opentext™

WHITE PAPER

Examining mobile devices:

Identifying private internet browsing activity in Mobile Safari

opentext™

Contents

opentext™

Discover how uncovering private internet browsing activity in Mobile Safari is an important part of any digital forensics and incident response (DFIR) investigation and how this information can be examined and extracted using OpenText™ EnCase™ software.

Executive summary

Internet browsing activity is an important part of any digital forensics and incident response (DFIR) investigation. The general browsing history provides some insight, but private internet browsing can be more enlightening, revealing activity an individual wanted to keep hidden. While the effectiveness of private browsing varies from browser to browser, at the very least it limits the recording and retention of searches and other browsing activity in the history databases. This has an obvious impact on investigating the internet activity of the user and is no different on a mobile device.

Mobile Safari has been the default web browser for both iPhone and iPad since the initial release of iPhone OS. The introduction of the private browsing functionality in iOS 5 gave users the ability to conceal their browsing activity.

This white paper shares specific examples of the type of information that can be extracted from Mobile Safari using OpenText™ EnCase™ software for DFIR investigations.

A case for OpenText EnCase solutions

Using OpenText EnCase software, including OpenText™ EnCase™ Forensic, OpenText™ EnCase™ Endpoint Investigator, OpenText™ EnCase™ Mobile Investigator and EnCase EnScript programs, the last state of Mobile Safari from an iPhone or iPad can be examined. The browser state is maintained in the BrowserState.db database, and the information that it contains allows the device user to exit or suspend Mobile Safari and return to it at a later time with the browser in the same or similar state.

For acquisition and forensic examination of the mobile device, this information forms part of a backup created by iTunes or Finder (if created using macOS Catalina) so it can be expected that a logical acquisition of an iPhone or iPad will include this database. Since the release of iOS 13, internet activity is only included if the device has been set to encrypt its backup. This is the favored setting for earlier iOS versions due to the increased content that can be acquired, including Apple's Health and Keychain.

In iOS 13, the internet history (history.db) and the BrowserState.db are located here: var\mobile\Library\Safari

In the structure of a backup, they would be found in the HomeDomain.

In iOS 12, both the history.db and BrowserState.db databases are located in the Application Data folder (com.apple.mobilesafari).

For example, an initial review of Mobile Safari internet history shows a limited number of records. It indicates that the user accessed:

- gov.uk
- cbp.gov

Displaying the user's Google search history, one search conducted was for how to use private browsing on Mobile Safari.

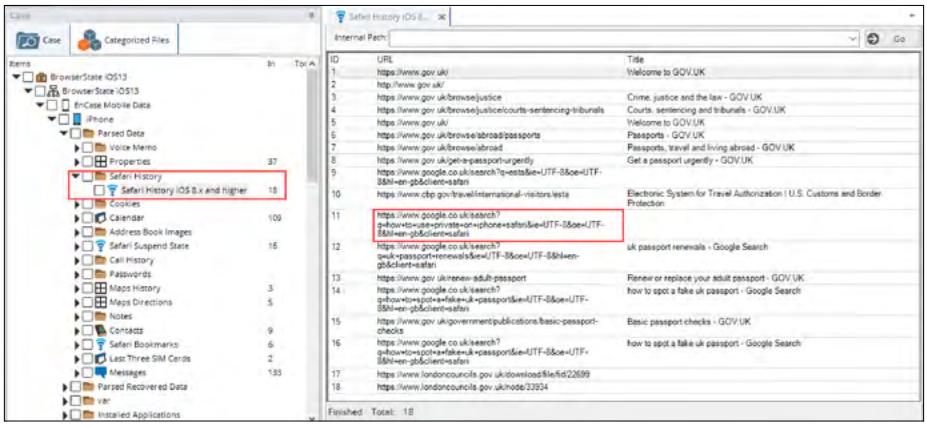


Figure 1: Mobile Safari internet history viewed in OpenText EnCase Mobile Investigator

Continuing the examination, further artifacts may provide more insight into the user's internet activity. Across the various browser versions, there has been a mechanism to maintain the state of the browser when it has been exited, the user has returned to the main iOS user interface or switched to another application. This information is maintained in the BrowserState.db.

Database examination

Although EnCase Mobile Investigator has built in SQLite viewing capability, if a query needs to be run across the database it must be performed using a third-party viewer, such as SQLite Expert.The database can be extracted directly from EnCase Mobile Investigator or EnCase Endpoint Investigator, with either an external viewer or the **View SQLite with WAL** EnScript plugin.

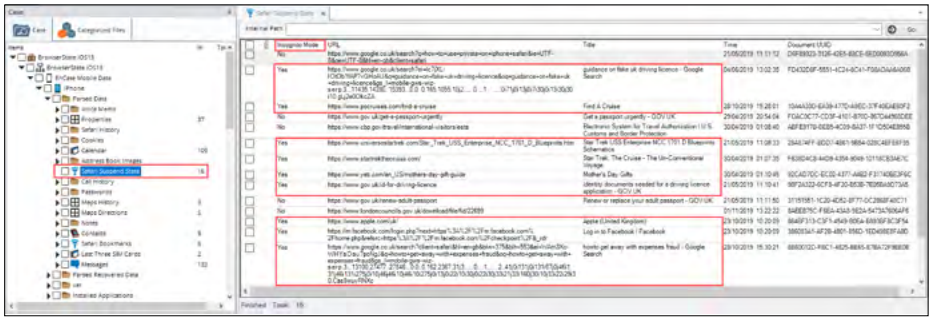


Figure 2a: Safari Suspend State, indicating the tabs viewed "Private"

Figure 2b: BrowserState.db viewed using SQLite Expert

Database tabs

The database contains two tables:

- tabs
- tab_sessions

The **tabs** table provides the current state of open tabs within Mobile Safari. The **tab_sessions** contains a record for each open tab and a data structure which maintains a record of websites visited in the active tab.

The tabs table includes:

- A flag indicating if the tab is being viewed privately
- The URL of the open webpage
- The Title of the open webpage
- A universally unique identifier (UUID)

As illustrated above in Figure 2, the table contains URLs and titles that had not been previously identified, including a Google search on obtaining a “fake UK driving license.”

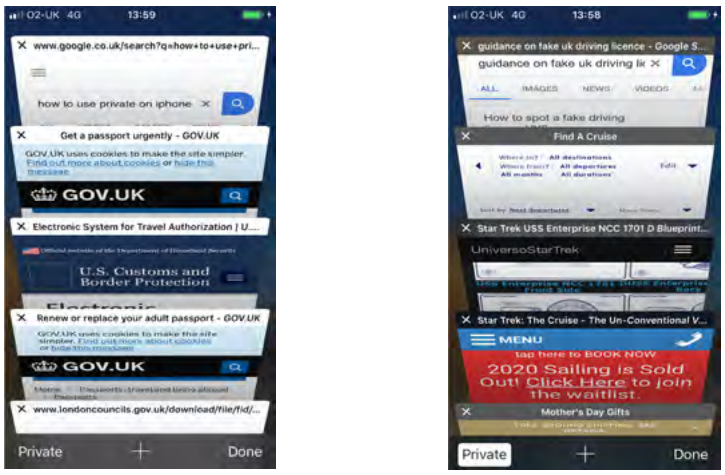


Figure 3: Open tabs, including those set to private, in Mobile Safari

Although it is now clear which tabs remain open from the last Mobile Safari browsing session, it is the **private_browsing** column that is of particular interest.

As the name suggests, it indicates that the user of the device had been using the private setting for that tab in Mobile Safari. While the internet history will not be recorded in the history.db database, the examiner can still see a single URL and title in the tabs table, which offers an important starting point.

Tab sessions

So far, the BrowserState.db database has yielded valuable information that had not been previously identified in the internet history. Focus now turns to the tab_sessions table. This table maintains records where the **tab_uuid** equals the **UUID** column on the tabs table with the data type for **session_data** being Binary Large Object (BLOB).

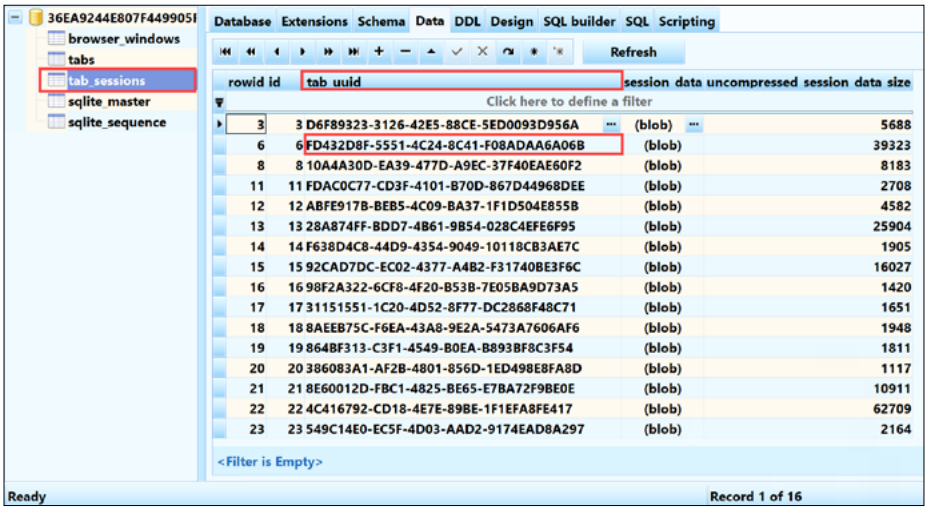


Figure 4: The tab_sessions table, showing the UUID of the tab

Examination with EnScript

The session_data column on the tab_sessions table showed a BLOB data type and, upon examination, revealed a binary property list (bplist), highlighted in blue in Figure 5. There is a four-byte offset from the beginning of the data to the start of the binary property list. While it may initially appear insignificant, it is important for automating the parsing of the enclosed data structure with EnScript programs.

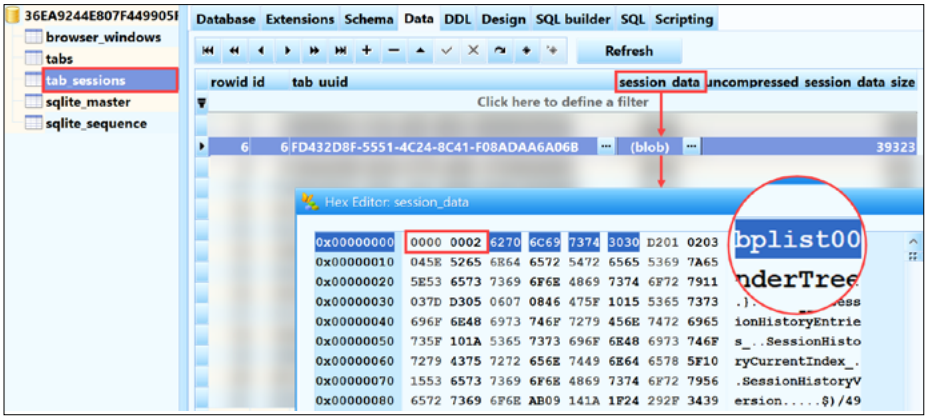
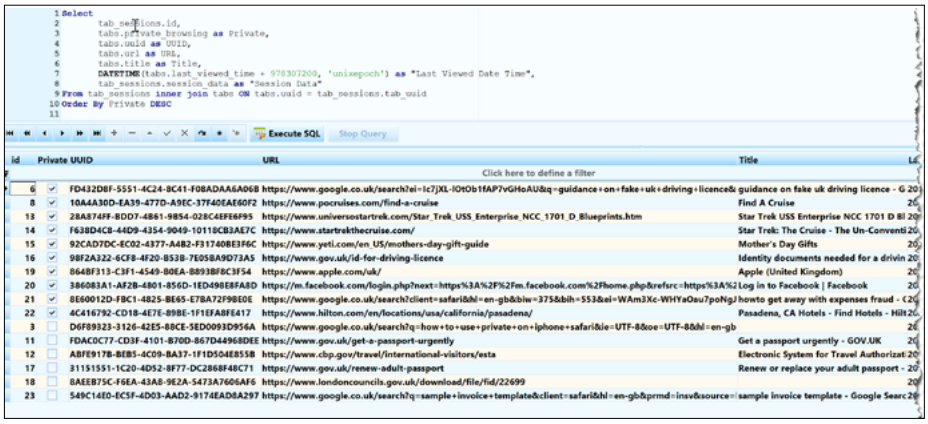


Figure 5: Apple binary property list with a four-byte offset from the start of data

Executing a SQLite query to determine the number of tabs open in private mode, combined with webpage titles and URLs, reveals ten tabs set to private. That the device user made the decision to conceal their browsing is of interest.



```
Select
      tab_sessions.id,
      tabs.private_browsing as Private,
      tabs.uuid as UUID,
      tabs.url as URL,
      tabs.title as Title,
      DATETIME(tabs.last_viewed_time + 978307200, 'unixepoch') as "Last Viewed Date Time",
      tab_sessions.session_data as "Session Data"
From tab_sessions inner join tabs ON tabs.uuid = tab_sessions.tab_uuid
Order By Private DESC
```

Execute SQL | Stop Query

id	Private	UUID	URL	Title
		Click here to define a filter		
6	✓	FD432D8F-5551-4C24-8C41-F08ADAA6A06B	https://www.google.co.uk/search?ei=Ic7jXL-IOtOb1fAP7vGHoAU&q=guidance+on+fake+uk+driving+licence&	guidance on fake uk driving licence - G
8	✓	10A4A30D-EA39-477D-A9EC-37F40EAE60F2	https://www.pocruises.com/find-a-cruise	Find A Cruise
13	✓	28A874FF-BDD7-4861-9B54-028C4EFE6F95	https://www.universostartrek.com/Star_Trek_USS_Enterprise_NCC_1701_D_Blueprints.htm	Star Trek USS Enterprise NCC 1701 D Bl
14	✓	F63BD4C8-44D9-4354-9049-10118CB3AE7C	https://www.startrekthecruise.com/	Star Trek: The Cruise - The Un-Conventi
15	✓	92CAD7DC-EC02-4377-A4B2-F31740BE3F6C	https://www.yeti.com/en_US/mothers-day-gift-guide	Mother's Day Gifts
16	✓	9BF2A322-6CF8-4F20-B53B-7E05BA9D73A5	https://www.gov.uk/id-for-driving-licence	Identity documents needed for a drivin
19	✓	864BF313-C3F1-4549-B0EA-B893BF8C3F54	https://www.apple.com/uk/	Apple (United Kingdom)
20	✓	3B6083A1-AF2B-4801-856D-1ED49BE8FA8D	https://m.facebook.com/login.php?next=https%3A%2F%2Fm.facebook.com%2Fhome.php&refsrc=https%3A%2	Log in to Facebook | Facebook
21	✓	8E60012D-FBC1-4825-BE65-E7BA72F9BE0E	https://www.google.co.uk/search?client=safari&hl=en-gb&biw=375&bih=553&ei=WAm3Xc-WHYaOau7poNgJ	howto get away with expenses fraud - C
22	✓	4C416792-CD18-4E7E-89BE-1F1EFA8FE417	https://www.hilton.com/en/locations/usa/california/pasadena/	Pasadena, CA Hotels - Find Hotels - Hilt
3		D6F89323-3126-42E5-88CE-5ED0093D956A	https://www.google.co.uk/search?q=how+to+use+private+on+iphone+safari&ie=UTF-8&oe=UTF-8&hl=en-gb	
11		FDAC0C77-CD3F-4101-B70D-867D44968DEE	https://www.gov.uk/get-a-passport-urgently	Get a passport urgently - GOV.UK
12		ABFE917B-BEB5-4C09-BA37-1F1D504E855B	https://www.cbp.gov/travel/international-visitors/esta	Electronic System for Travel Authorizat
17		311515S1-1C20-4D52-8F77-DC2868F48C71	https://www.gov.uk/renew-adult-passport	Renew or replace your adult passport -
18		8AEEB75C-F6EA-43A8-9E2A-5473A7606AF6	https://www.londoncouncils.gov.uk/download/file/fid/22699	
23		549C14E0-EC5F-4D03-AAD2-9174EAD8A297	https://www.google.co.uk/search?q=sample+invoice+template&client=safari&hl=en-gb&prmd=insv&source=i	sample invoice template - Google Searc

Figure 6: Result of SQLite query, showing the output for tabs and tab_sessions tables

To automate the extraction of BLOB data from the BrowserState.db database, the **SQLite BLOB Extractor** EnScript program can be used and the extracted data collected into a logical evidence file (LEF) for further processing and examination. The database(s) for the EnScript program to run against for mobile data need to be identified with a tag.

In this example, the extracted session_data will take the form of a binary property list that will require additional parsing with another EnScript program. The data extraction will need to commence four bytes into the BLOB.

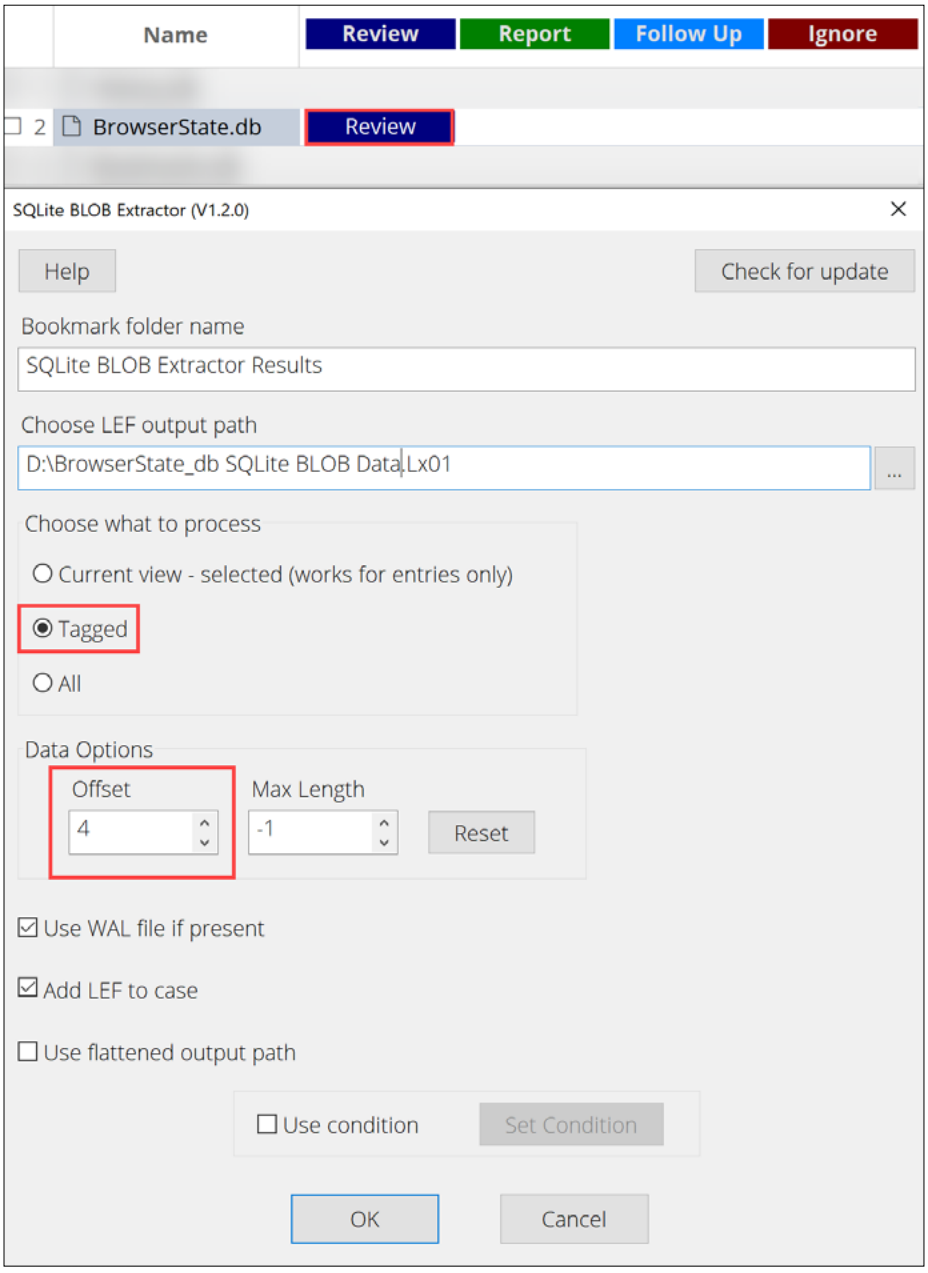


Figure 7: Using the SQLite BLOB Extractor EnScript to extract the session_data BLOBfrom BrowserState.db

The output from the SQLite BLOB Extractor is presented in EnCase, where the original path to the database is retained.

The extracted BLOB data is referenced by the:

- Table it has been extracted from
- RowID
- Column name from which it has been extracted

In the example, the extracted data takes the form of a binary property list and further processing will be required using a relevant EnScript program, such as the Plist Viewer Plugin.

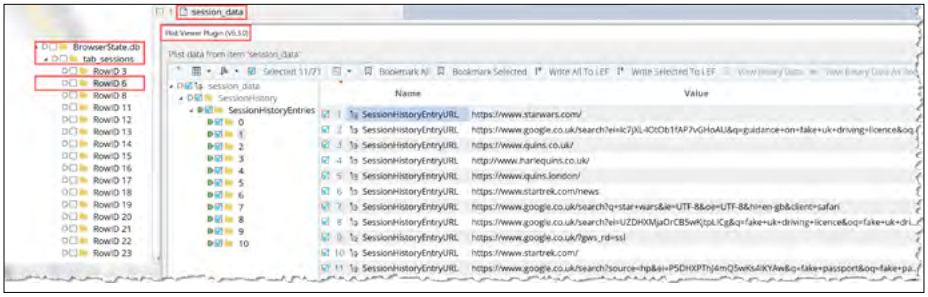


Figure 8: Parsing the binary property list extracted from session data using Plist Viewer Plugin

Figure 8 illustrates the content from **session_data** of RowID 6 from the **tab_sessions** table of the BrowserState.db database. This tab was viewed in private, as identified earlier by the UUID from the **tabs** table.

There are a further 10 URLs, in addition to the Google search for “guidance on fake uk driving license,” in the **tabs** table. That is a total of 11 pieces of internet activity that would not have been recorded in the history.db database due to private viewing.

Plist parsing

The example uses a small dataset with a total of ten tabs set to private. An actual examination may contain significantly more, so the Plist Viewer Plugin may not be the most efficient EnScript program to use.

Once the SQLite BLOB Extractor EnScript program has been used to extract the BLOB data, the extracted plists can be parsed en masse using the Plist Parser EnScript.

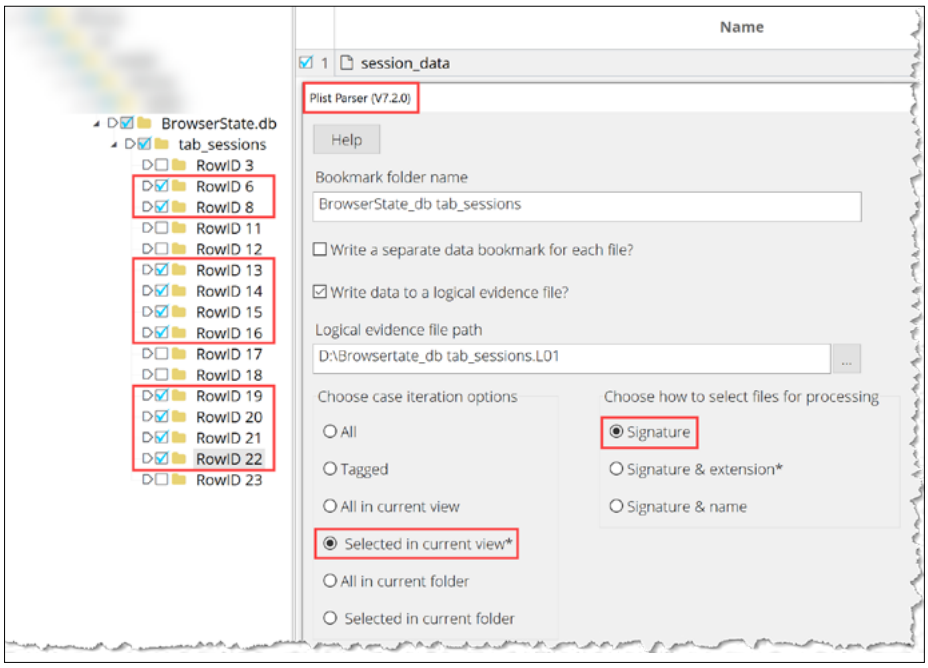


Figure 9: Parsing each of the session data plists using the Plist Parser EnScript

When plist parsing is complete, the results can be viewed and examined in the EnCase Bookmarks. In the example, there are 43 records of internet activity resulting from the tabs that had been set to private.

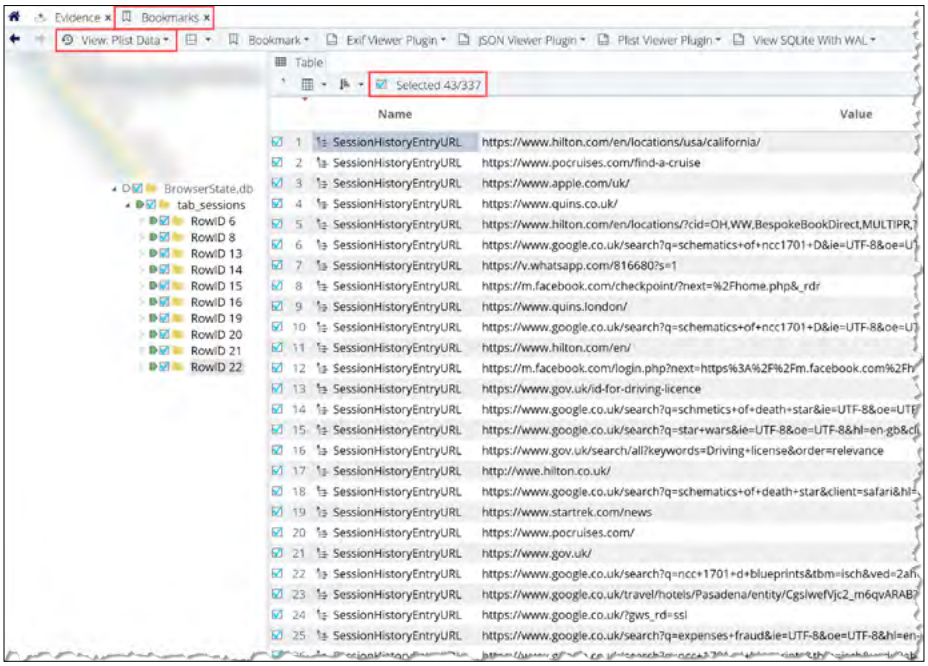


Figure 10: URLs extracted from session data plists from tabs set to private

BrowserState.db Parser EnScript program

The BrowserState.db Parser EnScript program is an alternative to the method combining the SQLite BLOB extractor and Plist Parser EnScript programs described above.

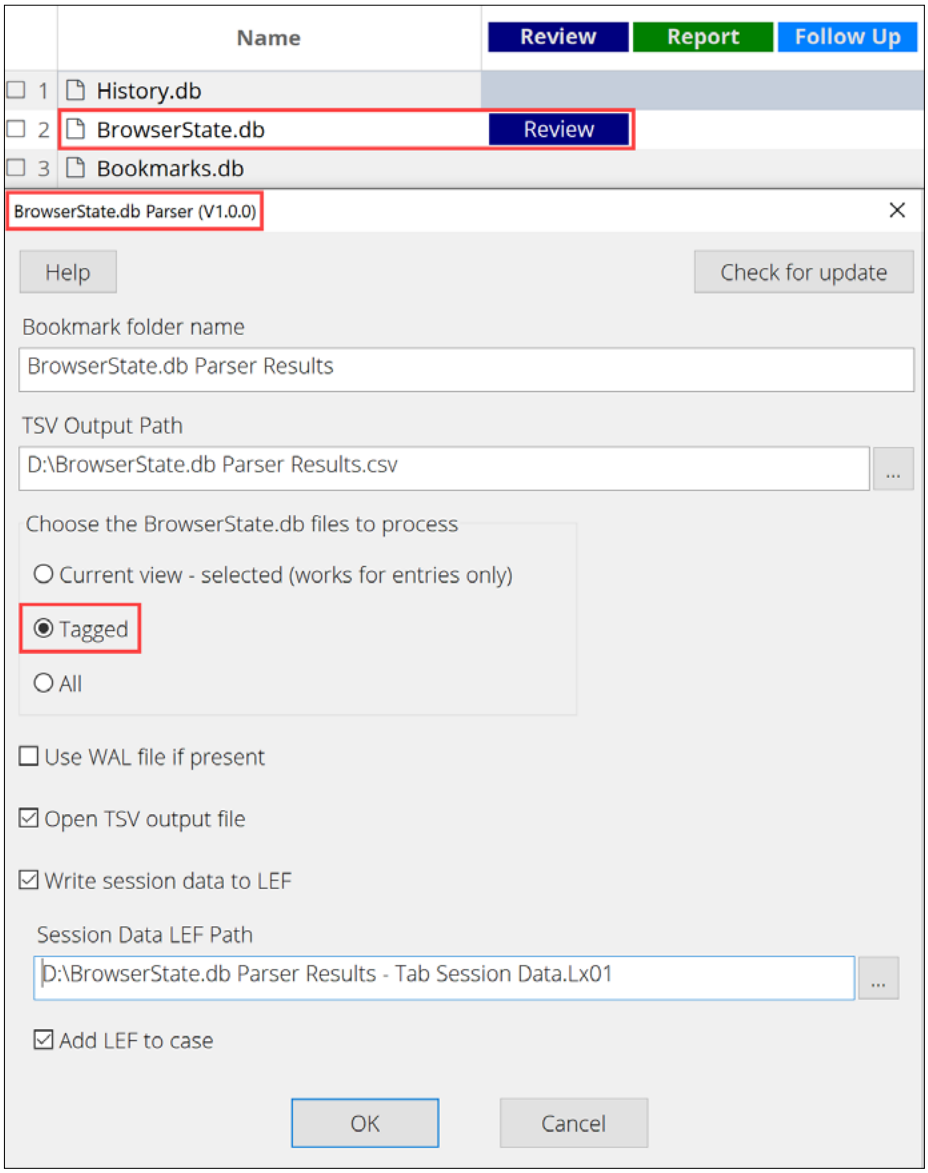


Figure 11: BrowserState.db Parser EnScript

The main output of this EnScript program is a TSV file, which can be viewed and filtered in Microsoft® Excel®. It will contain all parsed content from each session_data BLOB, as well as whether the tab had been set to private.

Tabs-Private_Browsing	Tab_Sessions.ID	SessionHistoryEntryIndex	SessionHistoryEntryURL
1	6	0	https://www.google.co.uk/search?q=star+wars&ie=UTF-8&oe=UTF-8&hl=en-gb&client=safari
1	6	1	https://www.starwars.com/
1	6	2	https://www.startrek.com/
1	6	3	https://www.startrek.com/news
1	6	4	http://www.harlequins.co.uk/
1	6	5	https://www.quins.co.uk/
1	6	6	https://www.quins.london/
1	6	7	https://www.google.co.uk/?gws_rd=ssl
1	6	8	https://www.google.co.uk/search?source=hp&ei=P5DHXPThJ4mQ5wKs4IKYAw&q=fake+passport&oq=fake+pass&gs_l=mobile-gws-wiz-hp.1.0.0l8.9374.15424..17728...7.0..0.95.952.14.....0....1.....0..0i131j46j46i131i275j0i10.xQk6Hsuylqo
1	6	9	https://www.google.co.uk/search?ei=UZDHXMjaOrCB5wKjtpLICg&q=fake+uk+driving+licence&oq=fake+uk+driving+&gs_l=mobile-gws-wiz-serp.1.0.0l8.20627.40116..42262...4.0..0.156.1775.22j2.....0....1.....0i71j41j0i67j0i131j46j0i70i249j0i22i30.Qvie2o87sAw
1	6	10	https://www.google.co.uk/search?ei=lc7jXL-lOtOb1fAP7vGHoAU&q=guidance+on+fake+uk+driving+licence&oq=guidance+on+fake+uk+driving+licence&gs_l=mobile-gws-wiz-serp.3...11435.14280..15393...0.0..0.165.1055.10j2.....0....1.....0i71j0i13j0i7i30j0i13i30j30i10.gLj2e0OkcZA

Figure 12: Sample output from BrowserState.db Parser EnScript

Summary

The Mobile Safari BrowserState.db database is populated with data regardless of whether a user browses privately. By employing knowledge of SQLite, identifying Apple binary property lists and using EnCase in concert with EnScript programs, a database can be parsed with ease. In the example, an additional 43 pieces of internet activity were recovered which would have been overlooked had only the history.db been examined.

OpenText Security solutions

OpenText Consulting Services

OpenText Learning Services EnCase training packages

OpenText EnCase Mobile Investigator

DF125—Mobile Device Examinations with EnCase (course)

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact