©2010 International Journal of Computer Applications (0975 – 8887)
Volume 1 – No. 11

A Generic Framework for Network Forensics

Emmanuel S. Pilli
Department of Electronics & Computer Engineering,
Indian Institute of Technology, Roorkee, India

R.C. Joshi
Department of Electronics & Computer Engineering,
Indian Institute of Technology, Roorkee, India

Rajdeep Niyogi
Department of Electronics & Computer Engineering,
Indian Institute of Technology, Roorkee, India

ABSTRACT
Internet is the most powerful medium as on date, facilitating varied services to numerous users. It has also become the environment for cyber warfare where attacks of many types (financial, ideological, revenge) are being launched. The e-commerce transactions being carried out online are of major interest to cybercriminals. The Internet needs to be protected from these attacks and an appropriate response has to be generated to handle them to reduce the impact. Network forensics is the science that deals with capture, recording, and analysis of network traffic for investigative purpose and incident response. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. This paper presents a generic framework for network forensic analysis by specifically identifying the steps connected only to network forensics from the already proposed models for digital investigation. Each of the phases in the framework is elucidated. A comparison of the proposed model is done with the existing models for digital investigation. Research challenges in various phases of the model are approached with specific reference to network forensics.

Categories and Subject Descriptors
K.4.2 [**Computers and Society**]: Social Issues – *Abuse and crime involving computers;* K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Unauthorized access (e.g., hacking, phreaking)*

General Terms:
Security

Keywords
Network Forensics, Traffic Analysis, Traceback, Attribution, Incident Response

1. INTRODUCTION
The Internet was created to serve the communication needs of the defense establishments. It has, over the last few years, enhanced itself to accommodate a much wider community of users and provide varied services with commercial interests. It has transformed into a medium where unsuspecting users are attacked by hackers. These hackers steal the users' identity and commit financial fraud or compromise a host and launch malicious attacks on other systems.

There are many reasons which are motivating the attackers to be brave in carrying out their attacks. The speed with which an attack can be carried out, anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects.

This paper proposes a generic framework for network forensic analysis. The model is built, based on the many digital investigation frameworks proposed till date, with a specific emphasis on network crimes.

The paper is organized as follows: section 2 defines network forensics and introduces the network forensic analysis tools. Section 3 surveys related frameworks for digital investigation of which network forensics is a part. A generic model for network forensic analysis is proposed and various phases are explained in detail in section 4. The various steps in the proposed model are compared with phases in the existing models. We conclude in section 5, where the research challenges are highlighted.

2. NETWORK FORENSICS
The concept of network forensics deals with the data found across a network connection mostly ingress and egress traffic from one host to another. Network forensics analyzes the traffic data logged through firewalls or intrusion detection systems or at network devices like routers. The goal is to traceback to the source of the attack so that the cybercriminals are prosecuted.

Network forensics is defined in [14] as "the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities".

Ranum [17] is credited with defining network forensics as "the capture, recording, and analysis of network events in order to discover the source of security attacks." Network forensics involves monitoring network traffic and determining if there is an anomaly in the traffic and ascertaining whether it indicates an attack. If it is so then the nature of the attack is also determined. Network traffic is captured, preserved, analyzed and an incident response is invoked immediately.

The large number of security incidents affecting many organizations and the increase in sophistication of these cyber attacks are the main driving forces behind network forensics. The attacker is covering the tracks used to cause the attacks making it more difficult to traceback. Companies doing business on Internet cannot hide a security breach and are now expected to prove the state of their security as a compliance measure for regulatory purposes. Internet Service Providers (ISPs) are also being made responsible for what passes over their network [15]. Hence, having the network forensics process in place will meet the requirements of all – users, organizations, and ISPs.

2.1 Types of Network Forensic Systems

Garfinkel [10] classifies the network forensic systems into two types:

- **Catch-it-as-you-can systems**

All the packets passing through a particular traffic point are captured and written to storage. Analysis is subsequently done in batch mode. This approach requires large amounts of storage.

- **Stop-look-and-listen systems**

Each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This requires a faster processor to match the pace of incoming traffic.

2.2 Network Forensics and Network Security

Network forensics is being researched for several years but it still seems a very young science as many issues are still not very clear. Network forensics is not another term for network security. Network security is an essential part in network forensics as data for forensic analysis can be collected from security products placed to detect and prevent intrusions. Network forensics involves certain crimes which are legally prosecutable but they may not breach the network security policies [4].

Network security protects the system against attack while network forensics does not. Network security products look for possible harmful behaviors related with various attacks and monitor the network 24 hours a day. Network forensics is post mortem investigation of the attack in many cases. It is case restricted and is started after crime notification specifically addressing a particular attack.

Network forensics ensures that the attacker spends more time and energy to cover his tracks making the attack costly. Network criminals are also cautious to avoid prosecution for their illegal actions. This acts as a deterrent and reduces network crime rate, thus improving security. Network forensics also can initiate investigation in real time provided resources are available to handle the traffic and analyze it.

2.3 Network Forensic Analysis Tools

Network forensic analysis tools (NFATs) [24] allow administrators to monitor the networks, gather all information about anomalous traffic, assist in network crime investigation and help in generating a suitable incident response. NFATs also help in analyzing the insider theft and misuse of resources, predict attack targets in the near future, perform risk assessment, evaluate network performance, and protect intellectual propriety.

NFATs capture the entire network traffic, allow the users to analyze the network traffic according to their needs and discover significant features about the traffic. NFATs synergize with IDSs and Firewalls and make possible the long term preservation of network traffic records for quick analysis [9]. The attack traffic can be replayed and attackers' moves can be analyzed for malicious intent. NFATs facilitate organization of the captured network traffic packets to be viewed as individual transport layer connections between machines, which enable the user to analyze protocol layers, packet content, retransmitted data, and extract traffic patterns between various machines.

There are many proprietary and open source tools used for network forensic analysis. Table 1 shows gives a partial list of the NFATs popularly used:

Table 1. Network Forensic Analysis Tools

Proprietary	Open Source	
NetIntercept	Wireshark	tcptrace
NetDetector	Snort	tcpstat
NetWitness	Bro	nmap
SilentRunner	tcpdump	p0f

Many commands in the popular operating systems also support the role of NFAT: nslookup, traceroute, netstat, nbtstat, whois, ping, wget. There are two more tools which are popular with network forensic analysis: PyFlag and SiLK which analyze pcap files and netflow records respectively.

2.3.1 PyFlag

PyFlag [16] (Python Forensic Log Analysis GUI) is an advanced forensic tool for the analysis of large volumes of log files like hard disk images and network captures. PyFlag is used in the following areas: disk forensics, file carving, memory forensics, log analysis, and network forensics. PyFlag is also able to analyze network captures in tcpdump format (.pcap files) while supporting a number of network protocols.

Network forensics tools must be able to process very large capture files, extract high level information and be able to substantiate each deduction. The network forensic module of PyFlag integrates all the above aspects as it provides higher level information, while pinpointing accurately where each piece of data was derived from. PyFlag architecture has the ability to recursively examine data at multiple levels and this is ideally suited for network protocols which are typically layered, with higher level protocols being carried over lower level protocols.

The major functional components of the network forensic module are stream reassembler, packet handler and stream dissectors. PyFlag parses the pcap files, extracts the packets and dissects them at low level protocols (IP, TCP or UDP). Related packets are collected into streams using reassembler. These streams are then dissected with higher level protocol dissectors (HTTP, IRC, etc). PyFlag makes HTML rendering possible and is also able to dissect higher level application specific data as in webmail [8].

PyFlag manages each case independently and uses a unique id for I/O source while loading. It recognizes the type and populates the virtual file system and displays in tree structure. The forward and reverse traffic between various source and destinations is shown. The contents of each packet and protocol information can be viewed. The connections established, chat conversations and DNS requests can also be viewed and analyzed.

2.3.2 SiLK

SiLK [22, 23] (System internet Level Knowledge) supports efficient capture, storage and analysis of network flow data based on Cisco NetFlow. The SiLK tool suite was developed by the CERT Network Situational Awareness (NetSA) group. The tool suite provides analysts with the means to understand, query, and summarize both recent and historical traffic data in network flow records. This tool supports network forensics in identifying artifacts of intrusions, vulnerability exploits, worm behavior, etc.

The suite consists of two primary components, the collection system and the analysis tool set [11]. The collection system converts Cisco NetFlow V5 protocol data units (PDU's) into a compressed binary format. A variety of analysis tools work on these records, manipulate and summarize data. Collection system minimizes the storage space by storing fields that are required, reduces the number of bits used to store some information and saves space by avoiding storage of redundant information.

There are six fundamental tools [21] in SiLK. rwfilter retrieves data and partitions it to isolate flow records of interest. rwstats provides a collection of statistical analysis and counting facilities that enables organizing and ranking traffic by different attributes. rwcount provides a time-binned count of the number of bytes, packets, and flow records. rwcut tool reads filter files and produces user-readable output in a pipe-delimited tabular format. rwsort is a high-speed sorting tool for SiLK flow records. rwuniq counts records per combination of multiple-field keys.

There are many analytical tools in SiLK that manipulate flow record files. rwcat and rwappend tools are used for combining flow record files. rwdedupe is designed to allow analysts to remove duplicate flow records efficiently. rwsplit divides a large flow record file into pieces and concurrently analyze each piece separately. rwptoflow tool generates a single-packet flow record for every IP packet in a tcpdump file. rwpmatch takes a tcpdump file and filters it based on flow records from a SiLK record file.

SiLK has performance as a key element and manages the large volume of traffic by storing only the security related information, splits files into predefined categories to reduce lookup time and reads zipped files with equal ease. SiLK helps in analysis of scanning activity, worm detection and SYN flooding.

3. RELATED WORK

The first attempt to apply digital forensic science to networked environments was taken up as one of the objectives in the first Digital Forensic Research Workshop (DFRWS), 2001 and a framework [13] was proposed. The framework included the following steps: identification, preservation, collection, examination, analysis, presentation, and decision.

Reith et al [19] improvised the above model and produced an abstract digital forensic model that is not dependant on a particular technology or crime. Authors have added preparation and approach strategy phases and included returning the evidence in place of decision. Mandia and Prosise [12] develop an incident response methodology which is simple and accurate. An initial response phase to ascertain the incident and formulation of a response strategy are added. The investigation phase includes collection and analysis phases as in the earlier models. Presentation is called reporting and resolution phase suggest improvements, changes, and long term fixes.

Casey and Palmer [6] proposed an investigative process model to encourage a complete rigorous investigation, ensure proper evidence handling and reduce chance of mistakes. Apart from the common phases, assessment phase validates the incident and a decision is taken whether to continue with the investigation. Harvesting, reduction, organization & search phases arrange the data so that it is the smallest set with high potential evidence. Persuasion and testimony presents the case in layman terms. Carrier and Spafford [5] proposed an integrated digital investigation process based on the techniques used for physical investigations. Readiness phase ensures operations infrastructure is ready. Survey, search and collection phases gather and process the data. Reconstruction is similar to analysis phase. Documentation phase records all the evidence.

Ó Ciardhuáin [7] combined existing models and proposed an extended model of cybercrime investigations which represents the information flows and captures the full investigation. Awareness is the first step which announces investigation. Authorization is taken from internal and external entities. Planning involves strategies and policies. Dissemination is also done for guiding future investigations and procedures.

Baryamureeba and Tushabe [1] proposed an enhanced digital investigation process model reorganizing the phases in [5]. Two new phases traceback and dynamite are included. They have sub-phases like investigation, authorization, reconstruction and communication giving clarity and granularity to the major phases. Beebe and Clarke [2] propose a hierarchical, objectives based framework for digital investigative process in contrast to the single tier higher order process models. Their model consists of the common phases in first tier. These phases consist of sub-phases, placed in lower tiers, to provide specificity and granularity, guided by principles and objectives.

All the models mentioned above are applicable to digital investigation and include network forensics in a generalized form. Ren and Jin [20] were the first to propose a general process model for network forensics with the following steps: capture, copy, transfer, analysis, investigation and presentation.

4. A GENERIC FRAMEWORK

4.1 Purpose of the framework

We propose a generic framework for network forensic analysis in this section. We formalize a methodology specifically for network based digital investigation. This is necessary as network forensics is slowly emerging as an independent discipline and moving out of the shell of digital forensics. The earlier digital forensic models focus on investigation of a standalone computer and interpretation of data stored in it. Computer forensics investigator has the advantage of specialized tools which the attacker lacked whereas the network investigator and the attacker are at the same skill level. The difference is at the ethics level as the investigator uses the same tools and practices as the person being investigated [3].

Network forensics evolved as a response to the hacker community to discover and attribute the source of security attacks. Hence it is required to develop a framework specific to network forensic analysis as the modus operandi is totally at a different plane with reference to computer forensics.

4.2 Phases in the framework

The proposed framework is generic as it aggregates many of the phases available in the digital forensic models but builds on those phases which are specific to network forensics. The framework is shown in Figure 1. We give a detailed explanation for each of the following nine phases:

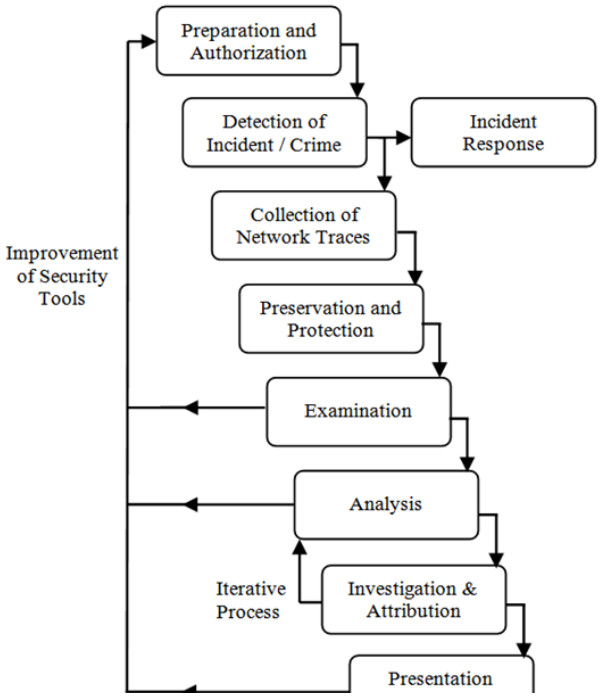

Figure 1: Generic Framework for Network Forensics

4.2.1 Preparation and Authorization

Network forensics is applicable only to environments where network security tools (sensors) like intrusion detection systems, packet analyzers, firewalls, traffic flow measurement software are deployed at various strategic points on the network. The staff handling these tools must be trained to ensure that maximum and quality evidence may be collected in order to facilitate attribution of the crime. The required authorizations to monitor the network traffic are obtained and a well defined security policy is in place so that privacy of individuals and the organization is not violated. Honeynets [18] and network telescopes [13] may also be placed to lure attackers, study their behavior and learn their strategy.

4.2.2 Detection of Incident / Crime

The alerts generated by various security tools, indicating a security breach or policy violation, are observed. Any unauthorized events and anomalies noticed will be analyzed. The presence and nature of the attack is determined from various parameters. A quick validation is done to assess and confirm the suspected attack. This will facilitate the important decision whether to continue investigation or ignore the alert as false alarm. Precaution should be taken in order that the evidence is not altered in the process. The confirmation of an incident yields two directions – incident response and collection of data.

4.2.3 Incident Response

The response to the crime or intrusion detected is initiated based on the information gathered to validate and assess the incident. The response initiated depends on the type of attack identified and is guided by organization policy, legal and business. An action plan on how to contain future attacks and recover from the existing damage in initiated. At the same time, the decision whether to continue with the investigation and gather more information is also taken. This phase is applicable only to cases where an investigation is initiated while the attack is underway and not *notitia criminis* (after notification of crime).

4.2.4 Collection of Network Traces

Data is acquired from the sensors used to collect traffic data. The sensors used must be secure, fault tolerant, have limited access and must be able to avoid compromise. A well defined procedure using reliable tools, hardware and software, must be in place to gather maximum evidence causing minimum impact to the victim. The network must be monitored to identify future attacks. The integrity of data logged and network events recorded must be ensured. Collection is the most difficult part as traffic data changes at a rapid pace and it is not possible to generate the same trace at a later time. The amount of data logged will be enormous requiring huge memory space and system must be able to handle different formats appropriately.

4.2.5 Protection and Preservation

The original data obtained in the form of traces and logs is stored on a back up device. A hash of all the trace data is taken and the data is protected. Standard procedures are used to ensure accuracy and reliability of the preserved data. Chain of custody is strictly enforced so that there is no unauthorized use or tampering. Another copy of the data will be used for analysis and the original collected network traffic is preserved. This is done so that the investigation done may be proved again on the original preserved data to meet the legal requirements.

Table 2. Comparison with existing frameworks for Digital Forensic Analysis

Proposed Framework 2009	DFRWS 2001	Reith, Carr & Gunsch 2002	Prosise & Mandia 2003	Casey & Palmer 2003	Carrier & Spafford 2003	Séamus Ó Ciardhuáin 2004	Baryamu-reeba & Tushabe 2004	Beebe & Clarke 2006	Ren & Jin 2006
Preparation & Authorization	---	Prepara -tion	Pre-incident Preparation	---	Readiness, Authoriza -tion	Awareness, Authorization, Planning	Readiness, Authorization, Confirmation	Prepara-tion	---
Detection	Identifica -tion	Identifica-tion	Detection of incident	Incident Alerts, Assessment	Detection, Notification	Notification	Detection,	Incident Response	---
Incident Response	---	Approach Strategy	Initial Response, Response Strategy	---	---	---	---	Incident Response	---
Collection	Collec-tion	Collection	Investigation (Data Collection)	Crime Scene Protocol, Identification & Seizure	Survey	Search & Identification, Collection	Submission	Data Collection	Capture
Preservation	Preserva -tion	Preserva-tion	---	Preservation	Preserva -tion	Transport, Storage	Preservation	---	Copy, Transfer
Examination	Examina -tion	Examina-tion	---	Recovery, Harvesting, Reduction, Organization & Search	Search & Collection	Examination	Survey	---	---
Analysis	Analysis	Analysis	Investigation (Forensic Analysis)	Analysis	Reconstruc -tion	Hypothesis	Search & Collection	Data Analysis	Analysis
Investigation	---	---	---	---	---	---	Traceback (Investigation) Reconstruction	---	Investiga -tion
Presentation & Review	Presenta -tion, Decision	Presenta-tion, Returning Evidence	Reporting, Resolution	Reporting, Persuasion & Testimony	Present -ation, Review	Presentation, Proof of Defense, Dissemination	Communication Review	Presenta -tion of Findings, Incident Closure	Presenta -tion

4.2.6 Examination

The traces obtained from various security sensors are integrated and fused to form one large dataset on which analysis can be performed. Mapping and time lining of this data is also performed. This is done so that crucial information is not lost or mixed up. Data hidden or camouflaged by the attacker needs to be recovered. The collected data is classified and clustered into groups so that the volume of data to be stored may be reduced to manageable chunks. It is easy to analyze large groups of organized data. Redundant information and unrelated data is removed and minimum representative attributes are identified so that the least information with the highest probable evidence needs analysis.

4.2.7 Analysis

The evidence collected is searched methodically to extract specific indicators of the crime. The indicators are classified and correlated to deduce important observations using the existing attack patterns. Statistical and data mining approaches are used to search the data and match attack patterns. Some of the important parameters are related to network connection establishment, DNS queries, packet fragmentation, protocol and operating system fingerprinting, running rogue processes, installed software or rootkits. The attack patterns are put together and the attack is reconstructed and replayed to understand the intention and methodology of the attacker. The result of this phase is the validation of the suspicious activity.

4.2.8 Investigation and Attribution

The information obtained from the evidence traces is used to identify who, what, where, when, how and why of the incident. This will help in source traceback, reconstruction of the attack scenario and attribution to a source. The most difficult part of the network forensic analysis is establishing the identity of the attacker. Two simple strategies of the attacker to hide himself are IP spoofing and stepping stone attack. Researchers have proposed many IP traceback schemes to address the first attack and is still an open problem. Stepping stones are created by attackers to use compromised systems to launch their attacks. They can be detected using similarity and anomaly based approaches applied to packet statistics. The approach of the investigation depends on the type of attack.

4.2.9 Presentation and Review

The observations are presented in an understandable language to the organizations management and legal personnel while providing explanation of the various standard procedures used to arrive at the conclusion. The systematic documentation is also included to meet the requirements. The conclusions may also be presented using visualization so that they can be easily grasped. The statistical data is interpreted in support of the conclusions arrived. A thorough review of the incident is done and counter measures are recommended to prevent similar incidents in future. The results are documented to influence future investigations and in improvement of security products.

Proposed model has preparation as the first phase as network forensics is applicable only when prerequisite security products are in place. Digital investigations can start with identification of attacks. Collection of network traces precedes the preservation of data as network data is volatile and recording the evidence in the available time is of prime importance. Physical media on standalone system needs preservation first and collection of logs is done as per convenience. A thorough investigation is required for traceback and attribution for network based digital evidence. Analysis will only give the direction and results have to be correlated to develop the proof. The network forensic framework has most of the phases as in a digital investigation model, but the order in which each phase is executed is different. Incident response is also not considered in many models for digital investigation as nothing much can be done after the attack is complete.

5. CONCLUSION

A first attempt was made in this paper to propose a framework for network forensic analysis. It is a generic aggregation of many models proposed till date and builds on the requirements specific to network based forensics. As part of our work, we intend to address the following problems in the various phases proposed in the framework:

- Fusion of data collected from various security products deployed in the network is required.
- There is a need to develop techniques to scrutinize large amount of data and understand the relationships.
- The network events useful to match attack patterns for investigative requirements need to be identified.
- The analysis of logs and network traces must enable attribution of the attack to a particular source.
- Attacks on new protocols also need investigation.

The shortfalls and challenges in various phases need to be urgently addressed so that the perpetuators are traced back, prosecuted and network crime rate is brought down drastically.

6. REFERENCES

[1] Baryamureeba, V. and Tushabe, F. 2004. The enhanced digital investigation process model. In Proceedings of the 4th Digital Forensic Research Workshop (Maryland, USA, 2004).

[2] Beebe, N.L. and Clark, J.G. 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation. *2* (2), 147-167.

[3] Berghel, H. 2003. The discipline of Internet forensics. Communications of the ACM. *46* (8). 2003, 15-20.

[4] Broucek, V. and Turner, P. 2001. Forensic computing: Developing a conceptual approach for an emerging academic discipline. In Proceedings of the 5th Australian Security Research Symposium, (Perth, Australia, 2001).

[5] Carrier, B. and Spafford, E.H. 2003. Getting physical with the digital investigation process. International Journal of Digital Evidence. *2* (2). 2003.

[6] Casey, E. and Palmer, G. 2004. The investigative process. in Casey, E. ed. Digital evidence and computer crime, Elsevier Academic Press, 2004.

[7] Ciardhuáin, S.Ó. 2004. An extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3 (1), 2004.

[8] Cohen, M.I. 2008. PyFlag - an advanced network forensic platform. Digital Investigation, 5 (1), 112-120.

[9] Corey, V. Peterman, C. Shearin, S. Greenberg, M.S. and Bokkelen, J.V. 2002. Network forensics analysis. IEEE Internet Computing, 6 (6), 60-66.

[10] Garfinkel, S. Network Forensics: Tapping the Internet. http://www.oreillynet.com/pub/a/network/2002/04/26/ nettap.html

[11] Gates, C., Collins, M., Duggan, M., Kompanek A., and Thomas M. 2004. More Netflow Tools: For Performance and Security. In Proceedings of the 18th Conference on *Large Installation Systems Administration,* (Atlanta, USA, 2004), 121-132.

[12] Mandia, K. and Procise, C. 2003. Incident Response and Computer Forensics. (Osborne McGraw-Hill, New York, 2003).

[13] Moore, D., Shannon, C., Voelker, G. M. and Savage, S. 2004. Network telescopes: Technical report. CAIDA. (April, 2004).

[14] Palmer, G. 2001. A Road Map for Digital Forensic Research, 1st Digital Forensic Research Workshop, (New York, 2001), 15-30.

[15] Perry, S. 2006. Network forensics and the inside job. Network Security. 2006, 11-13.

[16] PyFlag, http://www.pyflag.net

[17] Ranum, M. Network Flight Recorder, http://www.ranum.com/

[18] Raynal, F., Berthier, Y., Biondi, P., and Kaminsky, D. 2004. Honeypot Forensics Part I: Analyzing the Network, IEEE Security & Privacy. 2 (4). (Jul – Aug 2004), 72-78.

[19] Reith, M., Carr, C., and Gunsch, G. 2002. An examination of digital forensic models. International Journal of Digital Evidence. 1. 2002.

[20] Ren, W. and Jin, H. 2005. Modeling the network forensics behaviors. In Proceedings of the 1st Int'l Conf. Security and Privacy for Emerging Areas in Communication Networks (Athens, Greece, 2005), 1-8

[21] Shimeall, T., Faber, S., DeShon, M., Kompanek,. 2009. Using SiLK for Network Traffic Analysis, SiLK Analysts Handbook. (January, 2009).

[22] SiLK, http://silktools.sourceforge.net/

[23] SiLK, http://tools.netsa.cert.org/silk/

[24] Sira, R. 2003. Network Forensics Analysis Tools: An Overview of an Emerging Technology. GSEC (1.4), 2003.