ATTACK DEFENSE

by PentesterAcademy

Name	T1217: Browser Bookmark Discovery II
URL	https://attackdefense.com/challengedetails?cid=1770
Type	MITRE ATT&CK Linux : Discovery

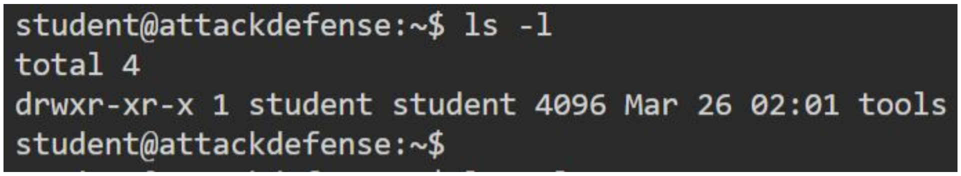
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Export all Google chrome records as sqlite3 database and Find the creation timestamp of ubid-main encrypted cookie of .amazon.com.

Solution:

Step 1: Check the content present in the current working directory.

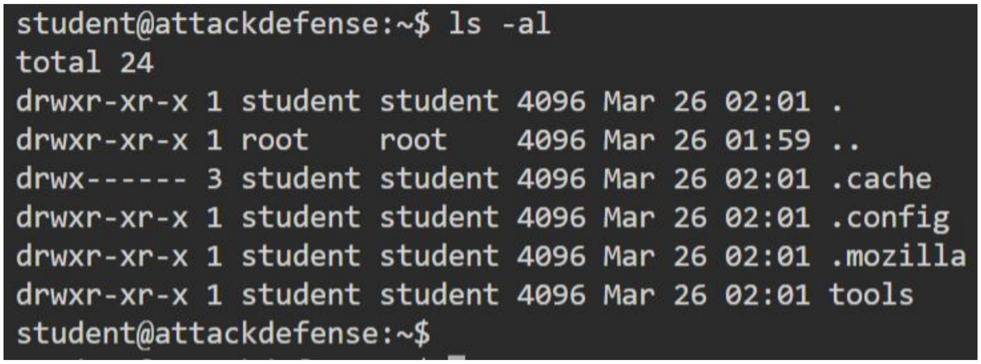
Commands: ls -l



```
student@attackdefense:~$ ls -l
total 4
drwxr-xr-x 1 student student 4096 Mar 26 02:01 tools
student@attackdefense:~$
```

Step 2: Also list the hidden directories.

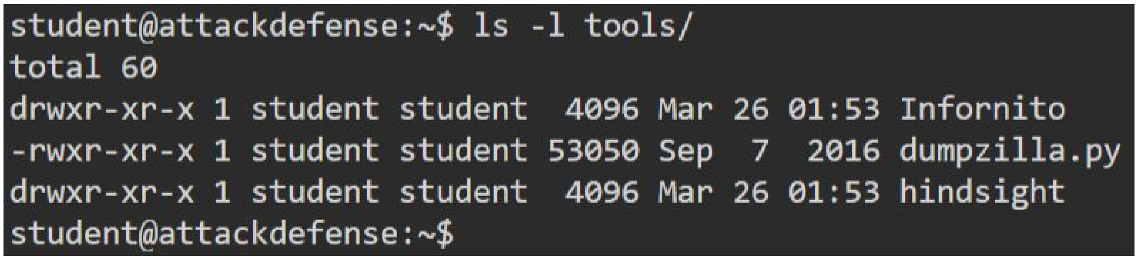
Command: ls -al



```
student@attackdefense:~$ ls -al
total 24
drwxr-xr-x 1 student student 4096 Mar 26 02:01 .
drwxr-xr-x 1 root    root    4096 Mar 26 01:59 ..
drwx------ 3 student student 4096 Mar 26 02:01 .cache
drwxr-xr-x 1 student student 4096 Mar 26 02:01 .config
drwxr-xr-x 1 student student 4096 Mar 26 02:01 .mozilla
drwxr-xr-x 1 student student 4096 Mar 26 02:01 tools
student@attackdefense:~$
```

Step 3: Check the contents of tools directory.

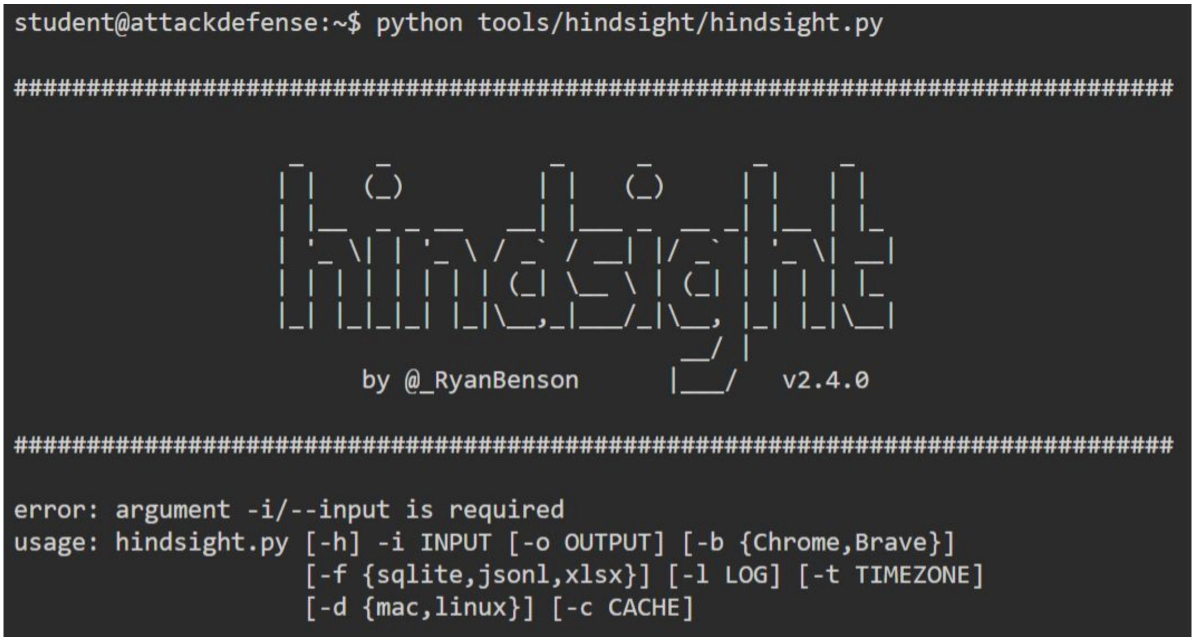
Command: ls -l tools/



```
student@attackdefense:~$ ls -l tools/
total 60
drwxr-xr-x 1 student student  4096 Mar 26 01:53 Infornito
-rwxr-xr-x 1 student student 53050 Sep  7  2016 dumpzilla.py
drwxr-xr-x 1 student student  4096 Mar 26 01:53 hindsight
student@attackdefense:~$
```

Step 4: Check the help option for hindsight tools.

Command: python tools/hindsight/hindsight.py

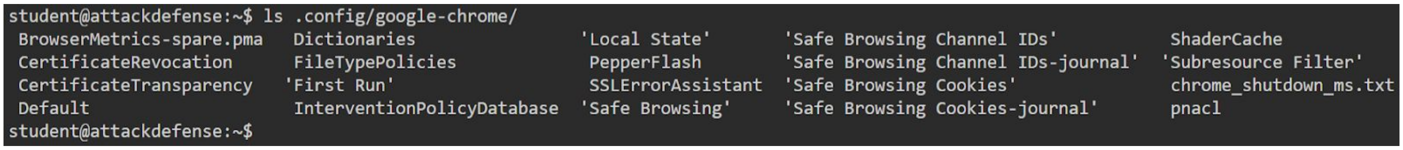


```
student@attackdefense:~$ python tools/hindsight/hindsight.py

################################################################################

                    _     _           _     _       _     _
                   | |   (_)         | |   (_)     | |   | |
                   | |__  _ _ __   __| |___ _  __ _| |__ | |_
                   | '_ \| | '_ \ / _` / __| |/ _` | '_ \| __|
                   | | | | | | | | (_| \__ \ | (_| | | | | |_
                   |_| |_|_|_| |_|\__,_|___/_|\__, |_| |_|\__|
                                               __/ |
                        by @_RyanBenson       |___/   v2.4.0

################################################################################

error: argument -i/--input is required
usage: hindsight.py [-h] -i INPUT [-o OUTPUT] [-b {Chrome,Brave}]
                    [-f {sqlite,jsonl,xlsx}] [-l LOG] [-t TIMEZONE]
                    [-d {mac,linux}] [-c CACHE]
```

Hindsight needs a path to the browser profile directory.

Step 5: Check the path to Google Chrome browser's profile directory

Command: ls .config/google-chrome/

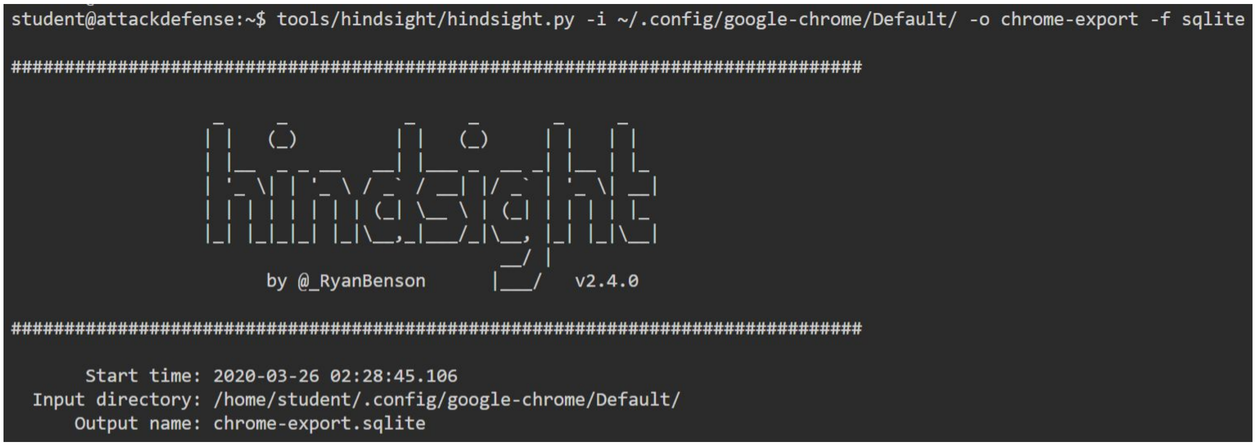


```
student@attackdefense:~$ ls .config/google-chrome/
 BrowserMetrics-spare.pma   Dictionaries               'Local State'         'Safe Browsing Channel IDs'          ShaderCache
 CertificateRevocation      FileTypePolicies            PepperFlash          'Safe Browsing Channel IDs-journal'  'Subresource Filter'
 CertificateTransparency   'First Run'                  SSLErrorAssistant    'Safe Browsing Cookies'               chrome_shutdown_ms.txt
 Default                    InterventionPolicyDatabase 'Safe Browsing'       'Safe Browsing Cookies-journal'       pnacl
student@attackdefense:~$
```

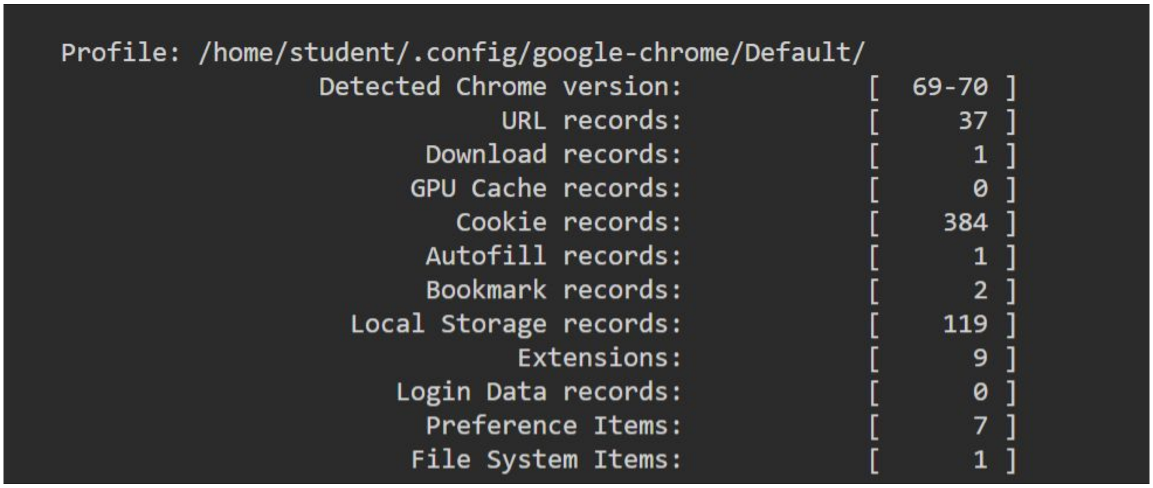
“Default” directory is the profile directory.

Step 6: Export all information to a sqlite3 database.

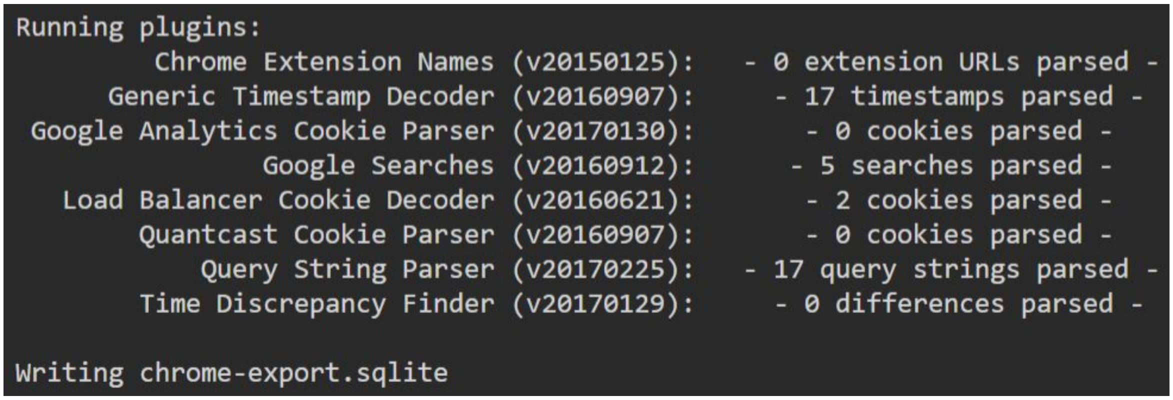
Command: tools/hindsight/hindsight.py -i ~/.config/google-chrome/Default/ -o chrome-export -f sqlite



```
student@attackdefense:~$ tools/hindsight/hindsight.py -i ~/.config/google-chrome/Default/ -o chrome-export -f sqlite

#############################################################################

                  _     _           _     _       _     _
                 | |   (_)         | |   (_)     | |   | |
                 | |__  _ _ __   __| |___ _  __ _| |__ | |_
                 | '_ \| | '_ \ / _` / __| |/ _` | '_ \| __|
                 | | | | | | | | (_| \__ \ | (_| | | | | |_
                 |_| |_|_|_| |_|\__,_|___/_|\__, |_| |_|\__|
                                             __/ |
                       by @_RyanBenson      |___/   v2.4.0

#############################################################################

       Start time: 2020-03-26 02:28:45.106
  Input directory: /home/student/.config/google-chrome/Default/
      Output name: chrome-export.sqlite
```



```
 Profile: /home/student/.config/google-chrome/Default/
                  Detected Chrome version:        [  69-70 ]
                              URL records:        [     37 ]
                         Download records:        [      1 ]
                        GPU Cache records:        [      0 ]
                           Cookie records:        [    384 ]
                         Autofill records:        [      1 ]
                         Bookmark records:        [      2 ]
                    Local Storage records:        [    119 ]
                               Extensions:        [      9 ]
                       Login Data records:        [      0 ]
                         Preference Items:        [      7 ]
                        File System Items:        [      1 ]
```

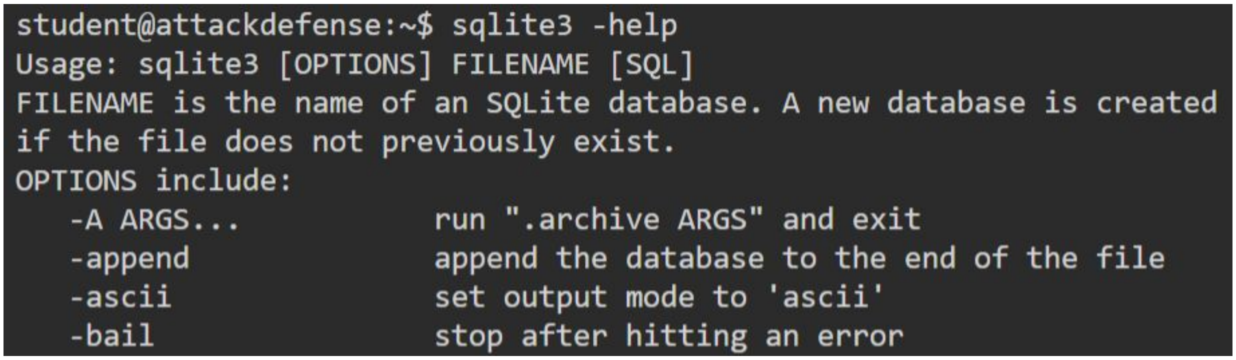


```
Running plugins:
         Chrome Extension Names (v20150125):   - 0 extension URLs parsed -
      Generic Timestamp Decoder (v20160907):     - 17 timestamps parsed -
 Google Analytics Cookie Parser (v20170130):       - 0 cookies parsed -
                Google Searches (v20160912):      - 5 searches parsed -
   Load Balancer Cookie Decoder (v20160621):       - 2 cookies parsed -
        Quantcast Cookie Parser (v20160907):       - 0 cookies parsed -
            Query String Parser (v20170225):   - 17 query strings parsed -
        Time Discrepancy Finder (v20170129):     - 0 differences parsed -

Writing chrome-export.sqlite
```

The data was exported to chrome-export.sqlite file.

Step 7: Check the help options for sqlite3 utility.

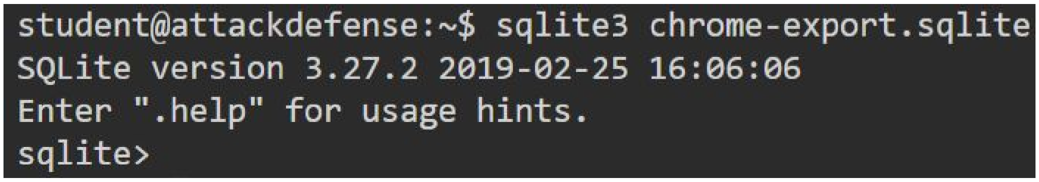
Command: sqlite3 -help



```
student@attackdefense:~$ sqlite3 -help
Usage: sqlite3 [OPTIONS] FILENAME [SQL]
FILENAME is the name of an SQLite database. A new database is created
if the file does not previously exist.
OPTIONS include:
   -A ARGS...           run ".archive ARGS" and exit
   -append              append the database to the end of the file
   -ascii               set output mode to 'ascii'
   -bail                stop after hitting an error
```

Step 8: Open the chrome-export.sqlite file with sqlite3

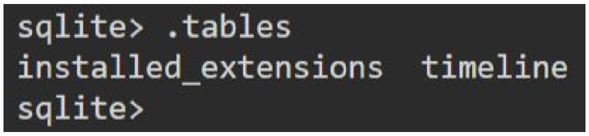
Command: sqlite3 chrome-export.sqlite



```
student@attackdefense:~$ sqlite3 chrome-export.sqlite
SQLite version 3.27.2 2019-02-25 16:06:06
Enter ".help" for usage hints.
sqlite>
```

Step 9: List the tables present in this database file.

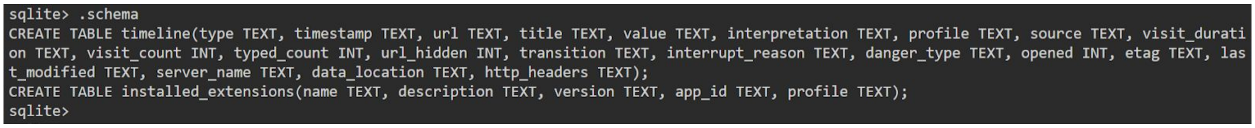
Command: .tables



```
sqlite> .tables
installed_extensions  timeline
sqlite>
```

Step 10: Check the schema of both tables.

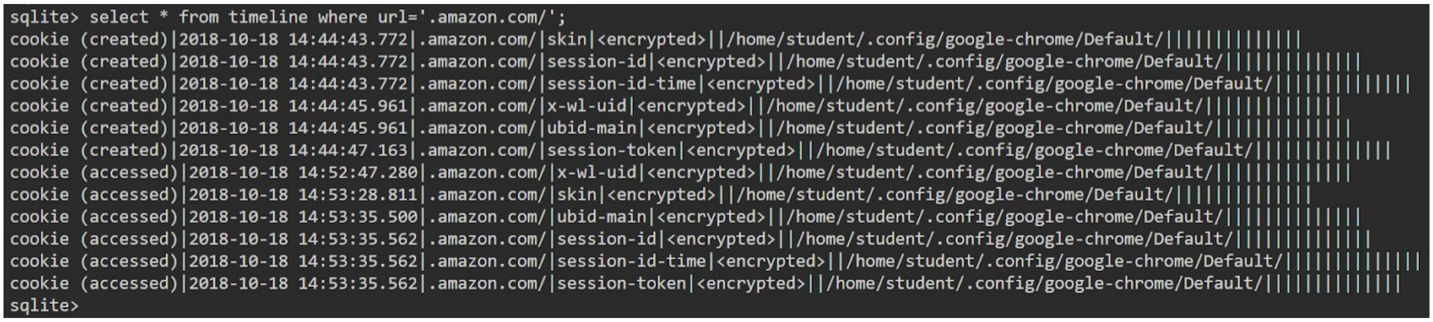
Command: .schema



```
sqlite> .schema
CREATE TABLE timeline(type TEXT, timestamp TEXT, url TEXT, title TEXT, value TEXT, interpretation TEXT, profile TEXT, source TEXT, visit_durati
on TEXT, visit_count INT, typed_count INT, url_hidden INT, transition TEXT, interrupt_reason TEXT, danger_type TEXT, opened INT, etag TEXT, las
t_modified TEXT, server_name TEXT, data_location TEXT, http_headers TEXT);
CREATE TABLE installed_extensions(name TEXT, description TEXT, version TEXT, app_id TEXT, profile TEXT);
sqlite>
```

Step 11: Run a query to list all records related to .amazon.com

Command: select * from timeline where url='.amazon.com/';



```
sqlite> select * from timeline where url='.amazon.com/';
cookie (created)|2018-10-18 14:44:43.772|.amazon.com/|skin|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (created)|2018-10-18 14:44:43.772|.amazon.com/|session-id|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (created)|2018-10-18 14:44:43.772|.amazon.com/|session-id-time|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (created)|2018-10-18 14:44:45.961|.amazon.com/|x-wl-uid|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (created)|2018-10-18 14:44:45.961|.amazon.com/|ubid-main|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (created)|2018-10-18 14:44:47.163|.amazon.com/|session-token|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (accessed)|2018-10-18 14:52:47.280|.amazon.com/|x-wl-uid|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (accessed)|2018-10-18 14:53:28.811|.amazon.com/|skin|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (accessed)|2018-10-18 14:53:35.500|.amazon.com/|ubid-main|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (accessed)|2018-10-18 14:53:35.562|.amazon.com/|session-id|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (accessed)|2018-10-18 14:53:35.562|.amazon.com/|session-id-time|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
cookie (accessed)|2018-10-18 14:53:35.562|.amazon.com/|session-token|<encrypted>||/home/student/.config/google-chrome/Default/||||||||||||||
sqlite>
```

The encrypted cookie ubid-main was created at 2018-10-18 14:44:45.961

Flag: 2018-10-18 14:44:45

References:

1. Browser Bookmark Discovery (https://attack.mitre.org/techniques/T1217/)
2. Hindsight tool (https://github.com/obsidianforensics/hindsight)