



MAGNET
FORENSICS®

Magnet AXIOM's Focus on Artifacts Leads to More Evidence

How Finding Nearly Twice as Many Forensic Artifacts Closed a High-Profile Cyber Threat Case in Taipei

THE CHALLENGE

Starting in October 2016, the Facebook page of Taipei City legislative councilor Ms. Wang was barraged with verbal abuse, harassment, bombing threats, and indecent pictures from nearly 200 false Facebook accounts.

After analyzing more than 300 sets of data and comparing that evidence to a targeted list of possible suspects, the culprit was identified and arrested. Regardless of the outcome, the Taipei CID faced multiple challenges including:

- Limited cooperation from Facebook to help identify IP addresses and respond to investigative requests in a timely manner
- Discovering critical evidence due to the suspect's use of a VPN
- No direct evidence found on the suspect's computer during the preliminary digital forensics investigation

Eventually police discovered a keyword match for "Karasawa Takahiro," which matched one of the harassing Facebook accounts, in the suspect's browser history. Evidence related to bomb threats at the Central Party Office of Kuomintang and records of suspicious VPN usage were also discovered on the suspect's computer.

AGENCY OVERVIEW

The 400+ officers of the Criminal Investigation Division (CID) of the Taipei City Government Police Bureau (CIPB) are responsible for:

- Investigation, detection and prevention of cybercrime
- Information research and development
- Intercepting communications activities
- Procuring equipment for investigations

HOW AXIOM HELPS

The first time the Taipei CID used Magnet AXIOM, investigators immediately achieved a breakthrough. Not only did AXIOM process all the case data in less than 6 hours; it also successfully recovered the key deleted evidence that proved criminal intent.

Overall, more than 860,000 photos and related digital records were recovered by AXIOM. This number is significantly larger than the 450,000 photos found by forensic tools which the CID used previously. In fact, these extra artifacts turned out to be what the CID needed to prove their case. The suspect, who initially denied the charges, ended up pleading guilty after seeing the evidence that AXIOM recovered.

Deputy Captain Hsieh was extremely satisfied with AXIOM's intuitive user interface, as it significantly minimized training time enabling investigators to hit the ground running and focus on analyzing the evidence. He said: "AXIOM has found all the data from the deleted sector and sorted it into different categories. The key information is all here. AXIOM emphasizes the feedback of practical experiences and is able to respond to the users' demand speedily. It is a powerful tool in digital forensics."

Learn more at magnetforensics.com

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

© 2018 Magnet Forensics Inc. All rights reserved. Magnet Forensics®, Internet Evidence Finder®, IEF®, Magnet™, AXIOM™, ACQUIRE™, Magnet. AI™ and related trademarks, names and logos are the property of Magnet Forensics and are registered and/or used in the U.S. and countries around the world.

