

[illegible]

Name	Chrome: Bookmarks
URL	https://www.attackdefense.com/challengedetails?cid=170
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: How many bookmarks are there in chrome (default and user added)?

Answer: 2

Solution:

This information is present in Bookmarks JSON file.

Command: cat Bookmarks

```
"bookmark_bar": {
  "children": [ {
    "date_added": "13184347503625749",
    "id": "5",
    "meta_info": {
      "last_visited_desktop": "13184348008583968"
    },
    "name": "Online shopping",
    "type": "url",
    "url": "https://www.amazon.com/"
  }, {
    "date_added": "13184347977294979",
    "id": "6",
    "meta_info": {
      "last_visited_desktop": "13184347977295492"
    },
    "name": "The New York Times - Breaking News, World News & Multimedia",
    "type": "url",
    "url": "https://www.nytimes.com/"
  } ]
}
```

Observe that there are two entries.

Question 2: Which e-commerce company is bookmarked by the target user?

Answer: Amazon

Solution:

This information is present in Bookmarks JSON file.

Command: cat Bookmarks

```
"bookmark_bar": {
  "children": [ {
    "date_added": "13184347503625749",
    "id": "5",
    "meta_info": {
      "last_visited_desktop": "13184348008583968"
    },
    "name": "Online shopping",
    "type": "url",
    "url": "https://www.amazon.com/"
  }, {
    "date_added": "13184347977294979",
    "id": "6",
    "meta_info": {
      "last_visited_desktop": "13184347977295492"
    },
    "name": "The New York Times - Breaking News, World News & Multimedia",
    "type": "url",
    "url": "https://www.nytimes.com/"
  } ],
}
```

Amazon is bookmarked.

Question 3: When was the entry for a NYtimes was added (Provide answer in DD-MM-YYYY HH:MM:SS GMT)?

Answer: 18-10-2018 2:52:57 PM GMT

Solution:

This information is present in Bookmarks JSON file.

Command: cat Bookmarks

Value mentioned in date_added field of NYtimes JSON record is 13184347977294979.

```

"bookmark_bar": {
  "children": [ {
    "date_added": "13184347503625749",
    "id": "5",
    "meta_info": {
      "last_visited_desktop": "13184348008583968"
    },
    "name": "Online shopping",
    "type": "url",
    "url": "https://www.amazon.com/"
  }, {
    "date_added": "13184347977294979",
    "id": "6",
    "meta_info": {
      "last_visited_desktop": "13184347977295492"
    },
    "name": "The New York Times - Breaking News, World News & Multimedia",
    "type": "url",
    "url": "https://www.nytimes.com/"
  } ],

```

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>

The screenshot shows a web browser at the URL <https://www.epochconverter.com/ldap>. The page title is "Convert 18-digit LDAP/FILETIME timestamps to human readable date". The text explains that 18-digit Active Directory timestamps are used in Microsoft Active Directory for various fields like pwdLastSet and accountExpires. It states that the timestamp is the number of 100-nanosecond intervals since Jan 1, 1601 UTC.

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

Enter number in full or in exponential notation:

Input field: 131843479772949790

Button: Convert 18-digit LDAP to human date/epoch

Epoch/Unix time: 1539874377

GMT: Thursday, October 18, 2018 2:52:57 PM

Your time zone: Thursday, October 18, 2018 8:22:57 PM GMT+05:30