Recovering Deleted Internet History

Introduction

The forensic examination of digital devices in support of law enforcement and civil investigations is a critical part of the evidence collection process. Almost every crime investigated by the police has an electronic evidence aspect. Over the last decade and a half, the Internet has consolidated itself as a powerful platform that has changed the way we do business, and the way we communicate.

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted, whilst also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography, and paedophile rings, but also drug trafficking and criminal organisations that are more intent upon exploitation than the disruption that is the focus of the hacking community.

The forensic examination and analysis of user activity on digital devices can be the pivotal point of any criminal or civil case. It is vital for digital forensics investigators to be able to extract this data, analyse it quickly and present the evidence in an understandable format. More importantly, as a forensic specialist, you need to be sure that the software you use is accurate, can pass your acceptance/validation testing and can correctly recover live and deleted data from a suspect system.

NetAnalysis is the industry leading software for the extraction and analysis of data from Internet browsers. It was developed in 2001 by a digital forensics practitioner working for a police Digital Forensics Unit in the United Kingdom. There are now over 10,000 licensed users worldwide from the law enforcement and civil communities.

NetAnalysis has a host of features to help with your forensic examination such as the ability to import history and cache data from Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera browsers. NetAnalysis can also rebuild cached pages for offline review and was the first forensic software designed for this purpose. It also has the ability to utilise powerful SQL queries to quickly identify relevant evidence and a number of other tools to assist in the review and decoding process. The forensic suite also includes HstEx, a software tool designed to recover deleted browser artefacts.

HstEx®

HstEx® is an advanced, Windows-based, multi-threaded, forensic data recovery solution which has been designed to recover deleted browser history and cache data from a variety of source forensic evidence files as well as physical and logical devices. Specifically designed to work in conjunction with NetAnalysis, this powerful software can recover deleted data from a variety of Internet browsers, whether they have been installed on Windows, Linux or Apple Mac systems.

HstEx® supports a number of different source evidence types such as EnCase® e01 (Expert Witness) image files, AccessData® FTK™ Image files or traditional monolithic and segmented dd image files. It also supports direct sector access to physical and logical devices such as hard disks. HstEx® is able to extract browser history and cache records directly from source forensic files enabling the recovery of evidence, not only from unallocated clusters, but also from cluster slack, memory dumps, paging files and system restore points amongst others. It is an extremely powerful tool in your forensic tool-box.