Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 10 (2017) pp. 2963-2972

http://www.ripublication.com

Proposing a Framework for Digital Network Forensic Evidence Accumulation in Cloud Environment

N. Venkataramanan
Research Scholar, Department of Computer Science
Periyar E.V.R. College (Autonomous), Trichy, Tamilnadu, India.

Dr. T.N. Ravi
Assistant Professor, Department of Computer Science
Periyar E.V.R. College (Autonomous), Trichy, Tamilnadu, India.

Abstract

As on date, Internet is the most intense medium which encourages the fluctuated services to various clients. Moreover, it has turned into nature for cyber issues where, it assaults of numerous sorts (ideological, revenge and financial) are being propelled. "Network Forensic is a sub-branch of advanced criminology identifying with the observing and examination of PC network activity for the reasons for data gathering, legitimate confirmation, or interruption recognition." The MPMLC data back up and synchronized in Cloud Storage. The proposed MPMPLC (Mist-Packet Marking and Packet Logs/Caches) framework is deployed for storing up the logs/Caches of an individual static IP address and also dynamic IP address. This framework will upgrade the examination in the network forensics if any crime has taken place.

Keywords: Network Forensic, Logs/Cache, Cloud Storage, MPMPLC Framework, Evidence Collection Methods

I. INTRODUCTION

In the recent development of technology, forensic turned as a leading network; investigators in their regular work with live frameworks that can't be taken disconnected from the net. It may incorporate switches, routers, and different sorts of network gadgets, and basic servers [1]. In hard drive forensics investigation,

investigators are formed to minimize framework alteration when directing forensics. It is much simpler to minimize framework change when working with a logged off duplicate of a compose ensured drive than with creation network server and equipment.

In network forensic, examiners furthermore, efficiently work to minimize framework adjustment due of measurable traffic [2]. Notwithstanding, in these cases, the investigators regularly don't have the advantage of a disconnected from the net duplicate. Also, network based evidence is regularly exceeding and unstable. And it must be gathered through dynamic implies that naturally adjust the framework facilitating the proof. So, when investigators can sniff the movement utilizing port observing or tapping a link, there is constantly some effect on nature.

This effect can once in a while be minimized through cautious choice of acquisition networks, yet it can never be killed completely.

Each interaction the investigator has a live framework somehow it changes, pretty much. In reality the investigator, adjusts a crime scene just by strolling on the floor. It utilizes the expression "impression or footprint" all through the scene to allude the effect that an investigator has on the frameworks under examination.

The crime will always leave some impression or footprint. In regular, the extent of the impression required must be weighed against the requirement for convenience in information accumulation. To take an ideal opportunity in recording exercises painstakingly with the goal that you can exhibit later that vital proof was not changed. Continuously be aware of your impression and tread daintily.

II. REVIEW OF LITERATURE

A. *Digital Evidence*

"Digital Evidence" [3] is a documentation that fulfills the necessities of "evidence" in a procedure, however exists in electronic computerized structure. Digital Evidence may rest in minute spots on spinning platters, charged to more prominent or lesser degrees in a to some degree nonvolatile plan, however in any case, indiscernible with the exception of through numerous layers of reflection and document framework protocols. In different cases, computerized proof might be charges held in unstable storage, which disseminate inside seconds of lost energy to the framework. Digital evidence might be not any more substantial, nor lasting, than voltage difference levels on copper wires, beats of photons or radio recurrence waves.

Digital Evidence which includes in the cases like:

• IM sessions and Emails

• Records of Installment received and Invoices

• Routinely keeps the access log.

B. ***Network Based Digital Evidence***

Network based Digital Evidence [3][4] is digital evidence that is delivered as an after effect of correspondences over a network. The essential and auxiliary storage media of PCs (e.g., the RAM and hard drives) have a tendency to be productive feed for forensic investigation. Because of information remanence, persevering capacity can hold forensically recoverable and important evidence for quite a long time, days, even years past document deletion and storage reuse. Conversely, network based digital evidence can be amazingly unstable. Packet dance over the wire in milliseconds, vanish from switches in a split second. Sites change contingent upon from where they're seen and when.

The prerequisites for suitability of network based digital evidence are cloudy. Regularly, the source that produced the proof is not realistic or can't be recognized. At the point when the evidence is a recording of a email, chat log or blog posting, the personality of the gatherings in the discussion (and along these lines the creators of the announcements) might be hard to demonstrate. At the point when the evidence is a site, the disputant may need to give supporting proof to exhibit that the picture displayed in court is the thing that really existed at the time and area that it was as far as anyone knows saw.

Examples of "network-based digital evidence" can include:

• IM sessions and Emails

• Web based email in browser activity

• Routinely keeps the packet logs

III. CHALLENGES RELATED TO NETWORK FORENSIC

Network based evidence [4] postures extraordinary difficulties in a few ranges, including storage, acquisition, seizure, privacy and tolerability. Some normal difficulties beneath in this paper.

Acquisition: It can be hard to find particular evidence in a system environment. Networks contain such a variety of conceivable wellsprings of proof—from remote access focuses to web proxies to focal log servers—that occasionally pinpointing the right area of the evidence is precarious.

Content: Unlike file systems, which are intended to contain all the substance of documents and their metadata, network gadgets might possibly store proof with the level of granularity wanted. Network gadgets frequently have extremely restricted

capacity limit. Typically, just chose metadata about the exchange or information exchange is kept rather than complete records of the information that crossed the network.

Storage: Network gadgets usually don't utilize optional or constant storage. As an outcome, the information they contain might be so unpredictable as to not survive a reset of the gadget.

Privacy: Depending on locale, there might be lawful issues including individual protection that are special to network based acquisition systems.

Seizure: Seizing a hard drive can trouble an individual or association. Regularly, in any case, a clone of the first can be developed and sent such that basic operations can proceed with restricted disturbance. Grabbing a network gadget can be considerably more problematic. In the most amazing cases, a whole network section might be cut down inconclusively. Under most circumstances, notwithstanding, specialists can minimize the effect on network operations.

Admissibility: At present File system based evidence is currently routinely conceded in both common and criminal procedures. For whatever length of time that the document framework based evidence is legally gained legitimately took care of, and important to the case, there are clear points of reference for verifying the proof and letting it be known in court. Interestingly, organize forensic sciences is a more up to date way to deal with computerized investigations. There are once in a while clashing or even non existing legitimate points of reference for confirmation of different sorts of network based digital proof. After some time, network based digital evidence will turn out to be more pervasive and case points of reference will be set and institutionalized.

IV. PROPOSED MPMPLC FRAMEWORK FOR DIGITAL NETWORK FORENSIC EVIDENCE ACCUMULATION

The figure 1 represents the proposed framework incorporates the primary, secondary IPS connection management units, evidence collective methods by Mist IP Trace and static and dynamic IP management of TCP and UDP control devices, authentication phase and auto backup synchronization model. The above challenges in the network forensic can be overcome by utilizing this framework for network forensic evidence in collecting phase.

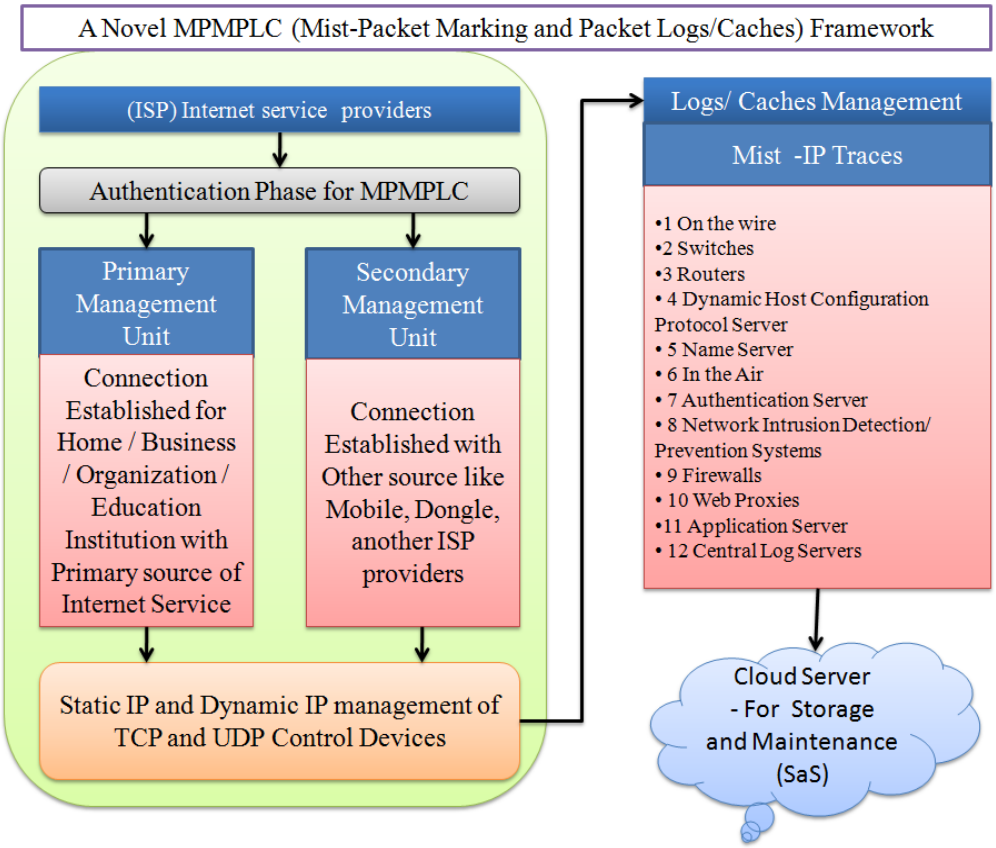

Figure 1: Proposed MPMPLC Framework for Digital Network Forensic Evidence Accumulation

A. ***Primary and Secondary Management Units***

This framework has primary and secondary management units. The connection established through ISP for Home/Business/organization/Education institution with Primary source of internet services in the primary management unit. And however, the internet connection established with other sources like Mobile, Dongle, or other ISP providers should registered with secondary management unit. The entire networks can be maintained effectively by MPMPLC's authentication phase.

B. ***Static and Dynamic IP Management of TCP and UDP Control Devices:***

The primary and secondary unit of the IP address is static/dynamic. In this process, static IP and dynamic IP can be managed the TCP and UDP controlled Hardware devices like laptops, PC's, The primary and secondary unit of the IP address is static/dynamic. In this process, static IP and dynamic IP can be managed the TCP and UDP controlled Hardware devices like laptops, PC's.

C. ***Authentication Phase***

The MPMPLC Framework registered with authentication ID of the clients. And the ID is the initial source for adding the primary and secondary units. In addition, it is synchronized with cloud storage by default. The function of the cloud services has been maintained by the government.

D. ***Auto backup and Synchronization Model:***

The MPMPLC's data has been stored automatically by the use of synchronization method.

E. ***Mist – IP Trace Evidence Collecting Methods:***

Each environment is interesting and unique. The huge money related organizations have altogether different network topologies, equipment and staff than local government offices or little human services and other workplaces. Actually, even in this form, in the event that you stroll into any association it will discover similitudes in network equipment and normal outline procedures for network base. There are numerous wellsprings of network based proof in any environment, including web proxies, intrusion detection network, routers, and that's only the tip of the iceberg.

1) On the Wire and in the Air

Physical cabling is deployed to give network between stations on a LAN and the nearby switches, in addition to amongst routers and switches. Network cabling frequently comprises of copper, as either coaxial link or twisted pair (TP) or coaxial link. Information is motioned on copper when stations on the mutual medium autonomously change the voltage. Likewise, Cabling can comprise of fiber-optic lines, which are made of flimsy strands of glass. The Stations are associated by means of fiber sign information through the nearness or nonattendance of photons. Both copper and fiber-optic mediums support advanced flagging (digital signaling).

Forensic Value: The Investigators of network forensic can take advantage of physical cabling to duplicate and safeguard the network traffic as it is transmitted over the line. The taps can extend from "vampire" taps, which truly cut the protection and reach copper wires, to surreptitious fiber taps, which twist the link and slice the sheathing to uncover the light flags as they cross the glass. Moreover, numerous business merchants produce base taps, which can connect to regular link connectors and particularly intended to repeat signs to an aloof station without debasing the first flag.

2) Switches

Switches [5] are the paste that holds our LANs together. They are multiport spans that physically associate different stations or network sections together to shape a LAN. In advanced deployments', it tends to see the changes which are associated with different switches relentlessly to shape the complex exchanged network environment.

In an ordinary deployment, associations have "center" switches, which total activity from a wide range of portions, and additionally "edge" switches, which total stations are individual sections. Thus, traffic starting with one station then onto the next inside an endeavor may navigate any number of switches, contingent upon the physical network topology and the areas of the stations inside it. Forensic Value: Switches contain a "Content addressable memory" (CAM) table, which stores the mappings between physical ports and every network card's MAC address [5]. In given to a particular gadget's MAC address, network agents can look at the change to decide the relating physical port, and possibly follow that to a divider jack and an associated station. In further, switches give a stage from which, examiners can catch and save network traffic. With numerous sorts of switches, network staff can design one port to "reflect" (duplicate) activity from any or all different ports or VLANs, in permitting examiners to catch traffic from the reflecting port with a packet sniffer.

3) Routers, Web Proxies and Central Log Server

Routers connect diverse subnets or networks together and encourage transmission of packets between various network fragments; notwithstanding it have distinctive addressing plans. Routers [5] include a layer of deliberation that empowers the stations on one LAN to send traffic bound for stations on another LAN. Internet working and utilizing routers is the gadget that permits us to construct grounds wide metropolitan networks (MANs) or interface remote workplaces around the world through wide area networks (WANs). From a specific viewpoint, the whole worldwide Internet is only a global area network (GAN), which is associated through a complex multilayer web of routers.

Forensic Value: There is a routing tables for routers, where switches have CAM tables. Routing tables map ports on the router to the networks that they interface. This permits a forensic examiner to follow the way that network movement takes to navigate the different networks. (Note that this way can change powerfully taking into account network traffic levels and different components.) Depending on the particular gadget's capacities, routers may likewise work as packet filters, precluding the transmission from claiming certain sorts of traffic in view of source, destination, or port routers may record the denied traffic (or here and there keep up insights on permitted activity). Numerous venture class routers can be arranged to send logs and stream record information to a focal logging server, which is to a great degree in

accommodating for investigator, as this makes it simple to connect the incidents from different sources. The logs stored on the switch itself might be unstable and subject to eradication if the gadget is rebooted or if the accessible stockpiling is surpassed.

4) Dynamic Host Configuration Protocol (DHCP) Server

The Dynamic Host Configuration Protocol (DHCP) [6] is broadly utilized as the mechanism for relegating the IP addresses to LAN stations, accordingly they can speak with different stations on the nearby network, and in addition with the networks crosswise over the internetworked associations. From the commencement of networks services, the chairmen need to be physically design the singular desktops with static IP addresses. DHCP was produced to give computerized IP address assignments, which could change strongly as required and significantly diminishing the manual workload for executives. DHCP service is recurrently given by the edge gadgets that accomplish routing between networks (switches, remote access focuses, and so on.), on the other hand, it is not exceptional to determine this service provided by foundation servers.

Forensic Value: Frequently, the investigation starts with the IP address of a host which is associated with being required in some kind of aggressive circumstances—whether it was the casualty of an assault, the beginning, or maybe both. One of the primary assignments is the investigator must embrace to discriminate and/or physically find the gadget in view of its IP address. At this instance when DHCP servers relegate (or "rent") the IP addresses, they typically make a record of the incidents, which integrates the doled out IP address, the MAC address of the gadget accepting the IP address, and in that phase the lease was given or restored. The dissimilar subtle elements, for instance, the asking for network's hostname, might be logged also. As a result, DHCP logs can exhibit an investigator accurately whereas physical network card was relegated the IP address being referred towards amidst of the predetermined time allotment.

5) Dynamic Host Configuration Protocol (DHCP) Server

As it needs a mechanism to guide MAC locations to IP addresses greatly and it likewise requires a mechanism to guide IP locations to the intelligible (human-readable) names that it allocates to the networks. To perform this, ventures normally utilize the Domain Name Network (DNS), in which singular host’s query focal DNS servers [7] when they have to outline IP location to a hostname, or the other way around. DNS is a recursive hierarchical distributed database; if a venture's local DNS server does not have the data to determine an asked for IP address and hostname, it can query another DNS server for that data.

Forensic Value: DNS servers can be designed to log query for IP address and hostname resolutions. These queries can be exceptionally uncovering. For instance, if a client on an inner desktop skims to a site, the client's desktop will make a DNS query to determine the host and space names of the web server preceding recovering the page. Therefore, the DNS server may contain logs that uncover association endeavors from inside to outer frameworks, including sites, SSH servers, outside email servers, and the sky is the limit from there. DNS servers can log inquiries, as well as the comparing times. Along these lines, forensic investigator can influence DNS logs to manufacture a course of events of a suspect's exercises.

6) Dynamic Host Configuration Protocol (DHCP) Server

Authentication servers [8] are intended together for authentication services to clients all through the association. So the client records can be overseen in one spot, instead of hundreds or a large number of individual PCs. This permits the undertakings to streamline the account in provisioning and reviewing the assignments. Forensic Value Authentication servers usually log productive and/or fizzled login endeavors and other related occasions. Investigators can break down authentication logs to distinguish brute force password guessing assaults, account logins at suspicious hours or abnormal areas, or sudden advantaged logins, which may demonstrate flawed exercises. Not at all like investigation of authentication logs on a solitary hard drive, the center authentication server can give confirmation of occasion data approximately all gadgets inside a whole authentication space, including network gadgets, desktops, servers and then some.

F. ***Advantages of MPMPLC Framework:***

- Each and every record of an individual network log details can be stored into the cloud in scheduled manner and no need to remember the backup date and time.
- By implementing MPMPLC Framework no one can retrieve any information without proper authentication.
- The logs/caches in the cloud is considered as the lawfully evidence because it can’t be altered, deleted and included any fake entries.
- The information as collected from A to Z logs/caches by deploying the MPMPLC.
- A to Z entries in the cloud can be classified the whole details effectively in the case of crime in the forensic network and manage the time lawfully.

CONCLUSION

The investigations in the Network forensic pose a myriad of challenges from the distributed evidence to the internal politics in questioning the evidence admissibility. And to encounter these challenges the investigators must cautiously evaluate the each investigation in advancing the realistic problems that precedes the account in both the investigative goals and also in the available resources. The proposed framework will augment the methodology of digital forensic network. Moreover, it supports to accumulate the lawful information from the cloud and also it creates provision to continue the investigation. Finally, it assists to complete the investigation within the stipulated time and also deviates without the other investigations of the forensic network. Through this MPMPLC framework, the future will be carried out in the reality and this method will be used for the investigation of the future IP trace back problems in the network.

REFERENCES

[1] Grover S. Kearns, "Countering Mobile Device Threats: A Mobile Device Security Model", Journal of Forensic and Investigative Accounting, Volume 8: Issue 1, January - June 2016,pp.36-48.

[2] David Gugelmann, Fabian Gasser, Bernhard Ager and Vincent Lenders, "Hviz: HTTP(S) Traffic Aggregation and Visualization for Network Forensics", Digital Investigation, Proceedings of the Second Annual DFRWS, Europe, Volume 12, March 2015, pp.s1-s11.

[3] Quick Darren, "Digital Forensic Data and Intelligence: Using Data Reduction to Enable Intelligence Analysis", Journal of the Australian Institute of Professional Intelligence Officers, Volume 23, Issue 2, 2015.

[4] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Muhammad Shiraz and Iftikhar Ahmad, "Network Forensics: Review, taxonomy, and Open Challenges", Journal of Network and Computer Applications, 2015, pp. 1-22.

[5] H. Shah, E. Rosen, F. Le Faucheur and G. Heron, "IP-Only LAN Services (IPLS)", Internet Engineering Task Force (IETF), 436 January 2015.

[6] D. Binet, M. Boucadair, A. Vizdal, C. Byrne, G. Chen, "Internet Protocol Version 6 (IPv6) Profile for Mobile Devices", V6OPS Working Group, 2013.

[7] Marwan Radwan and Reiko Heckel, "Detecting and Refactoring Operational Smells with the Domain Name Network", EPTCS 181, 2015, pp. 113–128.