



CRA Insights: Forensic Services

CRA Charles River
Associates

December 2017

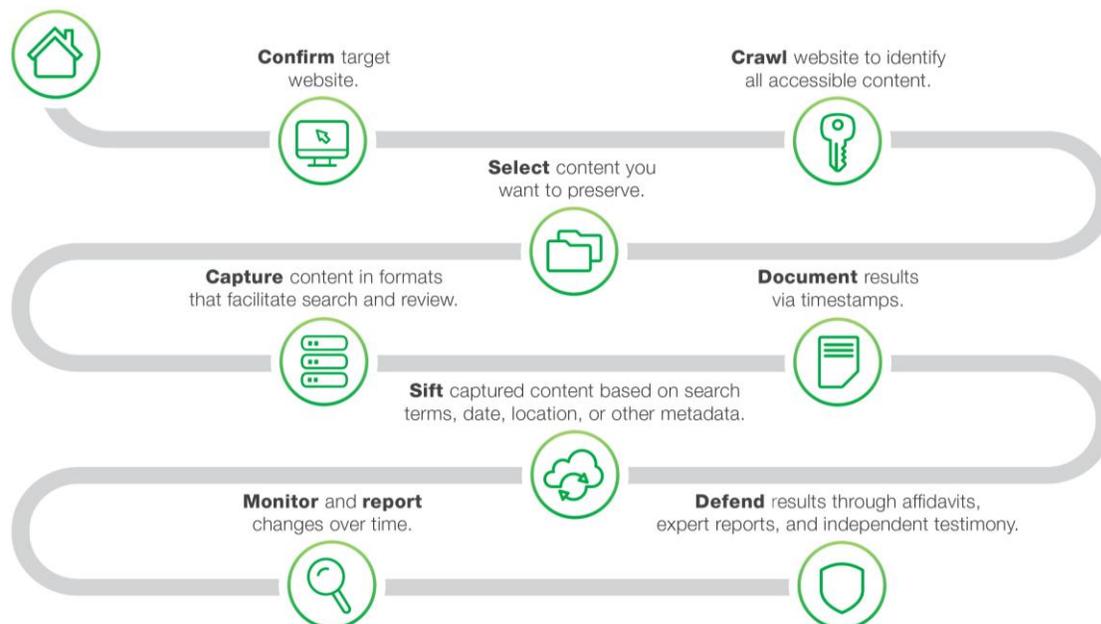
This article was included in the ACC's New York City Chapter Winter 2017 newsletter.

Strategic discovery considerations: preservation and analysis of web and social media content

Services to host and construct web sites abound, providing easy access to creating and hosting content online. However, the increased use of the Internet to share information poses issues for attorneys and their clients regarding the investigation and discovery of web sites, social media, and other Internet-hosted resources.

The methods used to capture Internet-hosted information can vary, and as such, there are preferred methods for capture that help validate the authenticity of the information captured.

Preserve and search dynamic websites and social media.



Capture, sift, document

A web site is effectively a collection of files transferred from the hosting location, and assembled in a particular order by the accessing device. For small web sites, a screen capture program can be used to collect pictures or video of a user browsing pertinent web pages. This works if the site is small and the person collecting the data has the time to visit each page. It should be noted, however, that while this produces a record, it does not provide any information outside of a visual comparison. This may be sufficient for the requirements of an individual case, but for many this method is not sufficient, nor is it cost effective.

A sophisticated vendor will have software at their disposal to automatically “crawl” or access every publicly accessible part of an Internet-hosted resource, so a forensic investigator doesn’t have to manually access and document each page. Typically, this type of software will “hash” the source and download files to ensure proper duplication and create a time stamp to record the date and time of access.

The digital fingerprint

The process to verify digital files is typically conducted using a value known as a “file hash.” A hash is a calculated value created using an algorithm which takes into account the value and location of each bit in a file and is an alpha-numeric character string representing a “digital fingerprint” of the file. Changing a single bit value will alter the hash value. This value is typically calculated on an original file and a copy to validate the copy is exactly the same as the original. This hash value can also be used to find specific files (if the hash is known) or copies of a file. This is helpful in cases where the identification of all copies of a file is important, as in intellectual property theft.

When capturing Internet resources, it is best to work with a vendor who respects the value and employs hash calculations in their Internet resource collection methodology. This will provide validation that the copied web site or resource is an exact duplicate of what was hosted on the web page on the day of collection.

Additionally, some collection software can take screenshots of how a web page displays on screen as well as copying the underlying files so that the page is captured as it appeared to the user.

Social media discovery methods

The ability to capture, preserve, and analyze social media postings and messaging is critical to the investigation and discovery process. Similar to the web site capture information discussed earlier, software exists to record the information available on a social media account.

Occasionally, the continual monitoring of an account is preferred. A vendor should have the ability to grab regular snapshots of a social media account without duplicating what was already captured. This ensures that posts or pictures available in one capture, but deleted in a future one, will persist in the collection record.

Anyone with access to software and training can handle the technological aspects of web sites and social media accounts. For attorneys, the difficult part is finding someone who can not only collect and

analyze the data, but has the experience and expertise to testify about the work, the authenticity of the evidence, and the method employed to collect the information. While many vendors can produce a copy of a web site, not as many have the experience to provide the testimony frequently needed in these matters. When selecting a consultant, ensure they have the technical capabilities and inquire about how many times the expert has testified and in what forums. Although affidavits and expert reports may be listed on a resume, in-person testimony tends to be scarce.

To continue the conversation about digital discovery contact one of the individuals below.

Contacts

Kristofer Swanson, CPA/CFF, CAMS, CFE

Vice President and Practice Leader, Forensic Services

Chicago

+1-312-619-3313

kswanson@crai.com

Cuyler Robinson, CISSP, CIPT

Vice President

Chicago

+1-312-619-3394

crobinson@crai.com

Louis Scharringhausen, EnCE, GCFA

Principal

Dallas

+1-214-414-9216

Louiss@crai.com



The conclusions set forth herein are based on independent research and publicly available material. The views expressed herein do not purport to reflect or represent the views of Charles River Associates or any of the organizations with which the authors are affiliated. The authors and Charles River Associates accept no duty of care or liability of any kind whatsoever to any party, and no responsibility for damages, if any, suffered by any party as a result of decisions made, or not made, or actions taken, or not taken, based on this paper. If you have questions or require further information regarding this issue of *CRA Insights: Forensic Services*, please contact the contributor or editor at Charles River Associates. This material may be considered advertising. Detailed information about Charles River Associates, a registered trade name of CRA International, Inc., is available at www.crai.com.

Copyright 2017 Charles River Associates