

The P2P Observer System

Detecting P2P Usage

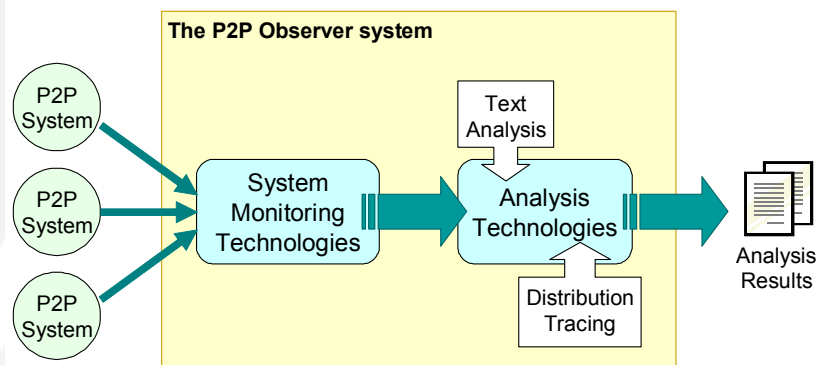


The Challenge

Recent studies have shown that Peer-to-Peer (P2P) systems are the biggest source of internet traffic, accounting for more than 40% of all data that is transferred. P2P systems empower the user by allowing them to search and distribute files on a global scale. However, although such systems can be used for legitimate purposes they can also be used to carry out activities that maybe illegal or cause harm. Being able to monitor these vast and technically evolving systems and then analyse the collected data, can be a daunting and resource intensive task.

The Solution

Isis Forensics' P2P Observer system uses state of the art technologies to monitor and analyse P2P network usage. In contrast to many existing technologies, the P2P Observer system can perform *external* monitoring of a network, observing data at the P2P level in real-time as it is being broadcast to the wider internet. A key advantage of this is that P2P usage can be observed without having to gain access to specific networks (for example, belonging to an organisation). This makes it impossible for Isis Forensics' monitoring technologies to cause network interference.



Overview of the P2P Observer System

System Monitoring - high performance monitoring technologies are used to capture the vast amounts of the data that are broadcast on P2P systems. Isis Forensics' monitoring technologies are flexible, allowing them to be applied to 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 reference point (IP, location, time, etc) and to categorise the files that are being shared. The continuous monitoring of data means that traces over time can also be built up that can be used, for example, to determine how a file is being distributed across various P2P networks. In addition Isis Forensics' other technologies can also be drawn upon; the Natural Language Analysis technologies support finer grained analysis, for example, to help determine if a file is of a copyrighted or pornographic nature; the Device Fingerprint technologies can be used to more accurately identify the distributors of files.

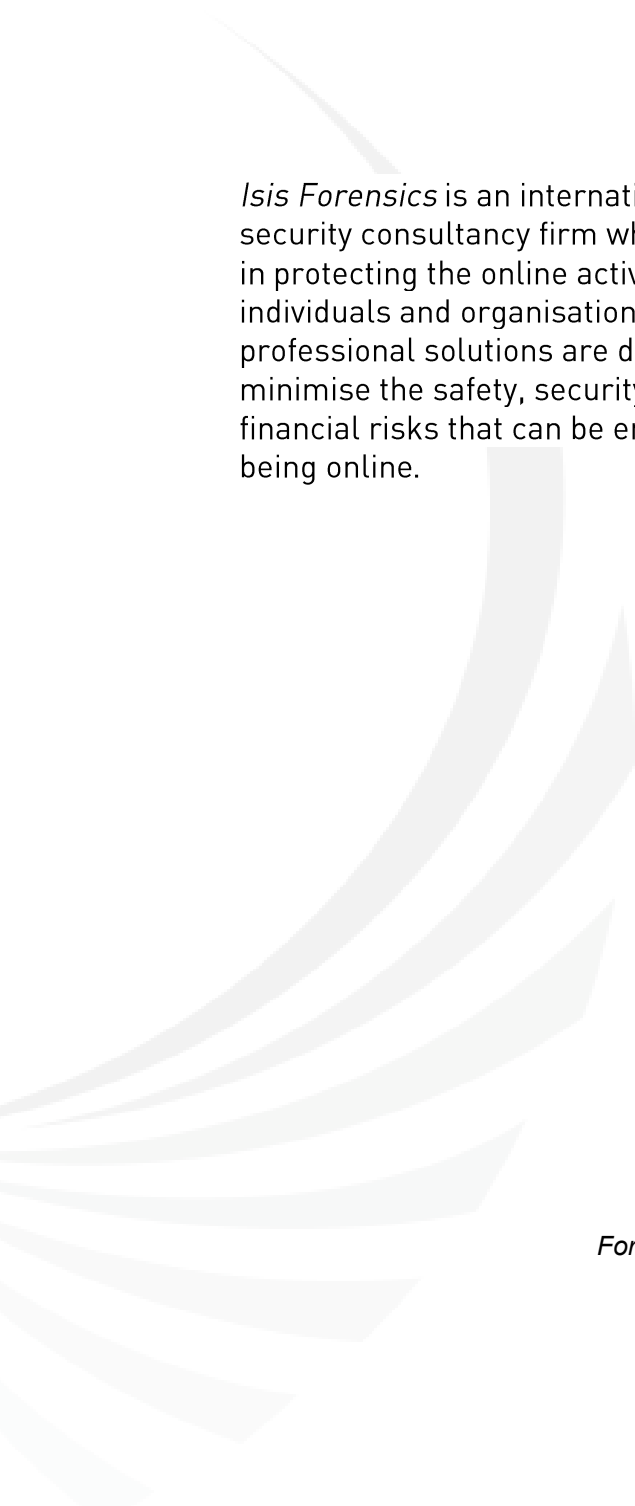
Information Capture – The P2P Observer System is able to capture two types of data: Resource Discovery Traffic – that describes what users are searching for on the P2P file sharing system; and File Offerings – that contain details of the files that a user is sharing (typically file names and file sizes), when they publish this information, and the source of this publication (the computer, IP, country, etc).

Auditing and Alerts – The output of the P2P Observer System is a refined analysis over a given time period that can be used in a broad manner (for example, auditing P2P activity on a global scale), or be more targeted (auditing P2P activity emanating from a specific network). The P2P Observer System is also able to provide real-time alerts should certain IP's be detected or files be shared at a given point.

The Benefits

Isis Forensics' P2P Observer System provides a complete solution for monitoring and analysing activity that occurs on P2P networks. The P2P Observer System provides a number of key benefits:

- **Global capacity** – the system is able to monitor P2P activity across the globe from one location.
- **Non invasive nature** – access to specific networks is not required. Instead it is the P2P activity that emanates from these networks that is monitored.
- **Sophisticated analysis** – data is captured over time and analysed with Natural Language Analysis techniques. This allows for sophisticated automated analysis over a given timescale.



Isis Forensics is an international online security consultancy firm which specialises in protecting the online activities of individuals and organisations. Isis Forensics professional solutions are designed to minimise the safety, security, legal, and financial risks that can be encountered from being online.

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

Isis Forensics
The Knowledge Business Centre
InfoLab21
Lancaster University
LA1 4WA

Tel:+44(0)7092 891873
Fax:+44(0)7092 891895
Email:enquiries@isis-forensics.com
Web: www.isis-forensics.com