ARTICLE:

PRACTITIONER NOTE

PRESERVING CYBER INVESTIGATION EVIDENCE: THE SCREEN TOOL WITNESS SIGNATURE

By **Benjamin Wright**

Commonly, a cyber investigation examines how a digital resource, such as an application, a hyperlink or a web search box – works. For example, the investigator observes that when mouse clicks on hyperlink 'X' browser goes to a web page containing 'Y' content. The investigator observes how a resource works. The investigator wants to record what he sees and hears. He wants the recording so he can establish to a third party such as a court what the resource did at the time of the investigation. Without a recording, valuable evidence can disappear. A web page or a Facebook wall, for instance, may display one thing now and something different five minutes later.

The question is how an investigator preserves a competent recording of what is observed and heard.

These notes compliment a video located at http://www.youtube.com/watch?v=UgH6hzwAg5Y.

The video demonstrates a method of recording how digital resources look and perform at a particular time. It makes a 'screencast' record of what emerges from the investigator's browser as he uses digital resources such as hyperlinks. It further demonstrates how to authenticate the record as the verifiable, legally-signed work and testimony of the investigator.

The video brings together two simultaneous video records: a screencast of what appeared through the investigator's browser as he clicked and typed, and a webcam image of the investigator observing and talking in real time as the screencast was captured.

The split-screen video product makes for compelling, easy-to-understand evidence. Arguably, it constitutes a legal affidavit by the investigator.

To capture these two records into a single movie, software called BB Flashback was used.

The movie depicts the investigator (John Smith) reading prepared remarks (i.e., his testimony as a witness) on camera, as he looks at written notes off to his right. This seems odd because he is not looking into the camera the way Hollywood might prefer. But this is not Hollywood. This is evidence destined for a court. The investigator is reading and recording his testimony.

Notice that the investigator looks to his left briefly to confirm time on a clock before he speaks the time.

Notice that the demonstration movie achieves its status as a verifiable, authenticated, legally-signed digital record without relying on additional, future performance by the investigator himself. By this is meant the existing conventional practice of computer investigations. After an investigator captures a record as a file, under conventional practice she applies her 'digital signature' to authenticate the file as evidence she has secured.

Digital signature

In the demonstration video, a digital signature was not used because a digital signature can be problematic, for the reasons noted below.

In classic implementations, a digital signature relies on a public key infrastructure (PKI). The digital signature involves the investigator holding, using and protecting a private key.

Verification of a digital signature after it is created depends on a wide variety of issues, such as proof that the investigator possessed the private key; possessed the relevant training for the use and protection of the private key; possessed the considerable resources needed to protect the private key, and in fact took adequate steps to protect the private key. Often in practice all of this proof requires the existence of a substantial and expensive infrastructure, which typically includes extensive records and a certification authority. This infrastructure raises numerous problems, such as:

1. The infrastructure can be corrupted.

2. The certification authority can make mistakes.

3. The certification authority can go out of business before its work is done (that is the certification authority can go bankrupt and stop supporting verification of the investigator's report before the report is used and verified in court).

Additionally, a digital signature depends on sustained work and cooperation by the investigator after the signature is applied to the investigation report. For the digital signature scheme to work, the investigator must continue to support the security of her private key. That requirement for continued support is risky.

For example, suppose the investigator works for XYZ Corporation at the time she creates the investigative record and signs it with a digital signature using her private key. Then suppose XYZ Corporation dismisses her. The investigator may be angry at XYZ. She may stop protecting her private key, or corrupt the historical records related to her key and its protection, or undertake both actions. She may refuse to provide any cooperation or testimony on behalf of XYZ when required in the future, or for an arbitration hearing. If she is really upset at being dismissed, she might compromise the security of her private key by publishing it on leaflets she distributes in Times Square. (There are ways to mitigate some of these risks, but they are expensive and entail their own risks.)

Webcam signature

Instead of using a digital signature, the demonstration movie employs a webcam signature. A webcam signature captures real time testimony by a signing party and links it to some evidence. In the demonstration video, the evidence to which the webcam signature is linked is the entire activity in the demonstration movie (activities in web browser, vocal observations by investigator, facial expressions by investigator and so on). A webcam signature records verbal and visually persuasive evidence of authentication. In the demonstration, it records the human investigator indicating his intent by using the unambiguous words 'I hereby sign and affirm this recording . . .' A jury will know what the investigator meant when it sees and hears these words.

Contrast this with a digital signature. A digital signature is inanimate. It does not explicitly express the intent of a human (the investigator). A digital signature is machine evidence that a certain key was used in the execution of a certain algorithm. It is possible that the members of a jury could have difficulties understanding the meaning of a digital signature.

E-mail for integrity

A good webcam signature could benefit from a bit of extra security that is not apparent in the demonstration movie. The additional security could comprise of the investigator sending a copy of the recording as an attachment to an e-mail, which in turn is addressed to a number of people. Those to whom it is sent could include (but is not necessarily limited to) the investigator, the investigator's manager and the attorney who is advising the investigation. In that way, a number of copies of the recording would be distributed, thus preventing the possibility of making any undetectable alteration. A webcam signature, supported by the records, controls, passwords and reliability in e-mail provides a record of authentication, the integrity of which is reasonably well assured.

Furthermore, a webcam signature is complete as soon as it is sent as an attachment to an e-mail. A good webcam signature involves the signing party (the investigator) stating on camera a date and time that match up with the timestamp on the e-mail. In typical e-mail systems, the timestamp, supported by appropriate logs and audit trails related to it, is outside the control of the different parties to which the e-mail is addressed. Changing or manipulating the timestamp would be detectable.

Hence, the webcam signature creates a trustworthy record that does not rely on future performance by a

certification authority or the investigator herself. The webcam signature is a direct, recorded video and audio testimony by the investigator.

Thus, the movie record can be considered to be a rough equivalent to an affidavit written on paper and signed in ink by the investigator. In other words, the webcam signature secures the testimony of an expert witness so that the testimony is available in the future, regardless of whether the witness is available or refuses to cooperate.

Offering as evidence

How might the investigator's split-screen video record be offered into evidence in a judicial proceeding? The precise methods can vary depending on the nature of the proceedings, the agreement of the parties, the purposes for which the evidence is offered and the formalities normally observed in the court. (In the US a federal court observes more formality than a county court, for example.) In some cases an American court could deem the content of the split-screen video to be hearsay that is inadmissible. Or, the court may forbid introduction of the video unless the proponent of the evidence establishes its scientific reliability under *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993) and related cases.

If the video is inadmissible as evidence, it might still serve as the notes or records of an investigator, which may be used to refresh the memory of the investigator as he testifies as a witness. Generally in the US, the notes of a witness may not be used to refresh his memory until his memory is exhausted through testimony. The purpose of taking his testimony is to ascertain what he remembers, not to ascertain the content of his notes. However, as he testifies, the witness may come to particular details that he can remember no further. He may then be presented with his notes so that he can refresh his memory. After refreshing his memory, he then testifies as to his memory, which is stronger because he has just examined his notes.

Any kind of relevant item can be used to refresh the memory of a witness. The item need not be notes written on paper. It could be a physical object, such as a gun. For purposes of refreshing an investigator's memory, his notes and records could be the split-screen video displayed to him, for his individual examination, on a mobile computer such as a laptop. Only he would see and hear the content of the video. To prevent others (such as the members of the jury) from hearing the audio portion of the video, the investigator might be required to wear headphones.

In some cases the split-screen video might be admissible into the proceedings as evidence. For example, even though the video is hearsay, it might be admissible under the "prior inconsistent statement" exception to the hearsay rule. (Some US jurisdictions recognize an exception to the hearsay rule for a prior, written and signed, statement that is inconsistent with the testimony taken of a witness.) If the video is to be admitted as evidence, the attorney offering it would usually need to lay a foundation for it with a sponsoring witness. The sponsoring witness would establish the relevance and authenticity of the video before its presentation in the court.

Many US courts today have equipment for displaying audio and video in open court. Commonly the proponent of audiovisual evidence would bring it as a file stored on a mobile computer, which would plug into the court's audiovisual system. In those courts that are not so equipped, the proponent would typically also bring the projector, screen and speakers necessary to present the video in court.

In a jury trial, a video admitted as evidence would normally not be available to the jury for review while it is deliberating in the seclusion of the jury room. If the jury desires to observe the video again, the jury would need to request the court for the opportunity. Then the video would usually be presented to the jury under supervision of the court and in the presence of the parties.

Comments

The author welcomes comments from the reader, either through the journal or directly.

The author thanks Stephen W. Harris, member of the Texas Bar Association, for help in understanding the practical steps in offering evidence into court proceedings. Benjamin Wright is a practicing member of the Texas Bar Association. He has a blog at benjaminwright.us.

