韓國 컴퓨터情報學會 論文誌
第13卷 第2號, 2008. 3.

2008-13-2-2-3

UCC와 관련된 인터넷 범죄에 대한 네트워크 포렌식 연구

이 규 안*, 박 대 우**, 신 용 태***

A Study of Network Forensics related to Internet Criminal at UCC

Gyu-an Lee *, Dea-Woo Park **, Young-Tae Shin ***

요 약

인터넷 이용자의 74%가 UCC를 이용하고 있고, You Tube를 이용한 총기범죄가 발생하였다. 인터넷 범죄는 온라인에서 비대면성, 익명성, 은닉성으로 발생되고 있다. 본 논문에서는, 인터넷 UCC속에 나타난 인터넷 범죄의 양태를 분석하고 추적하는 네트워크 포렌식 방법과 기법을 연구한다. 인터넷 UCC의 범죄와 관련된 경찰과 검찰의 UCC 검색 방법 연구와 저장방법을 이용한 UCC의 증거 자료 수집 및 네트워크 포렌식을 통한 ID, IP 역추적과 위치 추적을 연구한다. 증거자료는 암호화하여 저장하며 접근제어와 사용자 인증을 통한 전송 및 저장 후에 무결성 검증을 통해 법정의 증거자료로 채택되도록 연구한다. 본 연구를 통해 인터넷 범죄 모의와 발생 등을 사전에 차단할 수 있도록 추진하고, 수사기관의 인터넷 범죄에 대한 포렌식 연구 발전에 기여하게 될 것이다.

Abstract

74 % of Internet users use the UCC, and You Tube using firearms in a crime occurred. Internet crime occurred in the online, non-face transaction, anonymous, encapsulation. In this paper, we are studied a Network Forensic Way and a technique analyze an aspect criminal the Internet having appeared at Internet UCC, and to chase. Study ID, IP back-tracking and position chase through corroborative facts collections of the UCC which used UCC search way study of the police and a public prosecutor and storage way and network forensic related to crimes of Internet UCC. Proof data encrypt, and store, and study through approach control and user authentication so that they are adopted to legal proof data through integrity verification after transmission and storages. This research via the Internet and criminal conspiracy to block the advance promotion, and for the criminal investigative agencies of the Internet will contribute to the advancement forensics research.

▸ Keyword : integrity verification, internet criminal, network forensics, UCC

• 제1저자 : 이규안 교신저자 : 박대우
• 접수일 : 2008. 2. 25, 심사일 : 2008. 2. 29, 심사완료일 : 2008. 3. 8.
* 숭실대학교 대학원 컴퓨터학과 **호서대학교 벤처전문대학원
***숭실대학교 컴퓨터학부

Ⅰ. 서 론

인터넷 기술과 초고속 네트워크의 발달로 인하여, 대한민국의 인터넷 사용 인구는 3,301만 명으로 ITU기준 세계에서 6위를 차지하고 있고, 지구 전체의 인터넷 사용 인구도 2005년 말을 기준으로 9.8억 명을 넘어서게 되었다[1].

인터넷의 정보 전달 방식도 텍스트를 이용한 전자 우편에서, 동영상과 멀티미디어 데이터를 전송하는 방식으로 변화되어 가고 있다. 최근의 웹에서의 초고속 인터넷 정보 전달 방식은 개인의 취미, 여가의 활동 및 동영상 촬영의 편리의 보편화로 UCC가 급격하게 성장하고 있다. 이러한 동영상 UCC의 급속한 확산은 인터넷 웹 서비스 업계의 전략이기도 하지만, 인터넷 컨텐츠 유통의 다양화와 제작 기법의 편의성, 웹2.0의 등장 등과 함께 사용자의 성향이 웹서비스에 대한 일방향성의 의견게시(댓글달기)에서 벗어나 자기만의 독창성을 가지고 서비스에 적극적인 참여로 변화되었고, 다양한 분야에 대한 자기만족, 홍보, 생생한 동영상 정보의 공유 성격이 짙게 나타나고 있다[2].

인터넷 범죄의 수사에서는 디지털 정보 안에서 발생하는 범죄에 대한 증거를 수집하고, 분석하여 법정에 제출하는 포렌식(Forensics)을 수행하며, 그중에서 네트워크를 이용하거나 네트워크에서 발생한 범죄에 대한 디지털 자료를 추출하는 증거를 수집하는 네트워크 포렌식과 이동단말이나 이동기기인 차량, 선박, 비행기, 기차 및 이동단말기를 사용하는 모바일 포렌식을 수행한다. 현대와 미래의 범죄에서는 이동기기와 이동단말의 발달로 인하여 UCC는 모바일과 연합하여 범죄에서의 이용이 더욱 증가할 것이다[3].

인터넷을 통해 범죄에 대한 죄의식이 없이 범죄의 사전 예고 또는 범죄의 진행을 인터넷에 게시하고 있으며, 이 결과 인터넷 UCC를 통한 범죄 예고와 범죄 발생은 인터넷을 통한 온라인에서 비대면성, 익명성, 은닉성으로 이루어지고 있다. 그리고 인터넷 네트워크에서 발생하는 범죄의 모의 또는 예고 및 범죄의 실행은 특정한 그룹에게만 공개되거나 전송되는 특징이 있으므로, 수사기관에서 미리 검색하거나 ID나 IP 역추적을 통한 수사 증거를 수집하는 데는 많은 어려움이 있다. 또한 이 증거자료를 법정의 증거자료로 채택하게 하고, 책임을 판단하는 증거로 사용하기 위해서는 암호화된 저장과 무결성에 대한 검증이 필요하다[4].

본 논문에서는 이러한 문제점을 해결하기 위해 네트워크 포렌식 자료의 추출과 검색, ID, IP 역추적 연구를 통한 인터넷 범죄 수사에 활용하기 위한 증거수집 방법을 연구한다. 또한 인터넷을 통해 전 세계에 흩어져 범죄에 대한 모의 과정에서부터 위치를 추적하고, 디지털 증거를 수집하여 수사를 진행한 다음 범정에 제출되어 증거로 채택되는 일련의 연계방안과, 이를 현실적인 범죄 수사와 재판의 실무과정에 연계하는 과정을 연구한다.

본 논문의 II. 관련 연구에서 UCC와 인터넷 범죄 폐해 및 네트워크 포렌식을 연구하고, Ⅲ. UCC의 범죄 검색 및 증거수집 연구, Ⅳ. 범죄 관련 UCC의 연계 수사와 네트워크 포렌식 자료 수집 및 검증을 통한 디지털 증거의 암호화와 무결성을 입증함으로써 컴퓨터 범죄에 대한 명확한 증거를 확보하고, 증거자료의 공정성을 유지하여 인터넷 범죄 모의와 발생 등을 사전에 차단할 수 있도록 추진하고, 수사기관의 인터넷 범죄에 대한 포렌식 연구 발전에 기여하게 될 것이다.

II. 관련 연구

인터넷과 컴퓨터를 이용한 인터넷 범죄에 대한 수사와 재판을 위해 증거를 수집하는 일련의 과정들을 포렌식이라고 하고, 포렌식은 학자에 따라, 디스크 포렌식, 네트워크 포렌식, 데이터베이스 포렌식, 모바일 포렌식 등으로 구분한다[4].

현재 네트워크 포렌식은 관련 연구를 매우 활발하게 진행되고 있으며 인터넷에서 UCC를 통한 인터넷 UCC의 이용실태와 전 세계에서 범죄에 이용되거나 범죄예고를 한 사례를 것을 살펴보고 범죄의 폐해 및 증거수집과 관련하여 무결성을 보장하는 수사 연계방안인 네트워크 포렌식의 분야 및 유형을 연구한다.

2.1. UCC 이용 현황

2.1.1. UCC이용 현황

한국인터넷진흥원의 2007년 5월 UCC이용실태조사에 의하면 대한민국 인터넷이용자의 74.0%가 UCC를 이용하고 있는 것으로 나타났으며, UCC 이용자라 함은 다른 사람이 작성·제작한 UCC보거나 이용한 경험이 월1회 이상자를 말한다. UCC이용자들은 주 평균 4.7시간을 이용하며, 주로 동영상과 사진, 애니메이션, 플래시 등의 순서로 보는 것으로 나타났다. 무엇보다 UCC를 이용하는 경로로 포털사이트의 UCC전용 게시판이 77.0%로 가장 많고 블로그, 미니홈피가 71.1%를 사용하는 점으로 미루어 거의 모든 UCC 자료들에 대한 검색과 조사를 위한 대상으로는 포털사이트와 블로그, 미니홈피를 제공하는 업체를 통한 제재가 가능하다고 할 수 있다[5].

2.1.2. UCC 동영상 서비스 제공

가) 다음

2007년 3월에 UCC동영상 서비스를 TV팟으로 통합하여 운영하기 시작하였으며, 전문가들이 제작한 동영상 지식 UCC인 "노하우팟", 개인 방송서비스인 "라이브팟", 영화, 애니메이션, 스포츠, 게임 등 컨텐츠를 무료로 상영하는 "비이소팟"으로 구분하여 운영하고 있다.

나) 네이버

2007년 5월 동영상 UCC서비스인 "플레이"를 오픈하여 제공하였으며, 현재는 "네이버 비디오"로 명칭을 바꾸어 동영상 플랫폼에 대한 지원을 강화하고 있다. 특징으로는 장면검색 등 동영상 검색기능이 뛰어나다.

다) 판도라TV

UCC 배너 및 동영상광고를 통해 수익을 창출하고 수익일부를 UCC 저작자에게 큐피로 지급하고 있다. 2006년 7월 미국으로부터 60억원의 투자를 받고, 2007년 4월 미국 벤처캐피털 DCM으로부터 1천만달러의 투자를 받아 UCC를 상용화하고 있다.

라) SM온라인

2006년 12월 SM엔터테이먼트의 계열사로 편입되어 SM 엔터테이먼트 소속 연예인 관련 컨텐츠와 UCC를 결합한 엔터테이먼트 컨텐츠 플랫폼을 지원하고 있다[6].

2.2. UCC의 폐해 및 문제

2.2.1. 저작권 문제

UCC가 게시되는 동영상이나 사진, 글 중에서 정작 본인의 생산물은 10% 미만이다. 대부분은 저작권이 있는 내용을 불법 또는 무단으로 복사해서 올린 것이다. 결국 타인의 저작물로 광고 수익을 챙기는 문제가 발생하고 있어, 제작한 저작권자의 의욕을 상실케 하거나 저작권자의 의도와 다른 결과를 초래함으로 법적인 문제를 야기한다.

2.2.2. 불건전한 불법 내용

음란물을 비롯해 욕설, 엽기 소재, 제목과 내용이 일치하지 않는 낚시성 내용들은 물론, 인터넷 상에서 범죄를 모의하고, 예고하고, 실행하는 경우가 있다. 핀란드 투술라 고등학교에서 발생한 고등학생 총기사고와 미국의 버지니아공대에 총기난사사건 등의 경우에는 자신의 범죄를 예고하여 충격을 주었다.

2.2.3. 초상권, 사생활 침해

디지털카메라와 동영상 촬영용 카메라 폰의 상용화로 일반적인 휴대폰과 카메라 폰을 이용하여 일반 사람을 감시하고 촬영하여 인터넷에 UCC을 올릴 수 있는 시대가 되었다. 이 결과로 심각한 인권 침해 사례가 계속 발생할 수 있어, 파파라치에 의한 영국 왕세자비의 죽음 등과 유명 연예인의 사생활 침해로 정신병원에 입원하고, 구속되는 사생활 침해와 개인정보의 노출이 범죄에 악용 사례는 갈수록 늘어가고 있다.

2.2.4. 잘못된 문화 형성

UCC의 편리성을 역이용하여 청소년들이 집단 성폭행, 집단구타, 따돌림, 살해사건 등으로 이어지는 인명경시 풍조가 일어나고 있다. 절도나 강도 후에 신고를 못하는 협박의 수단으로 성폭행 후 촬영하거나 집단 폭행 등의 UCC를 인터넷에 게시하여 불법적인 행위가 예술의 일부인 것처럼 잘못 생각하는 문화가 확산되고 있다.

2.3. UCC와 인터넷 범죄와 관련 현황

2.3.1. 음란물, 퇴폐물

UCC를 이용하여 유명 연예인의 성행위를 노출시키거나, 일부분을 모자이크 처리한 후 그림 1처럼 키스알바, 애인 대행 등의 내용을 달고 게시판에 업로드하여 자신을 성 상품화하거나 불법 성매매의 자료로 활용하는 일이 발생하고 있다.

그림 1. 판도라 TV에서 퇴폐물 검색화면
Fig. 1. Search for decadents screens at PanDoRa TV

2.3.2. 악성코드

2007년 초부터 UCC를 보고 나서 컴퓨터가 오동작을 일으키고 동작을 멈추게 하거나, UCC를 이용한 스파이웨어의 삽입으로 개인 컴퓨터의 정보를 불법적으로 유출하여 경제 범죄에 이용되었다. 또한 UCC를 보기위한 플레이어를 다운받게 되는 경우 중요한 자료를 숨김 폴더에 암호화하여 저장이 된 다음에 그 파일을 되찾기 위해서는 인증을 받게 하고 인증

수수료를 요구하는 불법적인 랜섬웨어가 확산되는 사례가 발생하였다[7].

2.3.3. 범죄에 대한 예보 및 범죄 실행

2007년 4월 16일 버지니아공대에서 미국 역사상 최악의 총기난사 범죄사건이 발생하였는데 위 사건의 범인인 조XX는 사건 전에 자신의 총격행위를 예고하는 동영상을 게시하였으며, 폴란드의 투술라 고등학교 총기난사 사건 범인도 자신의 범행에 대한 예고 동영상을 '요켈라 고교 학살-11/7/2007'이라는 You Tube를 통하여 인터넷 UCC에 게시하였다.

그림 2. 고등학생 총기난사 예고 UCC
Fig. 2. Notice UCC. of a high school student firing a gun

2.3.4. 스팸전송

UCC에서 게시된 저작물들은 링크기능을 통하여 메일주소를 수집한 후 스팸메일을 전송하거나 피싱(Phishing)[8] 기능을 이용하여 주소를 메일에 링크하여 불법적인 스팸 전송하는 수법으로 광고 또는 음란물을 전송한다.

2.3.5. 명예훼손, 비방, 전파

대선기간을 통하여 많은 UCC홍보물이 포탈사이트에 게시되고 중앙선거관리위원회는 UCC 제작물이 선거법에 위반되는지 여부를 확인 하였다. 경찰 및 검찰의 수사기관에서도사이버 상에서 발생하는 선거법위반 행위를 검색하였다. 국제적인 테러리스트들도 이념을 전파하기 위한 저작물로 UCC를 이용하고 있다. 알카에다의 자살폭탄 테러리스트가 신의 계시임을 천명한 후 자살폭탄을 하는 장면이 You Tube에 게시되기도 하였고, 미국 병사를 저격하는 장면이 게시되는 등 이념을 전파하고 공포를 심어주었다[9].

2.4. 네트워크 포렌식

네트워크 포렌식은 네트워크를 통하여 전송되는 데이터나 패스워드 등 데이터 트래픽을 분석하거나, 접근·에러 로그, 네트워크 환경 등을 조사하여 인터넷 범죄의 수사단서를 찾아내는 분야이다. 네트워크 포렌식은 인터넷을 통하여 서비스되는 월드 와이드 웹, ftp, Usenet 등 인터넷 응용 프로토콜에서 증거를 수집하고 분석한다. 인터넷상에서 불법행위를 한 해커와 같은 용의자의 DDoS(Distributed DoS) 공격이나 Worm공격[10]을 추적하기 위한 웹 히스토리(WWW history)분석, 전자우편 헤더분석, 전자우편 수신자 추적(E-Mail Tracking), WHOIS 검색 및 IP 추적 등이 네트워크 포렌식의 주요 내용이 된다.

이는 게시판에 불법정보를 업로드 하거나, 명예 훼손성 글을 올린 용의자추적, 전자메일 발신자 및 수신자 확인, 인터넷 서핑 내용 추적을 위하여 인터넷 로그기록, 히스토리, 다운로드 받은 파일이나 문서를 분석하는 작업이 필요하다.

2.5. 네트워크 포렌식 절차

2.5.1. 증거확보

디지털 저장장치에 저장된 정보의 유형과 형태를 확인하는 확인단계로, 증거자료 확보가 관건이다. 네트워크를 통하여 데이터가 전송되는 과정에서 생성되는 자동 로그 기록을 분석하거나 Sniffer와 같은 프로그램을 사용하여 트래픽 데이터를 직접적으로 가로채는 방법을 증거를 획득할 수 있다. 대부분의 네트워크는 사용자의 행위를 감시하고 추적하기 위한 장치를 가지고 있다.

2.5.2 증거입증

보존단계로서 디지털로 저장된 자료를 확인 한 후, 변경되지 않도록 암호화하거나 무결성을 보존하는 단계이다. 자료뿐만 아니라 자료를 읽을 수 있는 기기의 변경도 포함하여 변경이 될 경우에는 법적 절차에 따라 변경된 원인을 설명해야 한다.

2.5.3. 증거분석

네트워크 포렌식 자료를 추출, 처리, 판단하는 단계로 분석용 도구를 이용하여 디지털자료를 분석[11]하는 단계이다. 자료 분석 시에는 검사대장 자료가 변경되지 않도록 포렌식 증거 분석 절차를 준수하여야 한다.

2.5.4. 증거제출

마지막 단계로서 법정제출을 의미한다. 법정에서 진술방법, 발표자의 전문적인 기술과 위의 세 가지 단계가 지켜진

법적 증거자료로서, 신뢰성 있게 서술될 수 있도록 체계적으로 준비하는 것을 의미한다.

III. UCC의 범죄 검색 및 증거수집 연구

범죄와 관련한 UCC 검색은 보통 사용자의 요청이니 신고에 의하게 된다. 강력 범죄, 상호비방, 흑색선전, 명예훼손 등과 관련한 인터넷 범죄에 대한 정보를 수집하여 분석을 실시하게 되는데, 통합 및 컨텐츠별로 검색을 할 수 있는 포털서비스의 기능을 이용한다.

3.1. UCC 범죄 검색 기법

UCC의 범죄 검색은 통상적으로 디렉토리 검색, 키워드검색, 메타검색기법을 사용한다. 디렉토리 검색은 탑다운 방식으로 숭실대학교를 검색할 경우 "교육기관→대학→숭실대학교"의 순서로 검색의 범위를 좁혀가지만 실제 사용하기에는 어려움이 있고, 보통 키워드 검색을 주로 사용한다. 현재는 포탈사이트마다 키워드 검색을 이용하여 메타검색을 지원하고 있다. 즉 범죄 수사에 필요한 용어를 키워드를 사용하여 검색하면 어느 사이트에 있는 정보의 정확도가 몇%의 확률정도로 정확하다고 제공하는 방식이다. 이러한 방식은 empas. *google* 등 거의 모든 업체에서 제공한다.

아울러 UCC 동영상을 지원하는 업체별로 사회윤리나 범죄에 대한 내용의 동영상을 검색하여 이용을 제한하기도 하는데 그 기법은 다음과 같다.

3.1.1. 수사기관의 UCC 검색 기법

경찰과 검찰에서는 보다 광범위한 모니터링을 하게 된다. 모니터링 요원에 대한 인원과 방법을 특정하기는 기관마다 수사 환경이 상이하지만 시기와 상황에 따라 특정용어, 금칙어에 대한 집중적인 검색을 실시하게 된다.

선거기간동안에는 "대선"이라는 용어를 모니터링 툴에서 수시로 검색토록 하여 위법성 여부를 검토한 후 선거관리위원회와 협의하여 수사를 개시해야 된다면 수사보고서를 작성하여 수사를 시작하게 된다.

검찰청의 경우 대검찰청과 지방검찰청에 모니터링 요원이 별도로 존재하고 다른 산하 검찰청의 경우에는 컴퓨터수사요원이 모니터링을 겸하여 업무에 임하고 있다.

경찰청의 경우 경찰청 수사부 산하의 사이버테러대응센터가, 산하경찰청의 사이버범죄수사대에서 모니터링을 실시하고 있으며, 산하 경찰서마다 사이버수사반이 조직되어 수사팀원이 근무하고 있다.

3.1.2. 판도라 TV 검색 기법

판도라 TV는 게시물 등을 자체 검색과 모니터링을 통하여 사회윤리나 범죄에 대한 내용의 상시 감시체제를 운영하고 있으며, 특정한 용어가 사용되는 게시물에 대하여 자체 규정으로 판단이 어려울 경우에 관계기관에 문의를 하는 형식을 취하고 있다. 심의 또는 관계 기관으로부터 회신 결과 게재에 불가하다는 판단을 하게 되면, 삭제를 요청하게 되고 이에 불응하게 되면 검색되지 않도록 조치하거나 결과가 보이지 않게 처리를 한다.

모니터링 요원은 국내담당이 30명 내외, 중국과 아시아를 담당하는 직원이 20명 내외로 구성하여 24시간 3교대 모니터링을 하고 있다. 1차로 새로운 게시물에 대한 모니터링을 시도하고, 2차로 금칙어, 미풍양속에 저해되는 음란물, 저작물 키워드를 이용하여 검색을 실시하게 된다. 3차로 모니터링 툴을 이용하여 제목과 설명문에 있는 키워드를 이용하여 검색하게 된다.

3.1.3. 네이버 등 포탈업체의 검색 기법

네이버 등 포탈업체의 경우에는 UCC 동영상 만을 특정하여 검색하지는 않지만, 180여명으로 구성된 모니터 요원들이 3교대로 랜덤하게 게시물에 대한 모든 검색을 실시하고, 모니터링 툴을 이용하여 특정한 용어, 금칙어 들을 대상으로 검색을 실시한 후, 심의를 거쳐 게시불가 판정이 내리게 되면 게시자에게 삭제요청하고 범죄내용은 수사기관에 신고하게 된다.

최근 세종대학교 컴퓨터공학과에서 개발한 UCC검색 시스템에 의하면 그림 3과 같이 살색이 많이 나오는 동영상을 검색하여 야동(야한 동영상)으로 판독하는 시스템이다. 이 프로그램은 야동의 경우 전체 화면에서 살색을 표시하는 %가 많이 나타나는 경우를 표본으로 하여 검색하는 기법이다[12].

그림 3. UCC 야동 판독 시스템
Fig. 3. An UCC indecency decoding system.

3.2. UCC 범죄에 대한 증거수집

인터넷 범죄 수사 기관에서는 UCC 동영상의 경우에는 일반 동영상의 저장방법을 이용하여 저장한 후에 포렌식 증거로 채증하게 된다.

이를 위한 저장프로그램은 그림 4의 Camtasia, VOD Recorder, Net Transport, Hinet Recorder, Capture Solution 등이 있다.

Camtasia의 경우 화면에서 진행되는 동작이 모두 캡처되고 저장되므로 증거를 수집하는 채증하기에 적합한 프로그램으로 사용한다.

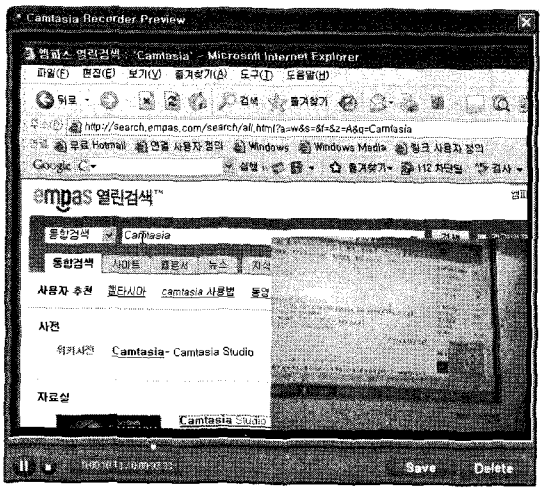

그림 4. Camiasia을 이용한 증거수집
Fig. 4. The proof collection which used Camiasia

3.3. 증거 수집 자료의 무결성 입증

검색 후에 인터넷 범죄와 관련하여 수집된 증거자료가 사건당시의 일시에 수집되었으며, 훼손되지 않았음을 입증할 수 있도록 주의를 하여야 한다.

이러한 사실을 입증하기 위하여 디지털 포렌식의 절차에 의하여 진행하여야 하고, 수집된 일시를 확인할 수 있도록 MAC를 지원할 수 있는 방안을 강구해야 한다. 보통 휴대폰의 시간 기능을 캡처하는 도중 삽입하기도 하고 GMT를 지원하는 프로그램이 설치된 컴퓨터에서 증거를 수집 한다. 수집된 동영상 자료는 수사 관계인의 입회하여 확인을 받은 후 CD/DVD에 저장하고 서명날인을 받는다.

IV. 범죄 관련 UCC의 연계 수사와 네트워크 포렌식 자료 수집 및 검증

4.1. 네트워크 포렌식의 연계 수사 방법

4.1.1. 사건 접수와 증거 확보 및 ID, IP 역추적

범죄 관련 UCC의 네트워크 포렌식의 절차는 사건접수, 혹은 모니터링을 통한 범죄행위를 발견하는데서 수사가 시작되어, 로그 및 증거자료를 확보하게 된다. 이때 UCC 동영상과 같은 자료는 위에서 언급한 캡처 프로그램을 이용하여 저장하고 로그분석을 통하여 범죄자를 추적하게 된다.

네트워크의 관문 역할을 하는 라우터에는 routing table, arp cache table, login해 있는 사용자, TCP connection과 관련된 정보, NAT translation과 관련된 정보가 존재하기 때문에 침해시스템을 조사할 때 라우터의 분석을 실시한다.

인터넷 컴퓨터 통신을 이용하여 정보를 송수신하기 위해서 사용하는 프로토콜로서 고정 IP와 유동 IP로 구분할 수 있으며, 초고속네트워크에서는 거의 유동 IP를 사용하고 있다. 범죄자의 ID와 IP를 추적하여 확인한 후, 동일한 IP와 ID를 이용하여 다른 사이트에 접속 또는 자료를 업로드여부 등을 심도 있게 검색하여 자료를 취합한다. ID와 IP를 UCC 관련기관들에게 수사 협조 공문을 보내고, 협조를 의뢰하여 범죄자의 실명과 운영이 되고 있는 위치 등을 파악한 후 법원의 압수수색영장에 의하여 인터넷 범죄의 추가 자료와 수사에 필요한 범죄 증거를 압수하게 된다.

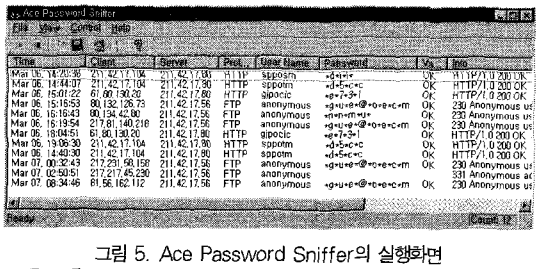

그림 5. Ace Password Sniffer의 실행화면
Fig. 5. An execution screen of Ace Password Sniffer

그림 5는 인터넷 범죄 수사에 Sniffer 프로그램을 이용하여 인터넷 사용자의 패스워드를 획득하는 과정을 보여주고 있다.

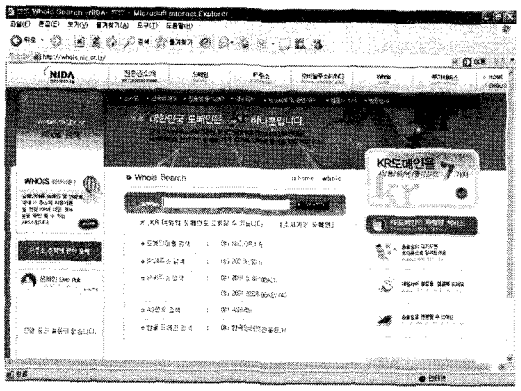

그림 6. WHOIS 조회 서비스
Fig. 6. WHOIS inquiry service

ID와 IP를 역추적하는 인터넷 범죄의 수사에 있어서 초고속 인터넷 서비스를 제공하는 업체와의 협조는 필수적이다. 그림 6은 WHOIS을 이용한 조회 서비스이다.

4.1.2. 범죄 관련 UCC 피의자 위치추적

범죄 혐의가 있는 UCC 자료의 게시 사이트에 대한 게시자의 정보가 없는 경우와 국내의 사이트가 아니라고 판단되는 경우에는 인터넷을 통하여 특정 사이트에 대한 루트를 추적하는 것이 필요하게 되고 이때 사용할 수 있는 유틸리티로서 Tracert 프로그램이 있다. 이 유틸리티는 인터넷상에 혐의가 있는 네트워크를 추적하고 경로를 파악하는 게이트웨이 경로를 GUI 방식으로 지원해 준다.

이러한 프로그램을 통해 범죄 관련 UCC 피의자의 위치가 추적되면 압수수색 영장을 발부 받거나, 형사대를 급파하여 범인을 체포한다.

4.2. 네트워크 포렌식 자료의 수집 및 검증

4.2.1. 네트워크 포렌식 자료의 수집

인터넷 네트워크에서 UCC를 이용한 관련 범죄에 대한 중요한 정보자료를 획득 및 게시하기 위해서 자료 파일에 대한 로그인을 하여야 한다. 따라서 인터넷 범죄관련 수사할 때, 수사요원들은 네트워크 포렌식에서 로그기록을 최우선적으로 확보하여야 한다.

UCC 관련 범죄자가 자료 등을 게시, 이용하기 위한 네트워크 접속 세션동안 다양한 응용 프로세스를 실행하는 네트워크상의 사용자의 로그인, 로그아웃 정보와 명령어 실행 정보 등의 자료를 네트워크 포렌식을 위한 보안 감사 자료로 실시간 백업하고, 이 보안 감사 자료를 이용하여 침입자에 대한 ID, IP 역추적과 수사 자료 수집을 수행한다.

또한 네트워크 운영시스템은 네트워크에서 단절하고 격리시켜서 포렌식 자료를 수집해야 한다. 또한 시스템의 전원을 끄고 시스템에 장착된 저장장치의 저장내용들을 분석시스템에 슬래이브로 부착하여 자료를 분석[4]하여야한다. 인터넷 멀티미디어 매체를 통한 범죄 관련 UCC에 대한 네트워크 포렌식 자료는 웹 브라우저에서 정보를 수집하는데, 이때 일부 전송 중인 UCC 데이터는 암호화된 파일이 있으므로 암호화를 해독하는 기술이 필요하다.

또한 UCC 동영상의 파일을 통해 범죄를 일으킨 후에 추적을 피하기 위해 다른 파일의 일부로 변형하거나 다른 자료로 갑옷처럼 숨겨져 있을 수 있기 때문에 이를 확인하기 위한 포렌식 기술이 필요하다. 또한 범죄에 이용된 증거자료를 감추기 위해 파일을 삭제하는데, 삭제된 파일을 복구하여 원래의 자료를 추출하기 위한 포렌식 과정들이 필요하다.

네트워크 포렌식의 경우 인터넷 범죄가 발생할 수 있는 예방 방법으로부터 인터넷 범죄가 발생하여 인지하고 피해가 발생한 후로부터 범죄 수사에서 증거 수집 및 포렌식 자료를 수집하여 법정에 증거자료로 제출되기 까지 연계 방법이 표준화되고 통일되어야 한다. 특히 네트워크 포렌식 자료를 확보하기 위해서는 사건에 대한 일련의 과정들이 모두 수사 자료와 포렌식 자료로 기록되고 정리되어야 하며, 특이한 사항은 비고란에 기재함으로써 법정에서 포렌식 증거의 연계성이 훼손되지 않아야 한다.

UCC 관련 증거를 수집하고 목록을 작성한 다음 분석결과와 함께 수집된 증거들은 해시 함수를 이용하여 압축하거나, PDF파일로 변환하여 저장하여야한다. 이는 PDF파일의 속성상 위변조의 가능성이 줄어들기 때문이다.

4.2.2. 네트워크 포렌식 자료의 무결성 검증

인터넷 네트워크에서 UCC를 통한 범죄에 이용된 자료들은 암호화와 접근제어 및 사용자 인증을 통한 수사자료 보안조치를 하여 자료의 훼손과 위변조하지 못하도록 하여야 한다.

수집된 자료에 대한 접근 시에도 로그 파일에 대한 보안을 실시하고 자료 전송 시에도 공인인증에 의해 암호화하여 전송하여야 하며 수사기관에 연결된 DB에 암호화된 상태로 저장한다. 수사본부의 DB파일에 대한 접근 시에도 반드시 접근제어와 쓰기금지를 실시하여야한다. 이러한 과정과 절차들은 현재 개인의 경험과 상황에 따라 진행되므로 네트워크 침해사고 분석규정 등을 통하여 통일된 지침을 만들고 지침에 충실하게 진행하면서 상황에 따라 예외적인 상황이 발생할 경우에는 사진, 동영상, 장부에 기재하는 방법 등을 통하여 디지털 증거의 무결성을 법정에 입증하여야 한다.

V. 결론

UCC의 확산은 세계적인 추세이지만 인터넷 범죄를 수사를 하는 현장에서는 자국마다 상이한 법적용과 네트워크 환경에 따라 다르게 해석되는 적용되는 어려움이 있다.

본 논문에서는, 인터넷 UCC속에 나타난 인터넷 범죄의 양태를 분석하고 인터넷 범죄에서 UCC와 관련한 불법과 범죄에 이용되는 문제점 및 폐해상황을 살펴보고, 인터넷 UCC의 범죄와 관련된 경찰과 검찰의 UCC 검색 방법 연구와 UCC의 증거 자료 수집 및 네트워크 포렌식을 통한 ID, IP 역추적과 위치 추적을 연구하였다. 증거자료는 암호화하여 저장하며 접근제어와 사용자 인증을 통한 전송 및 저장 후에 무결성 검증을 통해 법정의 증거자료로 채택되도록 연구하였다. 본 연구 결과를 통해 UCC의 확산과 건전한 생활을 위하여 범죄의 모의, 예고 등을 미연에 방지할 수 있도록 이여 할 것이며 네트워크 포렌식 연구 발전에 기여할 것이다.

향후 연구는, UCC의 국제적인 공조를 위한 법체계의 연구와 네트워크 포렌식의 각 분야에 대한 정의와 표준화된 지침, 그리고 새롭게 등장하는 신기술과 개념에 대한 포렌식의 절차 등에 관한 연구를 실무에 적용함으로써 발생하는 새로운 문제점들을 발굴 보완해야 할 것이다.

참고문헌

[1] 인터넷통계정보검색시스템. http://isis.nada.or.kr 2006. 10.

[2] 천홍말, 윤종수, "Web2.0과 UCC:진화경향과 전략적 시사점" 한국컴퓨터정보학회2007하계학술발표논문집, 제15권 제1호, 2007. 6.

[3] 오세근, "최근 UCC Trens와 진화, PCC" 주간기술동향, 2007. 2. 7.

[4] 이규안, 박대우, 신용태 "포렌식자료의 무결성 확보를 위한 수사현장의 연계관리방법연구". 한국컴퓨터정보학회논문지. 제11권 제6호, pp175-184. 2006. 11. 6.

[5] UCC이용실태조사. 한국인터넷진흥원, 2007. 5.

[6] 임순옥, "UCC의 국내외 동향", 정보통신정책 제19호 4권 411호. 2007. 3. 2

[7] 한겨레21. http://www.hani.co.kr. 2007. 11. 14.

[8] 박대우, 서정만. Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구. 한국컴퓨터정보학회논문지. 제12권 제2호, 2007. 5.

[9] 월간 말. "테러리스트들의 반미구호의 새통로" p220-221 2007. 3.

[10] 박대우, 서정만. TCP/IP 공격에 대한 보안 방법 연구. 한국컴퓨터정보학회논문지. 제10권 제5호, 2005. 11.

[11] Vigi Gurushanda, "e-evidence Stand" http://radio.weblogs.com/0117653/gems/ARMA2005eEvidenceStd.pdf. 2007. 12.

[12] 보안뉴스. http://www.boannews.com 2007. 4. 17.

저 자 소 개

이 규 안

2006년 숭실대학교 컴퓨터학과 재학 (박사과정)
2000년 벽성대학 정보통신과 겸임교수
2002년 대검찰청 중앙수사부 컴퓨터 수사과근무
2005년 대검찰청 디지털수사담당관실 모바일 분석 팀장
〈관심분야〉 유비쿼터스 보안, 컴퓨터 포렌식, 해상 디지털 포렌식

박 대 우

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과(공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원(KISA) 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
〈관심분야〉 정보보호, 유비쿼터스 네트워크 및 보안, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

신 용 태

1985년 한양대학교 산업공학과 학사
1990년 Univ.of Iowa 전산학과 석사
1994년 Univ.of Iowa 전산학과 박사
1994년 ~ 1995년 Michigan State Univ. 전산학과 객원교수
1995년 ~ 현재 숭실대학교 컴퓨터학부 교수
〈관심 분야〉 멀티캐스팅, 실시간통신, 이동통신, DRM 등