Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

# Procedure guidance for Internet forensics coping with copyright arguments of client-server-based P2P models[☆]

Shiuh-Jeng Wang [a,*], Da-Yu Kao [b], Frank Fu-Yuan Huang [b]

[a] Department of Information Management, Central Police University, Taoyuan, 333, Taiwan
[b] Department of Crime Prevention and Corrections, Central Police University, Taoyuan, 333, Taiwan

ARTICLE INFO

*Article history:*
Received 27 April 2007
Received in revised form 26 September 2008
Accepted 28 September 2008
Available online 1 November 2008

*Keywords:*
Copyright protection
P2P models
Cybercrime
Digital content
Forensic analysis

ABSTRACT

Digital technology for transferring and controlling data has made substantial advances in recent years. It is important to protect innovations and to curb the copyright infringements in computer-based systems. Copyright is a legal framework of basic rights, allowing the owner to control or permit someone else to reproduce copyrighted works with commercial value. In recent decades, copyright violations have been moving into the criminal realm. This paper focuses on the procedure guidance of a fictitious P2P model, and discusses whether it contributes to the crime of copyright infringement in dealing with the distribution of digital content. From the perspective of internet forensics, the action research and the whole control mechanism, it is shown that a commercial server has full control over the P2P model.

## 1. Introduction

A case study is examined in this paper. It took place in the U.S.A. and involved the case of the Copyright infringement of Sony Corp. v. Universal City Studios. At the time, in 1984, it gave rise to large amounts of discussion. The Court held that the producers of home-use video recording devices could not be held responsible for copyright infringement, because the instruments were sold for legitimate purposes and had authentic non-infringing uses [15]. The case was a windfall for the private use of recorded television shows as the ruling had created a legal safe haven for the technology market by determining that later viewing constituted fair use. However, file sharing of unauthorized copies was popular at the same time and the peer-to-peer (P2P) architecture of the internet provoked new legal issues worldwide. In recent decades, copyright violations have been moving into the criminal realm. To clarify some of the more subtle points when facing P2P scenes, the proposal in this paper unveils some basic concerns and suggests some feasible solutions. P2P networks exist for searching and downloading files. Before that can happen, the IP address of the intended destination is required, prior to or at the moment of downloading the file. The illegal downloading of online digital properties is taking a big bite out of the bottom line of the rightful owners of that property. To battle the problem, efficient investigations by local authorities are required.

Arguments in this type of P2P case are often about the need to strike a balance between safeguarding creativity through copyright protection and limiting infringement liability. It is also necessary to effectively understand both the raw data and the filtered output. Original copyright owners have lost huge amounts of business and profits through the illegal duplication of their copyrighted works [10]. Copyright owners are suing those who provided the P2P devices that allow for an environment of easy file transfer over the internet. The diversity of legal systems has resulted in some jurisdictions finding that P2P developers are not doing anything inherently illegal by providing these technologies [16]. Thousands upon thousands of different illegal digital copyright materials are widely distributed at present. The popularity of P2P software is also prevalent on the internet, such as Ezpeer (Taiwan), Kuro (Taiwan), Napster (USA), Aimster (USA), MMO (Japan), and KaZaA (Holland). While Ezpeer, Kuro and Aimster charge a small fee for using the service, others generate income by selling advertising space. In addition, user authentication is optional with Ezpeer, Napster, MMO and Aimster for their system management requirements [13]. Most operators of P2P networks are aware that users employ their software primarily to download copyrighted files, although the networks do not record which files are copied, and when. These above observations indicate that it is easier and more effective to litigate against P2P developers than it is to sue the millions of people who transferred files illegally. Although the systems have important differences, commercial software has similar requirements to keep track of their profit through

[☆] This work was supported in part by National Science Council in ROC under Grant NSC 97-2221-E-015-001.

[*] Corresponding author.
*E-mail address:* sjwang@mail.cpu.edu.tw (S.-J. Wang).

0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.09.009

identification, authentication, index schemes, account records and other audit trails.

The remainder of this paper is organized as follows. Section 2 describes a related work on P2P copyright infringement. Section 3 provides a case study to be the follow-up guidance on internet forensics. The investigation of the above mentioned case is presented in Section 4. Finally, conclusions are drawn in Section 5.

## 2. Related work

A P2P is a computer network that focuses on communication between peers. Some P2P networks share files of popular but copyrighted material, duplicated in a variety of digital formats. The Motion Picture Association (MPA), the International Federation of the Phonographic Industry (IFPI) and other organizations all over the world have taken aggressive action of copyright protection to combat these potential losses in P2P-based file-swapping networks, which are exploding on the net with pornography, popular songs, and famous movies [13]. The sharing of these copies is illegal in most jurisdictions. This situation poses a great potential threat to the rather recent online copyright protection laws, even though some decisions are still pending [15]. One promising classification is to consider the relationship of P2P, cybercrime investigation and cyber forensics. To fully understand the whole array of P2P issues, this study will discuss the lack of pure P2P networks, analytical challenges of cybercrime investigation, and anti-forensics in cyber forensics.

### 2.1. Scarcity of pure P2P networks

Comparing a P2P network to a client-server architecture is a matter of personal perception or preference, because each has its own merits. It is common to see both architectures employed together. Basically, it is difficult to decouple the P2P network from the client-server architecture. Many P2P systems use stronger super-nodes as servers, while client-peers are connected in a star-like fashion to a single super-peer. The Skype P2P Internet Telephony Protocol is a good example [1]. Consequently, pure peer networks are rare. Any P2P software system still needs to provide all peers with the information of IP address, file directory, and file location. Therefore, most networks and applications described as P2P usually contain some elements of the "server" and "client" architecture, such as client IP lists or index servers. Technically, a pure P2P structure would only operate the peering protocols. Real world applications, however, often act as client, server, and peer simultaneously. A conflict between P2P model and client-server structure can arise when verifying the personal identification of the enterprises' benefits. No matter how it actually works, the whole mechanism can be designed to suit the process.

### 2.2. Analytical challenge to cybercrime investigation

The criticism of sharing technologies has shaped some analytical challenges in the courts. Courts do not universally agree that the providers of P2P “file-sharing” software can be held liable for the individual online act of file transferring. Fact-finders should focus their attention on what kind of significant technique goes into committing a cybercrime. Software often has one main purpose, and most commercial software packages often care only about what the customer wants. There are literally thousands of categories of expertise. No one knows the whole breadth of technologies that underlie a legal case. Within the legal community, the advances and changes in technology make it difficult for any one individual to explain all the technical issues, suggest strategies, investigate facts, conduct research, and at the end prepare a presentation [9]. That is the reason why we need experts for forensic examinations on a case-by-case basis. An expert is a spectator, who by virtue of education, profession, or experience is believed to have extraordinary knowledge in a topic that is beyond that of the average person [6]. Otherwise, too much excursive data makes it difficult to know the difference between the truth and the defendant's sophistry.

### 2.3. Anti-forensics in cyber forensics

Sustained innovation is based upon both challenge and knowledge. Knowledge is a precondition for taking the strategic approach to innovation. When forensic science becomes popular, criminals keep the scientific and investigative techniques in mind [12]. The view on information-sharing between the commercial P2P developers and criminal investigators usually results in controversy when a copyright infringement is committed. The developer pays much attention to any

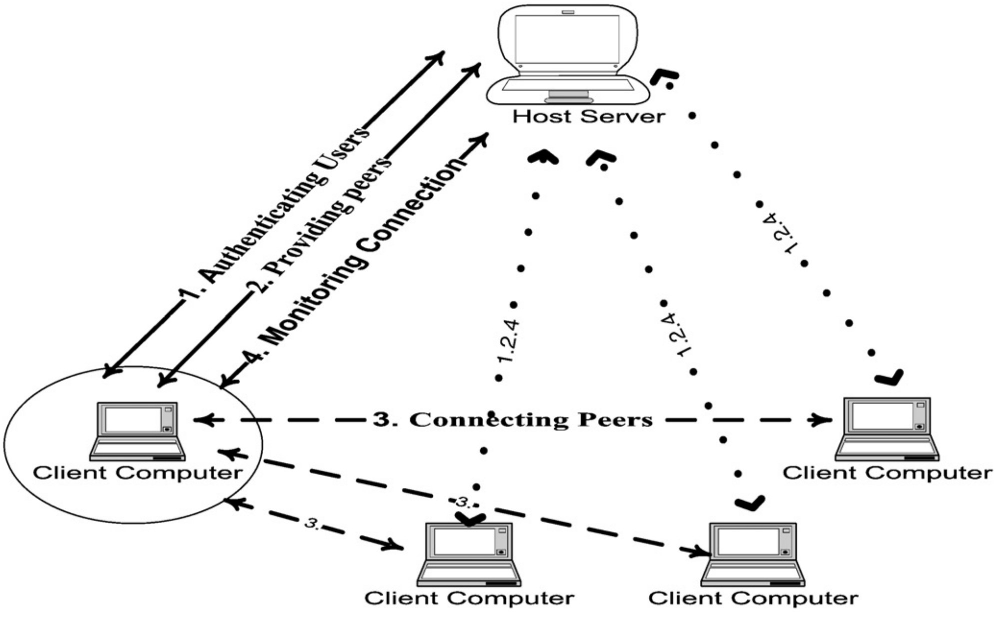

**Fig. 1.** The structure of Ezpeer P2P mechanism.