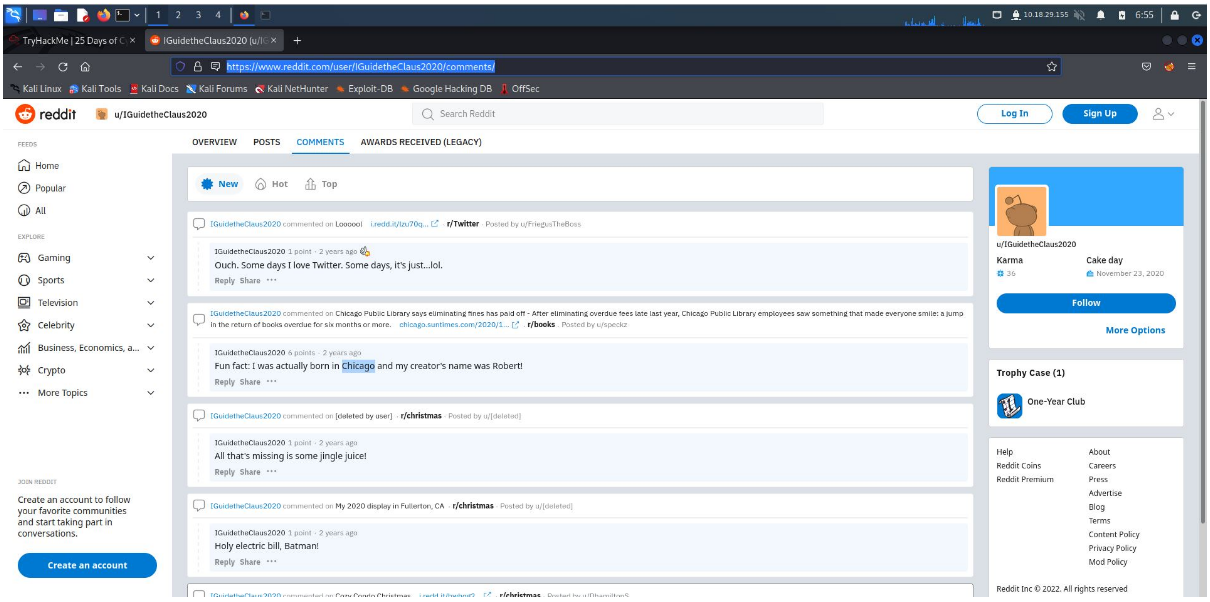
Day 14 - [OSINT] Where's Rudolph?

Tool Used: firefox, Google Image, Twitter, Reddit, Exif data viewer

Solution/walkthrough:

Q1



https://www.reddit.com/user/IGuidetheClaus2020/comments/

u/IGuidetheClaus2020

OVERVIEW POSTS COMMENTS AWARDS RECEIVED (LEGACY)

IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... · r/Twitter · Posted by u/FriegusTheBoss

IGuidetheClaus2020 1 point · 2 years ago
Ouch. Some days I love Twitter. Some days, it's just...lol.

IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more. chicago.suntimes.com/2020/1... · r/books · Posted by u/speckz

IGuidetheClaus2020 6 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!

IGuidetheClaus2020 commented on [deleted by user] · r/christmas · Posted by u/[deleted]

IGuidetheClaus2020 1 point · 2 years ago
All that's missing is some jingle juice!

IGuidetheClaus2020 commented on My 2020 display in Fullerton, CA · r/christmas · Posted by u/[deleted]

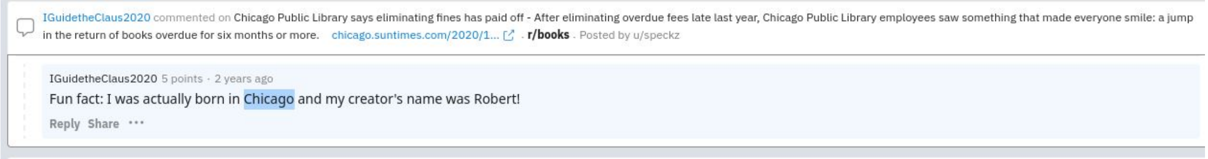
IGuidetheClaus2020 1 point · 2 years ago
Holy electric bill, Batman!

u/IGuidetheClaus2020
Karma 36
Cake day November 23, 2020

Trophy Case (1)
One-Year Club

Search the ‘IGuidetheClaus2020' in Reddit, to directly get into comment history, use the url after choosing comments options.

Q2

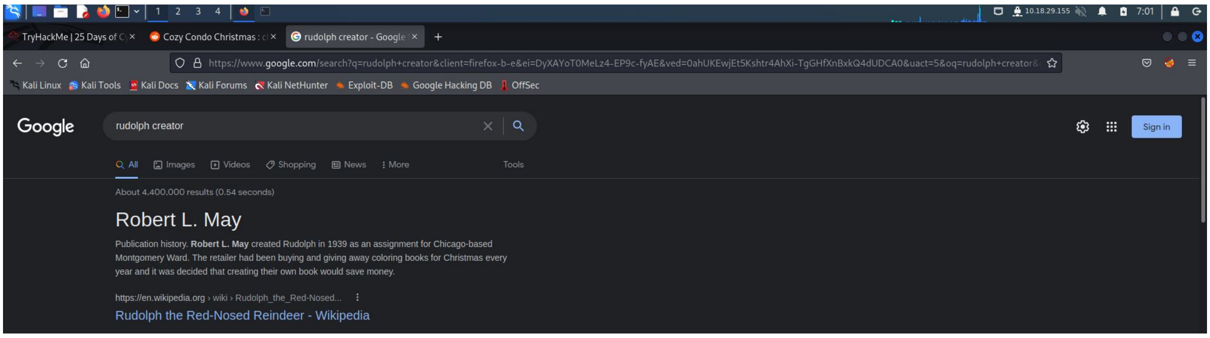


IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more. chicago.suntimes.com/2020/1... · r/books · Posted by u/speckz

IGuidetheClaus2020 5 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!

From the comment, we can know where he was born.

Q3



https://www.google.com/search?q=rudolph+creator&client=firefox-b-e&ei=DyXAYoT0MeLz4-EP9c-fyAE&ved=0ahUKEwjEt5Kshtr4AhXi-TgGHfXnBxkQ4dUDCA0&uact=5&oq=rudolph+creator&

rudolph creator

About 4,400,000 results (0.54 seconds)

Robert L. May

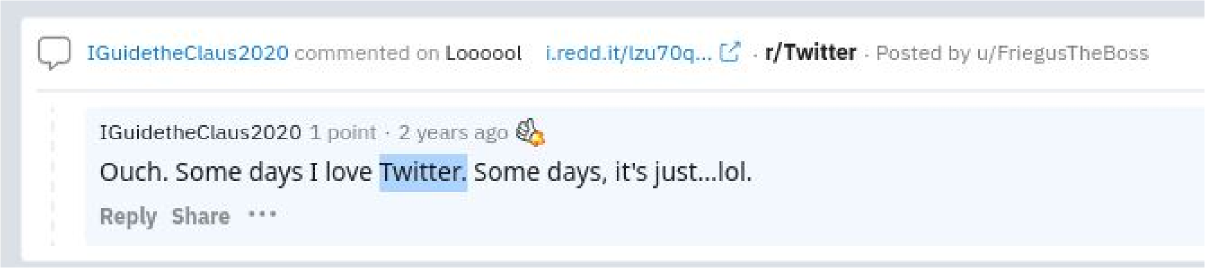
Publication history. **Robert L. May** created Rudolph in 1939 as an assignment for Chicago-based Montgomery Ward. The retailer had been buying and giving away coloring books for Christmas every year and it was decided that creating their own book would save money.

https://en.wikipedia.org › wiki › Rudolph_the_Red-Nosed...

Rudolph the Red-Nosed Reindeer - Wikipedia

Search ‘rudolph creator’ in google to find.

Q4



IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... · r/Twitter · Posted by u/FriegusTheBoss

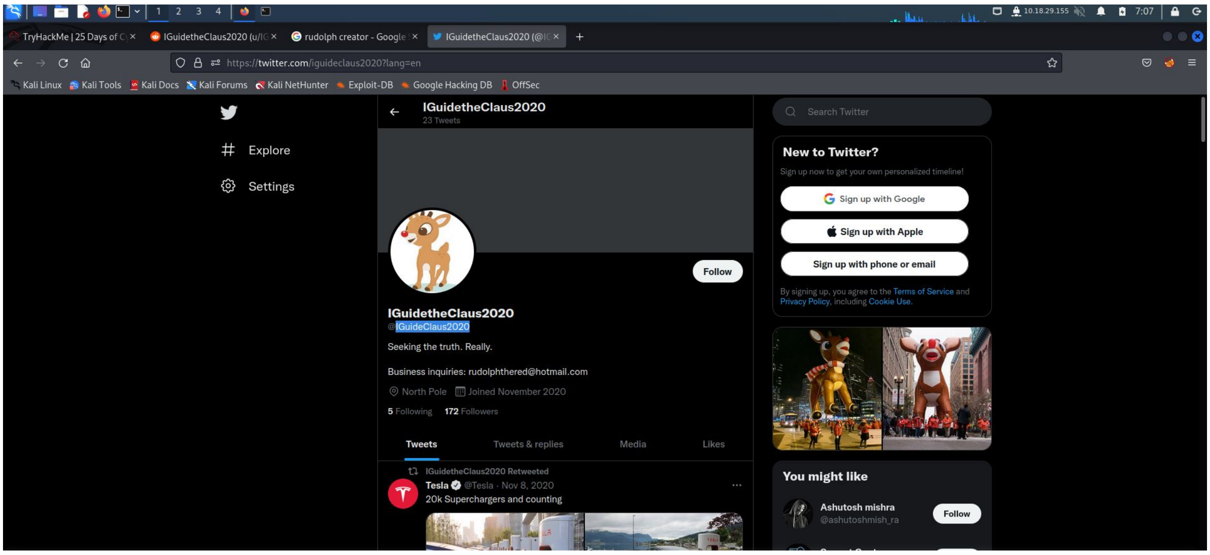
IGuidetheClaus2020 1 point · 2 years ago

Ouch. Some days I love Twitter. Some days, it's just...lol.

Reply Share ···

Rudolph had mentioned the previous social media platform used in the comment.

Q5



https://twitter.com/iguideclaus2020?lang=en

IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

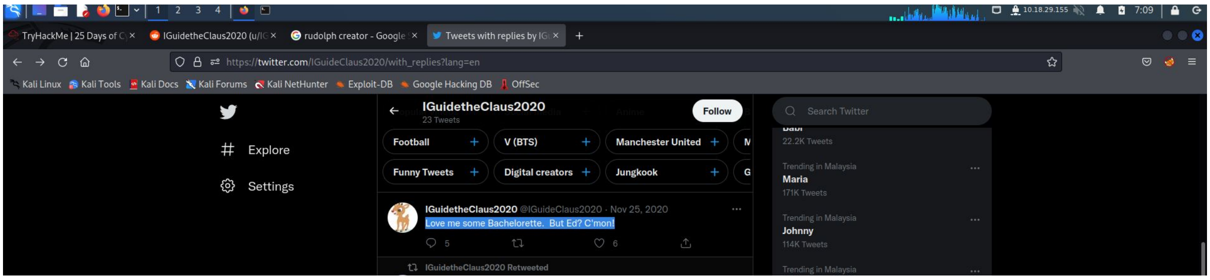
North Pole Joined November 2020

5 Following 172 Followers

IGuidetheClaus2020 Retweeted
Tesla @Tesla · Nov 8, 2020
20k Superchargers and counting

On Twitter, searching for the same name as in Reddit, then the name has been revealed.

Q6



https://twitter.com/IGuideClaus2020/with_replies?lang=en

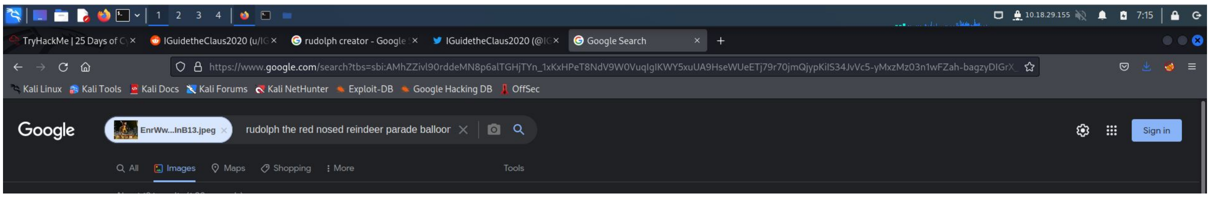
IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Love me some Bachelorette. But Ed? C'mon!

IGuidetheClaus2020 Retweeted

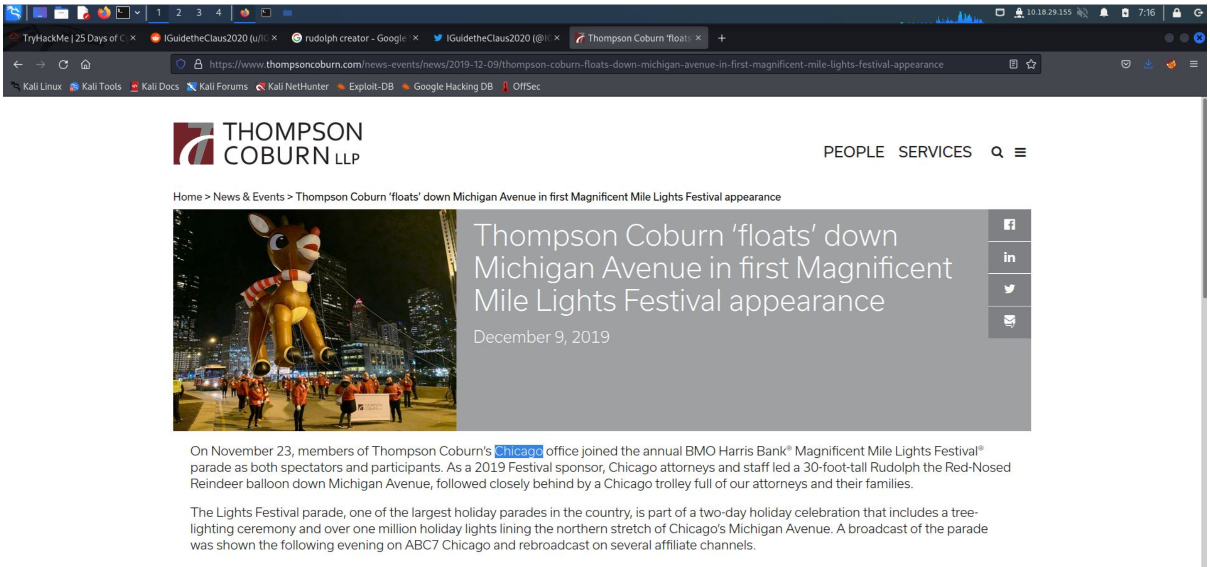
In the tweet below, Rudolph has posted his favourite TV show.

Q7



https://www.google.com/search?tbs=sbi:AMhZZivl90rddeMN8p6alTGHjTYn_1xKxHPeT8NdV9W0VuqIgIKWY5xuUA9HseWUeETj79r70jmQjypKilS34JvVc5-yMxzMz03n1wFZah-bagzyDlGrX

rudolph the red nosed reindeer parade balloor



https://www.thompsoncoburn.com/news-events/news/2019-12-09/thompson-coburn-floats-down-michigan-avenue-in-first-magnificent-mile-lights-festival-appearance

Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

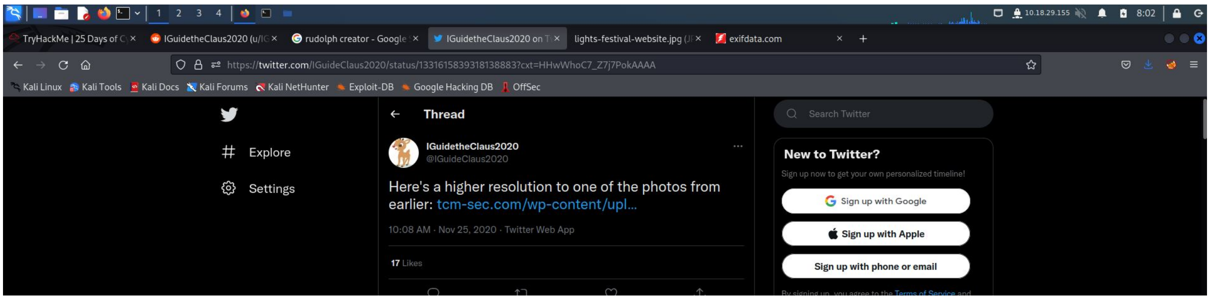
December 9, 2019

On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following evening on ABC7 Chicago and rebroadcast on several affiliate channels.

In the post, use the posted picture to find related info using google image. Then investigate the relevant post. After some investigation, the place was found in the news.

Q8



https://twitter.com/IGuideClaus2020/status/1331615839318138883?cxt=HHwWhoC7_Z7j7PokAAAA

Thread

IGuidetheClaus2020
@IGuideClaus2020

Here's a higher resolution to one of the photos from earlier: tcm-sec.com/wp-content/upl...

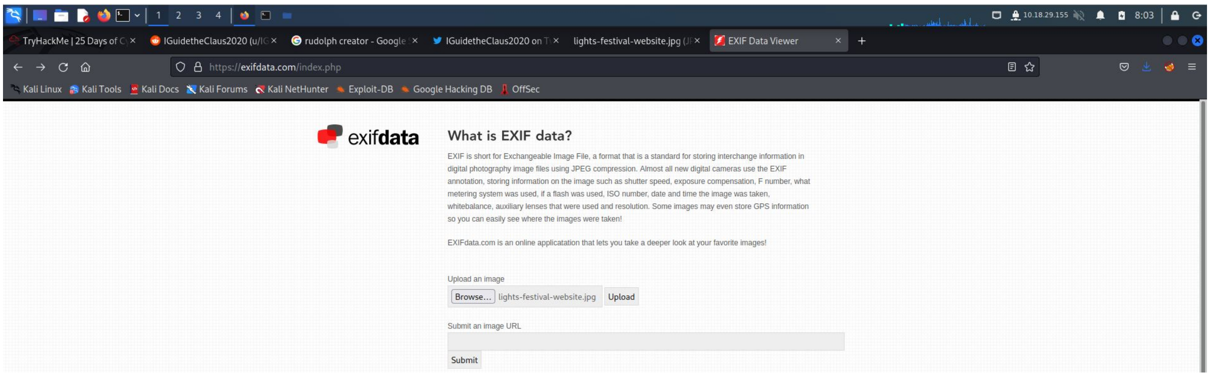
10:08 AM · Nov 25, 2020 · Twitter Web App

17 Likes

New to Twitter?

Sign up now to get your own personalized timeline!

Since Rudolph does post a higher resolution photo, the photo can be used for further investigation.



What is EXIF data?

EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Almost all new digital cameras use the EXIF annotation, storing information on the image such as shutter speed, exposure compensation, F number, what metering system was used, if a flash was used, ISO number, date and time the image was taken, whitebalance, auxiliary lenses that were used and resolution. Some images may even store GPS information so you can easily see where the images were taken!

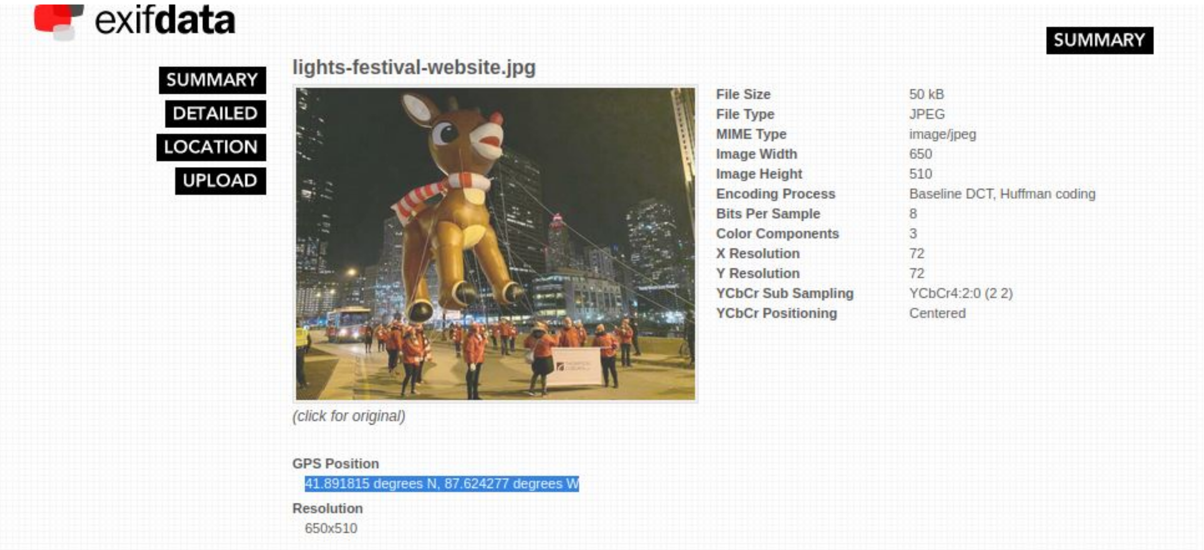
EXIFdata.com is an online applicatation that lets you take a deeper look at your favorite images!

Upload an image

lights-festival-website.jpg

Submit an image URL

Use the EXIF viewer to see the EXIF data of the high resolution photo.



lights-festival-website.jpg

File Size	50 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered

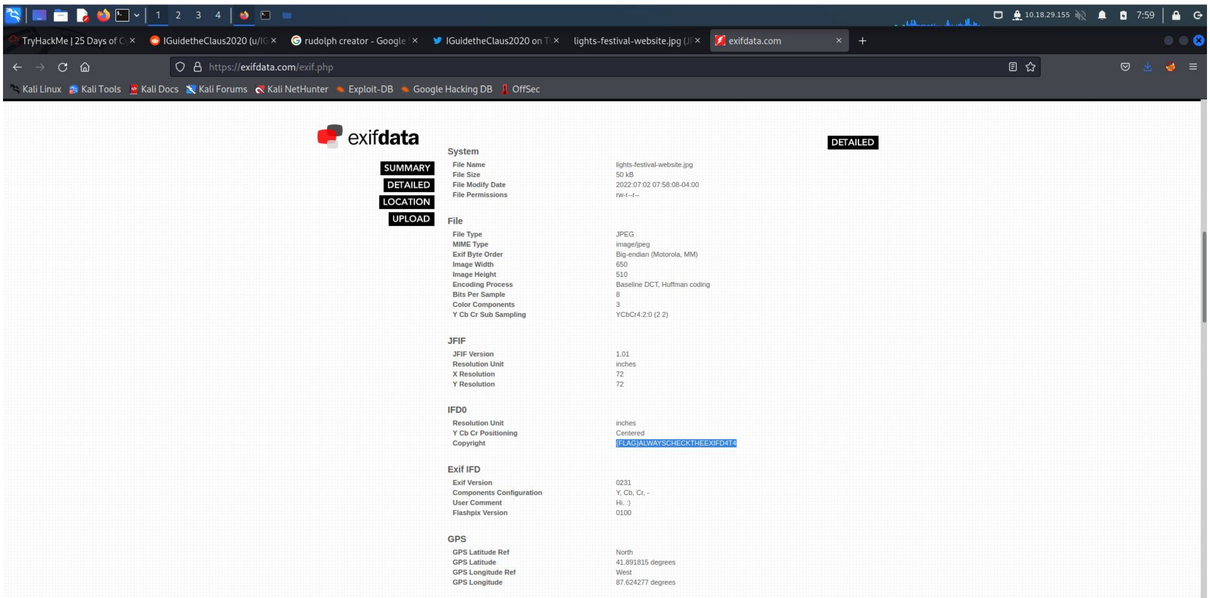
(click for original)

GPS Position
41.891815 degrees N, 87.624277 degrees W

Resolution
650x510

In the result, the position is revealed.

Q8



System

File Name	lights-festival-website.jpg
File Size	50 kB
File Modify Date	2022:07:02 07:58:08-04:00
File Permissions	rw-r--r--

File

File Type	JPEG
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

JFIF

JFIF Version	1.01
Resolution Unit	inches
X Resolution	72
Y Resolution	72

IFD0

Resolution Unit	inches
Y Cb Cr Positioning	Centered
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4

Exif IFD

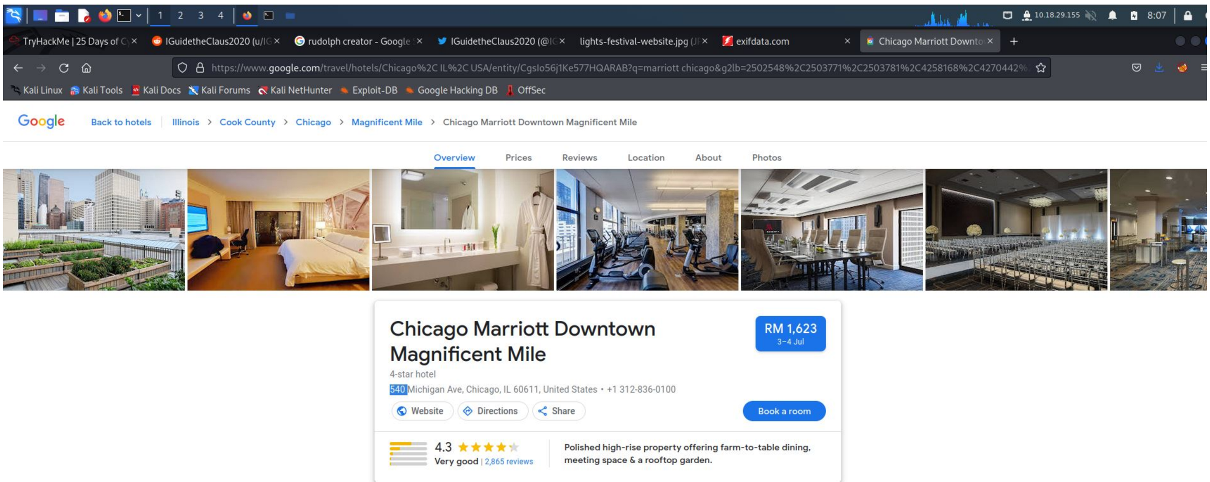
Exif Version	0231
Components Configuration	Y, Cb, Cr, -
User Comment	Hi. :)
Flashpix Version	0100

GPS

GPS Latitude Ref	North
GPS Latitude	41.891815 degrees
GPS Longitude Ref	West
GPS Longitude	87.624277 degrees

The flag is found in the details of EXIF data.

Q11



https://www.google.com/travel/hotels/Chicago%2C IL%2C USA/entity/CgsIo56j1Ke577HQARAB?q=marriott chicago&g2lb=2502548%2C2503771%2C2503781%2C4258168%2C4270442%

Illinois > Cook County > Chicago > Magnificent Mile > Chicago Marriott Downtown Magnificent Mile

Chicago Marriott Downtown Magnificent Mile

RM 1,623
3–4 Jul

4-star hotel

540 Michigan Ave, Chicago, IL 60611, United States • +1 312-836-0100

4.3 ★★★★★
Very good | 2,865 reviews

Polished high-rise property offering farm-to-table dining, meeting space & a rooftop garden.

Since Rudolph does mention he is in marriott, and he is in chicago, search ‘chicago marriott’ in google, we can find the detailed info about the hotel, which contains the street number.