

CASE STUDY:

# INTELLECTUAL PROPERTY THEFT

Simplify data exfiltration cases with an artifacts-first approach



## IT GROUP

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.

## 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.



Magnet has revolutionized 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

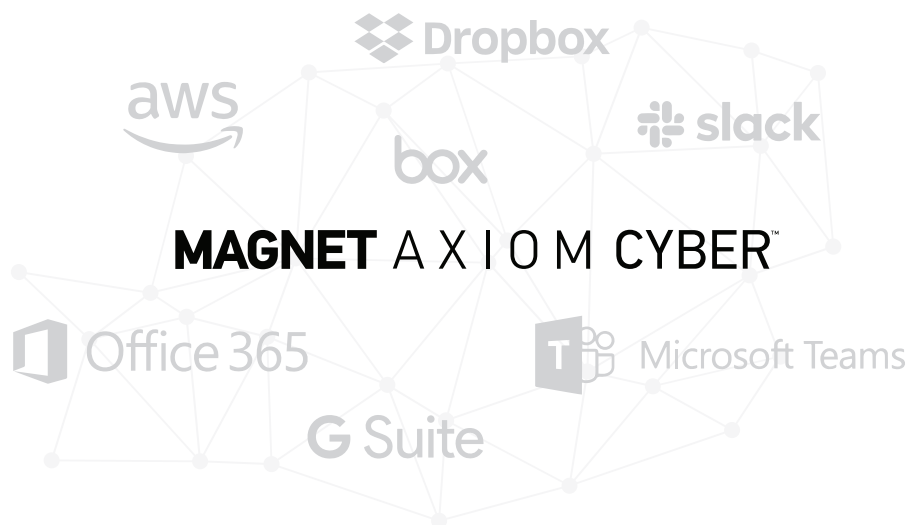
## HOW AXIOM CYBER HELPS

### ARTIFACTS-FIRST

AXIOM Cyber's artifacts-first approach immediately presents evidence from the file system and memory from as well as other evidentiary sources if available like mobile devices and cloud services. This approach quickly arms investigators with the all artifacts they need to ensure that the investigation moves as quickly as possible.

AXIOM surfaces many essential artifacts commonly needed in an IP Theft investigation, such as LNK files, USB history, Shimcache, emails, shellbags, and enterprise cloud services like AWS or Azure.

Evidence is not just restricted to one source like computers, or mobile devices, or the cloud. Rather evidence is inevitably interspersed in each of those sources. And this is definitely true for IP Theft cases. A bad actor will often move documents or files to multiple locations to try to conceal their tracks. It's crucial to follow the evidence as it moves and likewise to acquire from each of those sources. With Magnet AXIOM Cyber, you can acquire evidence from computer, mobile, and cloud sources with the ability to analyze all the evidence in a single case file which makes the presentation of artifacts quick and easy.



### SEE AXIOM CYBER IN ACTION FOR YOURSELF

If you'd like to learn more about Magnet AXIOM Cyber and how it can help you simplify your remote forensic investigations, visit [magnetaxiomcyber.com](https://magnetaxiomcyber.com). While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM Cyber expert, and request a free trial version.

Learn more at [magnetforensics.com](https://magnetforensics.com)

Book a demo today, call us at 1-844-638-7884 or email [sales@magnetforensics.com](mailto:sales@magnetforensics.com)