A Simulation of Logical Traffic Isolation Using Differentiated Services

I. Dlamini[1], M. Olivier[2] and M. Grobler[3]

[1, 2]Information and Computer Security Architectures Research Group (ICSA)
Department of Computer Science, University of Pretoria
[1, 3]Defence, Peace, Safety and Security (CSIR DPSS)
e-mail: idlamini@csir.co.za, molivier@cs.up.ac.za, mgrobler1@csir.co.za

Abstract

This paper extends work on a forensic model for traffic isolation based on Differentiated Services (DiffServ) and measures its performance by using a simulation. The simulated model has four basic components: traffic generators, the DiffServ network domain, a preservation station and a sink server. On the client side, the simulation has two traffic generators that generate either normal or suspicious traffic. The network domain isolates the suspicious traffic by using an ingress router to mark it as suspicious, whereas the preservation station preserves the isolated traffic/evidence to ensure forensic soundness. On the DiffServ server side, a sink server receives and processes all requests. The authors simulated the proposed DiffServ model by using the Network Simulator (NS2) tool. Preliminary results show that the simulated concept has improved support for evidence preservation, whilst also providing an easy means for cyber investigators to gather evidence.

Keywords

Differentiated Services, preservation station, Network Forensics, suspicious traffic

1. Introduction

Ever since the evolution of the digital computing field, Network Forensics has played an important role in analysing the cause of cyber crimes (Kim *et al.* 2004). This evolution has had a direct impact on producing the necessary evidence to prosecute cyber criminals successfully. Investigating and neutralising these cyber incidents usually cost an organisation a lot of money.

To identify malicious network traffic, Network Forensics sometimes requires the isolation of malicious network packets (Zantyko, 2007). This isolation depends on easy and accurate identification of the malicious packets as well as on forensically sound evidence collection. In 2006, (Strauss *et al.*) proposed a scheme that utilises Differentiated Services (DiffServ) to isolate malicious traffic logically from normal traffic. Since DiffServ is a standard technique, this could well reduce cost. More importantly, if a DiffServ infrastructure was already in place where an investigation needs to be performed, evidence collection could be facilitated with minimal changes to the network. The DiffServ approach allows Network Forensic investigators to attach both their marking station (ingress router) and isolation station to a cyber victim's network to investigate the case at hand. The advantage of this approach is minimal network downtime and minimal network reconfiguration.

This DiffServ-based scheme makes provision for a preservation station to store records of the isolated traffic and view with a later analysis (Strauss *et al.* 2006). However, in order to minimise network transmission problems, such as transmission delays and high network traffic, the preservation station only stores records related to malicious network traffic.

Traffic isolation is a new concept in Network Forensics and the DiffServ application a novel solution. To apply this solution successfully, it is necessary to determine the introduced delay and the extent to which the capturing of malicious packets can be relied on. An ideal system will introduce no delay (an attacker may infer that his/her actions are monitored if an unexpected delay is introduced) and it will capture all evidence without loss. While the proposal seems plausible, it has not been tested empirically yet.

This study investigates the viability of a traffic isolation station concept based on DiffServ simulation and analyses its performance. The simulation models four nodes (*traffic generators, ingress router*, *preservation station* and *sink server*) and is set up in an environment where both malicious and normal traffic is generated. This simulation determines how well the system copes with isolating generated malicious traffic under various assumptions. Section 2 introduces some of the theoretical background concepts regarding Network Forensics and the DiffServ architecture. Section 3 presents an overview of the architecture design, whilst Section 4 presents the results and the observations analysis based on the simulation. Section 5 indicates future work and Section 6 concludes this study.

2. Network Forensics

Network Forensics is a sub section of the Digital Forensics discipline (Zantyko, 2007; Vidas and Wilson, 2006; Solomon *et al.* 2005) that focuses specifically on network investigations of cyber crime. The distribution of network nodes to the number of locations can potentially increase the number of crime scenes. Multiple crime scenes complicate a Network Forensic investigation and increase the time needed to collect, preserve and analyse evidence (Casey, 2002).

The network forensic discipline fully integrates two related fields: networking and forensics. Network Forensics can be defined as *"... capturing network traffic in a proper manner using scientific and legal procedures that are acceptable in a court of law*." The discipline involves the gathering, preserving and analysis of network events in discovering the source of an attack or other network problem (Solomon *et al.* 2005; Corey *et al.* 2002; Köhn *et al.* 2006).

By applying the DiffServ model in the Network Forensics discipline, a significant improvement is made with regard to evidence storage. This can contribute greatly to the acceptance and integration of Network Forensics in the application of

Information Technology. This is possible since the DiffServ model consists of a preservation station that captures volatile network data that might have been lost otherwise.

3. Differentiated Services

Differentiated Services is one of the Internet Engineering Task Force schemes that are used to implement Quality of Service in the network (Blake *et al.* 1998). This scheme is used to map multiple network flows onto limited service levels, resulting in different groups/classes of traffic being treated according to their assigned priority. The current study assigns high priority to suspicious traffic (potential evidence).

The DiffServ-based network enables network investigators to plug their forensic tools into the network, within their legal jurisdiction. However, such investigation is only legitimate if a judge or magistrate issues a valid search warrant. When more than one network is involved, investigators should take care to attach the marking station, isolation station or network forensic tool to a specific section of the DiffServ domain (Jacobson *et al.* 1999; Heinanen *et al.* 1999).

The intention of the investigators is to capture and analyse suspicious traffic, internal and external to the targeted network. One of the main differences between the DiffServ network and other networks is that all classifying and policing functions are performed at the boundaries of DiffServ network, leaving the switch routers at the core of the DiffServ domain to focus on their specific routing tasks. This significantly reduces transmission delay, packet loss, etc.

The DiffServ network is generally more flexible and offers service differentiation for the aggregated flows to an Internet Protocol network. When simulating the DiffServ *logical traffic isolation model*, the marking characteristic helps to isolate traffic that is of forensic interest from the normal traffic. In the event that suspicious traffic is identified, it is easy to mark the packets in question and logically isolate them from the rest of the traffic. In addition, the model allows for assigning special routing to these suspicious packets. The marking/ isolation concept adds value to the forensics discipline and safely preserves suspicious traffic before it is sent to its destination for later recovery and analysis.

4. Architectural Design

The previous section described the logical traffic isolation scenario, using the DiffServ approach. This section presents the design of this approach with its components. Figure 1 provides a conceptual view of the DiffServ model for isolating suspicious traffic. The model consists of two traffic generators on the client side to initiate suspicious and normal traffic; and the DiffServ network with three routers (ingress, interior and egress) for experimental purposes.

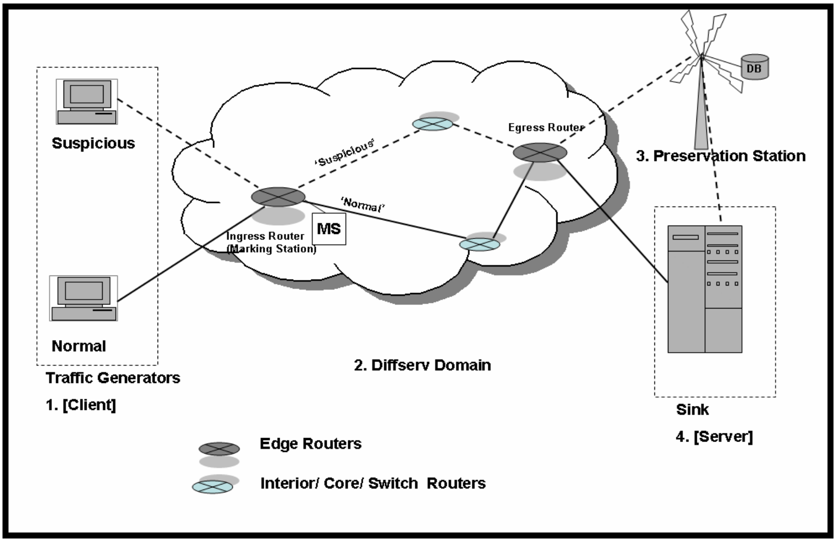


Figure 1: The Conceptual view of the Logical Traffic Isolation Using DiffServ

The preservation station ensures forensic soundness and system reliability, while the sink server receives and responds to all the requests generated by the traffic generator. This nodal setup is however for simulation purposes only. A real network might be composed of additional nodes. The two clients generate normal and suspicious traffic and forward these packets onto the DiffServ domain. The ingress edge router at the entrance boundary of the DiffServ domain is the first domain recipient and serves as a marking station. This router is responsible for *packet classification* and has *marking, shaping* and *dropping* capabilities. The ingress router marks the suspicious traffic by using the packet classifier and forwards them to the nearest core router. The core routers are found within the centre of the DiffServ domain, and they forward traffic towards the egress router.

The egress router is found at the exit boundary of the DiffServ domain. It unmarks the traffic and decides the destination of each network packet according to its behaviour: compromised traffic is forwarded to the preservation station and then to the sink server, while normal traffic is sent directly to the sink server. In a network-related cyber incident, the investigator searches the preservation station when conducting his/her investigation and captures all recorded suspicious network packets as evidence.

4.1. Traffic Generator

The traffic generator (number 1 in Figure 1) is situated on the client side and generates normal and suspicious network traffic. These types of network traffic are discussed next.

- *Normal traffic* is general flowing traffic of passing packets through the ingress router (which acts as marking station). These packets are then forwarded by the intermediate routers through the network domain, from the egress router to the sink server (number 4 in Figure 1).
- *Suspicious traffic* uses a specific dedicated route that leads to the preservation station (number 3 in Figure 1). It is transmitted in a process similar to the transmission of normal traffic, except that all suspicious packets are marked for easy identification and isolation. This ensures that all suspicious packets are recorded at the preservation station before being forwarded to the sink server.

4.2. DiffServ Domain

The most significant function that is performed in the DiffServ domain (number 2 in Figure 1) is the marking of suspicious traffic. This is done by the edge ingress router at the entrance boundary of DiffServ network. All the different routers that are found in this domain are discussed below.

4.2.1. Edge Routers: Ingress

The ingress router serves as the *marking station* of the DiffServ domain and the initiation of the traffic generators activates this router to mark suspicious traffic. The station routes all normal traffic to the sink server, while suspicious traffic is routed to the preservation station. The traffic generated from the suspicious generator is marked differently to ensure easy identification within the network. This technique presents the logical isolation of suspicious traffic from normal network traffic. The *traffic classifier* in Figure 2 combines the traffic into different aggregates. Each aggregate is monitored by the traffic conditioner, which in turn marks the packets according to their aggregate rate (Pang and Gao, 2003). In our system, the aggregation starts at the ingress node, where the suspicious network packets are isolated from the normal traffic packets.

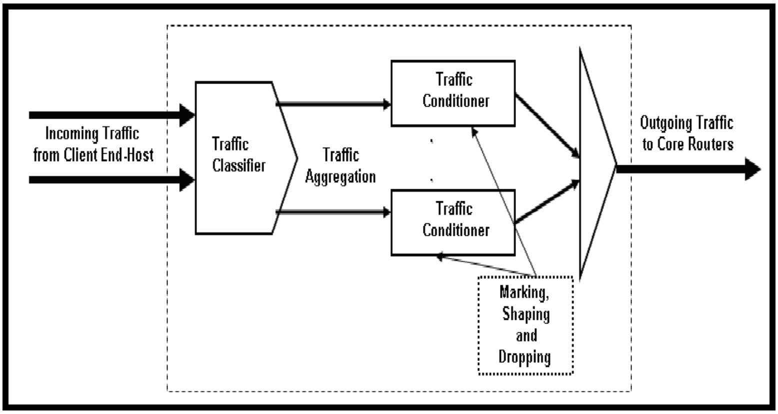

Incoming Traffic from Client End-Host
Traffic Classifier
Traffic Aggregation
Traffic Conditioner
Traffic Conditioner
Marking, Shaping and Dropping
Outgoing Traffic to Core Routers

Figure 2: Ingress router

4.2.2. Interior Routers

Interior routers are found within the DiffServ network. There is no limit to the number of interior routers within a system. The main function of these routers is to forward traffic within the network domain from one router to another, until it reaches the egress router.

4.2.3. Egress Router

The egress router is part of the edge routers in the DiffServ domain, found at the exit boundary of the network (Ngo-Quynh *et al.* 2001). All packets leave the DiffServ network through this router for either the preservation station (suspicious traffic) or the sink server (normal packets). Its main function is to unmark the packets, read each packet's destination and calculate the shortest route towards it.

4.3. Preservation Station

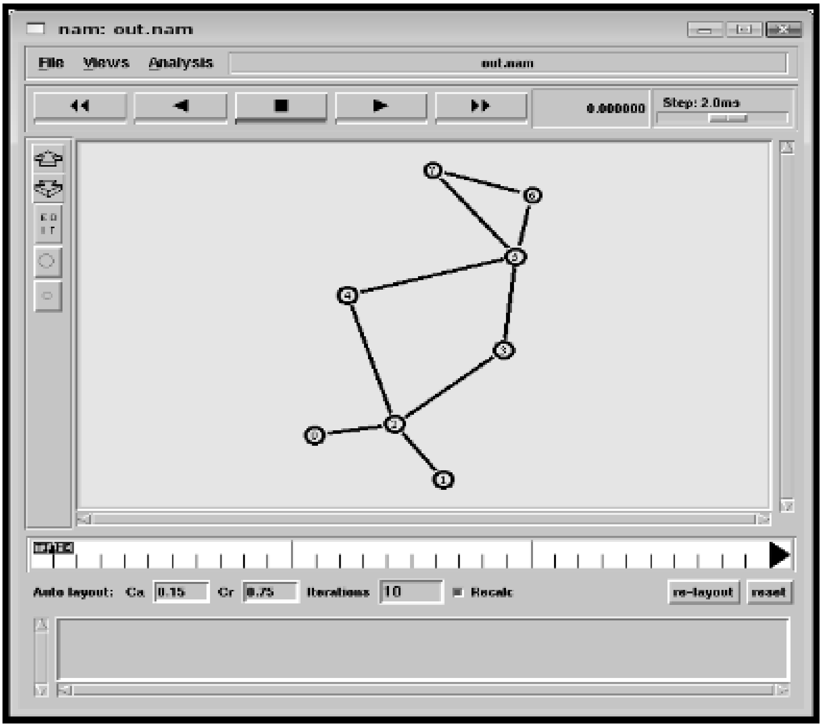
The preservation station is the storage medium situated outside the DiffServ domain. It is specifically designed to record all suspicious traffic for later analysis. The utilisation of a preservation station eases the task of the network forensic investigators.

4.4. Sink Server

The sink server is the destination of all network traffic. It receives normal traffic directly from the DiffServ network and suspicious traffic from the preservation station. The sink server receives the source signals and requests and processes all the server response data or requests directly. The combination of these components achieves the main goal of this study - *the isolation of suspicious traffic and its preservation by simulating the DiffServ model.* The section that follows next discusses the performance of the simulation.

5. Performance Evaluation

Logical traffic isolation based on the DiffServ network model was simulated in version 2.31 of the NS2 tool, (available from http://www.isi.edu/nsnam/ns), running on the Ubuntu Linux 7.04 operating system. This system has a CMU extension of NS2. It was necessary to run some initial experiments to test our DiffServ simulation and to get estimates of its capabilities. Figure 3 presents the topology that was used, consisting of eight nodes (node 0 to node 7). Nodes 0 and 1 are the traffic generators: Node 0 generates normal traffic and Node 1 generates malicious traffic. Both these nodes are forwarded to Node 2, the marking station. Node 2 marks the incoming packets according to their behaviour and subsequently forwards malicious traffic to Node 3 and normal traffic to Node 4, the core routers.



Auto layout: Ca 0.15 Cr 0.75 Iterations 10 ■ Recalc

Figure 3: Network Topology

These core routers forward the traffic to the egress router, Node 5, to avoid network congestion in other nodes. Node 5 unmarks the traffic and forwards malicious traffic to Node 6, the preservation station, and normal traffic to Node 7, the sink server. Node 7, the final destination for both types of traffic, processes all the received requests and responds accordingly. This process flows smoothly without disturbing or unplugging any machine within the network. When the network is congested, each node in the simulation uses its buffer to temporarily store packets that are awaiting transmission. This is done by using the drop-tail queue management algorithm. In this type of buffer, packets are transmitted on a first-come-first-served basis: if the buffer is full, new packets are dropped from the buffer.

For the first simulation, the study changes the buffer size to determine this variable effect on packet loss at the different nodes. The buffer size varies between 2 and 10 to prove its effectiveness. At buffer size 2, more packets are dropped than at buffer size 10. The impact of the buffer size on packet loss clearly depends on the rate at which packets arrive. For the first simulation, a constant transmission rate of 1 packet per 0.02 seconds was used. This is the minimum rate at which traffic is generated by the traffic generators at Nodes 0 and 1. When the rate was set to 1 packet per 0.01 seconds, even more packets were dropped due to a rate too fast for the buffers in the nodes. More packets are dropped at the rate of 1 packet per 0.02

seconds than at the rate of 1 packet per 0.1 seconds. A time of 500 seconds was sufficient to observe the effects of the buffer size.

PacketLoss	Time	BufferS	TRate	PacketLoss (SuspiciousT)	PacketLoss (NormalT)
1548	500	2	0.02	1050	498
1547	500	3	0.02	1038	509
1510	500	4	0.02	1001	509
1499	500	5	0.02	989	510
1487	500	6	0.02	971	516
1485	500	7	0.02	993	492
1470	500	10	0.02	966	504

Table 1: Packet Loss and Buffer Size of the Nodes

Table 1 depicts the simulation where both transmission rate (*TRate*) and time are kept constant, and the buffer size (*BufferS*) is varied between 2 and 10. The column *PacketLoss* shows the total number of packets dropped from the generators to the sink server. Figure 4 shows that when *TRate* = 1 packet per 0.02 second, *Time* = 500 seconds and *BufferS* = 2, a total number of 1 050 suspicious packets are dropped. Packet loss is calculated as follows:

PacketLoss = Total Number of packets sent – Total Number of packets received

Compared with normal traffic packets, a considerably larger number of suspicious packets are dropped. This may be ascribed to the extra node that suspicious packets have to pass through, as well as to network congestion that generally occurs during the recording period at this extra node (the preservation station). It is therefore suggested that a higher buffer size be introduced at the preservation station than at other nodes in the system. During the simulation, the suspicious traffic behaved strangely when the buffer size was greater than 6 (refer to figure 4 below). This could be the result of packets with inconsistent sizes, or the random arrival of packets to the queue.

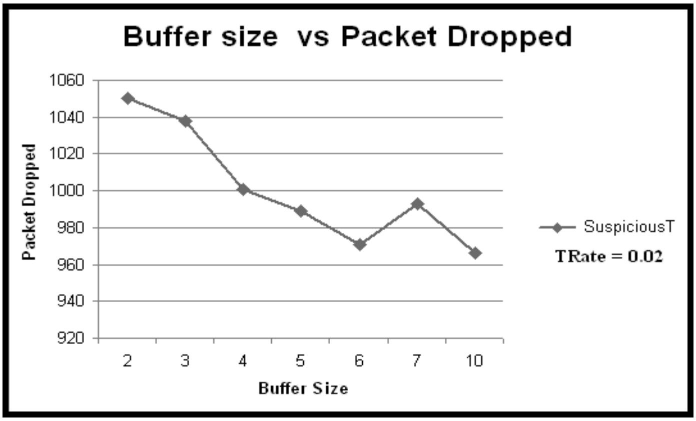


Figure 4: Packet Dropped versus Buffer Size

If the size of the network is established, it is possible to adjust only the preservation station's buffer size. This will not have an adverse effect on network behaviour. Suppose all buffers of other stations are set at 2, the preservation buffer has to be at least 66 or more in order for it not to lose any traffic (refer to Table 2). This is to avoid high volumes of evidence packets from being dropped before reaching the sink server, thereby potentially alerting cyber criminals to the ongoing investigation.

TRate	Time	BufferS (All Other Stations)	BufferS (Preservation Station)	PacketLoss (SuspiciousT)
0.02	500	2	2	1050
0.02	500	2	10	966
0.02	500	2	20	873
0.02	500	2	30	750
0.02	500	2	40	592
0.02	500	2	50	398
0.02	500	2	60	167
0.02	500	2	65	17
0.02	500	2	66	0

Table 2: Packet Loss and Buffer Size of the Preservation Station

Table 3 presents PacketLoss in relation to the transmission rate of the network traffic. The total number of suspicious packets dropped is always higher than the number of normal traffic dropped. Most of these packets are dropped at the preservation station.

PacketLoss	Time	BufferS	TRate	PacketLoss (SuspiciousT)	PacketLoss (NormalT)
1489	500	10	0.02	972	517
960	500	10	0.03	648	312
726	500	10	0.04	464	262
594	500	10	0.05	393	201
493	500	10	0.06	345	148
426	500	10	0.07	298	132
297	500	10	0.1	194	103

Table 3. Packet Loss and the Transmission Rate of traffic

The conclusion that can be drawn from this simulation is that a smaller number of packets are dropped when the buffer size is bigger. However, a varied transmission rate and a constant buffer size and time tend to have more packets dropped at a slower speed of transmission. At this point in the research, this is merely an observation and dropped packets rates cannot be guaranteed.

Figure 5 indicates that a larger number of suspicious packets are dropped when a slower transmission rate is introduced. However, this seems to be a mere tendency, since the drop rate can vary even if the transmission rate is increasing. When the client hosts are generating too much traffic at any point in time, the number of packets dropped can also increase.

Figure 6 shows the behaviour of both normal and suspicious traffic against the increasing number of generated packets. The increasing number of packets does not delay normal traffic; in fact, its transmission rate remains constant. However, the delay is different for suspicious traffic since normal traffic passes through fewer nodes than suspicious traffic. The delay can also result from the recording of each packet at the preservation station, and it is quite possible that this may cause the suspect to become suspicious.

The behaviour of normal and suspicious traffic can surely be more or less the same if the maximum size of the preservation buffer mentioned in Table 2 is used – provided that the buffer size of the other stations is kept constant at size 2. Our preliminary results show that the simulated concept results in improved support for evidence preservation. At the same time, the DiffServ model provides the Network Forensic investigators an easy means of gathering evidence. Therefore, the research discussed in this paper will make a direct contribution to the enhancement of the Network Forensics discipline.

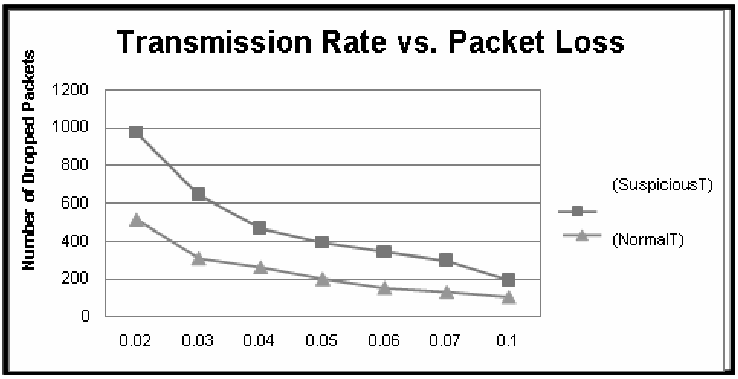


Figure 5: Packet Loss versus Transmission Rate

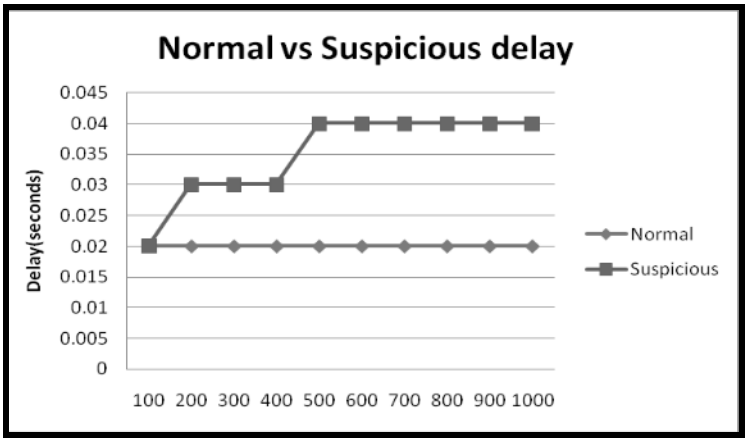


Figure 6: Delay of Normal Traffic versus Suspicious Traffic

6. Future Work and Conclusion

Traditionally it has been difficult to prosecute cyber criminals since networks do not keep data for long periods. The work in hand addresses this gap by making it possible to collect real-time forensic evidence. It points out the critical measurements that should be kept in mind when making use of such evidence, including its location in the network. The proposed scheme can be applied in real-life situations with minor alterations.

In this paper, the focus lies on the preservation of evidence – the system's preservation station records logically isolated traffic as evidence to be analysed during the forensic investigation. The simulation performance was measured and revealed an improved support for evidence preservation and evidence gathering. Future work that has emerged from the current analysis includes the following:

- *Developing a scheme that can minimise the loss of suspicious traffic.* This can be done by utilising one or two of the network methods for resource reservation (e.g. DiffServ Bandwidth Broker, Intserv or RSVP).
- *Developing mechanisms to deal with cases where incoming traffic is already tagged with Quality of Service (QoS).* It will be interesting to investigate how DiffServ architecture can be explored to solve this issue.
- *Securing the system*. The Logical Traffic Isolation framework does not address false positives or negatives of the classifier, nor how an attacker could take advantage of these.

The preservation station that is introduced as part of the DiffServ model is a sensible and practical concept and can contribute greatly to more successful Network Forensic investigations. However, to further improve the discipline, it is necessary to conduct additional investigations into the problems pointed out above.

7. References

Blake, D., Black, S., Carlson, M., Davies, E., Wang, Z. & Weiss, W. 1998, An architecture for differentiated services, *RFC 247*

Casey, E. 2002, *Handbook of Computer Crime Investigation*, Forensic tools and technology, pp 201-282, Elsevier Ltd.

Corey, V., Peterman, C., Shearin S., Greenberg, M.S. & Van Bokkelen, J. 2002, Network Forensics Analysis, *Internet Computing*, Volume 6, pp 60-66, *IEEE*.

Kim, J.S., Kim, M. & Noh, B.N. 2004, Fuzzy Expert System for Network Forensic, in A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.J.K. Tan and O. Gervasi, (Eds), *Lecture Notes in Computer Science*, Volume 3043, pp 175-182, Springer Berlin / Heidelberg.

Köhn, M., Eloff, J. & Olivier, M.S. 2006, Framework for a Digital Forensic Investigation, in H.S. Venter, J.H.P. Eloff, L. Labuschagne and M.M. Eloff (Eds), *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, Sandton, South Africa (published electronically).

Heinanen, J., Baker, F., Weiss, W. & Wroclawski, J. 1999, Assured Forwarding PHB Group, *RFC 2597*

Jacobson, V., Nichols, K. & Poduri, K. 1999, An Expedited Forwarding Per Hop Behavior, *RFC 2598*.

Ngo-Quynh, K.H., Wolisz, A. & Rebensburg, K. 2001, The Influence of Proportional Jitter and Delay on End to End Delay in Differentiated Service Network, in *Proceedings of IEEE International Symposium on Network Computing and Application NCA 01*, Cambridge, MA, USA.

Pang, B. & Gao, W. 2003, An Edge-To-Edge Congestion Control Scheme For Assured Forwarding, *2003 IEEE International Conference on Communications ICC*, Volume 2, pp i-xlv, IEEE.

Solomon, M.G., Barrett, D. & Broom, N. 2005, *The Need for Computer Forensics*, in L. Newman and W.G. Kruse (Eds), Computer Forensics Jump Start, pp 01-20, SYBEX inc.

Strauss, T., Olivier, M.S. & Kourie, D.G. 2006, Differentiated Services for Logical Traffic Isolation**,** in M.S. Olivier and S. Shenoi (Eds), *Advances in Digital Forensics II,* pp 229-237, Springer.

Vidas, T. & Wilson, J. 2006, Cyber Forensics the basics*, CERTconf2006*, NUCIA, [Online] Available at: www.certconf.org/presentations/2006/files/WD4.pdf as on April, 10, 2008.

Zantyko, K. 2007, Commentary: Defining Digital Forensics*, Forensic Magazine*, 20, Vicon Publishing, Feb-Mar 2007 issue, [Online] Available at: http://www.forensicmag.com/articles.asp? pid=130, as on April, 12, 2008.