International Journal of Academic Research [**ISSN**: 2075-4124].
Vol.4 Issue. 2 & pp. 124-139

ECMA: A Novel Technique for Implementing Digital Evidence against Internal Attack Vectors

G.Ononiwu[1], K.C Okafor[2] , Anulika, Okoye Joy[3]

[1&2]Dept.of of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria.
[3]Dept. of Electrical and Electronic Engineering, Chukwuemeka Odumegwu Ojukwu University Uli, Anambra, Nigeria.
[1]gordon.ononiwu@yahoo.com, [2]kennedy.okafor@futo.edu.ng, [3]joynuli.ok98@gmail.com

ABSTRACT

In today's private cloud networks, data theft and various attack payloads remains a challenge yet to be fully addressed. A novel strategy to attack vectors, payloads and mitigation procedure for organizational models is presented. The work approached computer forensics from the perspective of cyber digital evidence generation using a developed application interface referred to as Evidence Capturing and Monitoring Application (ECMA). This facilitates forensic data gathering and evidence dataset in form of Online Service Computing (OSC) used for digital evidence log. User activities such as Universal Resource Locator (URL), IP address, date and time are captured in real time via textiles at an average cycle of 5 to 15secs in a Virtual Local Area Network (VLAN) Setup. The ECMA API clone obtains evidence dataset and populates the ECMA VLAN server directory. Finally, the analysis of forensic VLAN for ECMA users was carried out which showed various performance observations for enterprise adoption. This security scheme seeks to protect internal vulnerabilities at all cost.

Keywords: *Attack Vectors, Digital Evidence, Forensic VLAN, Cyber Act, Attack Payloads*

1. INTRODUCTION

1.1. Background Study

Attack Vectors (AVs) are the specific tools and methods that explore specific vulnerabilities in a company's security model while gaining access (Verizon Data Breach, 2015). It can be further divided into Initial Vectors (IVs) which is the method that grant an attacker an entry point into the network, and Linkage Vectors (LVs) which is a combined attack with the Initial Vector to achieve full compromise of a target network (Verizon Data Breach, 2015). In a simpler term, an attack vector is a path or means by which an insider, hacker/cracker can gain access to a computer or network server in order to deliver a malicious payload. These attack vectors enable hackers to exploit system vulnerabilities. These include: viruses, e-mail attachments, web pages, pop-up windows, instant messages, chat rooms, and deception/social engineering. More often, they have been used severally to hijack mission critical organizations.

Again, in most organization's cyberspace, internal threats and attacks could be launched by disgruntled employees. These entities use organization data and other critical information to perpetrate havocs. Criminal activities executed using "Bring Your Own Device (BYOD)", is now becoming commonplace in today's digital workforce organizations. With theses devices, the most common malicious payloads are viruses (which can function as their own attack vectors), Trojan horses, worms, and spyware. The top initial vectors are (Verizon Data Breach, 2015): weak passwords (35%), NetBIOS spoofing (21%), system misconfigurations (15%), social engineering (13%), missing patches (9%) while the top linkage vectors includes: weak passwords (34%), system misconfigurations (29%), missing patches (12%), unsupported legacies (10%) and web management console (6%).

Similarly, a report from (Deb, 2011), on Cyber Security Watch Survey, it was revealed that (58%) of attacks are caused by outsiders while 21% of the attacks are caused by insiders. About 33%

respondents had the perspective that insider attacks are more costly. Currently, it interesting to note that insider attacks are becoming more sophisticated, with a growing number of insiders (22%) using root kits or hacker tools, etc compared to 9% in 2010, as these tools are increasingly automated and readily available, (Deb, 2011).

As a result of the new digital economy, it could be clearly observed that most organizations in Nigeria now have complex information systems that are growing on exponential basis. As organizational networks become more complex, more vulnerability is to be expected. This implies that security will remain a continuos engagement and any minute gap in security surfaces can result in system been compromised. Just in November, 2015, Nigeria was reported to have lost over 8billion USD from malicious cyber criminals. But, it must be noted that security costs are extremely difficult to calculate, especially with regard to return on investment. Although only 30% or less are attacks originating from inside the network, these attacks cannot be ignored. Disgruntled and negligent employees are causing 70% of the damage, making companies squirm as insiders ravage their networks, (Kristophe, 2003).

Interestingly, full protection from organizations systems administrator can never be guaranteed (B.Ruppert & R.Wanner, 2009). The most reliable remedy is to reduce the possibility of an incident occurring and lessen the damage when it does occur (Kristophe, 2003). Creating a secure subnet could mitigate the possibility of an attack but securing and separating the different groups of critical systems into secured subnets could provide a damage control mechanism when an incident occurs. Once the user's logs into the network, the Dynamic Host Configuration Protocol (DHCP) allocates VLAN tagged IP addresses to the users and activates the background read algorithm which captures users computing activities on the network.

By properly terminating an employee, attempts and successes of deliberate attack by disgruntled employee can be reduced and managed within the system. Also, with a well implemented VLAN framework, network forensics which captures, records, and analyses network events (in order to discover the source of security attacks or other problem incidents) could be achieved. These components when combined could provide a powerful road map for maximum security against attack payloads. This paper used the proposed system to carry out a pilot study at the Electronic Development Institute Awka (ELDI) situated in the south eastern Nigeria, for user activities. This was used as forensic digital evidence. The solution satisfactorily achieved the intended objectives of the Nigerian Cyber Act legislation of 2015.

1.2. Research Motivations

Generally, large and small companies will always seek to deal with expansion and reduction in their employee workforce as the business and economy changes. Modifications in job roles could affect the delegation or consolidation of roles in the organization. As roles change, permissions and access to specific assets ought to be changed in order to fit the current role of that employee. Lack of processes to ensure that employee access is limited to systems (or data that is required to do his or her job is controlled), is a major issue facing most companies (B.Ruppert & R.Wanner, 2009). In IT security, protecting against attacks from an insider is most often neglected, but an insider employee of a company has greater access to sensitive information and also have better understanding of internal processes. This insider, still have knowledge of high-value targets as well as the sources of potential weaknesses in security architecture. Consequently, an insider attack has the potential to cause significant, even catastrophic damage to the targeted IT-infrastructure, (Dimitrakos, 2007). While this problem is recognized in the security and law-enforcement communities, many companies still tend to rely on audit logs after the insider attack has occurred instead of focusing on developing tools and techniques for analysing and solving the actual problem. There are no forensic intrusion detection

systems that can isolate insider attacks via audit log detection. A forensic logging mechanism as well as appropriate VLAN segmentation user workgroup in an enterprise is vital in critical production systems. In this paper, a novel tracking tool for digital evidence generation against a malicious insider in an organization network will be developed. The tool runs on an organization forensic VLANs network always. The network has an Internal Network Firewalls (INF) deployed rapidly with minimum disruption while keeping up the multi-gigabit speeds of internal networks (Dignan, 2003, & K.C. Okafor, et al. 2015). A discussion on attack vectors, digital Evidence Efforts and research gaps is presented below.

1.3. Attack Vectors

Owing to prevalence of code injection attacks, (Michalis, 2010), presented a detection method for the identification of Return Oriented Programming (ROP) payloads in arbitrary data such as network traffic or process memory buffers. Their technique speculatively drives the execution of code that already exists in the address space of a targeted process according to the scanned input data, and identifies the execution of valid ROP code at runtime. The experimental evaluation demonstrates that the prototype implementation can detect a broad range of ROP exploits against Windows applications without false positives, while it can be easily integrated into existing defences based on shell-code detection.

Similarly, (Collin & Matthias, 2015), proposed a novel defensive strategy called Code Freeze which a system that removes unused code from an application process to prevent attacks from using code as well as the APIs that would otherwise be present in the process memory but normally are not used by the actual application. The system is only active during process creation time, and, therefore, incurs no runtime overhead and thus no performance degradation. (Christian, et al.2010) introduced the usage, management and operation of Tele-Lab as well as its architecture which offers a system for hands-on IT security training within a remote virtual lab environment over the web, accessible by everyone. Their major security objective is to achieve authentication, authorisation and availability. Attack vectors such as web app, remote desktop, admin web interface and control services, and virtual machine pool were discussed. It is important to review the efforts so far made in digital evidence generation.

1.4. Digital Evidence Efforts

In the work carried out by (Yudi, 2014), the author developed a model of Digital Evidence Cabinets as a new approach in implementing the digital evidence handling and chain of custody. The model was constructed through three approaches: Digital Evidence Management Frameworks, Digital Evidence Bags with Tag Cabinets as well as access control and secure communication. It was opined that the proposed framework is expected to be a solution for the availability of an environment handling of digital evidence and to improve the integrity and credibility of digital evidence. Similarly, (Ramesh, et al. 2014) proposed a cyber forensic tool for transmitting huge amount of illegal data through the internet. The proposed tool was developed with the help of image mining system and neural network concepts. Also, (Aadil Al-Mahrouqi et al 2015) presents the building blocks for a model for automated network readiness and awareness. The idea of their model is to utilize the current network security outputs to construct forensically comprehensive evidence. The proposed model covers the three vital phases of the cybercrime management chain, which are: 1) Forensics Readiness, 2) Active Forensics, and 3) Forensics Awareness.

Considering a more advanced system, (Saif et al. 2011) focused on homogenous and heterogeneous tracking with emphasis on pedestrian and vehicular tracking for forensic and surveillance purpose. The

contribution of their work is on building an algorithmic solution for multi-modal tracking, which is a mixed environment combining both pedestrian and vehicular settings. (Catherine & Hiroyuki) proposed Gringotts as a system in which data is signed on the device that generates it, transmitted from multiple sources to a server using a novel signature scheme, and stored with its signature on a database running Evidence Record Syntax, a protocol for long-term archival systems that maintains the data integrity of the signature, even over the course of changing cryptographic practices. The processing throughput and storage over head were obtained from the system.

Also, (Achumba, et al, 2015), in their work, proposed online spyware solution. This represents modular, extensible cloud architecture with intrinsic support for efficient security monitoring. Their implementation architecture facilitates dynamic interface with OpenFlow hardware to create a flexible security decisions. Their work proposed a security foundation for next-generation enterprise-grade cloud computing.

Clearly, efforts have been made by various researchers to deal with the issue of forensic digital evidence using software and network based approaches. However, approach followed in this work is to study an existing forensic and evidence generation tools while collecting data from the network and then making evaluations on its metrics performance.

1.5. Research Gaps

The following are the identified research gaps from literature survey:

1. Existing works lacks a time session control for continuously logging in a user so as to monitor performed actions.
2. Communication with a remote log server for evidence documentation has not been explored.
3. Existing works have failed to use internally generated snapshots in .JPG for evidence storage.
4. A combined integration of JAVA and MySQL object oriented programming in the context of digital evidence generation in VLAN scenario is yet to be explored.

The ECMA was used to fast track the process of generating digital evidence in a very short time. On the server, ECMA is Vmware enabled thereby allowing for enterprise consolidation. To further illustrate the VLAN network scenario for ECMA service computing, Riverbed Modeller version 17.5 was used. During the digital evidence data generation, the network scenario was used to study network metrics necessary to classify users on the network architecture.

The major contributions of the paper is to show an efficient and secure online event tracking streamed from BYOD multiple sources to a single server as well as a distributed datacenter network, which uses the stored snapshots to verify the existence and integrity of data as digital evidence.

The remaining part of this paper is organized as follows. Section 2 provides context for the project and describes related research. Section 3 discussed the research methodology as well as the process model context for application deployment. Section 4 presents the results and discussions. Section 5 summarizes, concludes and outlines future trends for this research.

2. METHODOLOGY

2.1. Design Process Model

Using the incremental and rapid prototyping software process model, this work implemented object oriented analysis and design (OOAD) method with Java for the client interface and MySQL server for the backend interface (ECMA). Four major class hierarchies were used in the implementation viz: class Full screen Sample, class MyDB_connection, class screen capture Timer, and class Spyware FA. This

could be deployed in the network architecture of Fig.1 for real time event capturing activities. The figure shows a typical network with numerous attack vector possibilities having internal firewall remediation (Fortinet, 2015). It shows a conceptual illustration of the compute network for forensic application deployment. The OOAD paradigm was used to develop the Evidence Capturing and Monitoring Application (ECMA). This was meant to scale efficiently in the test organization (Electronic development Institute Awka, ELDI).

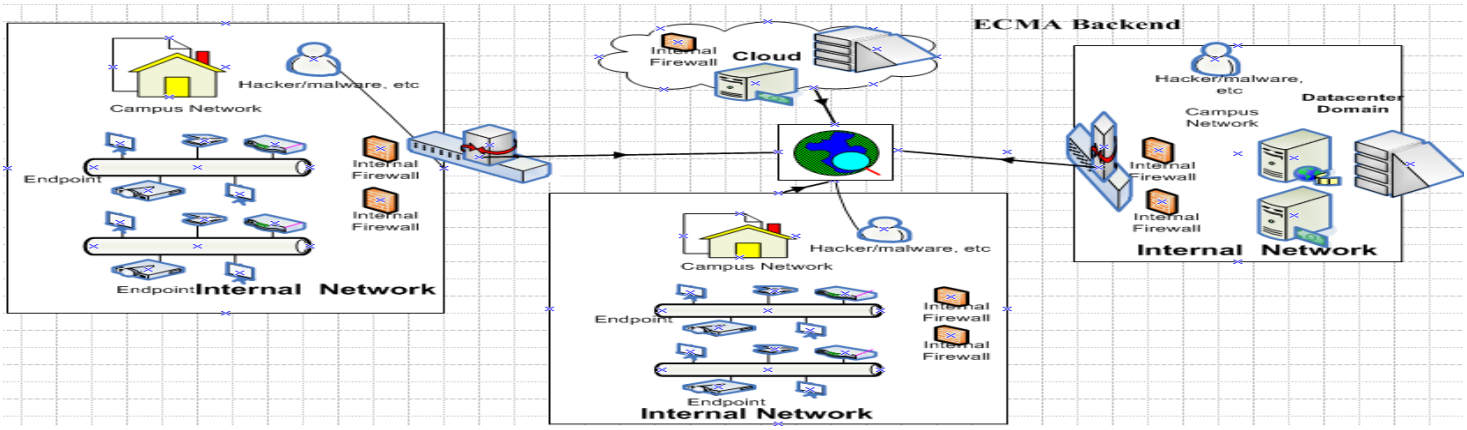

Figure.1: A conceptual network with numerous attack vector possibilities and having internal firewall

2.2. System Architecture

Considering Fig.1, there are two major subsystems in system architecture. The first subsystem is the ECMA client server based solution whose block diagram is shown in Fig. 2. In this model, there are six modules that make up the system viz: admin password generator, client log, spyware timer routine, domain name to IP converter, pop up digital certificate and ECMA (Slog) server.

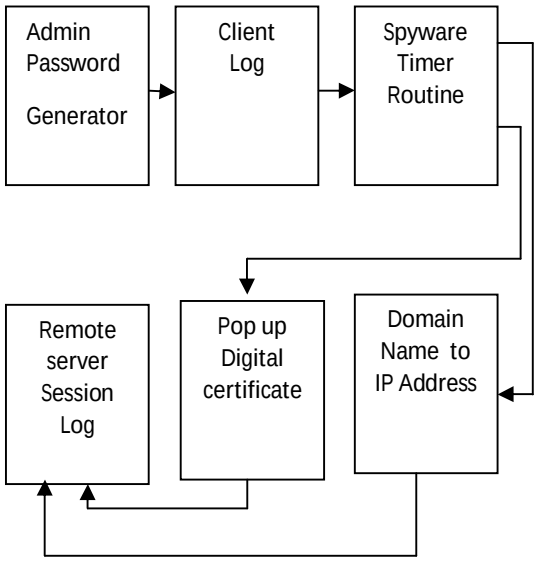

Figure 2: ECMA System Block diagram

From Fig.2, all the users in the networked environment run on a VLAN map. Upon user authentication from the server, the spyware timer is enabled based on the preset time by the system admin. After 5-15 seconds, a digital certificate pops up and takes the snapshot of the user online activities. This snapshot is sent to a remote server session log. The constituent of the Slog in the remote server forms the repository digital evidence for the ECMA. The administrator can call up the log from any IP network. In the second

subsystem, the VLAN network map for various users is defined. The VLAN is responsible for logical segmentation of users based on their workgroup listings. After acquiring traffic flows from the VLANS, simple comparisons were made between VLAN ECMA online service forensic service and the case without VLAN setup considering the diagram in Fig.1. The simplified procedure for session initialization is shown in Fig. 3.

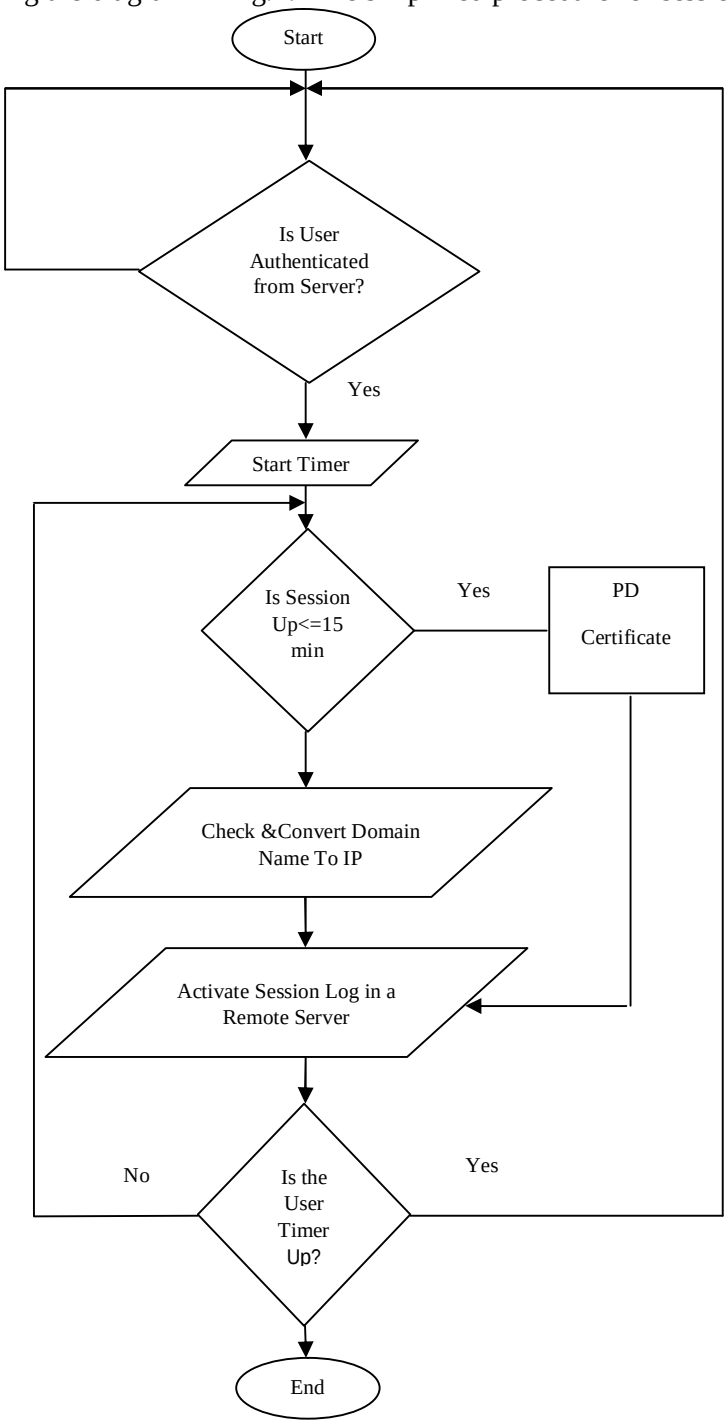

Figure 3: ECMA System flowchart

To understand the implementation of the ECMA, the flowchart in Fig. 3 clearly illustrates the procedure. Once a user is authenticated from the server (using a certificate authority), a session timer is triggered. Also, the session in the remote server is triggered so as to be keeping the logs of the user events.

This implementation was done with Java Netbeans and MySQL software tools while carrying out the real network simulation with Riverbed Modeller environment.

In the initial approach, the NetBeans Platform was used a reusable framework for ECMA clone. This was used for simplifying the development of Java ECMA application. In developing the application, the NetBeans IDE bundle for Java SE contains the tools ECMA plug-in, as such there was no need for additional SDK in this case. The platform offered reusable services allowing for a complete focus on the logic specific to their application as shown in Fig. 4.

Some of the management features of the platform explored in the design include: the user interface (e.g. menus and toolbars), user settings storage, window, wizard framework, NetBeans Visual Library and Integrated Development Tools.

3. RESULTS AND DISCUSSIONS

3.1. ECMA Interfaces

Using the programming tools above, Fig.3 was simplified via object oriented coding to yield Fig.4. This shows the client front end interface for authentication. Upon authenticating a user, the timer routine and Pop up Digital Certificate (PDC) are enabled. Fig.5 shows some of gathered log files from users which serve as the digital evidence in this research. This was tested at ELDI on daily basis to obtain a representative digital evidence datasets.

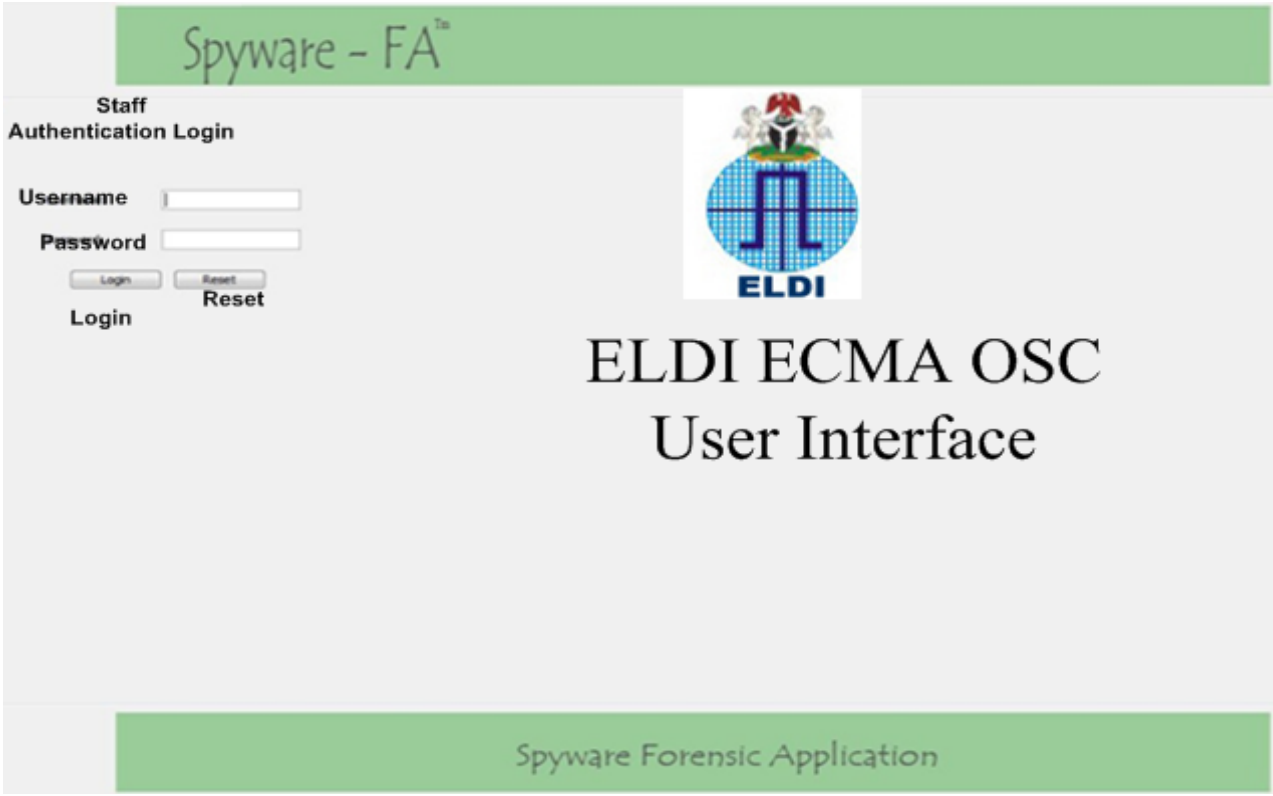

Figure 5: ECMA Client interface

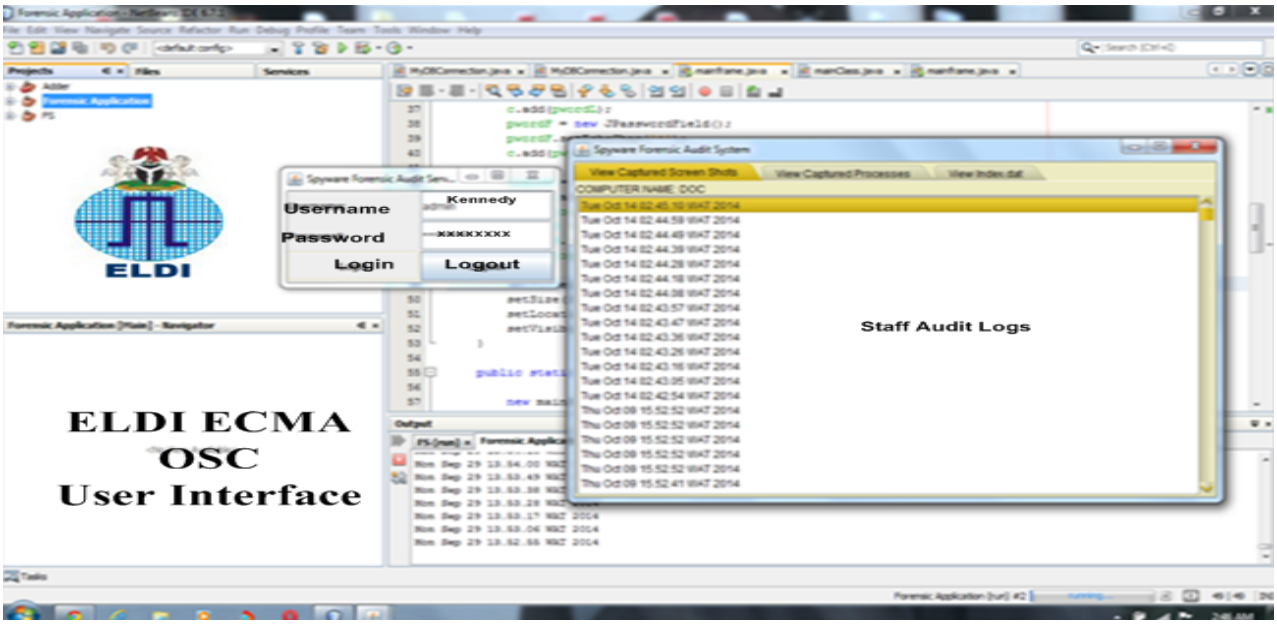

Figure 6: ECMA Real time captured digital evidence logs

3.2. Forensic VLAN Service Computing

To achieve a high performance network backbone for the ECMA application, a VLAN setup star topology was developed for the ECMA background processes. Essentially, various user scenarios were created for digital evidence captures. Using Riverbed Modeller version 17.5, the simulation duration was set to 0.5hour in the discrete event simulation window. In order to create and configure the real world network scenario, network components were aggregated via the object palette dialog box. The internet toolbox was selected also from the pull-down on the object palette. Afterwards, the Ethernet switches, routers, clients, connection links as specified in Table 1 were properly configured and saved.

Table 1: Experimental Design Parameters (Source: DCCN, 2015)

SN	Parameters	Specifications
1	No of Scenarios	2 (VLAN 10 and 20)
2	No of Switches	5 (16Port Ethernet)
3	No of Routers	3 (CS_47000)
4	VLAN Types	Port Based Scheme
5	VTP version	2
6	No of ECMANodes	7 (Clients= 4 ; Servers = 3) 5 (Clients = 3; Servers = 2)
7	Profile Utility	15rows (Engineering, Research, E-commerce, Sales, Multimedia users, Vlan Profile, Vlan DB, FTP Profile, Vlan Profile)
8	Applications	Server Services: Web browsing, FTP and Database
9	Kernel Type	32-bit Address Space
10	Event Summary	36,088
11	Avg.Speed	462,660Events/Secs
12	Client Address	Auto Assigned (DHCP)

13	Server Model	Sun Ultra 10, 1333MHz,1CPU, 1Core
14	Trunk Ports	6
15	Broadcast Domain	12

Next, the traffic demands were configured with respect to the servers and the client nodes using ECMA service. On the VLAN switches, the link ports were then configured to identify two types of captures discussed below.

i. Forensic Catch-it-as-you-can systems (FCiaycS), in which all packets passing through the VLAN traffic points are captured and written to server storage with analysis being done subsequently in batch mode as audit logs. It was observed that this approach requires large amounts of storage, usually involving a Redundant Array of Inexpensive disk (RAID) system.
ii. Forensic Stop, look and listen systems (FSllS), in which each packet is analysed in a rudimentary way in memory and only certain information saved for future analysis in the ECMA server logs. Interestingly, this approach requires less storage but may require a faster processor to keep up with incoming traffic.

In either case, both approaches require efficient storage machines which will need occasional updating of old forensic data to make room for new capture records. Hence, the ECMA application was used for data capture while the running on the VLAN setup. The major concern with the FCiaycS approach is privacy since all packet information (including user data) is captured via the Internet service providers (ISPs) who are expressly forbidden by Service Level Agreement (SLA) from eavesdropping or disclosing intercepted contents except the organizational consent or under a court order. The performance analysis of the former approach was considered using basic network metrics.

3.3. Performance Evaluation

From the ECMA VLAN setup, the results were viewed and the datasets for the respective forensic metrics selected for analysis. From the design setup environment for forensic OSC VLAN10, five client devices/users were loaded. Similarly, forensic OSC VLAN20 setup was loaded with 10 users. It would be recalled that the problem with Fig. 1 is that of slow and rather delays collision and broadcast connectivity. This will create a terrible experience for online users particularly in the event of making online payment or carrying transactions that require little delay time. Hence, this work will only focus on the VLAN 10 and VLAN 20 scenarios for the system evaluations.

3.3.1. Forensic Online Service Computing in VLAN 10 (Packet Drop Response)

Fig. 7 shows the plot of VLAN10 packet drop responses for type *a*, *b*, *c* and *d* users in a workgroup domain. It was observed that users in VLAN10a, and VLAN10b experienced more collision and broadcast traffic leading to higher packet drops compared with users in VLAN10c and VLAN 10d. This is because, the lower the number of users on the network under the influence of ECMA service, the lesser the packet dropped experienced in the network. Again, misconfiguration on any of the VLANs can result in a packet loss and slowness. With increased packet loss when higher traffic rates occur on the link, the ECMAservers will be working at lower capacity. Hence, it is recommended that the network users in forensic OSC (ECMA) must balance with the ECMA server computing capability to avoid drops of any evidence dataset.

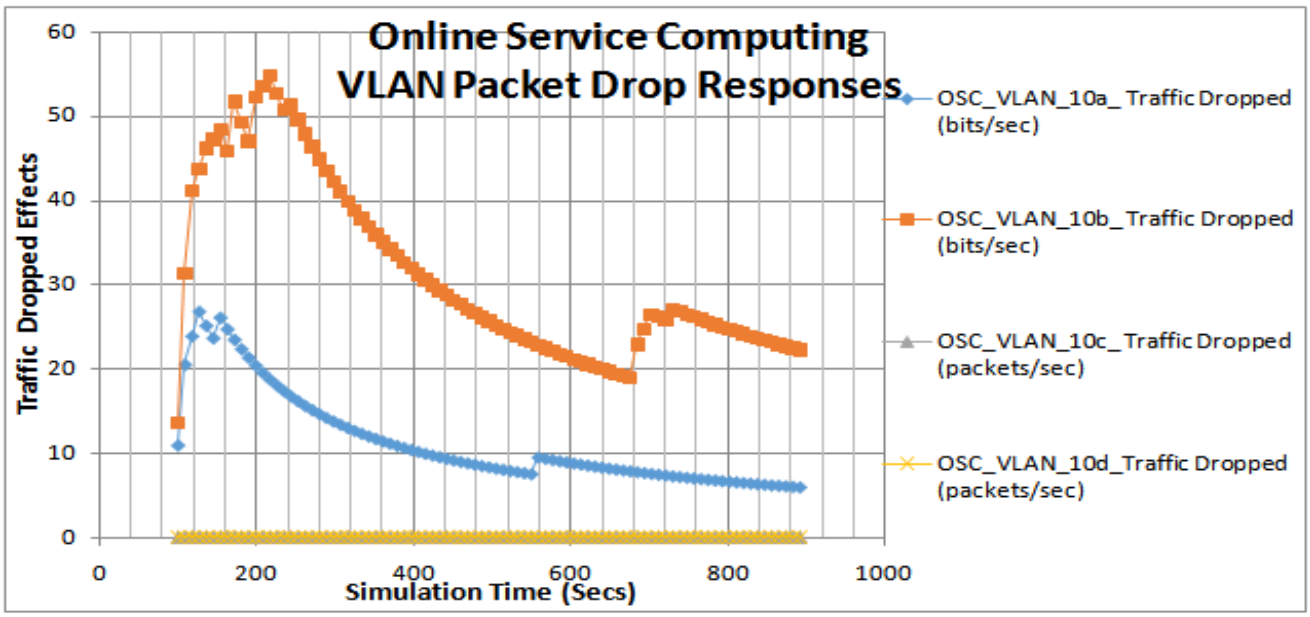

Figure 7: Forensic Packet DropinVLAN10

3.3.2. Forensic Online Service Computing in VLAN 10 (Traffic Sent/Received)

As shown in Fig.8, there is a relationship between packet received and workload classification in the respective VLANS for tracking workgroup users. It was observed that packet reception rate in VLAN 10c and 10d is marginally lower (less than 50%) compared VLAN 10a and 10b (over 50%). This could result from users opting in or out of the network. Poor inter-Vlan communication occurring at VLAN 10c and 10d could affect traffic received. When there is weak data reception, this will affect evidence data generation as well as the logs.

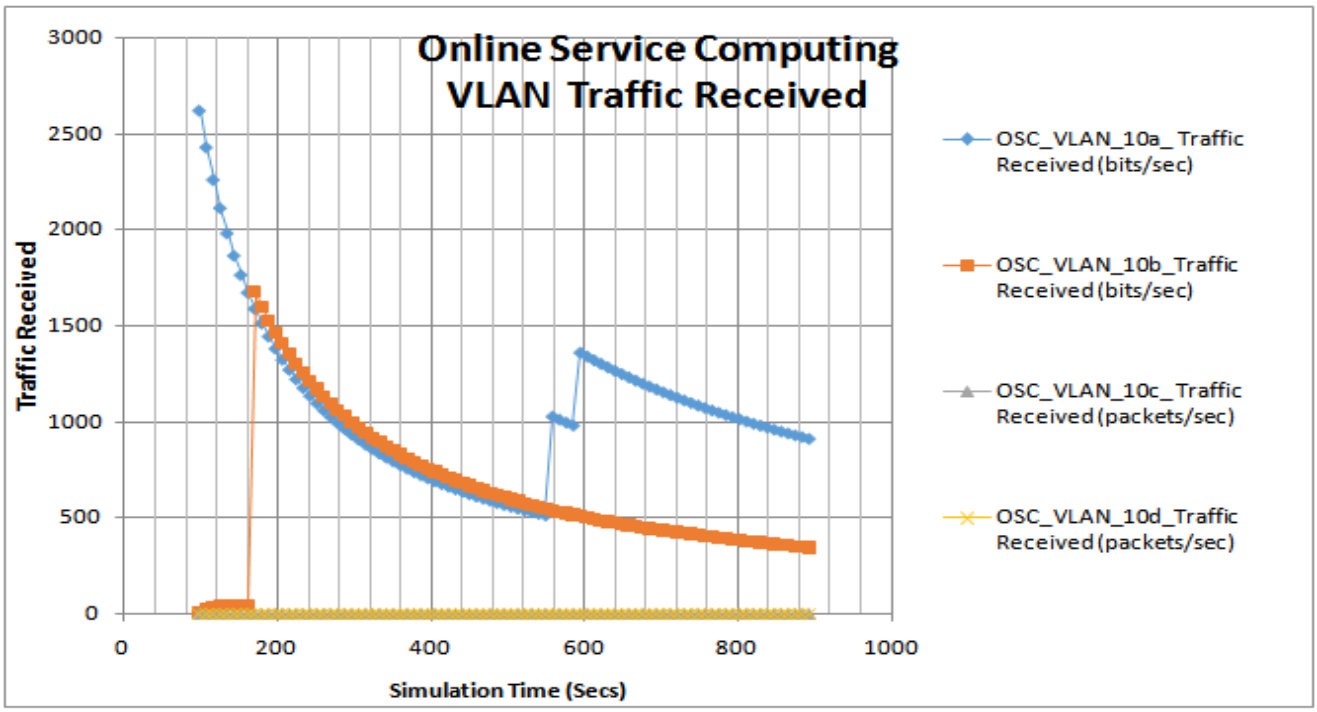

Figure 8: Forensic Packet received in VLAN10

3.3.3. Forensic Online Service Computing in VLAN 20 (Packet Drop Response)

As shown in Fig.9, a similarity trend was observed just like in Fig.7 for tracking workgroup users. Again, the plots show a progressive packet drop responses in VLAN 20. Accordingly, users in VLAN10a, and VLAN10b experienced more collision and broadcast traffic leading to higher packet drops compared with users in VLAN10c and VLAN 10d. Again, the lower the number of users on the network, the lesser the packet dropped experienced in the network. With increased packet loss when higher traffic rates occur on the link, the servers will be working at lower capacity. Hence, the recommendation given in Fig.7 remains valid for VLAN20 in the context of packet drops.

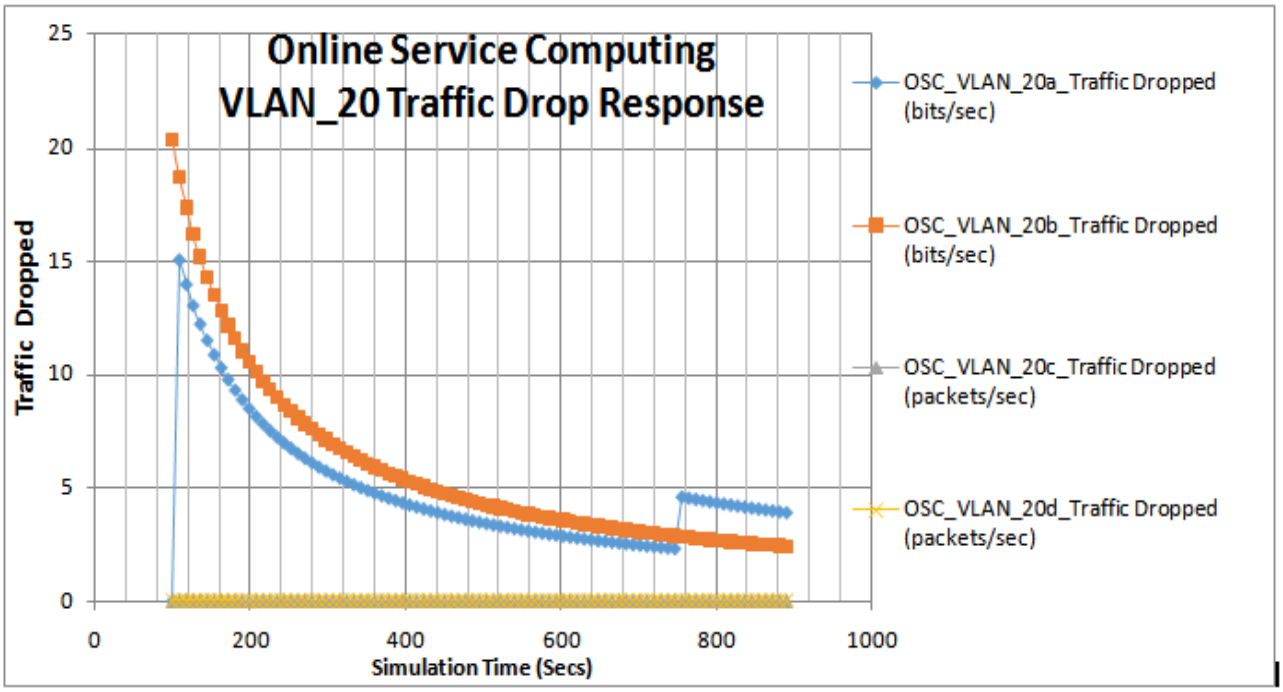

Figure 9: Forensic Packet Drop received in VLAN10

3.3.4 Forensic Online Service Computing in VLAN 20 (Throughput Behaviour)

In the forensic network setup, capturing, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents places demand on throughput. Throughput behaviour is the average rate of successful message delivery over a VLAN communication channel measured in packet/secs, bits per second (bit/s or bps), or bytes/secs.

It is the sum of the data rates that are delivered to ECMA nodes in the network. The mathematical models describing this metric have been discussed in a previous work.

Now, owing to the observed similarities in VLAN 10 and VLAN20, in evaluating the throughput behaviour, higher throughputs were observed for VLAN20a and 20b just as in VLAN 10a and 10b. From Fig 10, the average throughputs of VLAN20a and 20b are 0.68packets/sec and 0.59packest/secs respectively. Those of VLAN 10a and 10b are 0.07packets/sec and 0.05packest/secs respectively. These VLANs have reduced collision domains when communicating with the ECMA serves as well as with other possible nodes on the network. In order to satisfy the performance requirements, the forensic VLAN concept basically ensure that maximum throughput is derived for forensic data or workload sent to the server. In this case, the throughput now depends on the number of users and events in a given VLAN subnet. This observation now leads to a conclusion that OSC using VLAN can improve service delivery particularly for high density forensic network.

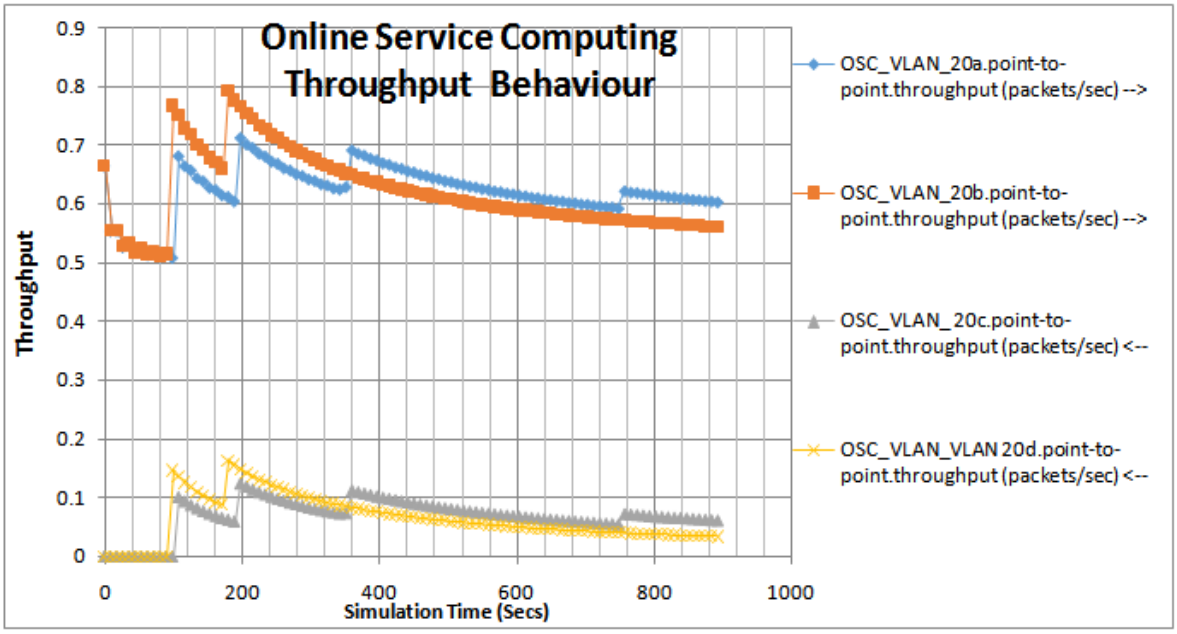

Figure 9: Forensic Throughput (Packets/Secs)plot in VLAN20

3.3.5. Forensic Online Service Computing in VLAN 20 (Queuing Delay Response)

Fig. 10 explains the effect of the forensic VLAN mapping on the queuing delays. Basically, because the queuing delays d_n incurred in all VLAN networks with N nodes are assumed to be statistically independent, the of the total queuing delay from the server was observed as Nt. Now, from Fig. 10, a plot of OSC VLAN20 queuing delay showed that VLAN 20c and VLAN 20d have the lowest queuing delay which measures the average time a packet takes to reach a VLAN sink from the instant it was generated. Long queuing delays as shown in VLAN 20a and 20b will result in packets reaching the EMCA server when the information is no longer useful. Hence, presenting packet drops at its peak.

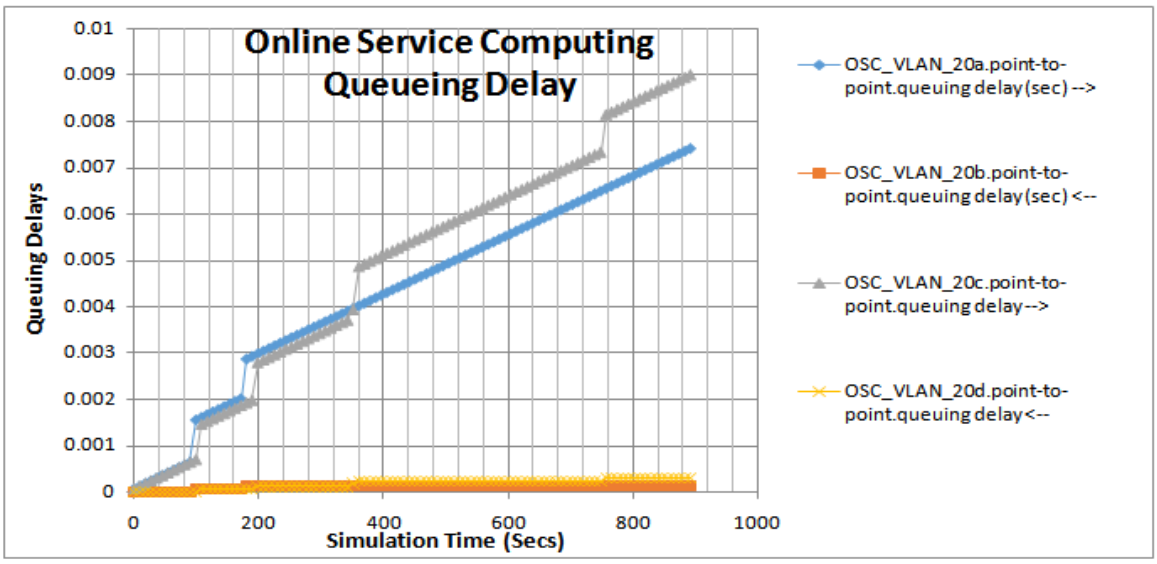

Figure 10: Forensic Queuing Delay (Secs) in VLAN 20

3.3.6. Forensic Online Service Computing in VLAN 20 (Utilization Response)

Fig. 11 shows a plot of OSC VLAN 20 utilization response under ECMA activity. In this regard, VLAN20a and 20b, those are crowded with users, hence having more utilization response in terms of the network resources compared with VLAN20c and 20d that have smaller number of users. The implication is that for forensic VLANs with more throughputs having more number of users, the utilization of resources will be higher. These tradeoffs are certainly inevitable in any network service computing event.

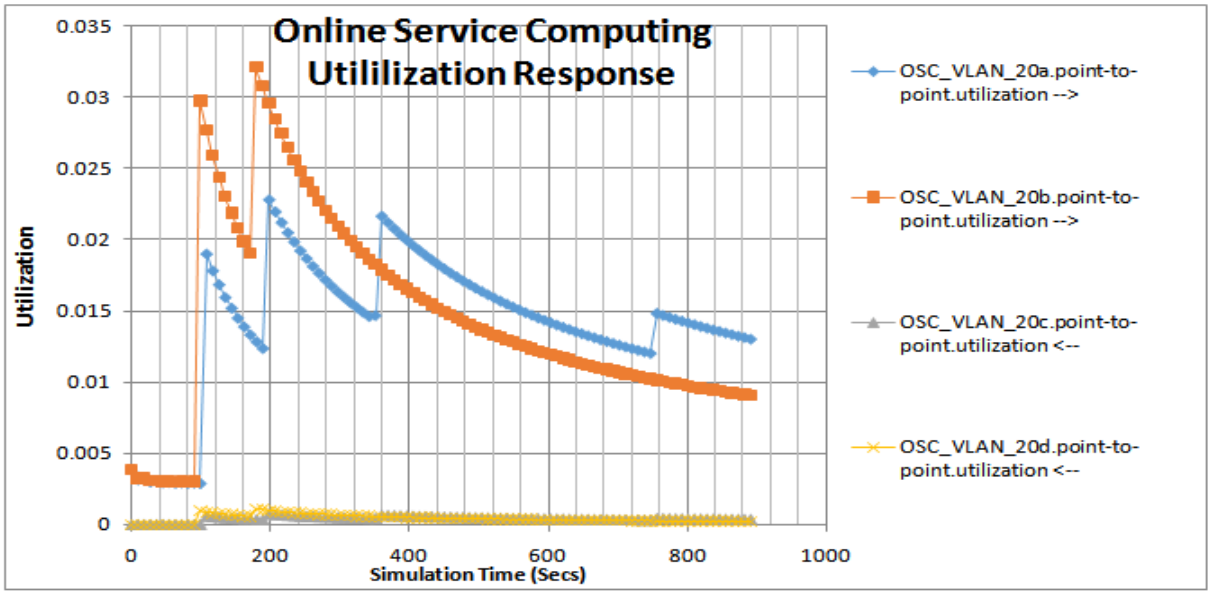

Figure 11: Forensic resource Utilization in VLAN20

3.3.7. Forensic Online Service Computing in VLAN 20 (Combined Metrics)

By plotting a common forensic VLAN metric, Fig. 12 was obtained. This represents the previously discussed plots collectively made from Fig. 7 to 11. Similar trend was noted for VLAN20b, 20c, 20d as well as VLAN 10a, 10b 10c and 10d.

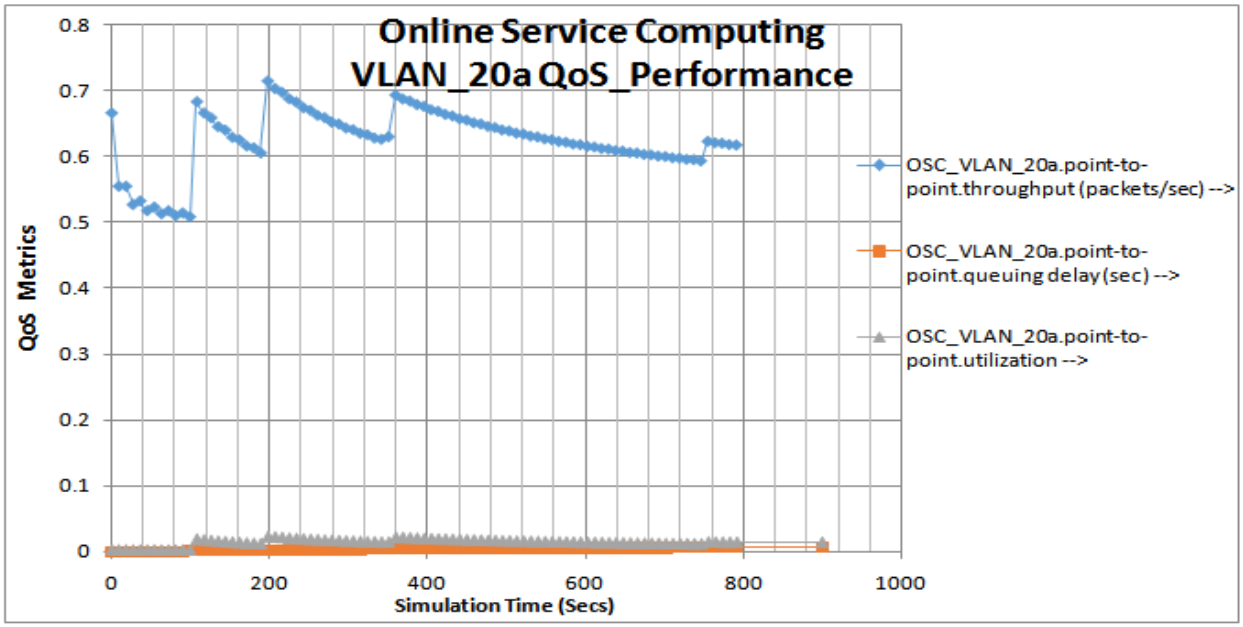

Figure 11: Forensic OSC VLAN20 (Combined QoS metrics)

4. Discussions and Analysis of Results

For ECMA service to work effectively in a production network such as ELDI, the forensic OSC VLAN must be well implemented. On a wired network, the use of truck link is recommended. From the trace file perspective, it was observed that OSC VLAN significantly regulated broadcasts and improved security mapping, i.e. it accurately handles user traffic segmentation. With increase in organization ECMA users, bandwidth optimization on the core switch must be maintained by forensic VLAN.

From the Riverbed process environment of Fig.1, the forensic VLAN switch supports FIFO Queues which holds packets or evidence data based on service the established ECMA services policy, hence the switch is capable of determining the number users whose log files or data are stored in the ECMA server. The transmission of the log files to the server represents an incoming service/packet arrival. The results of the forensic VLAN subsystem for both users and ECMA application server show that forensic VLANs have significant impact on the traffic performance metrics. Considering the various VLAN users, their activities on the network design reveals important perspectives to resource utilization, throughput and queuing delays. This research has shown that the network architecture for supporting ECMA OSC systems is feasible in a production design, not through hypothesis as seen in (Seyed, et al. 2014)

With the ECMA service running on the forensic VLAN, combating internal attacks and cyber related crimes can easily be traced and realized with ease. With its JAVA virtual platform (JVM), 75% of system resources are conserved as no additional security tool is required. For this application, the platform independent feature of Java makes it portable, secure and easily deployable on Sun Ultra 10, 1333MHz, 1CPU, 1Coreplatform. Security legislation can leverage this solution for securing critical infrastructure as well as its information assets. This solution offers a form of protection where a separation is created between the assets and the threats. It took into account the actions of people attempting to cause destruction and perpetrate threats to organizations assets and saliently monitors users' activities without their prior knowledge.

5. CONCLUSION

This paper has presented a digital evidence tool known as ECMA from both software implementation and forensic VLAN perspectives. Both schemes have been designed and analysed. This was carried out to facilitate the current cybercrime legislation in Nigeria. The system carries out hidden monitoring on the end users and then generates the digital evidence as log files on the server. The design block and system description has been presented. For the ECMA, the implementation technologies make for the application portability, hence offering zero drain on system resources. The digital evidence discussed is based on text file with date, time, JPEG, audio, pictures. This is highly secure and cost effective for production deployment purposes. Graphical results on illustrate that the forensic VLAN bounds can be used effectively to determine the number of users needed to achieve desirable level of accuracy and performance on the network.The results obtained from this paper shows that exact digital evidence generation via ECMA is possible under forensic VLANs. Using the proposed forensic scheme, this research seeks to adequately reposition Nigeria for the new era of cybercrime legislation. Future work will focus on developing methods to collect and process data form the ECMA server directory in real time for rapid response to security incidents.

6. REFERENCE

[1] **Verizon 2015 Data Breach Investigations Report - MS-ISAC M** (Attack vector reports**). Available online,** https://msisac.cisecurity.org/**whitepaper**/documents/**1.pdf** **(2015)**

[2] Deb Shinder, Protecting against Insider Attacks in Today's Network Environments **(2011).**

http://www.windowsecurity.com/articles-tutorials/misc_network_security/Protecting-Against-Insider-Attacks-Todays-Network-Environments.html, Retrieved on 11th, **2016.**

[3] Kristopher Harms, Global Information Assurance Certification Paper, GSEC ver 1.4b Option 1, SANS Institute **(2003)**.

[4] B.Ruppert, R.Wanner, Protecting Against Insider Attacks, 2009GIAC (GCIH) Gold Certification, SANS Institute **(2009)**.

[5] Dimitrakos, Theo, Martinelli, Fabio, Ryan, Peter, & Schneider, Steve, *Formal Aspects in Security and Trust*. Hamilton, Ontario: Springer, **(2007).**

[6] Dignan, Larry. "Who Can You Trust" Baseline, Ziff Davis Media Inc. March 1, pg 23. **(2003)**

[7] K.C. Okafor, G.N.Ezeh, I.E. Achumba, O.U.Oparaku, U.Diala, "DCCN: A Non-Recursively Built Data Center Architecture for Enterprise Energy Tracking Analytic Cloud Portal, (EEATCP), In AASCIT Computational and Applied Mathematics Journal, USA,1(3): Pp.107-121, **(2015).**

[8] K.C, Okafor, F.N Ugwoke, O.U.Oparaku, U.Diala, "Performance Evaluation of Discrete Event Process Algorithms for a Two-Tier High Performance Cloud Computing Network Architecture (DCCN)", in International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), India, Vol 4.No.2, , Pp.295-313, **(2015)**

[9] Michalis Polychronakis, and Angelos D. Keromytis, "ROP Payload Detection Using Speculative Code Execution" *Available Online* https://www3.cs.stonybrook.edu/~mikepo/ **(2010)**

[10] Collin Mulliner , Matthias Neugschwandtner, "Breaking Payloads with Runtime Code Stripping and Image Freezing, **(2015).**

[11] Christian Willems, WesamDawoud, Thomas Klingbeil, and ChristophMeinel , Protecting Tele-Lab – attack vectors and countermeasures for a remote virtual IT security lab", International Journal of Digital Society (IJDS), Volume 1, Issue 2.Pp.113-122, **(2010)**

[12] Yudi Prayudi, Ahmad Ashari, Tri K Priyambodo, Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications (0975 – 8887)* Vol.107 – No 9, Pp.30-36, **(2014).**

[13] P Ramesh Babu, HundeMergaDugassa, AbebeGemeda, The Proposal of an Efficient Cyber forensics tool using Neural Networks and Image Mining concepts", IJECS Volume 3 Issue 4, Pp.5275-5282, **(2014).**

[14] Aadil Al-Mahrouqi, SamehAbdalla, TaharKechadi Cyberspace Forensics Readiness and Security Awareness Model", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 6.Pp. 123-127, **(2015).**

[15] Saif Mohammed S. A. Al-Kuwari, Forensic Tracking and Surveillance: Algorithms for Homogeneous and Heterogeneous Settings, PhD, Technical Report. Department of Mathematics Royal Holloway, University of London England, **(2011)**.

[16] Catherine MS Redfield, and Hiroyuki Date, "Gringotts: Securing Data for Digital Evidence, IEEE Security and Privacy Workshops, IEEE computer society, DOI 10.1109/SPW.2014.11,**(2014)**.

[17] I.E. Achumba, K.C, Okafor, G.N.Ezeh, U.Diala, OpenFlow Virtual Appliance: An Efficient Security Interface for Cloud Forensic Spyware Robot" In International Journal of Digital Crime and Forensics (IJDCF), Vol. 7, No. 2, Pp.31-52., USA, **(2015)**.

[18] Fortinet White Paper: Protecting Your Network From The Inside–Out – Internal Network Firewall (INFW), www.fortinet.com, **(2015)**.

[19] Seyed M. H.O., Hormoz M, Hosein D, Evaluation the Effect of Objective Dimensions of Electronic Payment on the use of Electronic Payment Systems with the Mediating Role of Mental Dimensions in Electronic Payment in Mellat bank branches in Gorgan Province, International Journal of Academic Research, Pp: 107-115, **(2014).**