Encrypted Hard Drive Dangers

August 21st, 2008

You have requested a hard drive clone or image and discover that the contents cannot be culled or reviewed. One reason may be hard drive encryption. Encryption involves ”scrambling” the contents of a file or hard drive so that they cannot be viewed without the appropriate key or password.

To secure data, companies and individuals are increasingly encrypting the contents of their hard drives or USB flash drives. Manufacturers are also building hard drives that automatically encrypt the contents. BitLocker encryption, for example, is available in Windows Vista. Hard drive encryption often requires a ”live” acquisition, which takes place when the system is running and the decrypted contents of the drive can be accessed and copied. Employing best practices, which handles hard drive encryption, is important and will increase in the months and years to come as encrypted hard drives become more common. Here are a few pointers:

1. Ask the IT contact if any known encryption method is in place.
2. Computer forensic examiners have tools, such as X-Ways Capture, which will detect several encryption methods.
3. If drive encryption is identified, create a live image of the system. Creating a live image can take several times longer than a normal acquisition.

Encrypted hard drives pose a challenge and potential delays for both computer investigations and electronic discovery processing. Work with a vendor who is capable of handling encrypted hard drive collections.