opentext[™]

WHITE PAPER

Examining mobile devices:

Identifying private internet browsing activity in Mobile Safari



opentext[™]

Contents

Executive summary	3
A case for OpenText EnCase solutions	3
Database examination	4
Database tabs	5
Tab sessions	6
Examination with EnScript	6
Plist parsing	9
BrowserState.db Parser EnScript program	11
Summary	12

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.

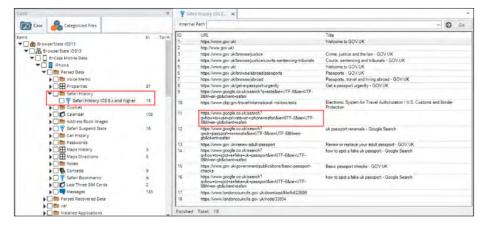


Figure 1: Mobile Safari internet history viewed in OpenText EnCase Mobile Investigator

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.

En Lant A Comparing Fires		-	Fact				~ 0 %
ers V Dru-serStern 10513	in Spin	8 6	Travegrate Mode No	1995. Hitte Tenne google oa uk hearch Tyrkow Konzennym aan wyter en after Band (177- Banne 117 - Banne chaffer Instrumenter	Tde	Ting 21.05/2019 19 19 17	Counter USD DIFENDS 1026-025-43CE-0ED00000986A
Call Brokerstatts (OS18 Call Broker Mobile Data Call Broker Mobile Data Call Phone Call Call Call Phone Call Call	- 1		Yes	https://www.google.co.uk/search?heidc200; IOOD:10077-08-loil.looputateces-an-date-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-an-date-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-ak-drimg-konnosikop-gudance-on-bate-ak- ak-mg-loon-gudance-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak- drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drimg-konnosikop-gudance-on-bate-ak-drim	guidance or faile uit driving licence - Google Search	0+062019 13:02:35	F043208F-9551-4C24-8C41-F354CA464068
Carto Antonio			100	Https://www.pocruses.com/html a-stuse	First A Cruise	2810/2019 15:28:01	10444300-6439-4770-4960-37F4064690F2
CIE frogenies	47	0	760	https://www.gov.ukipet-e-pesspon-urgently	Get a passport-urgerdy - 00VUK	2904/2018 20:54:04	FDAC9C77-CD3F-4101-8710-367D445600EE
Satari History	- S. H	D	160	htps://www.cbp.po.itra-el/nametional-visitorsitete	Bectronic System for Travel Authenization 112 S. Customa and Border Protection		ABFEN170-0685-4039-0437-111050483850
Coskins	108		Yes	https://www.universite/bell.com/Ster_Tesk_USS_Enterprise_MCC_1701_D_BLeproits.htm	Star Trek USS Enterprise NCC 1701 D Elugovity Schematics		284824FF-80007-4863-9854-028048FE8F35
ARTIVES BOOK INVEST	_	D	Ten	Hips //www.startraktwordia.com/	Star Trek: The Cruise - The Un-Convertional Visuage		FE38D4C3-4409-4354-8049-10118C834E7C
Setter Support State	16	11	Yes	Mpe //www.yet Janvier, US/methers-der-pill-puller	Mother's Day Gills	3054/2019 01.1045	10CAD70C-ECID-4377-A482-F317406E3F6C
Call History		Ū	Tag	https://www.gov.ukid-lar-driving-licence	identity documents seaded for a driving licence application - QCV UK	21/05/2019 11:10:41	98F7A322-6CF3-4F20-8538-76385A3075A8
► C I Maps History			No	htps://www.gov.jk/ranse-adult-passport	Fenew or replace your eduit passport - GOV UK	2105/2019 11:11:50	31151581-1C20-4D52-8F77-0C2868F48C71
► □ 田 Maps Directions	4		765	htps://www.kondotcouncils.ptv.uk/dowelkad/Nie/Kat22699		01/11/2019 15:22:22	\$486875C F36A 43A3 362A 5473A76364F6
Notes			Yes	https://www.apple.com/uk/	Apple (United Kingtom)	23 10/2019 10 20 09	8640F313-C3F3-#549-8064-80830F3C3F54
Có-Mains			Yes	htps://withcebook.com/login.phg?nextwittps?i34129712Fer tecebook.com/li 2Fhome.phg/kellec.htps?i3472F12Fer tecebook.com/L2Fcheckpoint?i2F8_ptr	Log in to Facebook / Facebook	23102019 10:20:09	38601345-AF28-4805-1960-1E0408E3F480
States Bookmanks Constrained	1 1 10		Yes	Edita Avera projeto ca Averanti Victoria edita Universidado en 200an - Michael Antonio, UNITES Cas. (2006) Sectores spectramentaria un di expensasi e tracidore devote spectramen, enti- responsa de addiga, la modela pos enci- erare 3. 1 1992 (2017) 21948, Sec. 404 (2018) 111.0.1.2.4.4.6.1.2.4.4.6.0.1.2.4.4.6.0.1.2.4.4.6.0.1.2.4.6.0.1.2.4.6.0.1.2.4.6.0.1.2.4.6.0.1.2.2.4.6.0.1.2.2.4.6.0.1.2.2.2.6.3.1. 2. Casel loss of Mice. 2017 (2018) 210.0.2.0.1.3.2.4.6.0.1.2.4.6.0.0.1.0.1.0.1.2.2.2.6.3.1. 2. Casel loss of Mice. 2017 (2018) 210.0.2.0.1.2.2.4.6.0.1.2.4.6.0.0.1.0.1.0.1.2.2.2.6.3.1. 2. Casel loss of Mice. 2017 (2018) 210.0.2.0.1.0.2.0.0.2.3.0.2.3.0.2.3.0.2.3.0.2.2.2.2	having per avery with respenses final - Galopte Search	28/10/2019 15 30:21	48800120-FIE1-ADS-8885-878472F98808
Immiliant Applications		4	-				

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

104		Refresh	
	bios bi bios	private browsing title	-
agite master ¥		Click hars to define a D	
-off	Image: Section 2, 1-2, 4-2, 5-44, 5-44, 5-40, 500001000-004, 1-2, 7-44, 5-44, 5-44, 5-40, 50000100-004, 1-2, 7-44, 5-44, 5-44, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40, 5-40,	gradianse net for a driving license - Georgie Earsch ter da A Coulde Georg assupert regardly - GOULK Georgenerity - Goulky Georgenerity Georgenerity - Goulky Georgenerity Georgener	In spectrowang serging the advancember for some professor en updates and the spectromagnetic serging serging and the spectromagnetic serging s

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).

- 36EA9244E807F449905	Database	Extensions Schema Data DDL Design SQL builder SQL Scr	ipting
browser_windows		• • • • + − • ✓ × α * '* Refresh	
tab_sessions	rowid id		data uncompressed session data size
sqlite_master	Ψ	Click here to define a filter	
sqlite_sequence	> 3	3 D6F89323-3126-42E5-88CE-5ED0093D956A	5688
	6	6FD432D8F-5551-4C24-8C41-F08ADAA6A06B (blob) 39323
	8	8 10A4A30D-EA39-477D-A9EC-37F40EAE60F2 (blob) 8183
	11	11 FDAC0C77-CD3F-4101-B70D-867D44968DEE (blob) 2708
	12	12 ABFE917B-BEB5-4C09-BA37-1F1D504E855B (blob) 4582
	13	13 28A874FF-BDD7-4B61-9B54-028C4EFE6F95 (blob) 25904
	14	14 F638D4C8-44D9-4354-9049-10118CB3AE7C (blob) 1905
	15	15 92CAD7DC-EC02-4377-A4B2-F31740BE3F6C (blob) 16027
	16	16 98F2A322-6CF8-4F20-B53B-7E05BA9D73A5 (blob) 1420
	17	17 31151551-1C20-4D52-8F77-DC2868F48C71 (blob) 1651
	18	18 8AEEB75C-F6EA-43A8-9E2A-5473A7606AF6 (blob) 1948
	19	19864BF313-C3F1-4549-B0EA-B893BF8C3F54 (blob) 1811
	20	20 386083A1-AF2B-4801-856D-1ED498E8FA8D (blob) 1117
	21	21 8E60012D-FBC1-4825-BE65-E7BA72F9BE0E (blob) 10911
	22	22 4C416792-CD18-4E7E-89BE-1F1EFA8FE417 (blob) 62709
	23	23 549C14E0-EC5F-4D03-AAD2-9174EAD8A297 (blob) 2164
	<filter e<="" is="" td=""><td>mpty></td><td></td></filter>	mpty>	
eady			Record 1 of 16

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.

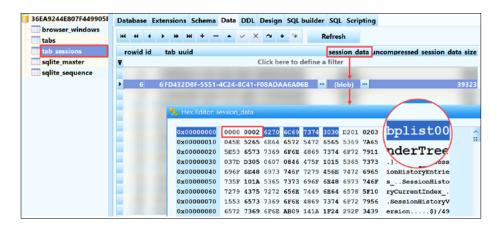


Figure 5: Apple binary property list with a four-byte offset from the start of data

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.

	234567891	<pre>let tab_sedFloos.id, tab_sedFloos.id, tab_sedFloos.id, tab_sedFloos.id, tab_sedFloor.id, tab_sedFloor.i</pre>		Contraction of the second s
	•	🗰 🗰 + X 🗥 • 🐨 🐺 Execute SQL Stop Query		- 1
id P	rivate	UUID URL 1	litle	LÉ
		Click here to define a filter		1
6	9	D432D8F-5551-4C24-8C41-F08ADAA6A068 https://www.google.co.uk/search?ei=Ic7iXL-IOtOb1fAP?vGHoAU&g=guidance+on+fake+uk+driving+licence& c	uidance on fake uk driving licence -	6 20
8		I0A4A30D-EA39-477D-A9EC-37F40EAE60F2 https://www.pocruises.com/find-a-cruise	ind A Cruise	26
13	-		itar Trek USS Enterprise NCC 1701 D	81 20
14		638D4C8-64D9-4354-9049-10118CB3AE7C https://www.startrekthecruise.com/	tar Trek: The Cruise - The Un-Conver	nti 20
15	4	IZCAD7DC-EC02-4377-A482-F317408E3F6C https://www.yeti.com/en_US/mothers-day-gift-guide	Mother's Day Gifts	20
16	4	R8F2A322-6CF8-4F20-B53B-7E058A9D73A5 https://www.gov.uk/id-for-driving-licence	dentity documents needed for a driv	in 20
19	4	064BF313-C3F1-4549-B0EA-8893BF8C3F54 https://www.apple.com/uk/	Apple (United Kingdom)	20
20	4	186083A1-AF28-4801-856D-1ED498E8FA8D https://m.facebook.com/login.php?next=https%3A%2F%2Fm.facebook.com%2Fhome.php&refsrc=https%3A%2L	og in to Facebook Facebook	20
21	4	3E60012D-FBC1-4825-BE65-E7BA72F9BE0E https://www.google.co.uk/search?client=safari&hl=en-gb&biw=375&bih=553&ei=WAm3Xc-WHYaOau7poNgJF	nowto get away with expenses fraud	. (20
22	4	IC416792-CD18-4E7E-89BE-1F1EFA8FE417 https://www.hilton.com/en/locations/usa/california/pasadena/	Pasadena, CA Hotels - Find Hotels - H	ilt 20
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		20
11		DAC0C77-CD3F-4101-870D-867D44968DEE https://www.gov.uk/get-a-passport-urgently 0	set a passport urgently - GOV.UK	20
12		RBFE917B-BEB5-4C09-BA37-1F1D504E855B https://www.cbp.gov/travel/international-visitors/esta	lectronic System for Travel Authoriza	ati 20
17		1151551-1C20-4D52-8F77-DC2868F48C71 https://www.gov.uk/renew-adult-passport F	Renew or replace your adult passport	- 20
18		3AEEB7SC-F6EA-43A8-9E2A-5473A7606AF6 https://www.londoncouncils.gov.uk/download/file/fid/22699		20
23		549C14E0-EC5F-4D03-AAD2-9174EAD8A297 https://www.google.co.uk/search?g=sample+invoice+template&client=safari&hl=en-gb&prmd=insv&source=is	ample involce template - Coople Sea	ar 20

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.

Name	Review	Report	Follow Up	Ignore
2 BrowserState	.db Review			
SQLite BLOB Extractor (V1.2	.0)			×
Help			Chec	k for update
Bookmark folder nam	e			
SQLite BLOB Extracto	or Results			
Choose LEF output pa	ath			
	SQLite BLOB Data Lx01			
Choose what to proc	ess			
	ected (works for entries	conly)		
		, only,		
Tagged				
O All				
Data Options				
Offset	Max Length			
4 2	-1 🗘	Reset		
Use WAL file if pres	ent			
Add LEF to case				
Use flattened outpo	ut path			
	Use condition	Set Conditio	on	
	ОК	Cancel		

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.

	Hož Vimier Hugin (V5.3.0)					
BrowserState.db	Plist data from item Setslovi_data					-
D Rowid 3	* III • J• • 🐼 Selectert 11/7	18	🔹 🖾 Bookmark Al 🗐 Bo	okmark Selected	If Write All To LEF IP Write Selected To LEF vow many same vow i	many Data Av Ree
PC RowID 6 PC RowID 8	Dig to session data Dig to SessionHistory		Name		Value	
PC RowiD 11 PC RowiD 12	SessionHistoryEntries	82	1 SessionHistoryEntryURL	https://www.st		
DC RowiD 13	Disting 1	2	1 19 SessionHistoryEntryURL		oogle.co.uk/search?ei=ic?jXL=OtOb1fAP?vGHoAU&q=guidance+on+take+uk+drv	ing+licence&oq
RowID 14 RowID 15	₩ 2	12	1 19 SessionHistoryEntryURL	https://www.g		
RowID 15 RowID 16	DE 3	12	1 19 SessionHistoryEntryURL	nttp://www.har	irlequins.co.uk/	2
RowID 17	PR 4	81	i 13 SessionHistoryEntryURL	https://www.q	uins.london/	4
owiD 18	00 0 6	87	5 19 SessionHistoryEntryURL	https://www.st	tartrek.com/news	1
with 19	D	18	1. SessionHistoryEntryURL	https://www.go	pogle.co.uk/search?q+star+wars&ie=UTF-8&oe=UTF-8&hi+en-gb&client+safari	
owID 20	8 - 94	2	5 1a SessionHistoryEntryURL	https://www.go	pogle.co.uk/search?el=UZDHXMiaOrCB5wK(toLlCg&g=fake+uk+driving+licence&c	og=fake+uk+dri_
towID 21 towID 22	₽2 • 9	100	12 SessionHistoryEntryURL	https://www.go	pogle.co.uk/hews.rd=ssl	
RowID 23	D = 10	81	() 12 SessionHistoryEntryURL	https://www.st	tartrek.com/	1
		100	1 % SessionHistoryEntryURL	https://www.ex	pogle.co.uk/search?source=hp&ei+P5DHXPThj4mQ5wKs4lKYAw&o+fake+passpc	et&og-take+pa.



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.

and the second se		Name
	🗹 1 🗋 session_data	de la companya
	Plist Parser (V7.2.0)	5
▲ D☑ BrowserState.db ▲ D☑ tab_sessions	Help	a de la companya de l La companya de la comp
-D 🔤 💼 Rowid 3	Bookmark folder name	5
D⊠ ■ RowID 6 D⊠ ■ RowID 8	BrowserState_db tab_sessions	
C RowID 11 C RowID 12	Write a separate data bookmark fo	ir each file?
DI IN RowID 13		ť
D☑ ■ RowID 14 D☑ ■ RowID 15	✓ Write data to a logical evidence file	2
D⊠ ■ RowID 16	Logical evidence file path	
D Rowid 18	D:\Browsertate_db tab_sessions.L01	
D⊠ ■ RowID 19 D⊠ ■ RowID 20	Choose case iteration options	Choose how to select files for processing
DI International RowlD 21	O All	Signature
D I ■ RowID 22	O Tagged	O Signature & extension*
	O All in current view	O Signature & name
	Selected in current view*	
	O All in current folder	2
	O Selected in current folder	5
معريس برجحح معسين جرجي جريبا صبغ بس	a and a second s	man par anon

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.

• • • • View: Plist Data • 🖽 • 🖽 Boo		ISON Viewer Plugin * 🕒 Plist Viewer Plugin * 🕒 View SQUite With WAL *
	III Table	
	* Ⅲ • № • 🗹 Selected 43/33	7
	Name	Value
	1 1= SessionHistoryEntryURL	https://www.hilton.com/en/locations/usa/california/
	2 1 SessionHistoryEntryURL	https://www.pocruises.com/find-a-cruise
A D BrowserState.db	3 1∋ SessionHistoryEntryURL	https://www.apple.com/uk/
▲ D W → Browser State, do	2 4 SessionHistoryEntryURL	https://www.quins.co.uk/
🕐 🖻 🗹 🍉 RowiD 6	5 12 SessionHistoryEntryURL	https://www.hilton.com/en/locations/?cid=OH,WW,BespokeBookDirect,MULTIP
P B 2 Rowid 8	Ø 6 1∋ SessionHistoryEntryURL	https://www.google.co.uk/search?q=schematics+of+ncc1701+D&ie=UTF-8&oe=
Rowid 13	7 1 SessionHistoryEntryURL	https://v.whatsapp.com/816680?s=1
Device Rowid 15	🕺 8 🖙 SessionHistoryEntryURL	https://m.facebook.com/checkpoint/?next=%2Fhome.php&_rdr
> DI Rowid 16	2 9 SessionHistoryEntryURL	https://www.quins.london/
RowID 19	10 1: SessionHistoryEntryURL	https://www.google.co.uk/search?q=schematics+of+ncc1701+D&ie=UTF-8&oe=
Rowid 20	11 1 SessionHistoryEntryURL	https://www.hilton.com/en/
Belle RowID 22	12 12 SessionHistoryEntryURL	https://m.facebook.com/login.php?next=https%3A%2F%2Fm.facebook.com%2i
	13 13 SessionHistoryEntryURL	https://www.gov.uk/id-for-driving-licence
	☑ 14 1 SessionHistoryEntryURL	https://www.google.co.uk/search?q=schmetics+of+death+star&ie=UTF-8&oe=U
	15 12 SessionHistoryEntryURL	https://www.google.co.uk/search?q=star+wars&ie=UTF-8&oe=UTF-8&hl=en-gbi
	☑ 16 SessionHistoryEntryURL	https://www.gov.uk/search/all?keywords=Driving+licenseℴ=relevance
	17 1: SessionHistoryEntryURL	http://wwe.hilton.co.uk/
	18 13 SessionHistoryEntryURL	https://www.google.co.uk/search?q=schematics+of+death+star&client=safari&l
	19 19 SessionHistoryEntryURL	https://www.startrek.com/news
	20 SessionHistoryEntryURL	https://www.pocruises.com/
	21 SessionHistoryEntryURL	https://www.gov.uk/
	22 12 SessionHistoryEntryURL	https://www.google.co.uk/search?q=ncc+1701+d+blueprints&tbm=isch&ved=2
	23 SessionHistoryEntryURL	https://www.google.co.uk/travel/hotels/Pasadena/entity/CgslwefVjc2_m6qvAR/
	24 1: SessionHistoryEntryURL	https://www.google.co.uk/?gws_rd=ssl
	25 1 SessionHistoryEntryURL	https://www.google.co.uk/search?g=expenses+fraud&ie=UTF-8&oe=UTF-8&hl=

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.

Name	Review	Report	Follow Up
🗆 1 🗋 History.db		_	
2 BrowserState.db	Review		
🗆 3 🗋 Bookmarks.db			
BrowserState.db Parser (V1.0.0)			×
Help		Chec	k for update
Bookmark folder name			
BrowserState.db Parser Results			
TSV Output Path			
D:\BrowserState.db Parser Results.csv			
Choose the BrowserState.db files to process O Current view - selected (works for entries Tagged O All	only)		
Use WAL file if present			
☑ Open TSV output file			
☑ Write session data to LEF			
Session Data LEF Path			
D:\BrowserState.db Parser Results - Tab Ses	sion Data.Lx01		
Add LEF to case			
ОК	Cancel		





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 JT	Tab_Sessions.ID -T	SessionHistoryEntryIndex -	SessionHistoryEntryURL
			https://www.google.co.uk/search?q=star+wars&ie=UTF-8&oe=UTF-8&hl=en-
1	6	0	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
			https://www.google.co.uk/search?source=hp&ei=P5DHXPThJ4mQ5wKs4IKYAw&
			fake+passport&oq=fake+pass&gs_l=mobile-gws-wiz-
			hp.1.0.0l8.9374.15424177287.00.95.952.140100l131j46j46i131i
1	6	8	5j0i10.xQk6Hsuylqo
			https://www.google.co.uk/search?ei=UZDHXMjaOrCB5wKjtpLICg&q=fake+uk+dr
			ng+licence&oq=fake+uk+driving+&gs_l=mobile-gws-wiz-
			serp.1.0.0l8.20627.40116422624.00.156.1775.22j2010i71j41j0i
1	6	9	0i131j46j0i70i249j0i22i30.Qvie2o87sAw
			https://www.google.co.uk/search?ei=Ic7jXL-
			IOtOb1fAP7vGHoAU&q=guidance+on+fake+uk+driving+licence&oq=guidance+on
			ake+uk+driving+licence&gs_l=mobile-gws-wiz-
			serp.311435.14280153930.00.165.1055.10j2010i71j0i13j0i7i3
1	6	10	i13i30j30i10.gLj2e00kcZA

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

Copyright © 2021 Open Text. All Rights Reserved. Trademarks owned by Open Text. For more information, visit: https://www.opentext.com/about/copyright-information • 07/21 | SKU18391