Mobile Forensics' Life-Saving Capabilities

How Magnet AXIOM Ties Digital Artifacts to the Suspects Who Created Them

THE CHALLENGE

Smartphones are the main source of evidence in 75 percent of the TTPS forensics lab's cases, so they encounter several main challenges.

First, unknown or hard-to-find artifacts are the result of the rapid pace of change in the mobile app development industry. New apps, updated versions of existing apps, new features, and other changes can all mean that forensic tools' support for apps can be inconsistent.

Second, password protection on encrypted devices can mean that examiners may need to be able to capture evidence from more than one data source, or use more than one tool to try to acquire locked devices.

AGENCY OVERVIEW

The Trinidad and Tobago Police Service (TTPS), located in the West Indies of the Caribbean Sea, operates in both civil and paramilitary capacities. Digital forensics supports the TTPS' nine divisions and 18 branches, squads and units with investigating crimes including Internet crimes against children (ICAC), homicide, and offenses related to drugs and gangs.

> "[AXIOM] has helped solved several cases and saved a life. I was able to easily show chats between a victim and suspect in a child exploitation case and prove the use of a specific Facebook ID by the suspect which was found on his phone."

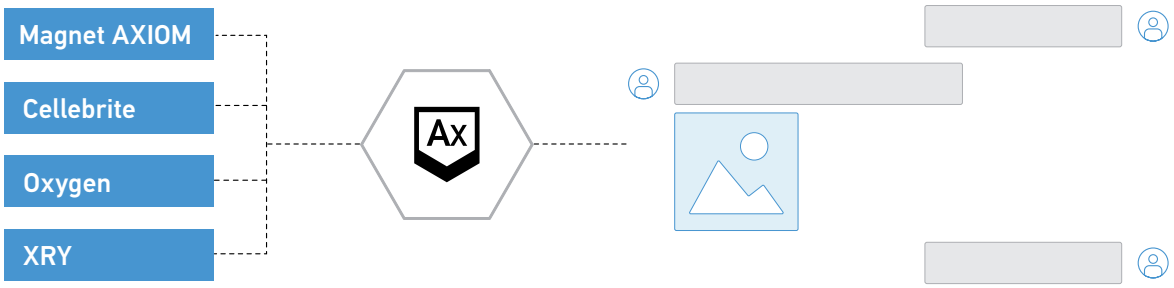
— Marvin Walker, Digital Forensic Investigator, Trinidad and Tobago Police Service

HOW AXIOM HELPS

When acquiring data, use AXIOM to not only get difficult-to-find artifacts from unsupported mobile apps, but to find more evidence from deleted or unallocated space, and carve and display key data — such as chat and internet browsing history. It's also about finding more evidence from deleted or unallocated space, and carving and displaying key data such as chat and Internet browsing history.

When dealing with locked smartphones, TTPS examiners rely on AXIOM's ability to easily ingest phone extractions from other tools—and to acquire data from other, synced sources, which AXIOM can then combine with mobile images into one case.

From there, AXIOM carves deleted, encoded, or encrypted data that other tools don't find in the file system or through a binary keyword search. When this data consists of chat evidence from social media or apps such as Facebook and Facebook Messenger, AXIOM rebuilds it into easy recognizable chat bubbles that are easy to present to any nontechnical stakeholder.



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. 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

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

MAGNET FORENSICS®