

AD Triage

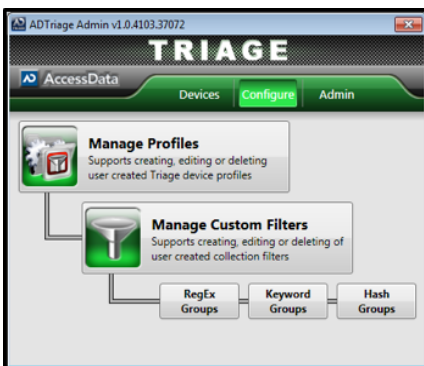
Preview and Collect Targeted Data
in Minutes

Forensically Acquire Data from Both Live and Shut-down Computers in the Field

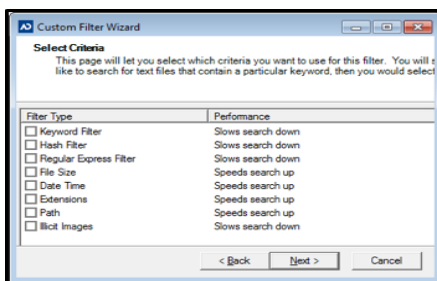
It's like carrying the power of FTK® in your pocket...



Easily manage your Triage devices.



Configure collection profiles and
manage filters.



Create filters using your own criteria.

Built on FTK technology, AD Triage is a portable computer forensics solution for use in the field. Forensic examiners and non-forensic personnel alike can acquire volatile and all or targeted hard drive data from a system in just minutes. It's a great option for corporate and government teams who often need to acquire data from live or dead boxes for internal investigations, FOIA or even subpoenas. Law enforcement officers can preserve evidence securely without having to wait hours for a forensics expert to arrive on scene. Finally, attorneys, paralegals and litigation support personnel can easily preserve ESI for the purposes of e-discovery when handling smaller legal matters.

Using AD Triage, you can search for and preserve data by criteria, including keyword, hash, regular expression, file size, date and time, extensions, file path and illicit images. In addition, users can collect network and system information, as well as memory. It allows you to acquire the full disk, a volume, or peripheral devices, saving data to a USB device, an external hard drive or exporting it to a designated location on the same network. Preconfigure your AD Triage device to automatically acquire only the data deemed necessary, allowing inexperienced users to safely and effectively use the tool. Or you can use AD Triage in manual mode for true triage on the fly.

How Does AD Triage Make On-Scene Acquisition Easier?

- Easily preserve volatile data, which is lost if the computer system is shut down.
- Supports shut-down Apple® computers that have Intel® processors.
- USBs can be programmed to auto-collect according to collection profiles.
- Auto-export data collected from the target system to a designated location on the same network.
- Create AD1, EO1, RAW, or SMART images of collected data.
- No need to carry a laptop and write blocker.