

# The P2P Observer System

*Detecting P2P Usage*

DECEMBER 2007



# Executive Summary

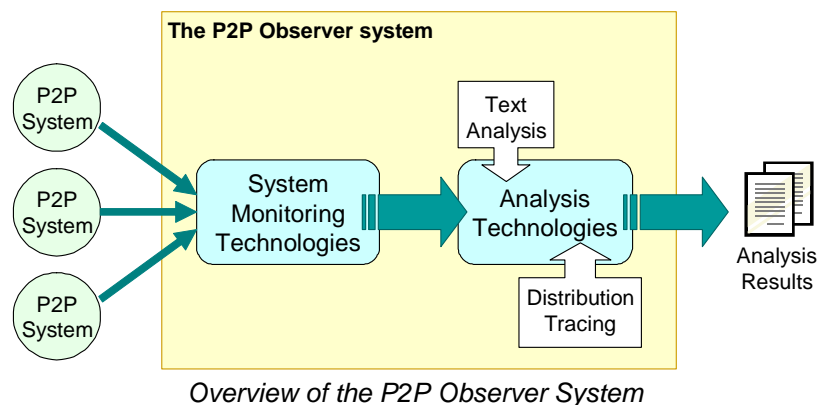
*Isis Forensics provides solutions to help businesses eliminate the risk that Peer-to-Peer (P2P) file sharing poses to their organisations. Central to these solutions is our **P2P Observer** system that allows for business networks to be monitored in an entirely passive and non-disruptive fashion.*

*This short paper provides an overview of Isis Forensics' P2P Observer system.*

## Architecture

The P2P Observer system uses state of the art technologies to monitor and analyse P2P network usage. In contrast to many existing monitoring technologies, the P2P Observer system can perform monitoring *externally* from an organisations network, observing data at the P2P level, in real-time as it is broadcast from business networks. A key advantage of this is that Isis can observe P2P usage on business networks without having to gain access to the networks being observed. This makes it impossible for Isis Forensics' monitoring activities to interfere with critical business applications.

The following figure illustrates the architecture of the P2P Observer system and Isis Forensics traffic analysis process.



As the diagram shows, the P2P Observer system uses a two stage process:

- **System Monitoring** - high performance monitoring technologies are used to capture the vast amounts of the data that businesses are broadcasting on P2P systems. Isis Forensics monitoring technologies are flexible, allowing them to be applied to all current P2P file sharing systems along with emerging systems. Data captured by the P2P observer system is then archived in a separate database for subsequent analysis.
- **Data Analysis** - statistical and text-based analysis technologies are used to examine the captured data. With these, the P2P Observer system is able to automatically associate data with a given organisation and to categorise the files that this organisation is sharing. Isis Forensics sophisticated analysis techniques are capable of determining if a P2P file is of a copyrighted or pornographic nature. Tracing technology can also be drawn upon to allow the P2P Observer system to determine how files are being distributed across P2P networks.

The P2P Observer System also provides real-time security warnings to those businesses which subscribe to Isis Forensics' *subscription alert service*. Furthermore, the system allows for the tracking of files as they are distributed across P2P networks. This functionality is used by Isis Forensics to offer a range of bespoke consultancy services.

The output of the P2P Observer System is a refined set of results that are used as the basis of Isis Forensics' *audit report*. This information allows Isis Forensics' clients to better protect themselves from the risk that P2P file sharing poses to their organisation.

### **Information Capture and Privacy Protection Policy**

The huge volume of data that is captured by the P2P Observer system can be broken down into two types:

- **Resource Discovery Traffic** – that describes what users are searching for on the P2P file sharing system
- **File Offerings** – containing details of the files that a user is sharing (typically file names and file sizes), when they publish this information, and the source of this publication (the computer and host organisation).

Isis Forensics has the utmost respect for the privacy of its clients. For this reason, all analysis of captured data is performed by an automated system without human intervention. Furthermore, all data is expunged from our system after 28 days, ensuring that only the businesses themselves have access to their data.

It is critical to consider that *if Isis Forensics can observe the P2P activities of a business - so can others.*

In contrast to Isis Forensics' approach, a range of companies have been established to trawl P2P file sharing networks with the intention of selling the acquired data to interested parties. Examples of such companies include MediaDefender, RedTeamProtection and BigChampagne. If employees use your business network to use P2P, these companies can detect you, and potentially pass on your details to copyright enforcement agencies. To quote John Kennedy, chief executive of the International Federation of the Phonographic Industry (IFPI):

***"We don't want to litigate - don't leave yourself exposed to litigation."***

*Isis Forensics* is an international security consultancy firm which specialises in securing business networks against Peer-to-Peer (P2P) and file sharing technologies. Isis Forensics professional solutions are designed to minimise the legal, security and financial risks that file sharing poses to business networks.

*For more information about how we can help you, contact us at:*

**Isis Forensics**

PO Box 793

Lancaster

Lancashire

LA1 9ED

UK

**Tel:**+44(0)7902891873

**Fax:**+44(0)7902891895

**Email:**[enquiries@isis-forensics.com](mailto:enquiries@isis-forensics.com)

**Web:** [www.isis-forensics.com](http://www.isis-forensics.com)