MAGNET
FORENSICS®

# Investigating Intellectual Property Theft

How IT Group Uses Magnet AXIOM to Reveal the Most Essential Artifacts

## THE CHALLENGE

IT Group is being asked to conduct a steadily increasing number of intellectual property (IP) theft investigations. In the last year alone, the value of the stolen IP has amounted to several million pounds.

Employers engage IT Group to investigate IP theft in one of two circumstances:

- An employee has left the business, often moving to a direct competitor
- Specific evidence, such as an intrusion detection alert, suggests theft may have taken place

Typically, IP theft occurs shortly before or after the employee hands in their employment termination notice. One of the biggest challenges during an IP theft investigation is narrowing down the vast amount of data to find the actual moment that the alleged IP theft occurred.

## COMPANY OVERVIEW

IT Group is a leading United Kingdom supplier of IT consultancy, forensic investigations and expert witness services.

They specialize in civil and criminal cases, along with corporate investigations, involving technology.

itgroup®

> “Magnet AXIOM has revolutionised [our] digital forensic investigations. In time-critical investigations, the ease of processing and the user-friendly interface allow for quick filtering of the most relevant artifacts.”

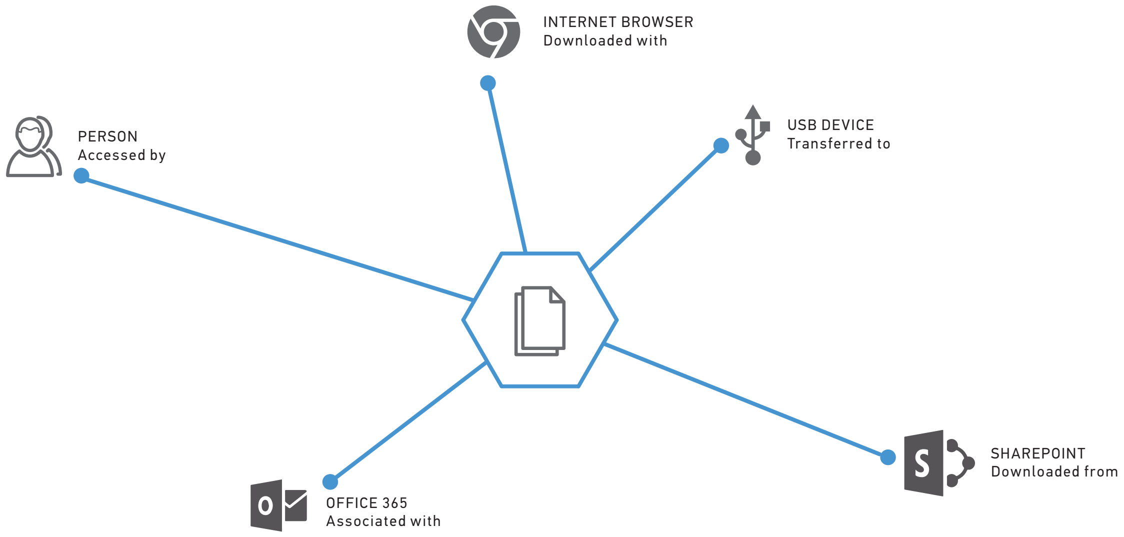
—George Jennings, Head of Digital Forensics & e-Disclosure, IT Group UK Limited

## HOW AXIOM HELPS

After seizing and imaging the device, investigators use AXIOM to concentrate on the artifacts that are critical to the investigation. Focusing on essential artifacts is critical to ensure that the investigation moves as quickly as possible. Creating a timeline of events is also a key requirement for securing a successful outcome.

In IP theft investigations, the most relevant artifacts are LNK files, USB history, Shimcache, cloud storage, emails and shellbags. Other key artifacts may include browser history and Google searches, as well as text and chat messages extracted from mobile phones and mobile backups.

AXIOM's easy-to-use interface presents all this data in a simplified view, providing examiners with a deep understanding of the evidence at a glance. AXIOM also enables rapid filtering to surface the most important artifacts, while its intuitive tagging features allow examiners to move quickly through the data before coming back to important evidence to build a final report. Lastly, AXIOM allows examiners to view the timeline between key evidence like LNK files and Shimcache.



## IP THEFT INVESTIGATIONS WITH AXIOM

- Verify what was downloaded
- Determine where the files were saved
- Identify who the files were shared with
- Build your case and prove intent

Learn more at magnetforensics.com

For more information call us at 1-844-638-7884 or email sales@magnetforensics.com