CASE STUDY

ACCESSDATA®

Finding the EZ-button for Targeted Collections with AD Triage

Background

A leading global water and wastewater treatment company decided to adopt AccessData's Triage solution—an intelligent data preview and acquisition tool. The water management company found AccessData's solution comprehensively addressed their need to perform remote in-the-field data collections. The following analysis reviews the findings and the benefits the organization achieved as a result of implementing AccessData® technology.

Introduction

As the world's leading supplier of water and wastewater treatment products, as well as systems and services for industrial and municipal customers, this company is relied on by millions of people and thousands of companies to meet their clean water needs. In terms of size, this company has over 200 offices, plants and factories in seven countries, and a workforce of 5,500 employees. In the U.S., it is estimated that 85% of the population is located within 100 miles of one of the company's technology service branches. This water treatment company differentiates itself from competitors by serving as a single-source provider that can design, manufacture, finance, operate, maintain and manage all manner of water and wastewater facilities, systems and operations. However, dealing with the world's water supply can expose the company to many civil, toxic tort and regulatory lawsuits.

LOST PRODUCTIVITY COSTS: REPRESENTATIVE FORMULA

Onsite Collection	Collection via FedEx®
32 Cases X	32 Cases X
6 Custodians X	6 Custodians X
2 – 4 hrs (range collection time) X	8 – 24 hrs (range collection time) X
$100/hr =	$100/hr =
$38,000 – $76,000	**$153,000 – $460,000**

Why AD Triage?

Even as a leader in the area of water reclamation technology, the company is faced with the daily grind of managing a very large, dispersed and fragmented enterprise network and mobile workforce without infinite IT resources—like so many of today's global organizations. When litigation occurs and data collections are required, the responsibility falls on the Global Information Security Officer (GISO). Working closely with the company's outside legal counsel, the GISO and his team begin the meticulous process of determining what constitutes relevant data and which employees/custodians are in possession of it. Once the custodians and scope of data are determined, the task of actually acquiring that data takes center stage.

Historically, the organization relied on employees to physically deliver relevant assets, such as laptops and mobile devices, or an investigator was sent into the field to collect the pertinent data.

Both approaches are far from efficient and result in "mixed results." Physical delivery of assets impacts productivity and—to some extent—morale. Those costs, when extrapolated out over a year or more, can be critical for many organizations. When circumstances or case requirements dictate an investigator travel to the employee's location, the travel costs alone can be significant for a global operator. Furthermore, the investigator is effectively out-of-band for the duration of the trip.

There can also be challenges relating to data integrity and format when forced to send staff to perform an acquisition—especially if that staff is inexperienced. In these instances, questions may arise relating to proper chain-of-custody procedures and/or scope of the data itself. Organizations should no longer be faced with tough decisions relating to data integrity and the incremental costs of doing an "OK" job versus doing the job right. This water treatment company made a commitment to do the job right every time, without question.

Looking Ahead

With neither of the aforemention approaches resulting in very much efficiency, the GISO reached out to his outside legal counsel for direction. The question he posed was, "Is there a way to effectively collect data from target custodians that doesn't rely on a knowledgeable end-user, is inexpensive, and doesn't require meaningful network connectivity." To assist their client, the firm reached out to AccessData in an effort to identify a solution.

Ironically, AccessData's AD Triage solution was designed to resolve this exact challenge. AD Triage is an easy-to-use, forensically sound, data acquisition solution. Built on FTK® technology, AD Triage is ideal for users who are inexperienced with more complex data collection products. In this particular case, the GISO and his team obtained a demo license of AD Triage and after thorough review and testing provided the following feedback:

> *"I have finished my review of Triage and was pleased enough with the solution that I bought two licenses. I have configured Triage to boot from an external (2 terabyte) USB drive and collect a physical drive image with very little interaction needed on the employees' side (just two button clicks after selecting the boot device).*
>
> *This solution will greatly benefit my collection efforts in a couple of ways: 1) Allow the employee to keep the target device in their possession longer—no shipping of laptops back and forth required (only the Triage device is shipped—collection happens overnight); 2) Save on travel costs sending an investigator to perform remote collections. Triage is incredibly close to the "EZ-button" we were looking for."*

AD Triage allows the water treatment company to preconfigure and automatically acquire only the data deemed relevant through filters that support keywords, hashes, regular expressions, file size, date and time, extensions, file path and even illicit images. With the pre-configuration option inexperienced users can safely and effectively use the tool with little need for explanation. In instances where investigators are involved, AD Triage can preview the file system to analyze the data and make onsite decisions. In either case, AD Triage can collect network and system information, as well as live memory a full disk, a volume, or peripheral devices, saving data to a USB device, an external hard drive or exporting the data to a designated location on the same network.

AccessData Group has pioneered digital forensics and e-discovery software development for more than 25 years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil e-discovery of any kind, including digital investigations, computer forensics, legal review, compliance, auditing and information assurance. More than 130,000 customers in law enforcement, government agencies, corporations and law firms around the world rely on AccessData® software solutions, and its premier digital investigations products and services. AccessData Group is also a leading provider of digital forensics training and certification, with its AccessData Certified Examiner® (ACE®) and Mobile Phone Examiner Certification AME programs. For more information, please go to www.accessdata.com.

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com

LEARN MORE
www.AccessData.com