information from network and further send for different work. Without the loss or drop of packets capturing real time data is an important challenge. Capturing all packet information gives very large amount of data. Collecting information from the network and the collection of usefull data is also a challenge. Filteration process requires separating only those data which is needed.
- **Preservation:** collected data is to be preserve for future. Back up devices keeps all the traced data alongside all the logs. In this case it ensures that the original data & its logs cannot be altered and affect for the legal requirements. This is the big challenge to preserve this original traffic intact.
- **Identification:** This phase identify all the protocol features that are altered during packet collection. It further forward for the correlation with the attack events and validation purpose. This is to be done in another investigation phase. All the packets further reorganize in transport layer separately. Next, replaying attack analyze the behavior of all kind of attacks.
- **Traffic analysis:** Analysis of identified sources is also an important challenge of research. To get the dataset for analysis purpose also a tedious job check. To classify these dataset, feature extraction is required. Algorithm may be tested for improving the accuracy. Irrespective of single classifier, ensemble based classifier can be analyzed for improving the results**.**
- **Investigation:** The validation process is being done by investigation phase. Here incident response will ensure the type and the identity of an attacker too. Attacker try to prevent himself through IP spoofing and stepping stone attack but the researcher can identify all these clues through the exhaustive investigation in network forensics. The attackers different techniques can create the hard challenge to the researcher.

VIII. RESEARCH CHALLENGES

Network Forensics plays a very important role in the field of the security and privacy and also as a part of the entire security model as it ensure the investigative capabilities. It has the ability to predict the future attacks by examining the attack patterns from the various sources of data. The incident response is much faster and also has the ability to generate authentic evidence which is admissible into a legal system.

In this paper we have studied about various digital forensics model and generic process model also and various network forensics framework implementations has been surveyed. There have been various limitations and research gaps related to these tools and techniques which we found during our survey. We have shown the anatomy related to the network forensics too. To overcome these problems and research gaps and make things easier the concept of ‘Neurofuzzy’ can be used for the further implementation. This exhaustive survey presented the challenges being faced by the network forensics. These challenges need to be addressed urgently so as to overcome the limitations and trace back.

REFERENCES

1. N. Shone, T. N.Ngoc, V.D. Phai and Q. Shi,” A deep learning approach to Network intrusion detection”, IEEE Trans. On Emerging topics in Computational Intelligence, 2017
2. S. Garfinkel, “Network forensics: tapping the Internet, ” http://www.oreillynet.com/pub /a/network/2002 /04/26/nettap.html.
3. S. Sitaraman, S. 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.
4. A.C.Shorren, C.Partridge, L.A.Sanchez, C.E.Jones, F.Tchakountio, B.Schwartz, S.T.kent and W.T.Strayer, “ Single-packet IP traceback”, IEEE/ACM Trans., Netw., 10(6):721-734,2002.
5. Abraham Yaar, Adrian Perrig, Dawn Song,‖ Pi: A Path Identification Mechanism To Defend Against Ddos Attacks‖ ,IEEE 2003.
6. E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation,* vol. 7, pp. 14-27, 2010.
7. E. Pilli, R. C. Joshi, and R. Niyogi, "A generic framework for network forensics," *International Journal of Computer Applications,* vol. 1, 2010.
8. Casey, E. and Palmer, G. 2004. The investigative process.in Casey, E. ed. Digital evidence and computer crime, Elsevier Academic Press, 2004.
9. Ciardhuáin, S.Ó. 2004. An extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), 2004.
10. Baryamureeba, V. and Tushabe, F. 2004. The enhanced digital investigation process model. In Proceedings of the 4th Digital Forensic Research Workshop (Maryland, USA,2004).
11. A.A. Ahmed, “Investigation approach for network attack intention recognition”, International journal of Digital Crime and Forensics, vol. 9(1), pp. 22, 2017.

12. P. Kaur, A. Bijalwan, R.C. Joshi and A. Awasthi, "Network Forensics Process Model and Framework: An Alternative Scenerio", Intelligent Communication, Control and Devices, pp. 493-502, 2018.
13. A. Bijalwan, M. Wazid, E.S. Pilli and R.C.Joshi, "Forensics of Random-UDP flooding Attacks", vol. 10, pp. 287-293, 2015.
14. P. Kaur, P. Chaudhary, A. Bijalwan and A, Awasthi, "Network Traffic Classification Using Multiclass Classifier", Advances in Computing and Data Sciences, pp. 208- 217, 2018.
15. Mohd Taufik Abdullah, Ramlan Mahmod, Abdul A. A. Ghani, Mohd A Zain And Abu Bakar M d S, ―Advances In Computer Forensics, International Journal Of Computer Science And Network Security, Vol. 8, No. 2, February 2008.
16. L.Spintzer, " Know your enemy: defining virtual Honeynets", http://www.honeynet.org.
17. Reith, M., Carr, C., and Gunsch, G. 2002. An examination of digital forensic models. International Journal of Digital Evidence. 1. 2002.
18. A.C.Shorren, C.Partridge, L.A.Sanchez, C.E.Jones, F.Tchakountio, B.Schwartz, S.T.kent and W.T.Strayer, " Single-packet IP traceback", IEEE/ACM Trans., Netw., 10(6):721-734,2002.
19. Jatinder Kaur, Gurpal Singh, Manpreet Singh,‖ Design & Implementation Of Linux Based Network Forensic Sy stem Using Honey net‖ , International Journal Of Advanced Research In Computer Engineering & Technology Volume 1, Issue 4, pp 231-238, June 2012.
20. Yang Xiang,Ke Li, Wanlei Zhou, ‖Low-Rate Ddos Attacks Detection And Traceback By Using New Information Metrics‖, IEEE transactions on information forensics and security, vol. 6, no. 2, pp 426-437, june 2011.
21. Nguy en H Vo, Josef Piep rzy k, ―Protecting Web 2.0 Services From Botnet Exp loitations‖ Cy bercrime And Trustworthy Computing Workshop IEEE, pp 18-28, 2010.
22. Mandia, K. and Procise, C. 2003. Incident Response and Computer Forensics. (Osborne McGraw-Hill, New York,2003).
23. D. Reilly , C Wren, T. Berry , ―Cloud Computing: Forensic Challenges for Law Enforcement‖, International conference on internet technology and secured transaction pp 1-7, 2010.
24. Sindhu. K. K , Dr. B. B. Meshram, ―A Digital Forensic Tool For Cy ber Crime Data Mining‖, IRACST – Engineering Science And Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, 2012.
25. Veena H Bhat, Member, IAENG, Prasanth G Rao, Abhilash R V, P Deepa Shenoy, Venugopal K R And L M Patnaik ,‖ A Data Mining Approach For Data Generation And Analysis For Digital Forensic Applicat ion‖, IACSIT, International Journal Of Engineering And Technology, Vol.2, No.3, June 2010.
26. Casey, E. and Palmer, G. 2004. The investigative process.in Casey, E. ed. Digital evidence and computer crime, Elsevier Academic Press, 2004.
27. E.J. Palomoa, Application of growing hierarchical SOM for visualisation of network forensics traffic data, Neural Networks, Vol. 32, no. 16, 2012, pp. 275–284.
28. X. Zhong, "The Application Of Apriori Algorithm For Network Forensics Analysis," *Journal of Theoretical and Applied Information Technology*, vol. 50, pp. 430-434, 2013.
29. V. Corey, C. Peterman, S. Shearin, M. S. Greenberg, and J. Van Bokkelen, "Network forensics analysis," *Internet Computing, IEEE*, vol. 6, pp. 60-66, 2002.
30. W. Wang and T. E. Daniels, "A graph based approach toward network forensics analysis," *ACM Transactions on Information and System Security (TISSEC)*, vol. 12, p. 4, 2008.
31. E. Raftopoulos and X. Dimitropoulos, "Technical report: Shedding light on data correlation during network forensics analysis," Technical Report 346 2012.
32. H. Shulman and M. Waidner, "Towards Forensic Analysis of Attacks with DNSSEC," *ieeesecurity.org*, 2014
33. M. Rasmi and A. Jantan, "A New Algorithm to Estimate the Similarity between the Intentions of the Cyber Crimes for Network Forensics," *Procedia Technology*, vol. 11, pp. 540-547, 2013.
34. C. Milling, C. Caramanis, S. Mannor, and S. Shakkottai, "Network forensics: random infection vs spreading epidemic," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, pp. 223-234, 2012.
35. J. Huang and X. Adviser-Fu, "A comprehensive study of network forensics in terms of laws and technologies," *ACM(dl.acm.org)*, 2013.
36. M. Thapliyal, A. Bijalwan, N. Garg, and E. S. Pilli, "A Generic Process Model for Botnet Forensic Analysis," in *Proceedings of the Conference on Advances in Communication and Control Systems-2013*, 2013.
37. D. Herrmann, K.-P. Fuchs, and H. Federrath, "Fingerprinting Techniques for Target-oriented Investigations in Network Forensics," in *Sicherheit*, 2014, pp. 375-390.
38. M. Scanlon and T. Kechadi, "Digital evidence bag selection for P2P network investigation," in *Future Information Technology*: Springer, 2014, pp. 307-314.
39. Amor Lazeez, " A survey about Network Forensics Tools", International Journal of Computer and Information Technology, (ISSN: 2279-0764), Volume 2, Issue-1, January 2013.
40. S.Parate, S.M.Nirkhi, " A Review of Network Forensics Techniques for the analysis of Web Based attack", International Journal of Advanced Computer Research,(ISSN(print): 2249-7277, ISSN(online): 2277-7970), Vol.2, No.4, Issue-6, Dec 2012.
41. Ahmad Almulhem, " Network Forensics: Notion and Challenges ", King Fahd University of Petroleum and Minerals, Dhahran.
42. 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.
43. N. Meghanathan, S. R. Allam, and L. A. Moore, "Tools and techniques for network forensics," *arXiv preprint arXiv:1004.0570,International Journal of Network Security & its Application(IJNSA), Vol. 1, No.1*, 2010.
44. 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.
45. S. Bellovin, M. Leech and T. Taylor, ICMP Traceback Messages, Internet Draft, February 2003.
46. US Department of Commerce, Federal Information Processing Standards, Publication 198, The Keyed-Hash Message Authentication Code (HMAC), March 6 2002.
47. C. Adams, Internet X. 509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, Available at http://www.ietf.org/
48. 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.
49. Igino Corona, Davide Ariu And Giorgio Giacinto,‖HMM-Web: A Framework For The Detect ion Of Attacks Against Web Ap p lications‖ IEEE International conference on communication, pp1-6, 2009.
50. Nidal Qwasmi, Fay y az Ahmed, Ramiro Liscano, ‖ simulation of ddos attacks on p2p networks‖ , IEEE International conference on HPCC, pp 610-614, 2011.
51. Slim Rekhis And Noureddine Boudriga , ―A System For Formal Digital Forensic Investigation Aware Of Anti-Forensic Attacks‖ IEEE transactions on information forensics and security, vol. 7, no. 2, pp 635 - 650 april 2012.
52. Meixing Le, Angelos Stavrou, Brent Byunghoon Kang, ‖Doubleguard: Detecting Intrusions In Multitier Web Applications‖, IEEE transactions on dependable AND secure computing, vol. 9, no. 4, pp 512-525, july/august 2012.
53. L.Spintzer," Honeypots: Definitions and Value of Honeypots", http://www.tracking-hackers.com/papers/honeypots.html.
54. B. Scottberg, W. Yurcik, and D. Doss, "Internet honeypots: Protection or entrapment?" in *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*, 2002.
55. K. Takemori, K. Rikitake, Y. Miyake, and K. Nakao, "Intrusion trap system: an efficient platform for gathering intrusion-related information," in *10th International Conference on Telecommunications*, vol. 1, 2003, pp. 614–619.
56. M.Ponec, P.Giura, H.Bronnimann, J.Wein, " Highly Efficient Techniques for Network Forensics", Alexandria, Virginia, USA, ACM 978-1-59593-703-2/07/0011, Nov 2007.
57. N. King and E. Weiss. Network Forensics Analysis Tools (NFATs) reveal insecurities, turn sysadmins into System detectives. Information Security, Feb. 2002. Available at www.infosecuritymag.com/2002/feb/cover.shtml.
58. K. Shanmugasundaram, N. Memon, A. Savant, and H. BrÄonnimann. ForNet: A Distributed Forensics Network. In *Proc. of MMM-ACNS Workshop*, pages 1-16, 2003.
59. A. Broder and M. Mitzenmatcher. Network Applications of Bloom Filters: A Survey. In *Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, Illinois, USA, October 2002.

60. M. O. Rabin. Fingerprinting by random polynomials. Technical report 15-81, Harvard University, 1981.
61. S. Schleimer, D. S. Wilkerson, and A. Aiken.Winnowing: local algorithms for document fingerprinting. In *SIGMOD '03: Proceedings of the 2003 ACM SIGMOD international conference on Management of data*, pages 76{85, New York, NY, USA, 2003. ACM Press.
62. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E.Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer. Hash-based IP traceback. In *ACM SIGCOMM*, San Diego, California, USA, August 2001.
63. K. Shanmugasundaram, H. BrÄonnimann, and N. Memon. Payload Attribution via Hierarchical Bloom Filters. In *Proc. of ACM CCS*, 2004.
64. C. Y. Cho, S. Y. Lee, C. P. Tan, and Y. T. Tan. Network forensics on packet ¯ngerprints. In *21st IFIP Information Security Conference (SEC 2006)*, Karlstad, Sweden, 2006.

AUTHORS PROFILE

Anchit Bijalwan is working as an Associate Professor in Faculty of Electrical & Computer Engineering, Arba Minch University, Ethiopia. He has chaired the technical session for IEEE international conference on RICE and he is a committee member for the umpteen conferences. He was a keynote speaker of the IEEE conference which was held in El Salvador, Central America. His research interests include network security& privacy, Botnet forensics. He is a reviewer of Inderscience, IGI Global and many other publishers. He has 15 years of teaching experience.

Satenaw Sando is working with Faculty of Electrical & Computer Engineering as a Dean of Faculty of Electrical & Computer Engineering in Arba Minch University, Ethiopia. He has organized many events, seminar, workshops in department and faculty level.

Muluneh Lemma is a Director of Research and Community Service, Arba Minch Institute of Technology in Arba Minch University, Ethiopia. He has done master degree from Indian Institute of Technology, Delhi and PhD from Pohang University of Science & Technology, Korea.