

Remote Device Fingerprinting

Beyond IP Based Identification



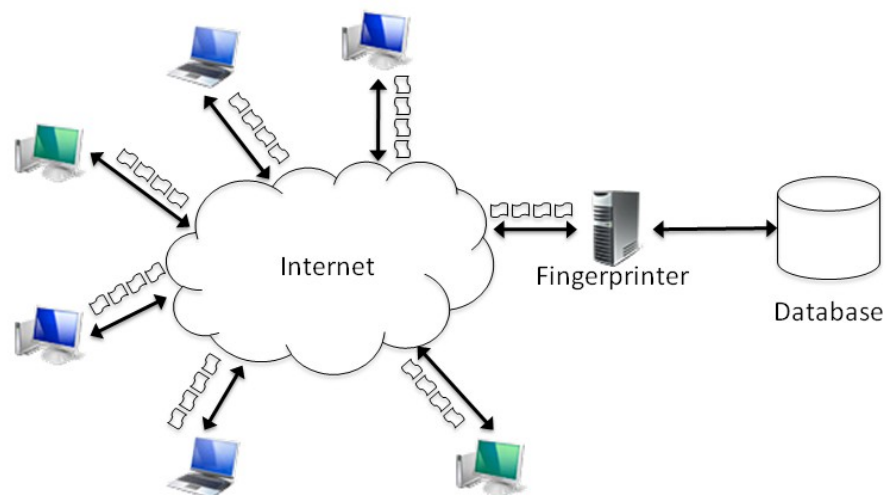
The Challenge

Traditionally, the means of identifying and tracking users on the Internet (for example, if they are suspected of participating in illegal activities), has involved the use of IP addresses. An investigator would collect the IP addresses of devices that are participating in such activity using distributed monitoring techniques (as, for example, used within Isis Forensics' P2P Observer System). The observer can then obtain the users' real identity by acquiring the appropriate authorisation and requesting the users' details from the relevant Internet Service Provider (ISP). However, basing investigations solely on the IP address could, for example, lead to innocent people being suspected and the guilty party evading capture. A number of limitations are associated with IP-based identification that can lead to incorrect accusations:

- **Mis-reported IP address** – a malicious user may spoof their IP address to frame an arbitrary IP address.
- **Mis-timed observations** – a suspect IP address could be passed onto an innocent user, but propagation delays and time-outs on the network mean the monitors are not made immediately aware of this fact.
- **Man-in-the-middle attack** – in a vast number of cases network connections are open and so unencrypted; this leaves them vulnerable to man-in-the-middle attacks with malicious users able to manipulate data to implicate arbitrary IP addresses.
- **Open wireless networks** – many wireless networks, particularly home wireless networks, are insecure and allow any passing user to connect. Any illegal activity conducted by the passing user will be attributed to the owner of the network.

The Solution

Isis Forensics has developed a remote *device fingerprinting* technology that removes the need to rely solely on IP addresses to identify and track a networked device. The fingerprinting technique relies on identifying the unique characteristics of a device's hardware, which can be viewed or inferred over the network as it communicates with the monitor. Over time this information can be collected and used to build a unique profile of the device that, in turn, can then be used to help identify and track the device even if its IP address changes.

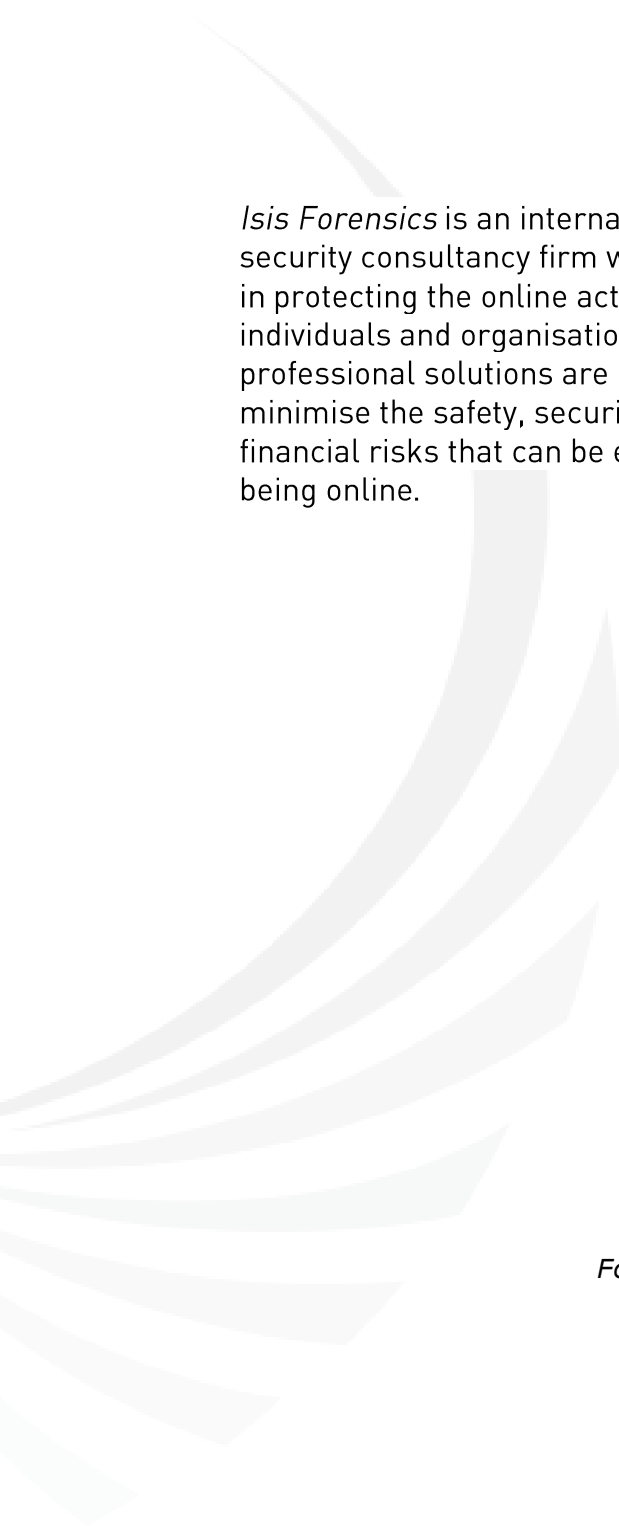


An extensive evaluation of the device fingerprinting technology has shown that it is able to provide a positive identification with a confidence of over 80% from transferring just 9Mb of data from the target device - with more data collected increasing the accuracy. This means that downloading a simple movie file from the target would be more than sufficient for building an accurate fingerprint of that device. Significantly, not only can this be used to help identify a device, it can also be used to eliminate a device from an investigation with a much higher degree of accuracy, thus preventing innocent users from being suspected.

The Benefits

Isis Forensics' remote fingerprinting technology provides an alternative approach to identifying a device that overcomes the disadvantages of IP based identification. The technology provides a number of key benefits:

- **Creation of a device fingerprint** – over time a fingerprint is built up that is unique to that device and which can be used to help track the device on the Internet.
- **IP address independent** – a device's fingerprint does not change, meaning that it can later be correctly identified even if the IP address does change.
- **Non-invasiveness** – no modification of the target device is required; the fingerprintee is unaware that the fingerprinting is taking place.
- **Universally applicable** – this technique can be applied irrespective of network protocol and distance from fingerprinter; all that is required is network connection established between fingerprinter and fingerprintee.
- **Eliminates spoofing** – this technique is not susceptible to the spoofing techniques commonly used in IP-based identification. It is impossible to implicate other devices.
- **No hiding** – the fingerprinting still works even if the device is behind a network address translator (NAT) or firewall.



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