



# Faster, Easier Corporate Investigations

## Magnet AXIOM Makes Obtaining a Variety of Artifacts More Efficient

### THE CHALLENGE

MSA forensic examiners need to acquire and parse a variety of artifacts associated with insider threats including intellectual property and trade secret theft, and employee misconduct including misuse of company resources. Email, Microsoft® Office® 365 documents, messages found in Skype for Business and Slack, and even browser plugins can all contain needed evidence.

Such a diverse range of artifacts isn't without challenges. For starters, they can take a long time to process. In addition, cloud services and encrypted machines or devices can make it difficult to acquire data. Even having acquired data, it's not always easy to conduct the kind of root cause analysis that can demonstrate malicious intent versus inadvertent access.

### COMPANY OVERVIEW

Mine Safety Appliances Company, a global organization on the S&P 500, develops, manufactures, and supplies safety products for people and facilities in the oil and gas industry, the fire service, construction, mining, and the military. These products include self-contained breathing apparatus, fixed and portable gas detection instruments, helmets and head protection, and fall protection devices.

“ [AXIOM] is truly a one-click solution vs. one of the competitors you have to process (takes a very long time) and then run scripts to find everything you are looking for. AXIOM is easy to use for a majority of high-level investigations.”

— Tony LeDonne, Digital Forensic Examiner, Mine Safety Appliances Company

## HOW AXIOM HELPS

AXIOM's ability to retrieve data from the cloud using Office 365 administrative credentials means that investigators don't need to ask the subjects of their investigations for system passwords. They can conduct a covert search without the user knowing it.

This kind of search allows investigators to quickly find internet artifacts including Torrent files, web pages, and chat. These artifacts give MSA's forensic team access to important evidence—including inappropriate web content and messages—faster and more easily. The installation of browser plugins can show intent, while messaging and email can be evidence of conspiracy.

Further, Office 365 administrative credentials make it possible to pull audit logs and metadata so an examiner can learn when files were accessed, which IP address they were accessed from, and whether changes such as modifications or deletions occurred.


### EVIDENCE SOURCES

#### CLOUD PLATFORM AUTHENTICATION

I have proper search authorization to access the target's information stored in the cloud.

Warrant number

To obtain evidence from a cloud-based social media platform, you must sign in with the target's user name and password.

PLATFORM	SIGN-IN STATUS	USER ACCOUNT	LAST ACTIVITY (UTC)	ACCOUNT SIZE
 Office 365	SIGNED IN	John.Doe@office.com	8/23/2018 2:39:25 PM	4688.59MB

## SEE AXIOM IN ACTION FOR YOURSELF

If you'd like to learn more about Magnet AXIOM and how it can help you run smoother investigations, visit [magnetforensics.com/magnet-axiom](https://magnetforensics.com/magnet-axiom). While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM expert, and request a free 30-day trial version.

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

For more information call us at 1-844-638-7884  
or email [sales@magnetforensics.com](mailto:sales@magnetforensics.com)