Introduction

Capture the Flag (CTF) Competition Analysis

A CTF file is a media collection catalog created by Where Is It, a discontinued Windows application. It contains a detailed record of a user's media collection, including physical CDs and DVDs, as well as digital files such as .MP3 and .MP4. The file not only lists these media items but also stores metadata about them, making it easier for users to manage and organize their media libraries. Through the CTF format, Where Is It enabled users to keep comprehensive and searchable catalogs of their diverse media collections (Galle, 2017).

Challenges:

1. Open-source intelligence (OSINT): Open-source intelligence involves collecting information from publicly available sources. OSINT tasks may include finding specific information about individuals, organizations, or other entities using social media, websites, and other public data.

Method: used The UserRecon tool

2. Geolocation: Geolocation tasks involve determining the physical location of a user. Methods include using the HTML5 API, cell signals, BSSID, and IP addresses. Pairing an IP address with a geographical location is commonly used in these challenges

Method: used wigle

3. **Cryptography:** Cryptography tasks typically involve decrypting or encrypting data. Participants must apply their knowledge of cryptographic techniques to solve these challenges.

Method: used cyberchef and cryptii

4. **Steganography:** Steganography tasks involve finding hidden information within files or images. Participants use various tools and techniques to uncover concealed data.

Method: used Neatnik

5. **Hash Cracking:** Cracking passwords is a crucial skill in penetration testing. Participants must crack hashes to reveal plaintext passwords or other data.

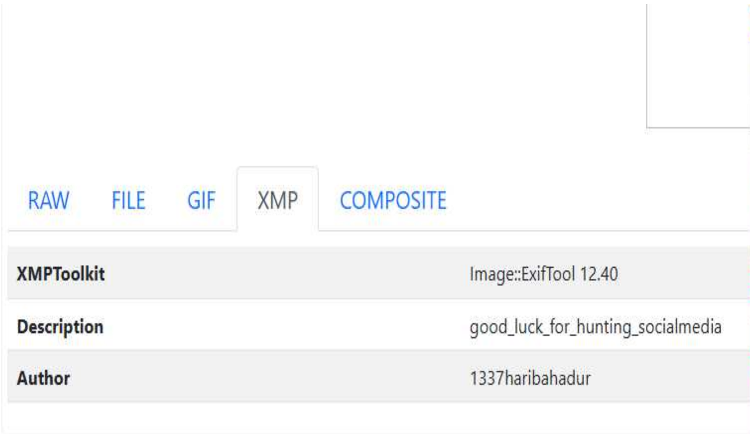
Method: used crackstation

6. **Unprintable Text Decoding:** This task involves decoding text that is not easily printable or visible. Participants may use different decoding techniques to uncover the hidden message.

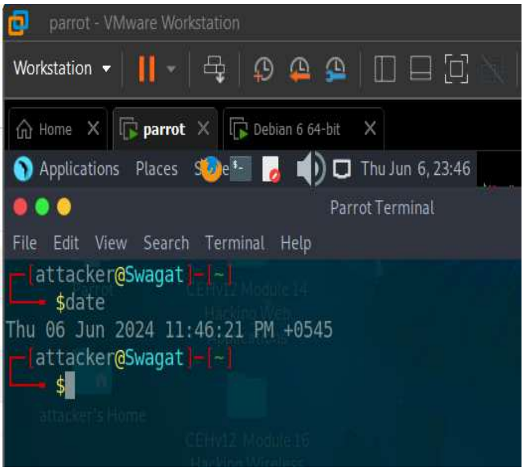
7. **Flag Submission:** For each challenge, participants must submit the flag to earn points. Flags are unique identifiers that confirm the successful completion of a task.

Ways to tackle challenges and process to capture the flag are as followed:

I downloaded the gif file named hari.gif. Then my first task was to find the author's name for further processing so I used exifmeta website to find the files metadata which might contain useful insights like author's name , Description and so on. From there I found author's name which was 1337haribhadur as shown in fig:

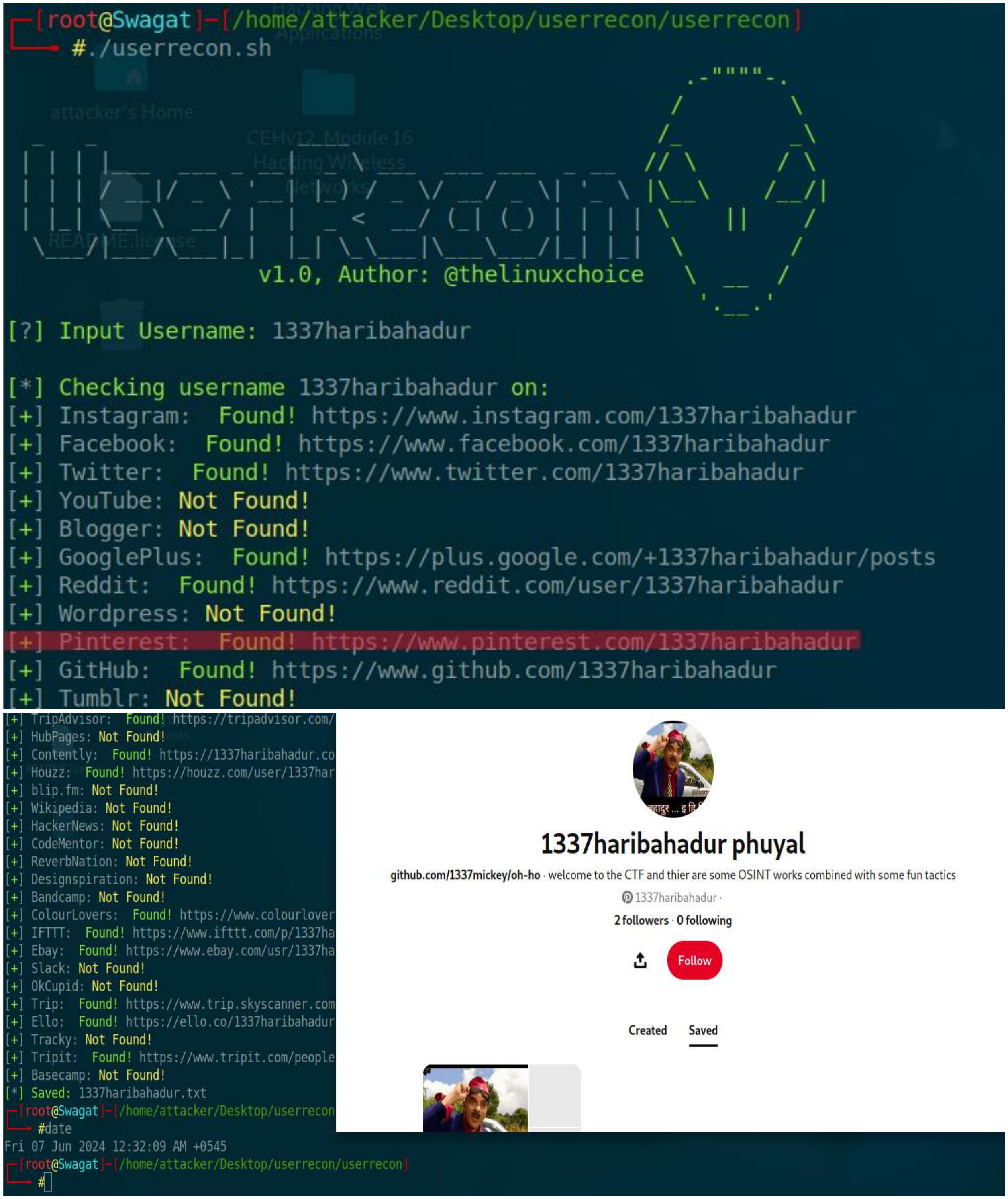


XMPToolkit	Image::ExifTool 12.40
Description	good_luck_for_hunting_socialmedia
Author	1337haribahadur



```
┌─[attacker@Swagat]─[~]
└──╼ $date
Thu 06 Jun 2024 11:46:21 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

After finding Auther’s name 1337haribahadur the OSINT phage begins where I used UserRecon to find Author’s social media. As expected, I got author's social media which was on pinterest as shown in fig below:



```
┌─[root@Swagat]─[/home/attacker/Desktop/userrecon/userrecon]
└──╼ #./userrecon.sh
                                                             .-"""""-.
                                                            /         \
 _   _                  ____                              /_           _\
| | | |___  ___ _ __  |  _ \ ___  ___ ___  _ __          // \         / \\
| | | / __|/ _ \ '__| | |_) / _ \/ __/ _ \| '_ \         |\__\       /__/|
| |_| \__ \  __/ |    |  _ <  __/ (_| (_) | | | |         \     ||     /
 \___/|___/\___|_|    |_| \_\___|\___\___/|_| |_|          \          /
                        v1.0, Author: @thelinuxchoice        \  __  /
                                                              '.__.'

[?] Input Username: 1337haribahadur

[*] Checking username 1337haribahadur on:
[+] Instagram:  Found! https://www.instagram.com/1337haribahadur
[+] Facebook:  Found! https://www.facebook.com/1337haribahadur
[+] Twitter:  Found! https://www.twitter.com/1337haribahadur
[+] YouTube: Not Found!
[+] Blogger: Not Found!
[+] GooglePlus:  Found! https://plus.google.com/+1337haribahadur/posts
[+] Reddit:  Found! https://www.reddit.com/user/1337haribahadur
[+] Wordpress: Not Found!
[+] Pinterest:  Found! https://www.pinterest.com/1337haribahadur
[+] GitHub:  Found! https://www.github.com/1337haribahadur
[+] Tumblr: Not Found!
[+] TripAdvisor:  Found! https://tripadvisor.com/
[+] HubPages: Not Found!
[+] Contently:  Found! https://1337haribahadur.co
[+] Houzz:  Found! https://houzz.com/user/1337har
[+] blip.fm: Not Found!
[+] Wikipedia: Not Found!
[+] HackerNews: Not Found!
[+] CodeMentor: Not Found!
[+] ReverbNation: Not Found!
[+] Designspiration: Not Found!
[+] Bandcamp: Not Found!
[+] ColourLovers:  Found! https://www.colourlover
[+] IFTTT:  Found! https://www.ifttt.com/p/1337ha
[+] Ebay:  Found! https://www.ebay.com/usr/1337ha
[+] Slack: Not Found!
[+] OkCupid: Not Found!
[+] Trip:  Found! https://www.trip.skyscanner.com
[+] Ello:  Found! https://ello.co/1337haribahadur
[+] Tracky: Not Found!
[+] Tripit:  Found! https://www.tripit.com/people
[+] Basecamp: Not Found!
[*] Saved: 1337haribahadur.txt
┌─[root@Swagat]─[/home/attacker/Desktop/userrecon
└──╼ #date
Fri 07 Jun 2024 12:32:09 AM +0545
┌─[root@Swagat]─[/home/attacker/Desktop/userrecon/userrecon]
└──╼ #
```

1337haribahadur phuyal

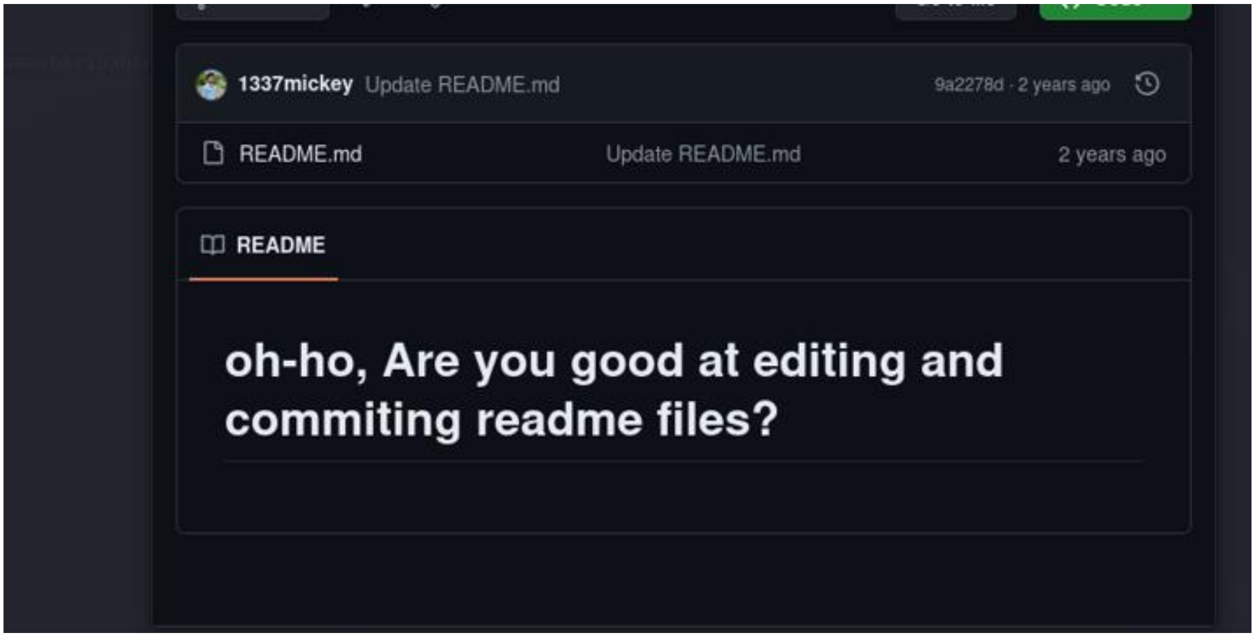
github.com/1337mickey/oh-ho · welcome to the CTF and thier are some OSINT works combined with some fun tactics

1337haribahadur ·

2 followers · 0 following

Link of Hari Bahadur social media account is: https://www.pinterest.com/1337haribahadur/

As we can see there is a GitHub link on the profile of Hari Bahadur if we go through the link then we can get A message “oh-ho, Are you good at editing and commiting readme files?” by seeing this message I was more curious and did a bit investigation and I got another lead as another person named “1337madhanbahad1” in Update README.md section As shown in fig below:

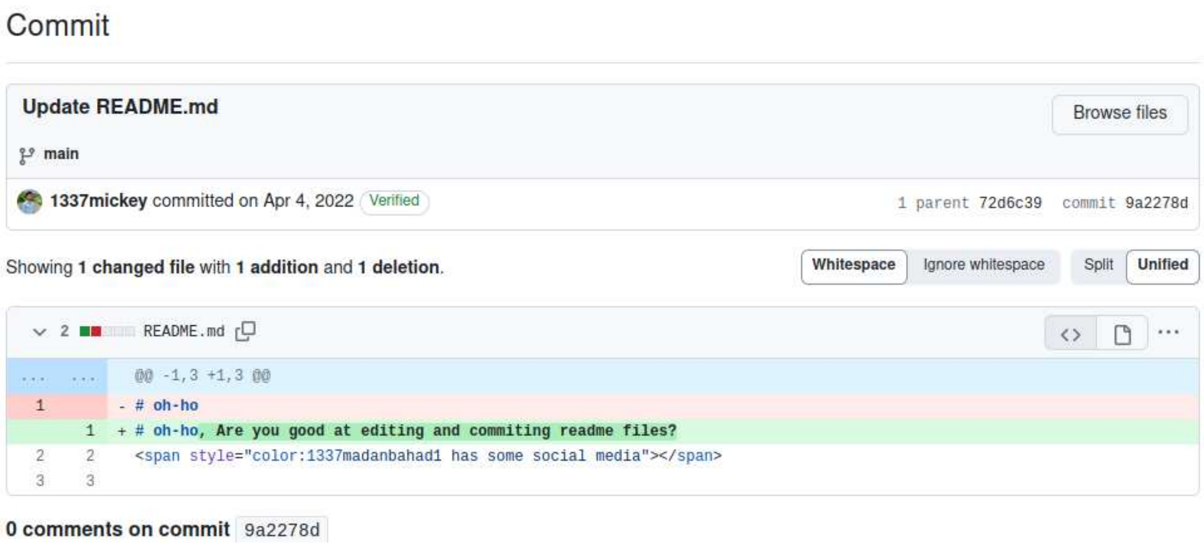


1337mickey Update README.md 9a2278d · 2 years ago

README.md Update README.md 2 years ago

README

oh-ho, Are you good at editing and commiting readme files?



Commit

Update README.md

main

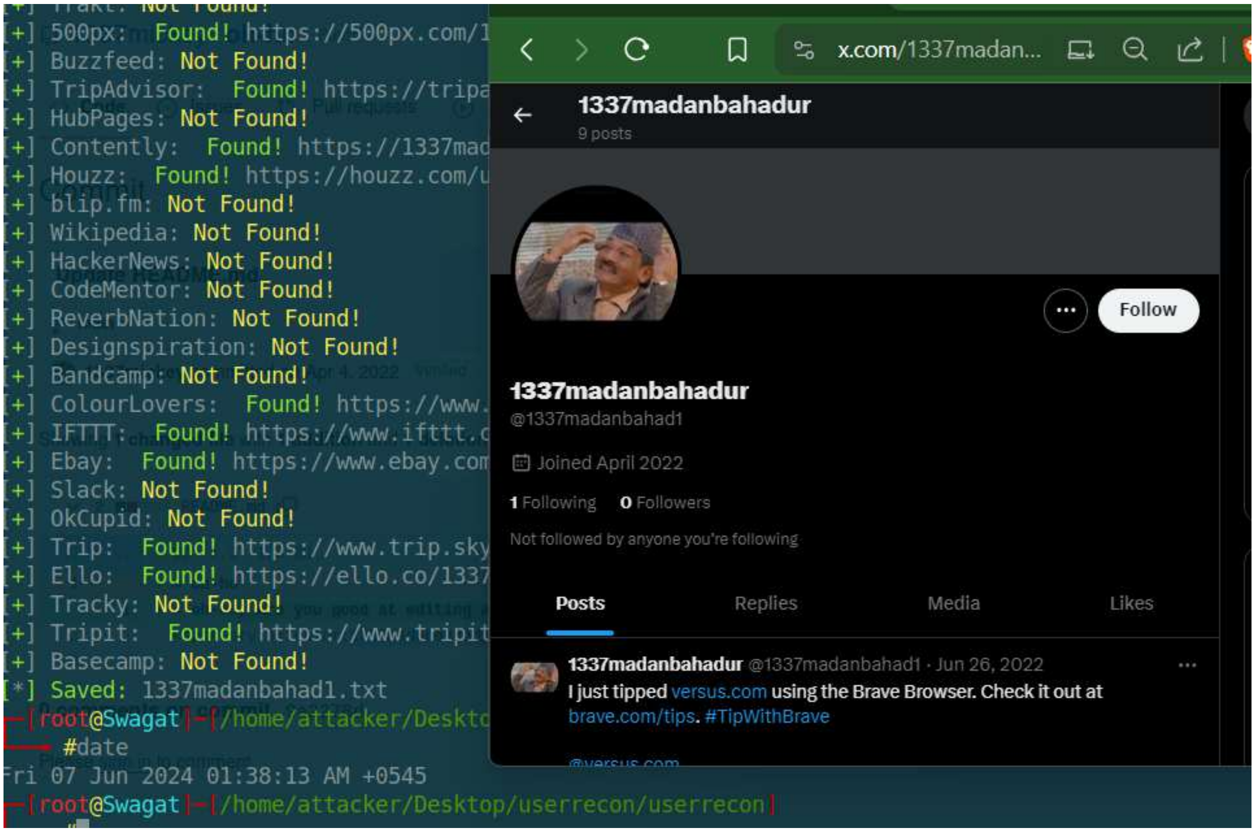
1337mickey committed on Apr 4, 2022 Verified — 1 parent 72d6c39 commit 9a2278d

Showing **1 changed file** with **1 addition** and **1 deletion**.

```
2  README.md
@@ -1,3 +1,3 @@
1    - # oh-ho
   1 + # oh-ho, Are you good at editing and commiting readme files?
2  2   <span style="color:1337madanbahad1 has some social media"></span>
3  3
```

0 comments on commit 9a2278d

After finding a new username I again use UserRecon to find his social media accounts. After doing further investigation I got a twitter account of that username as shown in fig below:



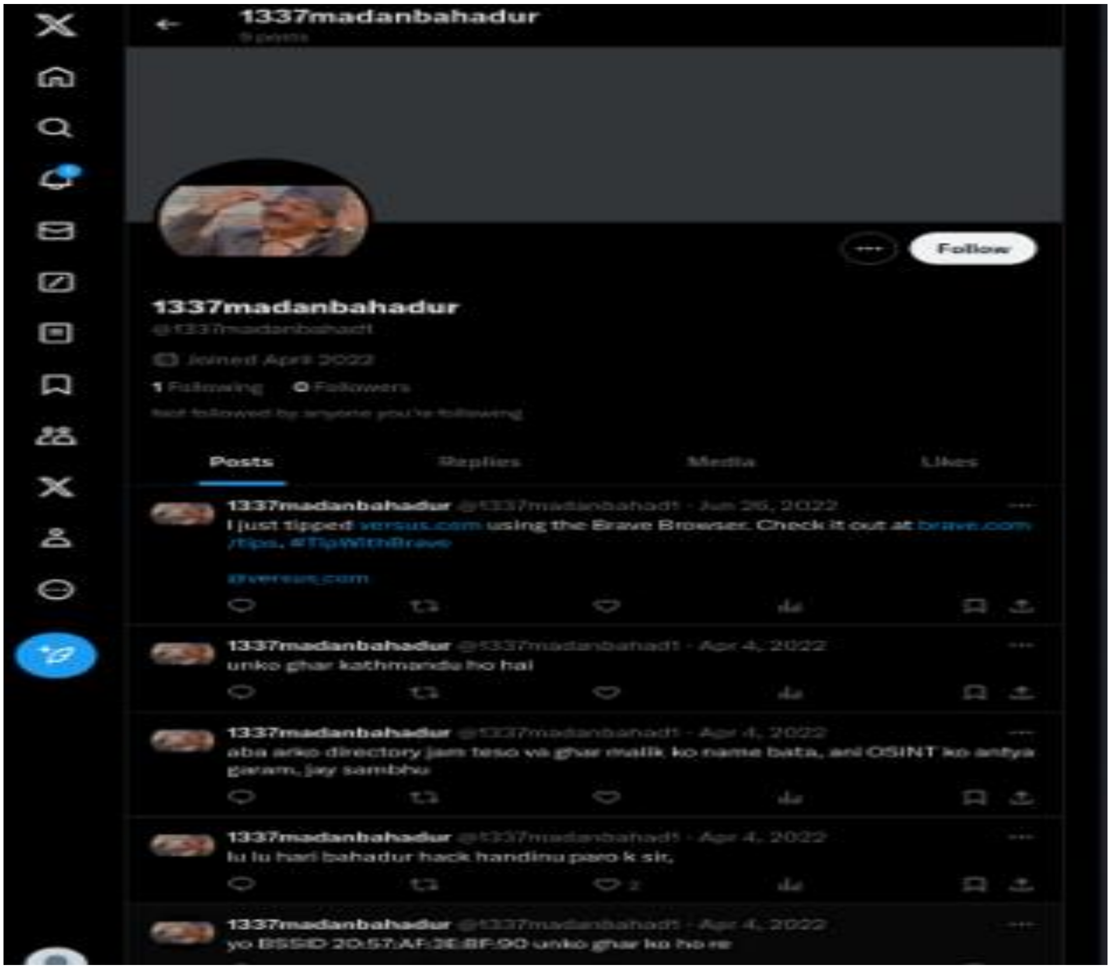
```
[+] Trakt: Not Found!
[+] 500px:  Found! https://500px.com/1
[+] Buzzfeed: Not Found!
[+] TripAdvisor:  Found! https://tripa
[+] HubPages: Not Found!
[+] Contently:  Found! https://1337mad
[+] Houzz:  Found! https://houzz.com/u
[+] blip.fm: Not Found!
[+] Wikipedia: Not Found!
[+] HackerNews: Not Found!
[+] CodeMentor: Not Found!
[+] ReverbNation: Not Found!
[+] Designspiration: Not Found!
[+] Bandcamp: Not Found!
[+] ColourLovers:  Found! https://www.
[+] IFTTT:  Found! https://www.ifttt.c
[+] Ebay:  Found! https://www.ebay.com
[+] Slack: Not Found!
[+] OkCupid: Not Found!
[+] Trip:  Found! https://www.trip.sky
[+] Ello:  Found! https://ello.co/1337
[+] Tracky: Not Found!
[+] Tripit:  Found! https://www.tripit
[+] Basecamp: Not Found!
[*] Saved: 1337madanbahad1.txt
┌─[root@Swagat]─[/home/attacker/Deskto
└──╼ #date
Fri 07 Jun 2024 01:38:13 AM +0545
┌─[root@Swagat]─[/home/attacker/Desktop/userrecon/userrecon]
```

1337madanbahadur
9 posts

1337madanbahadur
@1337madanbahad1
Joined April 2022
1 Following 0 Followers
Not followed by anyone you're following

1337madanbahadur @1337madanbahad1 · Jun 26, 2022
I just tipped versus.com using the Brave Browser. Check it out at brave.com/tips. #TipWithBrave
@versus.com

In that twitter account I got a lot of leads that was his post which contain a lot of information. After going through all posts I got a BSSID as shown in fig below:



1337madanbahadur
5 posts

1337madanbahadur
@1337madanbahad1
Joined April 2022
1 Following 0 Followers
Not followed by anyone you're following

1337madanbahadur @1337madanbahad1 · Jun 26, 2022
I just tipped versus.com using the Brave Browser. Check it out at brave.com/tips. #TipWithBrave

@versus.com

1337madanbahadur @1337madanbahad1 · Apr 4, 2022
unko ghar kathmandu ho hai

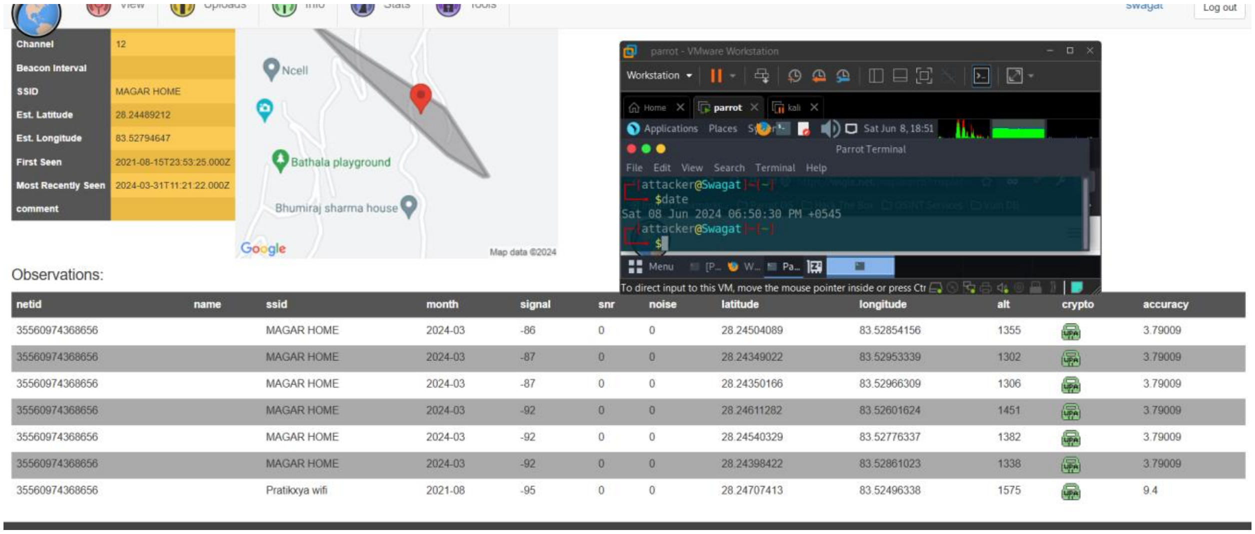
1337madanbahadur @1337madanbahad1 · Apr 4, 2022
aba anko directory jam teso va ghar malik ko name bata, ani OSINT ko antya garam, jay sambhu

1337madanbahadur @1337madanbahad1 · Apr 4, 2022
lu lu hari bahadur hack handinu paro k sir,
2

1337madanbahadur @1337madanbahad1 · Apr 4, 2022
yo BSSID 20:57:AF:3E:BF:90 unko ghar ko ho re

Link of “1337madanbahadur” is https://x.com/1337madanbahad1

After knowing BSSID I opened Wigle to track it and in Wigle at first, I got SSID MAGAR HOME and after little more I got another SSID As Pratikxyawifi which was now changed to MAGAR HOME. Now I got another clue as Pratikxya as shown in fig below:



Channel	12
Beacon Interval	
SSID	MAGAR HOME
Est. Latitude	28.24489212
Est. Longitude	83.52794647
First Seen	2021-08-15T23:53:25.000Z
Most Recently Seen	2024-03-31T11:21:22.000Z
comment	

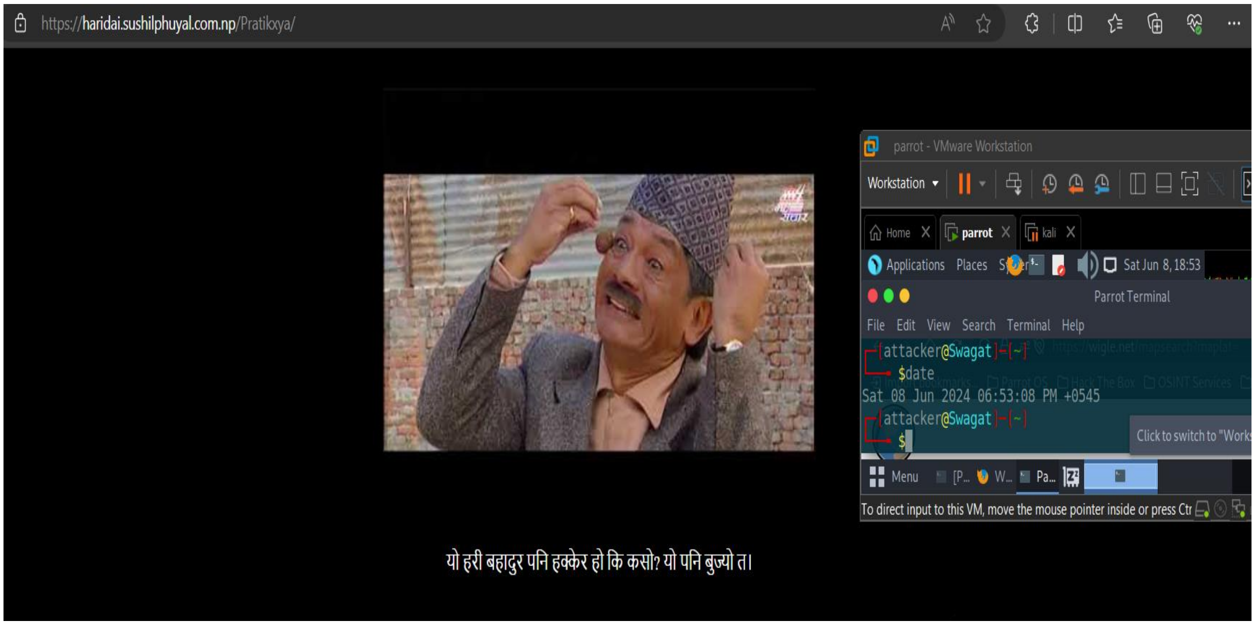
```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:50:30 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

Observations:

netid	name	ssid	month	signal	snr	noise	latitude	longitude	alt	crypto	accuracy
35560974368656		MAGAR HOME	2024-03	-86	0	0	28.24504089	83.52854156	1355	WPA	3.79009
35560974368656		MAGAR HOME	2024-03	-87	0	0	28.24349022	83.52953339	1302	WPA	3.79009
35560974368656		MAGAR HOME	2024-03	-87	0	0	28.24350166	83.52966309	1306	WPA	3.79009
35560974368656		MAGAR HOME	2024-03	-92	0	0	28.24611282	83.52601624	1451	WPA	3.79009
35560974368656		MAGAR HOME	2024-03	-92	0	0	28.24540329	83.52776337	1382	WPA	3.79009
35560974368656		MAGAR HOME	2024-03	-92	0	0	28.24398422	83.52861023	1338	WPA	3.79009
35560974368656		Pratikxya wifi	2021-08	-95	0	0	28.24707413	83.52496338	1575	WPA	9.4

I modify the URL of that gif file as: https://haridai.sushilphuyal.com.np/Pratikxya/

And got this page as shown in fig:



https://haridai.sushilphuyal.com.np/Pratikxya/
parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 18:53
Parrot Terminal
File
Edit
View
Search
Terminal
Help
Click to switch to "Work
Menu
To direct input to this VM, move the mouse pointer inside or press Ctr

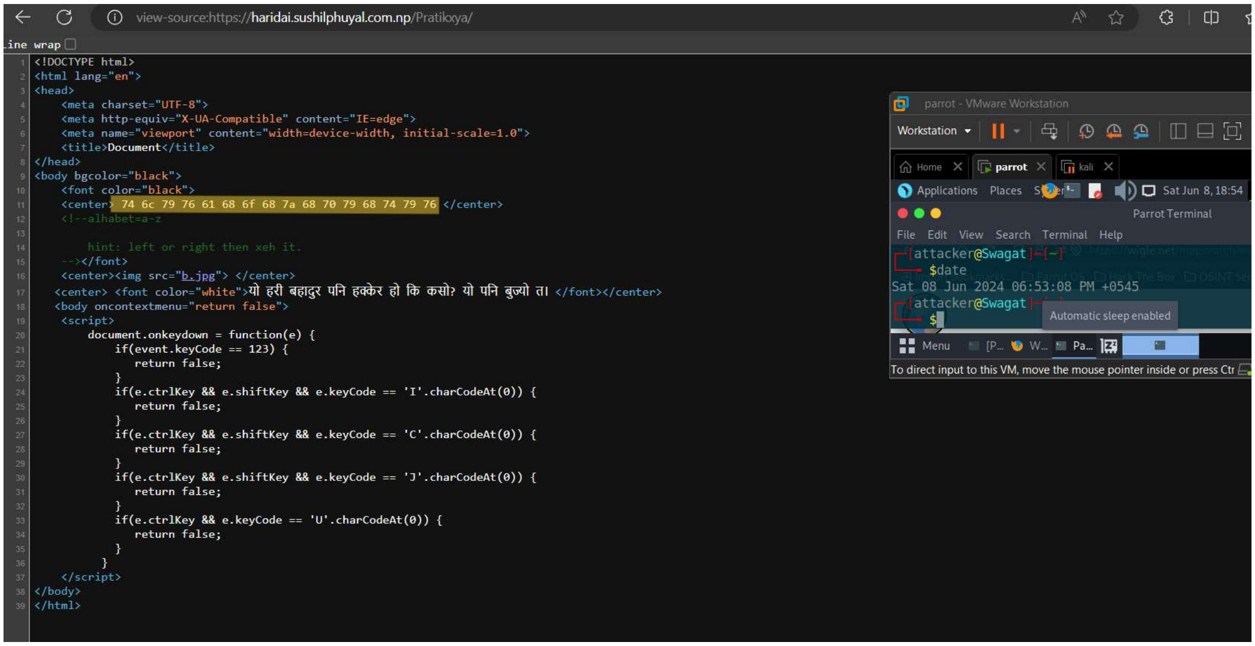
```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:53:08 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

यो हरी बहादुर पनि हक्केर हो कि कसो? यो पनि बुज्यो त।

I was curious to see the page source, so I did right click but right click was disabled and my curiosity changed to demand, and I modify its URL by adding "view-source" that is:

view-source:https://haridai.sushilphuyal.com.np/Pratikxya/

Then I got a big hint 'xeh' which is 'hex' just spelled from back as shown in fig below:



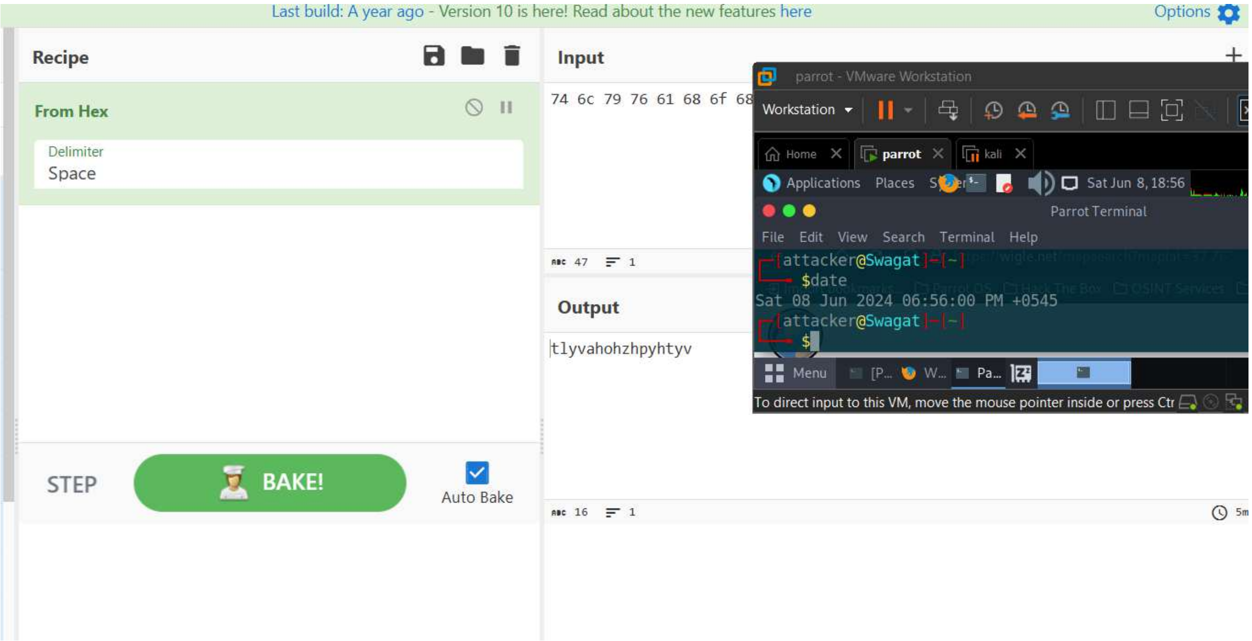
view-source:https://haridai.sushilphuyal.com.np/Pratikxya/

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Document</title>
</head>
<body bgcolor="black">
    <font color="black">
    <center> 74 6c 79 76 61 68 6f 68 7a 68 70 79 68 74 79 76 </center>
    <!--alhabet=a-z

        hint: left or right then xeh it.
    --></font>
    <center><img src="b.jpg"> </center>
   <center> <font color="white">यो हरी बहादुर पनि हक्केर हो कि कसो? यो पनि बुज्यो त। </font></center>
   <body oncontextmenu="return false">
    <script>
        document.onkeydown = function(e) {
            if(event.keyCode == 123) {
               return false;
            }
            if(e.ctrlKey && e.shiftKey && e.keyCode == 'I'.charCodeAt(0)) {
               return false;
            }
            if(e.ctrlKey && e.shiftKey && e.keyCode == 'C'.charCodeAt(0)) {
               return false;
            }
            if(e.ctrlKey && e.shiftKey && e.keyCode == 'J'.charCodeAt(0)) {
               return false;
            }
            if(e.ctrlKey && e.keyCode == 'U'.charCodeAt(0)) {
               return false;
            }
          }
    </script>
</body>
</html>
```

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:53:08 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

After getting that hex, I used cyberchef to decode it and got output xa “tlyvahohzhpyhtyv” as shown in fig below:



Input

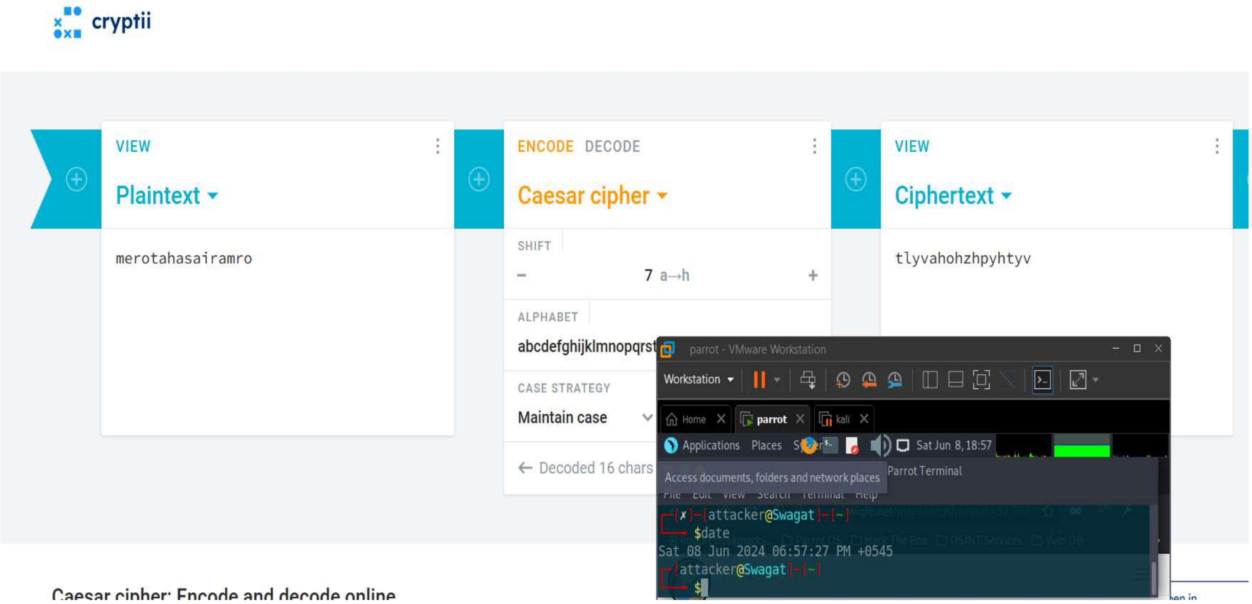
```
74 6c 79 76 61 68 6f 68
```

Output

```
tlyvahohzhpyhtyv
```

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:56:00 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

As I know the output didn't make sense, so I tried another tool named as cryptii and got another output as “ merotahasairamro” as shown in fig below:



merotahasairamro

SHIFT
7 a→h

ALPHABET
abcdefghijklmnopqrst

CASE STRATEGY
Maintain case

Decoded 16 chars

tlyvahohzhpyhtyv

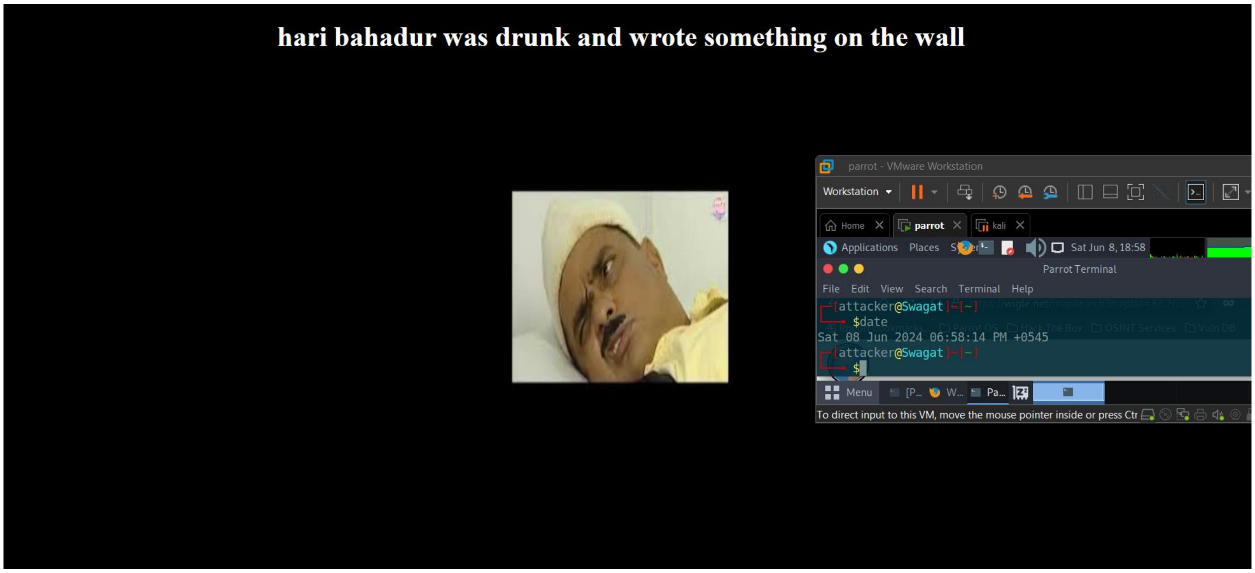
parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 18:57
Access documents, folders and network places
Parrot Terminal
File Edit View Search Terminal Help

```
┌─[✗]─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:57:27 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

Caesar cipher: Encode and decode online

This output makes sense then I checked if it is another directory by using this URL: https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/

and I was correct I got new information as shown in fig below:



hari bahadur was drunk and wrote something on the wall

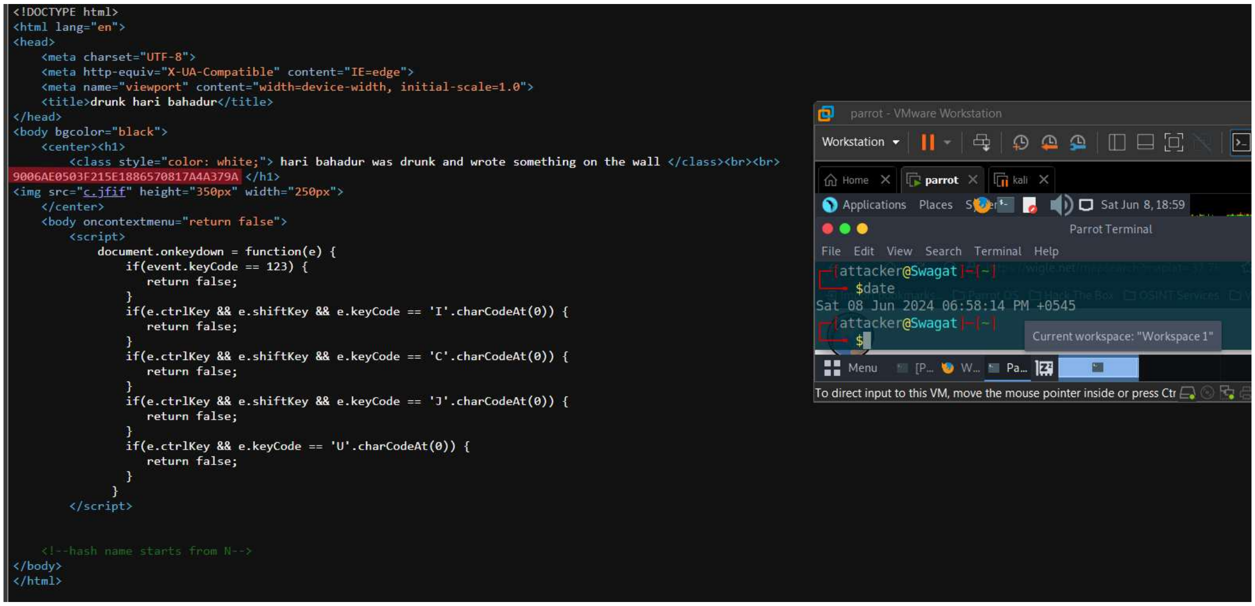
parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 18:58
Parrot Terminal
File Edit View Search Terminal Help
Menu
To direct input to this VM, move the mouse pointer inside or press Ctr

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:58:14 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

Then again, I did same thing as I have done previously i.e. writing 'view-source' in front of URL then the URL becomes:

view-source:https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/

Then I got another hash as shown in fig below:



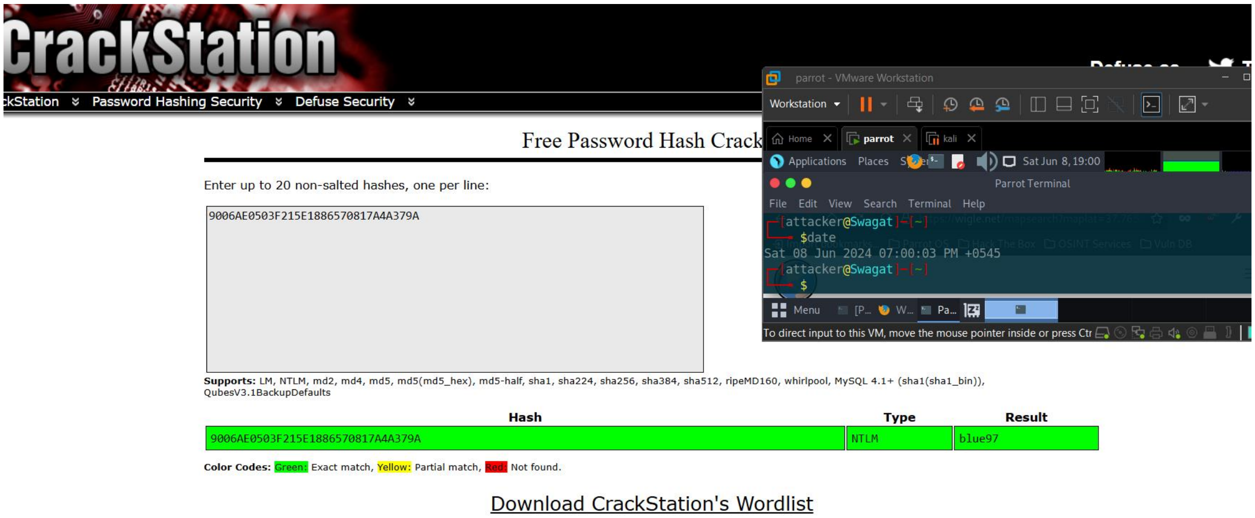
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>drunk hari bahadur</title>
</head>
<body bgcolor="black">
    <center><h1>
        <class style="color: white;"> hari bahadur was drunk and wrote something on the wall </class><br><br>
9006AE0503F215E1886570817A4A379A </h1>
<img src="c.jfif" height="350px" width="250px">
    </center>
    <body oncontextmenu="return false">
        <script>
            document.onkeydown = function(e) {
                if(event.keyCode == 123) {
                   return false;
                }
                if(e.ctrlKey && e.shiftKey && e.keyCode == 'I'.charCodeAt(0)) {
                   return false;
                }
                if(e.ctrlKey && e.shiftKey && e.keyCode == 'C'.charCodeAt(0)) {
                   return false;
                }
                if(e.ctrlKey && e.shiftKey && e.keyCode == 'J'.charCodeAt(0)) {
                   return false;
                }
                if(e.ctrlKey && e.keyCode == 'U'.charCodeAt(0)) {
                   return false;
                }
            }
        </script>


    <!--hash name starts from N-->
</body>
</html>
```

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 06:58:14 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

To direct input to this VM, move the mouse pointer inside or press Ctr

TO crack that hash i use crack station and i got another output as “blue97” which was NYLM hash as shown in fig below:



Free Password Hash Crack

Enter up to 20 non-salted hashes, one per line:

```
9006AE0503F215E1886570817A4A379A
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
9006AE0503F215E1886570817A4A379A	NTLM	blue97

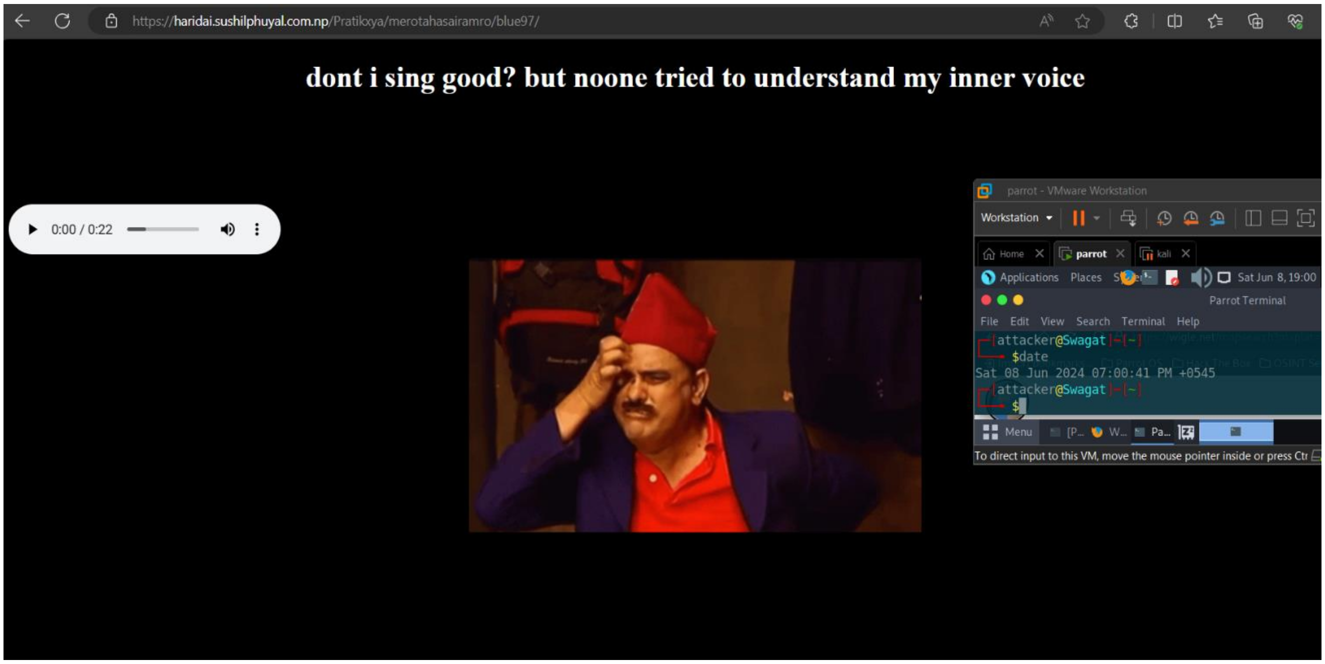
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:00:03 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

To direct input to this VM, move the mouse pointer inside or press Ctr

After knowing its result, I was forced to check if it was a new directory because of previous results and actions. Again, I was correct I got new page as shown in fig with very interesting audio which contain song I listened it more that 10 time doing this assignment as shown in fig below:

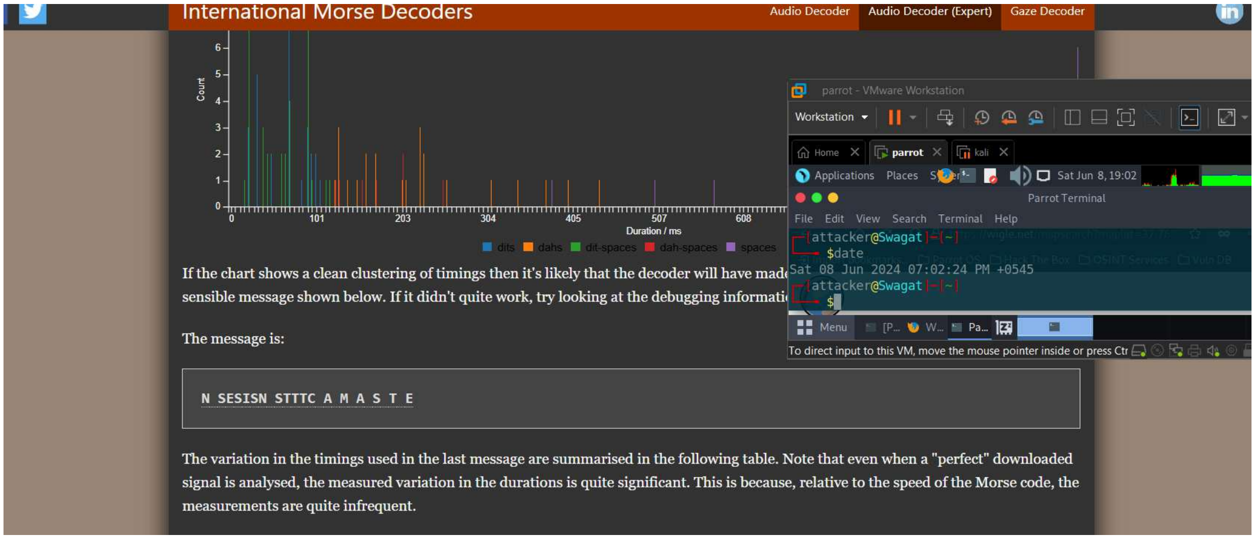


dont i sing good? but noone tried to understand my inner voice

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:00:41 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

To direct input to this VM, move the mouse pointer inside or press Ctr

The audio was not only song it was a morse code then using an online morse code decoder I decoded it and got an interesting output which is “NAMESTE” As shown in fig below:



```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:02:24 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

To direct input to this VM, move the mouse pointer inside or press Ctr

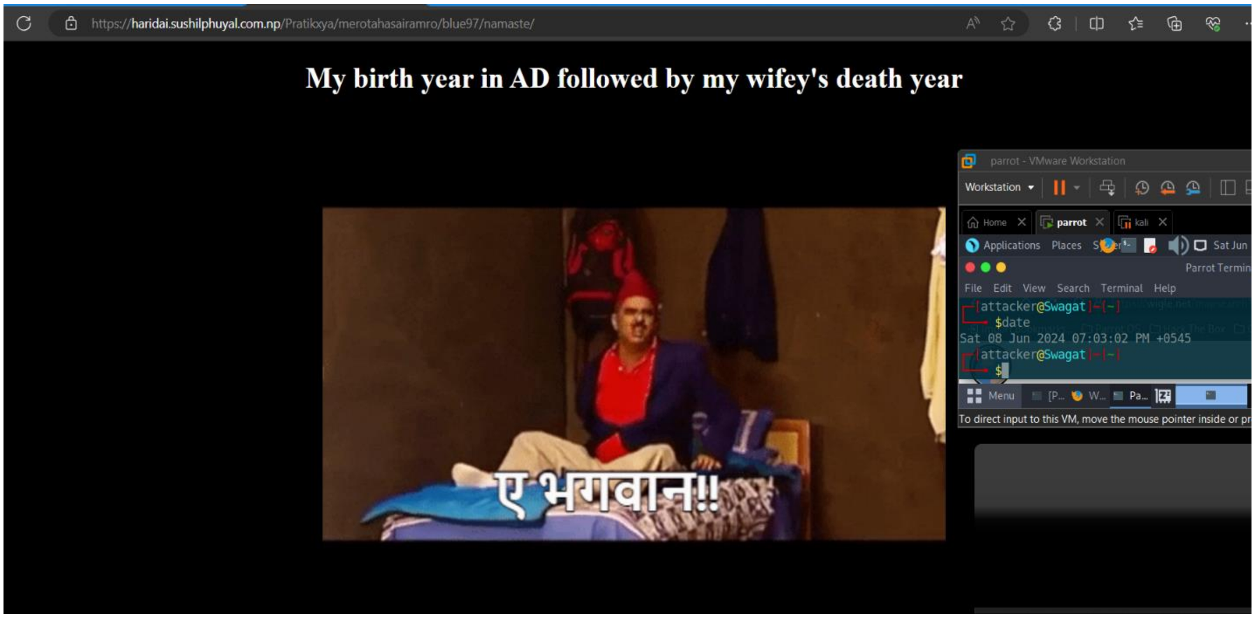
If the chart shows a clean clustering of timings then it's likely that the decoder will have made sensible message shown below. If it didn't quite work, try looking at the debugging informati

The message is:

```
N SESISN STTTC A M A S T E
```

The variation in the timings used in the last message are summarised in the following table. Note that even when a "perfect" downloaded signal is analysed, the measured variation in the durations is quite significant. This is because, relative to the speed of the Morse code, the measurements are quite infrequent.

Then again, I checked I can be another directory and I got something interesting as shown in fig below:



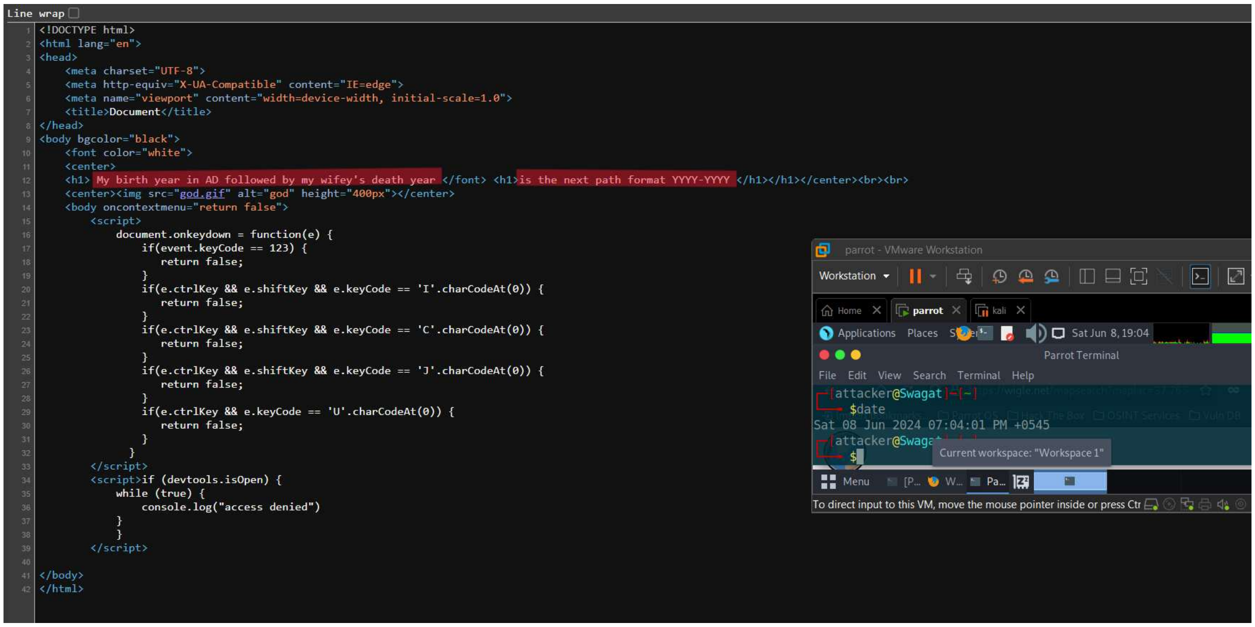
https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/blue97/namaste/

My birth year in AD followed by my wifey's death year

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:03:02 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

To direct input to this VM, move the mouse pointer inside or pr

I got message about birth year, but it was incomplete, so I again view source of it as done previously and got another lead as shown in fig below:



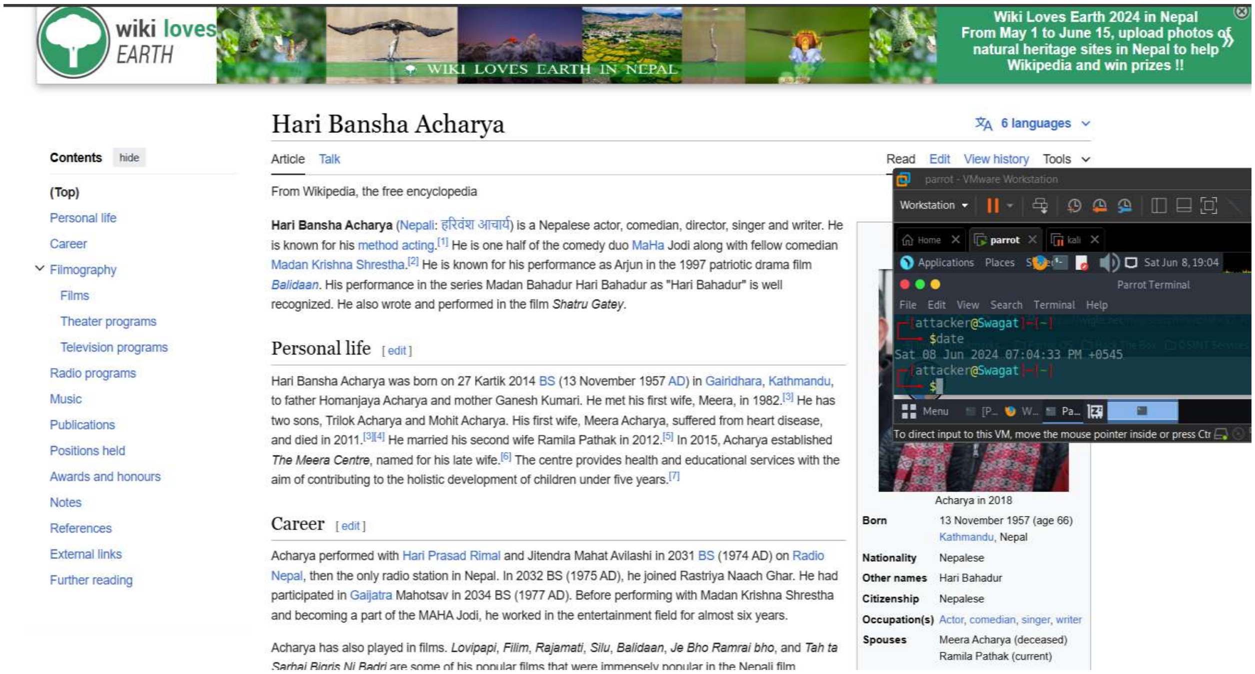
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Document</title>
</head>
<body bgcolor="black">
    <font color="white">
    <center>
    <h1> My birth year in AD followed by my wifey's death year </font> <h1>is the next path format YYYY-YYYY </h1></h1></center><br><br>
    <center><img src="god.gif" alt="god" height="400px"></center>
    <body oncontextmenu="return false">
        <script>
            document.onkeydown = function(e) {
                if(event.keyCode == 123) {
                   return false;
                }
                if(e.ctrlKey && e.shiftKey && e.keyCode == 'I'.charCodeAt(0)) {
                   return false;
                }
                if(e.ctrlKey && e.shiftKey && e.keyCode == 'C'.charCodeAt(0)) {
                   return false;
                }
                if(e.ctrlKey && e.shiftKey && e.keyCode == 'J'.charCodeAt(0)) {
                   return false;
                }
                if(e.ctrlKey && e.keyCode == 'U'.charCodeAt(0)) {
                   return false;
                }
              }
        </script>
        <script>if (devtools.isOpen) {
            while (true) {
                console.log("access denied")
            }
            }
        </script>

</body>
</html>
```

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:04:01 PM +0545
┌─[attacker@Swaga
└──╼ $
```

To direct input to this VM, move the mouse pointer inside or press Ctr

From the source I got to know” My birth year in AD followed by my wifey’s year” and” is the next path format YYYY-YYYY". Then I googled about Hari Bahadur and I got his details including birth year and so on as shown in fig below:



wiki loves EARTH
WIKI LOVES EARTH IN NEPAL
Wiki Loves Earth 2024 in Nepal From May 1 to June 15, upload photos of natural heritage sites in Nepal to help Wikipedia and win prizes !!

Hari Bansha Acharya

6 languages
Article Talk
Read Edit View history Tools

From Wikipedia, the free encyclopedia

Hari Bansha Acharya (Nepali: हरिवंश आचार्य) is a Nepalese actor, comedian, director, singer and writer. He is known for his method acting.[1] He is one half of the comedy duo MaHa Jodi along with fellow comedian Madan Krishna Shrestha.[2] He is known for his performance as Arjun in the 1997 patriotic drama film *Balidaan*. His performance in the series Madan Bahadur Hari Bahadur as "Hari Bahadur" is well recognized. He also wrote and performed in the film *Shatru Gatey*.

Personal life [edit]

Hari Bansha Acharya was born on 27 Kartik 2014 BS (13 November 1957 AD) in Gairidhara, Kathmandu, to father Homanjaya Acharya and mother Ganesh Kumari. He met his first wife, Meera, in 1982.[3] He has two sons, Trilok Acharya and Mohit Acharya. His first wife, Meera Acharya, suffered from heart disease, and died in 2011.[3][4] He married his second wife Ramila Pathak in 2012.[5] In 2015, Acharya established *The Meera Centre*, named for his late wife.[6] The centre provides health and educational services with the aim of contributing to the holistic development of children under five years.[7]

Career [edit]

Acharya performed with Hari Prasad Rimal and Jitendra Mahat Avilashi in 2031 BS (1974 AD) on Radio Nepal, then the only radio station in Nepal. In 2032 BS (1975 AD), he joined Rastriya Naach Ghar. He had participated in Gaijatra Mahotsav in 2034 BS (1977 AD). Before performing with Madan Krishna Shrestha and becoming a part of the MAHA Jodi, he worked in the entertainment field for almost six years.

Acharya has also played in films. *Lovipapi*, *Filim*, *Rajamati*, *Silu*, *Balidaan*, *Je Bho Ramrai bho*, and *Tah ta Sarhai Biqris Ni Badri* are some of his popular films that were immensely popular in the Nepali film

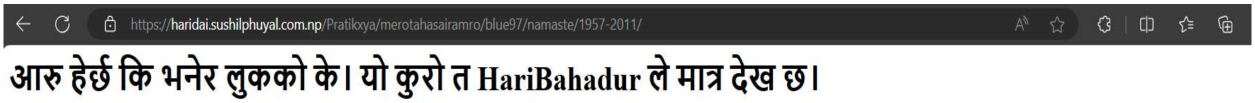
Acharya in 2018

Born	13 November 1957 (age 66) Kathmandu, Nepal
Nationality	Nepalese
Other names	Hari Bahadur
Citizenship	Nepalese
Occupation(s)	Actor, comedian, singer, writer
Spouses	Meera Acharya (deceased) Ramila Pathak (current)

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:04:33 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

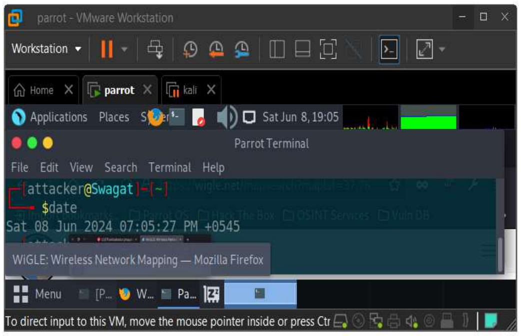
To direct input to this VM, move the mouse pointer inside or press Ctr

Which was 1957-2011 that took me to another path as shown in fig below:



https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/blue97/namaste/1957-2011/

आरु हेर्छ कि भनेर लुकको के। यो कुरो त HariBahadur ले मात्र देख छ।

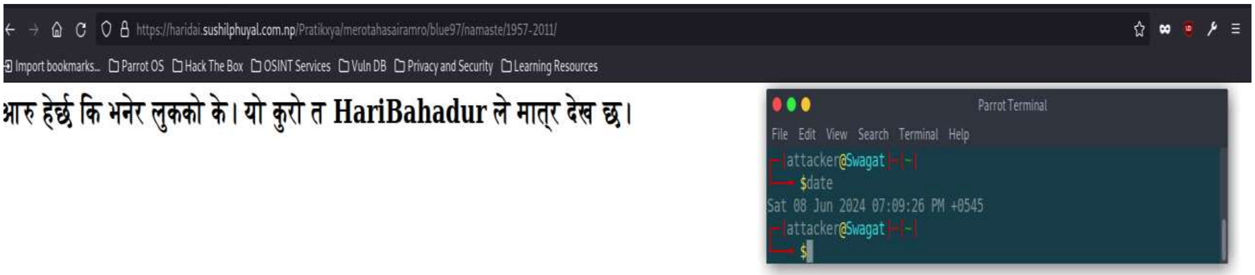


parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications Places
Sat Jun 8, 19:05
Parrot Terminal
File Edit View Search Terminal Help
WiGLE: Wireless Network Mapping — Mozilla Firefox
Menu [P... W... Pa...

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:05:27 PM +0545
```

To direct input to this VM, move the mouse pointer inside or press Ctr

From that lead I got to know Hari Bahadur can only view the site so I changed the useragent to HariBahadur and got another result as "(can you print the flag?)" As shown in the fig below:

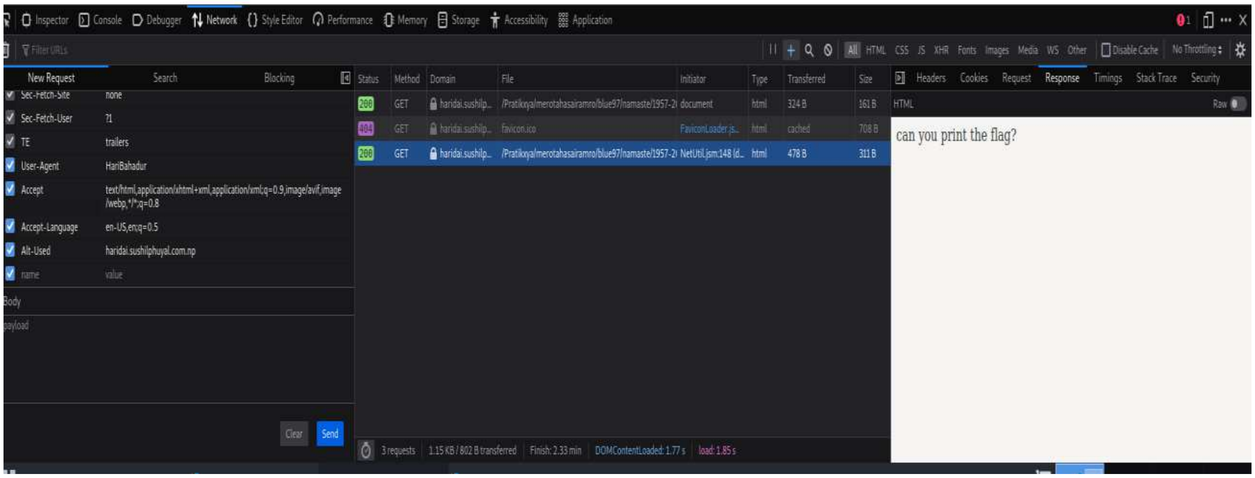


https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/blue97/namaste/1957-2011/
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources

आरु हेर्छ कि भनेर लुकको के। यो कुरो त HariBahadur ले मात्र देख छ।

Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:09:26 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```



☑ Sec-Fetch-Site	none
☑ Sec-Fetch-User	?1
☑ TE	trailers
☑ User-Agent	HariBahadur
☑ Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
☑ Accept-Language	en-US,en;q=0.5
☑ Alt-Used	haridai.sushilphuyal.com.np
☑ name	value

Body

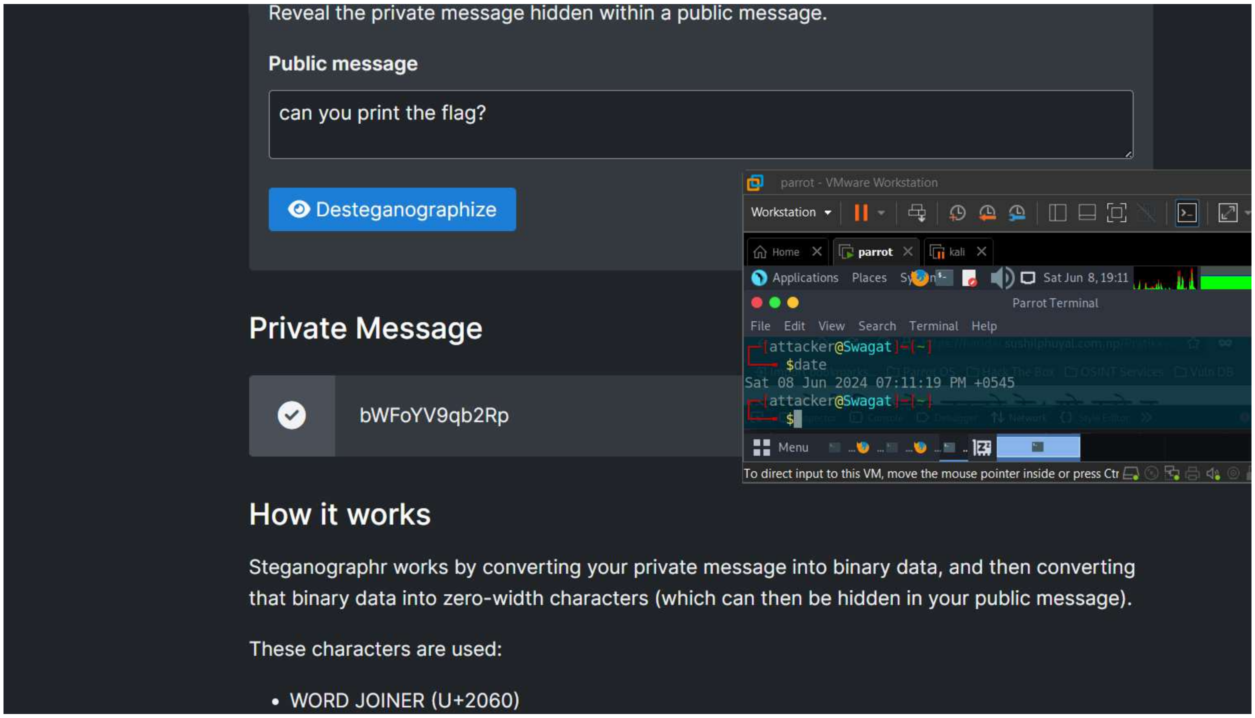
payload

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	haridai.sushilp...	/Pratikxya/merotahasairamro/blue97/namaste/1957-2(	document	html	324 B	161 B
404	GET	haridai.sushilp...	favicon.ico	FaviconLoader.js...	html	cached	708 B
200	GET	haridai.sushilp...	/Pratikxya/merotahasairamro/blue97/namaste/1957-2(	NetUtil.jsm:148 (d...	html	478 B	311 B

3 requests | 1.15 KB / 802 B transferred | Finish: 2.33 min | DOMContentLoaded: 1.77 s | load: 1.85 s

can you print the flag?

Then again, I decrypted the message using neatnik.net and got another message “bWFoYV9qb2Rp” as shown in fig below:



Reveal the private message hidden within a public message.

Public message

can you print the flag?

Private Message

bWFoYV9qb2Rp

How it works

Steganographr works by converting your private message into binary data, and then converting that binary data into zero-width characters (which can then be hidden in your public message).

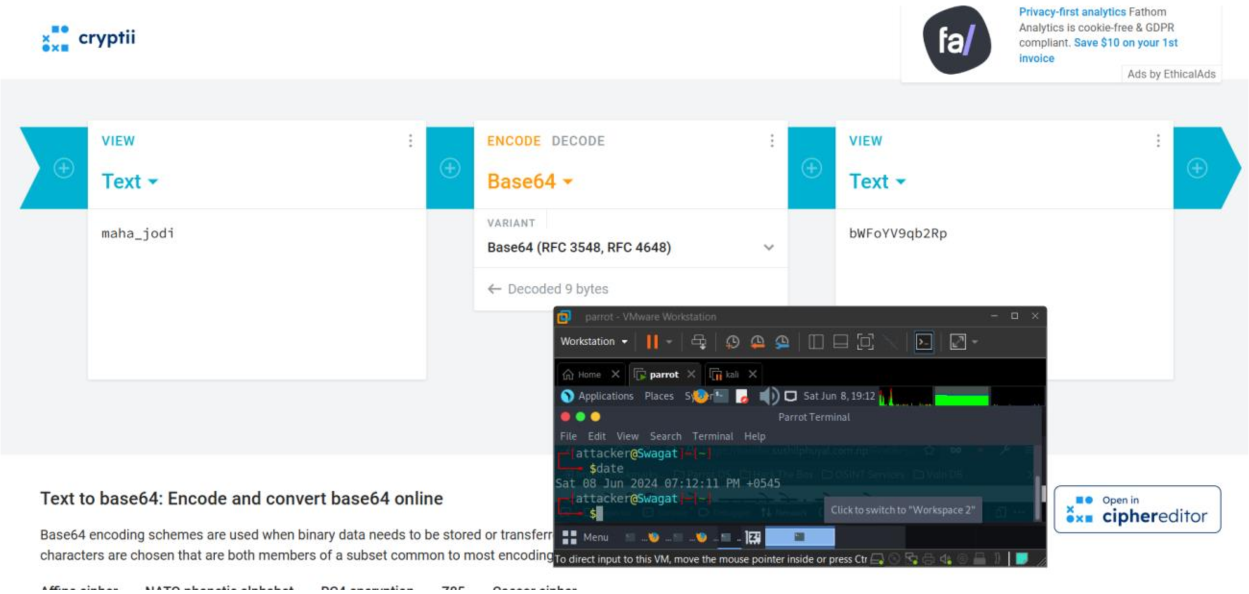
These characters are used:

- WORD JOINER (U+2060)

parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 19:11
Parrot Terminal
File Edit View Search Terminal Help
Menu
To direct input to this VM, move the mouse pointer inside or press Ctr

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:11:19 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

Aa that private message was not making sense, so I cracked it by using cryptii and got another message "maha_jodi" As shown in fig below:



maha_jodi

VARIANT
Base64 (RFC 3548, RFC 4648)

← Decoded 9 bytes

bWFoYV9qb2Rp

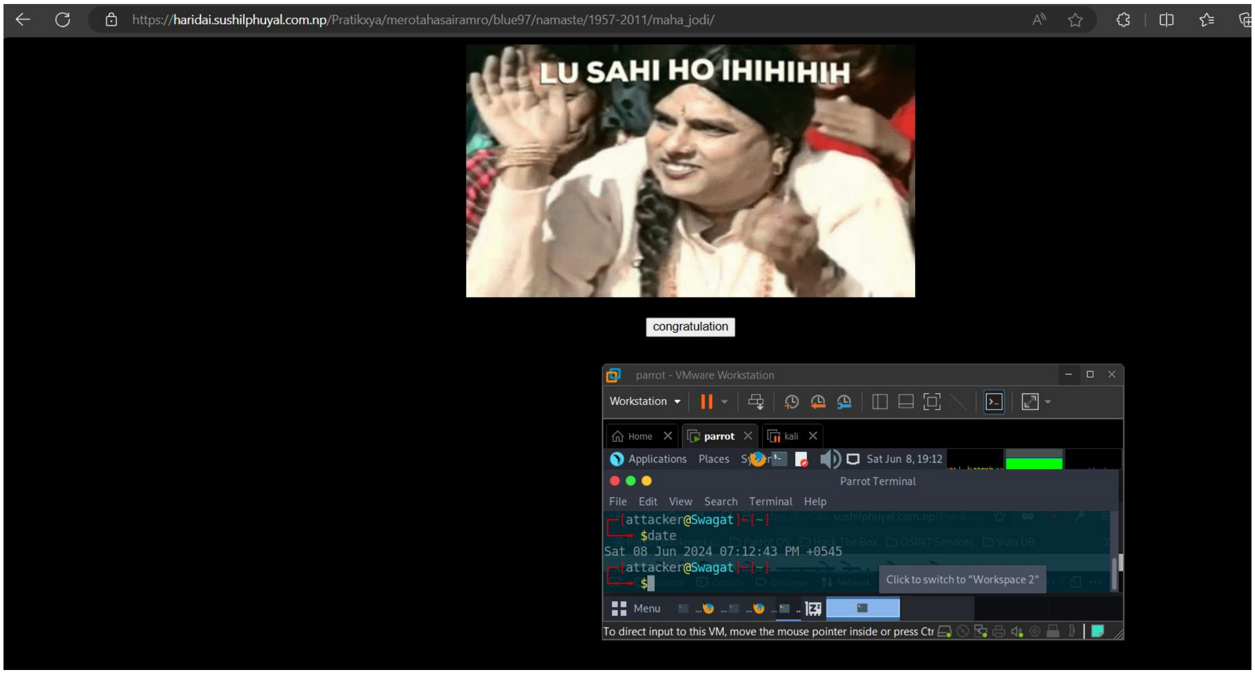
Text to base64: Encode and convert base64 online

Base64 encoding schemes are used when binary data needs to be stored or transferr characters are chosen that are both members of a subset common to most encoding

Open in ciphereditor
parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 19:12
Parrot Terminal
File Edit View Search Terminal Help
Click to switch to "Workspace 2"
Menu
To direct input to this VM, move the mouse pointer inside or press Ctr

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:12:11 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

Then I checked if it is another directory and got another result as shown in fig below:

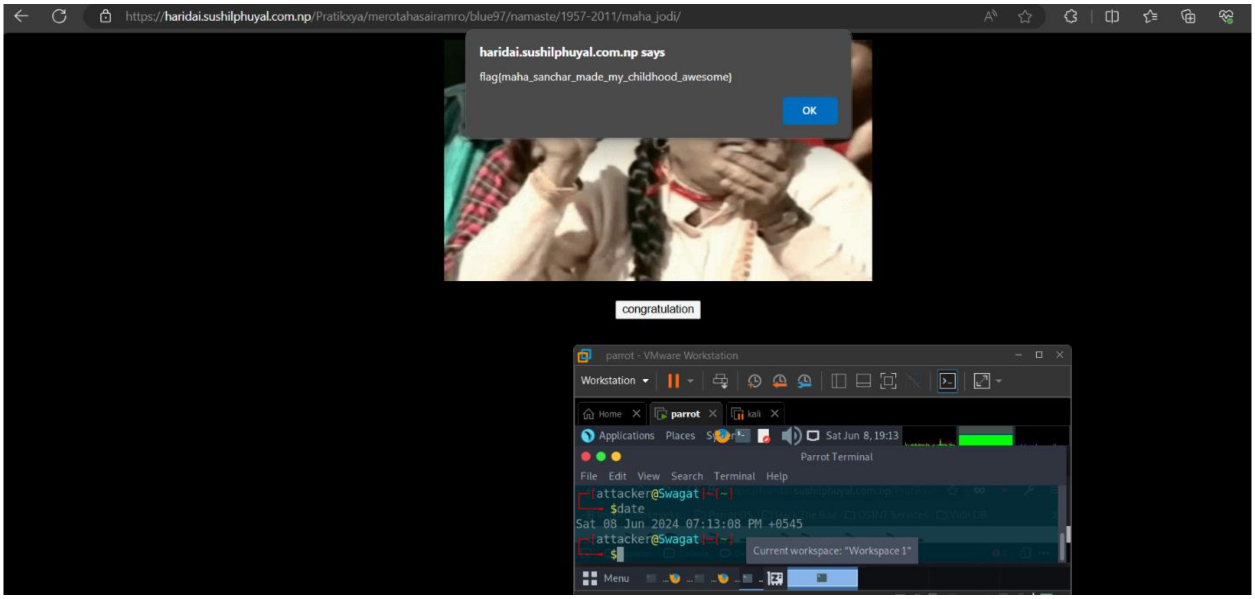


https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/blue97/namaste/1957-2011/maha_jodi/
LU SAHI HO IHIHIHIH
congratulation
parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 19:12
Parrot Terminal
File Edit View Search Terminal Help
Click to switch to "Workspace 2"
Menu
To direct input to this VM, move the mouse pointer inside or press Ctr

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:12:43 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

When I clicked on congratulation finally, I got a flag i.e. {maha_sanchar_made_my_childhood_awesome}

As shown below:



haridai.sushilphuyal.com.np says

flag{maha_sanchar_made_my_childhood_awesome}

https://haridai.sushilphuyal.com.np/Pratikxya/merotahasairamro/blue97/namaste/1957-2011/maha_jodi/
OK
congratulation
parrot - VMware Workstation
Workstation
Home
parrot
kali
Applications
Places
Sat Jun 8, 19:13
Parrot Terminal
File Edit View Search Terminal Help
Current workspace: "Workspace 1"
Menu

```
┌─[attacker@Swagat]─[~]
└──╼ $date
Sat 08 Jun 2024 07:13:08 PM +0545
┌─[attacker@Swagat]─[~]
└──╼ $
```

Answer the questions below from the above task performed

1. What was the social media you found author on?

Ans: pinterest.com

2. What was the Wi-Fi Name?

Ans: n\Now it is MAGAR HOME but previously it was Pratikxyawifi.

3. What was the Hash Type?

Ans: NTLM

4. What was the decrypted value of Hash?

Ans: Blue97

5. Who could access the site's original DOM?

Ans: HariBahadur

6. What was the unprintable text after decoding?

Ans: Maha_jodi

7. What was the flag?

Ans: flag{maha_sanchar_made_my_childhood_awesome}

Conclusion

Capture the Flag competitions are valuable for developing and testing cybersecurity skills. By solving challenges related to OSINT, geolocation, cryptography, steganography, and hash cracking, participants enhance their knowledge and problem-solving abilities. The key to success in CTF events is persistence and continuous practice.

Reference

CTF File - What is a .ctf file and how do I open it? (fileinfo.com)

Solving HariBahadur CTF. URL to join the CTF… | by sushil phuyal | Medium

https://en.wikipedia.org/wiki/Hari_Bansha_Acharya