Autopsy 4.10.0- SQLiteBroswer, Extracting iPhone Browsing History

Wednesday, November 20, 2024 8:43 PM

Activity File: Extracting Evidence for Offline Analysis

In this activity, you will continue your role as a digital forensics investigator.

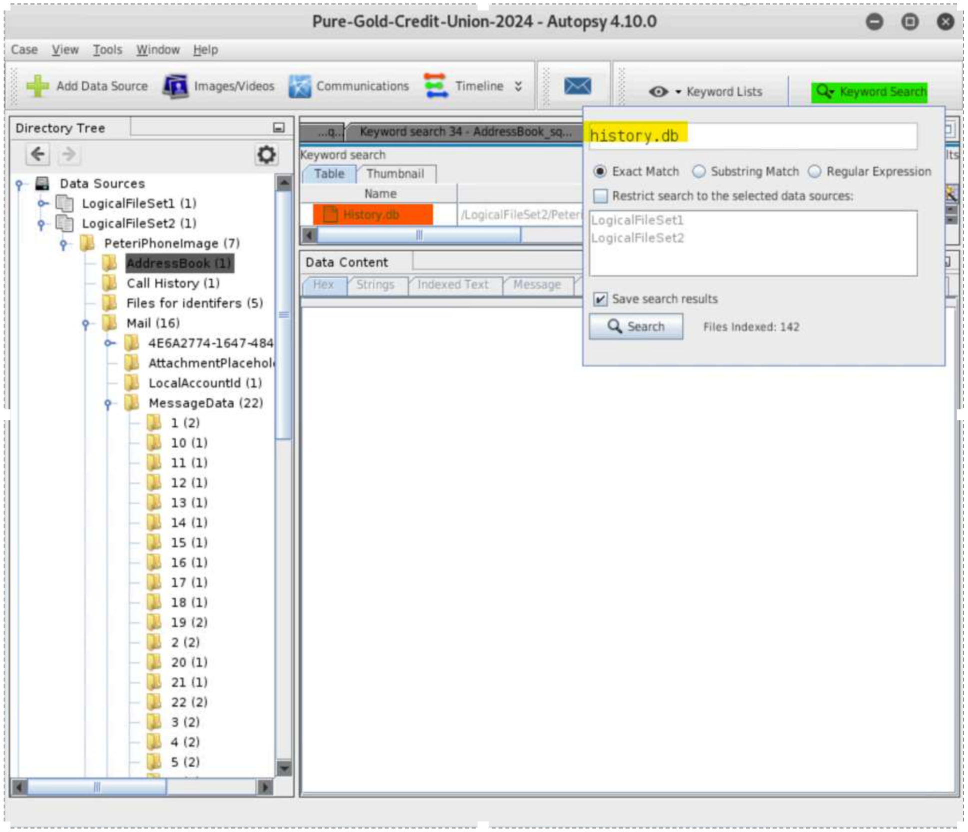
- You are tasked with exporting the browser history database for offline examination.
- This will allow other investigative team members to use alternative methods to analyze, parse, and create reports outside of Autopsy.
- The investigative team will use your file exports to identify if Peter has malicious intent.

Instructions

Single File Export

A senior investigative team member has asked you to export the history.db file for offline analysis.

1. Locate the history.db file in the iPhone image file.



history.db

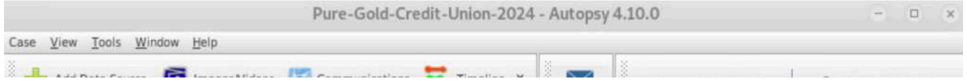
● Exact Match ○ Substring Match ○ Regular Expression

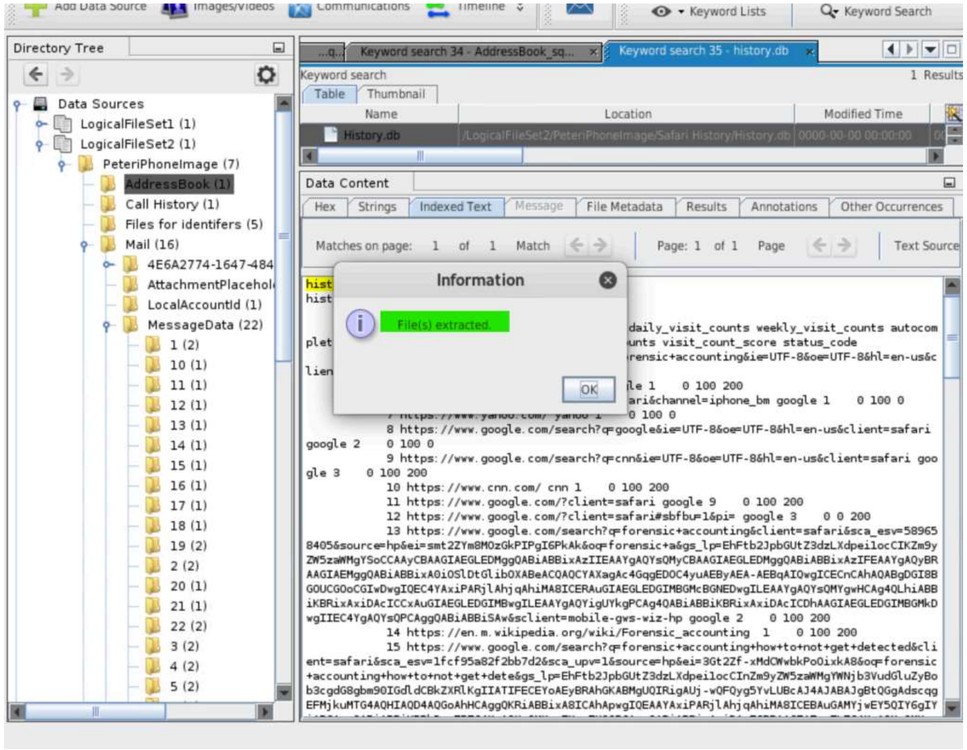
□ Restrict search to the selected data sources:

LogicalFileSet1
LogicalFileSet2

☑ Save search results

2. Extract the file to the Export directory.





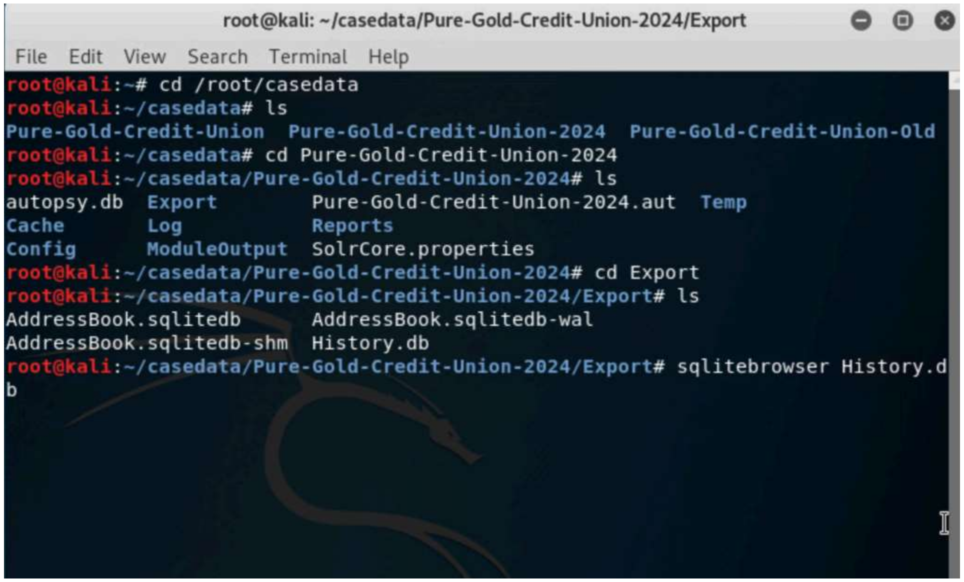
Name	Location	Modified Time
History.db	/LogicalFileSet2/PeteriPhoneImage/Safari History/History.db	0000-00-00 00:00:00

File(s) extracted.

```
hist
hist
                                         daily_visit_counts weekly_visit_counts autocom
plet                                     unts visit_count_score status_code
                                         rensic+accounting&ie=UTF-8&oe=UTF-8&hl=en-us&c
lien
                                         le 1    0 100 200
                                         ari&channel=iphone_bm google 1    0 100 0
            7 https://www.yahoo.com/ yahoo 1    0 100 0
            8 https://www.google.com/search?q=google&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari
google 2    0 100 0
            9 https://www.google.com/search?q=cnn&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari goo
gle 3    0 100 200
            10 https://www.cnn.com/ cnn 1    0 100 200
            11 https://www.google.com/?client=safari google 9    0 100 200
            12 https://www.google.com/?client=safari#sbfbu=1&pi= google 3    0 0 200
            13 https://www.google.com/search?q=forensic+accounting&client=safari&sca_esv=58965
8405&source=hp&ei=smt2ZYm8MOzGkPIPgI6PkAk&oq=forensic+a&gs_lp=EhFtb2JpbGUtZ3dzLXdpeilocCIKZm9y
ZW5zaWMgYSoCCAAyCBAAGIAEGLEDMggQABiABBixAzIIEAAYgAQYsQMyCBAAGIAEGLEDMggQABiABBixAzIFEAAYgAQyBR
AAGIAEMggQABiABBixA0iOSlDtGlibOXABeACQAQCYAXagAc4GqgEDOC4yuAEByAEA-AEBqAIQwgICECnCAhAQABgDGI8B
GOUCGOoCGIwDwgIQEC4YAxiPARjlAhjqAhiMA8ICERAuGIAEGLEDGIMBGMcBGNEDwgILEAAYgAQYsQMYgwHCAg4QLhiABB
iKBRixAxiDAcICCxAuGIAEGLEDGIMBwgILEAAYgAQYigUYkgPCAg4QABiABBiKBRixAxiDAcICDhAAGIAEGLEDGIMBGMkD
wgIIEC4YgAQYsQPCAggQABiABBiSAw&sclient=mobile-gws-wiz-hp google 2    0 100 200
            14 https://en.m.wikipedia.org/wiki/Forensic_accounting  1    0 100 200
            15 https://www.google.com/search?q=forensic+accounting+how+to+not+get+detected&cli
ent=safari&sca_esv=1fcf95a82f2bb7d2&sca_upv=1&source=hp&ei=3Gt2Zf-xMdCWwbkPoOixkA8&oq=forensic
+accounting+how+to+not+get+dete&gs_lp=EhFtb2JpbGUtZ3dzLXdpeilocCInZm9yZW5zaWMgYWNjb3VudGluZyBo
b3cgdG8gbm90IGdldCBkZXRlKgIIATIFECEYoAEyBRAhGKABMgUQIRigAUj-wQFQyg5YvLUBcAJ4AJABAJgBtQGgAdscqg
EFMjkuMTG4AQHIAQD4AQGoAhHCAggQKRiABBixA8ICAhApwgIQEAAYAxiPARjlAhjqAhiMA8ICEBAuGAMYjwEY5QIY6gIY
```

Now you will view the file using SQLite DB Browser, the third-party application used by your team. It is professional courtesy to verify your exports prior to handing them off to other team members.

3. Open a new terminal window and navigate to the Export directory.



```
root@kali:~# cd /root/casedata
root@kali:~/casedata# ls
Pure-Gold-Credit-Union  Pure-Gold-Credit-Union-2024  Pure-Gold-Credit-Union-Old
root@kali:~/casedata# cd Pure-Gold-Credit-Union-2024
root@kali:~/casedata/Pure-Gold-Credit-Union-2024# ls
autopsy.db  Export        Pure-Gold-Credit-Union-2024.aut  Temp
Cache       Log           Reports
Config      ModuleOutput  SolrCore.properties
root@kali:~/casedata/Pure-Gold-Credit-Union-2024# cd Export
root@kali:~/casedata/Pure-Gold-Credit-Union-2024/Export# ls
AddressBook.sqlitedb      AddressBook.sqlitedb-wal
AddressBook.sqlitedb-shm  History.db
root@kali:~/casedata/Pure-Gold-Credit-Union-2024/Export# sqlitebrowser History.d
b
```

4. Select **history_visits** in the Table dropdown menu to reveal the browser history.

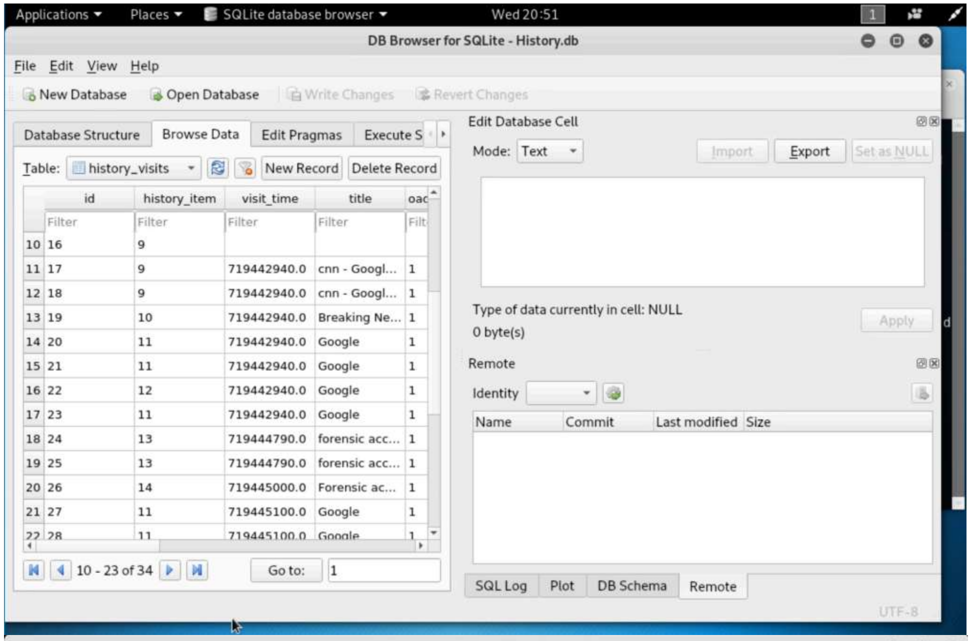


Table: history_visits

Mode: Text

	id	history_item	visit_time	title	oac
	Filter	Filter	Filter	Filter	Filt
10	16	9			
11	17	9	719442940.0	cnn - Googl...	1
12	18	9	719442940.0	cnn - Googl...	1
13	19	10	719442940.0	Breaking Ne...	1
14	20	11	719442940.0	Google	1
15	21	11	719442940.0	Google	1
16	22	12	719442940.0	Google	1
17	23	11	719442940.0	Google	1
18	24	13	719444790.0	forensic acc...	1
19	25	13	719444790.0	forensic acc...	1
20	26	14	719445000.0	Forensic ac...	1
21	27	11	719445100.0	Google	1
22	28	11	719445100.0	Google	1

10 - 23 of 34 Go to: 1

Type of data currently in cell: NULL

0 byte(s)

Name	Commit	Last modified	Size

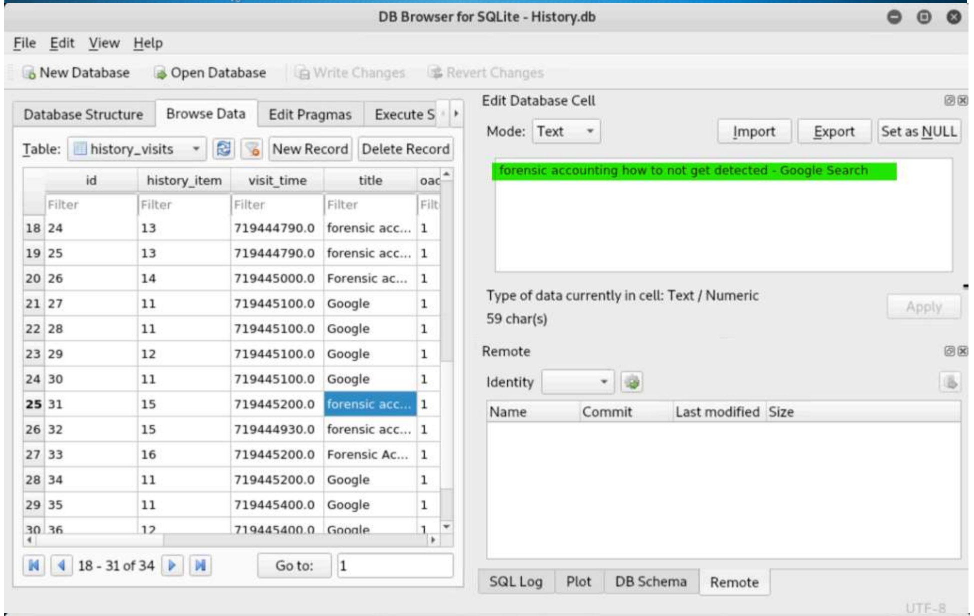


Table: history_visits

Mode: Text

forensic accounting how to not get detected - Google Search

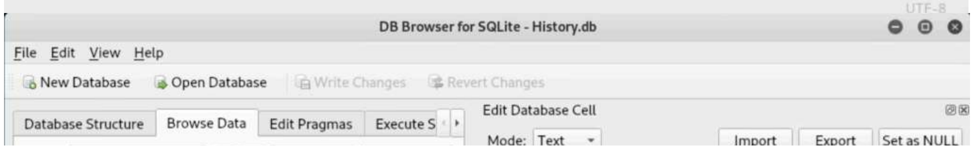
	id	history_item	visit_time	title	oac
	Filter	Filter	Filter	Filter	Filt
18	24	13	719444790.0	forensic acc...	1
19	25	13	719444790.0	forensic acc...	1
20	26	14	719445000.0	Forensic ac...	1
21	27	11	719445100.0	Google	1
22	28	11	719445100.0	Google	1
23	29	12	719445100.0	Google	1
24	30	11	719445100.0	Google	1
25	31	15	719445200.0	forensic acc...	1
26	32	15	719444930.0	forensic acc...	1
27	33	16	719445200.0	Forensic Ac...	1
28	34	11	719445200.0	Google	1
29	35	11	719445400.0	Google	1
30	36	12	719445400.0	Google	1

18 - 31 of 34 Go to: 1

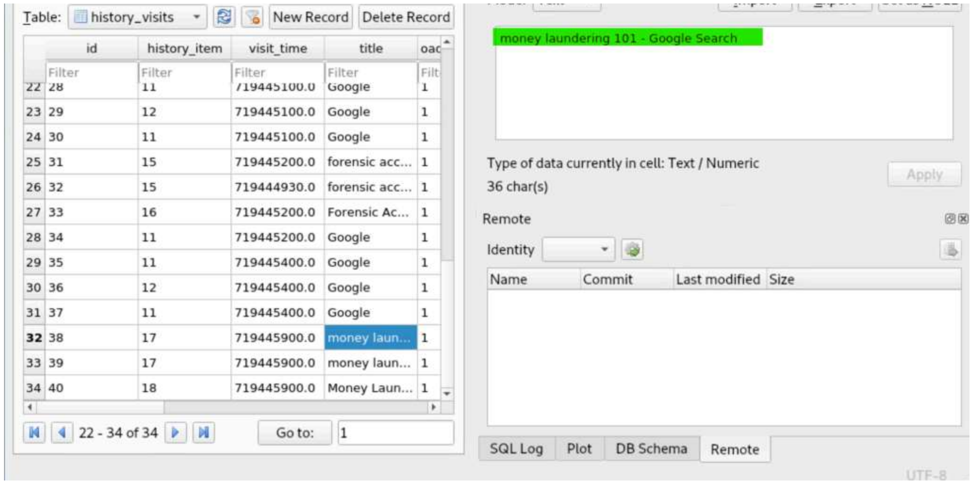
Type of data currently in cell: Text / Numeric

59 char(s)

Name	Commit	Last modified	Size



Mode: Text



	id	history_item	visit_time	title	oac
	Filter	Filter	Filter	Filter	Filt
22	28	11	719445100.0	Google	1
23	29	12	719445100.0	Google	1
24	30	11	719445100.0	Google	1
25	31	15	719445200.0	forensic acc...	1
26	32	15	719444930.0	forensic acc...	1
27	33	16	719445200.0	Forensic Ac...	1
28	34	11	719445200.0	Google	1
29	35	11	719445400.0	Google	1
30	36	12	719445400.0	Google	1
31	37	11	719445400.0	Google	1
32	38	17	719445900.0	money laun...	1
33	39	17	719445900.0	money laun...	1
34	40	18	719445900.0	Money Laun...	1

22 - 34 of 34 Go to: 1

money laundering 101 - Google Search

Type of data currently in cell: Text / Numeric
36 char(s)

Name	Commit	Last modified	Size

Bonus

- What is the command to launch and simultaneously open the call table?
  In the command line you type: sqlitebrowser -table call history.db