Walkthrough/ Write-up: OhSINT TryHackMe

Tamanna Agrawal · Follow

5 min read · Aug 15, 2023

Listen Share More

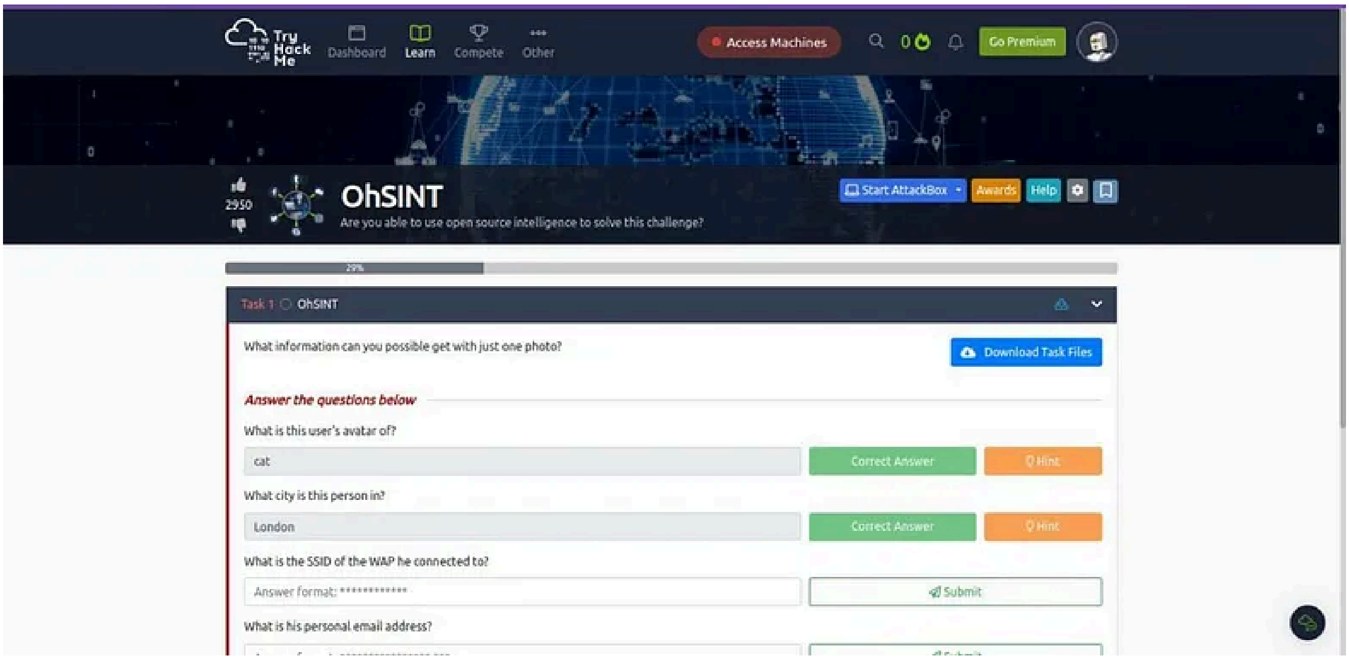
This *TryHackMe* activity is all about learning how to gather information from the internet, which we call open-source intelligence gathering or *OSINT*. You'll find out different ways to collect and study information from places like social media, websites, and other online sources.

If you're into *cybersecurity*, it's really important to know how to use OSINT to learn useful things about a target and find weak points that could be taken advantage of.

https://tryhackme.com/room/ohsint

There's just one main thing to do in this activity, but you'll need to answer seven questions to complete it.

To get started, we need to get the Task Files. Just click the blue button at the top of Task 1 that says 'Download Task Files,' like you can see in the picture below.



OhSINT

Are you able to use open source intelligence to solve this challenge?

Task 1 ○ OhSINT

What information can you possible get with just one photo?

Answer the questions below

What is this user's avatar of?

cat

What city is this person in?

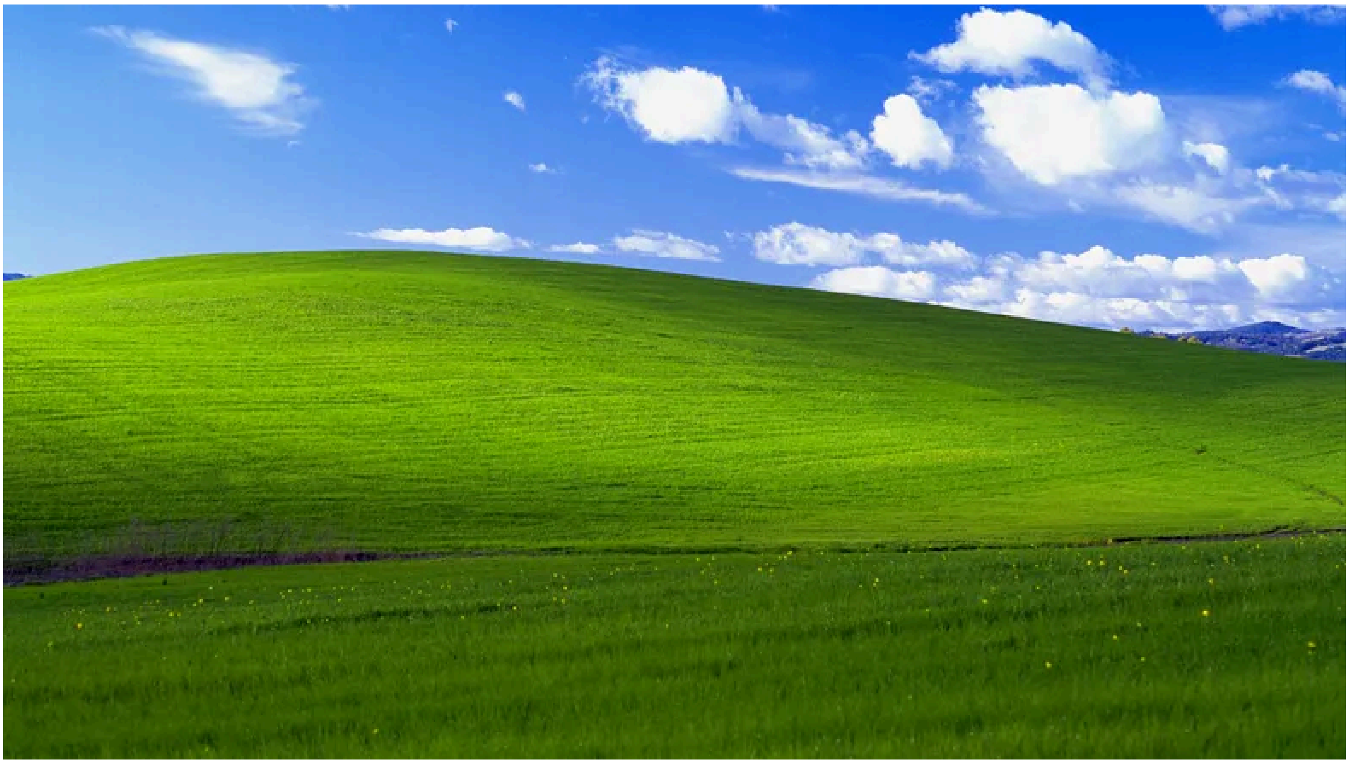
London

What is the SSID of the WAP he connected to?

Answer format: ************

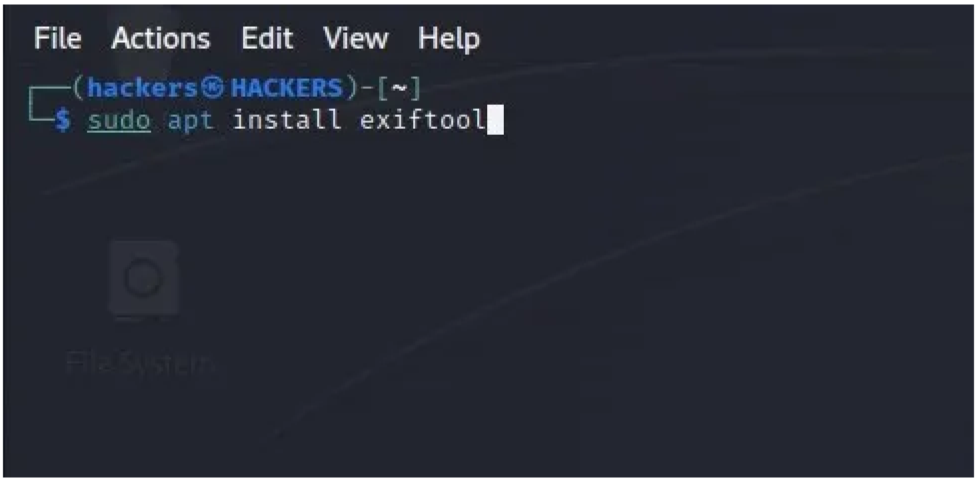
What is his personal email address?

This action will enable us to obtain an image file called “*WindowsXP.jpg*”, which is shown below.



If you see the image, you will find that there is no information available from the given image.

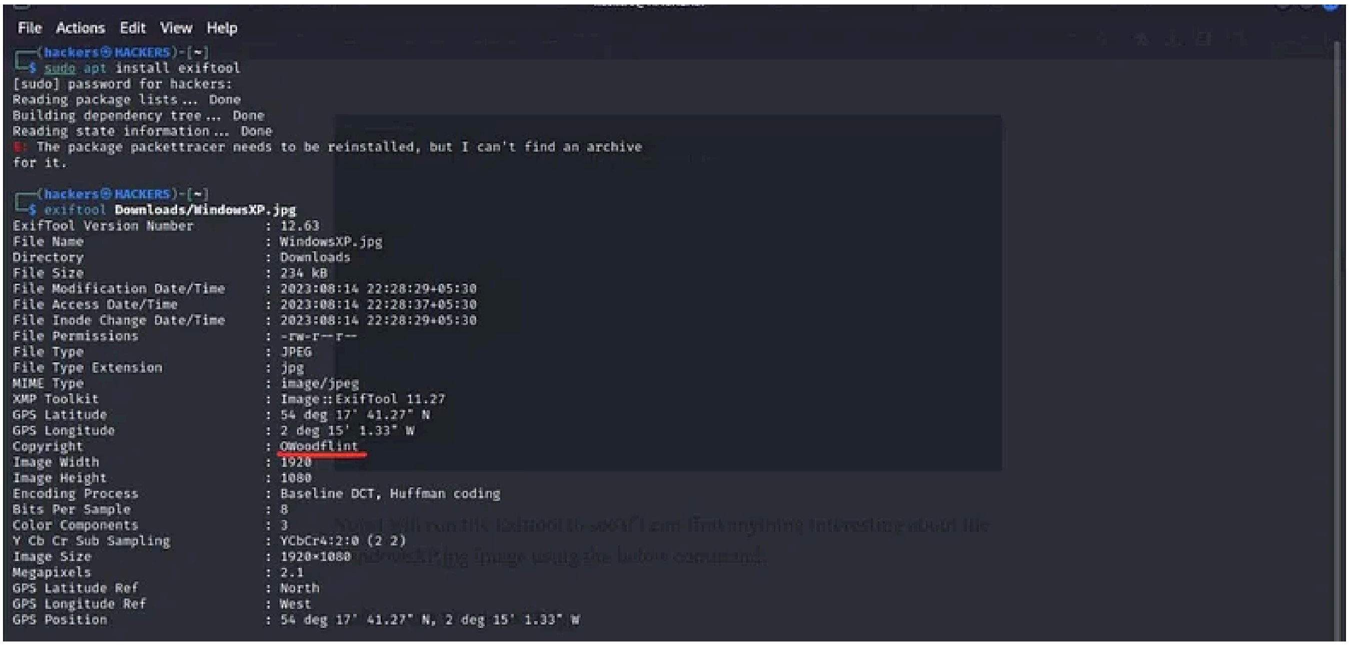
While looking online, I found a handy tool called ***ExifTool***. This tool is popular among photographers, digital forensics experts, and people who deal with digital files. It helps manage information about files, like when they were created or edited. You can use it by typing commands or with a user-friendly interface. Many other apps also work together with ExifTool. It was made by *Phil Harvey*, and you can get it from our *Terminal.*Use the commands given in the screenshort below.



```
┌──(hackers㉿HACKERS)-[~]
└─$ sudo apt install exiftool
```

Now I will run the Exiftool to see if I can find anything interesting about the WindowsXP.jpg image using the below command.

exiftool Downloads/WindowsXP.jpg

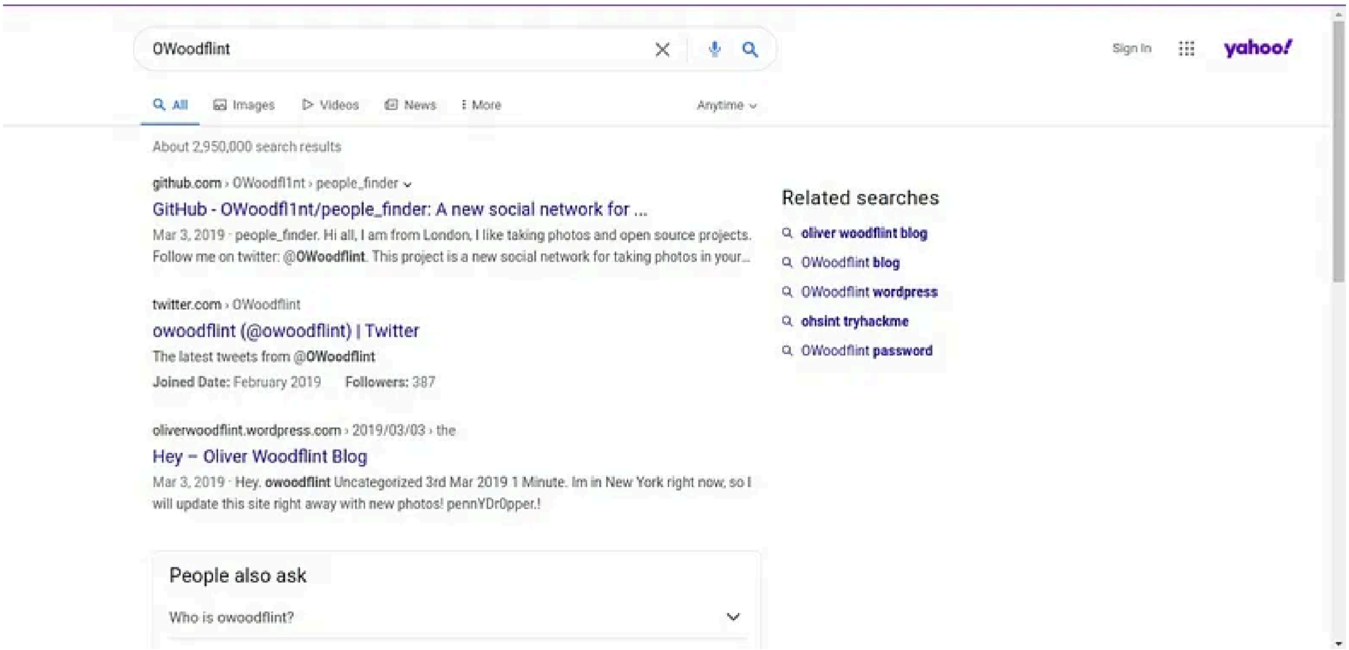


```
┌──(hackers㉿HACKERS)-[~]
└─$ sudo apt install exiftool
[sudo] password for hackers:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: The package packettracer needs to be reinstalled, but I can't find an archive
for it.

┌──(hackers㉿HACKERS)-[~]
└─$ exiftool Downloads/WindowsXP.jpg
ExifTool Version Number         : 12.63
File Name                       : WindowsXP.jpg
Directory                       : Downloads
File Size                       : 234 kB
File Modification Date/Time     : 2023:08:14 22:28:29+05:30
File Access Date/Time           : 2023:08:14 22:28:37+05:30
File Inode Change Date/Time     : 2023:08:14 22:28:29+05:30
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
XMP Toolkit                     : Image::ExifTool 11.27
GPS Latitude                    : 54 deg 17' 41.27" N
GPS Longitude                   : 2 deg 15' 1.33" W
Copyright                       : OWoodflint
Image Width                     : 1920
Image Height                    : 1080
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1920×1080
Megapixels                      : 2.1
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Position                    : 54 deg 17' 41.27" N, 2 deg 15' 1.33" W
```

As a result of doing this, we've uncovered some interesting details. We found out things like who owns the rights to the image and even where it was taken, as you can see in the picture above.

After doing a quick search on Google using the word 'OWoodflint', we found three web pages. One is on Twitter, another on GitHub, and a third one on WordPress. You can see them in the picture below. To answer the first question about the user's picture, there’s a hint that suggests they might have a social media account. So, it’s a good idea to check out their Twitter profile.



About 2,950,000 search results

github.com › OWoodfl1nt › people_finder
GitHub - OWoodfl1nt/people_finder: A new social network for ...
Mar 3, 2019 · people_finder. Hi all, I am from London, I like taking photos and open source projects. Follow me on twitter: @OWoodflint. This project is a new social network for taking photos in your...

twitter.com › OWoodflint
owoodflint (@owoodflint) | Twitter
The latest tweets from @OWoodflint
Joined Date: February 2019 Followers: 387

oliverwoodflint.wordpress.com › 2019/03/03 › the
Hey – Oliver Woodflint Blog
Mar 3, 2019 · Hey. owoodflint Uncategorized 3rd Mar 2019 1 Minute. Im in New York right now, so I will update this site right away with new photos! pennYDr0pper.!

People also ask
Who is owoodflint?

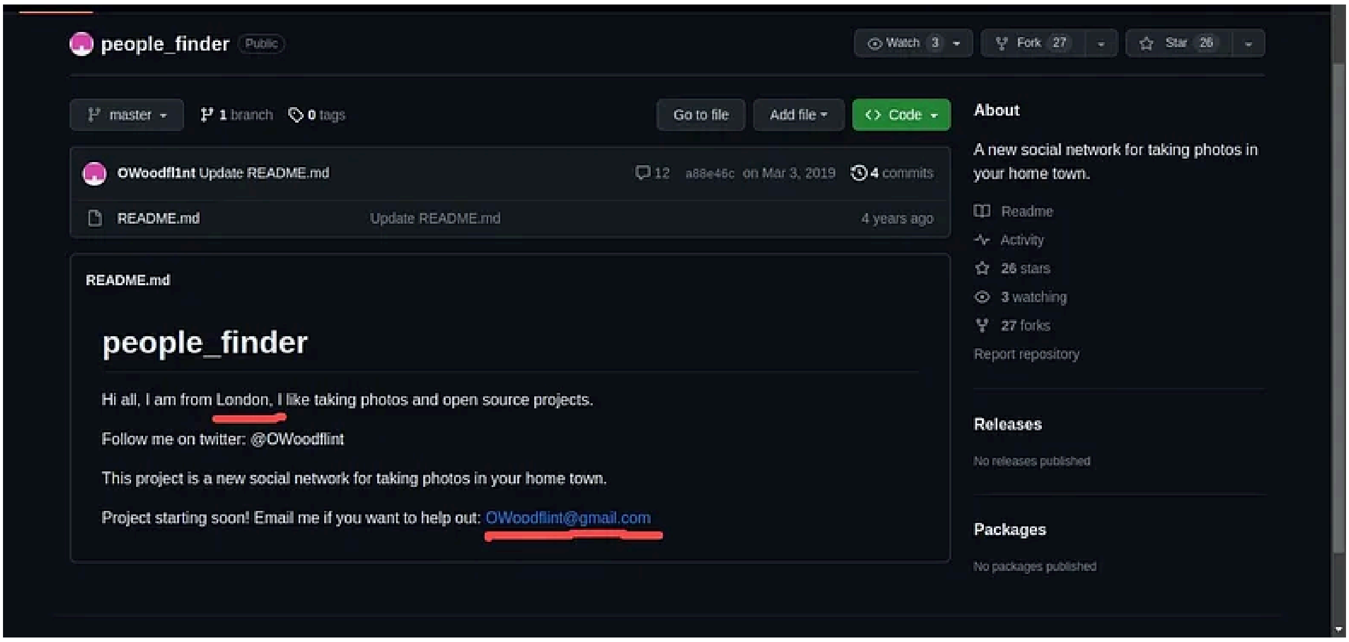
Related searches
oliver woodflint blog
OWoodflint blog
OWoodflint wordpress
ohsint tryhackme
OWoodflint password

Q.1 What is this user’s avatar of?

Ans: The user’s avatar is a cat.

Q.2 What city is this person in?

Ans:After open the Github like We That the person is from *London*. See the below screenshort.



OWoodfl1nt Update README.md 12 a88e46c on Mar 3, 2019 4 commits
README.md Update README.md 4 years ago

README.md

people_finder

Hi all, I am from London, I like taking photos and open source projects.

Follow me on twitter: @OWoodflint

This project is a new social network for taking photos in your home town.

Project starting soon! Email me if you want to help out: OWoodflint@gmail.com

About

A new social network for taking photos in your home town.

Readme
Activity
26 stars
3 watching
27 forks
Report repository

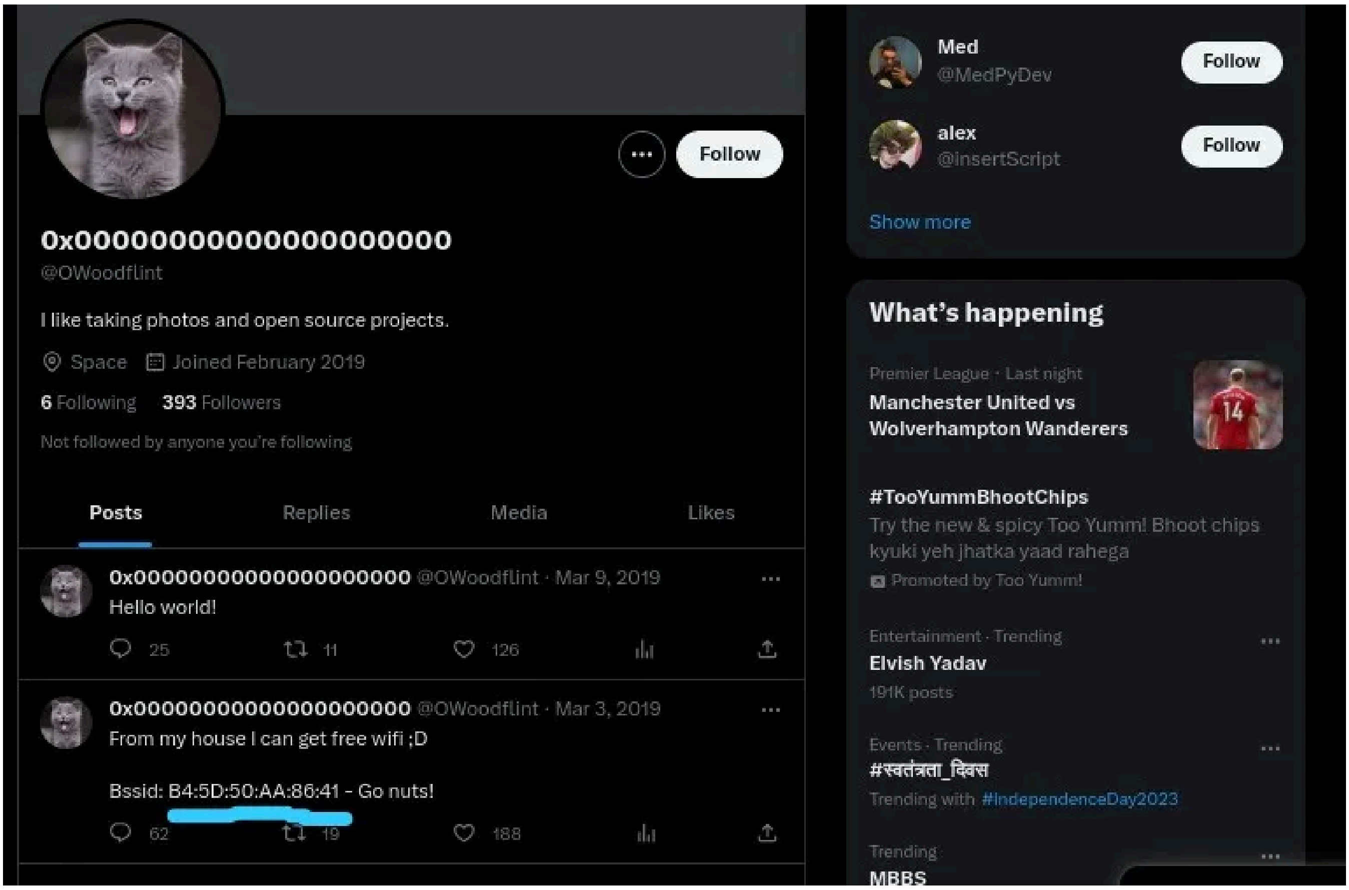
Releases
No releases published

Packages
No packages published

Q.3 What’s the SSID of the WAP he connected to?

Ans: Using the hint given in the question you get to know that to know the city where the person is you need to use BSSID and Wigle.net

If you open the Twitter link from the previous search you will see the BSSID value “Bssid: B4:5D:50:AA:86:41” in the tweets as shown in the below screenshot.



0x00000000000000000000

@OWoodflint

I like taking photos and open source projects.

Space Joined February 2019

6 Following 393 Followers

Not followed by anyone you're following

0x00000000000000000000 @OWoodflint · Mar 9, 2019

Hello world!

25 11 126

0x00000000000000000000 @OWoodflint · Mar 3, 2019

From my house I can get free wifi ;D

Bssid: B4:5D:50:AA:86:41 - Go nuts!

62 19 188

Med @MedPyDev

alex @insertScript

What's happening

Premier League · Last night
Manchester United vs Wolverhampton Wanderers

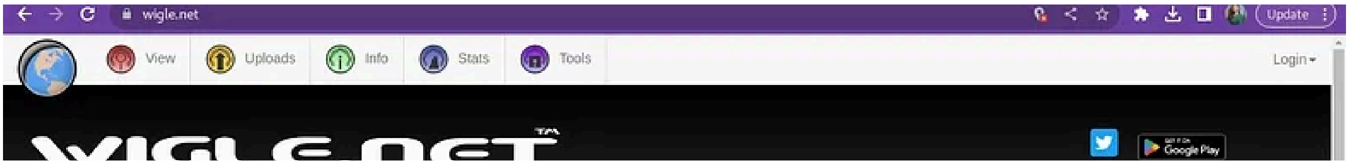
#TooYummBhootChips
Try the new & spicy Too Yumm! Bhoot chips kyuki yeh jhatka yaad rahega
Promoted by Too Yumm!

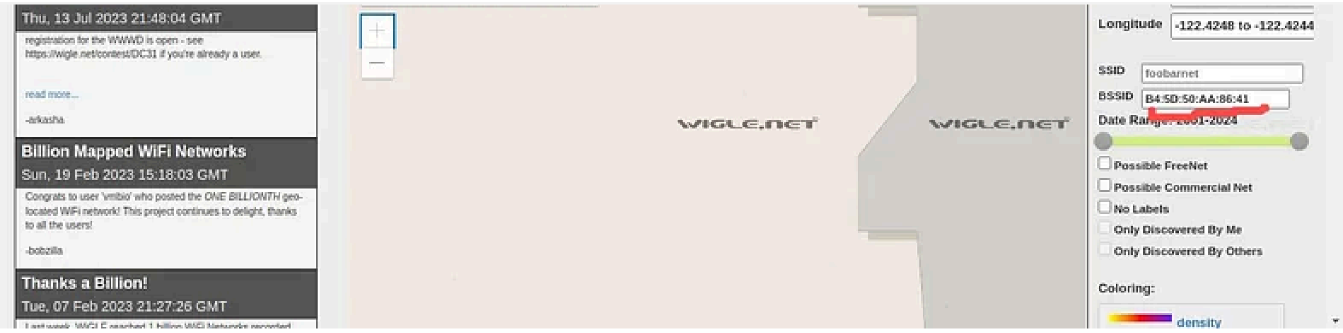
Entertainment · Trending
Elvish Yadav
191K posts

Events · Trending
#स्वतंत्रता_दिवस
Trending with #IndependenceDay2023

Trending
MBBS

Now once you have BSSID you need to go to Wigle.net and do an advanced search using BSSID .In the Network Characteristics section enter the BSSID value and click on Query. After querying you will get a result for that BSSID as shown in the below screenshot.




Thu, 13 Jul 2023 21:48:04 GMT

registration for the WWWD is open - see https://wigle.net/content/DC31 if you're already a user.

read more...

-arkasha

Billion Mapped WiFi Networks

Sun, 19 Feb 2023 15:18:03 GMT

Congrats to user 'vmbio' who posted the *ONE BILLIONTH* geo-located WiFi network! This project continues to delight, thanks to all the users!

-bobzilla

Thanks a Billion!

Tue, 07 Feb 2023 21:27:26 GMT

Longitude: -122.4248 to -122.4244

SSID: foobarnet

BSSID: B4:5D:50:AA:86:41

Date Range: 2001-2024

□ Possible FreeNet
□ Possible Commercial Net
□ No Labels
□ Only Discovered By Me
□ Only Discovered By Others

Coloring: density

Now, click on the map link from the results and you will get the location for that BSSID. So, the person whom we are looking for is based in London as per the BSSID he mentioned in the tweet from his Twitter account.The SSID is UnileverWiFi, you can get the SSID from the BSSID.

Q.4 What is his personal email address?

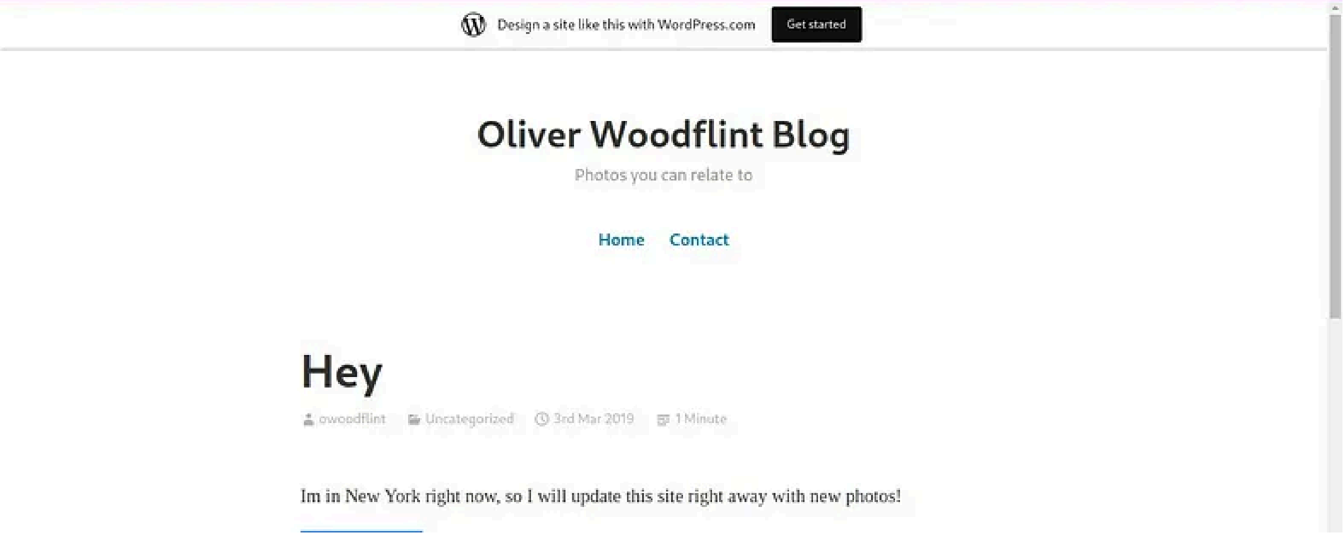
Ans: His personal email address is OWoodflint@gmail.com, this is available on his GitHub page github.com/OWoodfl1nt/people_finder

Q.5 What site did you find his email address on?

Ans: Github

Q.6 Where has he gone on holiday?

Ans: He has gone to New York for his holiday as he mentioned on his WordPress blog oliverwoodflint.wordpress.com/author/owoodflint/ as shown in the below screenshot.



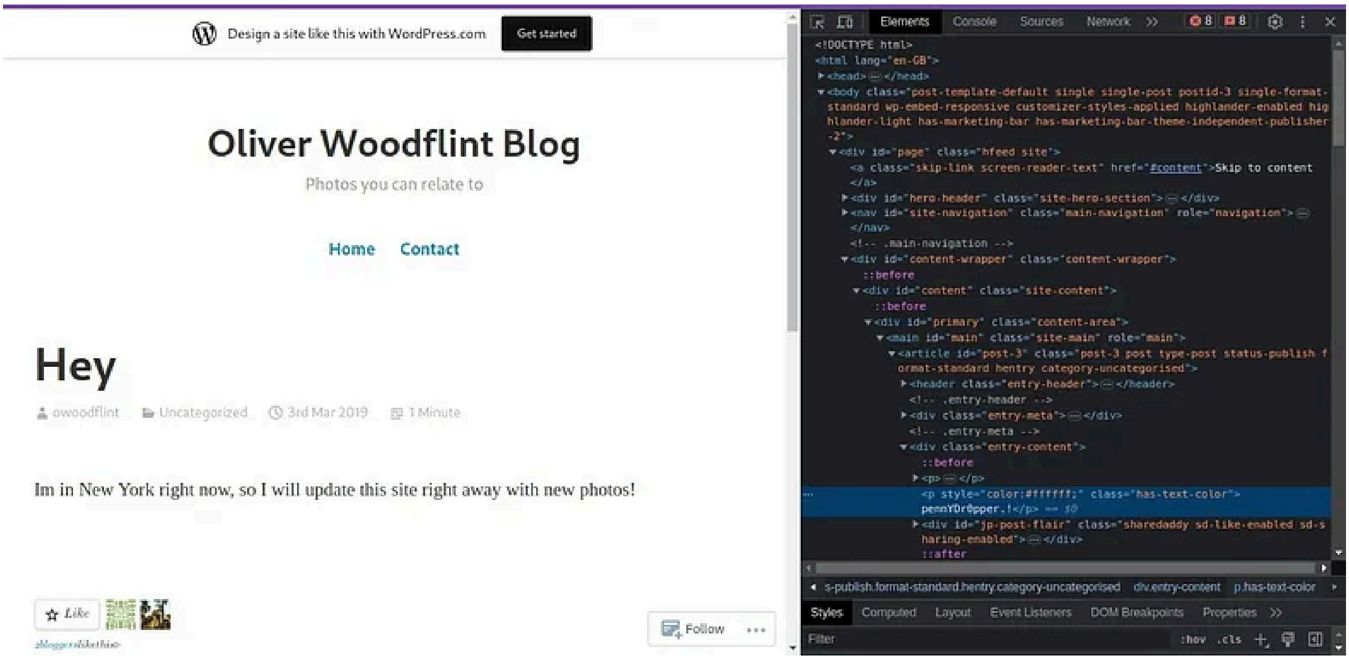
Hey

owoodflint · Uncategorized · 3rd Mar 2019 · 1 Minute

Im in New York right now, so I will update this site right away with new photos!

Q.7 What is this person's password?

Ans: I had to think carefully about the last question and figure out how to get the password and what it's used for. After checking Twitter and the GitHub page with no luck, I guessed that the WordPress Blog was our last chance. So, I decided to look at the code behind the WordPress website. When I did that, we found a weird set of characters that looked like a password.



Hey

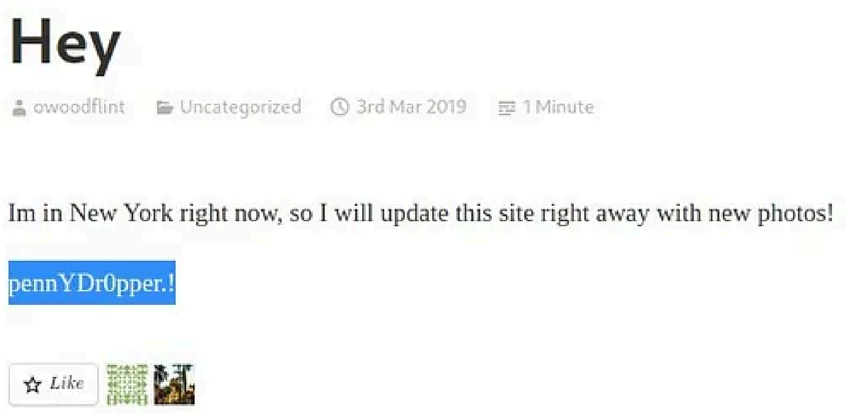
owoodflint · Uncategorized · 3rd Mar 2019 · 1 Minute

Im in New York right now, so I will update this site right away with new photos!

```
<!DOCTYPE html>
<html lang="en-GB">
▶<head>…</head>
▼<body class="post-template-default single single-post postid-3 single-format-standard wp-embed-responsive customizer-styles-applied highlander-enabled highlander-light has-marketing-bar has-marketing-bar-theme-independent-publisher-2">
  ▼<div id="page" class="hfeed site">
     <a class="skip-link screen-reader-text" href="#content">Skip to content</a>
    ▶<div id="hero-header" class="site-hero-section">…</div>
    ▶<nav id="site-navigation" class="main-navigation" role="navigation">…</nav>
     <!-- .main-navigation -->
    ▼<div id="content-wrapper" class="content-wrapper">
       ::before
      ▼<div id="content" class="site-content">
         ::before
        ▼<div id="primary" class="content-area">
          ▼<main id="main" class="site-main" role="main">
            ▼<article id="post-3" class="post-3 post type-post status-publish format-standard hentry category-uncategorised">
              ▶<header class="entry-header">…</header>
               <!-- .entry-header -->
              ▶<div class="entry-meta">…</div>
               <!-- .entry-meta -->
              ▼<div class="entry-content">
                 ::before
                ▶<p>…</p>
                 <p style="color:#ffffff;" class="has-text-color">pennYDr0pper.!</p> == $0
                ▶<div id="jp-post-flair" class="sharedaddy sd-like-enabled sd-sharing-enabled">…</div>
                 ::after
```

s-publish.format-standard.hentry.category-uncategorised div.entry-content p.has-text-color

Since the password was written in white font color, it was not visible on the page. However, by using the "ctrl+a" to select all and highlighting the entire text on the page, the password would become visible.



Hey

owoodflint Uncategorized 3rd Mar 2019 1 Minute

Im in New York right now, so I will update this site right away with new photos!

pennYDr0pper.!

So the Answer is “*pennYDr0pper*”.

Walkthrough Thm Writeup Writeup Tryhackme Osint

Follow

Written by Tamanna Agrawal

24 Followers · 5 Following

Cybersecurity enthusiast & technical writer passionate about simplifying complex concepts and sharing insights on trends tools & techniques in the Cybersecurity

No responses yet

What are your thoughts?

Respond

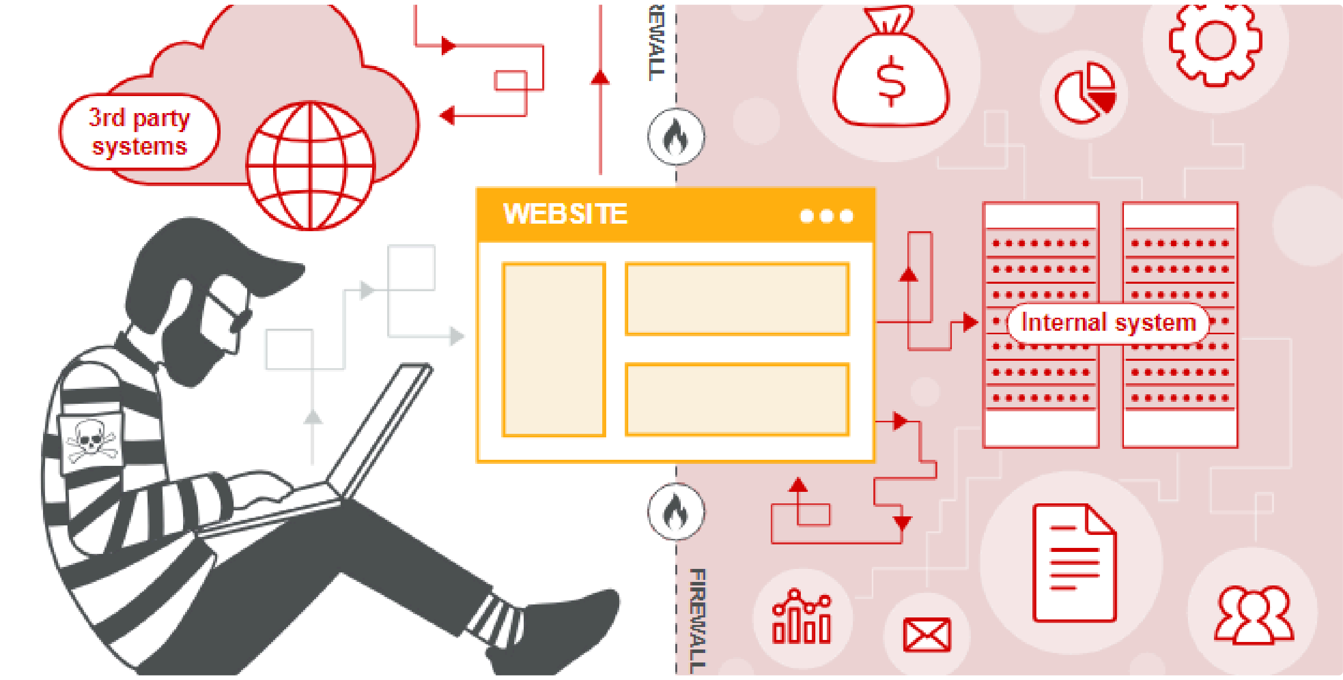
More from Tamanna Agrawal

Tamanna Agrawal

Advent of Cyber 2024 [Day5] Writeup with Answers | TryHackMe

Task 11- Day 5: SOC-mas XX-what-ee?

Dec 6, 2024 2



Tamanna Agrawal

Bypassing Common SSRF Protections: Techniques Attackers Use

Server-Side Request Forgery (SSRF) is a critical vulnerability that allows attackers to make requests from a server to unintended…

Aug 10, 2024 25 1

Tamanna Agrawal

Tryhackme- Brooklyn Nine Nine

Hello guys ‼ 🙋 welcome Back again with my new write Brooklyn nine nine from TryHackMe a box that is beginner friendly and a good box…

Mar 15, 2024 3

Tamanna Agrawal

Let Us C (Notes and Solution) ch-1

# What is C ?

Jun 23, 2023

See all from Tamanna Agrawal

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 5] Writeup with Answers | TryHackMe Walkthrough

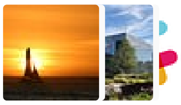
SOC-mas XX-what-ee?

✦ Dec 5, 2024 788 1

Lists

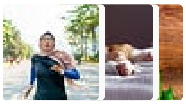
Staff picks

796 stories · 1561 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



Self-Improvement 101

20 stories · 3193 saves

Productivity 101

20 stories · 2707 saves

Advent of Cyber 2024
Dive into the wonderful world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!
I'm all atomic inside!
Day 4
Answers
cyberw1ng.medium.com

In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

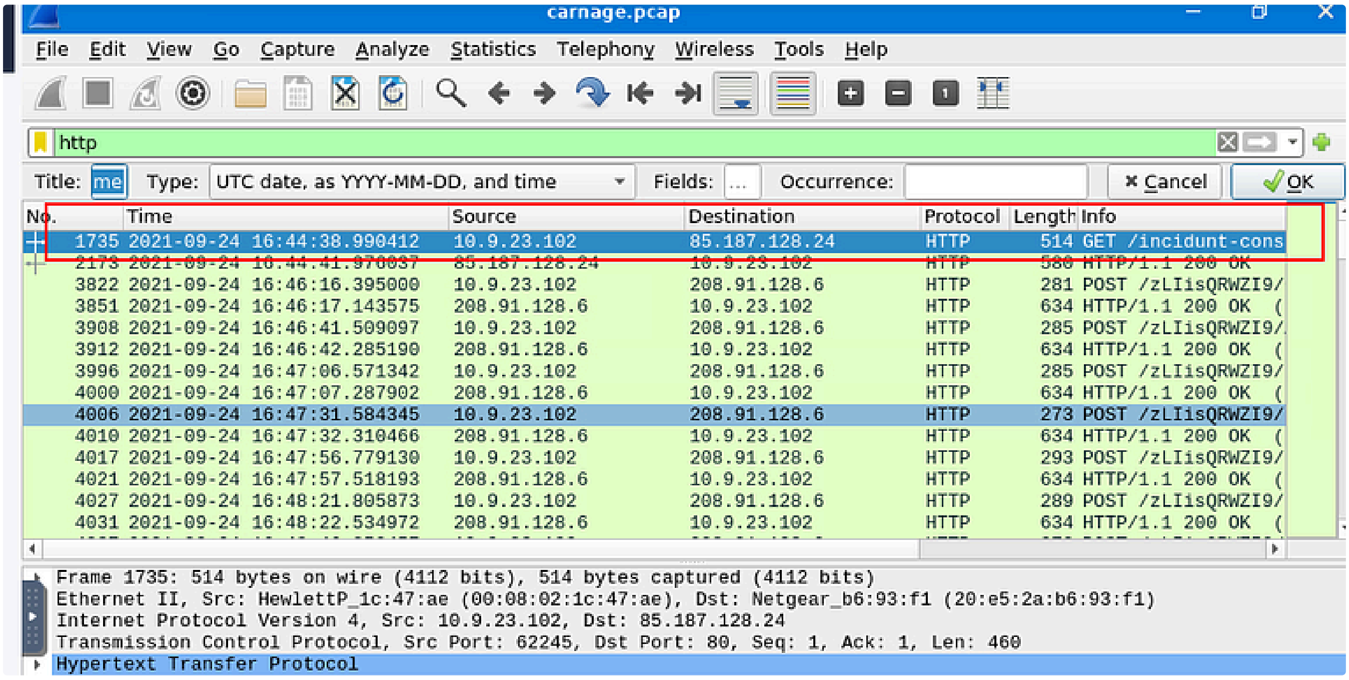
✦ Dec 4, 2024 882 1

In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!

Dec 11, 2024 855 1


carnage.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Title: me Type: UTC date, as YYYY-MM-DD, and time Fields: ... Occurrence: ✖ Cancel ✓ OK

```
No.   Time                        Source          Destination     Protocol Length Info
 1735 2021-09-24 16:44:38.990412  10.9.23.102     85.187.128.24   HTTP        514 GET /incidunt-cons
 2173 2021-09-24 16:44:41.970037  85.187.128.24   10.9.23.102     HTTP        580 HTTP/1.1 200 OK
 3822 2021-09-24 16:46:16.395000  10.9.23.102     208.91.128.6    HTTP        281 POST /zLIisQRWZI9/
 3851 2021-09-24 16:46:17.143575  208.91.128.6    10.9.23.102     HTTP        634 HTTP/1.1 200 OK  (
 3908 2021-09-24 16:46:41.509097  10.9.23.102     208.91.128.6    HTTP        285 POST /zLIisQRWZI9/
 3912 2021-09-24 16:46:42.285190  208.91.128.6    10.9.23.102     HTTP        634 HTTP/1.1 200 OK  (
 3996 2021-09-24 16:47:06.571342  10.9.23.102     208.91.128.6    HTTP        285 POST /zLIisQRWZI9/
 4000 2021-09-24 16:47:07.287902  208.91.128.6    10.9.23.102     HTTP        634 HTTP/1.1 200 OK  (
 4006 2021-09-24 16:47:31.584345  10.9.23.102     208.91.128.6    HTTP        273 POST /zLIisQRWZI9/
 4010 2021-09-24 16:47:32.310466  208.91.128.6    10.9.23.102     HTTP        634 HTTP/1.1 200 OK  (
 4017 2021-09-24 16:47:56.779130  10.9.23.102     208.91.128.6    HTTP        293 POST /zLIisQRWZI9/
 4021 2021-09-24 16:47:57.518193  208.91.128.6    10.9.23.102     HTTP        634 HTTP/1.1 200 OK  (
 4027 2021-09-24 16:48:21.805873  10.9.23.102     208.91.128.6    HTTP        289 POST /zLIisQRWZI9/
 4031 2021-09-24 16:48:22.534972  208.91.128.6    10.9.23.102     HTTP        634 HTTP/1.1 200 OK  (

Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
Hypertext Transfer Protocol
```

Chicken0248

[TryHackMe Write-up] Carnage

Apply your analytical skills to analyze the malicious network traffic using Wireshark.

Aug 17, 2024 50

Atharva

TryHackMe — Whiterose Writeup

Complete step-by-step writeup for TryHackMe challenge room Whiterose!

Nov 12, 2024 16

See more recommendations