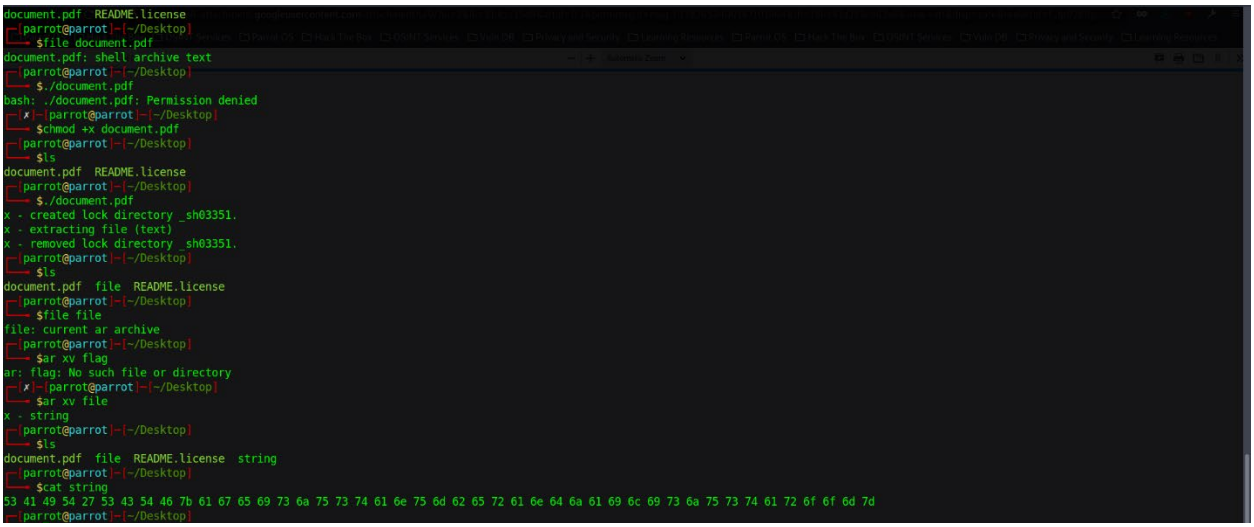
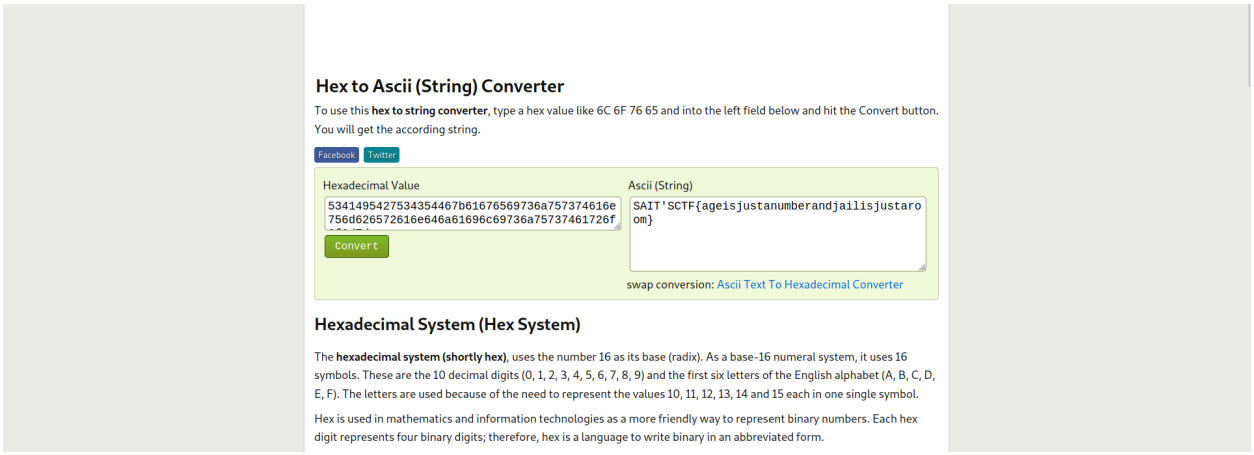
CTF ANSWERS

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}

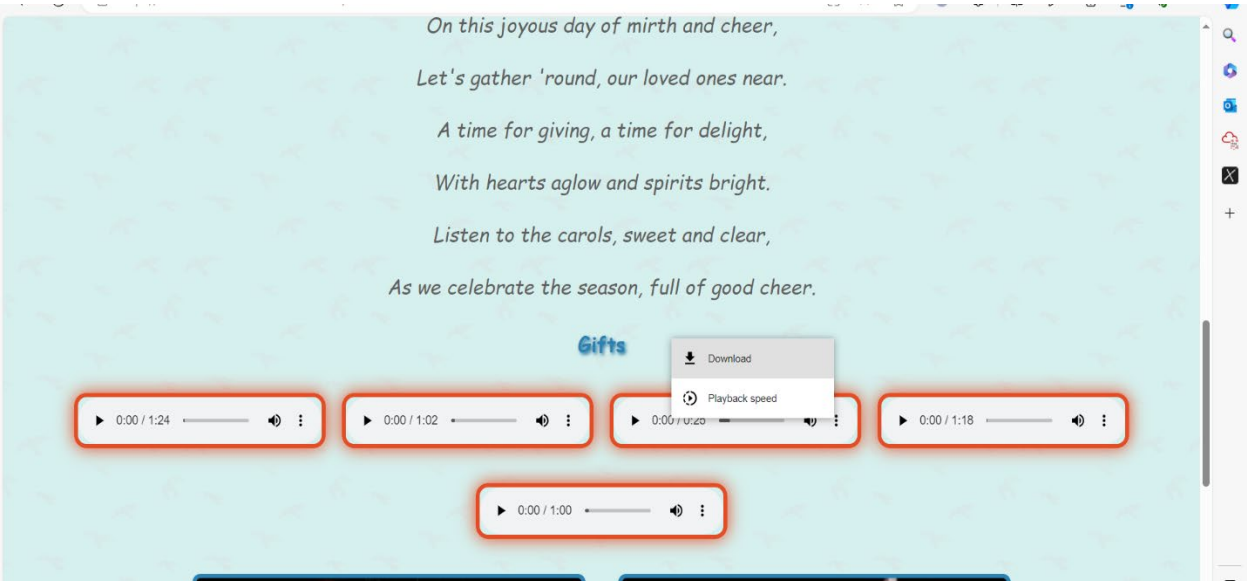




CHRISTMAS GIFT

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:




```
┌──(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.

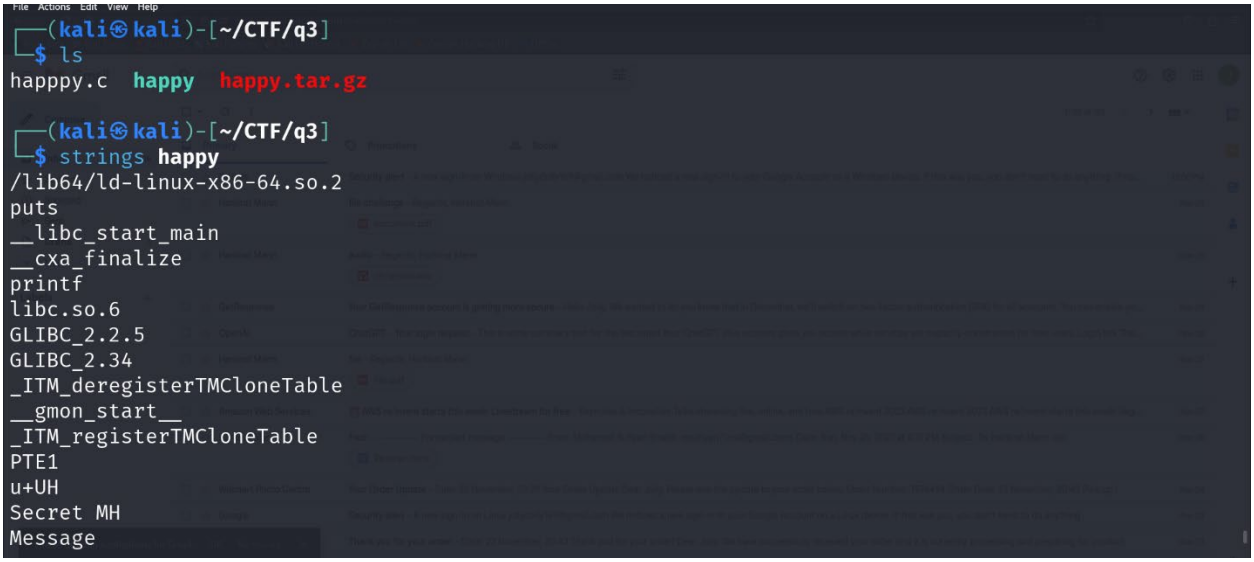
```
Silent whispers weave a cryptic tale,
A realm of secrets, elusive and frail.
In shadows cast by the moonlight's veil,
Trail the echoes, hear the flag's subtle wail.

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.
```

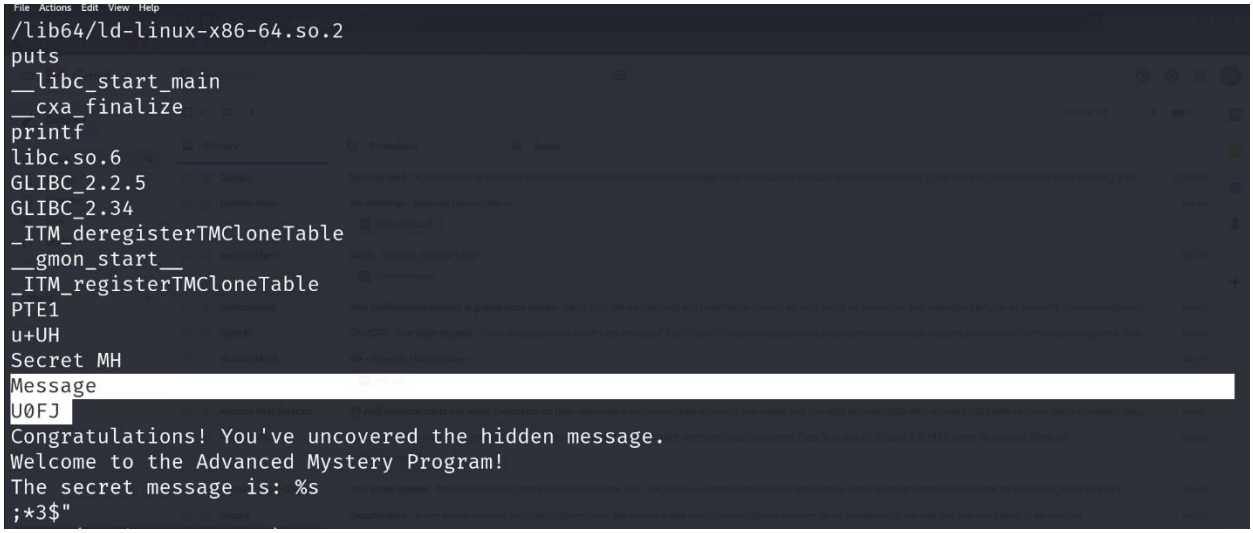
Flag: SAIT'SCTF{JOCKEASFJOCKSECTIAFA}

REVERSE QUESTIONS:

Question: Tie the knots together

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





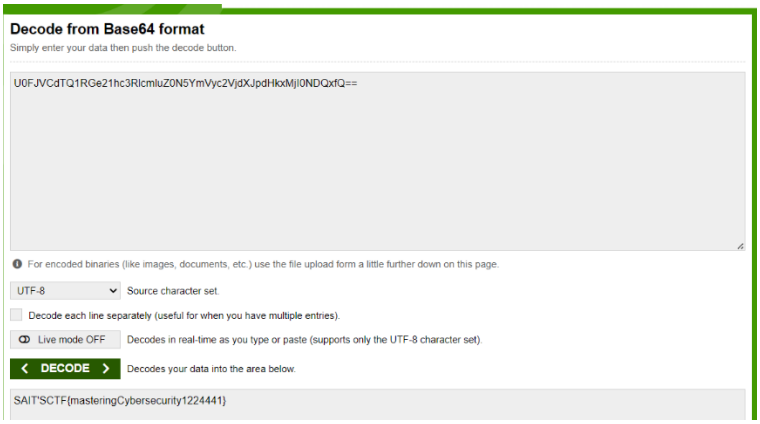
Picking up the piece: U0FJ

Analzying 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.#0122023-11-30T11:40:06.000104-05:00 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.#0122023-11-30T11:40:06.000104-05:00 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-
30T11:40:05.792823-05:00 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.#0122023-11-30T11:40:06.000104-05:00 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
2023-11-30T11:52:50.598975-05:00 kali dbus-daemon[1059]: [session uid=1000 pid=1059] Activating via systemd: service
name='org.freedesktop.thumbnails.Cache1' unit='tumblerd.service' requested by ':1.26' (uid=1000 pid=1285 comm="Thunar --sm-client-id 2d5c9873f-
2aad-4c39-8583-ccd")
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.freedesktop.thumbnails.Cache1'
2023-11-30T11:52:50.682745-05:00 kali systemd[1035]: Started tumblerd.service - Thumbnailing service.
```

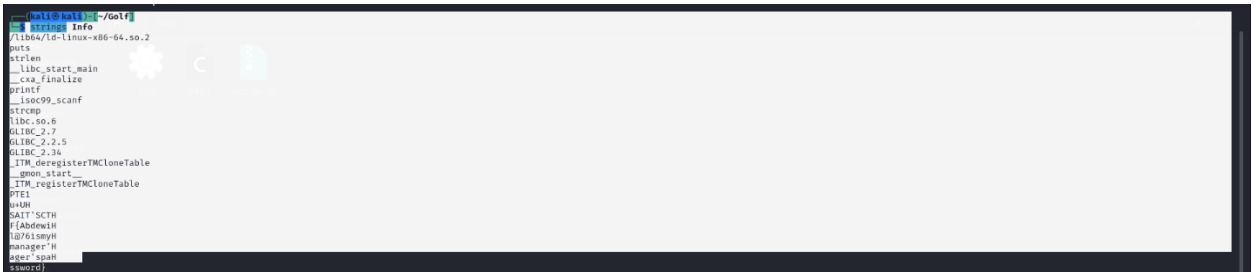
2nd piece: VCdTQ1RGe21hc3RlcmluZ0N5YmVyc2VjdXJpdHkxMjI0NDQxfQ==

Combining both : U0FJVCdTQ1RGe21hc3RlcmluZ0N5YmVyc2VjdXJpdHkxMjI0NDQxfQ==



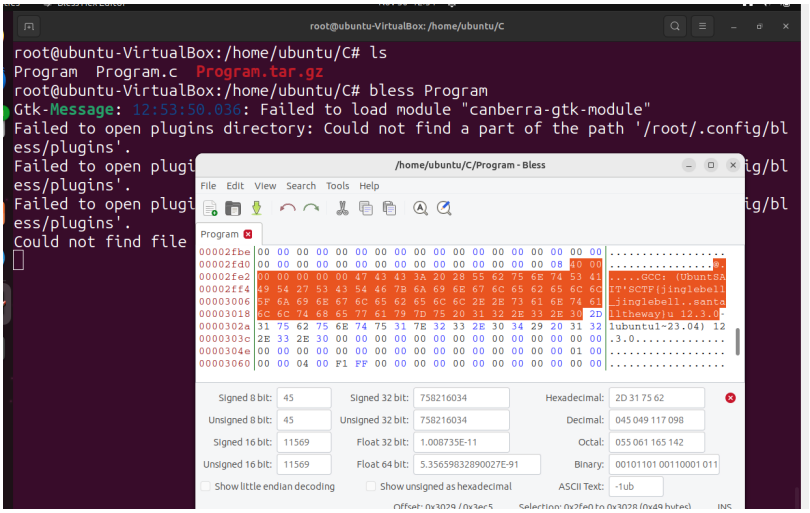
Question: Digital Mystery Unveiled: Crack the Code!

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!!



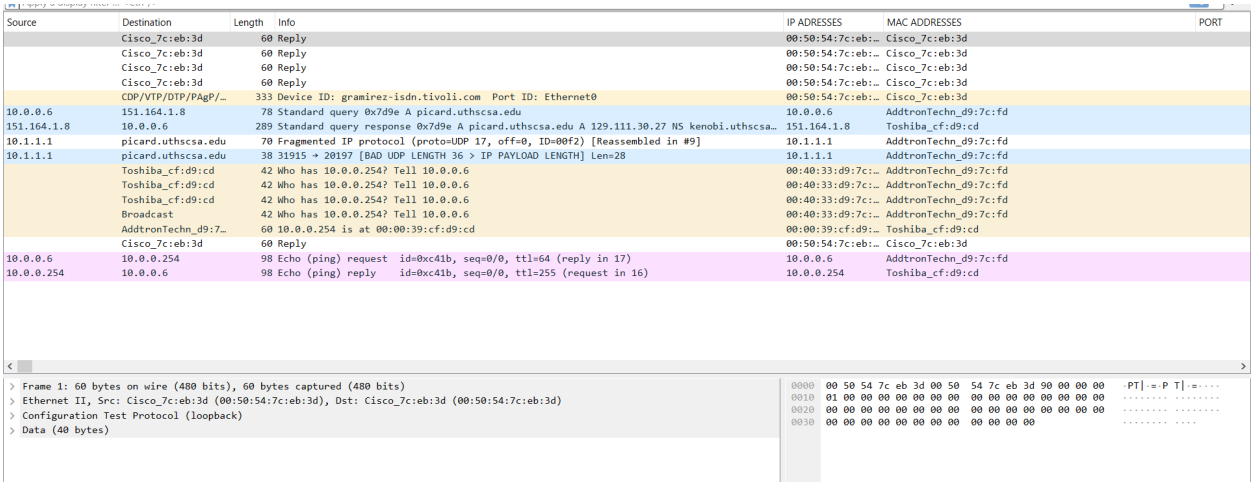
Question: Multiply the numbers

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



Networks

Question: Analyze the wireshark capture and name the attack.



Source	Destination	Length	Info	IP ADRESSES	MAC ADDRESSES	PORT
	Cisco_7c:eb:3d	60	Reply	00:50:54:7c:eb:…	Cisco_7c:eb:3d	
	Cisco_7c:eb:3d	60	Reply	00:50:54:7c:eb:…	Cisco_7c:eb:3d	
	Cisco_7c:eb:3d	60	Reply	00:50:54:7c:eb:…	Cisco_7c:eb:3d	
	Cisco_7c:eb:3d	60	Reply	00:50:54:7c:eb:…	Cisco_7c:eb:3d	
	CDP/VTP/DTP/PAgP/…	333	Device ID: gramirez-isdn.tivoli.com Port ID: Ethernet0	00:50:54:7c:eb:…	Cisco_7c:eb:3d	
10.0.0.6	151.164.1.8	78	Standard query 0x7d9e A picard.uthscsa.edu	10.0.0.6	AddtronTechn_d9:7c:fd	
151.164.1.8	10.0.0.6	289	Standard query response 0x7d9e A picard.uthscsa.edu A 129.111.30.27 NS kenobi.uthscsa…	151.164.1.8	Toshiba_cf:d9:cd	
10.1.1.1	picard.uthscsa.edu	70	Fragmented IP protocol (proto=UDP 17, off=0, ID=00f2) [Reassembled in #9]	10.1.1.1	AddtronTechn_d9:7c:fd	
10.1.1.1	picard.uthscsa.edu	38	31915 → 20197 [BAD UDP LENGTH 36 > IP PAYLOAD LENGTH] Len=28	10.1.1.1	AddtronTechn_d9:7c:fd	
	Toshiba_cf:d9:cd	42	Who has 10.0.0.254? Tell 10.0.0.6	00:40:33:d9:7c:…	AddtronTechn_d9:7c:fd	
	Toshiba_cf:d9:cd	42	Who has 10.0.0.254? Tell 10.0.0.6	00:40:33:d9:7c:…	AddtronTechn_d9:7c:fd	
	Toshiba_cf:d9:cd	42	Who has 10.0.0.254? Tell 10.0.0.6	00:40:33:d9:7c:…	AddtronTechn_d9:7c:fd	
	Broadcast	42	Who has 10.0.0.254? Tell 10.0.0.6	00:40:33:d9:7c:…	AddtronTechn_d9:7c:fd	
	AddtronTechn_d9:7…	60	10.0.0.254 is at 00:00:39:cf:d9:cd	00:00:39:cf:d9:…	Toshiba_cf:d9:cd	
	Cisco_7c:eb:3d	60	Reply	00:50:54:7c:eb:…	Cisco_7c:eb:3d	
10.0.0.6	10.0.0.254	98	Echo (ping) request id=0xc41b, seq=0/0, ttl=64 (reply in 17)	10.0.0.6	AddtronTechn_d9:7c:fd	
10.0.0.254	10.0.0.6	98	Echo (ping) reply id=0xc41b, seq=0/0, ttl=255 (request in 16)	10.0.0.254	Toshiba_cf:d9:cd	

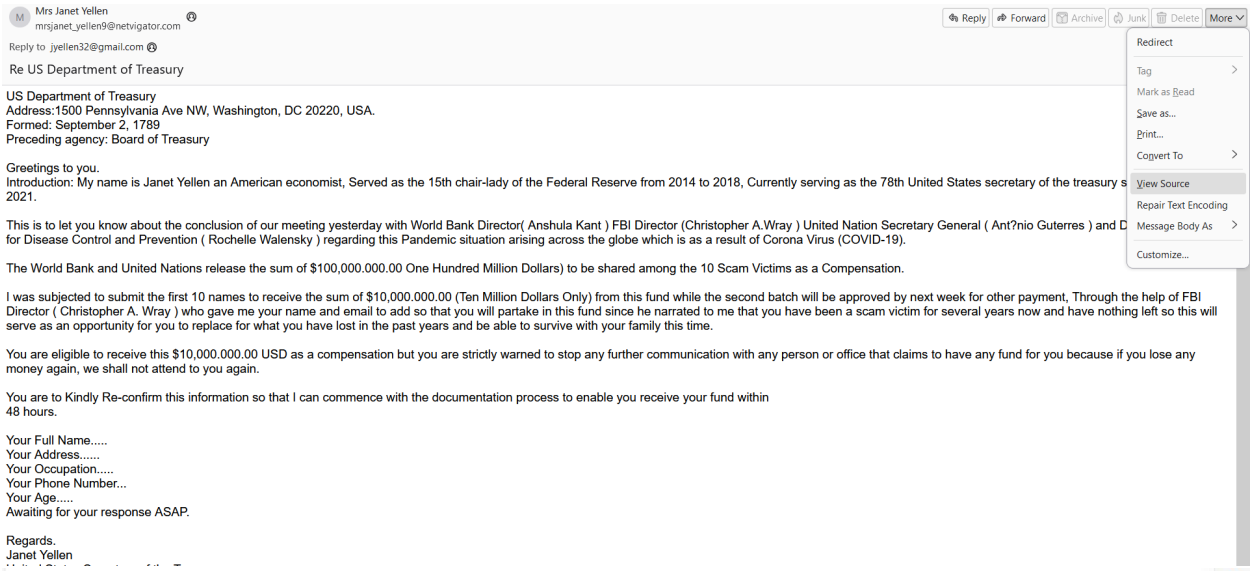
```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Cisco_7c:eb:3d (00:50:54:7c:eb:3d), Dst: Cisco_7c:eb:3d (00:50:54:7c:eb:3d)
> Configuration Test Protocol (loopback)
> Data (40 bytes)
```

```
0000  00 50 54 7c eb 3d 00 50  54 7c eb 3d 90 00 00 00   ·PT|·=·P T|·=····
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0030  00 00 00 00 00 00 00 00  00 00 00 00               ···· ····
```

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 to jyellen32@gmail.com

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 s
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 (Ant?nio Guterres) and D
for Disease Control and Prevention (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.

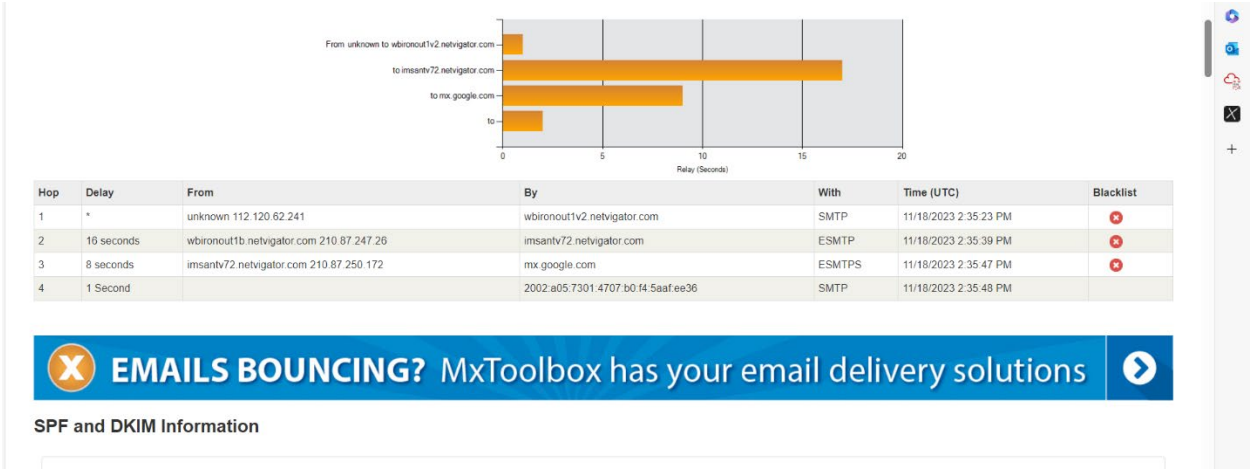
You are to Kindly Re-confirm this information so that I can commence with the documentation process to enable you receive your fund within
48 hours.

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

Regards.
Janet Yellen

Reply | Forward | Archive | Junk | Delete | More

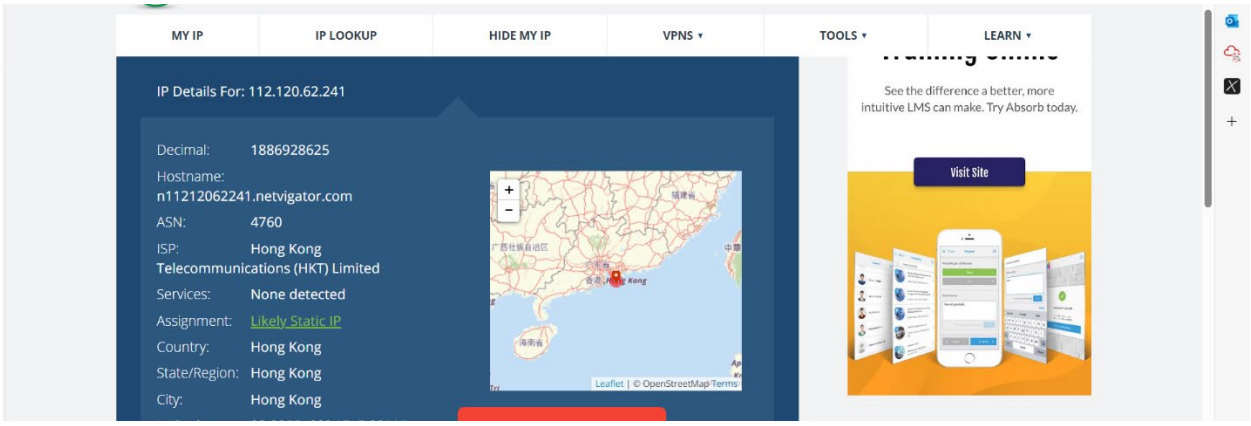
Redirect
Tag
Mark as Read
Save as...
Print...
Convert To
View Source
Repair Text Encoding
Message Body As
Customize...



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknown 112.120.62.241	wbironout1v2.netvigator.com	SMTP	11/18/2023 2:35:23 PM	
2	16 seconds	wbironout1b.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:f4:5aaf:ee36	SMTP	11/18/2023 2:35:48 PM	

SPF and DKIM Information

The ip of the sender is 112.120.62.241



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?"

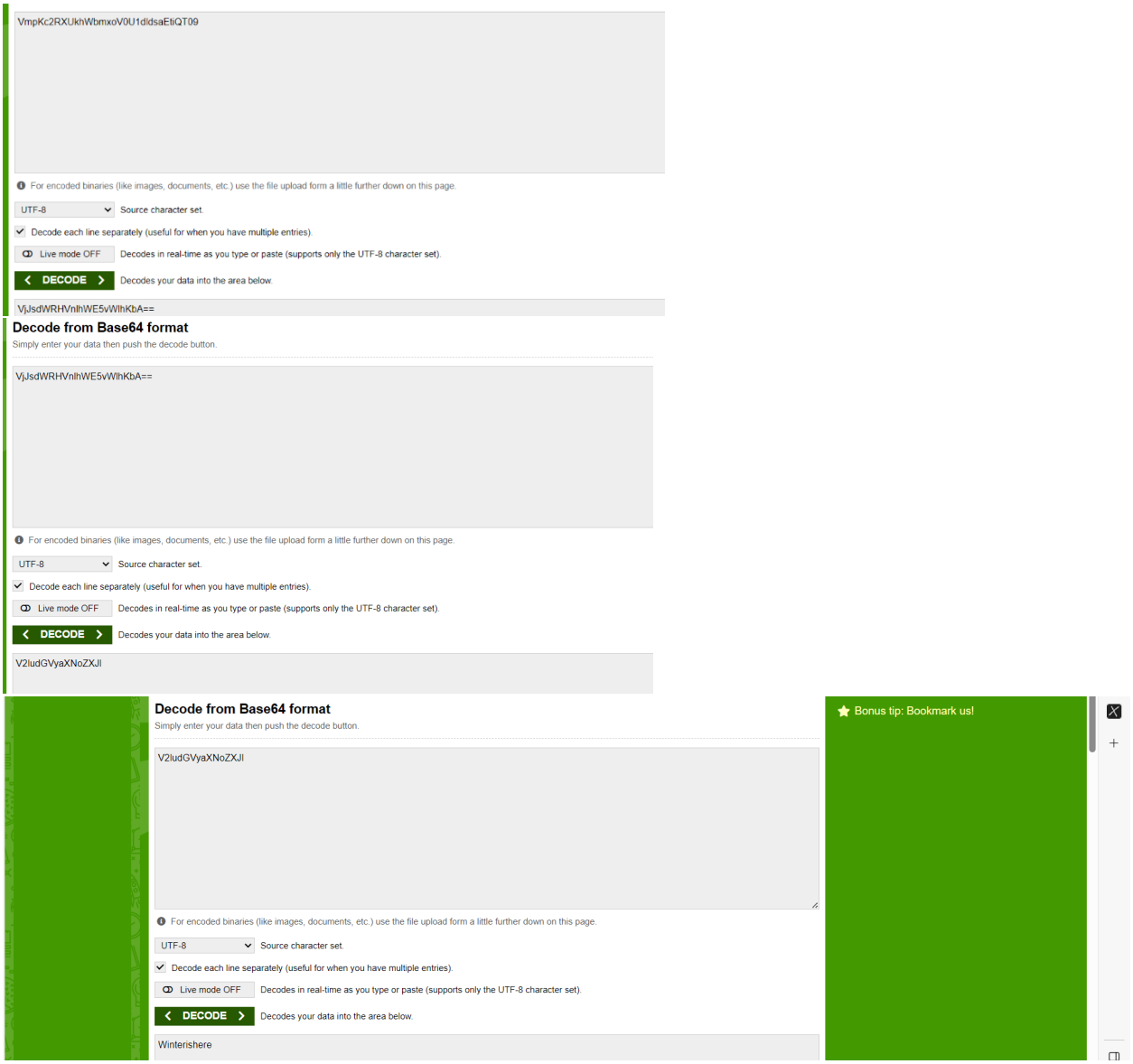
Table name is : foo

Question: Cryptic Pursuit

Veteran operative, you're in the crosshairs of "The Enigma Collective." They've concealed a vital message within the shadows of " VmpKc2RXUkhWbmxoV0U1dldsaEtiQT09" 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

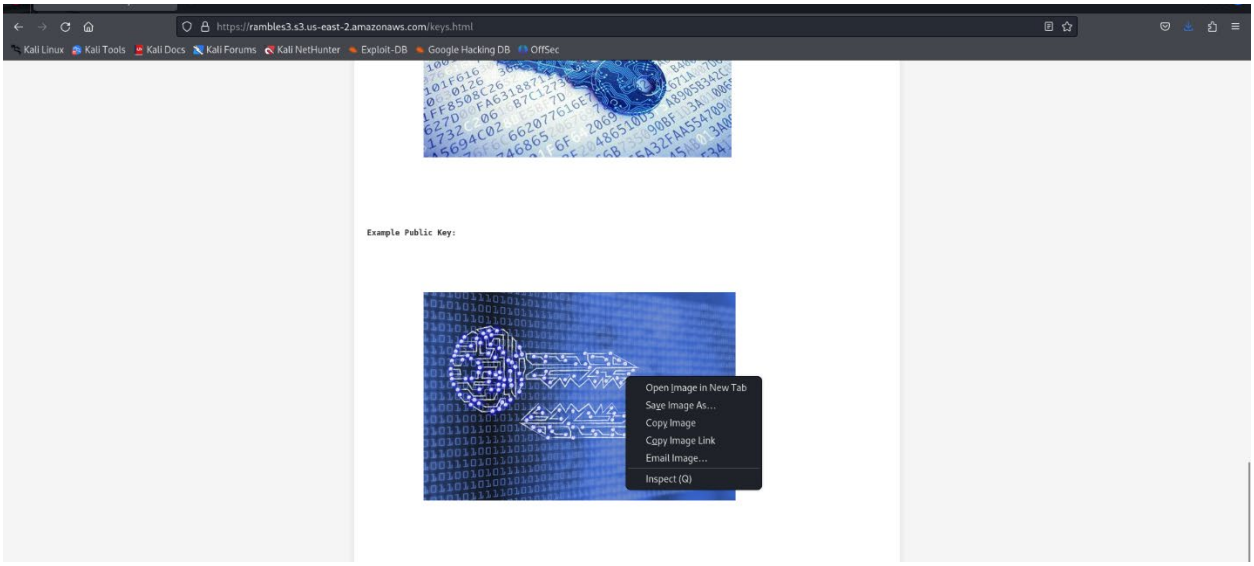


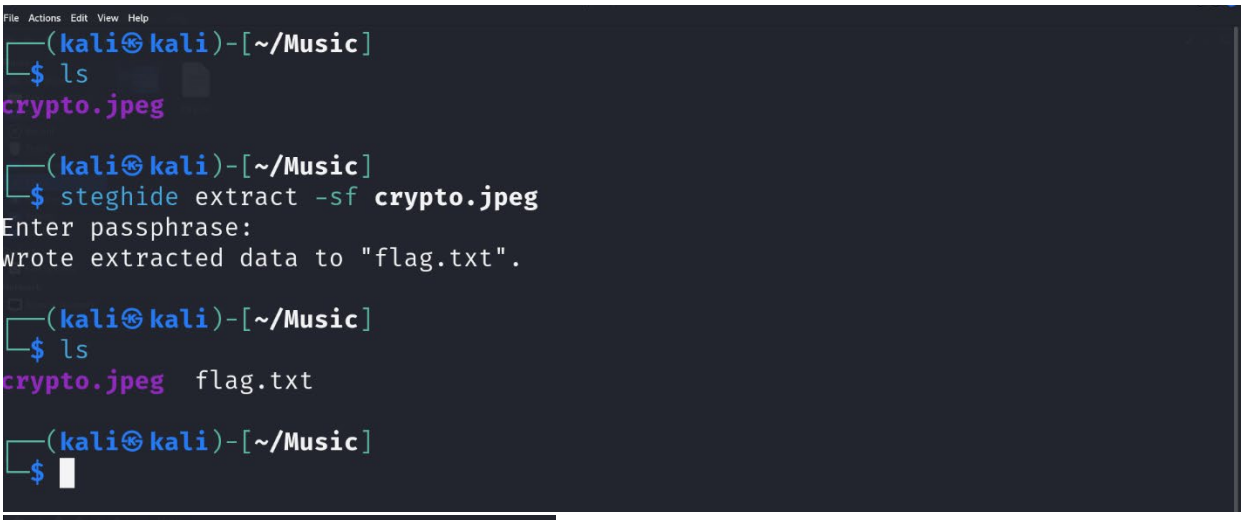
Question: Solve the mystery

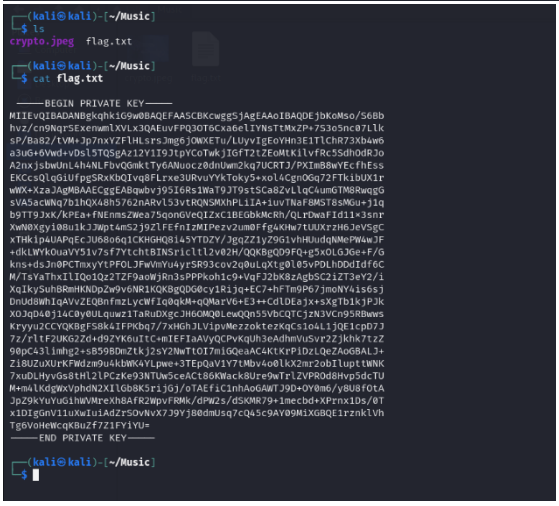
https://rambles3.s3.us-east-2.amazonaws.com/crypto.html has your private key.

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

Flag: SAIT'SCTF{You_found_it}

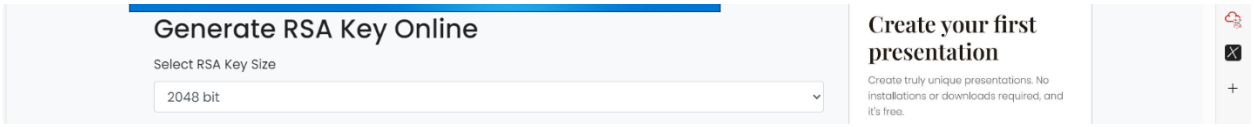


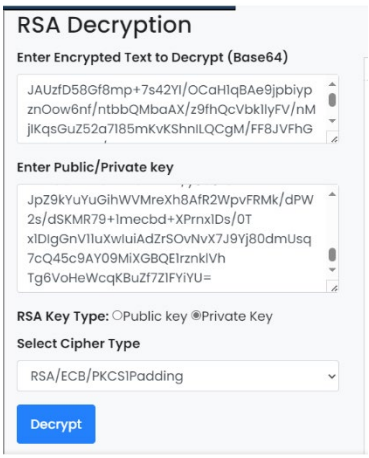


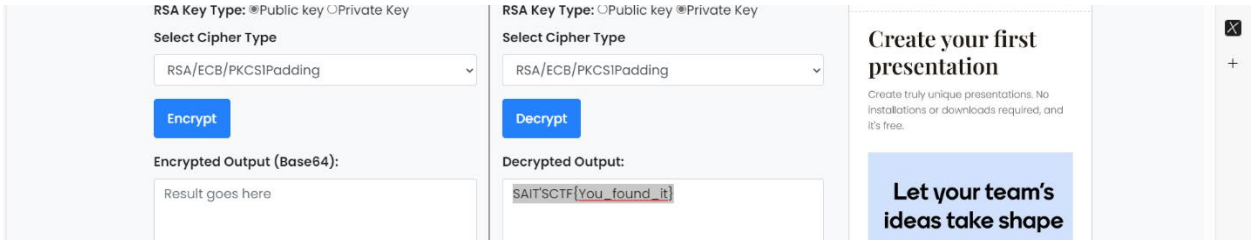


[RSA Encryption, Decryption And Key Generator Online | Devglan]

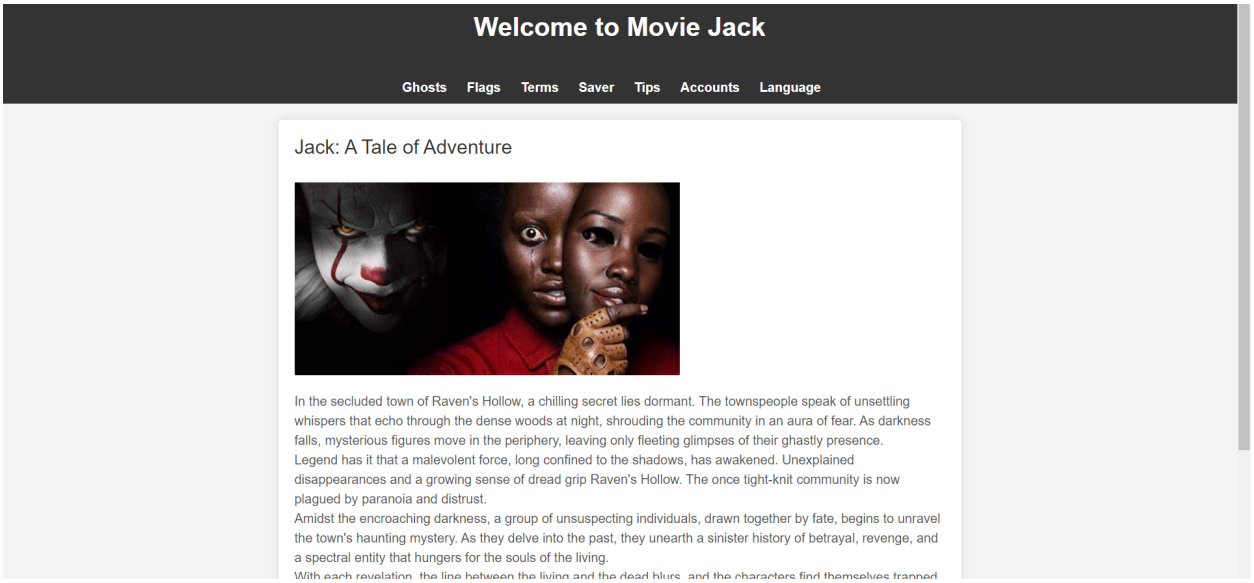
Algorithm is: RSA



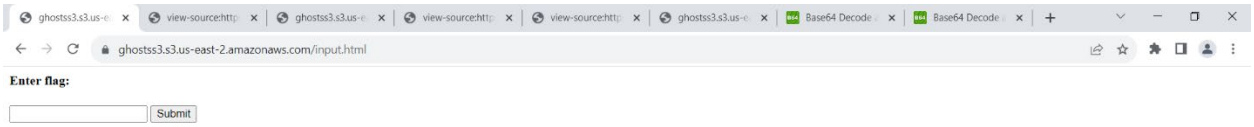

RSA Decryption
Enter Encrypted Text to Decrypt (Base64)
JAUzfD58Gf8mp+7s42YI/OCaH1qBAe9jpbiyp
znOow6nf/ntbbQMbaAX/z9fhQcVbkIlyFV/nM
jlKqsGuZ52a7l85mKvKShnlLQCgM/FF8JVFhG
Enter Public/Private key
JpZ9kYuYuGihWVMreXh8AfR2WpvFRMk/dPW
2s/dSKMR79+lmecbd+XPrnxIDs/0T
xlDlgGnV11uXwIuiAdZrSOvNvX7J9Yj80dmUsq
7cQ45c9AY09MiXGBQElrznklVh
Tg6VoHeWcqKBuZf7ZlFYiYU=
RSA Key Type: ○Public key ◉Private Key
Select Cipher Type
RSA/ECB/PKCS1Padding
Decrypt


RSA Key Type: ◉Public key ○Private Key
Select Cipher Type
RSA/ECB/PKCS1Padding
Encrypt
Encrypted Output (Base64):
Result goes here
RSA Key Type: ○Public key ◉Private Key
Select Cipher Type
RSA/ECB/PKCS1Padding
Decrypt
Decrypted Output:
SAIT'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

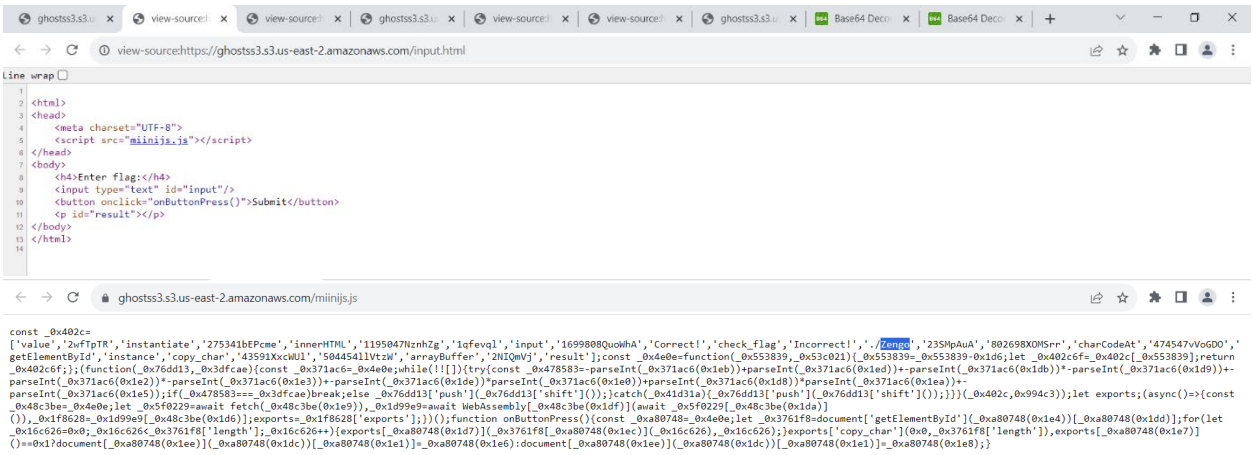
WEBSERVER: Main page



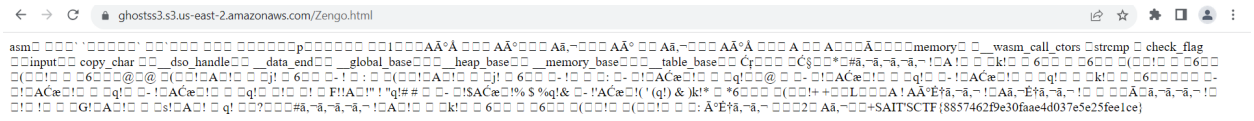
Going into the input.html page > hit ctrl+U



Go to miinijs.js

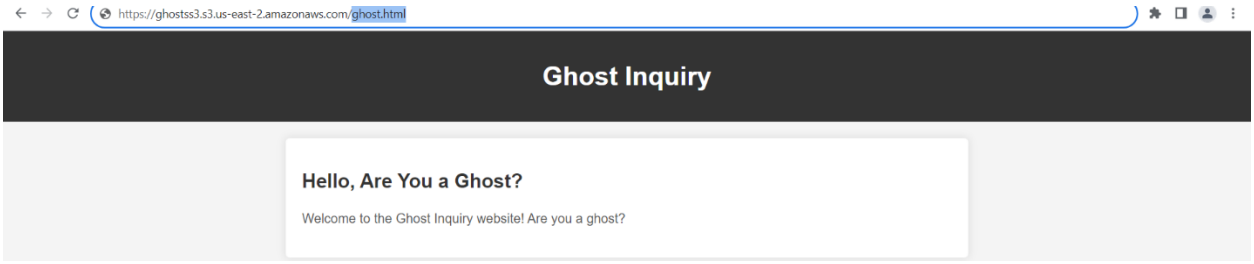


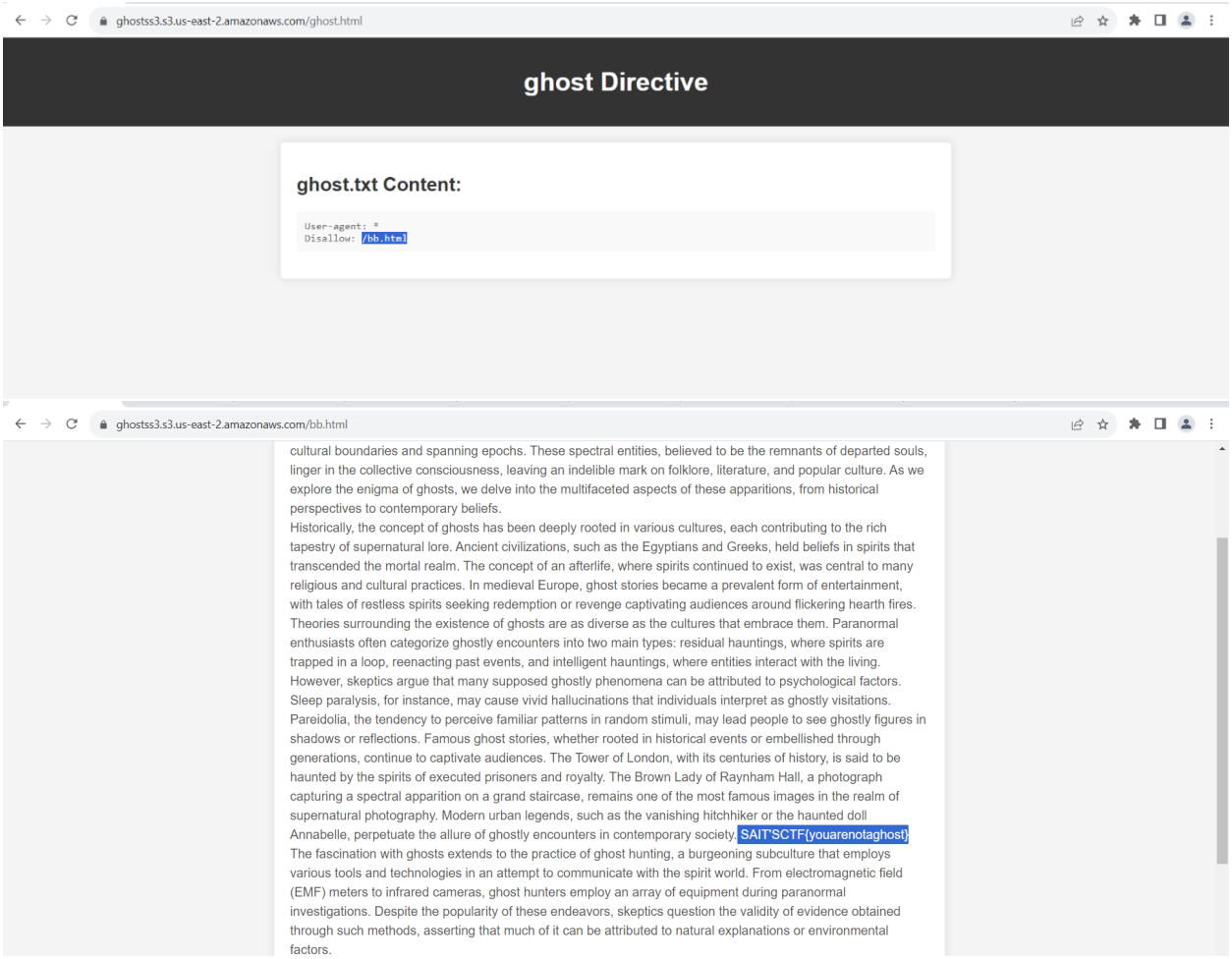
Zengo is the lead, try Zengo.html , Zengo.txt and see what we get:



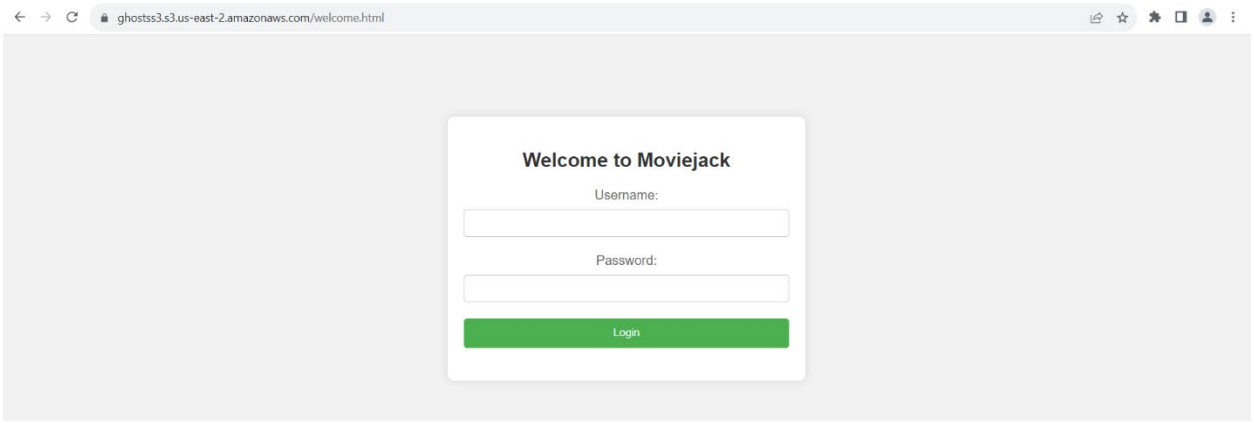
FLAG 2:

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





Flag 3: Welcome to moviejack page



Hit ctrl + u

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Movie CTF Login</title>
    <script src="index.js"></script>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f2f2f2;
            text-align: center;
            margin: 100px;
        }

        .login-container {
            max-width: 400px;
            margin: auto;
            background-color: #fff;
            padding: 20px;
            border-radius: 8px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
        }

        .login-container h2 {
            color: #333;
        }

        .form-group {
            margin-bottom: 20px;
        }

        .form-group label {
            display: block;
            margin-bottom: 8px;
            color: #666;
        }

        .form-group input {
```

Ahmmm...index.js

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

```javascript
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('U0FJVCdTQ1RGe3VjX2NhbGdhcnl9').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 === 'U0FJVCdTQ1RGe0lfYW1fbm90eW91cmZsYWd9') {
            alert('Login successful!');
        } else {
            alert('Invalid username or password');
        }
    });
```

base64decode.org

Decode from Base64 format

Simply enter your data then push the decode button.

U0FJVCdTQ1RGe3VjX2NhbGdhcnl9

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).

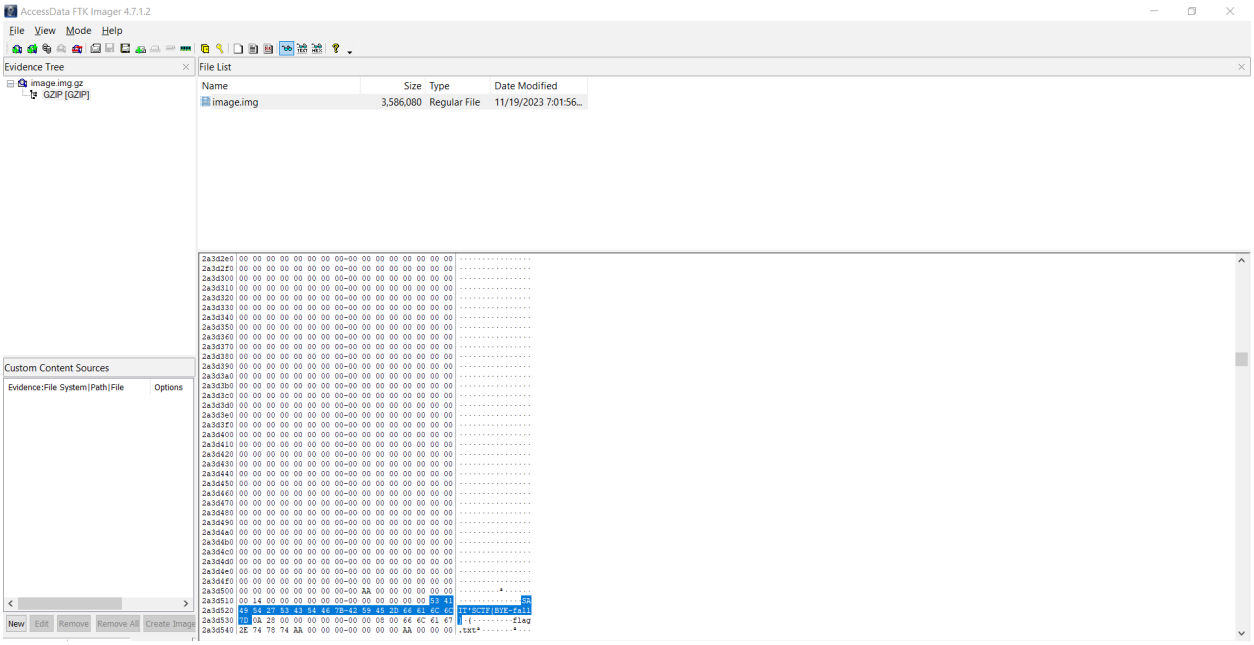
DECODE Decodes your data into the area below.

SAIT'SCTF{uc_calgary}

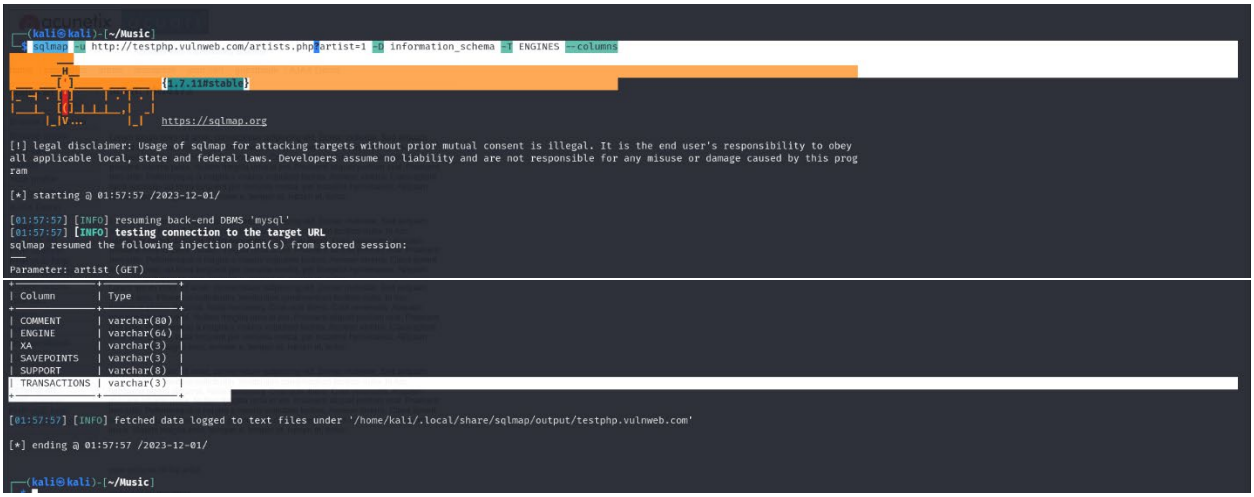
Bonus tip: Bookmark us!

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

Download ftk imager:

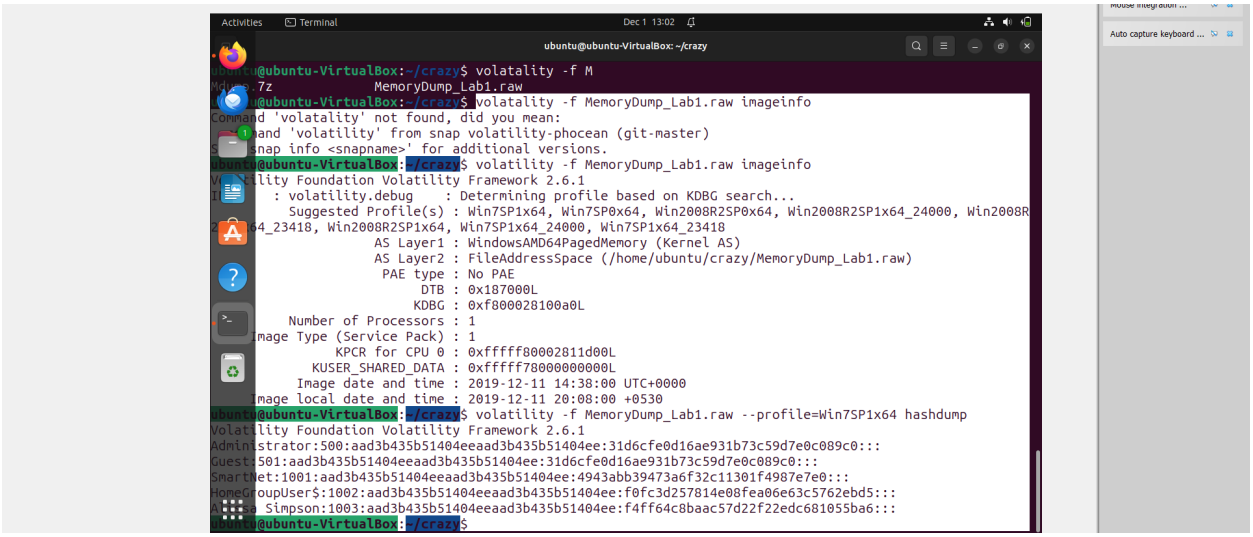


OSINT:

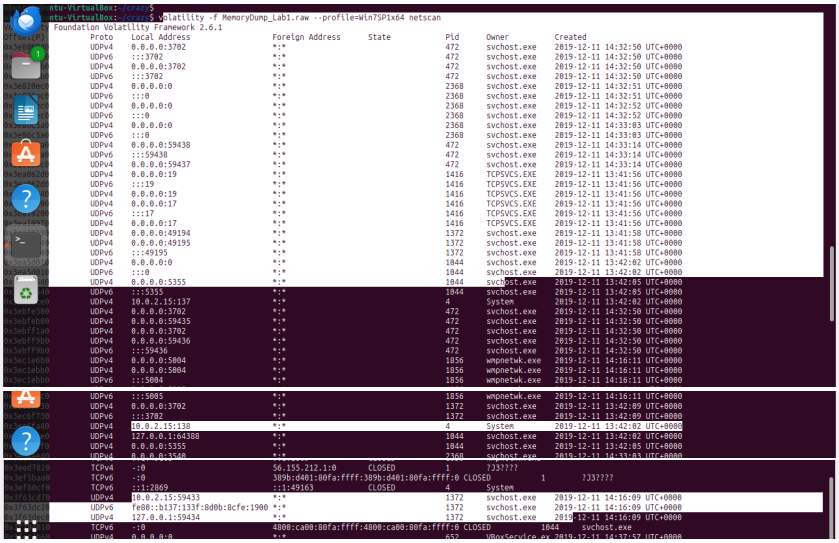

(kali㉿kali)-[~/Music]
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D information_schema -T ENGINES --columns
{1.7.11#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey
all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this prog
ram
[*] 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)
XA	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/
(kali㉿kali)-[~/Music]

DUMP THE PUMP:

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



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 "gsvhpbrhmlggsvornrgyfgblfinrmwrh" 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.

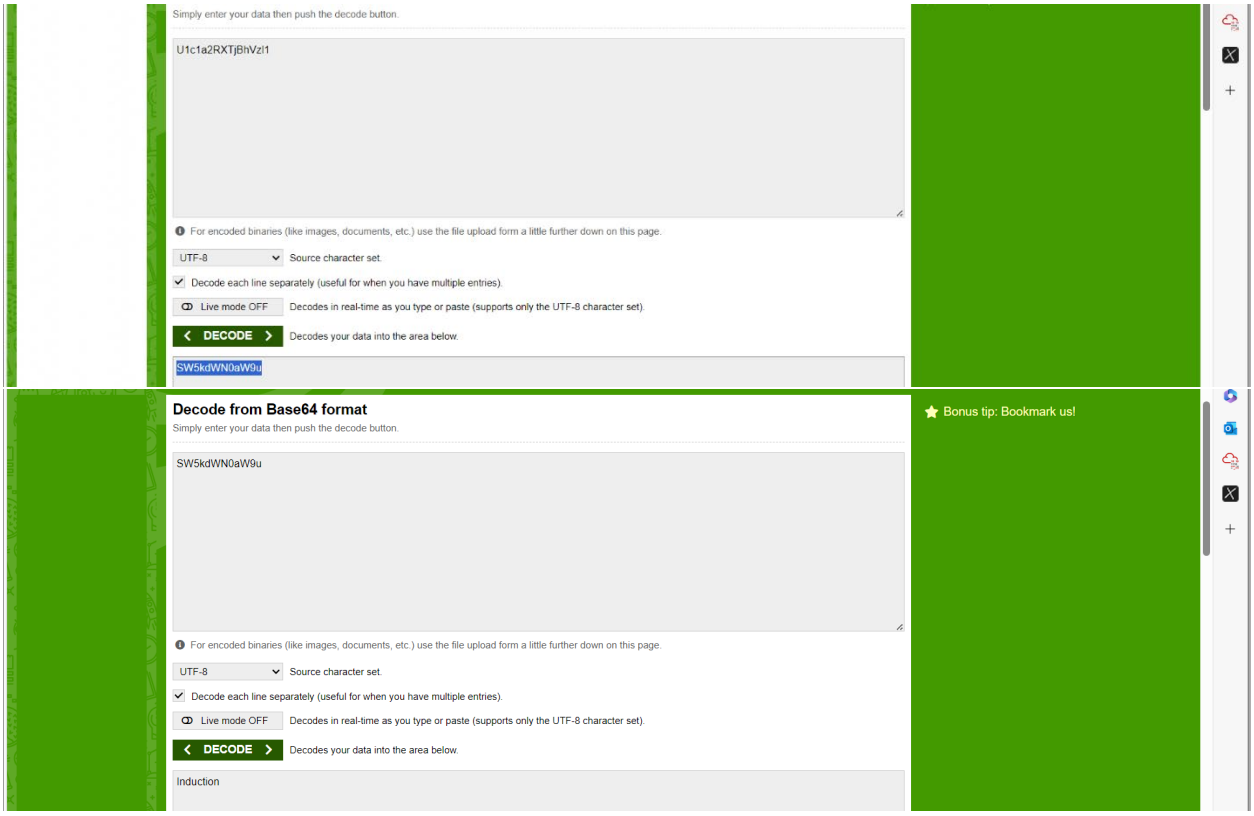
Hint: include your ans in SAIT'SCTF{}

Ans: SAIT'SCTF{ theskyisnotthelimitbutyourmindis}

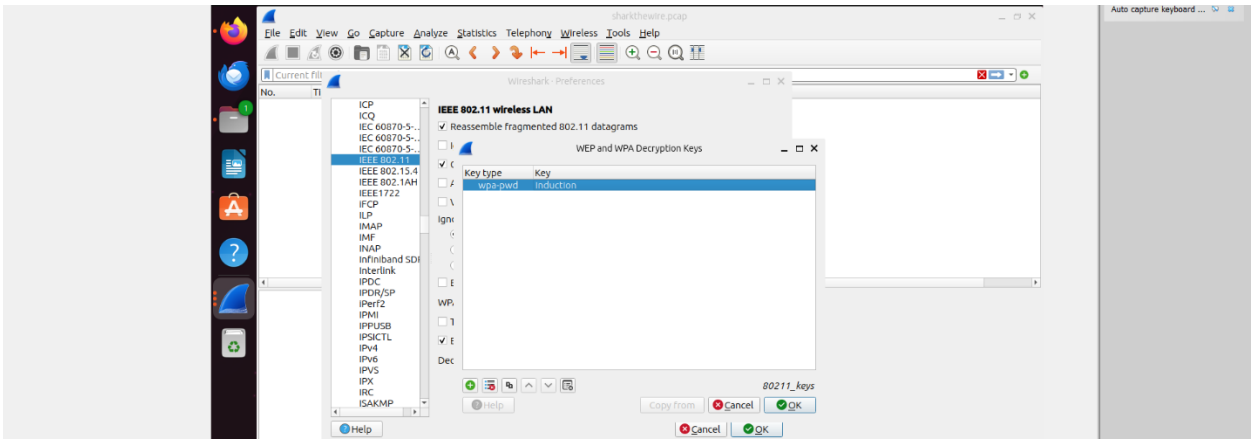
SHARKTHEWIRE

Your hint was your password

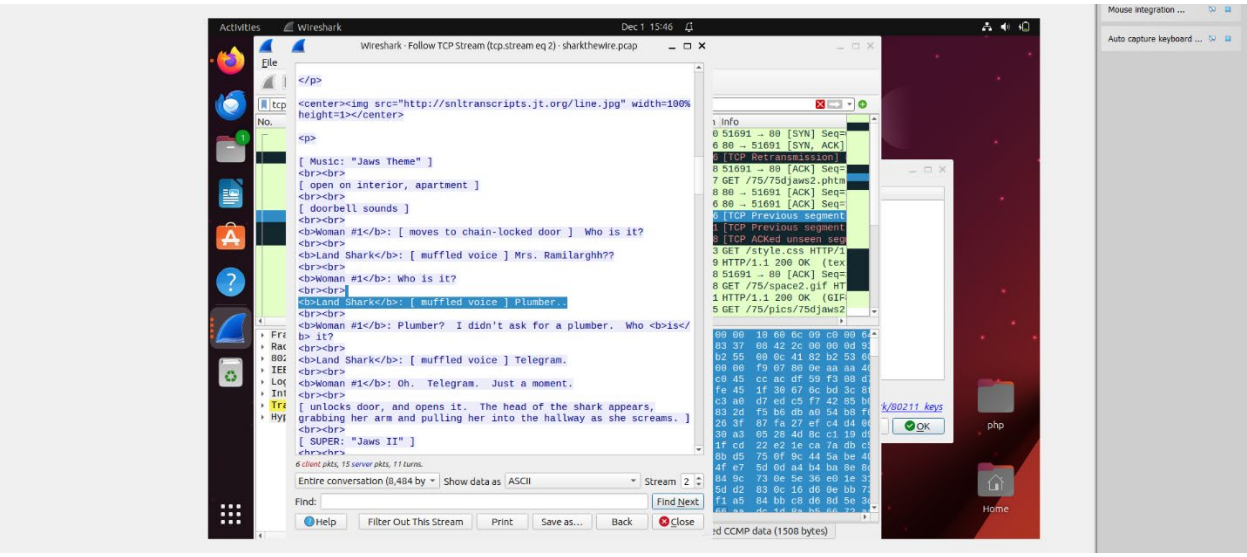
It was double encoded in base64



Adding the wpa password,



Search http, follow tcp. Stream eq 2



Its Plumber at her door.