ADF

Triage-Examiner Provides Quick Access to Closed Devices for Forensic Examinations

Challenge:

No. #1: The Miami-Dade Police Department's Digital Forensic Section was experiencing an increasing backlog in processing computer and other digital devices due to hard to access hard drives. The lab averages over 400 cases a year, with anywhere from one to dozens of digital devices per case. The laboratory examines more than 2000 media items a year, with this number growing exponentially. Not only was the sheer volume increasing, but (1) more devices were of closed (sealed) architecture, and (2) new miniaturized drive configurations were making it difficult or impossible to remove the drives for a traditional forensic examination.

As a result, traditional methods of data acquisition from the devices had become cumbersome if not impossible. In addition, there is a significant risk of damaging the devices when attempting to remove the drive. If a device is damaged during an examination from a "non-suspect" computer, the lab may be required to fix or replace it.

No. #2: Detailing the registry contents into a report was time consuming for the forensic teams using traditional forensic software. Entries from user information, Internet search and browsing histories, browser map search history, USB device history, and other key registry data had to be manually determined for the reports. This was cumbersome and time consuming.

The Solution:

No. #1: By using Triage-Examiner from ADF Solutions the lab was able to extract the data from 90% of all the computers containing "difficult to access drives" without extracting them. This is because Triage-Examiner was specifically designed to access computers running Windows, OSX and Linux. It is also one of the only solutions that can easily access Mac Air Books and similar devices. Using Triage-Examiner, the forensic teams are able to access the drive contents without having to remove the hard drive or risk damaging the device.

No. #2: The automated reporting process in Triage-Examiner was able to list all of the required information in an HTML or MS Word report template that was easily shared with investigators involved with the case. This saved them a lot of valuable time and resources.

The Result:

By eliminating the need to remove the drive from the device and applying a forensically sound automated triage solution, the lab was able to dramatically save time and resources:

- Increase the number of successful data acquisitions from "hard-to-open" devices to 90%.
- Reduce the decision time to send the device for a full forensic examination.
- Quickly share the triage results with case investigators through automated reporting.
- Eliminate the risk of device damage and the associated liabilities.

CASE STUDY