情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

BitTorrent를 이용한 저작물 불법 공유 조사 방법에 관한 연구*

박 수 영,† 정 현 지, 이 상 진‡
고려대학교 정보보호연구원 디지털포렌식연구센터

Methodology for digital investigation of illegal sharing using BitTorrent*

Soo-Young Park,† Hyun-Ji Chung , Sang-Jin Lee‡
Digital Forensic Research Center, Korea University

요 약

저작권자의 동의 없이 파일을 공유하는 행위는 불법이다. 그러나 BitTorrent를 통해 발생하는 불법 공유가 계속 증가하고 있다. 이러한 증가 추세에도 불구하고, 불법 공유자들을 처벌하기 위한 법적 근거와 수사 절차가 명확하지 않기 때문에 불법 공유자들을 처벌하기 어렵다. 또, 서버가 존재하지 않는 BitTorrent의 특성으로 인해 P2P를 통한 불법 공유에 대한 기존 수사절차의 적용 역시 어렵다. 본 논문에서는 BitTorrent를 이용하여 발생하는 불법 공유에 대한 형사상 수사 절차에 대해서 정립함으로서 수사절차에 적용 가능한 포렌식 프레임워크를 제시하고자 한다.

ABSTRACT

Sharing copyrighted files without copyright holder's permission is illegal. But, a number of illegal file sharers using BitTorrent increase. However, it is difficult to find appropriate digital evidences and legal basis to punish them. And, there are no framework for digital investigation of illegal sharing using BitTorrent. Additionally, role of server in BitTorrent had been reduced than server in conventional P2P. So, It is difficult to apply investigation framework for illegal sharing using conventional P2P to investigation process of illegal sharing using BitTorrent. This paper proposes the methodology about punishing illegal sharer using BitTorrent by suggesting the digital investigation framework.

Keywords: BitTorrent protocol, uTorrent, Illegal file sharing, Digital investigation framework, Packet analysis, Analysis of disk forensic

I. 서 론

저작물이란 어떤 아이디어를 독자적으로 표현한 창작물을 말한다. 지적 재산권은 저작자의 저작물 창조에 대한 의지 및 생산력 증진을 위해 저작자에게 주어지는 권리이다. 그러므로 지적재산권을 침해하는, 저작자의 동의 없이 이루어지는 불법 공유에 대해서는 반드시 적절한 절차를 거쳐 범죄의 입증 및 처벌이 이루어져야 한다. 저작물을 저작자의 동의 없이 업로드 할 경우 이는 저작자의 권리 중 복제권과 전송권을 침해하는 행위이며, 다운로드할 경우 이는 저작자의 복제권을 침해하는 행위이다. 저작권법 제 136조에 의하면, 저작물을 무단으로 복제하여 영리 행위를 한 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있다. 이러한 법적 재제에도 불

접수일(2012년 10월 19일), 수정일(2013년 1월 4일), 게재확정일(2013년 1월 4일)
* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, sooyoung011@korea.ac.kr
‡ 교신저자, sangjinlee@korea.ac.kr

구하고, P2P 네트워크를 통한 불법 공유가 증가하고 있다.

P2P(Peer-to-Peer network)은 개별 클라이언트들의 참여로 구성되는 통신망이다[1]. P2P의 종류로는 Opennap, Gnutella, Grokster, Freenet, eDonkey2000, BitTorrent 등이 대표적이며, 관련 기술들은 파일의 공유 혹은 데이터의 전송이 빠르게 진행될 수 있는 방향으로 발전해 왔다. 최근 가장 널리 사용되고 있는 BitTorrent는 파일을 일정한 크기로 나눈 Piece 들을 클라이언트 간에 동시다발적으로 공유하는 것을 가능하게 한 P2P 프로토콜이다[2].

기존의 P2P는 Centralized P2P 방식으로, 서버-클라이언트 형태였다. 중앙서버에서는 각 클라이언트들에 대한 정보를 가지고 있으며, 이 정보를 클라이언트들에게 제공함으로써 클라이언트 간 통신이 가능하게 하고, 통제한다. 이와 달리 BitTorrent는 hybrid P2P 방식으로, 서버의 역할은 타 클라이언트와 공유되는 파일에 대한 메타정보만을 제공하는 형태로 축소되었으며, 실질적으로는 동등계층에 있는 클라이언트 간에 통신망이 구축된다. 그리고 사용자들이 빠른 속도로 파일을 공유할 수 있도록 하기 위해서 데이터를 일정한 크기로 나눈 Piece 들을 클라이언트 간에 동시에 공유할 수 있게 했다는 점에서 기존의 P2P와 다르다.

과거 P2P를 통해 불법 공유가 발생한 경우, 법원은 P2P 서비스 제공자, 사이트 운영자들에게 기여책임 및 대위책임이 있다고 판결하였다. 법원은 이에 대한 처벌로 해당 사이트를 폐쇄하고 서비스 제공을 중지하도록 했다[3]. 그러나 BitTorrent의 경우 기존의 P2P 방식과 달리, 사이트에서는 실제 파일이 아닌 Torrent 파일을 공유하고 있으며, 실제 공유는 Torrent 파일이나 마그넷 링크를 BitTorrent 클라이언트 프로그램을 이용해 실행함으로써 이루어진다. Torrent 파일은 공유 대상이 되는 파일의 이름으로, 파일 조각의 길이, 해쉬 값 등의 정보를 포함하고 있으며, BitTorrent 클라이언트 프로그램을 통해 Torrent 파일을 실행함으로써 파일의 공유가 가능하다. 마그넷 링크는 Torrent 파일이 없더라도 파일의 공유가 가능하도록 만든 웹 url 이다.

클라이언트 간에 직접적으로 공유가 이루어지기 때문에, 단순히 관련 사이트들을 제재하는 것만으로는 불법 공유를 근절시킬 수 없다. BitTorrent 상에서 발생하는 불법 공유를 근절시키기 위해서는 직접 파일을 공유한 이들에 대한 제재가 필요하다. 따라서 실제 파일을 공유한 업로더와 다운로더들을 찾아내고 이를 처벌할 명확한 조사 프레임워크가 필요하다.

또, BitTorrent를 통한 공유는 Peer들이 서로 파일의 Piece를 주고받으면서 업로드와 다운로드가 동시다발적으로 발생하기 때문에 공유의 행위자를 업로더와 다운로더로 구분하는 기존의 방법을 적용하는 것은 큰 의미가 없다. 공유에 참여하는 이들은 모두 업로더이면서 동시에 다운로더이기 때문이다. 따라서 BitTorrent를 통한 공유과정의 각 단계를 기준으로 공유자들을 분류하고 이에 따라 법적 처벌을 어떻게 부과할 것인가에 대해 생각해 보아야 한다.

본 논문에서는 BitTorrent 클라이언트 프로그램 중에서 가장 많이 사용되고 있는 uTorrent를 통해 발생하는 공유과정에 대해 분석함으로써 공유자들의 정보를 수집하고 분류하는 방법에 대해서 정의하였다. 또한 공유자들의 PC에 남아있는 공유 관련 흔적들에 대하여 분석하였다. 그리고 불법 공유자들에 대한 형사상 수사절차 방법론을 제시함으로써 불법 공유자들의 위법사실을 입증하고 법적 책임을 부가할 수 있는 방안에 대한 기틀을 마련하고자 하였다.

P2P를 통해 발생하는 불법 공유에 대하여 기존의 연구사례가 몇 가지 존재한다. Ulric M.Lewen은 P2P를 통해 발생하는 불법 공유에 대하여, 법적 제도 측면에서 각 행위자가 어떤 법에 저촉되는가를 분석하였다[4]. 그러나 이는 기존 P2P와 다른 성격을 띄고 있는 BitTorrent에는 적용되기 어렵다. Karl Schrader는 네트워크 모니터링을 통해 BitTorrent 패킷 내의 info_hash 값을 확인함으로써 불법 공유 트래픽을 탐지하는 기법에 대해 제시하였다[5]. Sinan Hatahent 는 공유자의 행위패턴을 기반으로 불법 공유 트래픽을 탐지하고 차단하는 기법에 대해 제시하였다[6]. 그러나 실질적으로 네트워크를 모니터링하는 것은 한계가 있다. 그리고 BitTorrent를 통해 일어나는 공유의 경우, 공유를 위해 BitTorrent 프로토콜 뿐만 아니라 TCP, UDP 등 다양한 프로토콜을 사용하는데, 위의 기법들은 불법 공유 트래픽중 BitTorrent 프로토콜을 사용한 것에 대해서만 탐지할 수 있다. 또, 실제 불법 공유 트래픽임이 확인되었을 때, 이에 대해 어떻게 조사를 진행하고, 위법여부를 가려낼 것인가에 대한 방법은 제시하고 있지 못하다.

따라서 본 논문에서는 BitTorrent에 대한 기술적인 분석내용이 적용된 새로운 조사 프레임워크를 제시하고자 한다. 본 논문의 Ⅱ절에서는 불법 공유에 대한

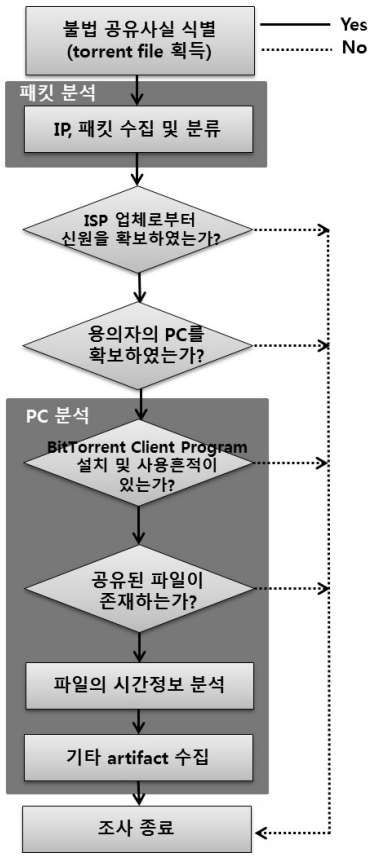
조사 프레임워크에 대해서 설명한다. Ⅲ절에서는 Ⅱ절에서 제시한 조사 프레임워크 내에서 불법사실 공유 식별과 IP 및 패킷을 수집해오고 분류하는 과정에 대해서 설명하였으며, Ⅳ절에서는 공유자의 PC 내에 남아있는 공유 흔적을 어떻게 찾을 것인가에 대하여 설명하였다. 그리고 마지막으로 Ⅴ장에서 결론을 내린다.

Ⅱ. 불법 공유에 대한 조사 프레임워크

저작물을 공유한 이들에 대하여는 기본적으로 방조죄가 성립한다. BitTorrent를 통해 파일의 공유에 참여함으로써 파일의 조각인 Piece를 다운받고, 보유하고 있는 Piece를 타인에게 전송하는 행위는 타인의 복제권 침해를 용이하게 해준다고 볼 수 있기 때문이다. 저작권법이 보호하는 복제권의 침해를 방조하는 행위란 복제권 침해를 용이하게 해주는 직접, 간접의 모든 행위를 말한다. 그리고 방조의 행위를 입증하는 과정에서 미필적 고의면 충분하며 객체 등의 구체적 인식이 불필요하고 정법의 확정적 인식이 불필요하다는 판결이 존재한다[7]. 그리고 BitTorrent를 통해 파일을 공유할 경우, Piece의 업로드와 다운로드가 동시다발적으로 일어나기 때문에 저작물 공유자들은 방조죄 뿐만 아니라 전송권과 복제권을 모두 침해한다고 보아야 한다.

따라서 공유가 일어나는 과정에 대해서 좀 더 자세히 살펴보고 공유가 일어나는 과정을 단계별로 나눈 뒤, 각 단계들에 속하는 case들에 대하여 상세히 분석하여, 범죄를 입증할 수 있는 근거들에 대해 살펴보아야 할 필요가 있다.

저작자 혹은 수사기관에서 저작권 파일이 불법 공유가 발생하였음을 식별하고, 이에 대한 Torrent 파일을 입수하면 [그림 1]에 제시된 프레임워크의 순서대로 조사를 진행할 수 있다. 획득한 Torrent 파일을 클라이언트 프로그램에서 실행시키면, 해당 파일의 공유가 시작됨과 동시에, Tracker나 DHT로부터 Peer의 정보를 자동적으로 수집해온다. Tracker는 공유 네트워크를 구성하는 공유자들에 대한 정보를 제공해주는 서버이다. DHT(Distributed Hash Tables)는 해시 테이블을 분산하여 관리하는 기술로, 어떤 항목을 찾아갈 때 해시 테이블을 이용할 경우, 중앙 시스템이 아닌 각 노드들이 이름을 값으로 맵핑하는 기능을 제공한다. 이러한 방법들을 통해 얻은 Peer들에 대한 정보는 공유과정의 각 단계에 대한 참여 여부를 구분하여 기록한다.



[그림 1] 불법 공유에 대한 조사프레임워크

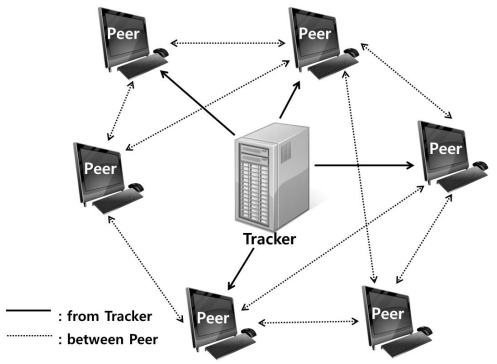
불법 공유에 가담한 Peer들의 IP를 수집하더라도, 공유자가 IP를 조작하여 통신했을 가능성이 존재하기 때문에, IP와 패킷 증거만으로 위법을 완벽하게 입증하기는 어렵다. 따라서 추가적인 증거 수집과정이 필요하다. 공유자가 죄를 범하였다고 의심할 만한 사정이 있고, 해당 사건과 관계가 있다고 인정할 수 있는 것에 대하여 수사기관은 압수·수색 영장을 발부받을 수 있다. 이에 의거하여, 수집된 IP들에 대하여 정확한 신원을 ISP 업체로부터 제공받은 뒤 공유자의 PC를 압수하기 위한 영장이 필요하다. 영장이 발부되면 공유자의 PC를 압수하고, 데이터 수집 및 분석과정을 진행한다. 공유자의 PC에서 공유와 관련된 흔적들이 발견된다면 이는 각 공유자들이 명백히 불법 공유에 가담하였던 것으로 간주할 수 있다. 각 공유자의 PC를 분석할 시에는 공유자가 실제로 파일을 공유했는가 여부를 확인하기 위해, BitTorrent 클라이언트 프로그램의 설치 및 사용 여부, 공유된 파일의 존재 여부, Torrent 관련 흔적정보 등을 확인해야 한다.

위의 절차를 통해 공유자의 위법사실이 명확해지면, 불법 공유한 저작물에 대한 몰수가 필요하다. 저작권법 제 139조 형사상 구제제도에서의 몰수규정에 따르면, 저작권, 그 밖에 이 법에 따라 보호되는 권리를 침해하여 만들어진 복제물, 도구, 재료는 몰수하는 것으로 정해져 있다.

III. 불법 콘텐츠 공유자 추적 기법

3.1. 공유자 IP 수집 기법

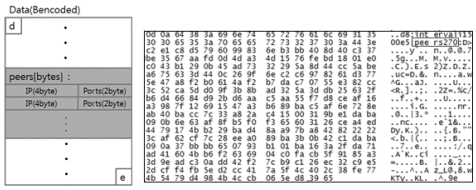
저작자 또는 수사기관이 불법 공유가 발생하였음을 식별하고, 불법 공유되고 있는 Torrent 파일, 또는 마그넷 링크를 입수하면, 이를 BitTorrent 클라이언트 프로그램에서 실행함으로써 공유와 연관된 IP와 증거패킷들을 수집할 수 있다. IP와 증거패킷을 수집하는 방법은, BitTorrent를 통하여 생성된 공유 네트워크에서 실제로 파일과 공유자에 대한 정보가 공유되는 과정을 응용하였다.



〔그림 2〕 BitTorrent를 통한 파일 공유 과정

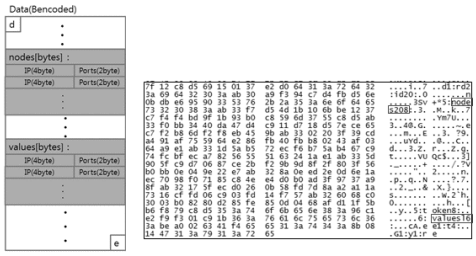
〔그림 2〕은 BitTorrent를 통한 파일 공유 과정을 보여준다. Peer는 공유 네트워크에 참여하기 위해 Tracker에게 다른 Peer들에 대한 정보를 요청함으로써, Tracker로부터 공유 네트워크를 구성하고 있는 타 Peer들에 대한 정보를 받는다. 이후 Peer는 타 Peer에 직접적으로 파일 공유 요청을 보냄으로써 Peer간에 파일의 조각인 Piece의 공유가 시작된다. Peer간에는 Piece의 공유뿐만 아니라, 공유 네트워크를 구성하고 있는 타 Peer들에 대한 정보의 공유도 계속적으로 이루어지는데, 이는 DHT 알고리즘을 통해 이루어진다. 이처럼 BitTorrent를 통한 파일의 공유과정에서 각 Peer는 Tracker나 DHT 알고리즘을 통해 타 Peer에 대한 정보를 얻기 때문에, 저작물을 불법 공유한 이들의 위치정보를 수집하는 과정에서 역시 위의 두 방법을 활용한다.

본 논문에서는 Peer 정보 요청에 대하여, 응답으로 받은 패킷으로부터 Peer의 정보를 추출함으로써 IP를 수집한다. 구체적으로 다음의 두 방법을 사용한다.



〔그림 3〕 HTTP GET 요청에 대한 응답 패킷 구조

첫 번째 방법은 Peer들에 대한 정보를 가지고 있는 Tracker에게 공유 파일의 info_hash 정보를 포함한 HTTP GET 요청을 보내고, 그에 대한 응답으로 받은 HTTP Response 패킷으로부터 Peer들의 정보를 추출해오는 것이다. 패킷의 데이터 부분에는 〔그림 3〕와 같은 형태로 Peer의 IP와 port 정보가 들어있다. 이 경우에는 HTTP 패킷의 bencoding 영역 내에서 key 'peers'가 존재할 때, 해당 key에 대응되는 value 데이터로부터 망을 구성하는 Peer들의 정보를 수집할 수 있다.



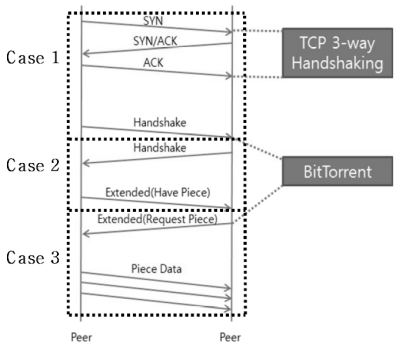
〔그림 4〕 'get_peer' 메시지에 대한 응답 패킷 구조

두 번째 방법은 BitTorrent 상에서 Peer에 대한 정보를 교환하기 위해 구현되어 있는 DHT 알고리즘을 이용하는 것이다. DHT 알고리즘 상에서 'get_peer' 메시지에 대한 응답으로 오는 UDP 패킷으로부터 Peer들에 대한 정보를 추출하는 것이 가능하다. Peer에 대한 정보를 담고 있는 UDP 패킷은 〔그림 4〕과 같은 형태로 되어 있다.

이 경우에는 UDP 패킷의 bencoding 영역 내에서 key 'nodes' 또는 'values'가 존재할 때, 'nodes'에 대응되는 value 데이터로부터 DHT을 구성하는 Node들의 정보를 수집할 수 있으며, 'values'에 대응되는 value 데이터로부터 망을 구성하는 Peer들의 정보를 수집할 수 있다. 경우에 따라 Node 정보만 포함하고 있는 패킷, Peer 정보만 포함하고 있는 패킷, Node와 Peer 정보 모두를 포함하고 있는 패킷이 있을 수 있으며, 위의 알고리즘은 모든 경우에 대하여 IP 정보를 추출하고 저장한다.

3.2. 공유자 분류 방법

공유자는 〔그림 5〕과 같이 TCP 세션까지만 통신이 성립한 경우, BitTorrent Handshake 교환과정까지 성립한 경우, 그리고 실제 파일의 공유가 일어나는 경우 3가지로 분류할 수 있다.



〔그림 5〕 Peer 간의 파일 공유 과정 분류

3.2.1. TCP 세션까지만 통신이 성립한 경우

BitTorrent 클라이언트 프로그램은 얻어온 Peer list에 포함되어 있는 Peer들에 TCP SYN 패킷을 보내어 세션을 맺고자 시도한다. 이에 대해서 세션 자체가 성립되지 않은 경우와, TCP 세션까지만 성립된 경우를 생각해 볼 수 있다. 첫 번째 경우는 TCP SYN에 대한 응답으로 TCP RST 패킷이 돌어오거나 아니면 응답조차 없는 경우가 여기에 해당한다. 두 번째 경우는 TCP 3-Handshaking이 완전히 수행되어 세션이 성립된 경우이다. 두 경우는 상대 Peer가 네트워크상에서 IP정보 수집 시간대에 활성화 되어 있었는가 여부만 다를 뿐이기 때문에, IP 분류 시에는 동일하게 간주한다.

이 범주에 속하는 Peer들은 과거에 공유에 참여할 의도를 가지고 있었으며, 이를 실행으로 옮긴 적이 있다고 간주할 수 있다. 이 경우, 이 범주에 속하는 Peer들이 과거에 파일을 공유한 내역에 대한 패킷 증거는 수집해올 수 없다. 그러나 Peer list에 IP가 남아있다는 것은, 공유에 참여한 적이 있음을 의미한다.

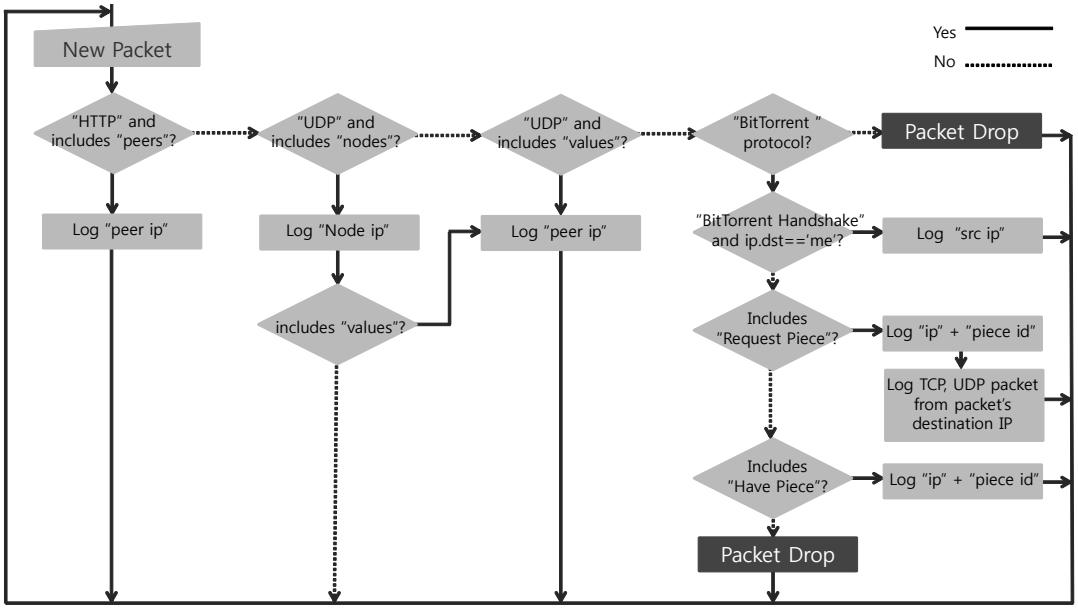
그러므로 이 경우에 대해서는, Peer list에 포함되어 있는 IP와 port 정보를 기록함으로써 불법 공유 관련 증거로 활용할 수 있게 한다.

3.2.2. BitTorrent Handshake 교환과정까지 성립한 경우

BitTorrent Handshake 패킷 내에는 공유하고자 하는 파일에 관한 정보로 구성된 info_hash 값이 들어있으며, 이 패킷을 보낸다는 것은 실제 파일의 공유가 일어나기 전에 각각의 Peer가 서로 보유하고 있는 파일의 조각을 서로 나누어 가질 의사가 있음을 의미한다. 그러므로 실제 파일 공유의 전단계에는 BitTorrent Handshake 패킷 교환과정이 있으며, 이를 주고받았다는 것 자체로도, 양자가 파일을 공유하고자 하는 의사를 충분히 내포하고 있다고 볼 수 있다.

BitTorrent Handshake 패킷 교환과정이 성공적으로 이루어지고 나면, 일반적으로 연결을 맺은 Peer 간에 서로 'Have, Piece' 메시지를 보낸다. 'Have, Piece' 메시지는, 자신들이 가지고 있는 Piece들을 타 Peer들에게 알림으로써, 요청한다면 언제든지 해당 Piece를 보내줄 수 있다는 의도를 포함하고 있다. 즉, 타 Peer들은 필요하다면 언제든지 'Have, Piece' 메시지를 보낸 Peer에게 'Request, Piece' 메시지를 보내어 원하는 Piece를 얻어올 수 있다. 실제 파일의 공유가 일어나지 않은 경우, 즉 'Have, Piece' 메시지를 주고받았으나, 'Request, Piece' 메시지가 있지 않았던 경우는 서로에게 원하는 Piece가 없음을 확인했기 때문일 가능성이 높다. 이 경우 역시 서로 공유하고자 하는 Piece가 없었을 뿐, 파일을 공유하고자 했던 의도가 명확한 것으로 봐야한다.

그러므로 이 경우에 대해서는, Peer list에 포함되어 있는 IP와 port정보, BitTorrent Handshake 패킷, 그리고 각각의 Peer가 어떠한 Piece들을 가지고 있었음을 알 수 있게 하는 'Have, Piece' 메시지 패킷을 기록함으로써 불법 공유 관련 증거로 활용할 수 있게 한다.



〔그림 6〕 공유와 관련된 IP 수집 및 분류 알고리즘

3.2.3. 실제 파일의 공유가 일어나는 경우

이 경우는 파일 공유를 위한 사전단계가 모두 진행된 뒤, 'Request, Piece' 메시지를 통해 Piece가 요청되고 공유 파일의 데이터가 실제로 전송된 경우이다. 이 경우에는 Peer간에 공유를 위해 오고간 패킷들을 기록할 뿐만 아니라, 전송되는 파일 데이터 패킷도 기록함으로써 불법 공유 관련 증거로 활용할 수 있게 한다.

3.3. 공유자 식별 및 분류 알고리즘

Torrent 파일 혹은 마그넷 링크를 실행시킨 뒤, 발생하는 모든 패킷을 〔그림 6〕의 알고리즘을 통해 불법 공유에 연관된 Peer들의 IP를 수집해 올 수 있으며, 공유자 정보를 분류하여 기록에 남기기 때문에 각 공유자가 공유과정에서 어떠한 역할을 하였는가를 알 수 있게 하였다. 〔그림 6〕의 알고리즘은 크게 공유와 연관된 IP를 수집하는 부분과, 각 IP가 실제 공유과정에서 어떤 역할을 하였는가를 구분하는 부분으로 구성되어 있다.

먼저 새로운 패킷이 들어오면 그 패킷이 Tracker로부터 받은 패킷인가, DHT를 통해 타 Peer로부터 받은 패킷인가, 아니면 실제 파일의 공유를 위해 맺어진 세션과 관련된 패킷인가를 구분한다. 만일 HTTP Response 패킷이고, 내부에 Peer에 대한 정보를 bencoding 형태로 포함하고 있을 경우, 이는 Tracker로부터 얻은 공유자에 대한 정보인 것으로 간주하고 이로부터 Peer의 IP 및 포트 정보를 추출하여 기록한다. 또는 만일 UDP 패킷이고, 내부에 Node 또는 Peer에 대한 정보를 bencoding 형태로 포함하고 있을 경우, 이는 DHT를 통해 얻은 공유자에 대한 정보인 것으로 간주하고, 이로부터 Node와 Peer의 IP 및 포트 정보를 추출하여 기록한다.

만일 BitTorrent 프로토콜 패킷일 경우에는 실제 공유를 위해 맺어진 세션과 관련된 패킷이라 간주하고, 패킷의 유형에 대해서 상세히 구분하여 기록한다. 첫 번째로, 들어오는 패킷 중에서 BitTorrent Handshake 패킷이면서 패킷의 송신자가 타 Peer라면, 이는 앞에서 살펴본 공유자 분류 케이스중 두 번째인, BitTorrent Handshake 교환과정까지 이루어진 경우로 간주한다. 본인이 BitTorrent Handskake 패킷을 먼저 보내고 이에 대한 응답으로 BitTorrent Handshake 패킷이 들어왔거나, 아니면 상대방이 먼저 BitTorrent Handshake 패킷을 본인에게 보내온 경우 모두, 결국은 상대방이 파일 공유 목적으로 본인에게 파일을 공유할 의사를 물은 것과 같기 때문이다. 그러므로 이 경우에 대해서는 BitTorrent Handshake 패킷을 보내온 상대방에 대한 정보를 기록한다. 두 번째로, Piece를 요청하는

패킷일 경우, 요청자의 IP와 요청한 Piece ID를 기록하고, 이 이후에 요청자와의 통신과정에서 TCP와 UDP를 통해 전송되는 실제 파일의 데이터가 포함된 패킷을 모두 기록한다. 세 번째로, 타 Peer들이 각자 어떠한 Piece들을 보유하고 있는가를 알리는 패킷일 경우, 전송자의 IP와 보유하고 있는 Piece ID를 기록한다.

IV. 공유자의 PC 분석

4.1. BitTorrent 클라이언트 프로그램 사용 확인

BitTorrent를 통해 불법 공유가 발생하였음을 증명하기 위해서는, 먼저 공유자의 PC에 BitTorrent 클라이언트 프로그램이 설치되어 있는가 여부를 확인해야 한다. BitTorrent 클라이언트 프로그램이 설치되어있지 않은 경우라도, 다음의 레지스트리 경로를 확인함으로써 공유자가 프로그램을 삭제했을 가능성을 고려해야 한다.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

위의 레지스트리 경로에 있는 프로그램들 중에서 BitTorrent 클라이언트 프로그램이 있는지를 확인해야 한다.

4.2. PC 내 공유된 파일의 존재 여부 확인

공유자가 불법 공유에 가담하였던 사실을 확인하기 위해서는 불법 공유를 통해 다운로드 했거나 업로드한 파일이 공유자의 PC 내에 있는가를 확인해야 한다. 파일이 삭제되었을 경우도 고려하여 파일시스템에 대한 카빙 역시 진행되어야 한다. 추가적으로 고려해 보아야 할 부분은, PC 내에 불완전한 파일이 있는 경우이다. 공유자가 공유에 일시적으로만 참여했을 경우, 공유자의 PC에는 일부의 Piece로만 구성된 불완전한 파일이 있을 수 있다. 불완전한 파일을 가지고 업로드 또는 다운로드 한 경우에도, 이를 저작권 침해로 보아야 하는가에 대해서는 각국마다 규정과 판례가 다르다. 그러나 확실한 것은 공유자의 PC에 완전한 파일이 있지 않더라도, 타 Peer에게 보유하고 있는 Piece를 전송함으로써 불법복제파일이 완성되는 것을 도울 수 있기 때문에 전송권과 복제권을 침해한다고 보아야 한다.

4.3. 파일의 시간 정보 분석

공유자의 PC 내에서 불법 공유된 파일이 있으면, 해당 파일의 메타 데이터 중 시각 정보를 고려해야 한다. 시각 정보의 분석은, 공유 파일의 생성 시각이 공유가 일어난 시각과 관련하여 유효한 범위 내에 있는가를 확인하는 과정으로 이루어져야 한다. 기본적으로 최초 배포자의 PC를 제외한 나머지 공유자들의 PC에 존재하는 공유 파일의 메타 데이터 중 시각은 Torrent 파일 내부에 포함되어 있는, Torrent 파일 생성 시각보다는 이후여야 한다. 구체적으로 파일의 메타 데이터 시각 정보는 공유 상태에 따라 조금씩 갱신된다. 공유 파일의 메타 데이터 시각 정보 중 만든 날짜와 액세스한 날짜는 공유자가 Torrent 파일을 실행한 후 최초로 다운로드를 시작한 시각이 기록되고, 그 뒤로 파일의 공유나 프로그램의 실행 및 종료 여부에 상관없이 최초 다운로드를 시작한 시각이 그대로 유지 된다. 그러나 수정한 날짜의 경우, 다운로드를 시작하고 다운로드가 진행되는 도중이거나 일시 정지한 경우에는 다운로드를 시작한 시각이 유지되나, 다운로드 도중에 정지하거나 프로그램을 종료한 경우에는 다운로드를 정지하거나 프로그램을 종료한 시각으로 갱신되며, 다운로드가 완료된 이후로는 다운로드를 완료한 시각이 유지된다. 그러므로 만든 날짜, 수정한 날짜, 액세스한 날짜간의 비교를 통해 공유자가 다운로드를 시작한 시각, 다운로드를 완료한 시각, 또는 다운로드가 진행되었던 가장 마지막 시각을 알 수 있다.

그러나 공유자의 PC에 존재하는 공유 파일의 메타 데이터 시각 정보가 다운로드를 시작한 시각, 다운로드를 완료한 시각 또는 다운로드가 진행되었던 가장 마지막 시간과 항상 일치한다고 볼 수는 없다. 공유 파일을 복사 또는 이동했을 경우를 고려해야하기 때문이다[8]. 운영체제 Windows XP 및 7 상에서, 파일을 한곳에서 다른 곳으로 복사할 경우 복사된 파일의 수정한 날짜는 원본 파일과 동일하게 유지되나, 복사된 파일의 생성한 날짜, 접근한 날짜는 파일의 복사가 진행된 시각으로 갱신된다. 또, 파일을 한 곳에서 다른 곳으로 이동할 경우 복사된 파일의 생성한 날짜와 수정한 날짜는 원본 파일과 동일하게 유지되나, 복사된 파일의 접근한 시간은 파일의 이동이 진행된 시각으로 갱신된다. 또, 다운받은 파일에 직접적으로 수정을 가할 경우, 파일의 수정한 날짜는 수정이 가해진 시각으로 갱신된다. 그러므로 각 공유자들의 PC에 존

재하는 공유 파일들의 메타 데이터 시각 정보를 가지고 파일을 공유한 시각을 유추하여 타임라인을 구성하는 것에는 무리가 있지만, 공유 파일의 메타 데이터 시각 정보가 Torrent 파일의 생성 시각보다 이후인 것을 확인함으로써 유효성을 검증하는 것이 가능하다.

또, 공유자들 개개인의 PC에 존재하는 공유 파일의 메타 데이터 시각 정보와 Torrent 파일의 생성 시각 정보를 비교하는 과정을 통해 최초 배포자를 식별해 낼 수 있다. 만일 공유 파일의 만든 날짜, 수정한 날짜, 액세스한 날짜 중에서 Torrent 파일의 생성 시각보다 앞서는 경우가 존재한다면 이 공유 파일이 존재하는 PC의 소유자가 최초 배포자일 가능성이 높다.

4.4. 기타 사용 흔적 확인

공유자의 PC에서 불법 공유와 관련하여 추가적으로 획득할 수 있는 증거들이 있는지에 대해서도 분석이 필요하다. 다음의 레지스트리 경로에서는 최근 실행한 Torrent 파일들을 확인할 수 있으며, 레지스트리의 데이터 부분에는 Torrent 파일의 이름이 들어있어, 불법 공유 파일과 관련된 Torrent 파일이 실행되었는가 여부를 확인할 수 있다[9].

HKEY_USERS\〈SID〉\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.torrent

그리고 uTorrent의 경우, 다음의 경로에 그동안 사용자가 다운받아 실행한 Torrent 파일들이 저장되어 있다.

〔표 1〕 uTorrent 관련 디렉토리 경로

OS 버전	경로
Windows XP	%Userprofile%\Application Data\uTorrent
Windows 7	%Userprofile%\AppData\Roaming\uTorrent

만일 공유자가 이전에 불법 공유 관련 Torrent 파일을 실행하여 특정 파일을 공유하고, Torrent 파일을 삭제했을지라도, 이 경로에는 Torrent 파일이 남아있을 수 있다. 또, 이 경로에는 Torrent 파일 이외에도 다음의 로그파일들이 존재한다.

〔표 2〕 디렉토리 경로에 남는 로그

이름	경로
dht.dat	DHT를 구성하는 Node 정보
Settings.dat	uTorrent 프로그램의 셋팅정보와 Tracker 정보

uTorrent의 경우, 프로그램 상에서 통계정보라는 기능을 제공하여 그동안 uTorrent의 사용기록에 대한 정보를 보여준다. 제공되는 정보 중 의미가 있는 항목들은 지난 31간 전송량, 총 업로드량, 총 다운로드량, 총 실행시간, 추가된 Torrent 파일 수, 프로그램 실행횟수, 마지막 실행시간이 있다.

V. 결 론

BitTorrent는 기존 P2P와 성격이 다르기 때문에, 기존의 조사절차를 이에 적용하는 것은 맞지 않다. 또한, 파일을 Piece로 나누어, 이를 동시다발적으로 공유하는 BitTorrent의 특징 때문에 현행법상 공유자들을 처벌하기가 매우 어렵다. 이러한 이유로 불법 공유건수는 줄어들지 않고 계속 증가하고 있다. 이러한 상황을 개선하기 위해서는 BitTorrent의 기술적 측면을 고려한 조사절차의 제시가 필요하며, 이러한 조사절차가 제대로 수행될 수 있도록 법적 개선 역시 필요하다.

본 논문에서는 BitTorrent를 통해 발생하는 파일 공유과정의 특징을 기반으로 불법 공유가 발생했을 때 적용될 수 있는 조사 프레임워크에 대해 제시하였다. 이 프레임워크를 따름으로써 조사관들은 불법파일 공유에 대한 수사를 더 체계적으로 진행할 수 있을 것이다.

참고문헌

〔1〕 P2P, URL : en.wikipedia.org/wiki/P2P
〔2〕 BitTorrent, URL : en.wikipedia.org/wiki/BitTorrent
〔3〕 MGM studios, Inc. v. Grokster, Ltd.,545 U.S.913, 2005.
〔4〕 Ulric M. Lewen, "Internet file-sharing :Swedish pirates challenge the U.S," Cardozo Journal of International and Comparative Law, pp. 173-177, Spring. 2008.

〔5〕 Karl Schrader, Barry Mullins, Gilbert Peterson and Robert Mills, "Tracking contraband files transmitted using BitTorrent," IFIP AICT 306, Advances in Digital Forensics V, pp. 159-173, 2009.
〔6〕 Sinan Hatahet, Yacine Challal and Abdelmadjid Bouabdallah, "BiTIT: throttling BitTorrent illegal traffic," Proceedings of the 2010 IEEE symposium on Computers and Communications, pp 708-713, June. 2010.
〔7〕 대법원 선고 2005도872 판결 (소리바다 저작권법 위반사건), 2007.12.14.
〔8〕 Jewan Bang, Byeongyeong Yoo and Sangjin Lee, "Analysis of changes in file time attributes with file manipulation," Digital Investigation, vol 7, Issues 3-4, pp.135-144, April. 2011.
〔9〕 Harjinder Singh Lallie and Philip James Briggs, "Windows 7 registry forensic evidence created by three popular BitTorrent clients," Digital Investigation, vol 7, Issues 3-4, pp.127-134, April. 2011.

〈著者紹介〉

박 수 영 (Soo-Young Park) 학생회원
2012년 2월: 서울여자대학교 정보보호학 공학사
2012년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식

정 현 지 (Hyun-Ji Chung) 학생회원
2010년 2월: 고려대학교 컴퓨터정보공학, 산업시스템공학 공학사
2012년 2월: 고려대학교 정보경영공학전문대학원 석사
2012년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 디지털 포렌식

이 상 진 (Sangjin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 컴퓨터 포렌식