LAWYERS JOURNAL

Forensics from a distance – defensible collection of remote data

By Brett Creasy and John Unice

Defensible collection of evidence is the critical foundation to the successful prosecution or defense of every case. Whether that evidence is a blood covered glove or a fleeting digital transmission from a computer, without preserving evidentiary integrity, the collected information does not become *evidence.* So, what are some of the best practices, practical steps and even missteps which every lawyer should be cognizant, particularly when it comes to electronic evidence that must be preserved remotely? Following some of the key evidentiary practices discussed below will help lawyers navigate the sometimes-murky waters created by key electronic evidence that, due to either its ephemeral nature or other logistical challenges, must be collected remotely.

Relevant and Authentic

Of course, a key tenet of entering evidence at trial is taking the right steps to ensure that it satisfies the evidentiary strictures governing relevance and, key to our discussion, authenticity, i.e. the offered item is what the offeror claims it to be. In the context of electronically stored information (ESI), examples might be an email or other form of electronic document, a log file generated by the operating system of a computer or a text message that is stored in a database found on a mobile phone. The most common method to prove that a piece of ESI is authentic is to show it was collected using appropriate methods for the ESI in question and establish that it has not been altered in any way. The use of hash values, such as MD5 hashes, which are sometimes called "digital fingerprints," is a popular way to help meet that burden. In fact, amendments to FRE 902 designate that ESI can be "self-authenticating" in some circumstances, a topic we at bit-x-bit have covered previously (see *https://bit.ly/2F5iJZ9*).

Typical Methods for Collecting ESI

A common ESI collection method is to hand over the physical device on which the ESI resides to a digital forensic specialist, so that chain of custody can be properly documented and the ESI can be electronically collected with appropriate methods, which typically results in the hash value described above. But what happens when devices or data sources cannot be physically collected by counsel or provided to a forensic firm? Even before COVID-19 forced the world into remote-work scenarios, for example, litigants have had a need to preserve ESI from corporate business servers that could not be shut down (and then physically sent out for imaging), third-party web-based services that the client could access but didn't own, negating the ability to provide the data directly to a forensic firm, and traveling employees who couldn't surrender work devices that served as the only means of conducting day-to-day work. For those remote-collection needs, different methods may be necessary.

Methods for Collecting ESI that is "Remote"

The good news with remote ESI is that most of the same principles of how to go about collecting it still apply. Data maps can still be built, albeit with slightly more complexity, and many of the same tools used to capture a laptop in a forensic lab can be used to tackle a laptop that is across the country. Third-party providers such as Onna for Slack data and X1 Social Discovery for social media accounts are also catching up to the needs of the legal industry and are building tools and processes designed to facilitate the collection of ESI for legal proceedings. Some other practical examples of remote options include:

- Shipping a USB hard drive that contains forensic collection software to the target custodian, and then follow up with a phone call and remote screenshare session between the custodian and a forensic consultant to collect the data.
- A forensic consultant can utilize a combination of collection tools to access cloud-based repositories such as Dropbox, Google Drive and others for data collection.
- Built-in tools such as the eDiscovery features of Microsoft 365 may be leveraged to collect emails, Microsoft OneDrive data and other data stored within Microsoft services.
- Because business-class services often have additional features not available in free or personal versions of the same service, in addition to the actual data or "documents," logs and other ancillary information may be available to address actions the user took while signed into the service, e.g. sharing of company documents or deleting data.

It is important to point out however, that all solutions are not created equal. For example, the search capability of a built-in tool of a service provider such as Microsoft or Google may not have the robust features or auditing and reporting capability necessary for every case. Likewise, the act of collecting various ESI forms could impact the integrity of the data if not handled appropriately, i.e. metadata such as creation or modification dates, could be altered.

Properly planning for ESI collection is something every lawyer should be familiar with, even if the work itself is to be performed by properly trained in-house IT professionals or third-party forensic experts. Bar associations in many states, including Pennsylvania, have even adopted ethics rules imparting upon lawyers a duty of technical competence, which could certainly come into play with ESI collection efforts. The above examples provide a brief look into just a

few of the options available for remote ESI collections and should lead to more detailed discussions between the stakeholders to satisfy the unique needs of the case at hand. ■

Brett Creasy, CCE, CISSP is President and Director of Digital Forensics at bit-x-bit LLC. John Unice, Esq. is Executive Vice President and General Counsel at bit-x-bit LLC.