# 디지털 포렌식 관점의 P2P 네트워크 정보 수집 방안 연구[1)]

*성진원 *백은주 *변근덕 *이상진 *임종인

*고려대학교 정보보호기술연구센터

*jinwonsung@korea.ac.kr

# Evidence acquisition of P2P network for digital forensics

*Jinwon Sung *Eunju Baek *Keunduck Byun *Sangjin Lee *Jongin Lim

*Center for Information Security Technologies(CIST), Korea University, Korea

## 요약

컴퓨터 포렌식 수사에서 인터넷 사용에 대한 분석은 증거 획득에서 중요한 부분을 차지한다. 인터넷 사용 분석에는 웹브라우저 분석, 메신저 분석 그리고 Peer to Peer (P2P) 분석 등이 그 대상이 된다. 그 중 본 논문에서는 최근 중요성이 대두되고 있는 P2P를 분석함으로써 P2P에서 컴퓨터 포렌식 수사에 도움이 되는 정보에 대해 알아보고 분석 방법을 제시한다.

## 1. 서론

인터넷 기술 발전은 우리 생활에 많은 편리성과 신속성을 제공한다. 인터넷을 이용하여 쇼핑, 인터넷 뱅킹, 그리고 자료 검색 등 많은 일을 컴퓨터 앞에 앉아 편리하고 신속하게 해결함으로써 오늘날 인터넷은 생활에 없어서는 안 될 중요한 부분이 되었다.

그러나 이러한 인터넷의 편리성, 신속성 등 많은 장점들 이면에는 익명성이 제공된다는 점을 이용하여 인터넷이 불법적으로 사용되고 있다.

따라서 컴퓨터 포렌식 수사에서 용의자의 인터넷 사용에 대한 분석은 인터넷의 불법적인 사용에 대한 증거를 발견할 수 있는 중요한 부분을 차지한다.

이러한 인터넷 사용에 대한 분석에는 컴퓨터 사용자 대부분이 사용하고 있는 마이크로 소프트의 인터넷 익스플로어(Internet Explorer)와 점차 많은 사용자를 확보하고 있는 파이어폭스(FireFox)와 같은 웹브라우저를 분석하는 방법이 있다. 웹브라우저를 통하여 용의자가 인터넷을 사용할 경우 컴퓨터에 자동으로 생성되는 쿠키, 인터넷 히스토리, 즐겨찾기, 인터넷 캐시 파일등에 남겨진 파일 또는 로그들을 분석함으로써 용의자의 인터넷 사용 기록, 개인 성향 그리고 개인 정보와 같은 증거를 획득한다..

메신져 분석은 MSN과 IRC 등의 소프트웨어를 통한 대화 기록과 파일 전송 기록 등을 분석하여 메신져 사용시간, 대화 상대와 같은 증거를 획득한다.

또한 최근 P2P 사용률이 증가함에 따라 P2P를 이용한 불법 음란물, 저작권으로 보호되는 컨텐츠들을 저장하고 교환하는 불법적 활동들도 증가 하고 있어 P2P 분석도 요구된다.

따라서 본 논문에서는 현재 사용되고 있는 P2P에 대해서 알아보고, 컴퓨터 포렌식 수사에 있어 P2P 분석을 통해 획득할 수 있는 증거물이 무엇인지 분석하고 앞으로 컴퓨터 포렌식 수사에서의 P2P 분석 방법을 제시하고자 한다.

## 2. P2P 란?

P2P란[1], 불특정 다수의 개인 사이에 직접 정보를 교환하는 인터넷 이용형태 또는 그것을 가능하게 하는 어플리케이션 소프트웨어를 말한다.

P2P방식은 연결방식에 따라 Hybrid P2P방식(혼합형 P2P방식)과 Pure P2P(순수 P2P방식)으로 분류할 수 있다.

Hybrid P2P방식은 PC끼리 상호연락을 원활하게 해주는 서버가 개입되는 형태로 Napster가 이에 해당된다. 이 방식은 중앙 서버에 지나치게 많은 정보를 관리함으로 서버 운영상 재정적 부담이 큰 단점이 있다.

Pure P2P 방식은 유사한 성능을 가진 개인끼리만 연결된 형태로 중간 서버를 거치지 않는 고유한 의미의 P2P방식이라고 할 수 있다. Gnutella, Limewire 그리고 Bearshare등이 이에 해당된다.

이러한 P2P들의 등장으로 사람들은 다양한 정보를 다운로드 하거나 공유할 수 있게 되었다. 그러나 P2P가 익명성이 제공된다는 점을 이용하여 불법 포르노그라피 또는 저작권이 있는 컨텐츠들을 다운로드 하거나 공유하는 불법행위들이 회사 또는 일반생활 속에서 증가하게 되었다.

따라서 컴퓨터 포렌식 수사에서 P2P 분석의 중요 목표는 용의자가 다른 사람들과 불법적인 파일을 다운로드 했거나 또는 공유 했던 정보를 찾아내는 것이다.

1) 본 연구는 과학재단 디지털 정보 획득 기반기술 연구(M10640010005-06N4001-00500)의 지원으로 수행되었습니다.

## 3. P2P 클라이언트 소프트웨어 분석

3장에서는 현재 많이 사용되고 있는 P2P 클라이언트 소프트웨어를 통해 파일의 다운로드 정보와 공유 정보를 분석했다. 분석한 소프트웨어는 중간에 서버가 없이 개인들끼리만 연결된 P2P방식인 Gnutella 기반의 클라이언트 소프트웨어 중 Bearshare version5.2.4.3 (Bearshare)이다.[2]

### 3.1 P2P 분석 절차

컴퓨터 사용자들이 P2P를 이용하기 위해서는 P2P 클라이언트 소프트웨어가 있어야 한다. P2P 클라이언트 소프트웨어를 이용하여 사용자들은 파일들을 저장하고 공유하는 일련의 작업들을 하게 되는 것이다.

따라서 컴퓨터 포렌식 수사에서는 이러한 클라이언트 소프트웨어를 분석하여 용의자가 저장하고 공유한 파일들이 어떠한 것들이 있는지 정보를 획득할 수 있는 것이다.

아래는 P2P 클라이언트 소프트웨어를 컴퓨터에 설치 시 폴더경로, 레지스트리 경로를 알아보고 프로그램 설정변경 시 변경되는 설정파일을 알아보기 위한 일련의 절차[4]를 나타낸 것이다.

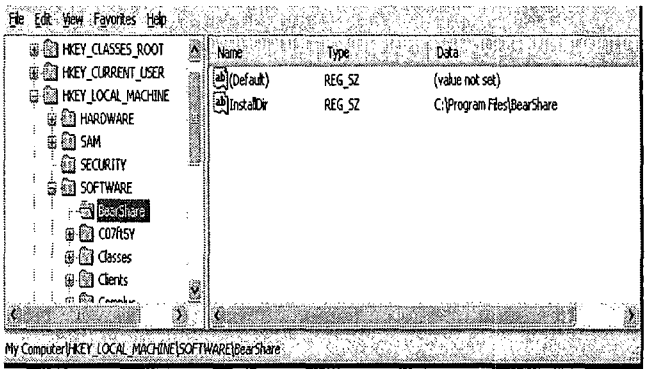
1. 분석을 위해 P2P 클라이언트 소프트웨어가 설치되어 있지 않은 초기설정 상태의 시스템을 구축한다.
2. 클라이언트 소프트웨어가 어떠한 파일들과 레지스트리와 관련되는지 확인하기 위해 Sysinternals사[5]의 Filemon과 Regmon을 설치하고 실행 시킨다.
3. P2P 클라이언트 소프트웨어을 설치한다.
4. 클라이언트 소프트웨어가 설치되면서 어떠한 디렉토리, 파일, 레지스트리가 어떠한 경로에 만들어지는지 Filemon과 Regmon을 이용하여 파악한다.
5. P2P 클라이언트 소프트웨어를 실행시켜 기본 옵션으로 저장되어 있는 다운로드 폴더와 공유 폴더의 경로와 이름을 확인한다.
6. 기본으로 저장되어 있는 경로와는 다른 경로에 폴더 두 개를 생성하여 기본 옵션으로 저장되어 있는 다운로드 폴더와 공유 폴더의 경로를 새로 생성한 폴더 경로로 변경한다.
7. 경로변경 확인 버튼이 눌려지면 어떠한 레지스트리와 파일들이 변경되는지 Filemon과 Regmon을 이용하여 확인한다.
8. 다운로드 폴더에 P2P 서비스를 이용하여 파일을 다운로드하고 공유폴더에 공유할 파일을 저장한다.
9. 파일을 다운로드하고 공유할 때 어떠한 설정파일들이 변경되는지 Filemon과 Regmon을 이용하여 확인한다.

이러한 일련의 과정들을 거쳐 사용자의 PC에서 P2P 클라이언트 소프트웨어의 다운로드 폴더와 공유폴더의 경로를 확인하고, 설정변경 시 Software가 접근하는 설정파일들을 확인하여 변경된 설정들이 저장되는 파일을 확인한다.

### 3.2 중요 설정 파일

Bearshare를 설치하면 기본으로 C:\Program Files\Bearshare 폴더에 프로그램이 설치된다. 그러나 설치경로는 사용자가 프로그램 설치 시 변경이 가능하여 용의자가 설치경로를 변경하였다면 설치경로를 찾아야 한다. 만약 기본으로 설정된 경로만 확인한다면 클라이언트 소프트웨어가 설치되지 않았다는 잘못된 판단을 하게 되는 오류를 범하게 된다. 설치경로에 대한 정보는 Sysinternals사의 Regmon으로 확인한 결과 레지스트리에 설치경로에 대한 정보가 저장되는 것을 확인할 수 있다.

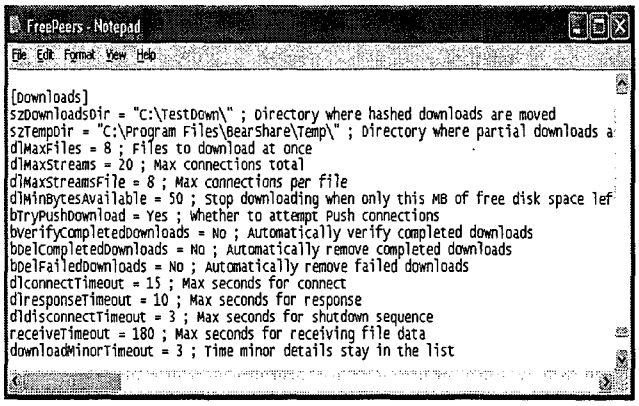
확인결과 HKEY_LOCAL_MACHINE\SOFTWARE\BearShare의 InstallDir 값에 설치경로가 저장되는 것을 알 수 이다.[그림 1]




[그림 1] Bearshare 설치경로에 대한 레지스트리 키 값

설치 폴더를 확인한 후 폴더 안에 있는 파일들을 확인해 보면 FreePeers.ini라는 파일을 볼 수 있다. 이 파일에서는 다운로드 및 임시 폴더경로, 다운로드 할 수 있는 파일의 수, 그리고 소프트웨어를 사용한 시간 등 소프트웨어 설정 정보를 저장하고 있는 설정파일이다.

[그림 2]에서 보는 바와 같이 szDownloadsDir key값을 통해 다운로드 폴더의 경로가 'C:\TestDown\'인 것을 확인 할 수 있다. 원래 다운로드 폴더의 기본경로는 'C:\My Downloads\'이나 'C:\TestDown\'으로 바뀐 것으로 보아 다운로드 폴더 경로를 사용자가 변경하면 FreePeers.ini 설정파일에서도 변경된 경로를 저장한다는 것을 확인할 수 있다.[4] 뿐만 아니라 szTempDir key값을 통해 Bearshare에서 다운받고 있는 파일이 임시로 저장되는 경로가 'C:\Program Files\BearShare\Temp\' 임을 확인 할 수 있다. 따라서 이 파일을 통해 용의자가 다운로드 파일을 저장하는 폴더의 경로를 확인할 수 있다.



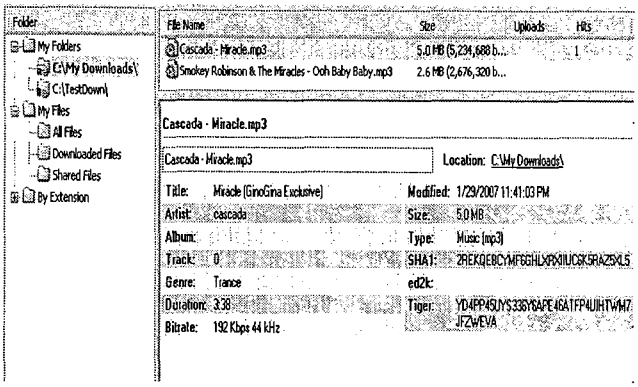

[그림 2] FreePeers.ini 설정 파일

### 3.3 다운로드

Bearshare는 설치 시 기본으로 'C:\My Downloads\'를 기본 다운

로드 경로로 저장한다. 이 폴더 안에는 다운받은 파일들이 저장되는데 저장되어 있는 파일들에 대한 몇 가지 중요한 정보를 Bearshare viewer로 확인할 수 있다.

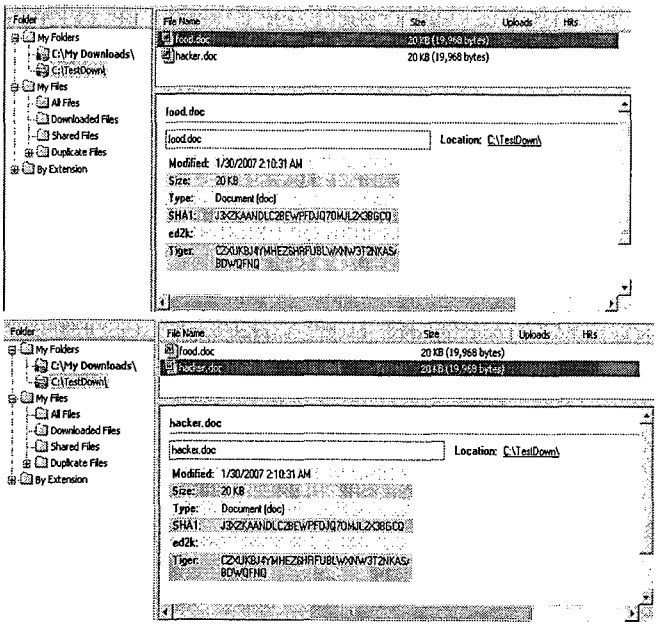
확인할 수 있는 정보는 파일을 다운받은 시간과 Gnutella network에서 파일을 식별할 때 사용하는 파일마다 독특한 해쉬값인 SHA1 등이 있다.[그림 3]




[그림 3] 파일에 대한 SHA1, Modified Time 등의 정보

SHA1 값은 동일한 파일에 대해 같은 값을 가지게 되는데 Gnutella network에서는 이를 이용하여 파일이름이 다르더라도 본질적으로 같은 파일을 검색할 수 있는 것이다. 만약 용의자가 저작권이 있는 문서를 공유했다는 혐의를 받고 있다면 다른 이름으로 저장하여 공유하였을 가능성을 두고 이와 같이 SHA1 값을 비교함으로써 동일한 문서임을 밝혀 낼 수 있다.

아래 [그림4]는 다른 이름으로 저장되어 있는 두 문서 SHA1 값을 비교한 그림이다. 다른 이름이지만 SHA1 값이 같은 것을 확인할 수 있다.



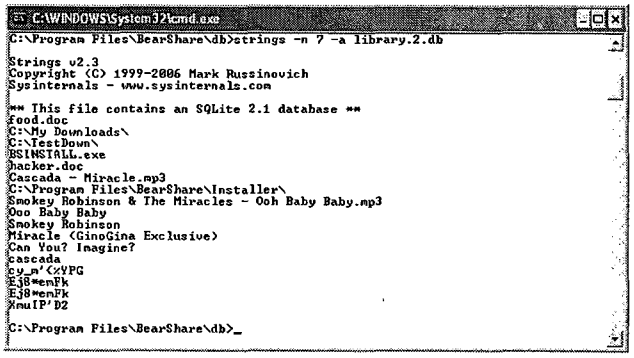

[그림 4] 파일명만 다른 두 파일에 대한 SHA1 비교

## 3.4 공유

Bearshare은 설치 시 다운로드 폴더와 같은 'C:\My Downloads\'를 기본 공유 폴더 경로로 저장한다. 이 외에도 사용자가 원하는 폴더를 공유할 수 도 있다.

Bearshare viewer를 통해 현재 공유되고 있는 폴더 목록과 폴더에 공유된 파일들을 확인 할 수 있지만 프로그램 설치 시 생성되는 폴더 안에 특정 파일에서도 공유폴더 목록과 공유 파일들이 무엇인지 확인할 수 있다.

프로그램 설치 시 생성된 'C:\Program Files\BearShare\db\'에서 확인해 보면 library라는 이름의 데이터베이스 파일을 확인할 수 있다. 이 파일을 Sysinternals사의 strings를 이용하여 파일에 저장되어 있는 ASCII 값을 확인해 보면 이 파일 안에도 공유된 폴더 목록과 파일들의 목록이 저장 되어 있는 것을 확인할 수 있다. [그림 5]에서 보이듯이 공유 폴더들과 공유 파일들을 확인할 수 있다.

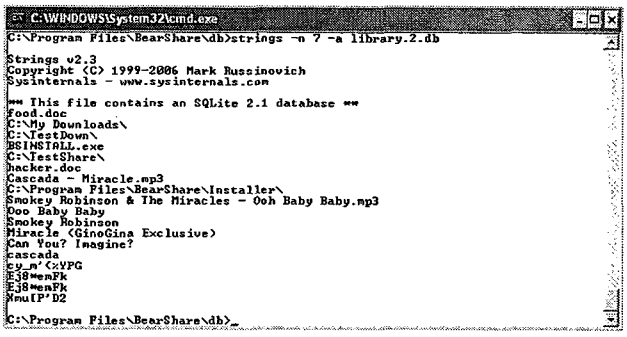



[그림 5] library.db 파일을 통한 공유폴더 및 공유파일 목록 확인

그런데 이 파일을 확인하는 중요한 이유는 Bearshare viewer에서는 현재 공유된 파일만 보여주지만 library.db 파일에는 삭제된 파일에 대한 정보가 남아 있기 때문이다.

만약 파일을 공유된 폴더 안에서 삭제 하고, Bearshare를 다시 실행 하지 않았다면 공유된 폴더 안에는 삭제된 파일이 없지만 library.db 파일에 저장된 ASCII값을 확인해 보면 삭제한 파일 이름이 여전히 존재하고 있음을 확인할 수 있다.

이것은 Bearshare가 실행되지 않았기 때문에 데이터베이스 파일이 갱신되지 않아 이전 정보가 남아 있는 것이다.[4]




[그림 6] hacker.doc 파일을 폴더에서 삭제 후 library.db 에서 hacker.doc 파일명 확인

[그림 6]에서 보는 바와 같이 공유했던 파일 food.doc와

hacker.doc중 hacker.doc를 삭제했을 경우 폴더안에는 hacker.doc가 삭제되어 확인을 할 수 없지만 library.db 파일에는 여전히 hacker.doc 파일에 대한 정보가 남게 되므로 용의자가 불법 파일을 공유한 것을 부인했을 경우에 증거로써 사용된다.

### 3.5 기타 정보

Bearshare에는 기능이 제공되지 않지만 많은 P2P 클라이언트 소프트웨어들은 다운로드와 업로드 기능 이외에도 채팅 기능을 가지고 있다. 이 채팅 기능을 이용하여 용의자는 다른 사람들과 정보를 교환할 수 있을 것이고 불법행위를 공모 할 수 도 있다.

따라서 P2P 클라이언트 소프트웨어를 분석시 다운로드, 업로드 파일들에 대한 분석뿐만 아니라 채팅 기록도 함께 분석 해야 한다.

## 4 결론

지금까지 살펴본 바와 같이 P2P 에서 컴퓨터 포렌식 수사에서 사용될 수 있는 다양한 정보들이 저장되어 있다는 것을 알 수 있다.

따라서 컴퓨터 포렌식 수사에 있어서 위와 같은 P2P를 분석하면 중요하고 결정적인 증거를 제공할 수 있음을 확인 할 수 있다.

하지만, 현재 사용자들에 의해 사용되고 있는 P2P들의 종류가 많고 그 기능 또한 다양하여 사건이 발생하였을 때 그 즉시 분석하기란 쉽지 않은 일이다.

따라서 향후 연구에서는 현재 사용자들에 의해 많이 사용되고 있는 P2P들의 종류를 파악하고 각각의 P2P에서 중요한 정보들을 분석하여 데이터베이스를 구축하는 작업이 요구된다. 또한 같은 P2P라 해도 버젼에 따라 설치, 다운로드, 업로드경로가 모두 다르고 설정파일 방식도 다르므로 버젼별 분석도 이루어져 한다.

데이터베이스 구축과 함께 P2P에 대한 컴퓨터 포렌식 수사에 있어 효율적인 분석을 위하여 정보들을 데이터베이스화 하는 것에 멈추지 않고 정보를 효율적으로 조사할 수 있는 컴퓨터 포렌식 도구로서 P2P 분석 프로그램이 개발 되어야 한다.

## 5 참고문헌


1. 이진순: Peer to Peer방식의 디지털콘텐츠 유통과 저작권 분쟁에 관한 연구
2. Bearshare, http://www.bearshare.com/
3. Eoghan Casey: Digital Evidence and Computer Crime: Computer and Internet, 2nd, Academic Press (2004) 199~205
4. Chad Steel: Windows Forensics. The Field Guide for Conducting Corporate Computer Investigations, (2006) 294-305
5. Sysinternals, http://www.sysinternal.com/
6. Harlan Carvey: The Windows Registry as a forensic resource, Digital Investigation (2004)
7. Jerry Honeycutt: Microsoft Windows XP Registry Guide (2003)
8. Eoghan Carvey: Handbook of Computer Crime Investigation (2003)