
ATTACK
DEFENSE
by PentesterAcademy

Name	Firefox: History
URL	https://www.attackdefense.com/challengedetails?cid=165
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.

History

Question 1: Which travel website the user used to check for flights?

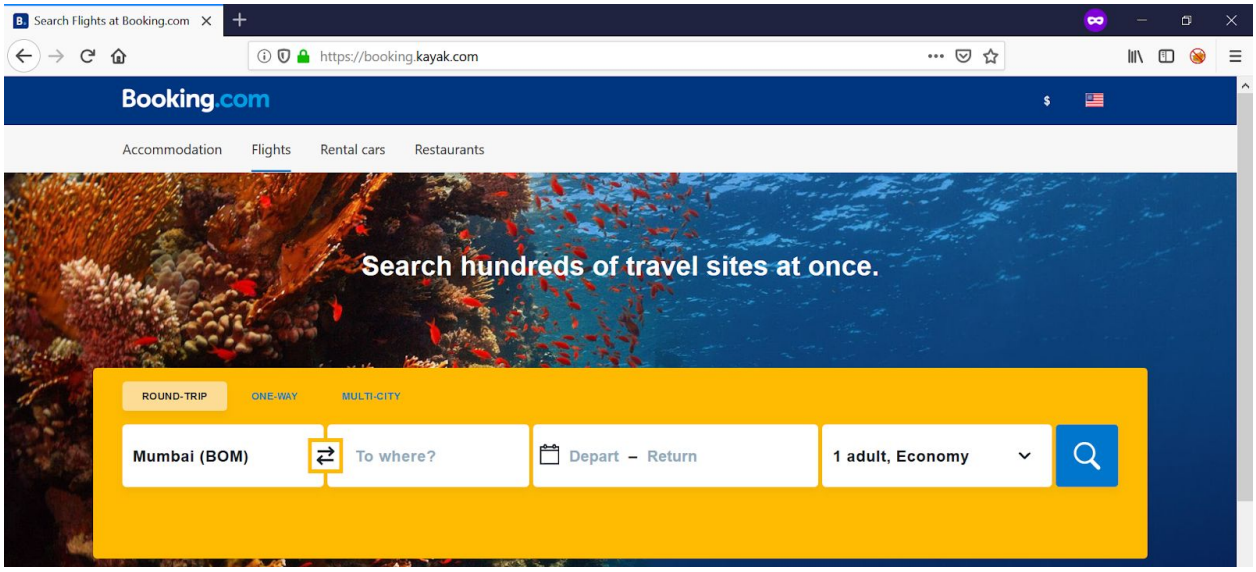
Answer: Booking.com

Solution:

Command: select * from moz_places;

```
35|https://booking.kayak.com/flights/SFO-AMS/2018-11-16/2018-11-16|SFO to AMS, 11/16 – 11/16|moc.kayak.gnikoob.|1|0|0|98|1539733784949166|EC9iu
zZjej-8|0|47358259728303|Booking.com searches hundreds of flight sites at once to find the information you need to make the right decisions on
flights.|https://booking.kayak.com/rimg/dimg/92/c5/5687cba1-city-1334-162d3e56fea.jpg?width=1200&height=630&crop=true&xhint=1873&yhint=1504
36|https://booking.kayak.com/flights/SFO-AMS/2018-11-16/2018-11-16?sort=bestflight_a|SFO to AMS, 11/16 – 11/16|moc.kayak.gnikoob.|1|0|0|98|1539
733798749179|5oSlwrG_p8Zk|0|47359115848050||
```

Subdomain “booking.kayak.com” belongs to booking.com.



Question 2: Which was the destination country for which the user checked/booked the flights?

Answer: Netherlands

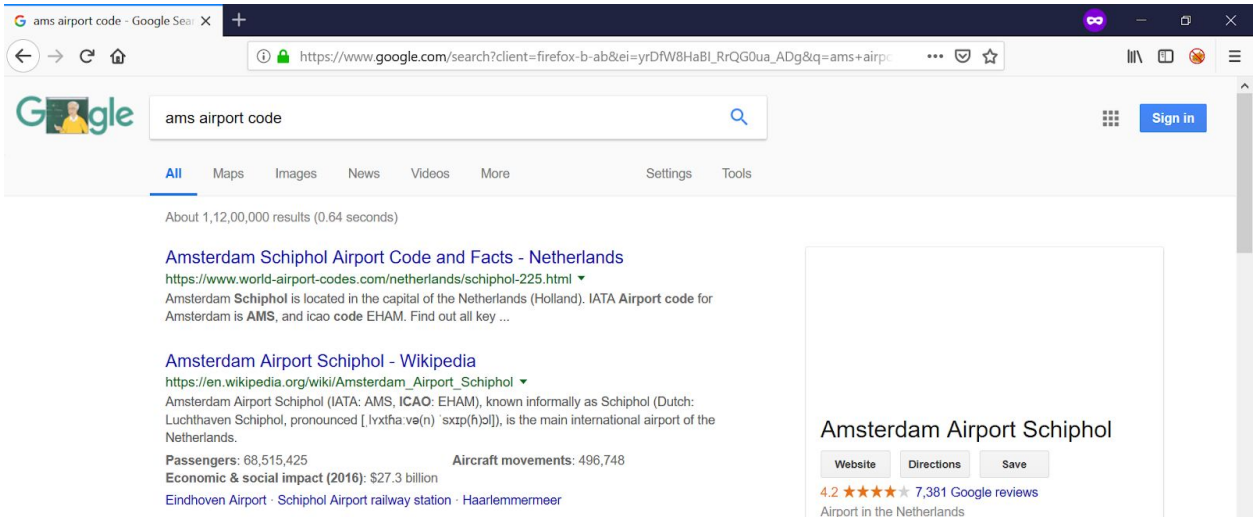
Solution:

Check the moz_places table.

Command: select * from moz_places;

```
35|https://booking.kayak.com/flights/SFO-AMS/2018-11-16/2018-11-16|SFO to AMS, 11/16 – 11/16|moc.kayak.gnikoob.|1|0|0|98|1539733784949166|EC9iu
zZjej-8|0|47358259728303|Booking.com searches hundreds of flight sites at once to find the information you need to make the right decisions on
flights.|https://booking.kayak.com/rimg/dimg/92/c5/5687cba1-city-1334-162d3e56fea.jpg?width=1200&height=630&crop=true&xhint=1873&yhint=1504
36|https://booking.kayak.com/flights/SFO-AMS/2018-11-16/2018-11-16?sort=bestflight_a|SFO to AMS, 11/16 – 11/16|moc.kayak.gnikoob.|1|0|0|98|1539
733798749179|5oSlwrG_p8Zk|0|47359115848050||
```

Searching for code AMS, gives us Amsterdam Airport which is in Netherlands.



Question 3: Which website was opened last?

Answer: nytimes.com

Solution:

Check the last entry of the moz_places table.

Command: select * from moz_places;

```
124|http://nytimes.com/||moc.semityn.|1|1|1|25|1539738567976272|x5lYErxyLAQs|0|125507682844000||
125|https://www.nytimes.com/|The New York Times - Breaking News, World News & Multimedia|moc.semityn.www.|1|0|0|2000|1539738568149660|61fJetiTE
rWf|0|47360170288137|The New York Times: Find breaking news, multimedia, reviews & opinion on Washington, business, sports, movies, travel, boo
ks, jobs, education, real estate, cars & more at nytimes.com.|https://static01.nyt.com/newsgraphics/images/icons/defaultPromoCrop.png
```

Question 4: What is the name (complete name with extension) of the torrent file downloaded by the user?

Answer: ubuntu-18.04.1-desktop-amd64.iso.torrent

Solution:

First option is to check the URL list for word torrent.

Command: select * from moz_places where url like '%torrent%';

```
sqlite> select * from moz_places where url like '%torrent%';
76|https://www.google.com/search?client=ubuntu&channel=fs&q=downoad+ubuntu+torrent&ie=utf-8&oe=utf-8|downoad ubuntu torrent - Google Search|moc
.elgoog.www.|1|0|1|2000|1539735035304558|R8fxVxHEtNH5|0|47358975148251||
78|http://releases.ubuntu.com/18.04/ubuntu-18.04.1-desktop-amd64.iso.torrent?_ga=2.212506516.1453540542.1539735050-487258626.1539735050|ubuntu-
18.04.1-desktop-amd64.iso.torrent|moc.utnubu.sesaeler.|0|0|0|0|1539735107178000|iDCEz_2gETo_|0|125509217591951||
sqlite>
```

Second option is to check moz_annos table.

Command: select * from moz_annos;

```
sqlite> select * from moz_annos;
1|12|5|UTF-8|0|4|3|1539646978768000|1539646978768000
2|15|5|UTF-8|0|4|3|1539650024946000|1539650024946000
3|23|5|UTF-8|0|4|3|1539732744919000|1539732744919000
4|26|5|UTF-8|0|4|3|1539732876149000|1539732876149000
5|28|5|UTF-8|0|4|3|1539733372952000|1539733372952000
6|75|7|file:///home/pentester/Downloads/80211-05_0123r1(1).pdf|0|5|3|1539735004808000|1539735015175000
7|75|8|{"state":1,"endTime":1539735015402,"fileSize":924274}|0|5|3|1539735005256000|1539735015402000
8|78|7|file:///tmp/mozilla_pentester0/ubuntu-18.04.1-desktop-amd64.iso-1.torrent|0|5|3|1539735070922000|1539735107201000
9|78|8|{"state":1,"endTime":1539735107238,"fileSize":74860}|0|5|3|1539735071277000|1539735107240000
sqlite>
```

Question 5: How many unique hosts (sub-domains) were accessed using Firefox?

Answer: 36

Solution:

Count the entries in table moz_hosts

Command: select count(*) from moz_hosts;

```
sqlite> select count(*) from moz_hosts;
36
sqlite>
```

Question 6: How many files the user downloaded using Firefox?

Answer: 2

Solution:

Second option is to check moz_annos table.

Command: select * from moz_annos;

```
sqlite> select * from moz_annos;
1|12|5|UTF-8|0|4|3|1539646978768000|1539646978768000
2|15|5|UTF-8|0|4|3|1539650024946000|1539650024946000
3|23|5|UTF-8|0|4|3|1539732744919000|1539732744919000
4|26|5|UTF-8|0|4|3|1539732876149000|1539732876149000
5|28|5|UTF-8|0|4|3|1539733372952000|1539733372952000
6|75|7|file:///home/pentester/Downloads/80211-05_0123r1(1).pdf|0|5|3|1539735004808000|1539735015175000
7|75|8|{"state":1,"endTime":1539735015402,"fileSize":924274}|0|5|3|1539735005256000|1539735015402000
8|78|7|file:///tmp/mozilla_pentester0/ubuntu-18.04.1-desktop-amd64.iso-1.torrent|0|5|3|1539735070922000|1539735107201000
9|78|8|{"state":1,"endTime":1539735107238,"fileSize":74860}|0|5|3|1539735071277000|1539735107240000
sqlite>
```

Question 7: How many time target user accessed https://facebook.com from the browser?

Answer: 2

Solution:

First, we have to check the ID for the facebook URL in moz_places

Command: select * from moz_places;

```
40|http://facebook.com/||moc.koobecaf.|2|0|1|2025|1539738549231120|GmqZv1hxQPWv|0|125509292233111||
41|https://facebook.com/||moc.koobecaf.|2|1|0|50|1539738549399943|8KXiSRDR78Fi|0|47356606673666||
42|https://www.facebook.com/|Facebook - Log In or Sign Up|moc.koobecaf.www.|2|0|0|90|1539738549815920|td_PQZ_53e90|0|47358661893743|Create an a
ccount or log into Facebook. Connect with friends, family and other people you know. Share photos and videos, send messages and get updates.|ht
tps://www.facebook.com/images/fb_icon_325x325.png
```

Now, we can query moz_historyvisits table using this id.

Command: select * from moz_historyvisits where place_id=41;

```
sqlite> select count(*) from moz_historyvisits where place_id=41;
2
sqlite>
sqlite>
sqlite> select * from moz_historyvisits where place_id=41;
26|25|41|1539733927634366|6|0
127|126|41|1539738549399943|5|0
sqlite>
```