Chapter 15
Forensic Investigation of Peer-to-Peer Networks

Ricci S.C. Ieong
The University of Hong Kong, Hong Kong

Pierre K.Y. Lai
The University of Hong Kong, Hong Kong

K.P. Chow
The University of Hong Kong, Hong Kong

Michael Y.K. Kwan
The University of Hong Kong, Hong Kong

Frank Y.W. Law
The University of Hong Kong, Hong Kong

Hayson K.S. Tse
The University of Hong Kong, Hong Kong

Kenneth W.H. Tse
The University of Hong Kong, Hong Kong

ABSTRACT

The community of peer-to-peer (P2P) file-sharing networks has been expanding swiftly since the appearance of the very first P2P application (Napster) in 2001. These networks are famous for their excellent file transfer rates and adversely, the flooding of copyright-infringed digital materials. Recently, a number of documents containing personal data or sensitive information have been shared in an unbridled manner over the Foxy network (a popular P2P network in Chinese regions). These incidents have urged the authors to develop an investigation model for tracing suspicious P2P activities. Unfortunately, hindered

DOI: 10.4018/978-1-60566-836-9.ch015

by the distributed design and anonymous nature of these networks, P2P investigation can be practically difficult and complicated. In this chapter, the authors briefly review the characteristics of current P2P networks. By observing the behaviors of these networks, they propose some heuristic rules for identifying the first uploader of a shared file. Also, the rules have been demonstrated to be applicable to some simulated cases. The authors believe their findings provide a foundation for future development in P2P file-sharing networks investigation.

INTRODUCTION

Since 1999, when the first peer-to-peer (P2P) system Napster came to life, P2P applications have accounted for a major force in total Internet traffic. In 2007, P2P was responsible for 50 - 90% of all Internet traffic in German (Bangeman, 2007). In North America, a report published by Sandvine suggested that around 41 - 44% of all bandwidth was used up by P2P file transfer (Cheng, 2008). From the latest Internet study released in February 2009 (Hendrik & Klaus, 2009), P2P generates the most traffic in all the eight monitored regions - ranging from 43% in Northern Africa to 70% in Eastern Europe. Though the popularity varies from country to country, the trend of P2P networks can be seen almost everywhere.

P2P networks are often credited for enabling the cost-free and efficient sharing of digital files without physical boundaries. Instead of having files stored on a single server as in traditional client-server based networks, files of P2P users are mutually shared among each other who is currently online. The good point is, everyone who downloads a file also acts as an uploader sharing the pieces he possesses. The concept of P2P effectively utilizes the uploading bandwidth of average users in a much better way, contributing to the speedy exchange of data on those networks.

Apparently, everyone would welcome this fascinating technology. However, one should note the issues of piracy and illegal downloads that came along. With the prevalence of P2P file sharing applications, the media industry and many software developers have suffered huge losses in these years. In 2007, the value of unlicensed music trafficked on P2P networks was US $69 billion, according to a MultiMedia Intelligence study (Scottsdale, 2008). Also, the MPAA estimates the P2P online piracy problem costs its member studios US $3.8 billion a year ("Anti-Piracy," n.d.). Apart from the piracy issues, the unintentional sharing of personal information has raised much attention in general public. In February 2008, hundreds of racy photos showing a local pop icon participating in sex acts with a series of female celebrities were wildly spread around the globe (Chesterton, 2008). The use of Foxy, a popular P2P software in the Chinese community, has been accused of the swift and uncontrollable spreading on the Internet. Besides, a number of cases involving the leakage of sensitive documents were reported in Taiwan and Hong Kong (Moy & Patel, 2008; "Serious leaks," 2008; "Response," 2008). All these figures and incidents urge us on having a closer look into the P2P world from the computer forensic perspective.

In the past few years, lots of research and tools (to be discussed in Section 4.1) for computer forensic examination have been engaged in P2P networks. Most of this research is, however, focused on revealing digital traces from computers that have been identified and seized. There is a lack of research on how to trace and locate the originating computer that has been used to upload the illicit file. Apart from the challenges of short distribution interval and anonymity, the numerous P2P protocols, which operate differently, make the investigation work even harder. Therefore, it is difficult for investigators to identify and to trace the whereabouts of the first uploaders. Even when someone has been identified