한국산학기술학회논문지
Vol. 12, No. 1 pp. 467-473, 2011

IDS 관제를 위한 네트워크 포렌식 연구

이기성[1*], 노시영[2], 박상준[2], 이종찬[2], 신성윤[2]
[1]호원대학교 컴퓨터·게임학부, [2]군산대학교 컴퓨터정보공학과

A Study of Network Forensic for IDS

Gi Sung Lee[1*], Si Young No[2], Sang Joon Park[2], Jong Chan Lee[2] and Seong Yoon Lee[2]
[1]Div. of Computer and Game, Howon University
[2]Dept. of Computer Information Eng., Kunsan National University

요 약 본 논문은 네트워크 패킷에 대한 무결성을 보장하여 법적 증거 자료로써 효력을 가질 수 있는 네트워크 포렌식 시스템을 제안하고자 한다. 본 논문에서 제안된 네트워크 포렌식 시스템은 기업이 네트워크 사고를 통한 법정 분쟁과 국가 기관에서 네트워크 범죄에 대한 수사에 대해 효과적인 해결 방법을 제시하며 사용자 중심의 보고서를 통한 효율적인 업무 인지도를 향상 시킬 수 있다.

Abstract The Network-packet in this Paper to ensure the integrity of the legal evidence is effect that can have is to offer an Network-forensics system.
The Paper proposed Network-forensics system in the company through legal disputes accident Networking and state agency (with investigative authority) for criminal investigations in networking for the effective and correct way to present a report of user-centric services through effective awareness can be improved.

Key Words : Forensic, Network Forensic, Integrity, Network packet, Intrusion Detection System

1. 서론

인터넷과 IT 기술의 발전은 정보를 디지털화를 가속화 시키는 계기가 되었다. 이러한 현상은 디지털 정보를 통해 우리의 삶이 자동화, 정보화되어 일상생활에 많은 도움을 주고 있다. 이로 인해 우리의 삶이 편해지지만 그에 따른 부작용으로 디지털을 이용하여 많은 범죄가 늘어나고 있으며 또한 일반 범죄 현장에서도 법정 증거로써 효력을 가지고 있는 많은 자료들이 디지털 기기 내에 보관되고 있는 경우가 증가하므로 이러한 증거 자료를 수집 및 분석하기 위한 방법으로 포렌식이 등장하였다[1,2].

포렌식이란 법의학 용어로 법정 증거로써 시작하여 지금은 컴퓨터 관련 수사 자료를 지원하며 각종 디지털 자료가 법적 효력을 갖도록 하는 과학적, 논리적 절차와 방법을 연구하는 학문을 일반적으로 컴퓨터 포렌식으로 정의를 하고 있다[3]. 이러한 포렌식의 경우 디지털 증거의 특성을 가지고 있을 뿐 아니라 포렌식의 특성을 가지고 있는 것을 말한다[8,9]. 네트워크 포렌식은 디지털 포렌식의 한 부분으로 사건 발생 시 개인 컴퓨터에 있는 네트워크 정보나 인터넷 접속 정보 등을 수집하는 용도로 사용하였다. 하지만 네트워크 공격의 성격이 더욱 정밀화 되고 있고 그에 따른 피해가 더욱 커지고 있다[5]. 따라서 이러한 네트워크 환경에 대처 할 수 있는 포렌식 환경을 구축하여야 한다. 본 논문에서는 현재 네트워크를 관제하는 시스템에 포렌식을 적용시켜 법정 증거로써 가치를 가지는 네트워크 패킷 분석 자료에 대한 방안을 제안한다.

이 논문은 2010년 호원대학교 교내연구비의 지원에 의하여 연구되었음.
*교신저자 : 이기성(ygslee@sunny.howon.ac.kr)
접수일 10년 11월 17일 수정일 10년 12월 15일 게재확정일 11년 01월 13일

2. 관련연구

2.1 네트워크 공격

서비스 거부(DoS: Denial-of-Service) 공격은 피해 호스트가 인터넷에 정상적인 서비스를 제공하거나 서비스를 받는 것을 방해하는 공격이다. DoS 공격의 방법으로 시스템의 취약성을 공격하는 방법이 있다[4]. 다른 방법으로 복잡한 계산을 요구하여 시스템의 처리 능력을 저하시킨다[6, 7]. 분산 서비스 거부(DDoS: Distributed DoS) 공격은 새로운 형태의 DoS 공격이다. 일반적인 DoS 공격과 달리 DDoS 공격은 특정 네트워크 프로토콜이나 시스템의 취약성을 이용하지 않는다. DDoS 공격은 다수의 감염된 호스트가 피해 호스트에게 다량의 무의미한 패킷을 전송하여, 피해 호스트와 인터넷 사이의 자원 불균형을 초래한다. 감염된 호스트로부터 전송되는 막대한 트래픽은 피해 호스트의 연결을 방해한다[10,11].

Hostscan과 Portscan은 몇몇 네트워크 공격의 준비과정으로 사용된다. 공격을 시행하기에 앞서 공격자는 취약성을 가진 서비스를 제공하는 공격 대상 호스트에 대한 정보를 가질 필요가 있다[10]. Hostscan은 작동 중인 호스트를 찾는 과정이다. 공격자는 Hostscan을 이용하여 어떤 호스트가 네트워크 공격에 취약한지 확인한다. 이 경과에 따라 공격자는 공격의 목표를 결정한다. 공격 목표가 결정되면 공격자는 목표 호스트의 열려있는 port를 찾기 위해서 Portscan을 수행한다. 공격자는 선택된 호스트의 port들을 검사하여 어떤 port가 공격에 대해 열려있는지 알 수 있다. 이후 공격자는 선택된 호스트의 열려있는 port를 이용하여 네트워크 공격을 수행한다. Hostscan은 다음 그림과 같이 특정한 근원지 주소로부터 다양한 목적지 주소로 패킷이 전송된다. 또는 Portscan과 동시에 수행되어 일정 근원지에서 다양한 목적지 주소, 목적지 포트로 패킷이 전송된다. Portscan의 경우 다음 그림과 같이 특정한 근원지에서 특정한 목적지를 향하여 다양한 목적지 port로 패킷이 전송된다.

웜은 스스로 자신을 복제하여 네트워크상에 연결된 다른 컴퓨터들 스스로 자신을 전송하는 특성을 가지고 있다. 바이러스처럼 스스로 자신을 복제하긴 하지만 웜의 경우 자신을 스스로 복사해서 네트워크상에 연결된 곳을 스스로를 전파 시킨다는 점에서 차이를 가지고 있다. 웜의 스캐닝 단계는 웜이 자신이 감염시킬 수 있는 네트워크에 연결된 호스트를 찾는 단계로 TCP 프로토콜을 사용하는 웜의 경우 TCP SYN 패킷을 보내서 응답을 받아서 스캐닝 정보를 받고 UDP의 경우엔 UDP request 메시지를 보내고 이에 대한 응답 메시지를 통해서 그 정보를 확인할 수 있다. 그리고 진화한 웜의 경우 스캐닝과 감염을 동시에 시키는 경우도 있다. 특히 UDP 프로토콜을 이용하는 경우가 많은데, 스캐닝 패킷에 자신의 전체 패킷을 담아서 스캐닝을 하면서 응답을 하는 호스트에 바로 자신의 복제 이미지를 전송하게 되는 것이다. 웜 패킷 특성을 살펴보면 하나의 패킷이 감염을 발생시켜 불특정 다수의 목적지 주소에 매우 폭넓게 분포하게 된다.

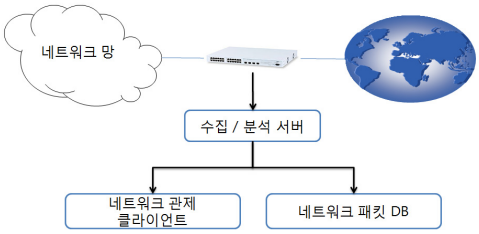
3. 네트워크 포렌식 기법

3.1 네트워크 관제시스템

최근 네트워크 공격에 대한 문제점이 많이 발생하고 있다. 최근에 발생한 DDoS 공격이 7.7대란의 경우 우리나라의 인터넷 망 뿐만 아니라 세계 주요 도시들까지 네트워크를 마비 할 정도로 규모가 큰 문제로 남았고 또한 이 문제로 네트워크 공격이 단순한 총으로 하는 전쟁이 아닌 인터넷 전쟁의 영향과 그 여파를 확인할 수 있는 문제로 남아 있다. 이러한 네트워크 공격을 탐지하기 위해서 네트워크 관제 시스템이 필요하다. 네트워크 관제 시스템이란 네트워크상에서 발생되는 각종 공격에 대한 실시간 모니터링 도구와 공격에 대한 상세 분석을 지원하는 분석 도구 등으로 구성되어 있으며 이러한 네트워크 관제 시스템은 네트워크 장치에 연결하여 네트워크를 지나는 패킷이나 보안 장비에 대한 관제를 한다. 이러한 네트워크 관제 시스템으로 허니넷을 예를 들을 수 있는데 많은 해킹 툴과 해킹의 방법을 연구하기 위한 시스템으로 해킹에 대해 무방비로 노출을 시켜 해킹을 시도한 패킷의 수집과 연구 분석용으로 많이 사용하고 있다.

3.2 네트워크 포렌식

네트워크 포렌식은 디지털 포렌식의 한 부분으로 사건 발생 시 개인 컴퓨터에 있는 네트워크 정보나 인터넷 접속 정보 등을 수집하는 용도로 사용하였다. 하지만 네트워크 공격의 성격이 더욱 정밀화 되고 있고 그에 따른 피해가 더욱 커지고 있다[5]. 따라서 이러한 네트워크 환경에 대처 할 수 있는 포렌식 환경을 구축하여야 한다. 따라서 현재 네트워크를 관제 하는 시스템에 포렌식을 적용시켜 네트워크 패킷에 대한 분석 자료를 활용하여 법정 증거로써 가치를 가지는 증거를 발견할 수 있어야 한다.



[그림 1] 네트워크 포렌식 구조도

네트워크 관제가 시작하면 관제 시스템에서는 각각의 방법으로 패킷을 분석한다. 이렇게 분석된 패킷의 정보는 GUI 클라이언트에서 보여주게 되는데 이러한 증거들이 법정 증거 자료로써 활용하기 위해서는 포렌식의 특성을 보장하여야 한다. 무결성을 보장하기 위해서는 패킷이 분석되기 전부터 완료까지의 패킷에 대한 정보를 표시하여 패킷에 대한 무결성을 보장하여야 한다.

본 논문에서 네트워크 패킷에 정보를 분석하는 과정에서 패킷의 관리는 중요하다. 법정에서 증거로 나온 자료들이 사건의 시간과 파일의 시간이 일치하지 못하여 증거로써 가치를 상실하는 경우가 많다. 따라서 사건의 증거에 대한 시간 정보는 무결성을 보장하기 위해서 중요하다. 하지만 네트워크 관제 프로그램에서 실시간 네트워크를 관제하기 위해서 이러한 시간 데이터를 소홀이 하는 경우가 있다. 이러한 패킷의 정보는 사건에 대한 시간과 일치하지 못하여 무결성을 보장할 수 없게 된다. 따라서 네트워크를 관제하는 과정에서 시간 정보와 함께 관리하여 무결성을 보장하여야 한다. 실시간 네트워크 관제 시스템은 수집 서버를 이용하여 네트워크 패킷에 대한 분석 정보를 클라이언트로 전해져서 사용자들에게 보이게 되는데 이러한 패킷은 실시간성을 최대로 보장하여 급박한 상황이 발생하였을 때에 대처하여야 한다. 따라서 네트워크에 대한 실시간과 무결성을 보장하기 위해서는 수집서버에서 클라이언트로 분석 정보를 보내는 동시에 서버에서 DB로 분석 정보를 같이 저장하여야 한다.

네트워크 관제 프로그램에서 패킷의 저장은 주로 PCAP 파일이나 NetFlow 파일등과 같이 사용자가 쉽게 확인 할 수 있는 파일 형식으로 저장이 된다. 이런 경우 패킷의 중요 정보를 변경 또는 삭제를 하여 중요 정보를 은닉할 수 있다. 또한 이러한 자료는 법정 증거 자료로써 사용 되더라도 무결성을 보장하지 못하여 포렌식 증거자료로는 사용 할 수 없게 된다. 또한 수사 측면에서도 현재 이러한 자료를 근거로 범인을 검색, 추적을 하는데 이러한 수사는 불공정한 수사가 될 수 있는 소지를 충분히 가지고 있다. 따라서 네트워크 패킷에 대한 포렌식을 적용시키기 위해서는 가장 먼저 무결성을 얼마나 보장할 수 있는 것이 문제이다.

이러한 무결성을 보장하기 위한 방법으로 많이 사용하는 방법으로 Hash 파일 비교를 많이 사용한다. 이러한 이유는 Hash 파일의 특성상 파일 내에 빈 공간이라도 수정이 되는 경우 Hash 파일 값이 변경이 되기 때문에 원본 파일과의 비교를 하여 Hash 값이 같을 경우 원본과 동일한 파일임을 증명할 수 있다. 이러한 Hash 파일의 최초의 알고리즘은 1993년에 미국 표준 기술 연구소(NIST)에 의해 Hash 표준(Secure Hash Standard, FIPS PUB 180)으로 개발되었으며, 다른 함수들과 구별하려 보통 SHA-0이라고 명칭 되었다. 1995년에 개정된 알고리즘(FIPS PUB 180-1)을 새로 개발되었으며 이를 SHA-1이라고 명칭 되었다. SHA-1은 SHA-0의 압축 함수에 비트 회전 연산을 하나 추가한 것으로 NSA에 따르면 SHA-0의 알고리즘에서 암호학적 보안을 감소시키는 문제점을 고친 것으로 SHA-1은 SHA-0보다 암호학적 공격이 힘든 것으로 알려져 있다. 현재까지 SHA-1의 공격법은 발견되었지만 이를 충돌할 방법은 아직 없다. SHA-0과 SHA-1은 최대 2^{64}비트의 메시지로부터 160비트의 Hash 값을 만들어 내며 로널드 라이베스트가 MD4 및 MD5 Hash 함수에서 사용했던 것과 비슷한 방법에 사용한다. NIST는 나중에 Hash 값의 길이가 더 긴 네 개의 변형을 발표했으며, 이들을 통칭하여 SHA-2라 부른다. SHA-256, SHA-384, SHA-512는 2001년에 초안으로 처음으로 발표되었으며, 2002년에 SHA-1과 함께 정식 표준(FIPS PUB 180-2)으로 지정되었다. 2004년 2월에 삼중 DES의 키 길이에 맞춰 Hash 값 길이를 조정한 SHA-224가 표준에 추가되었다. SHA-256과 SHA-512는 각각 32비트 및 64비트 워드를 사용하는 Hash 함수이며, 몇몇 상수들이 다르긴 하지만 그 구조는 라운드의 수를 빼고는 완전히 같다. SHA-224와 SHA-384는 서로 다른 초기 값을 가지고 계산한 SHA-256과 SHA-512 Hash 값을 최종 Hash 값 길이에 맞춰 잘라낸 것이다. SHA 함수들의 특성은 다음 표와 같다.

[표 1] SHA 함수 특성표

알고리즘	해쉬값 크기	내부 상태 크기	블록 크기	길이 한계	워드 크기	과정 수	사용되는 연산	충돌
SHA-0	160	160	512	64	32	80	+,and, or,xor, rotl	발견됨
SHA-1	160	160	512	64	32	80	+,and, or,xor, rotl	공격법만 존재
SHA-256/224	256/224	256	512	64	32	64	+,and, or,xor, shr,rotr	-
SHA-512/384	512/384	512	1024	128	64	80	+,and, or,xor, shr,rotr	-

이러한 Hash 파일 비교 검사를 통하여 파일의 위변조를 확인 할 수 있다. 다음 Hash 값 비교표는 간단한 테스트를 통한 Hash 함수 비교를 한 것이다.

[표 2] Hash 값 비교표

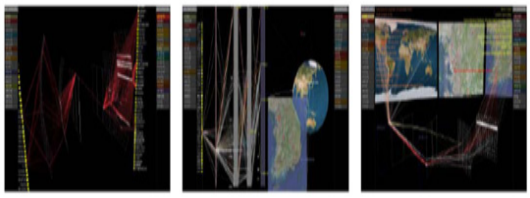
형식	기존값	변경값
내용	test	test.
SHA1	a94a8fe5ccb19ba61c4c0873d391e98798 2fbbd3	95ed7744c2076fc83d4c78f23f78b6a5b91 c147f
SHA256	9f86d081884c7d659a2feaa0c55ad015a3b f4f1b2b0b822cd15d6c15b0f00a08	4ee3df88f682d376531d8803f2ccbee56d0 75cd248fc300f55dfe8596a7354b7
SHA384	768412320f7b0aa5812fce428dc4706b3ca e50e02a64caa16a782249bfe8efc4b7ef1c cb126255d196047dfedf17a0a9	7cdb958fdb261552e501c80a442c2b0f94 7e512f7f4bda85d2d93cc2d2362a7a4af61 1aca95bf9a19d1aee19ff0f13e4
SHA512	ee26b0dd4af7e749aa1a8ee3c10ae9923f6 18980772e473f8819a5d4940e0db27ac18 5f8a0e1d5f84f88bc887fd67b143732c304 cc5fa9ad8e6f57f50028a8ff	bbc1df86d1994a5c762fab9e815bbe28c9 8789b8320348c8e4a8ac0f270b2260edd7 2712cc4fb75231ae8d0257900a86cc7154 1b13c2364e18639016fad126c6

위 표를 살펴보면 최초 텍스트인 ‘test'에서 ‘test.’로 ‘.’만 추가만 있을 뿐인데 값이 확연히 달라지는 것을 확인할 수 있다. 따라서 패킷에 대한 Hash 파일을 자동 백업하여 파일에 대한 무결성의 최소한의 보장을 하여야 한다.

3.3 네트워크 분석결과 보고

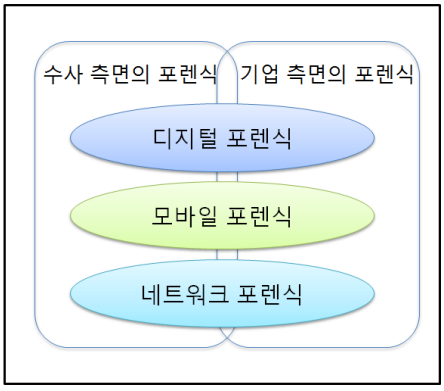
이러한 정보는 분석가들이 필요한 정보를 제공하지만 패킷에 대한 이해와 분석을 하기는 쉽지 않다. 이러한 분석 결과 보고는 패킷에 대한 정보를 판단하므로 분석 결과 모니터링 화면과 분석 결과 보고서는 누가 보더라도 쉽게 이해할 수 있어야 하며 또한 포렌식에 대한 다양한 측면에 대한 분석 필요하다.

패킷에 대한 정보는 패킷 헤더 값에 있는 정보로 표현할 수 있다. 이러한 정보를 단순한 수치상의 데이터를 출력하게 된다면 이를 분석하기 힘들뿐 아니라 분석가들의 판단으로 이를 해석을 잘못 할 수 있다. 따라서 이러한 화면 구성은 분석가들이 쉽게 이해 할 수 있는 구조로 설계를 하여야 하고 화면만 보더라도 패킷에 종합적인 판단을 할 수 있어야 한다. 그러기 위해서는 패킷에 대한 공격자 측과 목적지의 IP주소와 프로토콜 등의 정확한 정보가 표현되어야 하며 다양한 패킷에 대한 정보를 한눈에 확인 할 수 있는 구조로 표현되어야 한다. 네트워크 분석 모니터링 화면은 패킷에 대한 정보의 표현을 그래픽으로 표현하기 때문에 분석가들이 이해하기 쉽고 정확한 판단을 도와주기 위해서 표현되는 것으로 패킷에 대한 다양한 정보와 값을 화면에 정확히 표현하여야 한다. 네트워크 패킷에 대한 표현은 다양한 방법으로 표현할 수 있지만 중요한 것은 패킷에 대한 정확성과 분석가가 쉽게 인지 할 수 있어야 한다. 그래서 최근에는 네트워크 관제 시스템을 그래픽으로 표현하여 분석가들에게 자세한 표현을 보다 쉽게 제공하고 있는 추세이다.



[그림 2] 네트워크 보안관제 시스템

네트워크 보안관제 보고서 내용은 네트워크 패킷에 대한 여러 가지의 정보를 가지고 있다. 이러한 정보는 전문가들의 판단의 결정하기 위해 보다 많은 정보들을 담고 있다. 그러다 보니 보고서는 일반 사용자들이 이해하기 어려운 구조로 되어 있는 경우가 많고 이러한 보고서가 증거 자료로써 사용되게 되면 보고서에 대한 오해 혹은 이해를 하지 못하여 잘못된 판단을 할 수 있다. 따라서 보고서의 내용이 초보자도 이해하기 쉬운 구조로 만들어져 있어야 하며 판단에 오해의 소지가 없도록 구조를 만들어야 한다. 또한 각 상황에 맞는 보고서를 준비하여 신속성 및 증거물로써 가치를 향상시킬 수 있다. 예를 들면 포렌식의 형식 중 수사 측면의 보고서와 기업 측면의 보고서의 양식의 구분을 통해 증거에 대해 바라보는 시선이 다르게 표현될 수 있기 때문에 다양한 보고서 형식을 통해 증거를 표현하는 것이 인지도 향상을 위해 좋은 방법이 된다.



[그림 3] 포렌식의 관점

수사 측면의 보고서와 기업 측면의 보고서의 차이는 포렌식을 바라보는 관점의 차이에서 나올 수 있다. 수사 측면에서는 관제 시스템에서 네트워크 패킷에 대한 분석을 통하여 범인을 검거하는 목적으로 네트워크 포렌식을 사용하기 때문에 IP 추적에 관한 정보 즉 소스 측 IP 주소와 프로토콜, 공격 유형, 소스 측 사용자의 주소 등의 정보가 수사에 도움이 되므로 보고서에 추가하여 수사관의 업무에 도움을 줄 수 있어야 하며 기업 측면의 경우 네트워크에 침입 및 파일의 전송으로 기업의 재산에 피해를 준 타당한 증거를 확보하여 법정 분쟁에서 방어적인 측면에서 사용가능한 보고서를 제공한다.

	작성일자	문서번호	변경코드	화일/참고	페이지

네트워크 관제 보고서

제목	네트워크 위협 관제 보고
작성자	홍길동
상황일시	GL_20091020164935
보안상황	위협
보고내용	

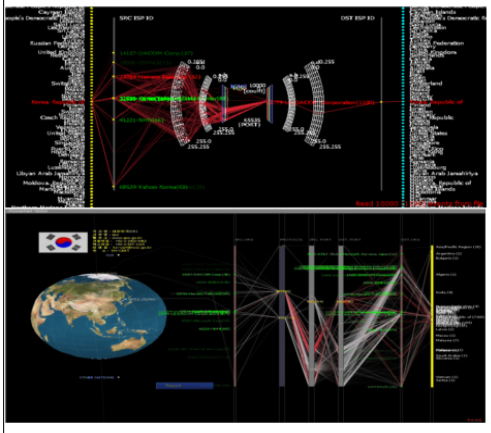
□ 네트워크 상황

소스측 IP주소	소스측 국가	소스측 ISP정보	목적지 IP주소	목적지 ISP정보
123.456.789.000	중국	ChinaISP	987.654.321.000	LG Dacom
123.456.789.001	중국	ChinaISP	987.654.321.001	LG Dacom
123.456.789.005	중국	ChinaISP	987.654.321.002	LG Dacom
123.456.789.006	중국	ChinaISP	987.654.321.003	LG Dacom
123.456.789.002	중국	ChinaISP	987.654.321.004	LG Dacom

□ 소스측 IP 정보

소스측 IP주소	소스측 국가	도시	프로토콜	위도	경도
123.456.789.000	중국	북경	TCP	39.904008	116.408644
123.456.789.001	중국	북경	TCP	39.904008	116.408644
123.456.789.005	중국	북경	TCP	39.904008	116.408644
123.456.789.006	중국	북경	TCP	39.904008	116.408644

□ 네트워크 관제 화면



[그림 4] 기업관점의 보고서

	작성일자	문서번호	변경코드	화일/참고	페이지

IP 추적 결과 보고서

제목	네트워크 위협 관제 보고
작성자	홍길동
상황일시	GL_20091020164935
보안상황	위협
보고내용	

□ 네트워크 상황

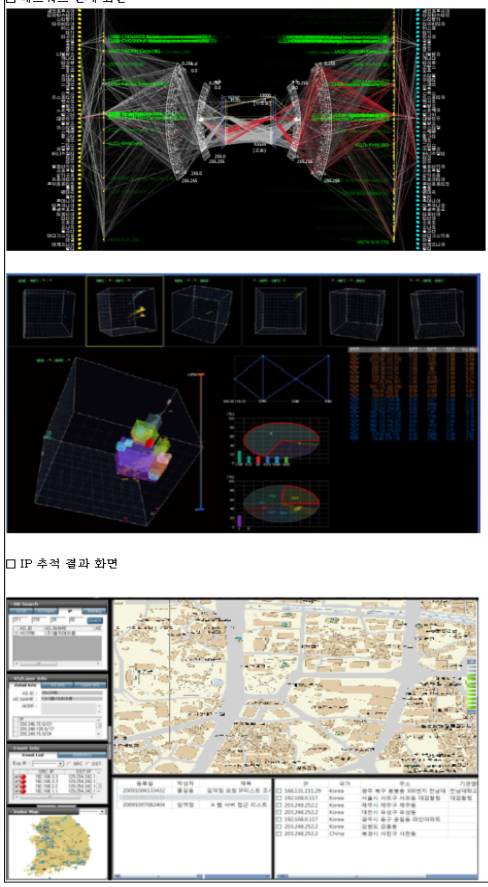
소스측 IP주소	소스측 국가	소스측 ISP정보	목적지 IP주소	목적지 ISP정보
123.456.789.000	중국	ChinaISP	987.654.321.000	LG Dacom
123.456.789.001	중국	ChinaISP	987.654.321.001	LG Dacom
123.456.789.005	중국	ChinaISP	987.654.321.002	LG Dacom
123.456.789.006	중국	ChinaISP	987.654.321.003	LG Dacom
123.456.789.002	중국	ChinaISP	987.654.321.004	LG Dacom

□ 소스측 IP 정보

소스측 IP주소	소스측 국가	도시	프로토콜	위도	경도
123.456.789.000	중국	북경	TCP	39.904008	116.408644
123.456.789.001	중국	북경	TCP	39.904008	116.408644
123.456.789.005	중국	북경	TCP	39.904008	116.408644
123.456.789.006	중국	북경	TCP	39.904008	116.408644

IP 정보	국가	주소	기관명
168.131.151.29	한국	광주 북구 용봉동 300번지	한국대
192.168.0.117	한국	서울시 서초구 서초동 23번지	
203.248.252.2	한국	제주시 제주구 제주동	
203.248.252.4	한국	대전시 유성구 유성동	
192.168.0.117	한국	광주시 동구 운림동 라인아파트	

□ 네트워크 관제 화면



□ IP 추적 결과 화면

[그림 5] 수사관점의 보고서

4. 결론

IDS 관제 시스템에서 네트워크 패킷에 대한 정보를 법정증거 자료로써 사용하기 위해서 포렌식의 기본 원칙을 보장하여야 한다. 그러기 위해서는 네트워크 패킷에 대한 관리와 저장, 분석 과정에서 네트워크 포렌식 시스템을 적용하여 네트워크 패킷에 대한 무결성을 보장 하여야 한다. 이렇게 법정 증거 자료로써 효력을 가지고 있는 증거들은 정부 기관의 네트워크 범죄에 대한 수사의 목적이나 기업의 네트워크 사고에 대한 법정 분쟁에서 효과적인 증거를 제시 할 수 있다. 또한 이러한 증거들을 그래픽으로 표현하여 네트워크 전체적인 상황에 대한 이해를 돕고 분석가들의 정확한 판단의 자료로써 사용되며 분석된 결과를 상황에 맞는 보고서를 통하여 신속성과 연개 보관성의 원칙을 보장 할 수 있어야 한다. 본 논문에서는 네트워크 관제를 통하여 네트워크 패킷에 대한 분석을 수행하는 네트워크 포렌식을 위한 방안을 고려하였다.

참고문헌

[1] 김민택 등, '다중 엔트로피를 이용한 네트워크 공격 탐지', 정보 보호 학회지 16_1, 2월, 2006.

[2] 이형우등, '컴퓨터 포렌식스 기술', 정보 보호 학회지 12_5, 10월, 2002.

[3] 장범환 등, '보안 이벤트 시각화를 이용한 보안 상황 인지 기술', 정보 보호 학회지 16_2, 4월, 2006.

[4] mark E. Russinovich and David A. Solomon, 'Microsoft Windows Internals, Fourth Edition', Microsoft Press, pp.200-211, 2004.

[5] 백승조등, '국가 디지털 포렌식 법률 체계와 국내외 디지털 포렌식 법제 현황', 정보 보호 학회지 18_1, 2월, 2008.

[6] 박상락, '공무원 정보보호 인터넷과 컴퓨터 수사', 정보 통신 교육원, 2002.

[7] 김종섭, '디지털 증거의 신뢰성 보증모델', 경기대학교 대학원 박사학위 논문, pp83-84, 2003.

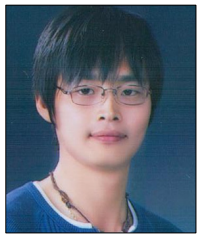
[8] 이규완등, '유비쿼터스환경에서 디지털 증거의 무결성 입증방안', 숭실대학교 정보과학대학원, 2006.

[9] 경찰청, '디지털 증거 처리 표준가이드라인', 12월, 2006.

[10] 전상덕, '디지털 포렌식의 기술 동향과 전망', 정보 통신 정책 제 13권 제 4호 pp. 3-19, 2006.

[11] 황현옥 등, '컴퓨터 포렌식스: 시스템 포렌식스 동향과 기술', 정보 보호 학회지 13_4, 8월, 2003.

노 시 영(Si-young No) **[정회원]**



- 2007년 2월 : 군산대학교 컴퓨터과학과 졸업(학사)
- 2010년 2월 : 군산대학교 컴퓨터공학과 졸업(석사)

<관심분야>
디지털 포렌식, 정보보안, 시스템 보안, 네트워크보안

박 상 준(Sang Joon Park) **[정회원]**

- 1998년 2월 : 숭실대학교 컴퓨터학과 석사
- 2002년 2월 : 숭실대학교 컴퓨터학과 박사
- 2002년 3월 ~ 2003년 2월 : 런던대 ISG 박사후 과정
- 2004년 3월 ~ 2007년 2월 : 숭실대학교 정보미디어기술연구소 연구교수
- 2007년 3월 ~ 현재 : 국립군산대학교 컴퓨터정보공학과 전임강사

<관심분야>
B3G, 센서 네트워크, 인터넷 망 분석, 디지털포렌식

이 종 찬(Jong Chan Lee) **[정회원]**

- 1996년 2월 : 숭실대학교 대학원 전자계산학과 석사
- 2000년 2월 : 숭실대학교 대학원 컴퓨터과학과 박사
- 2000년 ~ 2005년 ETRI 선임연구원
- 2005년 3월 ~ 현재 : 국립군산대학교 컴퓨터정보공학과 조교수

<관심분야>
이동통신, 센서 네트워크, 디지털포렌식

신 성 윤(Seong Yoon Sin) **[정회원]**

- 2003년 2월 : 군산대학교 컴퓨터과학과 이학박사
- 2006년 3월 ~ 현재 : 군산대학교 컴퓨터정보공학과 교수

<관심분야>
비디오 인덱싱, 비디오 요약, 멀티미디어, 색채공학

이 기 성(Gi-Sung Lee) **[종신회원]**

- 1993년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

<관심분야>
이동통신, 멀티미디어 통신, 네트워크 보안, 정보 검색, 모바일통신