THE IMPORTANCE OF MEMORY FORENSICS IN FRAUD INVESTIGATIONS

The use of dynamic data and encryption technology through gathering digital evidence are valuable methods of helping to crack down on fraudulent activity

Technology continues to proliferate in our day-to-day lives, introducing new challenges in how data can be accessed and analysed, as well as new opportunities for fraudsters to disguise their wrongdoing.

With this technological evolution, the reliance on electronically stored evidence to prosecute or defend fraud investigations is now a well-established norm, and digital forensics, the forensic science dedicated to securing, recovering and analysing material found on digital devices, has become an essential aspect of modern-day fraud investigations.

Persistent data

Digital forensics has traditionally relied on capturing and analysing persistent data. Common examples of this include user-created documents, spreadsheets, emails and pictures, all of which can be stored on hard drives, servers or external devices.

While persistent data is key for any digital forensic investigation, it is not the only source of data that should be considered, particularly for fraud investigations.

Digital evidence

Another equally valuable source of digital evidence is dynamic data, which is information that is periodically updated and may be inactive over a period of time, such as computer memory (commonly known as Random Access Memory or RAM).

Digital evidence located in RAM temporarily holds data that is being used by a computer's internal processes. This can include traces of processes that are currently running, private browsing history or even cryptographic keys.

While RAM is a potentially rich source of digital evidence, it is also volatile – when the computer is powered off, all data stored in RAM is lost. If this is not considered during the forensic collection, these ephemeral data sources can frustrate or even block further analysis.

Dynamic data

During a recent investigation our team located a password-protected file that we were not able to crack using traditional forensic tools.

Knowing the computer's RAM had been preserved, we were able to create a word list from the memory and then use that list to decrypt the protected file. Without access to the dynamic data from that computer we may not have been able to open that document.

The use of disk encryption is another example of how dynamic data can potentially aid an investigation. Encryption technology is increasingly used by IT departments to help secure corporate assets.

BitLocker

Microsoft Windows now includes a feature known as BitLocker that encrypts all data on the drive when the device is powered off. Without the correct decryption key, any data on that device cannot be accessed.

We encountered this scenario recently and were able to locate the decryption key in the computer's RAM and decrypt the drive, thereby allowing our investigators access to a trove of relevant data from that device.

Planning ahead

Other data that may reside in RAM can include data that has been copied and pasted from one document to another, email fragments from web-based email or cloud storage access.

All of these sources of digital evidence are commonly used by fraudsters to commit and hide their activity and all are easily captured with advanced planning.

By including memory analysis as a forensic component of a new or ongoing investigation, you will gather more data that may relate to fraud and possibly even prevent a fraudster from hindering your investigation.

Russell Miller, senior director

William Odom, director

FRA 20 YEARS ANNIVERSARY

2550 M Street NW, Washington, DC 20037, United States

Tel: +1 (202) 627-6580 **Email:** rmiller@forensicrisk.com, wodom@forensicrisk.com

Web: www.forensicrisk.com