
ATTACK
DEFENSE
by PentesterAcademy

Name	Firefox: Cookies
URL	https://www.attackdefense.com/challengedetails?cid=167
Type	Forensics : Browser

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.

Cookies

Question 1: How many cookies are present in Firefox cookie records?

Answer: 324

Solution:

Count the records in moz_cookies

Command: select count(*) from moz_cookies;

```
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$ sqlite3 cookies.sqlite
SQLite version 3.11.0 2016-02-15 17:29:24
Enter ".help" for usage hints.
sqlite>
sqlite> .tables
moz_cookies
sqlite>
sqlite> select count(*) from moz_cookies;
324
sqlite>
```

Question 2: How many cookie entries are there for nytimes.com?

Answer: 19

Solution:

Count cookies for domain nytimes.com

Command: select count(*) from moz_cookies where baseDomain="nytimes.com";

```
sqlite>
sqlite> select count(*) from moz_cookies where baseDomain="nytimes.com";
19
sqlite>
```

Question 3:. What is the name of the 11th field in cookie record?

Answer: isSecure

Solution:

Check the schema of moz_cookies

Command: .schema moz_cookies

```
sqlite> .schema moz_cookies
CREATE TABLE moz_cookies (id INTEGER PRIMARY KEY, baseDomain TEXT, originAttributes TEXT NOT NULL DEFAULT '', name TEXT, value TEXT, host TEXT,
 path TEXT, expiry INTEGER, lastAccessed INTEGER, creationTime INTEGER, isSecure INTEGER, isHttpOnly INTEGER, inBrowserElement INTEGER DEFAULT
0, sameSite INTEGER DEFAULT 0, CONSTRAINT moz_uniqueid UNIQUE (name, host, path, originAttributes));
CREATE INDEX moz_basedomain ON moz_cookies (baseDomain, originAttributes);
sqlite>
```

Question 4: When the latest cookie entry for “bing.com” is going to expire (Answer in DD-MM-YY HH:MM:SS GMT)?

Answer:. 11-11-2019 1:09:57 GMT

Solution:

Check cookie records for “bing.com” and take expiry value (columns).

Command: select * from moz_cookies where baseDomain="bing.com";

```
sqlite> select * from moz_cookies where baseDomain="bing.com";
77|bing.com||MR|0|.bat.bing.com|/|1555286276|1539736294240496|1539733489864225|0|0|0|0
917|bing.com||MUIDB|04ADB6141BA2699F35BCBA9E1FA26A80|bat.bing.com|/|1573432931|1539736294240496|1539736146869416|0|1|0|0
1175|bing.com||ANONCHK|1|.c.bing.com|/|1539739197|1539738597804097|1539738597804097|0|0|0|0
1176|bing.com||MUID|04ADB6141BA2699F35BCBA9E1FA26A80|.bing.com|/|1573434597|1539738597804183|1539733489864149|0|0|0|0
1177|bing.com||MR|0|.c.bing.com|/|1555290597|1539738597804216|1539738597804216|0|0|0|0
1178|bing.com||MUIDB|04ADB6141BA2699F35BCBA9E1FA26A80|c.bing.com|/|1573434597|1539738597804254|1539738597804254|0|1|0|0
sqlite>
```

Convert the value given to GMT date.

Command: date -d @1573434597

```
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$ date -d @1573434597
Mon Nov 11 01:09:57 UTC 2019
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$
```

Question 5: When was the twitter cookie with name "_ga" was accessed by the user last time (Answer in DD-MM-YY HH:MM:SS.uuu GMT)?

Answer: 17-10-2018 1:09:32.746 GMT

Solution:

Get the lastAccessed for _ga cookie of twitter.com from table moz_cookies

Command: select lastAccessed from moz_cookies where baseDomain="twitter.com" and name="_ga";

```
sqlite>
sqlite> select lastAccessed from moz_cookies where baseDomain="twitter.com" and name="_ga";
1539738572746348
sqlite>
```

The timestamp is in microseconds so leave last 6 digits out and convert the rest to dat.

Command: date -d @153978572

```
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$ date -d @1539738572
Wed Oct 17 01:09:32 UTC 2018
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$
```

Take remaining 746348, convert these into milliseconds, which will come to 746

Hence the answer, 17-10-2018 1:09:32.746 GMT

Question 6: Cookies of which baseDomain was accessed most recently?

Answer: facebook.com

Solution:

Find records with maximum Last accessed timestamp value.

Command: select * from moz_cookies where (lastAccessed) in (select max(lastAccessed) from moz_cookies);

```
sqlite> select * from moz_cookies where (lastAccessed) in (select max(lastAccessed) from moz_cookies);
425|facebook.com||sb|uXzGW3NTY-7fDjVrWLNi2fAK|.facebook.com|/|1602805927|1539738614018786|1539733928044516|1|1|0|0
435|facebook.com||datr|uXzGWwr4H0NQWmF-o8FLPn6G|.facebook.com|/|1602805939|1539738614018786|1539733939694772|1|1|0|0
1147|facebook.com||fr|0xeMXHKcJlUf4YFeM..BbxnsE.dm.FvG.0.0.Bbxou1.AWUIsIxl|.facebook.com|/|1547514549|1539738614018786|1539733490377637|1|1|0|0
sqlite>
```

All records belongs to facebook.com domain.

Question 7: How many cookies will be still valid on 1st Jan 2019 00:00:00 GMT

Answer: 217

Solution:

Convert the date to seconds

Command: date "+%s" -d "01/01/2019 00:00:00"

1546300800

Find out records with expiry value more than this number.

Command: select count(*) from moz_cookies where expiry > 1546300800;

```
sqlite> select count(*) from moz_cookies where expiry > 1546300800;
217
sqlite>
```

A total of 217 records or cookies will be still valid.