

CTF ANSWERS

Question : Open the PDF

This file was found among some files marked confidential but my pdf reader cannot read it, maybe yours can.

Answer: SAIT'SCTF{ageisjustanumberandjailisjustaroom}

```
document.pdf README.license
[+] parrot@parrot:[~/Desktop]
[+] $ file document.pdf
document.pdf: shell archive text
[+] parrot@parrot:[~/Desktop]
[+] $ ./document.pdf
bash: ./document.pdf: Permission denied
[+] x[-]parrot@parrot:[~/Desktop]
[+] $ chmod +x document.pdf
[+] parrot@parrot:[~/Desktop]
[+] $ ls
document.pdf README.license
[+] parrot@parrot:[~/Desktop]
[+] $ ./document.pdf
x - created lock directory _sh03351.
x - extracting file (text)
x - removed lock directory _sh03351.
[+] parrot@parrot:[~/Desktop]
[+] $ ls
document.pdf file README.license
[+] parrot@parrot:[~/Desktop]
[+] $ file
file: current ar archive
[+] parrot@parrot:[~/Desktop]
[+] $ ar xv flag
ar: flag: No such file or directory
[+] x[-]parrot@parrot:[~/Desktop]
[+] $ ar xv file
x - string
[+] parrot@parrot:[~/Desktop]
[+] $ ls
document.pdf file README.license string
[+] parrot@parrot:[~/Desktop]
[+] $ cat string
53 41 49 54 27 53 43 54 46 7b 61 67 65 69 73 6a 75 73 74 61 6e 75 6d 62 65 72 61 6e 64 6a 61 69 6c 69 73 6a 75 73 74 61 72 6f 6d 7d
[+] parrot@parrot:[~/Desktop]
```

Hex to Ascii (String) Converter

To use this hex to string converter, type a hex value like 6C 6F 76 65 and into the left field below and hit the Convert button. You will get the according string.

[Facebook](#) [Twitter](#)

Hexadecimal Value
5341495427534354467b61676569736a757374616e756d626572616e646a61696c69736a75737461726f

Ascii (String)
SAIT'SCTF{ageisjustanumberandjailisjustaroom}

Convert

swap conversion: [Ascii Text To Hexadecimal Converter](#)

CHRISTMAS GIFT

Question: Guess what happened when Santa accidentally stumbled upon the top-secret elf meeting while delivering presents? Did he discover the elves' hidden dance moves, their secret cookie recipe, or the decor ? Explore Santa's website here : <https://xmass3.s3.us-east-2.amazonaws.com/christmas.html>

Christmas4.wav audio has a flag in it:

The screenshot shows a media player interface with five separate audio tracks. Each track has a play button, a progress bar, and a volume icon. The first four tracks are highlighted with red boxes. Above the tracks, there is a text overlay of a poem:

*On this joyous day of mirth and cheer,
Let's gather 'round, our loved ones near.
A time for giving, a time for delight,
With hearts aglow and spirits bright.
Listen to the carols, sweet and clear,
As we celebrate the season, full of good cheer.*

Below the诗, there is a 'Gifts' section with a download button and a playback speed slider. The bottom track is not highlighted.


```
(kali㉿kali)-[~/q1]
$ steghide extract -sf christmas4.wav
Enter passphrase:
wrote extracted data to "christmas.txt".
(kali㉿kali)-[~/q1]
$ ls
christmas4.wav  christmas.txt  crypto.jpeg  flag.txt
```

In the fourth paragraph of poem till end, first word of each line combines the flag.

```
Silent whispers weave a cryptic tale,  
A realm of secrets, elusive and frail.  
In shadows cast by the moonlight's veil,  
Trail the echoes, hear the flag's subtle wail.  
  
Sneath the surface, where codes prevail,  
Crafted enigmas, elusive and stale.  
Tokens hidden in the cryptographic gale,  
Fragments entwined in a complex trail.  
  
Jovial Johny, elusive in the code,  
On paths of letters, a labyrinth's ode.  
Cryptic ciphers intertwine, a journey to decode,  
Keystrokes echo, in secrets he strode.  
  
Ethereal whispers echo in the cryptic tale,  
A dance of letters, a nuanced braille.  
Subtle hints beneath the moonlight's pale,  
Fragments of a puzzle in the cipher's trail.  
  
Juxtaposed characters, an elusive abode,  
On the parchment of cyberspace, stories are stowed.  
Cryptic symbols dance in a complex code,  
Keystrokes create an intricate ode.
```

Flag: SAIT'SCTF{JOCKEASFJOCKSECTIAFA}

REVERSE QUESTIONS:

Question: Tie the knots together

Using the attached files tie pieces together to pull the flag.

(kali㉿kali)-[~/CTF/q3]\$ ls
happy.c happy happy.tar.gz

(kali㉿kali)-[~/CTF/q3]\$ strings happy

```
#!/lib64/ld-linux-x86-64.so.2
puts
__libc_start_main
__cxa_finalize
printf
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Secret MH
Message
```

```
/lib64/ld-linux-x86-64.so.2
puts
__libc_start_main
__cxa_finalize
printf
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Secret MH
Message
U0FJ
```

Congratulations! You've uncovered the hidden message.
Welcome to the Advanced Mystery Program!
The secret message is: %s ;*3\$"

Picking up the piece: U0FJ

Analyzing the log file:

```

30T11:40:12.768672-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:12.769373-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:15.137547-05:00 kali rtkit-daemon[794]: Supervising
2023-11-30T11:50:53.145218-05:00 kali kali: #0122023-11-30T11:40:04.568573-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of
1 users.#0122023-11-30T11:40:05.791927-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-
30T11:40:05.792823-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:05.803121-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:05.803505-05:00 kali rtkit-daemon[794]: Supervising 8
threads of 5 processes of 1 users.#0122023-11-30T11:40:06.000695-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-
30T11:40:12.768672-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:12.769373-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:15.137547-05:00 kali rtkit-daemon[794]: Supervising
2023-11-30T11:51:32.195337-05:00 kali kali: lock is : VCdTQ1RGe21hc3RlcmluZ0N5YmVyc2VjdXJpdHkxMjI0NDQxfQ==
2023-11-30T11:51:34.726778-05:00 kali kali: #0122023-11-30T11:40:04.568573-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of
1 users.#0122023-11-30T11:40:05.791927-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-
30T11:40:05.792823-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:05.803121-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:05.803505-05:00 kali rtkit-daemon[794]: Supervising 8
threads of 5 processes of 1 users.#0122023-11-30T11:40:06.000695-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-
30T11:40:12.768672-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:12.769373-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:15.137547-05:00 kali rtkit-daemon[794]: Supervising
2023-11-30T11:51:37.303037-05:00 kali kali: #0122023-11-30T11:40:04.568573-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of
1 users.#0122023-11-30T11:40:05.791927-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:05.803121-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:05.803505-05:00 kali rtkit-daemon[794]: Supervising 8
threads of 5 processes of 1 users.#0122023-11-30T11:40:06.000695-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-
30T11:40:12.768672-05:00 kali rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:12.769373-05:00 kali
rtkit-daemon[794]: Supervising 8 threads of 5 processes of 1 users.#0122023-11-30T11:40:15.137547-05:00 kali rtkit-daemon[794]: Supervising
2023-11-30T11:52:05.598975-05:00 kali dbus-daemon[1059]: [session uid=1000 pid=1059] Activating via systemd: service
name='org.freedesktopthumbnails.Cache1' unit='tumblerd.service' requested by ':1.26' (uid=1000 pid=1285 comm="Thunar --sm-client-id 2d5c9873f-
2aad-4c39-8583-cd")
2023-11-30T11:52:50.611843-05:00 kali systemd[1035]: Starting tumblerd.service - Thumbnailing service...
2023-11-30T11:52:50.680971-05:00 kali dbus-daemon[1059]: [session uid=1000 pid=1059] Successfully activated service
'org.freedesktopthumbnails.Cache1'
2023-11-30T11:52:50.682745-05:00 kali systemd[1035]: Started tumblerd.service - Thumbnailing service.

```

2nd piece: VCdTQ1RGe21hc3RlcmluZ0N5YmVyc2VjdXJpdHkxMjI0NDQxfQ==

Combining both : U0FJVCDTQ1RGe21hc3RlcmluZ0N5YmVyc2VjdXJpdHkxMjI0NDQxfQ==

Decode from Base64 format

Simply enter your data then push the decode button.

U0FJVCDTQ1RGe21hc3RlcmluZ0N5YmVyc2VjdXJpdHkxMjI0NDQxfQ==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set

Decode each line separately (useful for when you have multiple entries).

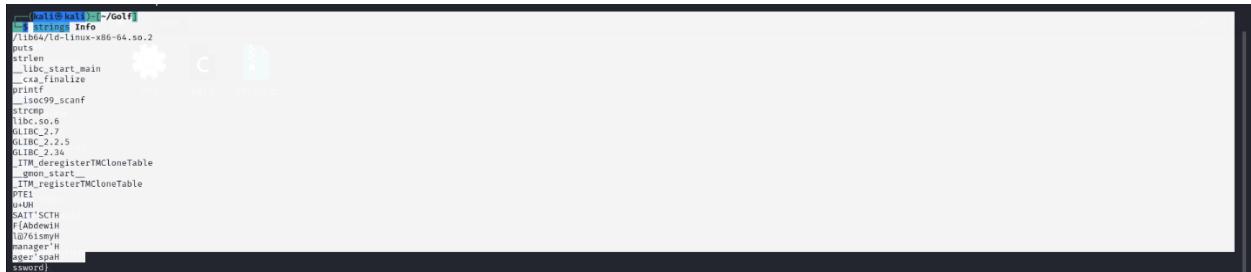
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

SAITSCFT(masteringCybersecurity1224441)

Question: Digital Mystery Unveiled: Crack the Code!

In the world of computers, something fishy's going on! Our tech team found a sneaky member within a hacking gang trying to send secret info to their buddy. Spill the beans!!



```
Bolt@Bolt:~/Golf$ strings Info
/usr/lib64/ld-linux-x86-64.so.2
putchar
strlen
__libc_start_main
__cxa_finalize
printf
__isoc99_scanf
strcmp
__libc_csu_init
__libc_csu_fini
GLIBC_2.0
GLIBC_2.1
GLIBC_2.2
GLIBC_2.3
GLIBC_2.4
__TMC_start
__TMC_registerTMCloneTable
__libc_start_main
__TMC_registerTMCloneTable
PTE1
main
SATT'SCTH
P{AbdewiH
10761smyH
msgag$H
age$spal
ssword}
```

Question: Multiply the numbers

The following program multiplies the number, manage to the flag from it.

root@ubuntu-VirtualBox:/home/ubuntu/C# ls
Program Program.c Program.tar.gz
root@ubuntu-VirtualBox:/home/ubuntu/C# bless Program
Gtk-Message: 12:53:00.030: Failed to load module "canberra-gtk-module"
Failed to open plugins directory: Could not find a part of the path '/root/.config/bl
ess/plugins'.
Failed to open plugin
ess/plugins'.
Failed to open plugin
ess/plugins'.
Could not find file

/home/ubuntu/C/Program - Bless

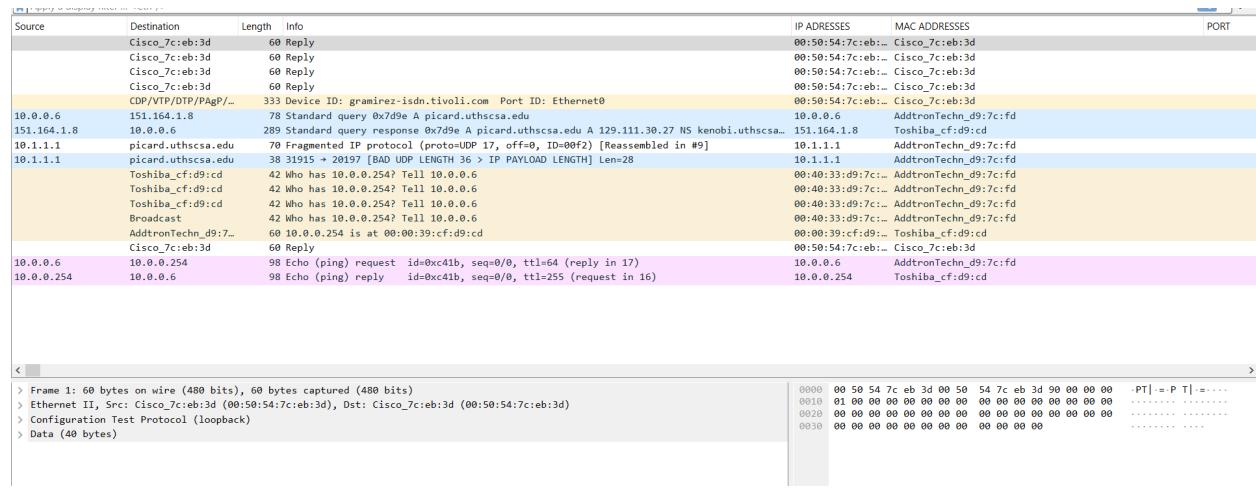
Program []

Signed 8 bit:	45	Signed 32 bit:	758216034	Hexadecimal:	2D317562
Unsigned 8 bit:	45	Unsigned 32 bit:	758216034	Decimal:	045049117098
Signed 16 bit:	11569	Float 32bit:	1.009735E-11	Octal:	055061165142
Unsigned 16 bit:	11569	Float 64 bit:	5.35659832890027E-91	Binary:	0010110100110001011

Offset: 0x3e09 / 0x29 Selection: 0x3e09 / 0x29 huted INC

Networks

Question: Analyze the wireshark capture and name the attack.



The Teardrop Attack is a type of Denial of Service (DoS) attack that targets the fragmentation handling of the IP protocol. Packets 8 and 9 show the overlapping IP fragments in a Teardrop attack.

Get \$10,000.000.00

Hunting for humor and scammers: In the email promising a fortune, Janet Yellen is apparently feeling generous. To get that sweet scam money, pull up the country the scammer claims to represent.

Mrs Janet Yellen mrsjanet_yellen9@netvigator.com [Reply](#) [Forward](#) [Archive](#) [Junk](#) [Delete](#) [More](#)

Re US Department of Treasury

US Department of Treasury
Address: 1500 Pennsylvania Ave NW, Washington, DC 20220, USA.
Formed: September 2, 1789
Preceding agency: Board of Treasury

Greetings to you.
Introduction: My name is Janet Yellen an American economist. Served as the 15th chair-lady of the Federal Reserve from 2014 to 2018, Currently serving as the 78th United States secretary of the treasury since 2021.

This is to let you know about the conclusion of our meeting yesterday with World Bank Director(Anshula Kant) FBI Director (Christopher A.Wray) United Nation Secretary General (Antônio Guterres) and CDC Director (Rochelle Walensky) regarding this Pandemic situation arising across the globe which is as a result of Corona Virus (COVID-19).

The World Bank and United Nations release the sum of \$100,000,000.00 One Hundred Million Dollars) to be shared among the 10 Scam Victims as a Compensation.

I was subjected to submit the first 10 names to receive the sum of \$10,000,000.00 (Ten Million Dollars Only) from this fund while the second batch will be approved by next week for other payment. Through the help of FBI Director (Christopher A. Wray) who gave me your name and email to add so that you will partake in this fund since he narrated to me that you have been a scam victim for several years now and have nothing left so this will serve as an opportunity for you to replace for what you have lost in the past years and be able to survive with your family this time.

You are eligible to receive this \$10,000,000.00 USD as a compensation but you are strictly warned to stop any further communication with any person or office that claims to have any fund for you because if you lose any money again, we shall not attend to you again.

You are to Kindly Re-confirm this information so that I can commence with the documentation process to enable you receive your fund within 48 hours.

Your Full Name....
Your Address.....
Your Occupation....
Your Phone Number...
Your Age....
Awaiting for your response ASAP.

Regards,
Janet Yellen

From unknown to wbironoutv2.netvigator.com
to imsantv72.netvigator.com
to mx.google.com
to -

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknown 112.120.62.241	wbironoutv2.netvigator.com	SMTP	11/18/2023 2:35:23 PM	✖
2	16 seconds	wbironoutv2.netvigator.com 210.87.247.26	imsantv72.netvigator.com	ESMTP	11/18/2023 2:35:39 PM	✖
3	8 seconds	imsantv72.netvigator.com 210.87.250.172	mx.google.com	ESMTPS	11/18/2023 2:35:47 PM	✖
4	1 Second		2002.a05.7301.4707.b0.f4.5aafe36	SMTP	11/18/2023 2:35:48 PM	

X EMAILS BOUNCING? MxToolbox has your email delivery solutions

SPF and DKIM Information

The ip of the sender is 112.120.62.241

MY IP IP LOOKUP HIDE MY IP VPNS TOOLS LEARN

IP Details For: 112.120.62.241

Decimal: 1886928625
Hostname: n11212062241.netvigator.com
ASN: 4760
ISP: Hong Kong Telecommunications (HKT) Limited
Services: None detected
Assignment: Likely Static IP
Country: Hong Kong
State/Region: Hong Kong
City: Hong Kong



See the difference a better, more intuitive LMS can make. Try Absorb today.

Visit Site

Question: Wacky Database

Someone sneaky played with our database. Your job: dig through the tech talk and uncover the secret SQL move. What's the name of the surprise table they made appear out of nowhere?"



Question: Cryptic Pursuit

Veteran operative, you're in the crosshairs of "The Enigma Collective." They've concealed a vital message within the shadows of "VmpKc2RXUkhWbmxoV0U1dIrsaEtiQT09". This covert code is your only lead. Navigate the labyrinth of cryptic challenges, decode the obscured intel, and unveil the veil shrouding their ominous agenda. This mission demands your utmost cunning and cryptographic finesse. Godspeed, agent. The clock is ticking.

Flag : SAIT'SCTF{Winterishere}

The challenge is thrice encoded in base64

The screenshot shows a web-based base64 decoder. At the top, there is a text input field containing the string "VmpKc2RXUkhWbmxoV0U1dIrsaEtiQT09". Below the input field are several configuration options: a dropdown menu set to "UTF-8", a checkbox labeled "Decode each line separately (useful for when you have multiple entries)", and a checkbox labeled "Live mode OFF" which is checked. A prominent green button labeled "DECODE" is centered below these settings. The background of the page is light gray.

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

VJsdWRHVnlnWE5vWlhKbA==

Decode from Base64 format

Simply enter your data then push the decode button.

VJsdWRHVnlnWE5vWlhKbA==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

V2IudGVyaXNoZXJl

This screenshot shows the same base64 decoder interface as the previous one, but with a different input value. The text input field now contains "V2IudGVyaXNoZXJl". The configuration options and the "DECODE" button are identical to the first screenshot.

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

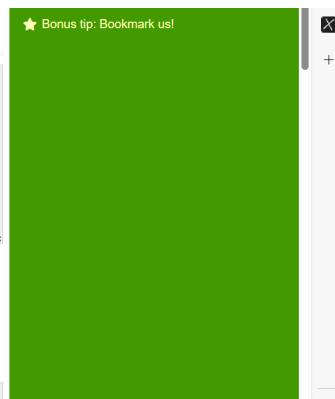
UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

Winterishere

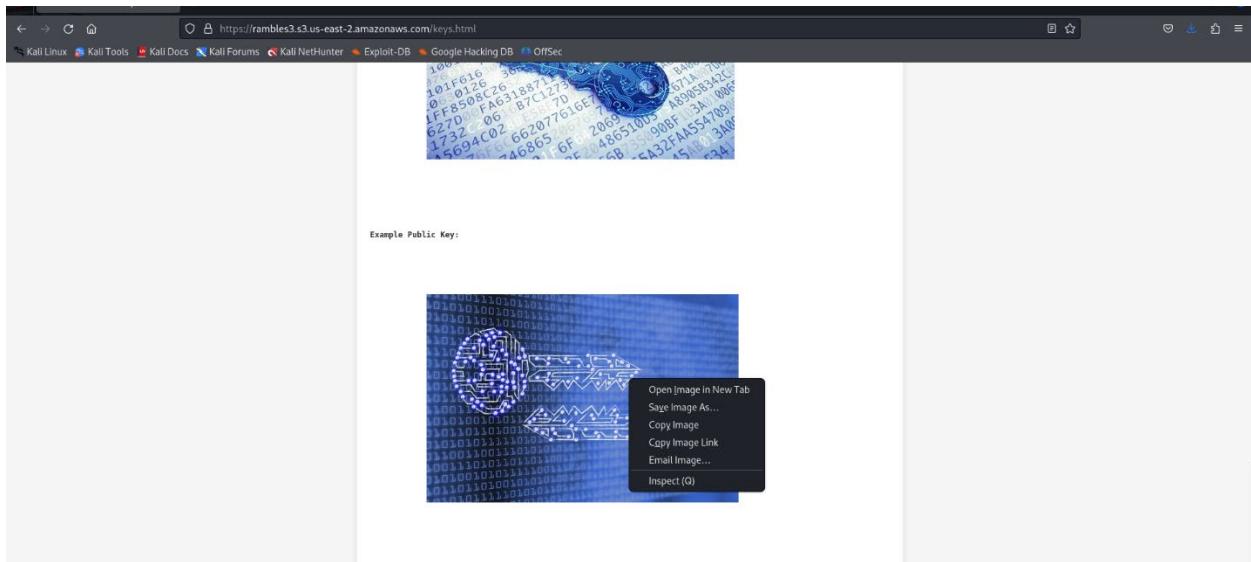


Question: Solve the mystery

<https://rambles3.s3.us-east-2.amazonaws.com/crypto.html> has your private key.

Your public key and Cipher are in the document attached. Guess the algorithm and solve the mystery.

Flag: SAIT'SCTF{You_found_it}



RSA Encryption, Decryption And Key Generator Online | Devglan

Algorithm is: RSA

Generate RSA Key Online

Create your first presentation

Create truly unique presentations. No installations or downloads required, and it's free.

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

```
JAUzfD58Gf8mp+7s42Yl/OCaHlqBAe9jpbiyp
znOow6nf/ntbbQMbaAX/z9fhQcVbkIlyFV/nM
jIKgs@UZ52a7lB5mKVKShnILQCgM/FF8JVFhG
```

Enter Public/Private key

```
JpZ9kYuYuGihWVMreXh8AfR2WpvFRMK/dPW
2s/dSKMR79+imecbd+XPrnxIDs/0T
xIDigGnVIIuxxiuiAdZrSovNVX7J9Yj80dmUsq
7cQ45c9AY09MIXGBQEIrznkIVh
Tg6VoHeWcqKBuZl7ZIFYiYU=
```

RSA Key Type: Public key Private Key

Select Cipher Type

RSA/ECB/PKCSIPadding

Decrypt

RSA Key Type: Public key Private Key

Select Cipher Type

RSA/ECB/PKCSIPadding

Encrypt

Encrypted Output (Base64):

Result goes here

RSA Key Type: Public key Private Key

Select Cipher Type

RSA/ECB/PKCSIPadding

Decrypt

Decrypted Output:

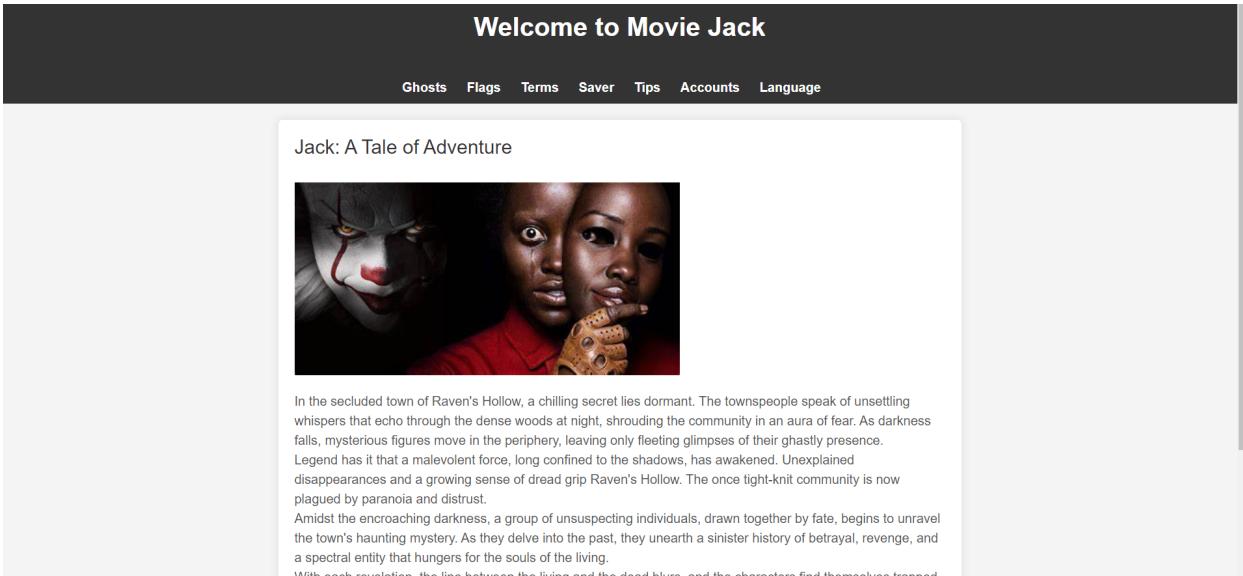
\$AIT'SCTF{You_found_it}

Create your first presentation

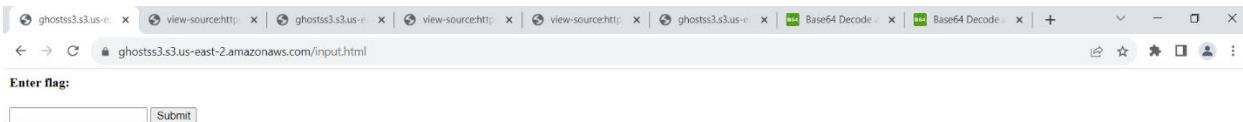
Create truly unique presentations. No installations or downloads required, and it's free.

Let your team's ideas take shape

WEBSERVER: Main page



Going into the input.html page > hit ctrl+U

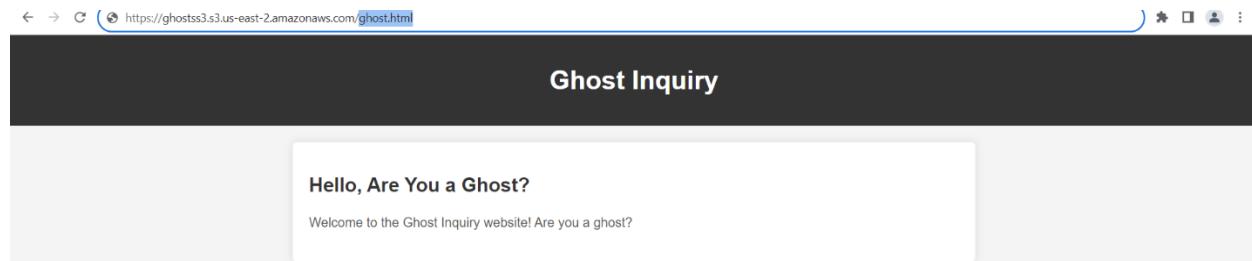


Go to miinijs.js

Zengo is the lead, try Zengo.html , Zengo.txt and see what we get!

FLAG 2:

Ghost has been repeated four times! Wow...try playing with the word ghost



The image contains two screenshots of web browser windows. The top window shows a file named 'ghost.txt' with the following content:

```
User-agent: *
Disallow: /bb.html
```

The bottom window shows a page titled 'ghost Directive' with the following content:

ghost.txt Content:

```
User-agent: *
Disallow: /bb.html
```

cultural boundaries and spanning epochs. These spectral entities, believed to be the remnants of departed souls, linger in the collective consciousness, leaving an indelible mark on folklore, literature, and popular culture. As we explore the enigma of ghosts, we delve into the multifaceted aspects of these apparitions, from historical perspectives to contemporary beliefs.

Historically, the concept of ghosts has been deeply rooted in various cultures, each contributing to the rich tapestry of supernatural lore. Ancient civilizations, such as the Egyptians and Greeks, held beliefs in spirits that transcended the mortal realm. The concept of an afterlife, where spirits continued to exist, was central to many religious and cultural practices. In medieval Europe, ghost stories became a prevalent form of entertainment, with tales of restless spirits seeking redemption or revenge captivating audiences around flickering hearth fires. Theories surrounding the existence of ghosts are as diverse as the cultures that embrace them. Paranormal enthusiasts often categorize ghostly encounters into two main types: residual hauntings, where spirits are trapped in a loop, reenacting past events, and intelligent hauntings, where entities interact with the living. However, skeptics argue that many supposed ghostly phenomena can be attributed to psychological factors. Sleep paralysis, for instance, may cause vivid hallucinations that individuals interpret as ghostly visitations. Pareidolia, the tendency to perceive familiar patterns in random stimuli, may lead people to see ghostly figures in shadows or reflections. Famous ghost stories, whether rooted in historical events or embellished through generations, continue to captivate audiences. The Tower of London, with its centuries of history, is said to be haunted by the spirits of executed prisoners and royalty. The Brown Lady of Raynham Hall, a photograph capturing a spectral apparition on a grand staircase, remains one of the most famous images in the realm of supernatural photography. Modern urban legends, such as the vanishing hitchhiker or the haunted doll Annabelle, perpetuate the allure of ghostly encounters in contemporary society. SAIT'SCTF{youarenotaghost} The fascination with ghosts extends to the practice of ghost hunting, a burgeoning subculture that employs various tools and technologies in an attempt to communicate with the spirit world. From electromagnetic field (EMF) meters to infrared cameras, ghost hunters employ an array of equipment during paranormal investigations. Despite the popularity of these endeavors, skeptics question the validity of evidence obtained through such methods, asserting that much of it can be attributed to natural explanations or environmental factors.

Flag 3: Welcome to moviejack page

The image shows a screenshot of a web browser displaying a login form. The title of the form is 'Welcome to Moviejack'. The form includes fields for 'Username:' and 'Password:', both represented by empty input boxes. Below the password field is a green 'Login' button.

Hit ctrl + u

```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Movie CTF Login</title>
7   <script src="index.js"></script>
8   <style>
9     body {
10       font-family: Arial, sans-serif;
11       background-color: #f2f2f2;
12       text-align: center;
13       margin: 100px;
14     }
15
16     .login-container {
17       max-width: 400px;
18       margin: auto;
19       background-color: #fff;
20       padding: 20px;
21       border-radius: 8px;
22       box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
23     }
24
25     .login-container h2 {
26       color: #333;
27     }
28
29     .form-group {
30       margin-bottom: 20px;
31     }
32
33     .form-group label {
34       display: block;
35       margin-bottom: 8px;
36       color: #666;
37     }
38
39     .form-group input {

```

Ahmmm...index.js

ghostss3.s3.us-east-2.amazonaws.com/index.js

```

document.addEventListener('DOMContentLoaded', function () {
  // Add event listener to the login form
  document.getElementById('loginForm').addEventListener('submit', function (event) {
    event.preventDefault(); // Prevent the form from submitting in the traditional way

    // Get the values entered by the user
    var username = document.getElementById('username').value;
    var password = document.getElementById('U0FJVcdTQ1RGe3VjX2Nhbgdhcnl0').value;

    // Perform basic client-side validation
    if (!username || !password) {
      alert('Please enter both username and password.');
      return;
    }

    // Simulate server-side authentication (this is just an example, not secure)
    if (username === 'admin' && password === 'U0FJVcdTQ1RGe01FYW1fbm90eW91cmZsYnd9') {
      alert('Login successful!');
    } else {
      alert('Invalid username or password');
    }
  });
}

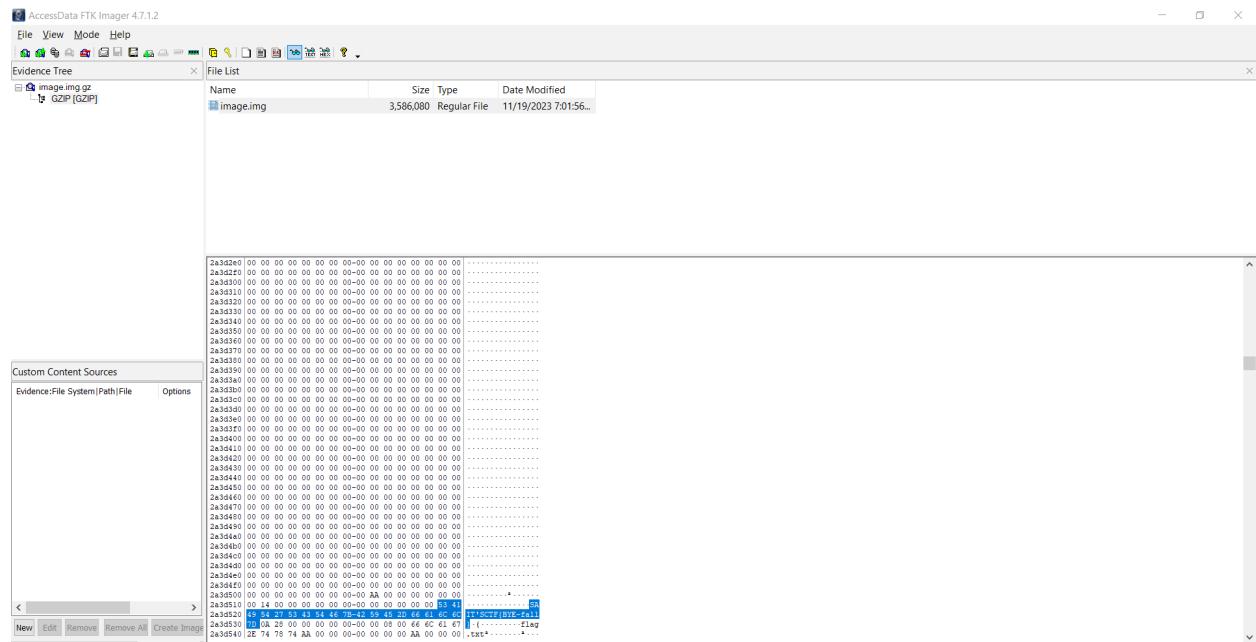
```

base64decode.org

The screenshot shows a web page titled "Decode from Base64 format". It contains a text input field with the value "U0FJVcdTQ1RGe3VjX2Nhbgdhcnl0". Below the input field are several configuration options: a dropdown menu set to "UTF-8" with the label "Source character set", a checkbox for "Decode each line separately", and a checkbox for "Live mode OFF" which is checked. A large green button labeled "< DECODE >" is prominently displayed. To the right of the button, the text "Decodes your data into the area below." is visible. At the top right of the page, there is a link "★ Bonus tip: Bookmark us!".

DIGITAL FORENSICS: Analyse the iso image to get the flag.

Download ftk imager:



OSINT:

```
(kali㉿kali)-[~/Music]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --columns --engines --stable
[!] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[*] starting @ 01:57:57 /2023-12-01

[01:57:57] [INFO] resuming back-end DBMS 'mysql'
[01:57:57] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)

+---+-----+
| Column | Type   |
+---+-----+
| COMMENT | varchar(80) |
| ENGINE  | varchar(64) |
| FK      | varchar(3)  |
| SAVEPOINTS | varchar(3) |
| SUPPORT | varchar(8) |
| TRANSACTIONS | varchar(3) |
+---+-----+

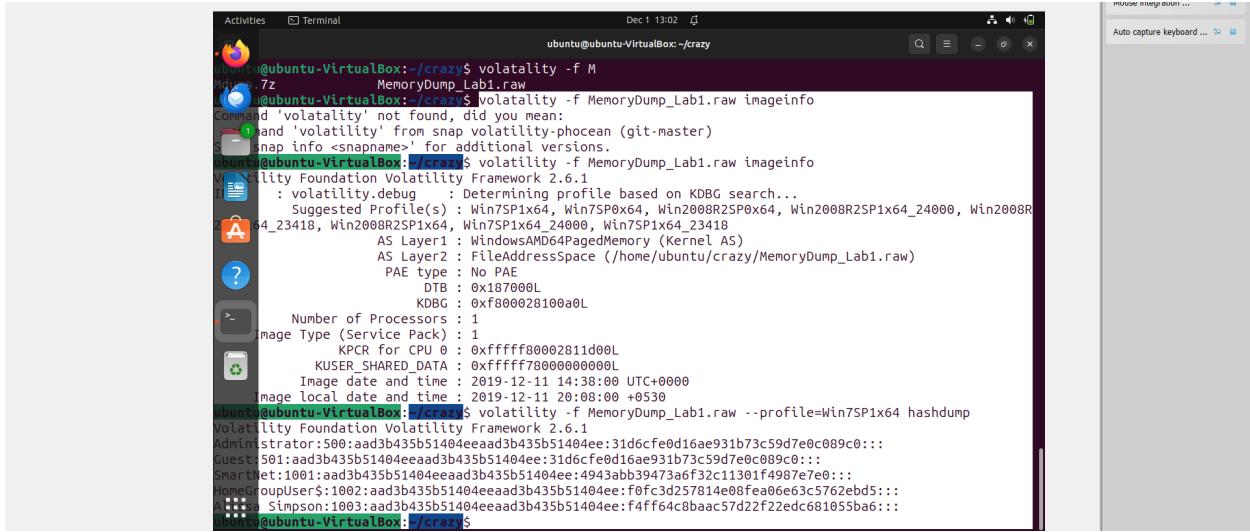
[01:57:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 01:57:57 /2023-12-01

└─$
```

DUMP THE PUMP:

QUESTION: Get the hash of the administrator by analyzing this memory dump.



The screenshot shows a terminal window on an Ubuntu system within a VirtualBox environment. The terminal session is as follows:

```
Activities Terminal Dec 1 13:02 ubuntu@ubuntu-VirtualBox: ~/crazy$ volatility -f M
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943ab39473aef32c11301f4987e7e0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c5762ebd5:::
Administrator:Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c0baac57d22f22edc681055ba6:::
ubuntu@ubuntu-VirtualBox: ~/crazy$
```

Question: Pull up the system ip by analyzing the disc image.

Title: "Cipher of the Lost Kingdom"

In a forgotten land, a mysterious cipher holds the key to ancient secrets. Adventurers decode the message "gsvhpbrhmlggsvornrgyfgbfinrmwrh" to uncover a hidden path in the enchanted forest. Each decoded clue leads them closer to the heart of the kingdom, where a final inscription reveals, "rgurfbzrjurer" – unlocking the cryptic message, "the secret is here." The adventurers become the guardians of the cipher, ensuring the magic of the kingdom endures for generations.

Hint: include your ans in SAIT'SCTF{}

Ans: SAIT'SCTF{ theskyisnotthelimitbutyourmindis}

SHARKTHEWIRE

Your hint was your password

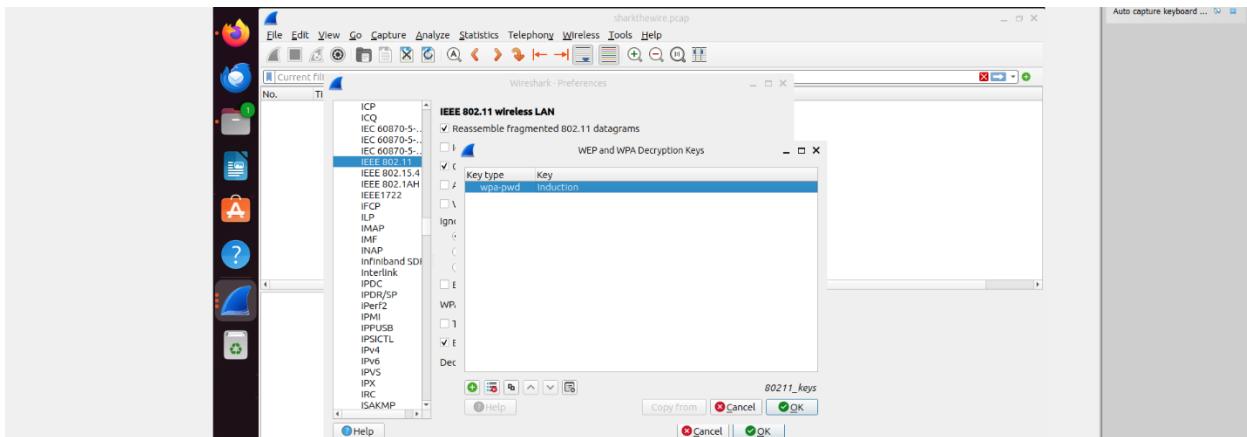
It was double encoded in base64

The image contains two side-by-side screenshots of a web-based Base64 decoder. Both screenshots show a form with a text input field and a 'DECODE' button.

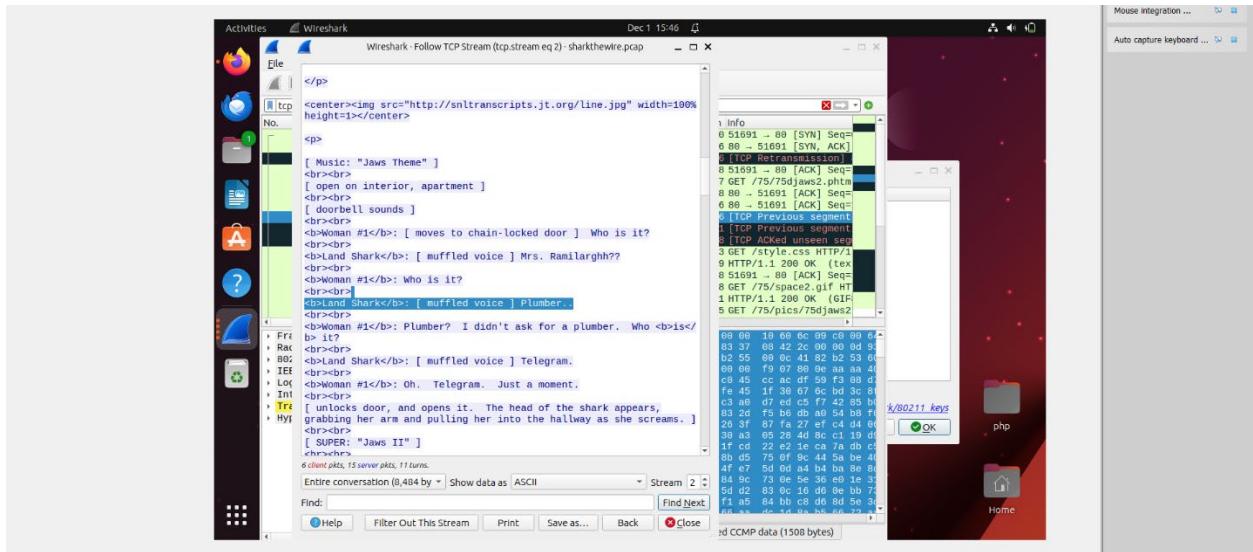
Top Screenshot:
Input: U1c1a2RXTjBhVz1
Output: SW5kdWN0aW9u

Bottom Screenshot:
Input: SW5kdWN0aW9u
Output: Induction

Adding the wpa password,



Search http, follow tcp. Stream eq 2



Its Plumber at her door.