Deloitte.

Remote Forensic Collections in the Enterprise Environment

Helping to address eDiscovery challenges: cost savings and efficiency

The marketplace continues to globalize as more and more businesses operate in multiple states and different countries. In many instances, businesses that operate in a single region have offices in more than one location, and even those with only one work site may permit (or require) telecommuting across a geographically dispersed work force. Within this context, managing electronic discovery and, in particular, collecting custodial data in the enterprise environment can be a daunting task.

Background

Traditionally, forensic imaging requires the physical availability of the machine to be preserved and the local presence of a forensic examiner. The hard drive is removed from the target machine and connected via a write-block device to the examiner's machine, onto which the data is copied to a forensic image. This process generally requires planning and coordination with building/security staff (to grant physical access to the examiner), the IT team (for discussing any machine technical aspects, such as operating system and encryption), and the owner of the machine (for obtaining possession of the target system). With traditional imaging, a forensic examiner can only image a limited number of systems at the same time, and the target machines are unavailable to their owners until the process completes. In the enterprise environment, this can require substantial efforts to efficiently schedule multiple collections and reduce business disruption.

On the other hand, remote imaging often can alleviate many of the logistical hurdles involved in traditional imaging. For example, remote imaging does not require the examiner to be in the same location as the machine from which a collection is to be made. It also does not require making the machine unavailable to its user during the collection process. A small piece of software (called an agent) can allow accessibility of the target machine to the collection tool, which pulls the data over a network and creates the forensic image on the examiner's machine. Thus, the target machine user does not necessarily need to give up possession of the computer. In fact, the remote imaging process can be invisible to the user and may not require any actions by the user to allow the process to run and complete.

There is one exception, however: remote imaging requires the target machine to be up and running and connected to the network. For obvious reasons, network speed and reliability are fundamental for a fast and effective remote collection. Slow network speeds can cause longer collection times, and logical or physical network problems can cause collection interruption or failure. Moreover, enterprise networks are typically protected by a firewall, and so it may be necessary to configure the proper port exceptions to allow the connection between the target machine and the collection tool before the remote preservation can start.

Application

Common targets for remote imaging include laptop and desktop computers, servers, network shares, and enterprise applications. Preserving ESI from a target machine without interrupting its availability to the user is a significant advantage in terms of reducing the inconvenience that traditional, on-site collections can cause for a company and its personnel. This aspect is particularly important for preservations involving a server or enterprise application. In these situations, system downtime can affect a large population and/or critical business functions (i.e. shutting down an email server to collect a user mailbox could cripple email communication for an entire company). For remote server collections, just as it is required to install the collection agent on computers, it is necessary to create a special service account with read access to the target data on network storage servers and enterprise services. While this aspect of remote collections does involve some level of coordination with IT administrators (for obtaining specific technical details of the enterprise logical infrastructure and required access permissions), it is generally far less time-consuming and disruptive than on-site collections.

In many contexts, the invisibility of the remote imaging process is not only desirable for business continuity reasons, but also vital to preservation. For example, a fraudster may attempt to destroy data before a pre-announced forensic collection. There is less risk of this type of strategic behavior with remote collection, because the collection may not need to be announced in advance (this will depend on applicable privacy laws and an enterprise's own privacy and related policies). Likewise, a team of forensic examiners setting up forensic imaging hardware in an office environment may create undesirable reactions and/or tip-off fraudsters about an ongoing investigation. Installing a collection agent on the target machine often can be a silent operation, as the small program can be pushed to the machine in the same, discreet manner that periodical security updates are pushed to the company's machines.

Benefits

One of the biggest advantages of remote collection is quick deployment. The collection can start right after the agent software is installed on the target machine or system, from virtually anywhere in the globe. This bypasses travel time, arrangements, and costs associated to the deployment of personnel and physical resources to remote locations. Moreover, it allows simultaneous collections on multiple machines in different locations, an especially valuable advantage for collections involving a large number of machines, multiple international locations, short turn-around time requirements, and budgetary limitations. Once the initial configurations are in place (firewall configuration and agent installation), a collection can be resubmitted multiple times with ease. This simplifies periodic recollections of a specific target and re-execution of collections that may not have completed.

These aspects of remote collections also can be beneficial in terms of consistency: by remotely performing the collections from a centralized location, having fewer examiners involved, and having an easily repeatable process, one could expect greater consistency in imaging naming conventions, notes, and documentation. Moreover, when using an enterprise remote collection tool, forensic images can be saved to a single storage location (generally a large storage server), thereby simplifying organization, management, and retrieval of the collected data. Additionally, the forensic images are available as soon as the collection process completes. With traditional imaging, images taken in different locations will be stored in different hard drives that will have to be transported by the examiner or shipped to the discovery team before analysis and processing can take place.

Additionally, if the examiner performing the remote collection participates in the EU-US Safe Harbor certification program, the examiner may be able to transfer data from an EU member state to the examiner's U.S. system without it being deemed an outbound transfer under EU law. There will still be limitations on how the collected information can be used (processed), or transferred to others in the U.S. not participating in the safe harbor program. But the value and benefits of being able to collect information from multiple locations over great distances all at one time, and efficiently place those collections on one system, should not be overlooked.

Remote imaging is generally performed via targeted logical images. Indeed, while network and internet speeds have exponentially improved in recent years, volumes of electronically stored information have grown at an even faster pace: today, virtually all business communications and documents are kept in digital form. Collecting terabytes of data over a network is not normally a feasible option but, in certain cases, targeted logical images may offer an acceptable alternative. A targeted logical image allows

collection of files of interest, often based on file creation/modification date, custodian, and/or file extension. Depending on the scope of discovery, this strategy can considerably reduce cost and the volume of data to collect while still satisfying a party's legal obligations.

Remote collection is not perfect, however. One of the major objections to remote collection in favor of traditional imaging is the comparison between logical and physical forensic images. In short, a forensic physical image preserves the entire hard drive, while a logical forensic image collects only selective content. Without delving too deep into the technical details, physical images include all active content, unallocated space, and non-partitioned space of a disk. In some situations, unallocated and non-partitioned space can be an important source of information, particularly in cases involving suspicions of file deletion and/or disk re-formatting. Conversely, logical images preserve only active files and do not include unallocated or non-partitioned space. Nevertheless, logical forensic images may be sufficient in many situations, even though physical forensic images are generally preferable and required when forensic analysis is needed. As for pure forensic defensibility, both logical and physical images are suitable and can be forensically matched up with digital fingerprinting techniques such as MD5 hashing.

The debate between logical and physical images is alleviated to some extent in situations involving encrypted computers. When decrypting a hard drive is not a feasible option (where, for example, the decryption key is not available or the encryption technology requires unique and unavailable measures), it is generally acceptable to acquire a logical image of the live system. Similarly, certain RAID systems can only be preserved via a live logical image. In these situations, traditional imaging and remote imaging will produce the same result: a logical image of the system.

As targeted logical images do not collect the entire data population, it is necessary to understand the specific issues in a given case and the party's related legal obligations, to determine if full physical preservations are required. Similarly, as noted, a number of countries have strict privacy regulations that protect personally identifiable information (PII) (and take a very broad view of what constitutes PII subject to protection). EU privacy laws, for example, require the specific consent of the data owner before it can be collected, and strictly regulate how and under what circumstances PII can be processed and transferred. In cross-border situations, targeted collections very often will be preferable to full collections as the volume of data deemed to be processed will be limited.

Considerations

Remote collection platforms can be costly to acquire, implement, and maintain. As discussed in the previous paragraphs, there are also technical, operational, and legal issues to evaluate before choosing specific solutions. In fact, it is not uncommon to come across enterprises that acquired remote collections solutions that did not meet their specific needs. Therefore, the requisite proficiency and guidance are key factors for the effective utilization of remote collections in the enterprise environment, and experienced professionals with specific technical, professional, and experiential knowledge should assist the enterprise during the process.

In each of the key phases of adopting a remote collection platform, having the appropriate skill set for implementation can help reap the full benefits of the platform's capabilities.

Key Phase	Crucial skill
Planning	• Analyze the underlying legal issues, the specific data to be collected, and the relevant IT environment • Conduct feasibility studies
Acquisition	• Translate eDiscovery needs into essential operational key functions • Compare and select best-fitting solutions
Implementation	• Facilitate coordination between IT team, platform users, and vendor(s) technical support team • Customize platform to achieve specified needs
Operation	• Design effective and defensible operational procedures and QC strategies • Develop rigorous solutions to handle exceptions and special cases
Management	• Understand and utilize platform functionalities fully • Continuously reassess efficiency and accuracy of collection/processing/export processes

Conclusion

Targeted remote imaging represents a potentially valuable solution in a modern, globalized enterprise environment. As with the use of any technology, there are many factors to consider before selecting and investing in a specific solution. In addition to technical considerations, legal and regulatory issues play an important role. Ultimately, with the appropriate guidance, global enterprises can adopt remote forensic collection procedures, in addition to traditional imaging, to meet their eDiscovery needs and achieve cost savings and increased responsiveness.

Authors:

Marco Ore
Discovery Manager
Deloitte Financial Advisory Services LLP
more@deloitte.com
+1 281 216 9018

Jon M. Talotta
Partner
Hogan Lovells US LLP
jon.talotta@hoganlovells.com
+1 703 610 6156

References

- Directive 95/46/EC, Official Journal L 281 p.31 of 23.11.1995
- Decision 2000/520/EC, Official Journal L 215 p.7-47 of 25.08.2000