Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing Network Flow Using Network Forensics

Sujata Mittal
M.Tech CSE Scholar, Department of Computer Science and Engineering, DCRUST, Murthal, Haryana, India

Rajvir Singh
Assistant Professor, Department of Computer Science and Engineering, DCRUST, Murthal, Haryana, India

***Abstract*— As Internet is growing rapidly i.e., everyone is using Internet, with increasing crimes and attacks being committed online there is always a threat of having malicious packets on network flow that can steal the information without showing that the data are being transmitted. It is vital for law enforcement and public security that forensics investigation of the nature and origin of these network attacks be effective and successful. In order to alleviate this problem and increase degree of relevance, there is need to investigate the network flow that contains malicious packets which can harm and affect the system. The prescribed report describes proposed approach for securing network flow that takes network data as input and apply detection technique to identify and capture malicious traffic. The output would be classifying the malicious and non-malicious network packets that are sent.**

***Keywords*— Network Security, Network Forensics, Malicious Data, Network Traffic, SVM**

I. INTRODUCTION

Network attacks are one of the most critical issues for Internet users nowadays. Although there are a lot of network attacks happened, they can be identified into one of two typical types: application level or network level attacks. To detect network level attacks, the information of network packet headers are usually analyzed to decide whether these packets contain any sign of attacks. The packet header analyzing approach is used to detect attacks such as port scan or DDOS attacks. The major limitation of this approach is it does not examine the data carried out in the network payload. Therefore, it cannot be applied to detect application level attacks. These attacks can only be detected by analyzing the content of payload data.

In order to deal with network attacks, some techniques have deployed such as firewall or intrusion detection systems. However, those techniques still contains drawbacks during the process of network attack investigation. Therefore, network forensics is addressed. From the definition of network forensics, it is well defined that network forensics is not another term for the network security. Network security protects system from attacks whereas network forensics focuses on the reconstructing the evidence of the attack. In **2001 DFRWS (Digital Forensic Research Workshop)[4]** determined network forensics as "The utilized of scientifically established proficiency to gather, mix, identify, examine, correlate, subject, and document digital evidence from multiple, actively processing and transmitting digital sources to resolve uncovering facts related to the projected intent, or evaluated success of unauthorized actions entailed to interrupt, corrupt, and/or compromise system components as well as rendering information to assist in answer to/or recovery from these activities".

The aim of network security is to detect malicious behavior in order to protect systems in real time. This process is continuous and never stops if the system is still running. On the contrary, network forensics deals with post-mortem investigation of the attack. In other words, network forensics focuses only on the stored network packets. Although network security and network forensics have different functionalities, network attack identification is the main purpose of them. In order to identify attacks, network packets must be intercepted and analyzed**M. Rasmi, A. Jantan, H. Al-Mimi [2].** However, interception of all network packets is impossible due to the large amount of data being transferred over high speed networks such as fiber optic nowadays. The main task of data analysis is to classify current network payload belonging to benign or malicious activities. Obviously, benign data is not the main focus or data analysis of network assault detection solutions. Only malicious data need to be stored for further analysis.

Moreover, malicious data analysis is the main task of network forensics, thus those data must be stored somewhere. A better malicious data detection solution will help to reduce the amount of data stored. Furthermore, malicious data in the network normally contains executable data, such as virus, spyware, worm and Trojan, which are harmful to the network systems or even adware programs that cause annoyance to Internet users. Therefore, identifying the executable data in network data traffic is very important in network forensics. Basically, an attack is indicated by network data in which executable content is carried. However, detection of executable content in network traffic is not an easy task. One of the main factors that affects seriously to executable content detection is accuracy. A low accurate detection rate leads to more false alarm warning or more wasting investigation efforts of network forensics programs.

II. WHAT IS NETWORK FORENSIC?

Network forensics is an act of capturing, recording, and analyzing network audit trials in order to detect the source of security violate or other information assurance problems. The term "network forensics" was precede by the computer and

firewall proficient Marcus J. Ranum in early 90s, but borrowed from legal and criminology fields where "forensics" is related to probe of crimes.

Why there is need of Network Forensic to secure network flow?

Following parameters needs to be considered while securing network flow from malicious packets:

- Network traffic recording and analysis: Network Traffic Analysis can also be used in network security by monitoring the traffic flow. Traffic Flow describe the destination IP address destination port number, source IP address, source port number and the amount of data i.e., size of packets are being sent.
- Anomaly detection: The network contains every type of packets while transmitting the data, the aim of network forensic is to detect anomalies i.e., harmful or malicious data. **Z. Like and G. B. White [1].**
- Incident recovery
- Network performance

Network forensic arrangements are categorized into two kinds every single established on assorted characteristics like patriotic, collection and nature. Purpose: 'General Web Forensics' to enhance web protection and 'Strict Web Forensics' to become facts fulfulling lawful principles and requirements. Collection of Traffic: 'Catch-it-as-you-can' arrangements whereas all packets bypassing across a particular traffic point are seized and analysis is afterward completed needing colossal numbers of storage and 'Stop-look-and-listen' arrangements whereas every single packet is analyzed in recollection and precise data is saved for upcoming analysis needing a faster processor. The web forensic arrangement is an appliance alongside hardware and pre-installed multimedia or completely a multimedia tool.

III. CHALLENGES

The frameworks and implementations for web forensic research have been surveyed in the preceding section. The limitations and specific research gaps associated alongside disparate periods in every single implementation are given below.

Collection and detection:-The early pace in web forensic research involves collection of web traces and detection of attacks. The traces involve Web forensics and firewall logs, logs generated by web services and requests, packet arrests by sniffers and NFATs. The trial is to recognize functional web events and record minimum representative qualities for every single event so that the least number of data alongside highest probable facts is stored. This aftermath in reduction of data storage requirements. A data digest will be adequate for invention of malicious deeds and a maximum arrest is needed for reconstruction of attack behavior.

Data mixture and examination:-The data seized from assorted instruments have to be aggregated and examined to notice whether investigation ought to be commenced. Data mixture of all the logs amassed from assorted protection instruments used in every single hosts on the whole web is a critical problem. The dependencies of packet qualities from assorted instruments and reconnaissance of qualities from disparate hosts validate an attack. Characterization of anomalous web events and discriminating attack traffic from legitimate traffic by hunting for outlines of anomalies is a main challenge.

Analysis :-The critical pace in the whole procedure of web forensics is to examine attack data and appear at a conclusion, pointing at the source. Association and clustering of web events demand to be completed so that scrutiny of colossal volumes of data to comprehend their connection alongside aggressions becomes easy. Parsing and research of convoluted protocols additionally needs focus. Outline credit of anomalies employing soft computing and data excavating methods can be requested for association, correlation and link analysis. The classification of assault outlines and assault reconstruction methods utilized to comprehend the aim and methodology of the attacker needs research focus.

Investigation:-The investigation have to enable attribution of an assault to a host or a network. The aftermath have to encounter the admissibility criteria in a court of law. The research of logs and supplementary web traces have to lead to the basis of attacks. IP traceback involves drawing back to the basis address of the attacker by vanquishing IP spoofing. Noticing and profiling TCP connection shackles can hold out the pacing stones utilized to raise an attack. Crafting a topology database and IP locale mapping to find an attacker geographically is a main challenge. As new protocols like IPv6, come to be operational and accepted, there will be a outstanding demand to ascertain events including these protocols.

Event response:-Active real-time reply to the web misuse is to be gave so that vital data are not capitulated by the period reply is initiated. The reply procedures are to be dispatched instantly after alerts begin. The key subject to be upheld is that the attacker have to not be cognizant of the response.

IV. RELATED WORKS

Several researches and studies have been conducted by researchers in order to secure network flow, detecting anomalies, capturing malicious packets, to investigate the network attacks.

E.S. Pilli et al. [5] proposed a generic framework for network forensics investigation. The framework is illustrated on Figure 2, consists eight important phases. Among those phases, the authors described Collection as difficult and important phase because the network changes rapidly. So, it is very difficult to reconstruct the traces of the evidence. The authors also described that the framework is used for both real time and post attack scenario. As, first five phases included incident response is used for real time network and after that for post attack. The phases of the generic framework are precisely explained.

A generic network forensics mode is proposed to detect, collect, analysis and investigation of the network traffic to prevent the network attacks and to investigate them.

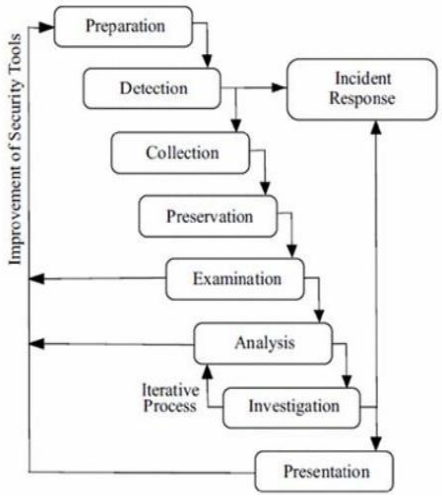

Figure 1 Generic process model for network forensics [16]

- Preparation Phase: Network Sensors (Like intrusion detection system, firewalls, packet analyzers) needs to be deployed at various points in a network for 10 network forensics. First to obtain authorizations and legal warrants to maintain privacy.
- Detection Phase: Alert is generated by sensors whenever there is a violation in protocols or a security breach. A quick validation is done to confirm the suspected attack.
- Incident Response Phase: A response is initiated to validate the attack and at the same time a decision is made whether to continue the investigation or gather more information.
- Collection Phase: The most difficult phase is collection phase because data changes vigorously on the network. At the later stage, it will be difficult to regenerate the same traces of evidence in a victim's network.
- Preservation Phase: Copies of original data is produced onto legal process is used and original data remain untouched.
- Examination Phase: The main thing is to integrate all the data collected from various sensors. There may be a chance of redundant data and overlapping time zone which is needed to be considered.
- Analysis Phase: Collected evidence is analyzed by using statistical, data mining approach to search the data and match the attack pattern with the existing patterns.
- Investigation Phase: The purpose is to determine a path between victim networks to the point of attack origin. The investigation phase and the analysis phase are iterative in nature. After investigation analysis is done to ensure the attack pattern match.
- Presentation Phase: It is the last stage in which an understandable documentation is presented in a systematic format along with the observation and explanations on how to prevent the future attacks.

The proposed network forensic model is used to collect, preserve and present the details of network traffic and evidence, the main part are to capture and analyze the network traffic for the better result.

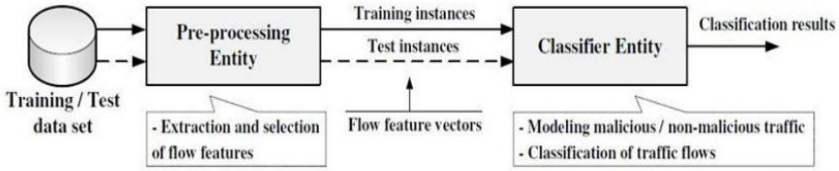

Figure 2 Flow-based botnet detection using supervised machine learning [3]

In Figure [2], the authors proposed a model to detect and classify malicious and no malicious traffic on the basis of feature extraction. List of features extracted:

1. Destination port
2. Source port
3. Total number of packets
4. Total number of Bytes (B)
5. Total payload length (in B)
6. Mean of number of B per packet
7. Percentage of packets < 128B
8. Percentage of packets in (128B, 1024B)
9. Percentage of packets in (1024B,1518B)
10. Percentage of packets > 1518B

MatijaStevanovic et al. [6] proposed a model. The purpose of this work is to detect malicious and non-malicious traffic using MLAs in which the author used supervised machine learning algorithms to classify the malicious and non-malicious packets and did some experimental analysis to classify CPU time to execute MLAs.

Experiments were conducted using ISOP dataset that represents the combination of four publicly available malicious and non-malicious datasets. The ISOP dataset includes two malicious traffic datasets. The author we consider eight highly regarded supervised MLAs: NB, B Net, LR, ANN, SVM, C4.5 decision tree, R Tree and R Forest. The proposed work describes the detection of malicious packets using supervised machine learning by extracting the selected features only.

The authors Khoa Nguyen et al. [8] proposed an approach established on Shannon entropy and machine acquiring techniques to describe feasible subject for anomaly-based network attack detection in network forensics systems.

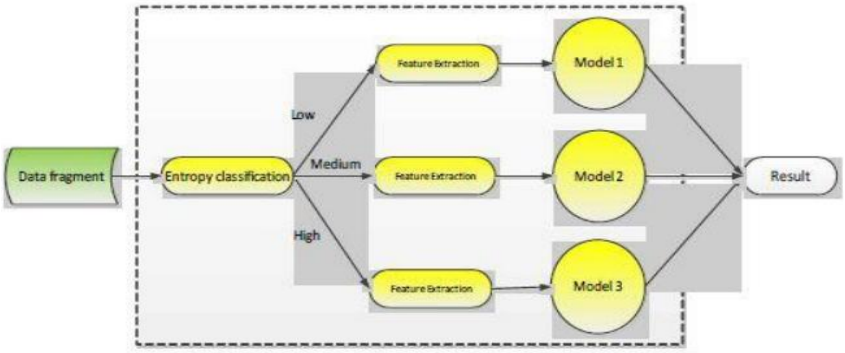

Figure 3 Diagram of executable data detection [8]

In the detection phase, a data fragment from network traffic is specified as a low medium or high entropy data fragment. Depending on its randomness value, the corresponding feature vector will be summarized from the data fragment then flowed into one of three models (Model 1, 2, or 3) in prescribe to identify whether or not this data fragment contains executable content.

The proposed architecture used Shannon entropy to calculate values before feeding to classifier that is low, medium, high that used to detect the executable files on the dataset used in the experiment.

S. Saad, I. Traore, A. Ghorbani, B. Sayed et al. [7] propose a novel technique for characterizing and observing botnets using network traffic behaviors. It focuses on detecting the bots before they launch their attack. A botnet is a collection of computers connected to the Internet which have been compromised and are being assured remotely by an attacker via malicious software called bots.

In this paper user use command and control (C&C) phase. it allows the detection of bots that spreadunder the radar through malicious email, websites, file sharingnetworks before these bots attack their victims. Although none of these techniquescan satisfy all the requirements of an online botnet detectionframework.it need new techniques to investigate that satisfy all the requirement .

SindhuKakuru [9] proposed an architecture which is based on behavior of the user, the model helps to monitor the activities of user and if any non-behavioral activities seen, an alert is sent to the network administrator.

The author used wire shark tool to analyze the activities of user. This paper has shown a method to prevent one of the vulnerabilities of network security. Since this tool works on user's behavior, the network administrator can identify the user even if the user changes his/her computer and works on different one.

TalaTafazzoli et al. [10]proposed an architecture to store the raw traffic using indexing to store in database and to analyze malware and network traffic in largescale networks. Network traffic collection and indexing subsystem:

- Database management subsystem
- Analysis scheme
- SOC Communication part
- Database.

Traffic data can be collected with two dissimilar engineering. First, span/mirror ports indicate the ability to copy traffic from all/one port to a single port. Second, Tap devices monitor the traffic flowing between two points in the network.

The main purpose of forensic systems is to help the detective to describe crook and crime signs. Strength of a network forensic system depends on its ability to treat network traffic with a speed proportional to data transmission and analysis.

John Haggerty, David Llewellyn-Jones et. al (2008)[11] in this paper, A main supremacy of data knowledge is the ease, speed and volume of data that could be public amid hosts. Though, this has given development to concerns above paedophile attention and the range of malicious digital pictures amongst this community. In web forensic investigations a wealth of data relevant to the investigation will reside inside the web itself and on disparate hosts. Current computer forensics instruments are projected for the scutiny of grabbed hard propels rather than investigating data inside a network. In this paper they present FORWEB, a novel scheme for automated file fingerprinting of malicious pictures resident on Web servers. The FORWEB instrument has been industrialized to assistance in investigations that need the

invention of digital pictures on Web servers and the Globe Expansive Web. It seizes a database of picture fingerprints generated employing the FORSIGS forensics instrument and negotiates a Web locale or collection of locations to recognize each relevant images. Across the use of a number of examination case studies on real globe Web locations they are able to clarify the viability of the procedure, and furnish an indication of the period demanded to find photo album and file allocating sites. Even though they ponder the instrument by now to have potentially functional request, more assessing will be needed to institute how well it assesses to a human operator. In upcoming work, they consequently target to accept more tests. At present, the robot is able to traverse locations established on a number of criteria.

Laurence D. Merkleet. al (2008) [12] in this paper, The intention of this scutiny is to examine the automated scutiny of web established facts in reply to cyberspace attacks. The automated scutiny methods to be industrialized and learned will join the efficiency of both continuing and novel innate find methods alongside the scalability and robustness of evolutionary computation and supplementary computational intellect techniques.

This scutiny will produce: A arrangement for producing realistic web forensics datasets. This evolutionary algorithm-based arrangement additionally will be functional in assessing the effectiveness opposing novel aggressions of assorted protection mechanisms, and in particular of intrusion detection systems.

- A proper characterization of the data needed and the data generated by every single of the periods of a average web forensics investigation.
- An automated web forensics instrument that integrates the average instruments utilized in every single of the periods of a web forensics investigation. The instrument will be open basis and obtainable to both web forensics researchers and practitioners. Furthermore, it will be extensible, thereby permitting supplementary researchers to give to the more automation of the web forensics process.

KeyunRuan, Prof. Joe Carthyet. al (2011) [13] in this paper, Cloud computing is approximated to be one of the most transformative technologies in the past of computing. Cloud associations, encompassing the providers and clients of cloud services, have yet to institute a well-defined forensic capability. Lacking this they are incapable to safeguard the robustness and suitability of their services to prop investigations of convict activity. The development of cloud computing is shoving digital forensics into a new horizon. Countless continuing trials are exacerbated in the Cloud, encompassing jurisdictional subject and the lack of global collaboration, as the new nature additionally brings exceptional opportunities for foundational standards and policies.

SrinivasMukkamala& Andrew H. Chanted et. al (2003) [14] in this paper, Web forensics is the discover of analyzing web attention in order to notice the basis of protection strategy violations or data assurance breaches. Seizing web attention for forensic scutiny is easy in theory, but moderately trivial in practice. Not all the data seized or recorded will be functional for analysis. Recognizing key features that expose data deemed worthy for more intelligent scutiny is a setback of prominent care to the researchers in the field.

A number of observations and conclusions are drawn from the aftermath reported:

- SVMs outperform ANNs in the vital respects of scalability (SVMs can train alongside a big number of outlines, as ANNs should seize a long period to train or flounder to encounter at all after the number of outlines gets large.); training period and running period (SVMs run an order of magnitude faster); and forecast accuracy.
- SVMs facilely accomplish elevated detection accuracy (higher than 99%) for every single of the 5 classes of data, even though of whether all 41 features are utilized, merely the vital features for every single class are utilized, or the coalition of all vital features for all classes are used.

We note, though, that the difference in accuracy figures incline to be extremely tiny and could not be statistically momentous, exceptionally in think of the fact that the 5 classes of outlines differ in their sizes tremendously. Extra definitive conclusions can merely be made afterward analyzing extra comprehensive sets of web traffic data.

Ahmad Almulhem, IssaTraoreet. al (2005) [15] in this paper,Network Forensics is an vital expansion to the ideal of web protection whereas emphasis is conventionally locale on prevention and to a lesser extent on detection. It focuses on the arrest, recording, and scutiny of web packets and events for investigative purposes. It is a youthful earth for that extremely manipulated resources are available. A web forensics arrangement can clarify to be a priceless investigative instrument to cope alongside computer attacks. In this paper, they discovered the case of web forensics and counseled design of web forensics system. They next debated our implementation and obtained results. The counseled arrangement manages to amass attack data at hosts and network. It is additionally capable of circumventing encryption if utilized by a hacker. In the upcoming, they design to spread our arrangement design alongside a fourth module shouted it expert module. The expert module, to be requested as an expert arrangement, will examine the logged data, measure and reconstruct key steps of assault. There are countless facts that can be utilized to systematically describe ongoing aggressions and thereby could assist to craft the vision center of such expert system.

Chia Yuan Cho, Sin Yeung Lee et. al (2006)[17] in this paper, They present an way to web forensics that makes it feasible to draw the content of all traffic that bypassed across the web via packet content fingerprints. They develop a new data structure exclaimed the “Rolling Bloom Filter” (RBF), that is established on a induction of the Rabin-Karp thread matching algorithm. This merges the two key gains of space efficiency and an effectual content matching mechanism. This additionally achieves analytically predictable Fake Affirmative Rates that can be manipulated by tuning the RBF parameters. Leveraging on these visions, they have projected and requested a useful Web Forensic Arrangement that gives the skill to reconstruct the sequence of events for post-incident analysis. They have gave an way to web forensics that makes it feasible to draw the content of all traffic that bypassed across the web via packet content

fingerprints. To accomplish this, they have industrialized the Rolling Bloom Filter, that is based on a generalization of the Rabin-Karp string-matching algorithm. This prosperously merged the two gains of space efficiency and an effectual content matching mechanism. Our method additionally attained analytically predictable Fake Affirmative Rates that can be manipulated by tuning the RBF parameters.

V. CONCLUSION AND FUTURE SCOPE

The internet is growing rapidly, in the past decade itself, a large number of papers have discussed different approaches and act for discovering and analysis of malware traffic and its security issues. Most of them proposed a generalized approach to secure the flow but the data is labeled on which existing pattern can be matched. Securing network is very essential now days. Everything is being done using Internet and most of the unauthorized users sent malicious files to keep track of the transactions being processed online. Using the approach, we can divide the traffic into clusters which can help in detecting and capturing malicious data and help in analyzing network traffic. Apart from this network forensics is used where malicious traffic will be found to overcome the malicious data and to investigate. Network forensics is not one more word for web security. It is an spread period of web protection as the data for forensic analysis are amassed from protection produce like firewalls and intrusion detection systems. The aftermath of this data analysis are utilized for investigating the attacks. Though, there could be precise offenses that do not rupture web protection strategies but could be lawfully prosecutable. In current trend, malicious packets are being sent to other hosts to steal information via Internet. With increase in attacks and crimes committed online, there is a need to analyze the Network Traffic and secure network flow by identifying harmful data. The objective of given project is "To secure Network flow by discover and catch malicious packets using Network Forensics". During this project, a user is able to learn about network forensics, network forensics tools, how to identify and capture malicious packets, how to store network traffic .The intended final outcome of project is the classification of malicious and non-malicious packets from network flow.

REFERENCES

[1] Z. Like and G. B. White, "An Approach to Detect Executable Content for Anomaly Based Network Intrusion Detection," in Parallel and Distributed Processing Symposium, 2007. IPDPS2007. IEEE International, 2007, pages 1-8

[2] M. Rasmi, A. Jantan, H. Al-Mimi, "A new approach for resolving cybercrime in network forensics based on generic process model", IEEE 6th International Conference on Information Technology, May 8th 2013, pages 265-271

[3] M.Rouse,http://searchsecurity.techtarget.com/definition/networkforensics accessed on 20th November 2015.

[4] Report from the First Digital Forensic Research Workshop (DFRWS), November 6th 2001

[5] Emmanuel S. Pilli, Ramesh C. Joshi, RajdeepNiyogi "A Framework for Network Forensic Analysis" 2010, Springer Berlin Heidelberg International Conference, ICT 2010, Kochi, Kerala, India, September 7-9, 2010,pages142-147

[6] MatijaStevanovic and Jens Myrup "An efficient flow-based botnet detection using supervised machine learning" 2014 International Conference on Computing, Networking and Communications (ICNC),3-6 February 2014, Honolulu, HI , pages 797 – 801

[7] S. Saad, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, J. Felix, and P. Hakimian, "Detecting p2p botnets through network behavior analysis and machine learning," in Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on, July 2011, pp. 174 –180

[8] Khoa Nguyen, Dat Tran, Wanli Ma, and Dharmendra Sharma." An Approach to Detect Network Attacks Applied for Network Forensics" 2014 IEEE 11th International Conference on Fuzzy Systems and Knowledge Discovery, 19-21 Aug. 2014, Xiamen, pages 655 – 66022

[9] SindhuKakuru "Behavior Based Network Traffic Analysis " 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN),Xi'an, 27-29 May 2011

[10] TalaTafazzoli, ElhamSalahi and HosseinGharaee"A PROPOSED ARCHITECTURE FOR NETWORK FORENSIC SYSTEM IN LARGESCALE NETWORKS" 2014 IEEE UK Sim -AMSS 16th International Conference on Computer Modeling and Simulation, 26-28 March 2014, Cambridge, pages.

[11] Haggerty, John, David Llewellyn-Jones, and Mark Taylor. "FORWEB: file fingerprinting for automated network forensics investigations." InProceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, p. 29. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[12] Merkle, Laurence D. "Automated network forensics." In Proceedings of the 10th annual conference companion on Genetic and evolutionary computation, pp. 1929-1932. ACM, 2008.

[13] Ruan, Keyun, Joe Carthy, and TaharKechadi. "Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis." InProceedings of the Conference on Digital Forensics, Security and Law, p. 55. Association of Digital Forensics, Security and Law, 2011.

[14] Mukkamala, Srinivas, and Andrew H. Sung. "Identifying significant features for network forensic analysis using artificial intelligent techniques."International Journal of digital evidence 1, no. 4 (2003): 1-17.

[15] Almulhem, Ahmad, and IssaTraore. "Experience with engineering a network forensics system." In Information Networking. Convergence in Broadband and Mobile Networking, pp. 62-71. Springer Berlin Heidelberg, 2005.

[16] Pilli, Emmanuel S., Ramesh C. Joshi, and RajdeepNiyogi. "Network forensic frameworks: Survey and research challenges." *Digital Investigation* 7, no. 1 (2010): 14-27.

[17] Cho, Chia Yuan, et al. "Network forensics on packet fingerprints." *Security and Privacy in Dynamic Environments*. Springer US, 2006. 401-412.

COMPARATIVE ANALYSIS

Table 1: Comparative analysis of papers

S.No.	Title	Work details	Pros	Cons
1.	A Framework for Network Forensic Analysis	The generic networkforensic model isproposed that is used to collect, preserveand present the detailsof network traffic and evidence.	(a) Uses to investigate the attacks. (b)Examine the network traffic attacks with the existing attacks to detect.	(a) Noprocedure to secure networkflow is described.
2.	**MatijaStevanovic et. al [6]**An efficient flow based botnet detection using supervised machine learning	Detecting malicious traffic using supervised machine learning algorithms.	(a) Classification of malicious and non malicioustraffic.	(a) Training dataset is needed to compute the result.
3.	**Khoa Nguyen et.al[8]** An Approach to Detect Network Attacks Applied for Network Forensics	Shannon entropy and machine learning techniques to describe feasible content for anomaly-based network attack detection in network forensics systems	(a) Data fragment from network traffic is determined as a low medium or high entropy data fragment.	(a) Calculating entropy is overhead to system after which MLAs applied.
4.	Behavior Based Network Traffic Analysis	Behavior based architecture is proposed that monitors the user activities.	(a) Uses Wire shark to capture user activities. (b) Matches the activities with existing in database.	(a) If user perform the activities from other system, alert sent to network dministrator.
5.	**TalaTafazzoli et. al [10]** A Proposed Architecture for Network Forensic System in Large-scale Networks	The proposed architecture provides analysis of malware and network traffic.	(a) Uses indexing while storing network traffic. (b) Store SEIMs in database which can be accessed through database management.	(a) No security of network flow by capturing malicious packets. (b) Uses for large scale system

