On the digital forensic analysis of the Firefox browser via recovery of SQLite artifacts from unallocated space

R.I. Ferguson, P. Leimich and R. Bagley

University of Abertay, School of Computing and Engineering Systems, Kydd Building, Bell St. Dundee, UK DD1 1HG <ian.ferguson,p.leimich,r.bagley>@abertay.ac.uk

Abstract

A technique and supporting tool for the recovery of browsing activity (both stored and deleted) from current and recent versions of the Firefox web-browser is presented. The generality of the technique is discussed: It is applicable to any software that uses the popular SQLite embedded database engine such as the Apple Safari web-browser and many Android apps.

The reconstruction of browsing activity is a well-recognised problem in digital forensics. Both commercial and open-source solutions for IE, Firefox and other browsers have been available for sometime. Why then, is this a problem worth revisiting? The developers of the Firefox browser have recently moved to a "rapid release" schedule which sees new versions of the software emerge every six weeks; a schedule with which the tool vendors struggle to keep pace. As part of this evolution, Firefox now uses a series of SQLite database tables to store details of browsing history, cookies, favourites etc. One approach employed by examiners has been to export the SQLite files used by Firefox and examine them with open-source SQLite tools. Whilst this technique will extract the current contents of the various database tables in which Firefox records its activity, it makes no attempt to recover deleted records. Recovery of browsing activity even after its deletion from the database is possible due to the journalling approach to handling database updates employed by recent versions (>=4) of SQLite (WAL files).

The technique presented here involves the analysis of unallocated disk space to recover fragments of the SQLite journalling files and hence the records associated with Firefox activity.

The approach, which has been evaluated both as a manual procedure and embedded in a software tool, comprises three stages:

1) *Identification Stage:* Potential records are located by performing a search for a sequence of bytes that consist of two constant values that appear in all *moz_places* records, followed by a URL protocol that appears at the beginning of the records' URL field.

2) *Verification Stage:* To filter out any false positives that were identified, further bytes that exist within the potential *moz_places* record are examined. Predetermined values and ranges are compared to these bytes to ensure only genuine records are recovered.

3) *Reading Stage:* Finally, with an authentic *moz_places* record located, its contents were read and extracted to a text file. An additional program was developed to organise the recovery result into a XML table and a summary document.

To evaluate the approach, a copy of Mozilla Firefox 10.0.2 was used over a period of two days to browse the Internet and local files. Subsequently the browsing history was deleted. A routine forensic disk imaging procedure was followed and the resulting

image examined using our technique. A total of 455 records from an original 469 records were recovered from unallocated space which was a recovery success rate of 97%. Although it was initially designed to recover deleted browsing history from Firefox version 10.0.2, the developed tool is capable of functioning on version 4.0 and above.

The conclusion of this project was that it is possible to recover individual deleted records of the Firefox browsing history in an accurate and forensically sound manner.

Future work will examine the broader applicability of the technique to other SQLite based systems including Apple's Safari browser and Android apps.