ATTACK DEFENSE

by PentesterAcademy

Name	Chrome: Cookies
URL	https://www.attackdefense.com/challengedetails?cid=171
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.

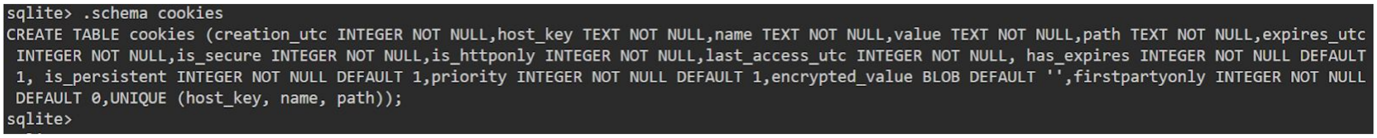
Question 1: What was the exact time at which _gid cookie for coursera.org was added (Provide answer in DD-MM-YYYY HH:MM:SS GMT)?

Answer: 18-10-2018 2:46:20 PM GMT

Solution:

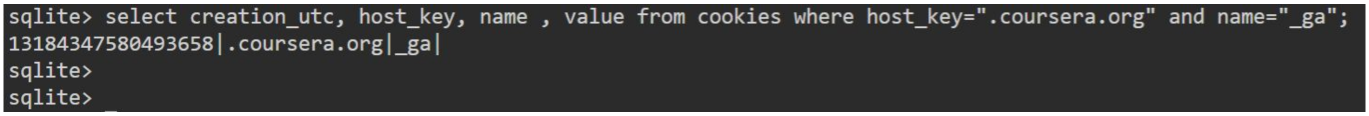
We have to query cookie table in Cookie database. Check the schema of the database.

Command: .schema cookie



```
sqlite> .schema cookies
CREATE TABLE cookies (creation_utc INTEGER NOT NULL,host_key TEXT NOT NULL,name TEXT NOT NULL,value TEXT NOT NULL,path TEXT NOT NULL,expires_utc
 INTEGER NOT NULL,is_secure INTEGER NOT NULL,is_httponly INTEGER NOT NULL,last_access_utc INTEGER NOT NULL, has_expires INTEGER NOT NULL DEFAULT
 1, is_persistent INTEGER NOT NULL DEFAULT 1,priority INTEGER NOT NULL DEFAULT 1,encrypted_value BLOB DEFAULT '',firstpartyonly INTEGER NOT NULL
 DEFAULT 0,UNIQUE (host_key, name, path));
sqlite>
```

Command: select creation_utc, host_key, name , value from cookies where host_key=".coursera.org" and name="_ga";

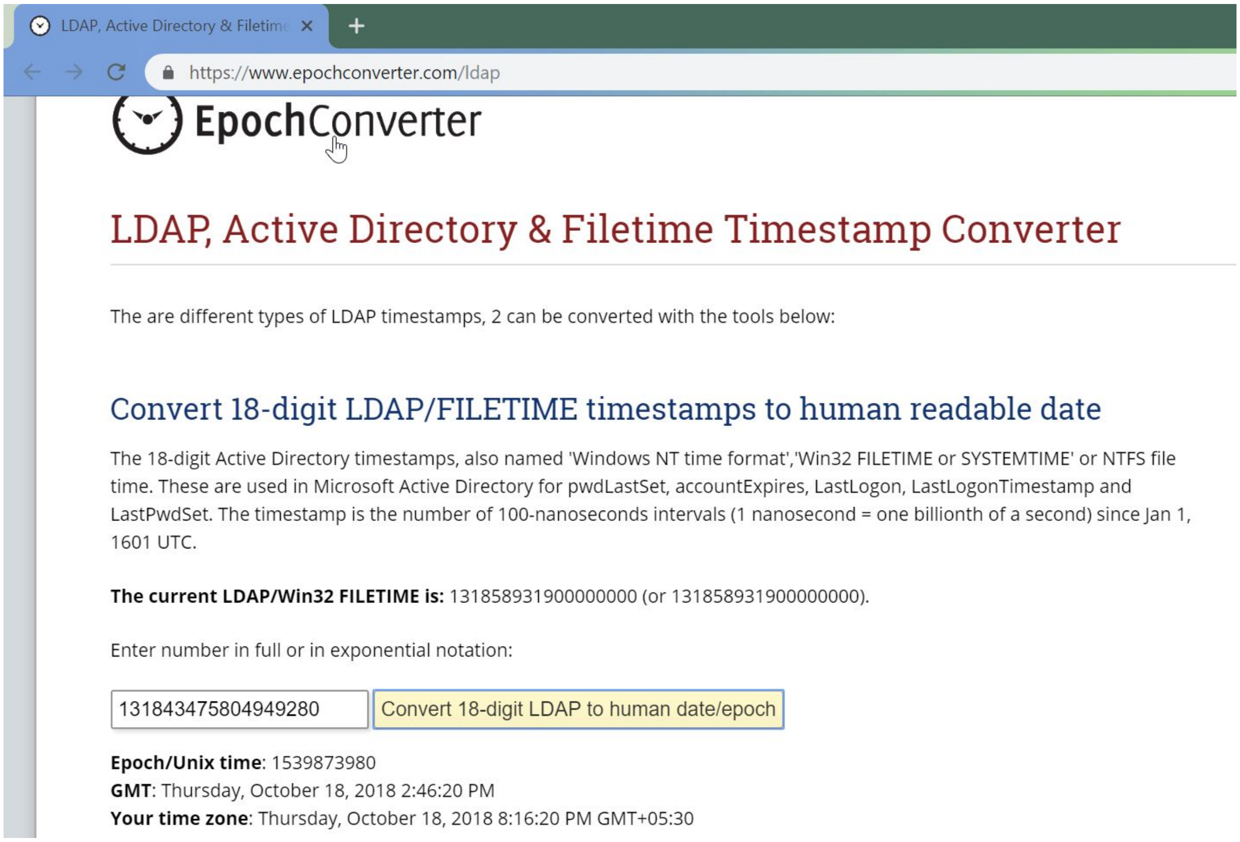


```
sqlite> select creation_utc, host_key, name , value from cookies where host_key=".coursera.org" and name="_ga";
13184347580493658|.coursera.org|_ga|
sqlite>
sqlite> _
```

13184347580494928

This value is seconds from epoch (1 Jan 1601). But, as it is only of 17 digits, so add a 0 to make it 18 digits long). Then, use an online converter to convert it to standard date format.

Converter: https://www.epochconverter.com/ldap



LDAP, Active Directory & Filetime
https://www.epochconverter.com/ldap
EpochConverter

LDAP, Active Directory & Filetime Timestamp Converter

The are different types of LDAP timestamps, 2 can be converted with the tools below:

Convert 18-digit LDAP/FILETIME timestamps to human readable date

The 18-digit Active Directory timestamps, also named 'Windows NT time format','Win32 FILETIME or SYSTEMTIME' or NTFS file time. These are used in Microsoft Active Directory for pwdLastSet, accountExpires, LastLogon, LastLogonTimestamp and LastPwdSet. The timestamp is the number of 100-nanoseconds intervals (1 nanosecond = one billionth of a second) since Jan 1, 1601 UTC.

The current LDAP/Win32 FILETIME is: 131858931900000000 (or 131858931900000000).

Enter number in full or in exponential notation:

131843475804949280 Convert 18-digit LDAP to human date/epoch

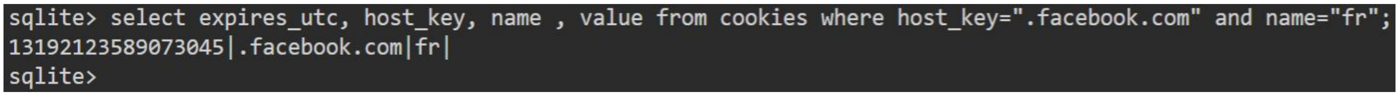
Epoch/Unix time: 1539873980
GMT: Thursday, October 18, 2018 2:46:20 PM
Your time zone: Thursday, October 18, 2018 8:16:20 PM GMT+05:30

Question 2: What is expiry time for “fr” cookie for facebook.com (Provide answer in DD-MM-YYYY HH:MM:SS GMT)?

Answer: 16-01-2019 2:46:29 PM GMT

Solution:

Command: select expires_utc, host_key, name , value from cookies where host_key=".facebook.com" and name="fr";

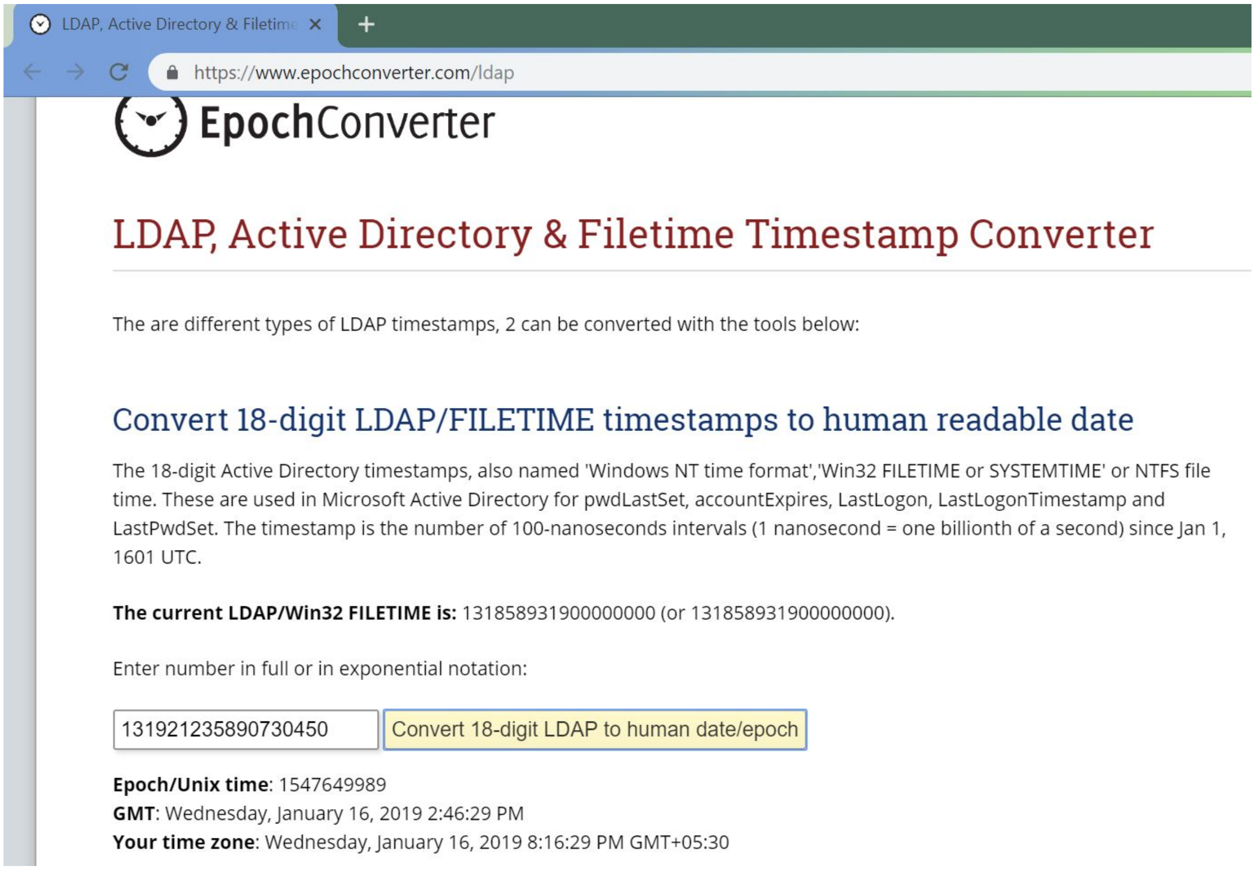


```
sqlite> select expires_utc, host_key, name , value from cookies where host_key=".facebook.com" and name="fr";
13192123589073045|.facebook.com|fr|
sqlite>
```

13192123589073045

This value is seconds from epoch (1 Jan 1601). But, as it is only of 17 digits, so add a 0 to make it 18 digits long). Then, use an online converter to convert it to standard date format.

Converter: https://www.epochconverter.com/ldap



LDAP, Active Directory & Filetime
https://www.epochconverter.com/ldap
EpochConverter

LDAP, Active Directory & Filetime Timestamp Converter

The are different types of LDAP timestamps, 2 can be converted with the tools below:

Convert 18-digit LDAP/FILETIME timestamps to human readable date

The 18-digit Active Directory timestamps, also named 'Windows NT time format','Win32 FILETIME or SYSTEMTIME' or NTFS file time. These are used in Microsoft Active Directory for pwdLastSet, accountExpires, LastLogon, LastLogonTimestamp and LastPwdSet. The timestamp is the number of 100-nanoseconds intervals (1 nanosecond = one billionth of a second) since Jan 1, 1601 UTC.

The current LDAP/Win32 FILETIME is: 131858931900000000 (or 131858931900000000).

Enter number in full or in exponential notation:

131921235890730450 | Convert 18-digit LDAP to human date/epoch

Epoch/Unix time: 1547649989
GMT: Wednesday, January 16, 2019 2:46:29 PM
Your time zone: Wednesday, January 16, 2019 8:16:29 PM GMT+05:30

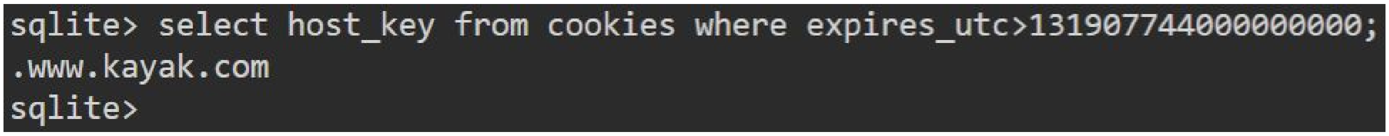
Question 3: How many cookies will be valid on 01-01-2019 12:00:00 AM GMT?

Answer: 1

Solution:

Convert 01-01-2019 12:00:00 AM GMT to seconds from epoch (1 Jan 1601) and drop last digit.

Command: select host_key from cookies where expires_utc>131907744000000000;



```
sqlite> select host_key from cookies where expires_utc>131907744000000000;
.www.kayak.com
sqlite>
```