SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

YEAR 3 – SEMESTER 2

IE3092 – INFORMATION SECURITY PROJECT

FINAL REPORT

# ACCIO FLAGS

## CTF WALKTHROUGH

### TEAM MEMBERS

IT18120462 – ABISHEKA P. A. C.

IT18152456 – KARUNATHILAKE K. K. H.

# ACCIO FLAGS – CTF WALKTHROUGH

## CONTENTS

## SCENARIO AND THEME

This CTF box is based on J.K Rowling’s Harry Potter Universe. Harry Potter is a series of fantasy novels written by the British author, J. K. Rowling. The novels chronicle the lives of a young wizard, Harry Potter, and his friends Hermione Granger and Ron Weasley, all of whom are students at Hogwarts School of Witchcraft and Wizardry. The series was later made into 8 movies which are popular all around the world.

This CTF is called “Accio Flags!” and the word “Accio” means “I summon” in Latin. So the meaning of this CTF name is “I summon Flags”.

Harry Potter along with his friends Ron and Hermione go through various challenges in order to defeat the dark wizard Lord Voldemort. To defeat him, Harry has to discover and destroy 7 Horcruxes. A Horcrux is an object formed by dark magic that is used by a wizard or witch to achieve immortality by splitting their soul into separate pieces.

This CTF was created based on the 7 Horcruxes. The player’s mission is to collect all 7 Horcruxes in order to defeat Lord Voldemort.

## CTF STRUCTURE

There are 7 categories namely:

- Horcrux 1 – The Diary
- Horcrux 2 – The Ring
- Horcrux 3 – The Cup
- Horcrux 4 – The Locket
- Horcrux 5 – The Diadem
- Horcrux 6 – The Diadem
- Horcrux 7 – The Snake

Each Horcrux has two levels dedicated to them. In the first level, the player has to discover the Horcrux and in the next level, the player has to destroy it, both by finding flags in each level. There is an additional level, Level 15, where the player will finally defeat Lord Voldemort by combining several findings from the previous 14 levels.

The first 14 levels are created under 7 categories as follows:

| Horcrux 1 The Diary | Horcrux 2 The Ring | Horcrux 3 The Cup | Horcrux 4 The Locket | Horcrux 5 The Diadem | Horcrux 6 Harry Potter | Horcrux 7 The Snake |
|---|---|---|---|---|---|---|
| The Diary - Discover | The Ring - Discover | The Cup - Discover | The Locket - Discover | The Diadem - Discover | Harry Potter - Discover | The Snake - Discover |
| The Diary - Destroy | The Ring - Destroy | The Cup - Destroy | The Locket - Destroy | The Diadem - Destroy | Harry Potter - Destroy | The Snake - Destroy |

## CONFIGURATIONS

- Operating System – Ubuntu Server 20.04 in which the .ova file is compatible with Oracle VM VirtualBox

- Server – Apache Server

- IDE – Notepad++ / Visual Studio Code / Sublime Text

- The CTF box will require the following specifications:

  1. 1 Core CPU

  2. 1024 MB RAM

- The VM will be set to a bridged network adapter by default.

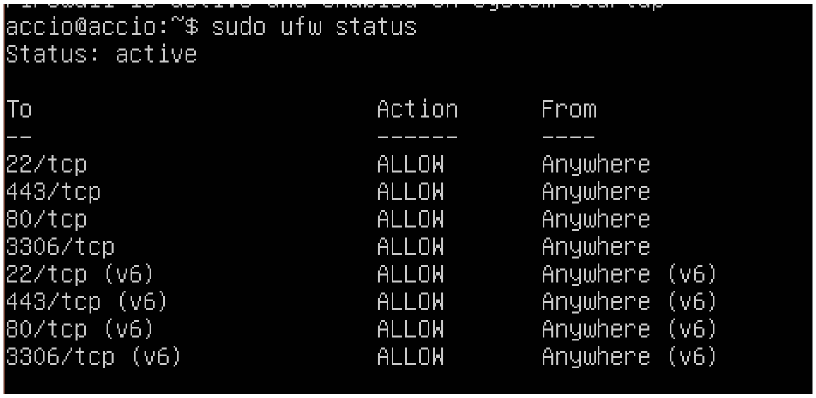
- The VM will acquire IP by default.

- The virtual machine has 2 users, “accio” is a superuser and there is an account called “accioplayer” for CTF players to log in. “accioplayer” is restricted from accessing the website files located in /var/www/html/accioflags.com.

- Steps to set accio as the owner:

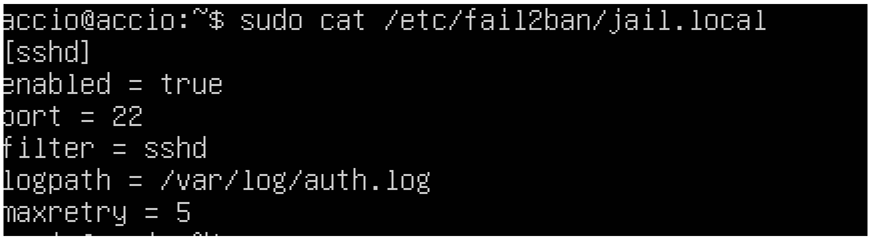
```
chown -R accio /var/www/http/accioflags.com/
chgrp -R www-data /var/www/http/accioflags.com/
chmod -R 750 /var/www/http/accioflags.com/
chmod g+s /var/www/http/accioflags.com/
```

- “ufw” was used to setup the firewall. Only ports 22-ssh, 443-https, 80-http and 3306-sql are allowed.



```
Firewall is active and enabled on system startup
accio@accio:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
3306/tcp                   ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
3306/tcp (v6)              ALLOW       Anywhere (v6)
```

- Intrusion prevention was implemented using fail2ban.



```
accio@accio:~$ sudo cat /etc/fail2ban/jail.local
[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
```

- Both URL navigation and backward navigation has been disabled via session management. If the player tries to perform one of the afore mentioned actions, they will be redirected to the homepage and therefore will have to restart the CTF.

## GETTING STARTED…

### STEP 1 - Import .ova to Oracle Virtualbox

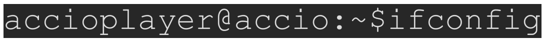
1. Open Oracle VirtualBox.
2. Go to “File” → “Import Appliance”.
3. Browse to the .ova file location and select it.
4. Select settings as follows:
   - Name – Preferred name for the VM
   - CPU – 1
   - RAM – 1024 MB
5. Wait for the VM to import.
6. Start VM.

### STEP 2 - Log In

USERNAME - accioplayer

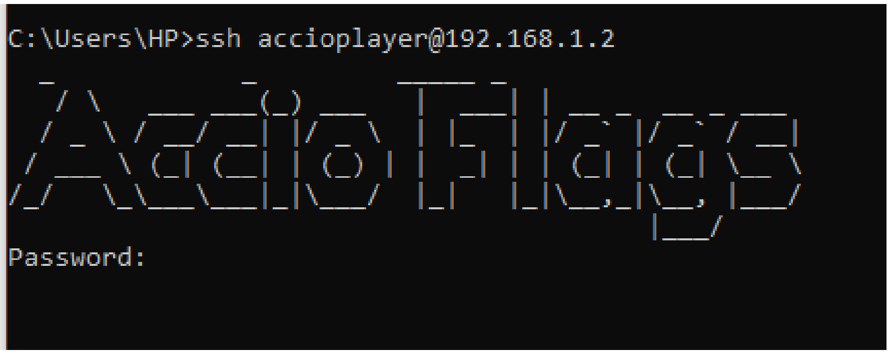
PASSWORD - accio@player

### STEP 3 - Find the IP address of the VM



```
accioplayer@accio:~$ifconfig
```

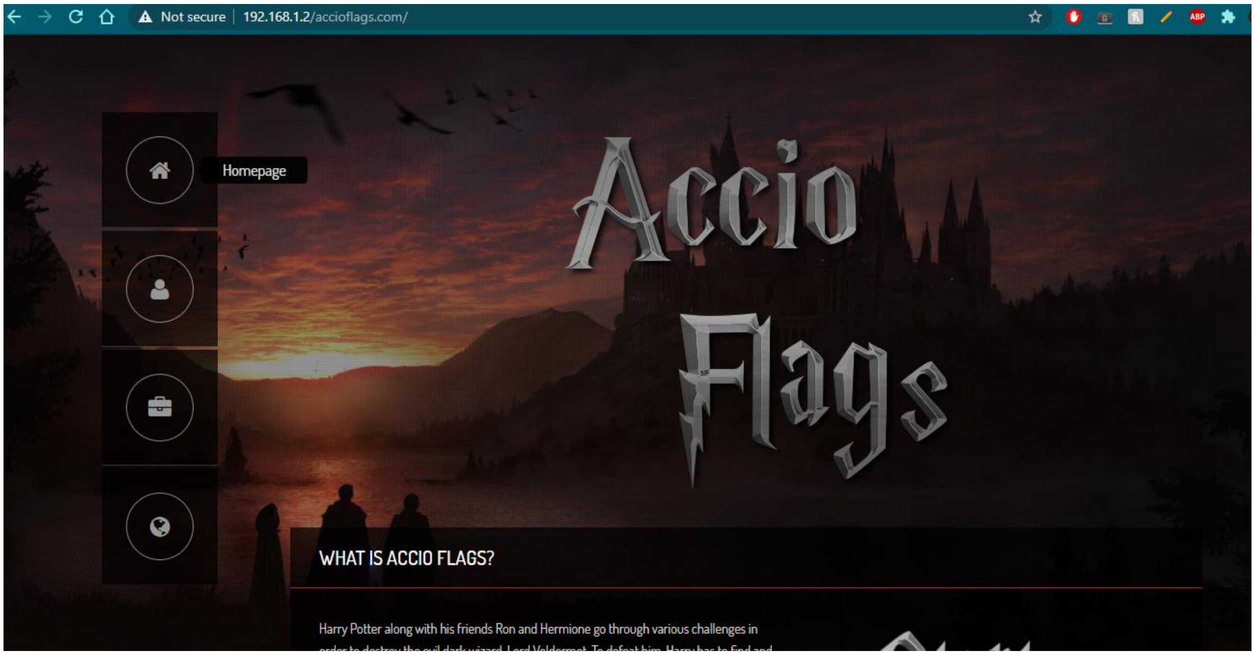
**STEP 4 - Connect to the VM through ssh by using PuTTY, Command Prompt or Powershell**



```
C:\Users\HP>ssh accioplayer@192.168.1.2
    _              _         _____ _
   / \   ___ ___ (_) ___   |  ___| | __ _  __ _ ___
  / _ \ / __/ __|| |/ _ \  | |_  | |/ _` |/ _` / __|
 / ___ \ (_| (__ | | (_) | |  _| | | (_| | (_| \__ \
/_/   \_\___\___||_|\___/  |_|   |_|\__,_|\__, |___/
                                          |___/
Password:
```

**STEP 5 - Navigate to the accioflags Website by using a Web Browser**

URL - <vm-ip-address>/accioflags.com



Not secure | 192.168.1.2/accioflags.com/

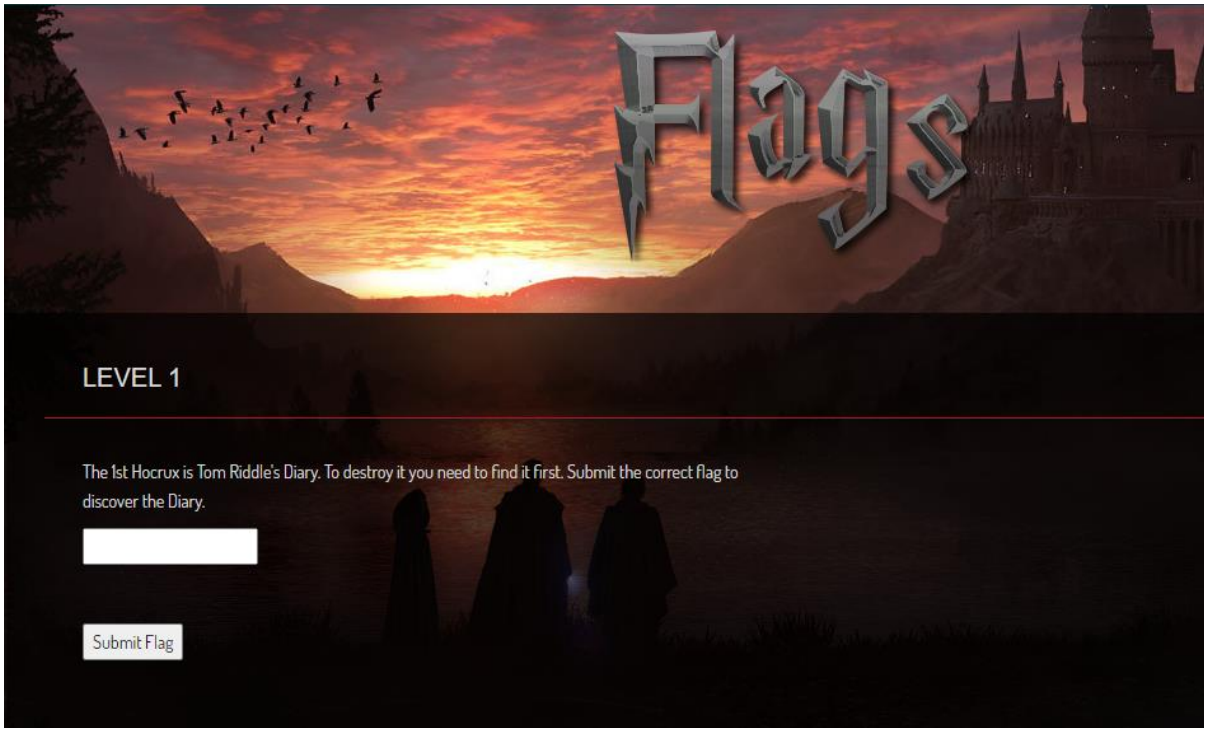
WHAT IS ACCIO FLAGS?

Harry Potter along with his friends Ron and Hermione go through various challenges in order to destroy the evil dark wizard, Lord Voldemort. To defeat him, Harry has to find and

**STEP 6 - Click Start to Play the CTF!**

# WALKTHROUGH

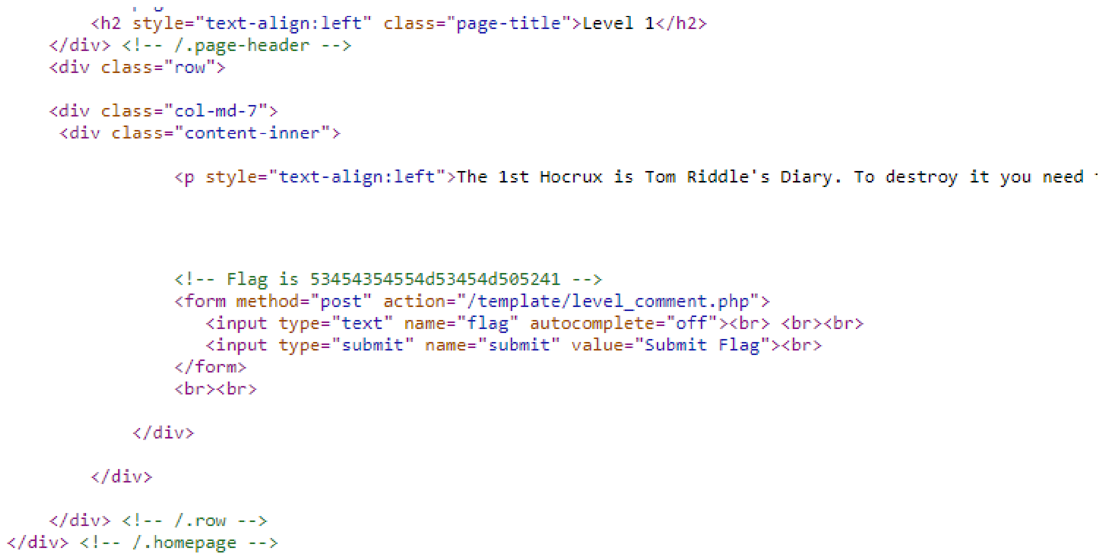
## LEVEL 1



LEVEL 1

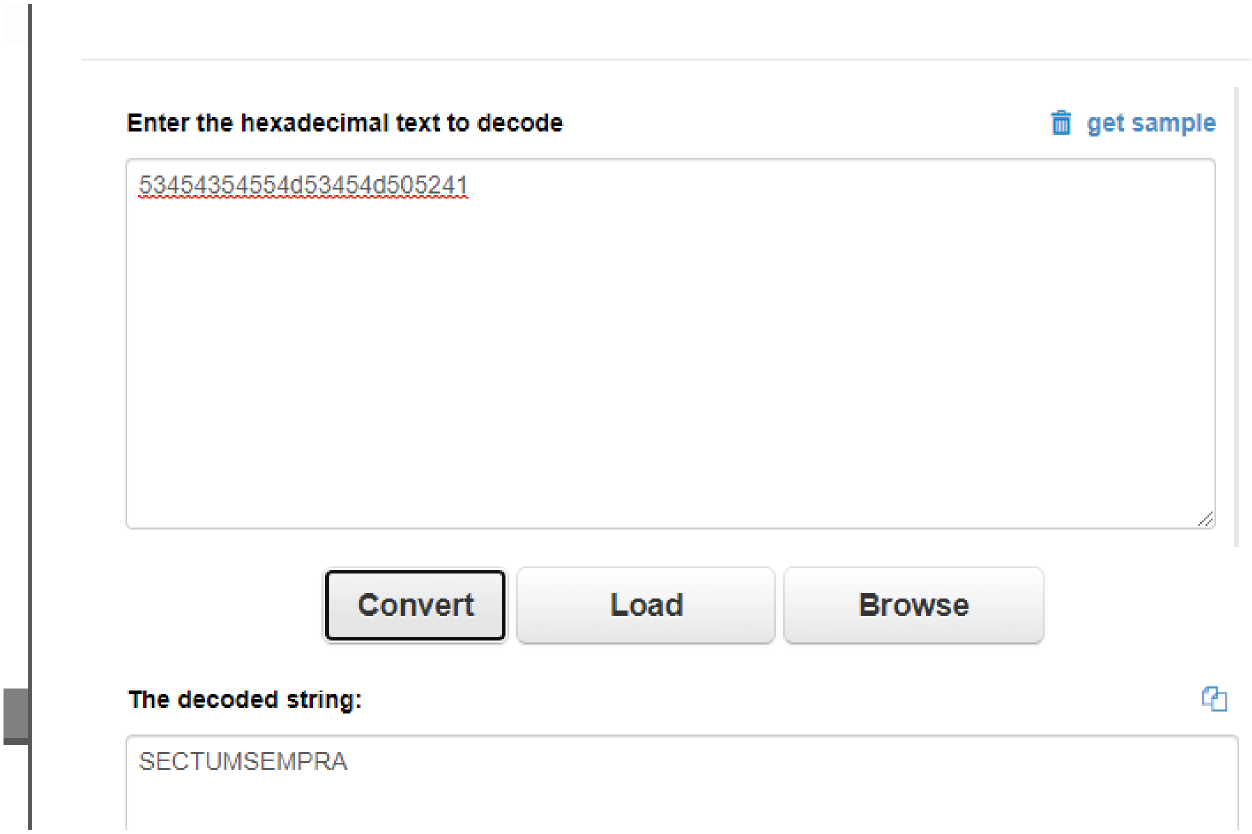
The 1st Hocrux is Tom Riddle's Diary. To destroy it you need to find it first. Submit the correct flag to discover the Diary.

The player must navigate to the source code of the webpage.



```
        <h2 style="text-align:left" class="page-title">Level 1</h2>
    </div> <!-- /.page-header -->
    <div class="row">

    <div class="col-md-7">
     <div class="content-inner">

            <p style="text-align:left">The 1st Hocrux is Tom Riddle's Diary. To destroy it you need


            <!-- Flag is 53454354554d53454d505241 -->
            <form method="post" action="/template/level_comment.php">
               <input type="text" name="flag" autocomplete="off"><br> <br><br>
               <input type="submit" name="submit" value="Submit Flag"><br>
            </form>
            <br><br>

        </div>

    </div>

    </div> <!-- /.row -->
</div> <!-- /.homepage -->
```

The flag is provided as a comment. However, if the player tries to submit this flag, it is said that the flag is wrong. By looking at the flag, it can be observed that it is in hexadecimal format. Hence, by using a hex to string converter, the flag could be obtained.



Enter the hexadecimal text to decode

53454354554d53454d505241

The decoded string:

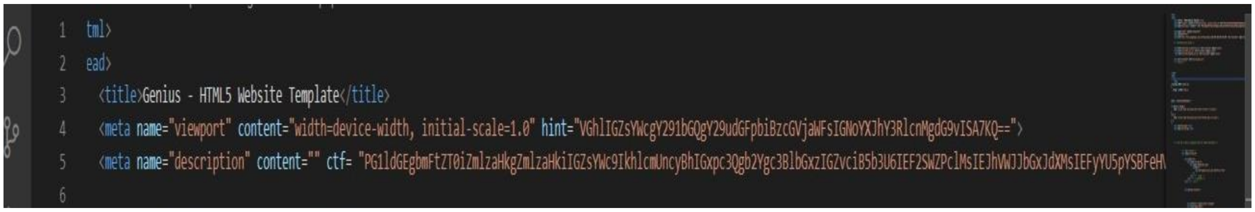
SECTUMSEMPRA

The flag would work only if it is entered in all capitals.

**FLAG: SECTUMSEMPRA**

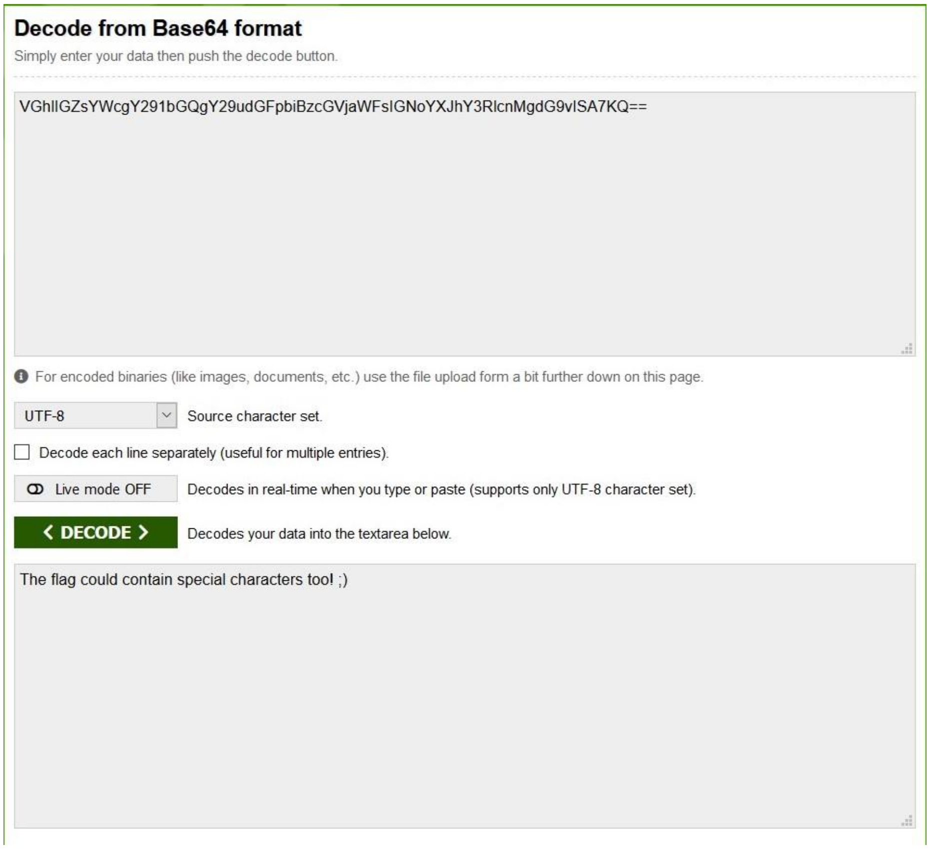
## LEVEL 2

The player could first navigate to the source code. There in the meta tags, they will be able to see two attributes called “hint” and “ctf” in two different meta tags.



```
tml>
ead>
  <title>Genius - HTML5 Website Template</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0" hint="VGhlIGZsYWcgY291bGQgY29udGFpbiBzcGVjaWFsIGNoYXJhY3RlcnMgdG9vISA7KQ==">
  <meta name="description" content="" ctf= "PG1ldGEgbmFtZT0iZmlzaHkgZmlzaHkiIGZsYWc9IkhlcmUncyBhIGxpc3Qgb2Ygc3BlbGxzIGZvciB5b3U6IEF2SWZPclMsIEJhWWJJbGxJdXMsIEFyYU5pYSBFeH
```

As it can be seen, the values of the attributes are both encoded in base64. The player could use an online base64 decoder for this and initially decode the hint.



**Decode from Base64 format**

Simply enter your data then push the decode button.

```
VGhlIGZsYWcgY291bGQgY29udGFpbiBzcGVjaWFsIGNoYXJhY3RlcnMgdG9vISA7KQ==
```

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

UTF-8 Source character set.

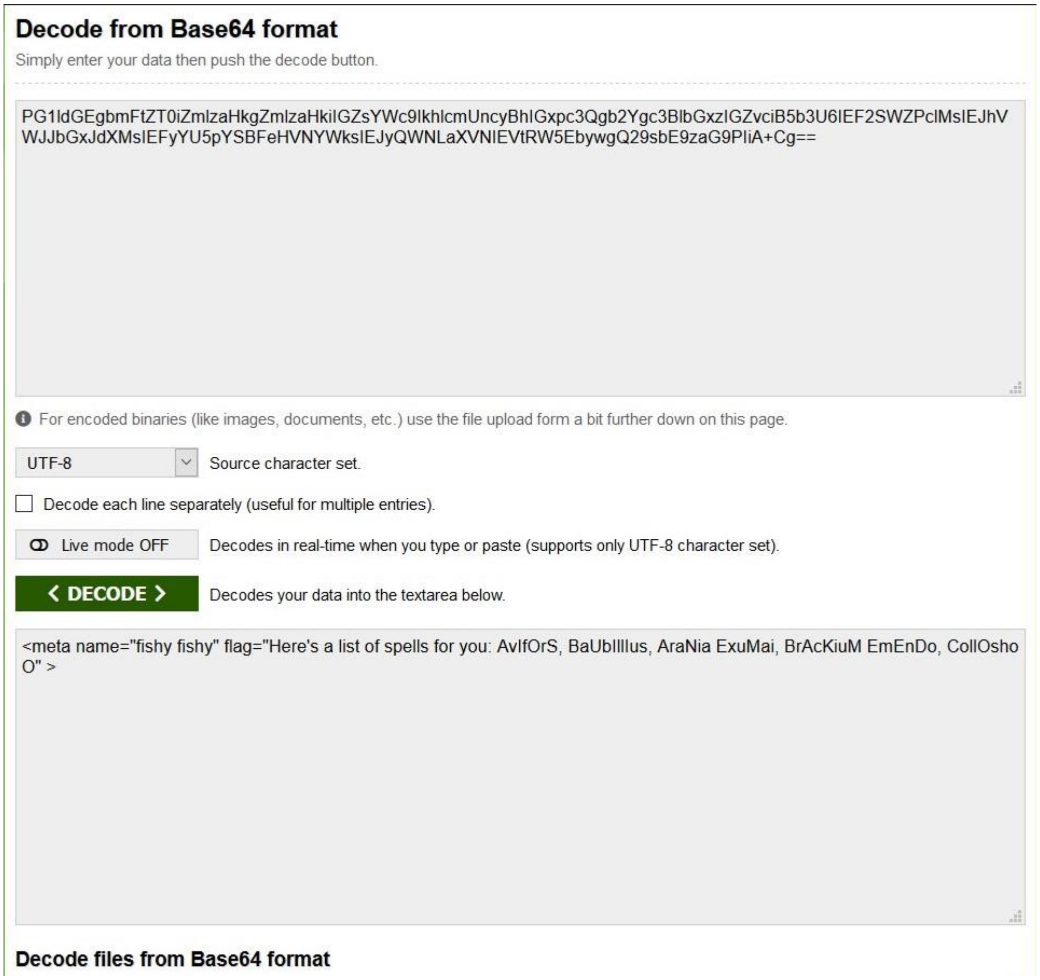
□ Decode each line separately (useful for multiple entries).

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

< DECODE > Decodes your data into the textarea below.

```
The flag could contain special characters too! ;)
```

The hint says that the flag could contain special characters as well. Now, the player can proceed to decode the ctf attribute.



**Decode from Base64 format**

Simply enter your data then push the decode button.

```
PG1ldGEgbmFtZT0iZmlzaHkgZmlzaHkiIGZsYWc9IkhlcmUncyBhIGxpc3Qgb2Ygc3BlbGxzIGZvciB5b3U6IEF2SWZPclMsIEJhV
WJJbGxJdXMsIEFyYU5pYSBFeHVNYWksIEJyQWNLaXVNIEVtRW5EbywgQ29sbE9zaG9PIiA+Cg==
```

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

UTF-8 Source character set.

☐ Decode each line separately (useful for multiple entries).

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

< DECODE > Decodes your data into the textarea below.

```
<meta name="fishy fishy" flag="Here's a list of spells for you: AvIfOrS, BaUbIllIus, AraNia ExuMai, BrAcKiuM EmEnDo, CollOsho
O" >
```

**Decode files from Base64 format**

The decoded tag gives a list of possible flags and the player is required to brute force them by combining with special characters to obtain the flag.

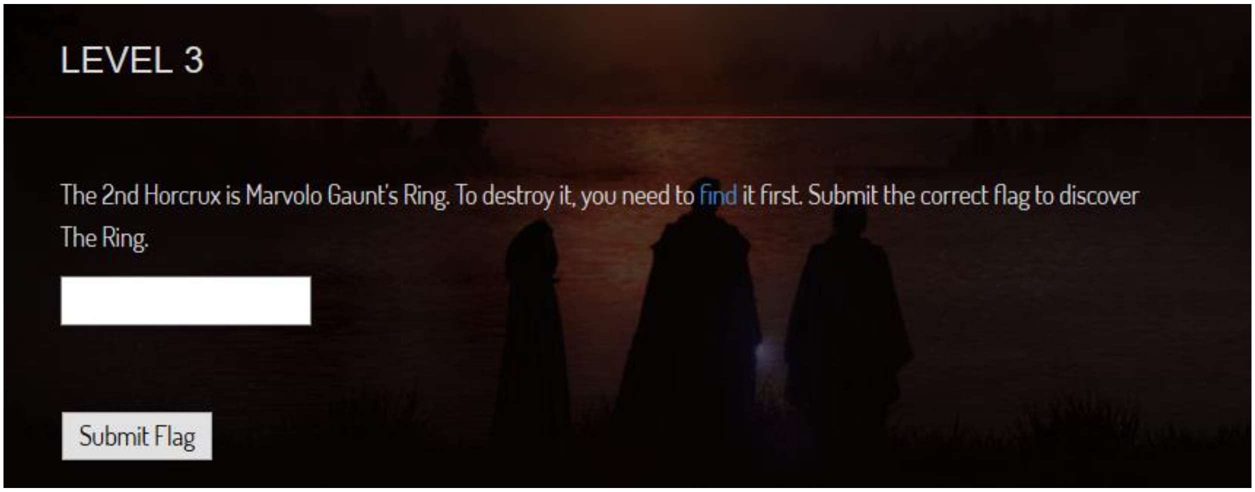
**The correct combination is: @r@Ni@ ExuM@i**

However, this will not be accepted since this level is about base64 encoding and decoding. Therefore, the player will have to encode the above value in base64 to obtain the correct flag.

**FLAG: QHJATmlAIEV4dU1AaQ==**

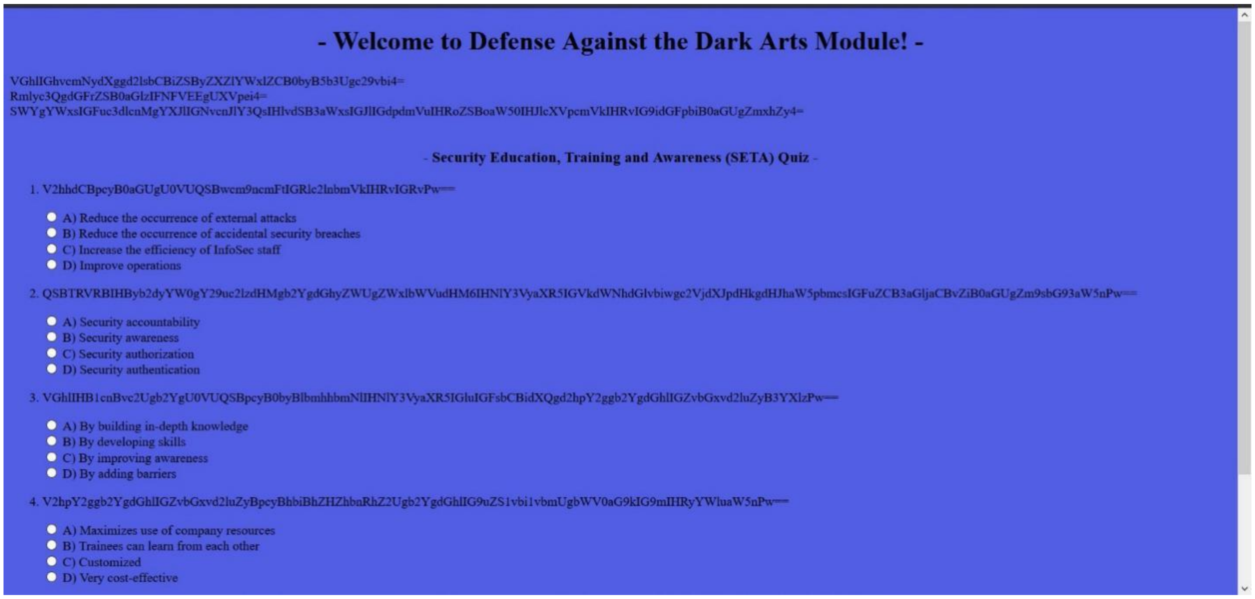
## LEVEL 3

Initially, the player will have to click on the link to navigate to the page with the quiz.



LEVEL 3

The 2nd Horcrux is Marvolo Gaunt's Ring. To destroy it, you need to find it first. Submit the correct flag to discover The Ring.



- Welcome to Defense Against the Dark Arts Module! -

VGhlIGhvcmNydXggd2lsbCBiZSByZXZlYWxlZCB0byB5b3Ugc29vbi4=
Rmlyc3QgdGFrZSB0aGlzIFNFVEEgUXVpei4=
SWYgYWxsIGFuc3dlcnMgYXJlIGNvcnJlY3QsIHlvdSB3aWxsIGJlIGdpdmVuIHRoZSBoaW50IHJlcXVpcmVkIHRvIG9idGFpbiB0aGUgZmxhZy4=

- Security Education, Training and Awareness (SETA) Quiz -

1. V2hhdCBpcyB0aGUgU0VUQSBwcm9ncmFtIGRlc2lnbmVkIHRvIGRvPw==

○ A) Reduce the occurrence of external attacks
○ B) Reduce the occurrence of accidental security breaches
○ C) Increase the efficiency of InfoSec staff
○ D) Improve operations

2. QSBTRVRBIHByb2dyYW0gY29uc2lzdHMgb2YgdGhyZWUgZWxlbWVudHM6IHNlY3VyaXR5IGVkdWNhdGlvbiwgc2VjdXJpdHkgdHJhaW5pbmcsIGFuZCB3aGljaCBvZiB0aGUgZm9sbG93aW5nPw==

○ A) Security accountability
○ B) Security awareness
○ C) Security authorization
○ D) Security authentication

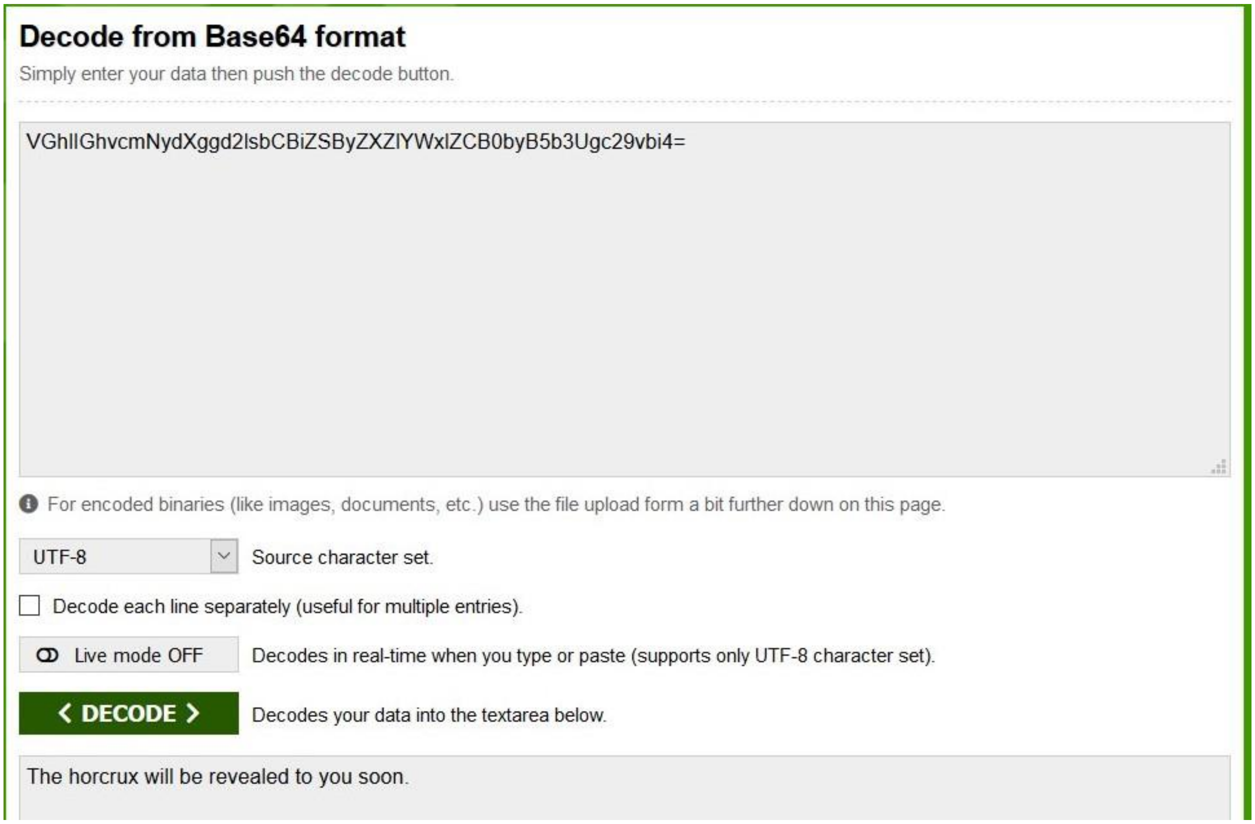
3. VGhlIHB1cnBvc2Ugb2YgU0VUQSBpcyB0byBlbmhhbmNlIHNlY3VyaXR5IGluIGFsbCBidXQgd2hpY2ggb2YgdGhlIGZvbGxvd2luZyB3YXlzPw==

○ A) By building in-depth knowledge
○ B) By developing skills
○ C) By improving awareness
○ D) By adding barriers

4. V2hpY2ggb2YgdGhlIGZvbGxvd2luZyBpcyBhbiBhZHZhbnRhZ2Ugb2YgdGhlIG9uZS1vbi1vbmUgbWV0aG9kIG9mIHRyYWluaW5nPw==

○ A) Maximizes use of company resources
○ B) Trainees can learn from each other
○ C) Customized
○ D) Very cost-effective

As it can be seen here, the quiz has 5 questions. However, the instructions and the questions are all base64 encoded. Therefore, they have to be decoded as a first step.



Decode from Base64 format

Simply enter your data then push the decode button.

```
VGhlIGhvcmNydXggd2lsbCBiZSByZXZlYWxlZCB0byB5b3Ugc29vbi4=
```

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

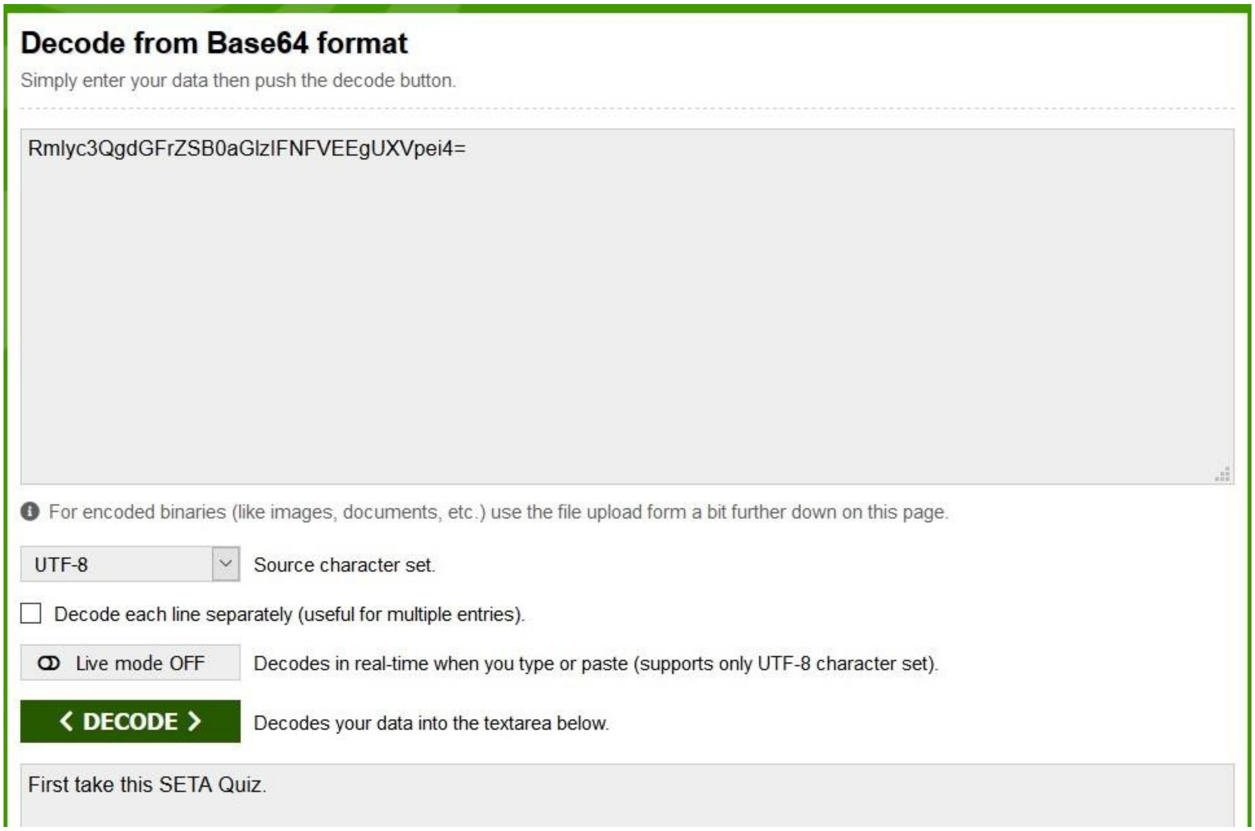
UTF-8 Source character set.

□ Decode each line separately (useful for multiple entries).

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

Decodes your data into the textarea below.

```
The horcrux will be revealed to you soon.
```



Decode from Base64 format

Simply enter your data then push the decode button.

```
Rmlyc3QgdGFrZSB0aGlzIFNFVEEgUXVpei4=
```

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

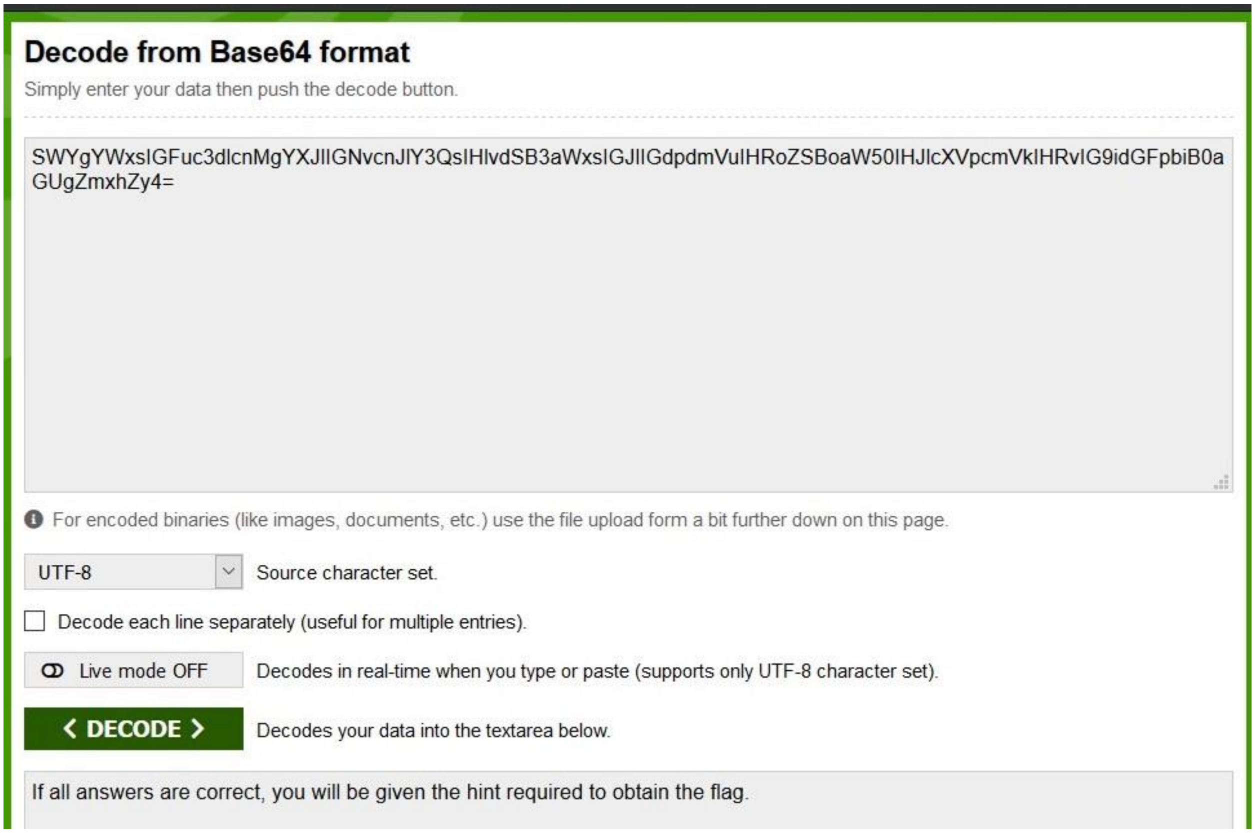
UTF-8 Source character set.

□ Decode each line separately (useful for multiple entries).

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

Decodes your data into the textarea below.

```
First take this SETA Quiz.
```



**Decode from Base64 format**

Simply enter your data then push the decode button.

```
SWYgYWxsIGFuc3dlcnMgYXJlIGNvcnJlY3QsIHlvdSB3aWxsIGJlIGdpdmVuIHRoZSBoaW50IHJlcXVpcmVkIHRvIG9idGFpbiB0a
GUgZmxhZy4=
```

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

UTF-8 Source character set.

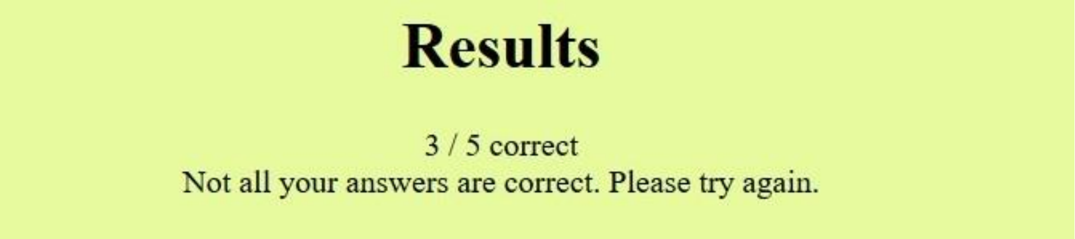
□ Decode each line separately (useful for multiple entries).

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

< DECODE > Decodes your data into the textarea below.

```
If all answers are correct, you will be given the hint required to obtain the flag.
```

The player is required to decode each and every question and give the correct answer and submit the form. If incorrect answers are given, an error message will be given.

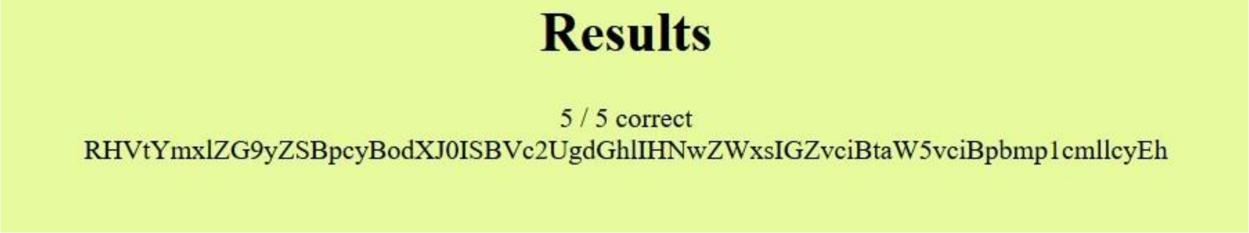


**Results**

3 / 5 correct

Not all your answers are correct. Please try again.

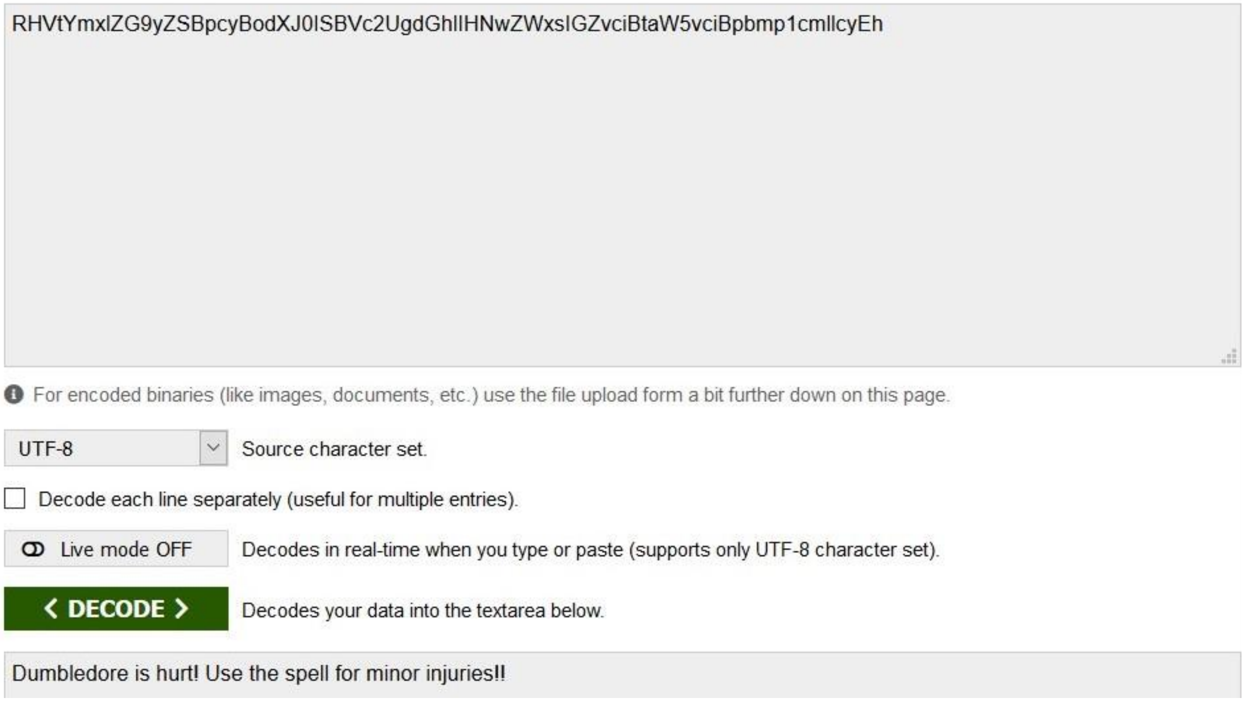
Once the correct answer is given, the hint regarding the flag will be given, also encoded in base64.



**Results**

5 / 5 correct

```
RHVtYmxlZG9yZSBpcyBodXJ0ISBVc2UgdGhlIHNwZWxsIGZvciBtaW5vciBpbmp1cmllcyEh
```



RHVtYmxlZG9yZSBpcyBodXJ0ISBVc2UgdGhlIHNwZWxsIGZvciBtaW5vciBpbmp1cmllcyEh

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

UTF-8 Source character set.

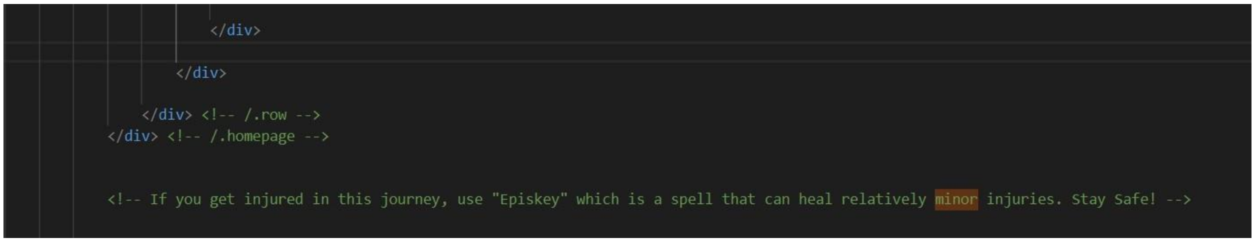
□ Decode each line separately (useful for multiple entries).

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

Decodes your data into the textarea below.

Dumbledore is hurt! Use the spell for minor injuries!!

This hint means that the flag would be related with the spell for minor injuries. This spell was hidden in the source code of a previous level.

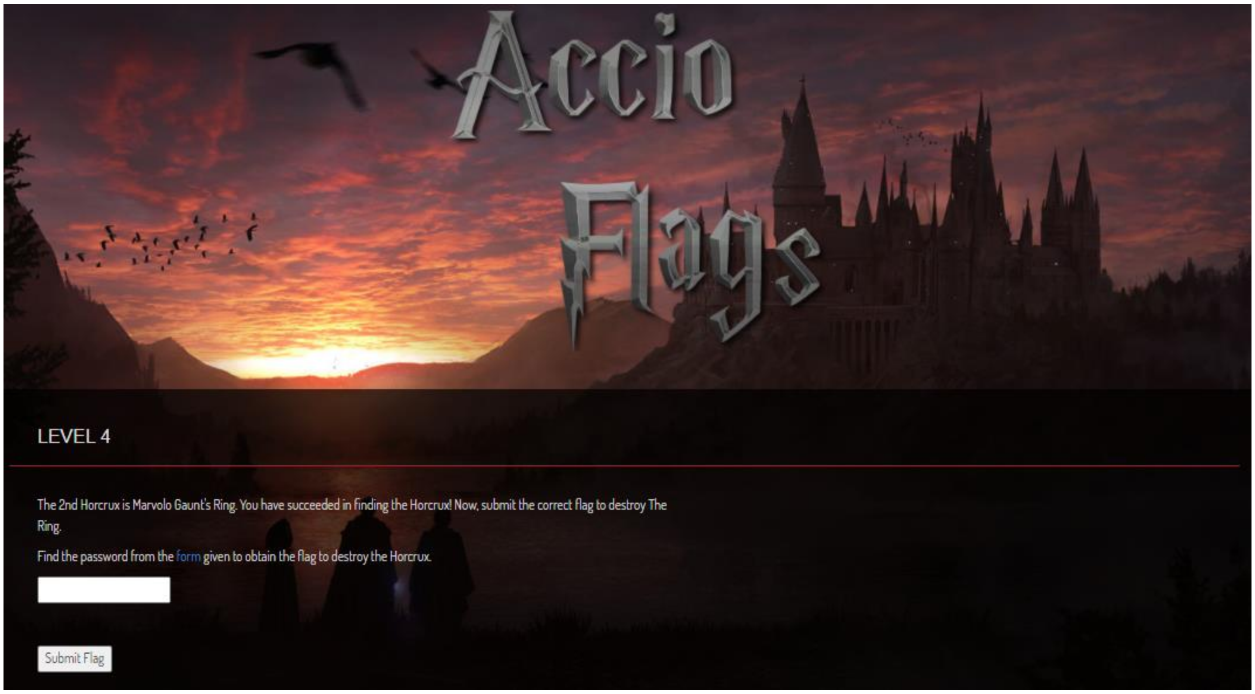


```
            </div>

        </div>

    </div> <!-- /.row -->
</div> <!-- /.homepage -->


<!-- If you get injured in this journey, use "Episkey" which is a spell that can heal relatively minor injuries. Stay Safe! -->
```

The spell is “Episkey!”. However, this will not work. Therefore, the flag will be the base64 encoded version of the spell.

**FLAG: RXBpc2tleSE**

## LEVEL 4

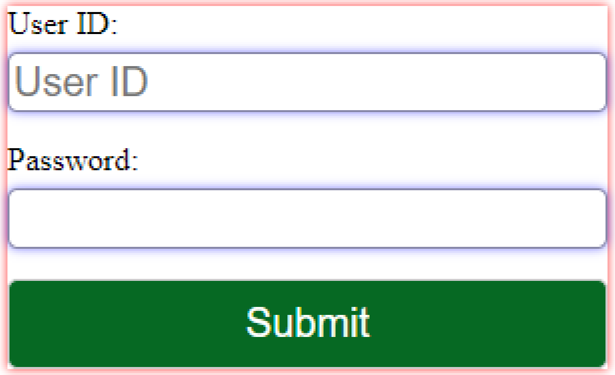


LEVEL 4

The 2nd Horcrux is Marvolo Gaunt's Ring. You have succeeded in finding the Horcrux! Now, submit the correct flag to destroy The Ring.

Find the password from the form given to obtain the flag to destroy the Horcrux.

Once the link is clicked on, the player will be directed to a form.

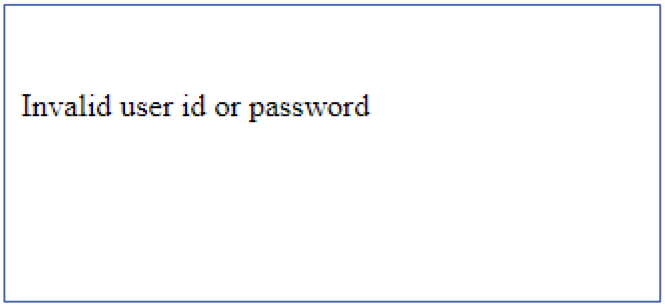


User ID:

User ID

Password:

Upon submission of incorrect data, an error message is given.



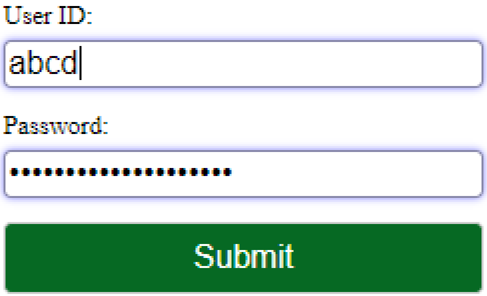
Invalid user id or password

The player must try and access all records in the database. This form is vulnerable to SQL injection attacks. Therefore, the player needs to find a query that is able to exploit this vulnerability.

If player provides **abcd** as userid and **anything' or 'x'='x** as password, then the query will be constructed as follows:

**$SQL = "select * from user_details where userid = 'abcd' and password = 'anything' or 'x'='x' ";**

Based on operator precedence, the "WHERE" clause is true for every row. Therefore, the query will return all records.

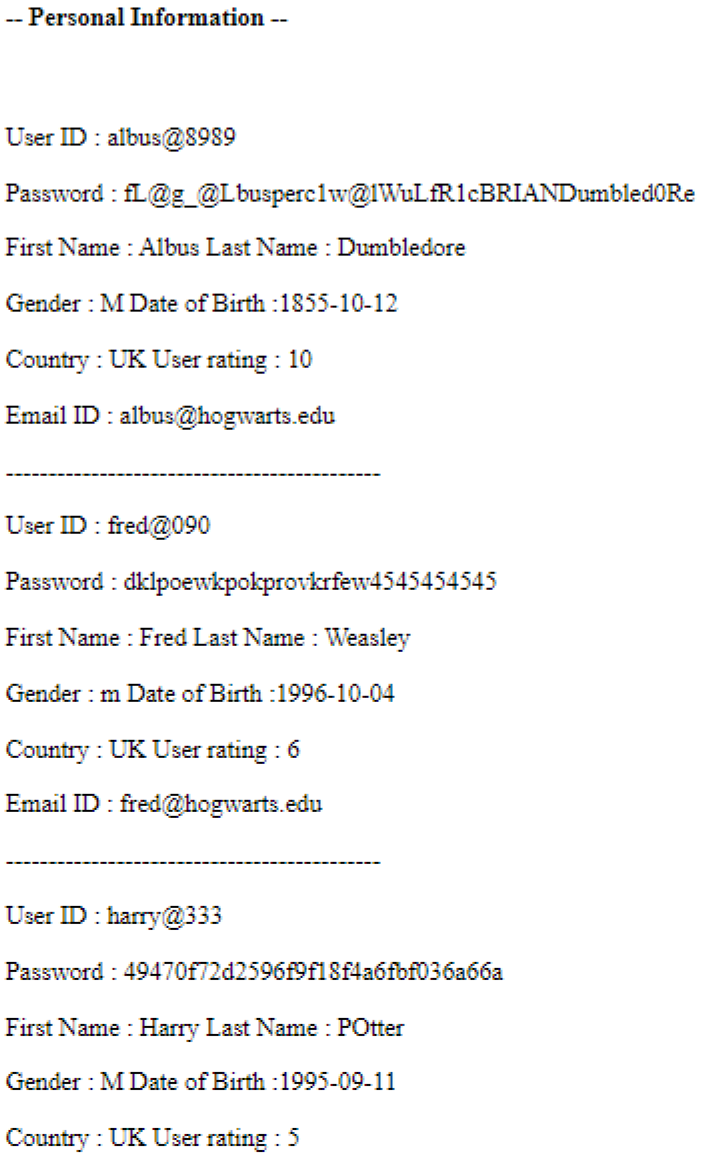


User ID:

abcd

Password:

••••••••••••••••••••



**-- Personal Information --**

User ID : albus@8989

Password : fL@g_@Lbusperc1w@lWuLfR1cBRIANDumbled0Re

First Name : Albus Last Name : Dumbledore

Gender : M Date of Birth :1855-10-12

Country : UK User rating : 10

Email ID : albus@hogwarts.edu

---------------------------------------------

User ID : fred@090

Password : dklpoewkpokprovkrfew4545454545

First Name : Fred Last Name : Weasley

Gender : m Date of Birth :1996-10-04

Country : UK User rating : 6

Email ID : fred@hogwarts.edu

---------------------------------------------

User ID : harry@333

Password : 49470f72d2596f9f18f4a6fbf036a66a

First Name : Harry Last Name : POtter

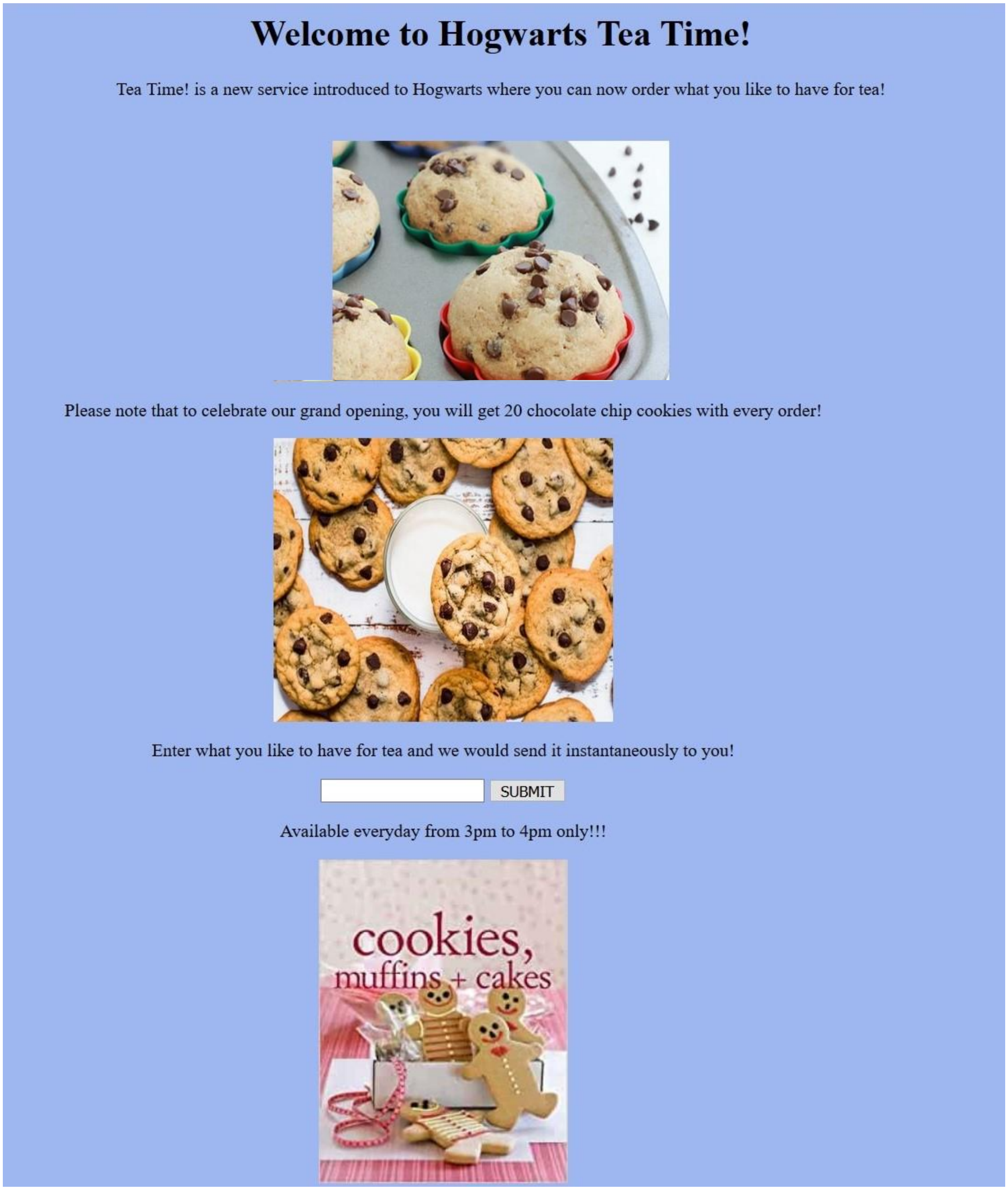
Gender : M Date of Birth :1995-09-11

Country : UK User rating : 5

**FLAG: fL@g_@Lbusperc1w@lWuLfR1cBRIANDumbled0Re**

## LEVEL 5

Initially, the player will have to navigate to the “Hogwarts Tea Time!” page link provided.



Welcome to Hogwarts Tea Time!

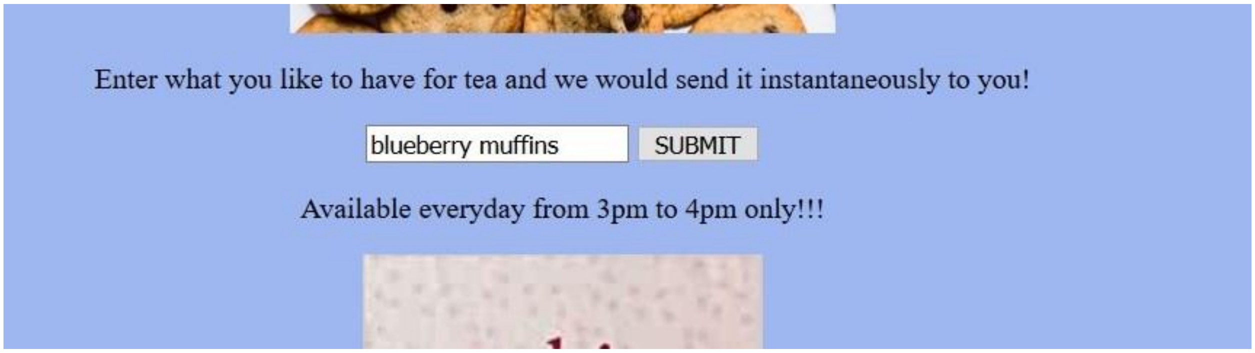
Tea Time! is a new service introduced to Hogwarts where you can now order what you like to have for tea!

Please note that to celebrate our grand opening, you will get 20 chocolate chip cookies with every order!

Enter what you like to have for tea and we would send it instantaneously to you!

Available everyday from 3pm to 4pm only!!!

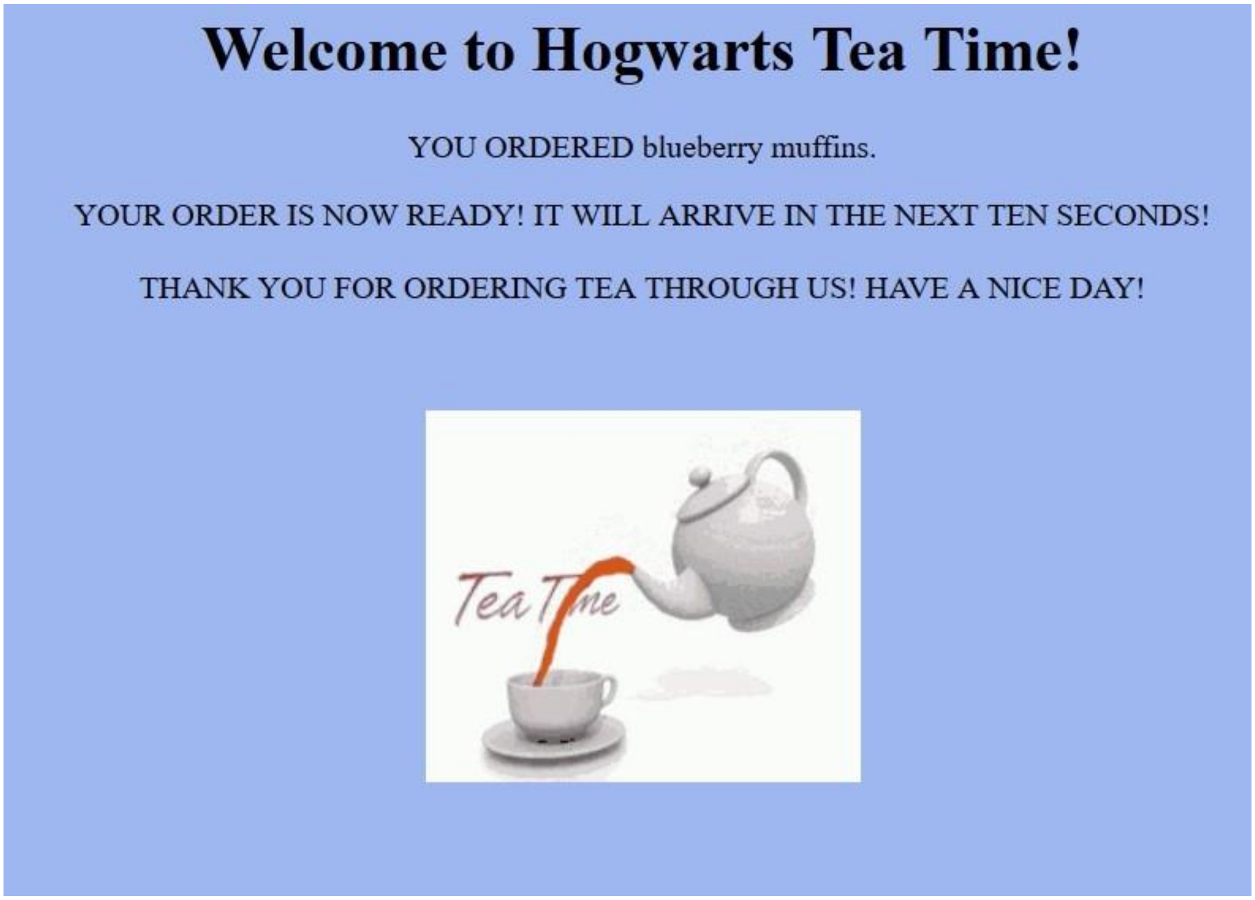
The user can enter the menu they would like to have for tea and submit it.



Enter what you like to have for tea and we would send it instantaneously to you!

blueberry muffins

Available everyday from 3pm to 4pm only!!!



Welcome to Hogwarts Tea Time!

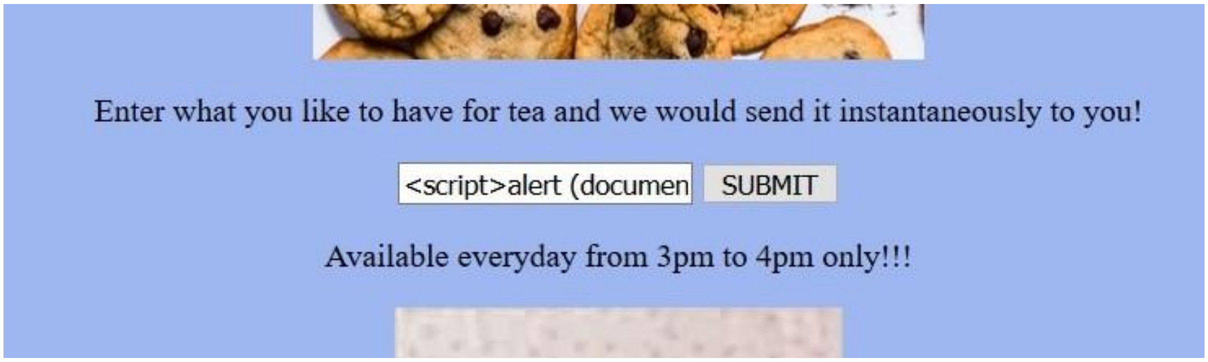
YOU ORDERED blueberry muffins.

YOUR ORDER IS NOW READY! IT WILL ARRIVE IN THE NEXT TEN SECONDS!

THANK YOU FOR ORDERING TEA THROUGH US! HAVE A NICE DAY!

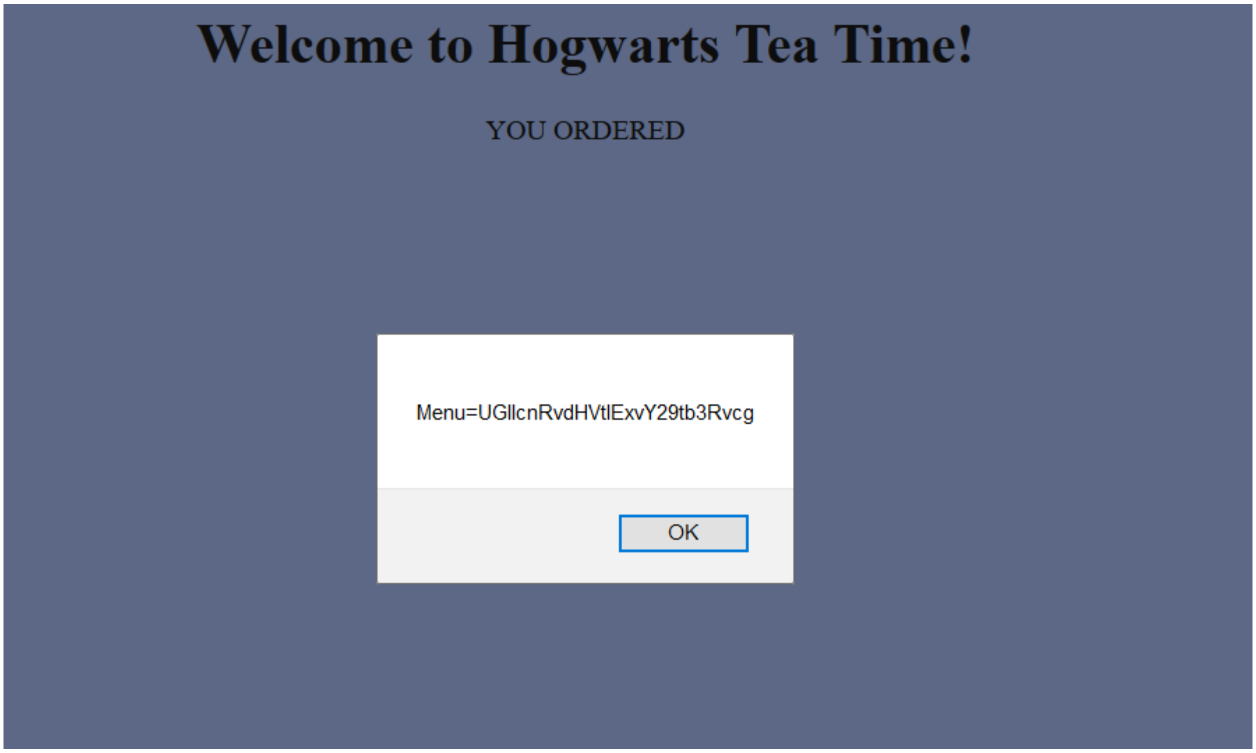
If the player executes an XSS attack as follows, the player can get the cookie value.

**<script>alert (document.cookie);</script>**



Enter what you like to have for tea and we would send it instantaneously to you!

Available everyday from 3pm to 4pm only!!!

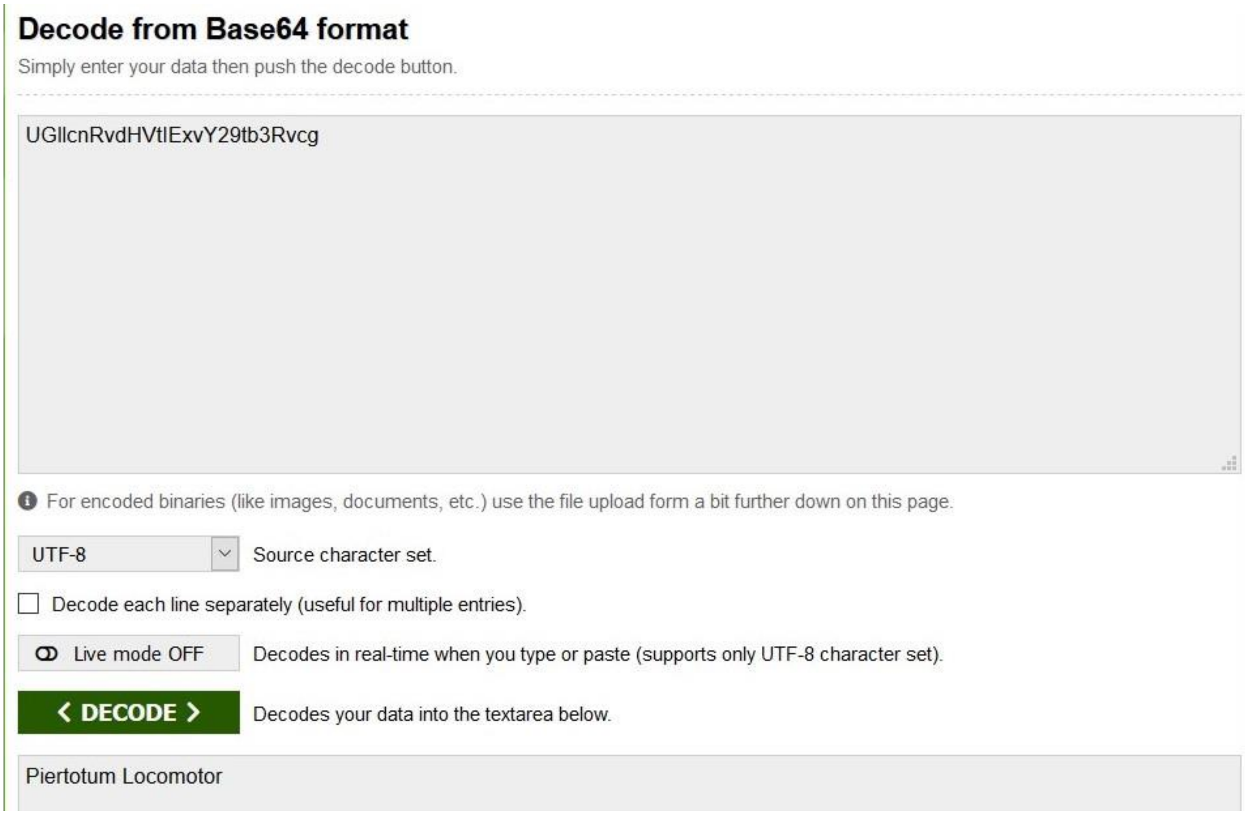


Welcome to Hogwarts Tea Time!

YOU ORDERED

```
Menu=UGllcnRvdHVtIExvY29tb3Rvcg
```

However, if the player submits the cookie value, an error message will be given. Therefore, if the player decodes this flag value in base64, they will get another spell.



**Decode from Base64 format**

Simply enter your data then push the decode button.

UGllcnRvdHVtIExvY29tb3Rvcg

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

UTF-8 Source character set.

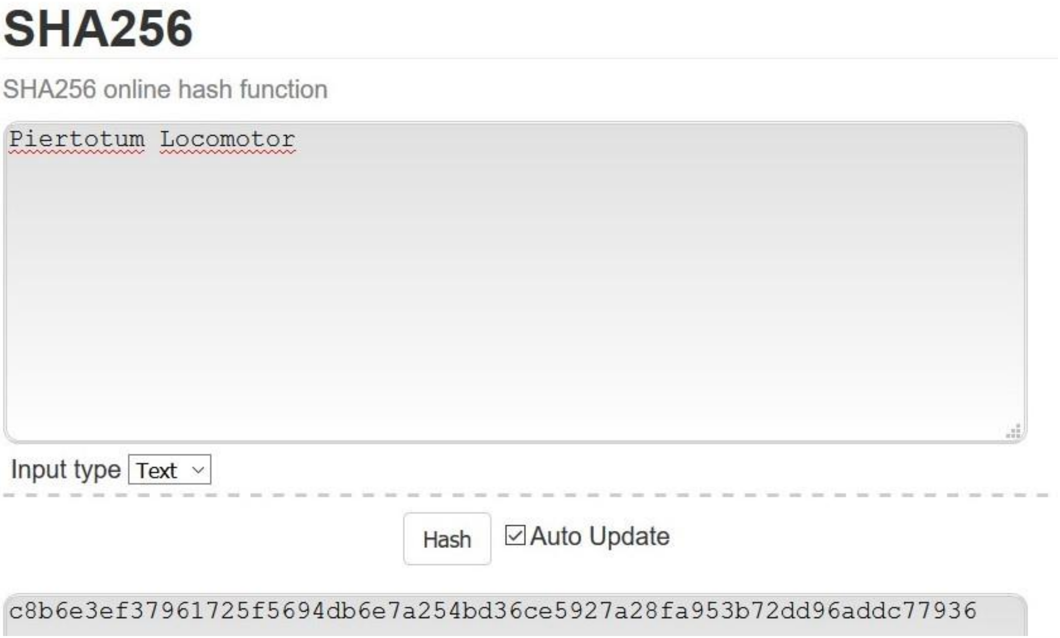
□ Decode each line separately (useful for multiple entries).

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

< DECODE > Decodes your data into the textarea below.

Piertotum Locomotor

According to the hint given in the source code, the SHA256 hash value of this spell would be the flag.



**SHA256**

SHA256 online hash function

```
Piertotum Locomotor
```

Input type Text

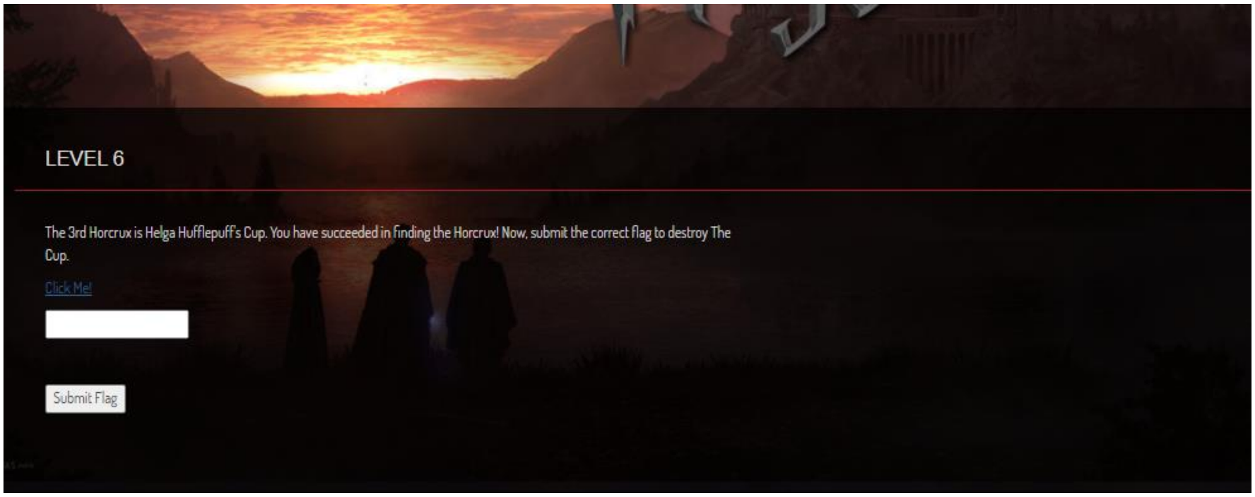
Hash ☑ Auto Update

```
c8b6e3ef37961725f5694db6e7a254bd36ce5927a28fa953b72dd96addc77936
```

**FLAG: c8b6e3ef37961725f5694db6e7a254bd36ce5927a28fa953b72dd96addc77936**

## LEVEL 6

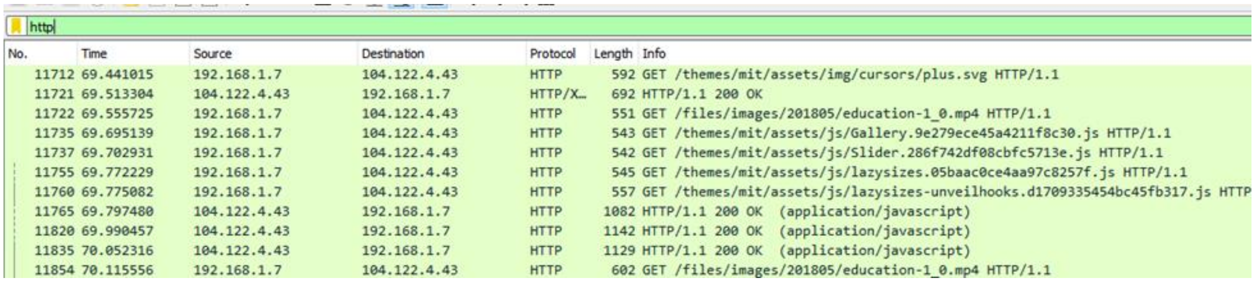
By clicking on the link provided, the player can download a .pcap file. This gives a hint to the player that Wireshark is the tool required to complete this level since .pcap files are data files created using Wireshark and they contain the data packets of a network. These files are mainly used in analyzing the network characteristics of certain data.



LEVEL 6

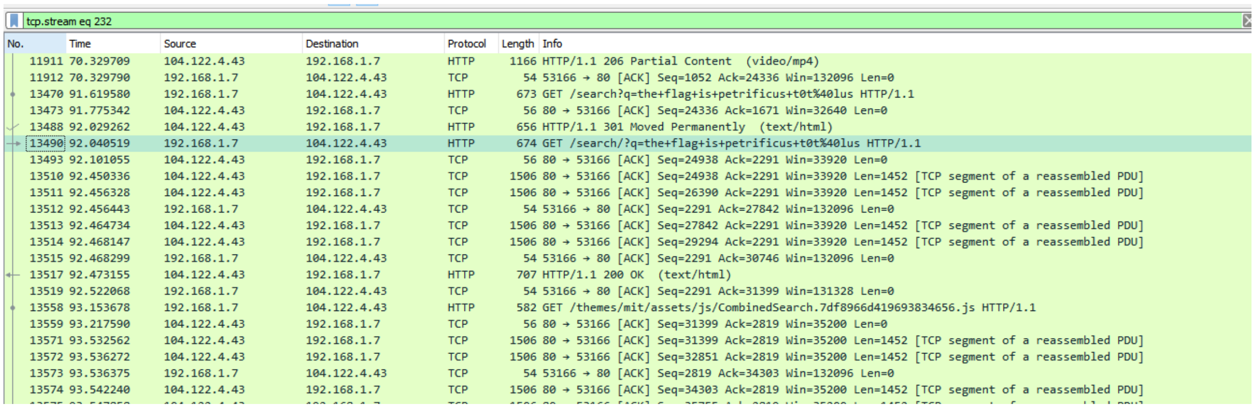
The 3rd Horcrux is Helga Hufflepuff's Cup. You have succeeded in finding the Horcrux! Now, submit the correct flag to destroy The Cup.

When the player opens the .pcap file using Wireshark, they can observe that there are 13, 996 captured packets. However, human readable and meaningful data are mostly in http packets. Therefore, http packets have to be filtered out.



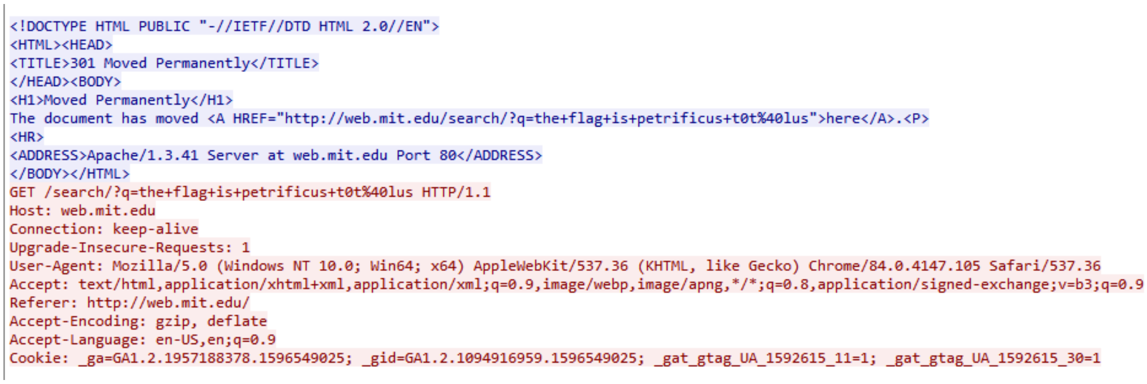
```
http
No.     Time       Source         Destination    Protocol Length Info
  11712 69.441015  192.168.1.7    104.122.4.43   HTTP      592 GET /themes/mit/assets/img/cursors/plus.svg HTTP/1.1
  11721 69.513304  104.122.4.43   192.168.1.7    HTTP/X…   692 HTTP/1.1 200 OK
  11722 69.555725  192.168.1.7    104.122.4.43   HTTP      551 GET /files/images/201805/education-1_0.mp4 HTTP/1.1
  11735 69.695139  192.168.1.7    104.122.4.43   HTTP      543 GET /themes/mit/assets/js/Gallery.9e279ece45a4211f8c30.js HTTP/1.1
  11737 69.702931  192.168.1.7    104.122.4.43   HTTP      542 GET /themes/mit/assets/js/Slider.286f742df08cbfc5713e.js HTTP/1.1
  11755 69.772229  192.168.1.7    104.122.4.43   HTTP      545 GET /themes/mit/assets/js/lazysizes.05baac0ce4aa97c8257f.js HTTP/1.1
  11760 69.775082  192.168.1.7    104.122.4.43   HTTP      557 GET /themes/mit/assets/js/lazysizes-unveilhooks.d1709335454bc45fb317.js HTTP
  11765 69.797480  104.122.4.43   192.168.1.7    HTTP     1082 HTTP/1.1 200 OK  (application/javascript)
  11820 69.990457  104.122.4.43   192.168.1.7    HTTP     1142 HTTP/1.1 200 OK  (application/javascript)
  11835 70.052316  104.122.4.43   192.168.1.7    HTTP     1129 HTTP/1.1 200 OK  (application/javascript)
  11854 70.115556  192.168.1.7    104.122.4.43   HTTP      602 GET /files/images/201805/education-1_0.mp4 HTTP/1.1
```

When going through the http packets there is an interesting packet which has the word “flag” on it.



```
tcp.stream eq 232
No.   Time      Source        Destination   Protocol Length Info
11911 70.329709 104.122.4.43  192.168.1.7   HTTP     1166 HTTP/1.1 206 Partial Content  (video/mp4)
11912 70.329790 192.168.1.7   104.122.4.43  TCP        54 53166 → 80 [ACK] Seq=1052 Ack=24336 Win=132096 Len=0
13470 91.619580 192.168.1.7   104.122.4.43  HTTP      673 GET /search?q=the+flag+is+petrificus+t0t%40lus HTTP/1.1
13473 91.775342 104.122.4.43  192.168.1.7   TCP        56 80 → 53166 [ACK] Seq=24336 Ack=1671 Win=32640 Len=0
13488 92.029262 104.122.4.43  192.168.1.7   HTTP      656 HTTP/1.1 301 Moved Permanently  (text/html)
13490 92.040519 192.168.1.7   104.122.4.43  HTTP      674 GET /search/?q=the+flag+is+petrificus+t0t%40lus HTTP/1.1
13493 92.101055 104.122.4.43  192.168.1.7   TCP        56 80 → 53166 [ACK] Seq=24938 Ack=2291 Win=33920 Len=0
13510 92.450336 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=24938 Ack=2291 Win=33920 Len=1452 [TCP segment of a reassembled PDU]
13511 92.456328 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=26390 Ack=2291 Win=33920 Len=1452 [TCP segment of a reassembled PDU]
13512 92.456443 192.168.1.7   104.122.4.43  TCP        54 53166 → 80 [ACK] Seq=2291 Ack=27842 Win=132096 Len=0
13513 92.464734 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=27842 Ack=2291 Win=33920 Len=1452 [TCP segment of a reassembled PDU]
13514 92.468147 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=29294 Ack=2291 Win=33920 Len=1452 [TCP segment of a reassembled PDU]
13515 92.468299 192.168.1.7   104.122.4.43  TCP        54 53166 → 80 [ACK] Seq=2291 Ack=30746 Win=132096 Len=0
13517 92.473155 104.122.4.43  192.168.1.7   HTTP      707 HTTP/1.1 200 OK  (text/html)
13519 92.522068 192.168.1.7   104.122.4.43  TCP        54 53166 → 80 [ACK] Seq=2291 Ack=31399 Win=131328 Len=0
13558 93.153678 192.168.1.7   104.122.4.43  HTTP      582 GET /themes/mit/assets/js/CombinedSearch.7df8966d419693834656.js HTTP/1.1
13559 93.217590 104.122.4.43  192.168.1.7   TCP        56 80 → 53166 [ACK] Seq=31399 Ack=2819 Win=35200 Len=0
13571 93.532562 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=31399 Ack=2819 Win=35200 Len=1452 [TCP segment of a reassembled PDU]
13572 93.536272 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=32851 Ack=2819 Win=35200 Len=1452 [TCP segment of a reassembled PDU]
13573 93.536375 192.168.1.7   104.122.4.43  TCP        54 53166 → 80 [ACK] Seq=2819 Ack=34303 Win=132096 Len=0
13574 93.542240 104.122.4.43  192.168.1.7   TCP      1506 80 → 53166 [ACK] Seq=34303 Ack=2819 Win=35200 Len=1452 [TCP segment of a reassembled PDU]
```

More details can be viewed by following the HTTP stream.



```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>301 Moved Permanently</TITLE>
</HEAD><BODY>
<H1>Moved Permanently</H1>
The document has moved <A HREF="http://web.mit.edu/search/?q=the+flag+is+petrificus+t0t%40lus">here</A>.<P>
<HR>
<ADDRESS>Apache/1.3.41 Server at web.mit.edu Port 80</ADDRESS>
</BODY></HTML>
GET /search/?q=the+flag+is+petrificus+t0t%40lus HTTP/1.1
Host: web.mit.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://web.mit.edu/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.2.1957188378.1596549025; _gid=GA1.2.1094916959.1596549025; _gat_gtag_UA_1592615_11=1; _gat_gtag_UA_1592615_30=1
```

**GET /search?q=the+flag+is+petrificus+t0t%40lus HTTP/1.1\r\n**

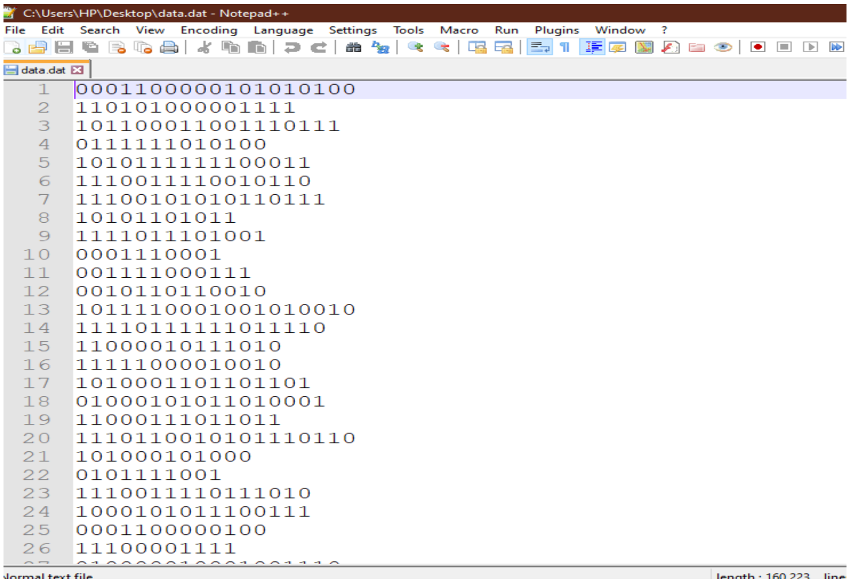
By observation, it can be concluded that the flag is petrificust0t%40lus.

But if the player tries to enter this as the flag they will get an error saying it's not the correct flag. That is because there is an encoded character in petrificust0t%40lus and it has to be decoded.

**FLAG: petrificust0t@lus**

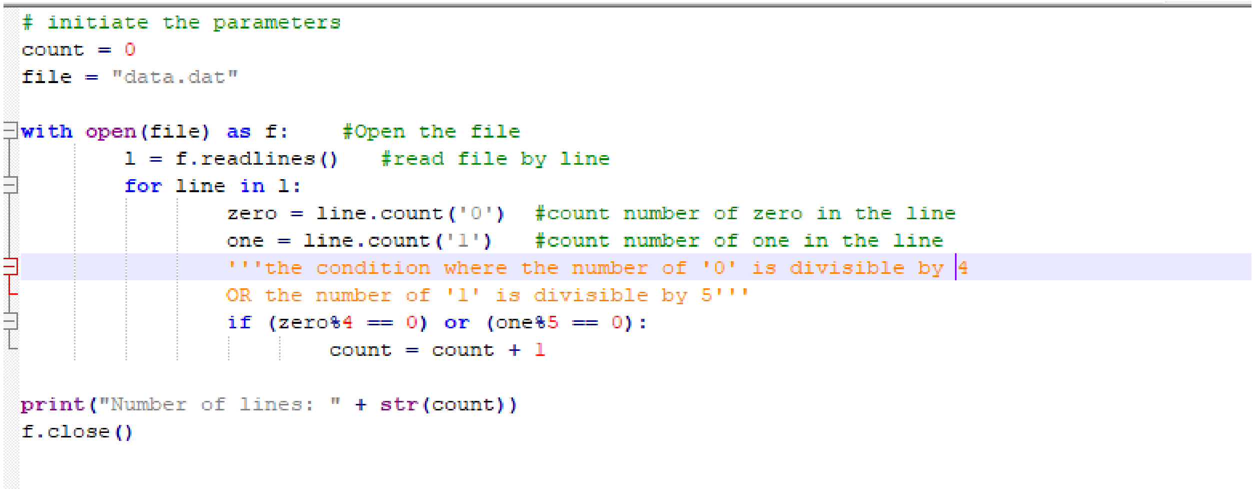
## LEVEL 7

The player is given a hint that the flag they need to find is a number. They are directed to download a data file once they click on the provided link.


C:\Users\HP\Desktop\data.dat - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
data.dat
Normal text file
length : 160,223 line

```
00011000001010100
11010100000001111
101100011001110111
0111111010100
101011111100011
111001111001011O
1110010101010110111
10101101011
11110111101001
0001110001
001111000111
0010110110010
101111000100101010010
111101111111011110
110000101111010
1111100000010010
101000110110101101
0100010101101010001
11000111011011
11101100101010111010110
101000101000
0101111001
111001111011110 10
1000101011100111
0001100000100
11100001111
```

This file consists of 10, 001 lines of binary strings. The player needs to make a program such that the number of 0s is a multiple of 4 or the number of 1s is a multiple of 5 is counted. They can use any programming language of their preference. The output after executing this program will be the flag. Following is a sample program created in Python.



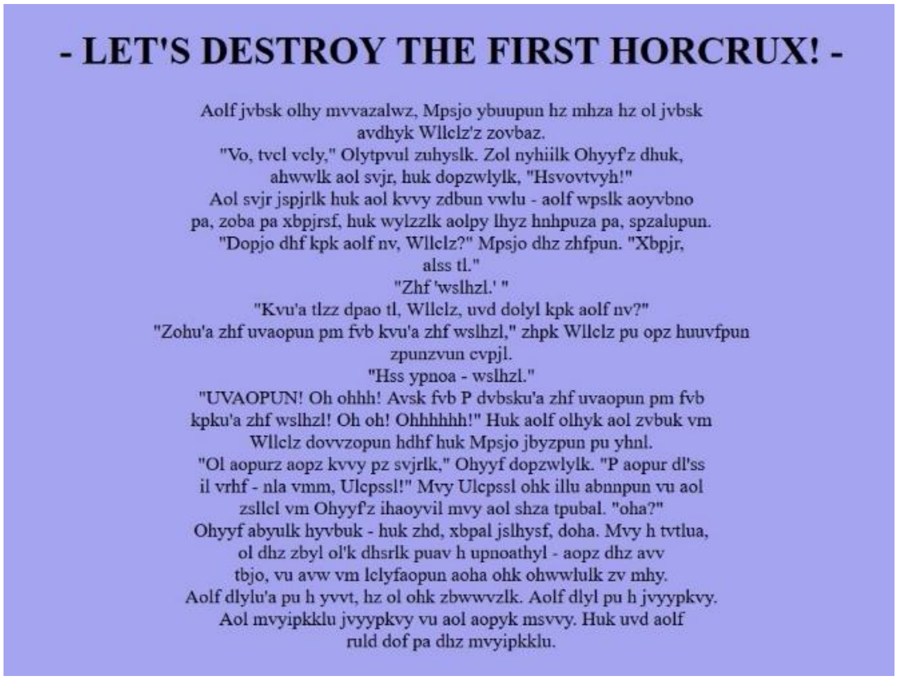
```python
# initiate the parameters
count = 0
file = "data.dat"

with open(file) as f:    #Open the file
        l = f.readlines()   #read file by line
        for line in l:
                zero = line.count('0')  #count number of zero in the line
                one = line.count('1')   #count number of one in the line
                '''the condition where the number of '0' is divisible by 4
                OR the number of '1' is divisible by 5'''
                if (zero%4 == 0) or (one%5 == 0):
                        count = count + 1

print("Number of lines: " + str(count))
f.close()
```

**FLAG: 4352**

## LEVEL 8

After successfully completing the previous level, the player will be navigated to the next level. There, a link to destroy the obtained Horcrux will be obtained. Once they click on that link, they will be navigated to another webpage.

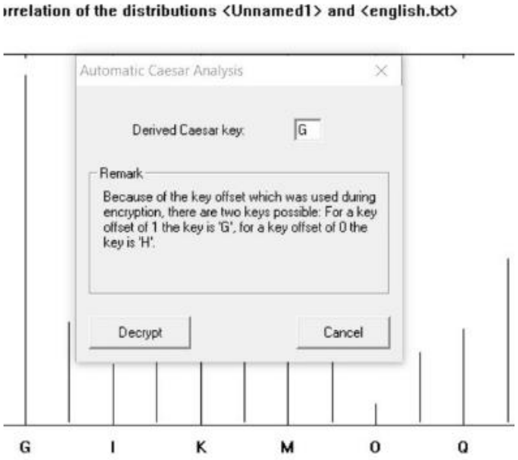
Here, the player will be required to perform a letter frequency analysis with Caesar Cipher on the encrypted text given using a software like CrypTool.



- LET'S DESTROY THE FIRST HORCRUX! -

Aolf jvbsk olhy mvvazalwz, Mpsjo ybuupun hz mhza hz ol jvbsk
avdhyk Wllclz'z zovbaz.
"Vo, tvcl vcly," Olytpvul zuhyslk. Zol nyhiilk Ohyyf'z dhuk,
ahwwlk aol svjr, huk dopzwlylk, "Hsvovtvyh!"
Aol svjr jspjrlk huk aol kvvy zdbun vwlu - aolf wpslk aoyvbno
pa, zoba pa xbpjrsf, huk wylzzlk aolpy lhyz hnhpuza pa, spzalupun.
"Dopjo dhf kpk aolf nv, Wllclz?" Mpsjo dhz zhfpun. "Xbpjr,
alss tl."
"Zhf 'wslhzl.' "
"Kvu'a tlzz dpao tl, Wllclz, uvd dolyl kpk aolf nv?"
"Zohu'a zhf uvaopun pm fvb kvu'a zhf wslhzl," zhpk Wllclz pu opz huuvfpun
zpunzvun cvpjl.
"Hss ypnoa - wslhzl."
"UVAOPUN! Oh ohhh! Avsk fvb P dvbsku'a zhf uvaopun pm fvb
kpku'a zhf wslhzl! Oh oh! Ohhhhhh!" Huk aolf olhyk aol zvbuk vm
Wllclz dovvzopun hdhf huk Mpsjo jbyzpun pu yhnl.
"Ol aopurz aopz kvvy pz svjrlk," Ohyyf dopzwlylk. "P aopur dl'ss
il vrhf - nla vmm, Ulcpssl!" Mvy Ulcpssl ohk illu abnnpun vu aol
zsllcl vm Ohyyf'z ihaoyvil mvy aol shza tpubal. "oha?"
Ohyyf abyulk hyvbuk - huk zhd, xbpal jslhysf, doha. Mvy h tvtlua,
ol dhz zbyl ol'k dhsrlk puav h upnoathyl - aopz dhz avv
tbjo, vu avw vm lclyfaopun aoha ohk ohwwlulk zv mhy.
Aolf dlylu'a pu h yvvt, hz ol ohk zbwwvzlk. Aolf dlyl pu h jvyypkvy.
Aol mvyipkklu jvyypkvy vu aol aopyk msvvy. Huk uvd aolf
ruld dof pa dhz mvyipkklu.

Here, the player will see that the derived Caesar key is “G”. This should be saved for later use and the decryption procedure should be proceeded with.



Automatic Caesar Analysis

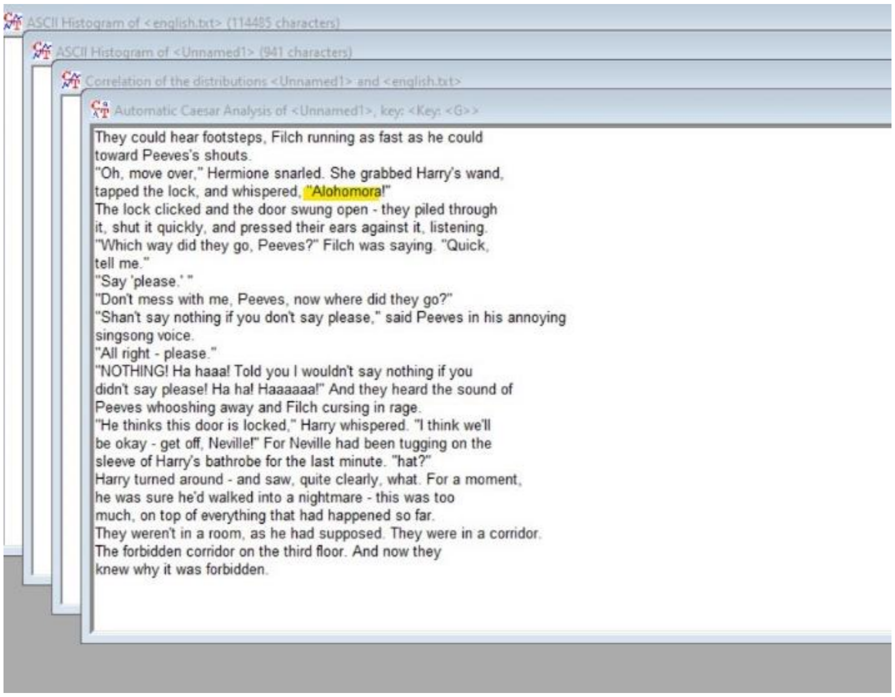
Derived Caesar key: G

Remark

Because of the key offset which was used during encryption, there are two keys possible: For a key offset of 1 the key is 'G', for a key offset of 0 the key is 'H'.

ırrelation of the distributions <Unnamed1> and <english.txt>
Decrypt
Cancel
G
I
K
M
O
Q

Here, the player can see a passage derived from Harry Potter book 1. The player should go through the passage and find the flag used.


ASCII Histogram of <english.txt> (114485 characters)
ASCII Histogram of <Unnamed1> (941 characters)
Correlation of the distributions <Unnamed1> and <english.txt>
Automatic Caesar Analysis of <Unnamed1>, key: <Key: <G>>

```
They could hear footsteps, Filch running as fast as he could
toward Peeves's shouts.
"Oh, move over," Hermione snarled. She grabbed Harry's wand,
tapped the lock, and whispered, "Alohomora!"
The lock clicked and the door swung open - they piled through
it, shut it quickly, and pressed their ears against it, listening.
"Which way did they go, Peeves?" Filch was saying. "Quick,
tell me."
"Say 'please.' "
"Don't mess with me, Peeves, now where did they go?"
"Shan't say nothing if you don't say please," said Peeves in his annoying
singsong voice.
"All right - please."
"NOTHING! Ha haaa! Told you I wouldn't say nothing if you
didn't say please! Ha ha! Haaaaaa!" And they heard the sound of
Peeves whooshing away and Filch cursing in rage.
"He thinks this door is locked," Harry whispered. "I think we'll
be okay - get off, Neville!" For Neville had been tugging on the
sleeve of Harry's bathrobe for the last minute. "hat?"
Harry turned around - and saw, quite clearly, what. For a moment,
he was sure he'd walked into a nightmare - this was too
much, on top of everything that had happened so far.
They weren't in a room, as he had supposed. They were in a corridor.
The forbidden corridor on the third floor. And now they
knew why it was forbidden.
```

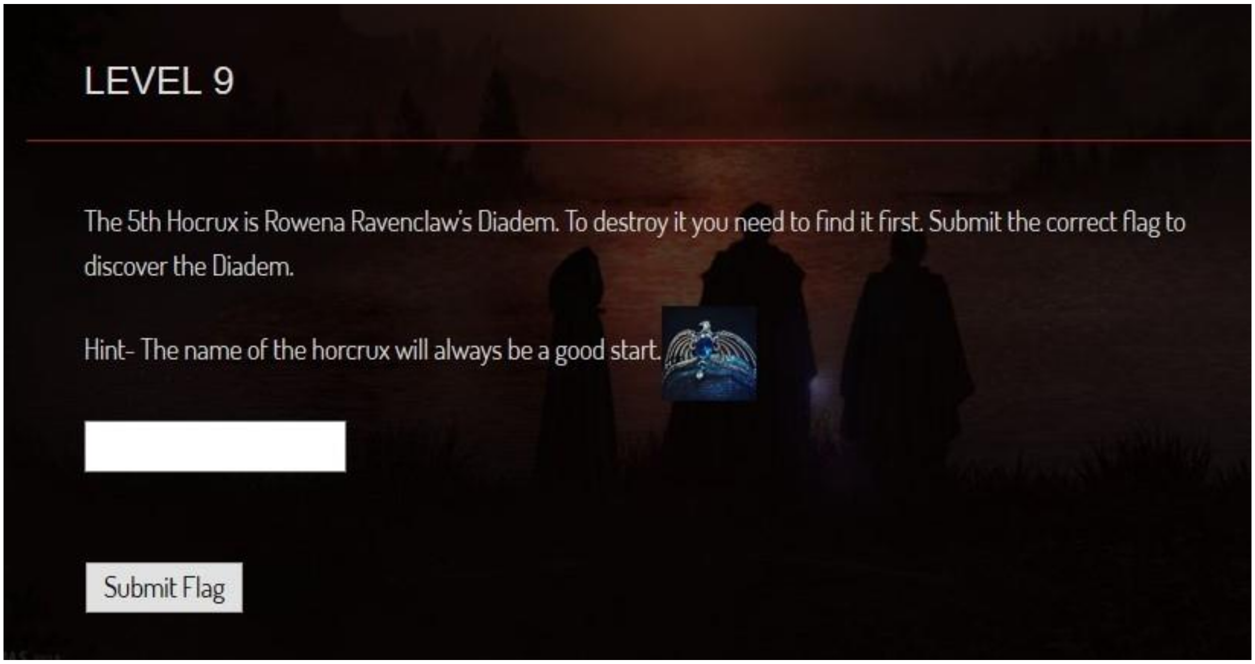
**Obtained spell: Alohomora**

The spell can be combined with all possible characters and numbers and brute forced to capture the flag.

**FLAG: @L0H0M0R@**

## LEVEL 9

The player has to click on the image as a first step.

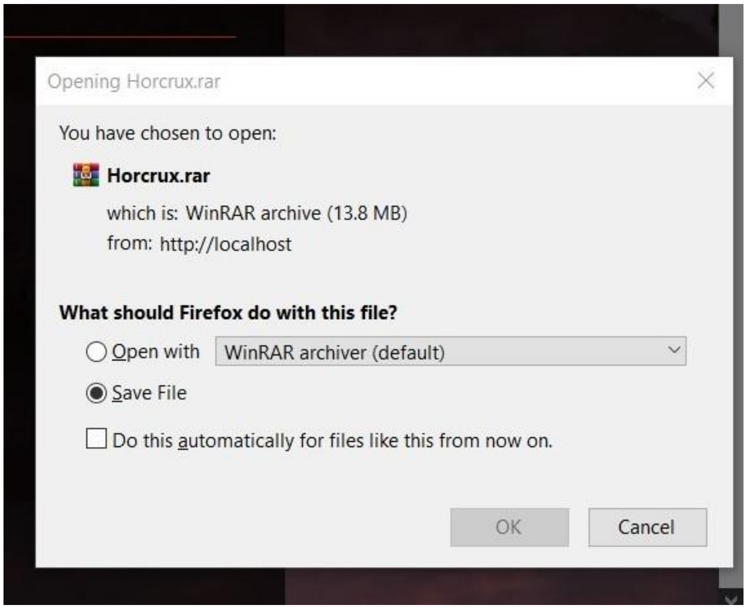


LEVEL 9

The 5th Hocrux is Rowena Ravenclaw's Diadem. To destroy it you need to find it first. Submit the correct flag to discover the Diadem.

Hint- The name of the horcrux will always be a good start.

Then, a .zip file will be downloaded. The player has to save it and unzip it.



Opening Horcrux.rar

You have chosen to open:

**Horcrux.rar**

which is: WinRAR archive (13.8 MB)
from: http://localhost

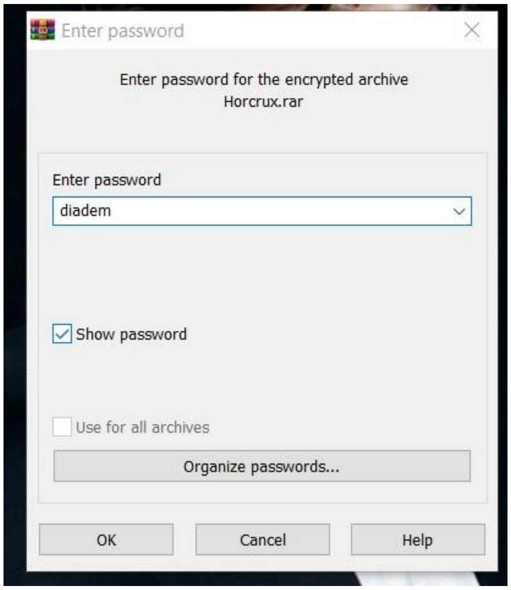
**What should Firefox do with this file?**

○ Open with WinRAR archiver (default)

● Save File

□ Do this automatically for files like this from now on.

The hint suggests that the name of the Horcrux will be a good start. Therefore, when the player tries to unzip this file, they can provide “diadem” as the password.



Enter password

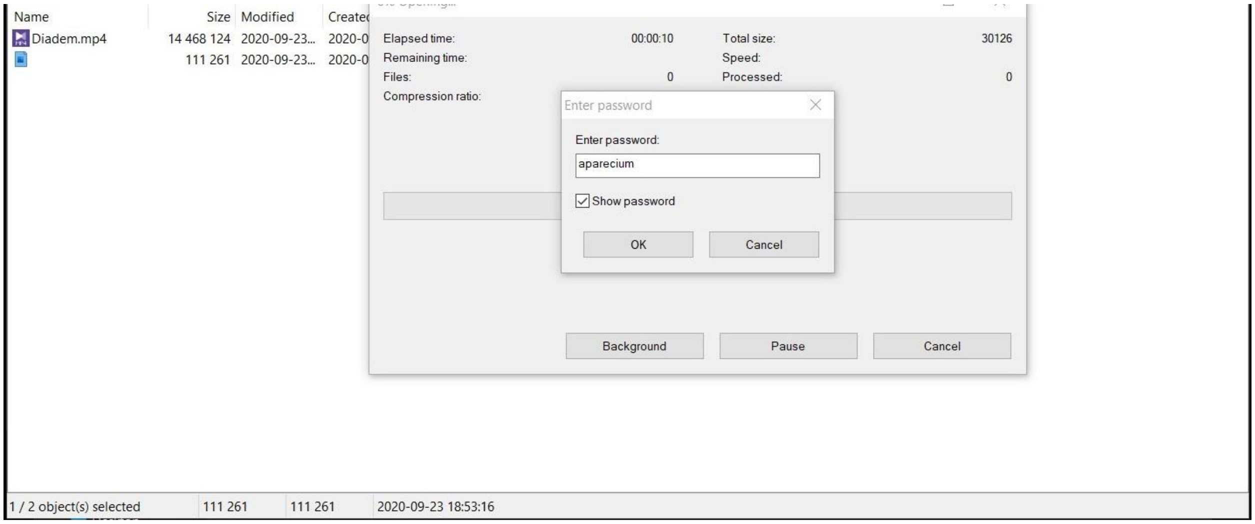
Enter password for the encrypted archive
Horcrux.rar

Enter password
diadem

☑ Show password

□ Use for all archives

This .zip file will have two files, one .mp4 file and another .jpg file. If explored with the 7 – Zip file manager, when opened, the .mp4 file will play a clip of the diadem being destroyed. However, if the .jpg file is opened, another password will be required. This means that a particular file has been concatenated with the image file. The password was mentioned in a previous level under steganography.



| Name | Size | Modified | Createc |
|---|---|---|---|
| Diadem.mp4 | 14 468 124 | 2020-09-23... | 2020-0 |
| | 111 261 | 2020-09-23... | 2020-0 |

Elapsed time: 00:00:10
Remaining time:
Files: 0
Compression ratio:

Total size: 30126
Speed:
Processed: 0

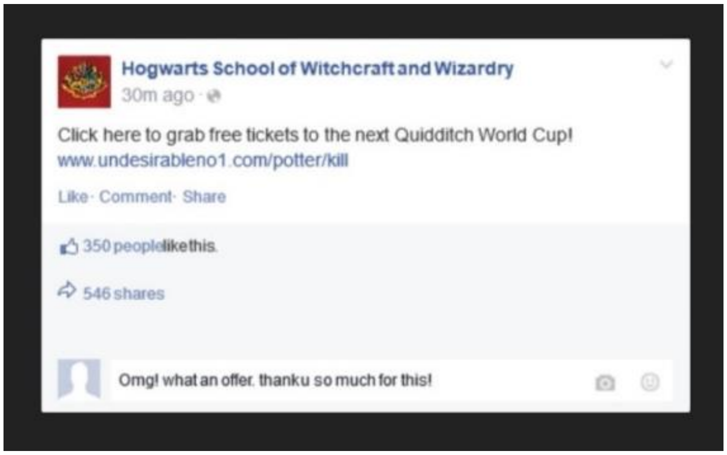
Enter password

Enter password:
aparecium

☑ Show password

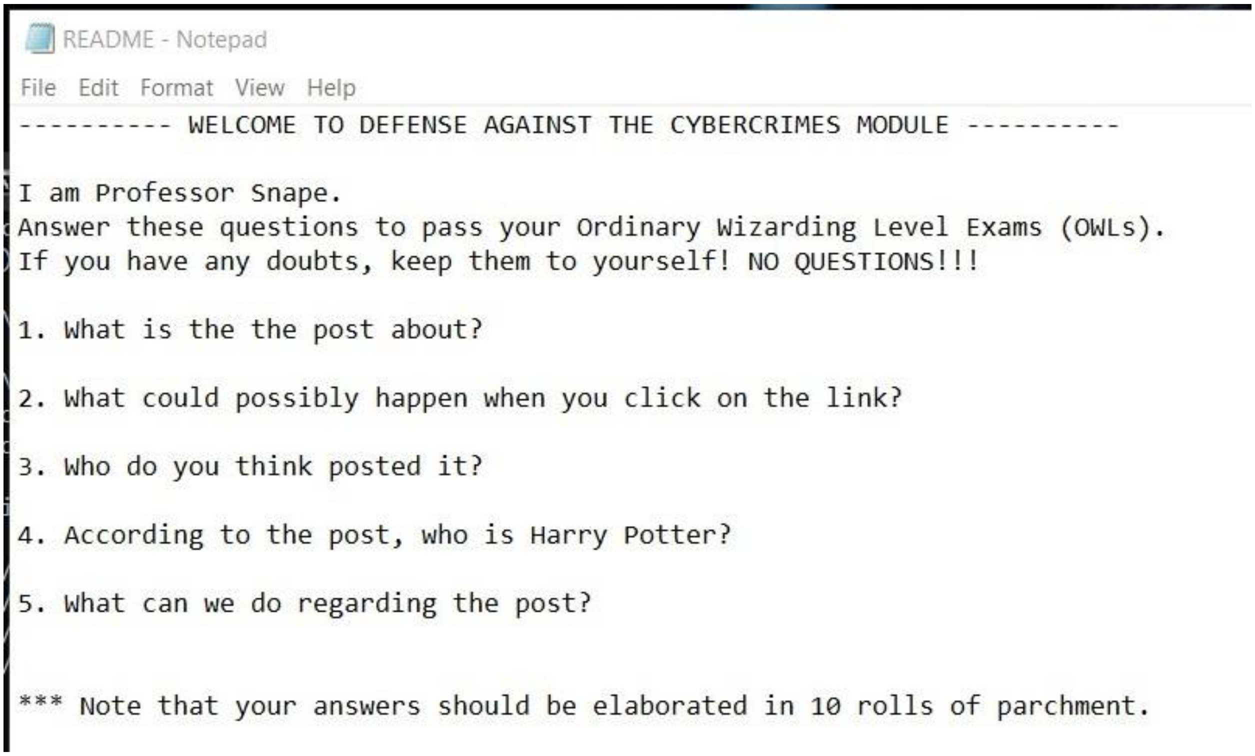
1 / 2 object(s) selected 111 261 111 261 2020-09-23 18:53:16

Once the password is entered, a new folder will be obtained. This folder will have another 3 files. It will have an image called "Click Me!.png", README.txt and ZIP2.rar. However, in order to extract the files from the .rar file, a password is required. This will be obtained by going through the other two files.



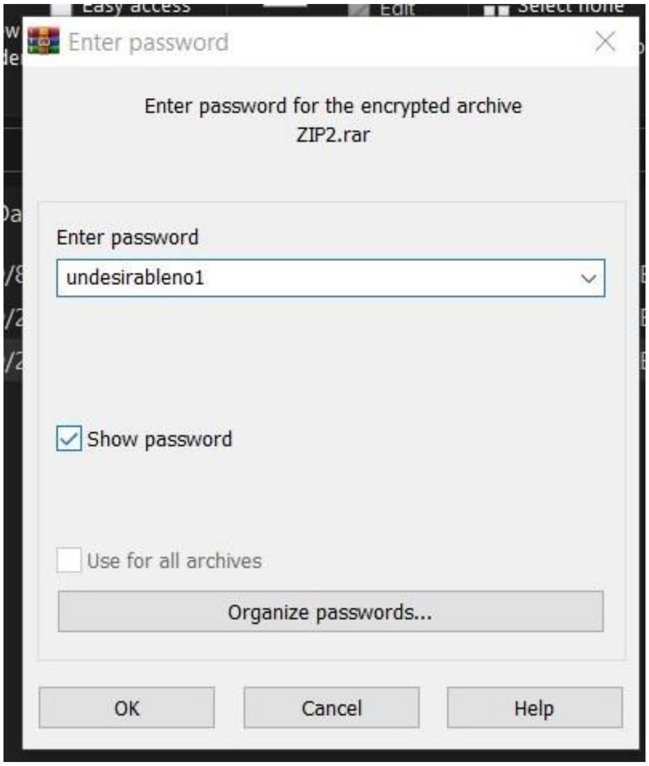
Hogwarts School of Witchcraft and Wizardry
30m ago

Click here to grab free tickets to the next Quidditch World Cup!
www.undesirableno1.com/potter/kill



```
---------- WELCOME TO DEFENSE AGAINST THE CYBERCRIMES MODULE ----------

I am Professor Snape.
Answer these questions to pass your Ordinary Wizarding Level Exams (OWLs).
If you have any doubts, keep them to yourself! NO QUESTIONS!!!

1. What is the the post about?

2. What could possibly happen when you click on the link?

3. Who do you think posted it?

4. According to the post, who is Harry Potter?

5. What can we do regarding the post?


*** Note that your answers should be elaborated in 10 rolls of parchment.
```

The player has to brute force the answers to the above questions with the help of the image and try to obtain the password of the .rar file.



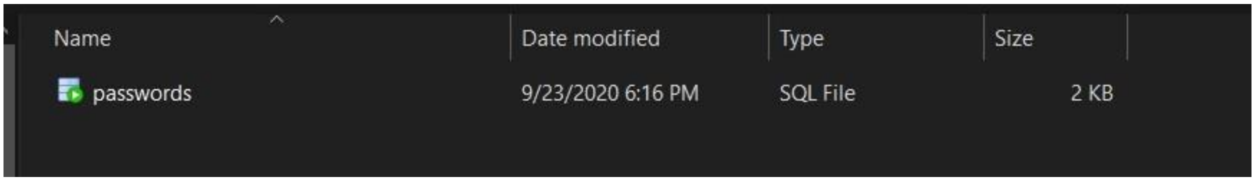
Enter password for the encrypted archive
ZIP2.rar

Enter password
undesirableno1

☑ Show password

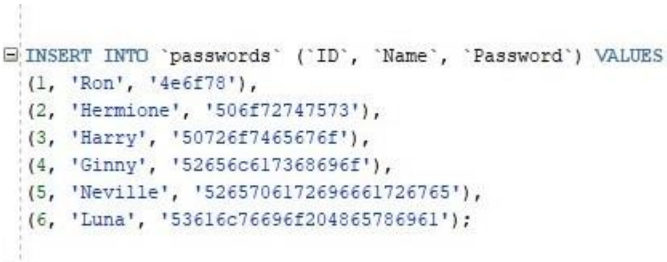
□ Use for all archives

Once unzipped, the new folder will have a file called passwords.sql.



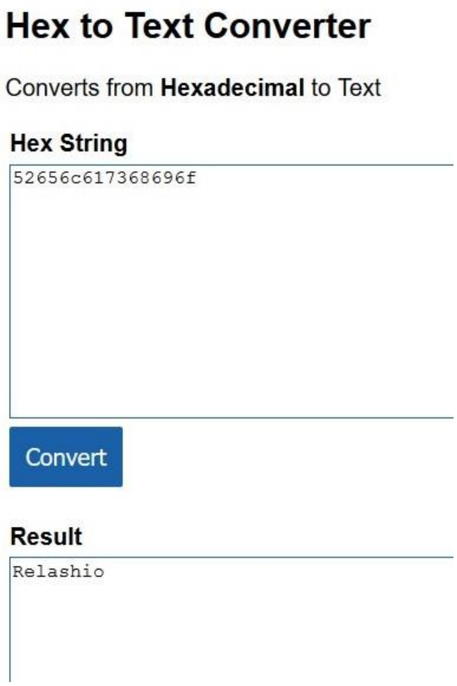
| Name | Date modified | Type | Size |
|---|---|---|---|
| passwords | 9/23/2020 6:16 PM | SQL File | 2 KB |

The player can import this script using any database management software and go through the queries.



```
INSERT INTO `passwords` (`ID`, `Name`, `Password`) VALUES
(1, 'Ron', '4e6f78'),
(2, 'Hermione', '506f72747573'),
(3, 'Harry', '50726f7465676f'),
(4, 'Ginny', '52656c617368696f'),
(5, 'Neville', '5265706172696661726765'),
(6, 'Luna', '53616c76696f204865786961');
```

The above part shows the queries used to enter the usernames and passwords to a database. As it can be seen, the passwords are saved as hexadecimal values. Hence, in order to obtain the flag, the player will have to convert all the hexadecimal values to text and brute force to obtain the flag.



Hex to Text Converter

Converts from **Hexadecimal** to Text

Hex String

```
52656c617368696f
```

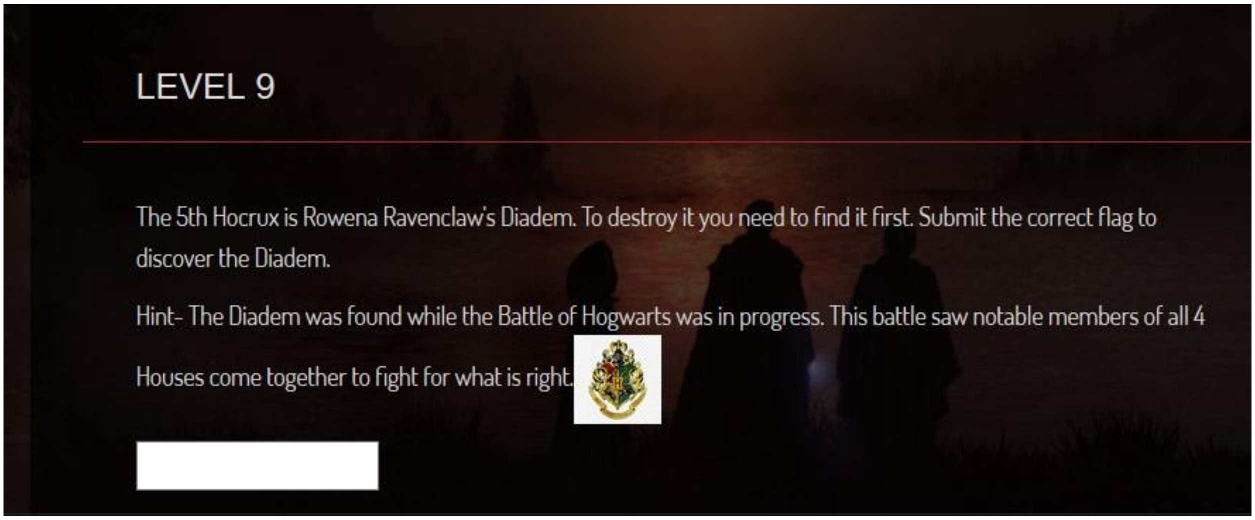
Result

```
Relashio
```

**FLAG: Relashio**

## LEVEL 10

Initially, the player will be navigated to this level after successful completion of the previous level.



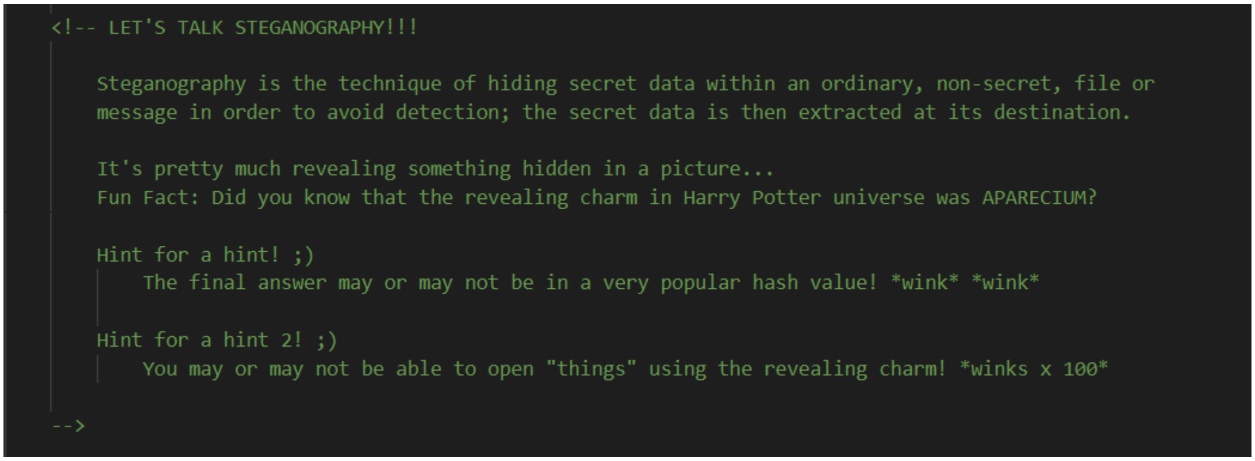
LEVEL 9

The 5th Hocrux is Rowena Ravenclaw's Diadem. To destroy it you need to find it first. Submit the correct flag to discover the Diadem.

Hint- The Diadem was found while the Battle of Hogwarts was in progress. This battle saw notable members of all 4 Houses come together to fight for what is right.

The hint suggests some facts about the 4 Houses. Right next to it is the image of the school crest which depicts all 4 Houses. The player can now save this image and perform steganography.

When performing steganography, a passphrase is required. However, this passphrase is revealed in a previous level as follows:

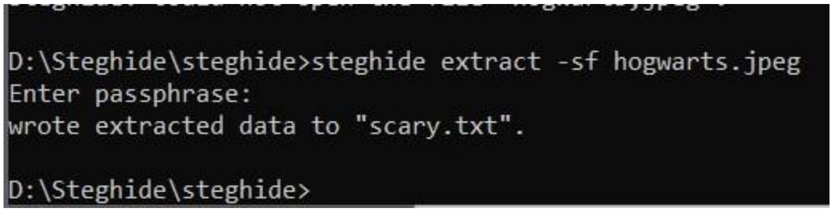


```
<!-- LET'S TALK STEGANOGRAPHY!!!

    Steganography is the technique of hiding secret data within an ordinary, non-secret, file or
    message in order to avoid detection; the secret data is then extracted at its destination.

    It's pretty much revealing something hidden in a picture...
    Fun Fact: Did you know that the revealing charm in Harry Potter universe was APARECIUM?

    Hint for a hint! ;)
        The final answer may or may not be in a very popular hash value! *wink* *wink*

    Hint for a hint 2! ;)
        You may or may not be able to open "things" using the revealing charm! *winks x 100*

-->
```

If this spell is given as the passphrase in all simple letters, the player can easily get the hidden text from the image.

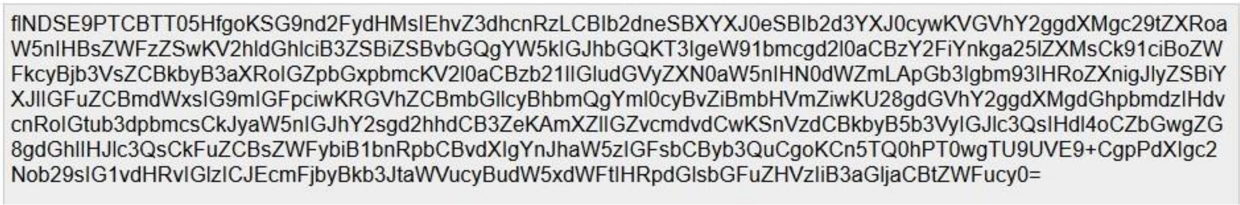
**The Passphrase: aparecium**

This image also gives another hint. It mentions that the final answer might be in a very popular hash value. Moving forward, the player is required to keep that in mind.

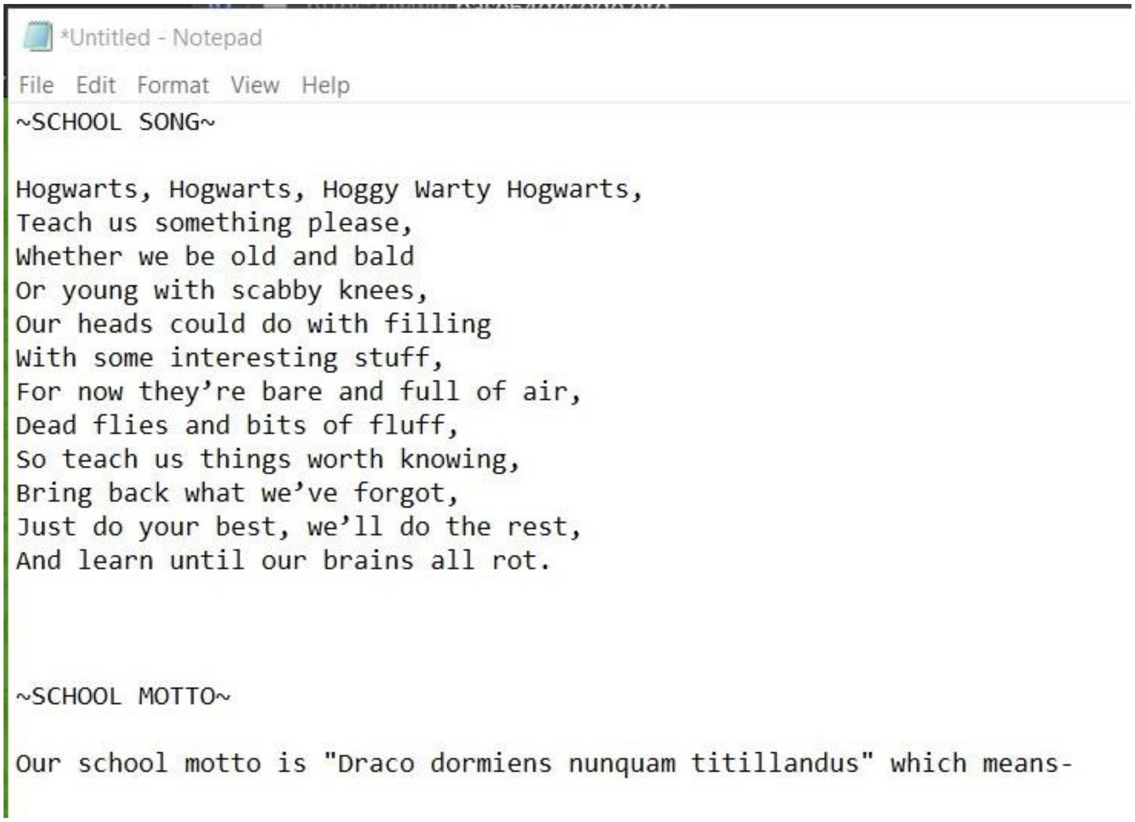


```
D:\Steghide\steghide>steghide extract -sf hogwarts.jpeg
Enter passphrase:
wrote extracted data to "scary.txt".

D:\Steghide\steghide>
```

Now, the player can see what the hidden message is by opening “scary.txt”. As it can be seen, the hidden message is base64 encoded. Therefore, the player can now decode it.

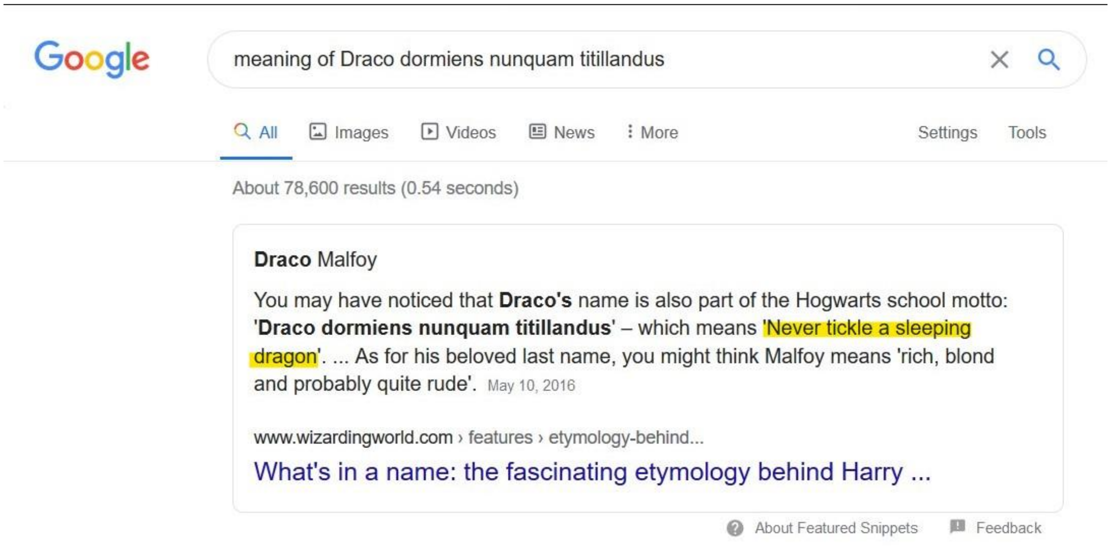


flNDSE9PTCBTT05HfgoKSG9nd2FydHMsIEhvZ3dhcnRzLCBIb2dneSBXYXJ0eSBIb2d3YXJ0cywKVGVhY2ggdXMgc29tZXRoa
W5nIHBsZWFzZSwKV2hldGhlciB3ZSBiZSBvbGQgYW5kIGJhbGQKT3IgeW91bmcgd2l0aCBzY2FiYnkga25lZXMsCk91ciBoZW
FkcyBjb3VsZCBkbyB3aXRoIGZpbGxpbmcKV2l0aCBzb21lIGludGVyZXN0aW5nIHN0dWZmLApGb3Igbm93IHRoZXnigJlyZSBiY
XJlIGFuZCBmdWxsIG9mIGFpciwKRGVhZCBmbGllcyBhbmQgYml0cyBvZiBmbHVmZiwKU28gdGVhY2ggdXMgdGhpbmdzIHdv
cnRoIGtub3dpbmcsCkJyaW5nIGJhY2sgd2hhdCB3ZeKAmXZlIGZvcmdvdCwKSnVzdCBkbyB5b3VyIGJlc3QsIHdl4oCZbGwgZG
8gdGhlIHJlc3QsCkFuZCBsZWFybiB1bnRpbCBvdXIgYnJhaW5zIGFsbCByb3QuCgoKCn5TQ0hPT0wgTU9UVE9+CgpPdXIgc2
Nob29sIG1vdHRvIGlzICJEcmFjbyBkb3JtaWVucyBudW5xdWFtIHRpdGlsbGFuZHVzIiB3aGljaCBtZWFucy0=



```
~SCHOOL SONG~

Hogwarts, Hogwarts, Hoggy Warty Hogwarts,
Teach us something please,
Whether we be old and bald
Or young with scabby knees,
Our heads could do with filling
With some interesting stuff,
For now they’re bare and full of air,
Dead flies and bits of fluff,
So teach us things worth knowing,
Bring back what we’ve forgot,
Just do your best, we’ll do the rest,
And learn until our brains all rot.



~SCHOOL MOTTO~

Our school motto is "Draco dormiens nunquam titillandus" which means-
```

As it can be seen, while typing the meaning of the school motto, the sentence has abruptly stopped. Therefore, the player can google the meaning of the school motto.



meaning of Draco dormiens nunquam titillandus

About 78,600 results (0.54 seconds)

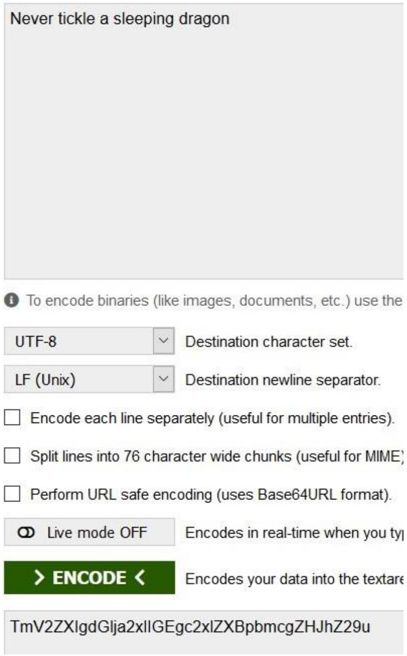
**Draco** Malfoy

You may have noticed that **Draco's** name is also part of the Hogwarts school motto: '**Draco dormiens nunquam titillandus**' – which means 'Never tickle a sleeping dragon'. ... As for his beloved last name, you might think Malfoy means 'rich, blond and probably quite rude'. May 10, 2016

www.wizardingworld.com › features › etymology-behind...

What's in a name: the fascinating etymology behind Harry ...

Now, the player can encode this meaning in base64 and hash it using MD5 to obtain the flag value.



Never tickle a sleeping dragon

To encode binaries (like images, documents, etc.) use the

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for multiple entries).

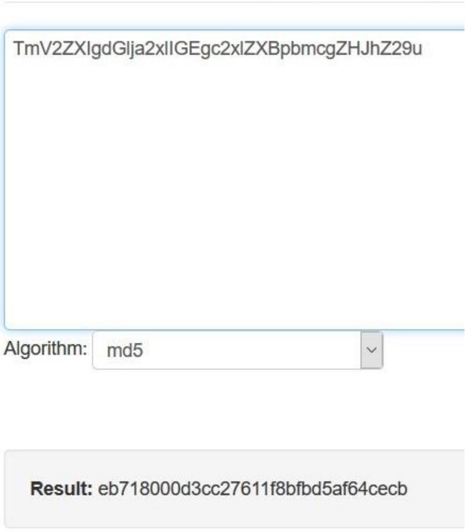
☐ Split lines into 76 character wide chunks (useful for MIME)

☐ Perform URL safe encoding (uses Base64URL format).

Live mode OFF Encodes in real-time when you ty

> ENCODE < Encodes your data into the textare

TmV2ZXIgdGlja2xlIGEgc2xlZXBpbmcgZHJhZ29u



TmV2ZXIgdGlja2xlIGEgc2xlZXBpbmcgZHJhZ29u

Algorithm: md5

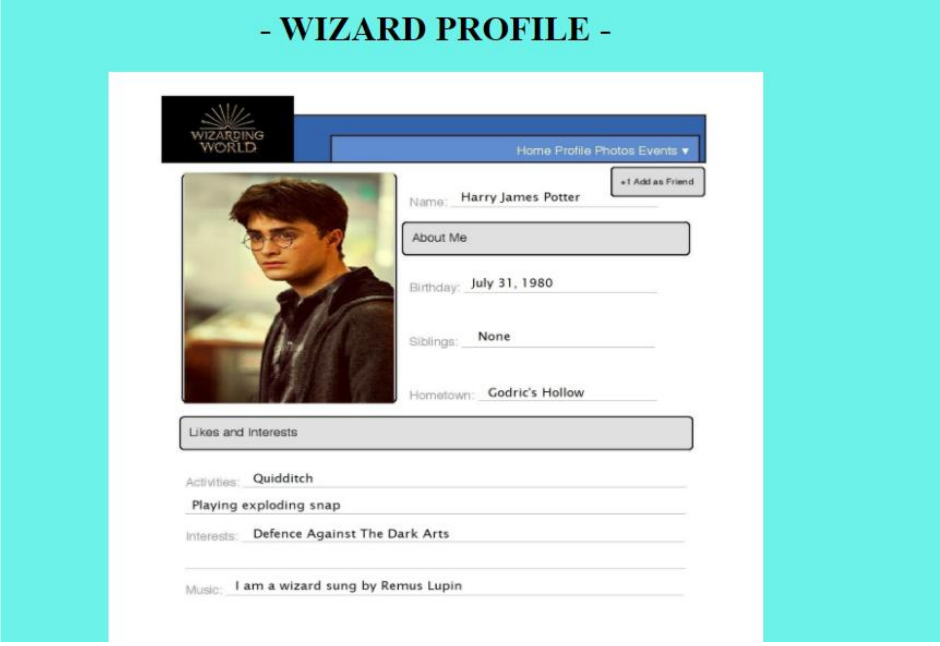
**Result:** eb718000d3cc27611f8bfbd5af64cecb

**The Encoded Value: TmV2ZXIgdGlja2xlIGEgc2xlZXBpbmcgZHJhZ29u**

**FLAG: eb718000d3cc27611f8bfbd5af64cecb**

## LEVEL 11

The social media profile of a user as given below could be obtained after clicking on the link.



- WIZARD PROFILE -

Name: Harry James Potter

About Me

Birthday: July 31, 1980

Siblings: None

Hometown: Godric's Hollow

Likes and Interests

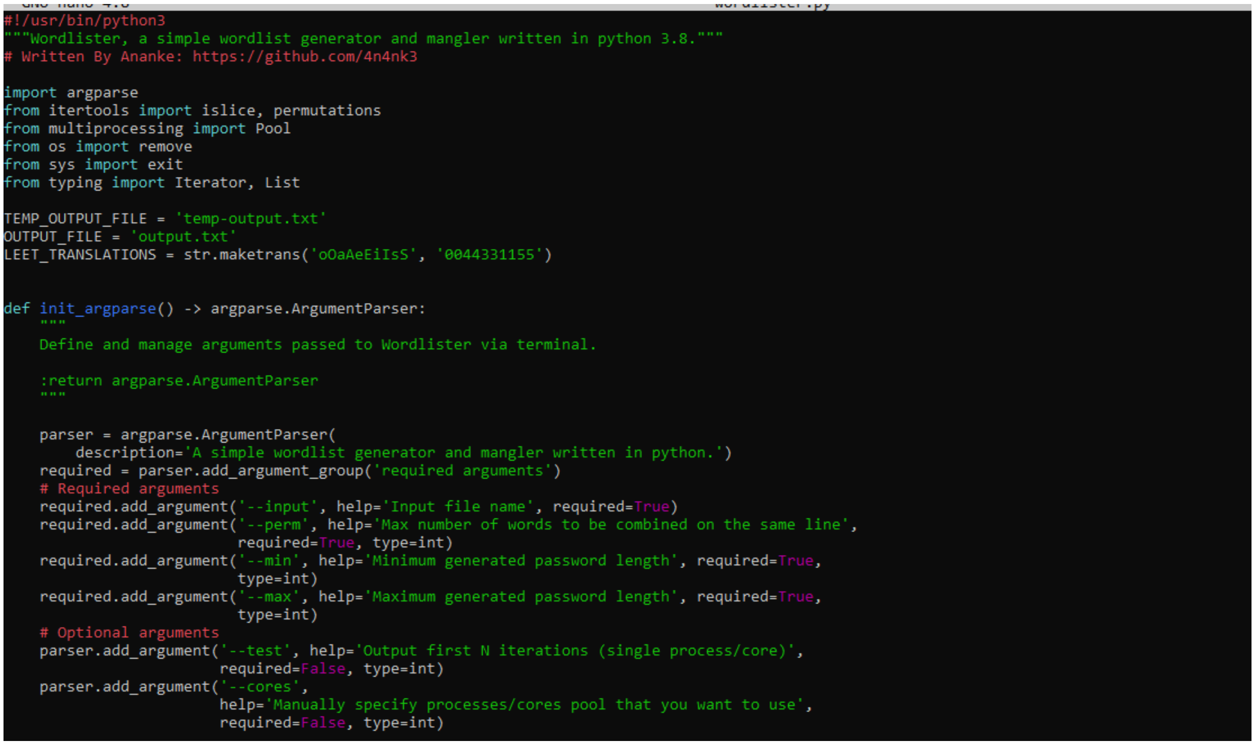
Activities: Quidditch

Playing exploding snap

Interests: Defence Against The Dark Arts

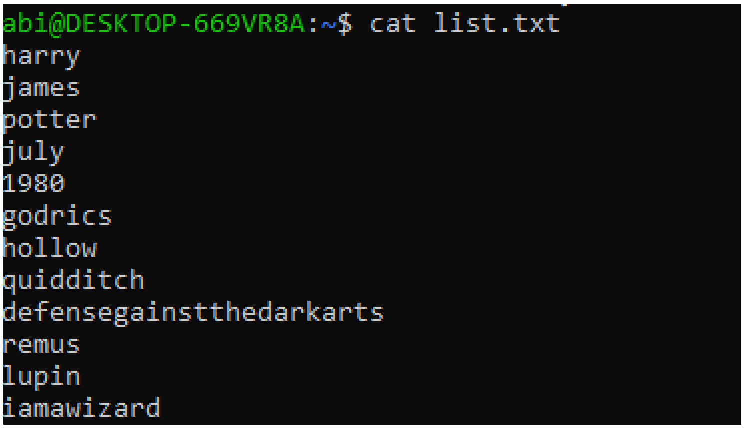
Music: I am a wizard sung by Remus Lupin

This provides some important personal details about the user which can be utilized in order to guess his password. Most users still tend to use their favorite people, dates, towns, birthdays and names as their passwords. The player has to input the user's personal details to a word-lister program. The word-lister given in [https://null-byte.wonderhowto.com/how-to/use-wordlister-create-custom-password-combinations-for-cracking-0206006/](https://null-byte.wonderhowto.com/how-to/use-wordlister-create-custom-password-combinations-for-cracking-0206006/) is used here.



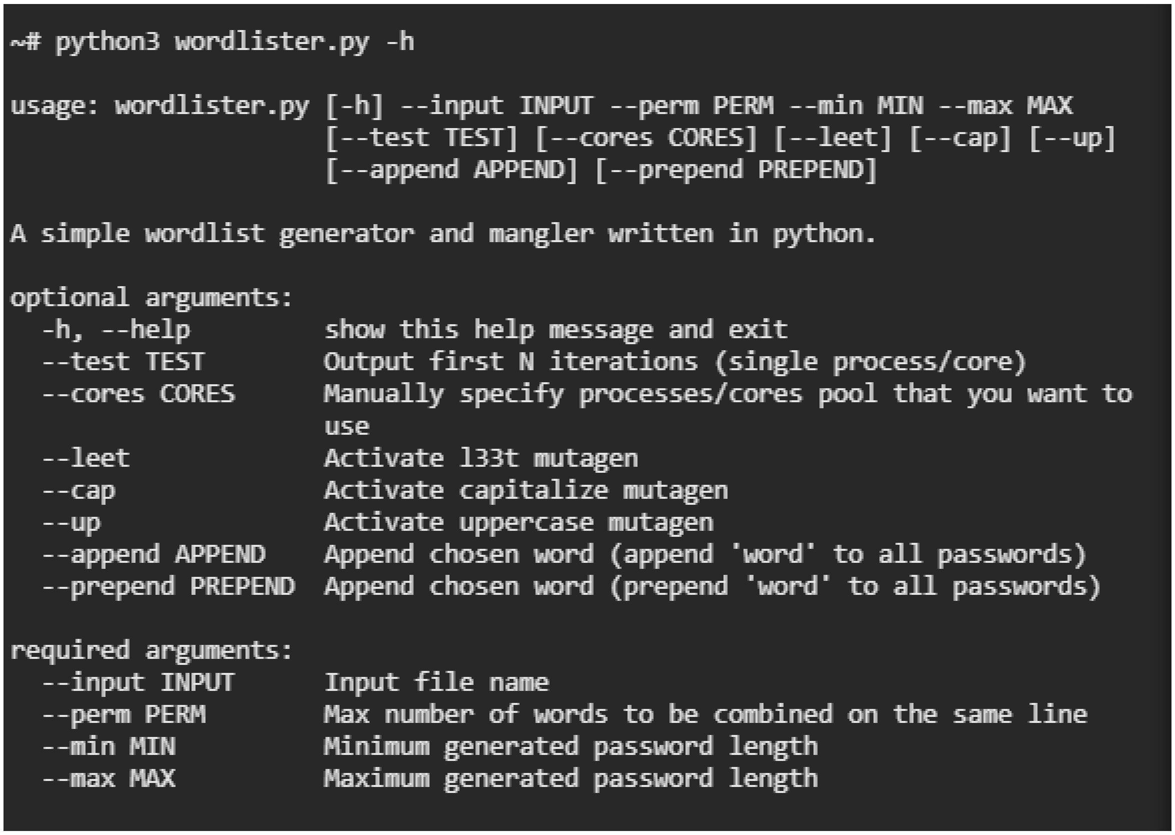
```
  GNU nano 4.8                                                    wordlister.py
#!/usr/bin/python3
"""Wordlister, a simple wordlist generator and mangler written in python 3.8."""
# Written By Ananke: https://github.com/4n4nk3

import argparse
from itertools import islice, permutations
from multiprocessing import Pool
from os import remove
from sys import exit
from typing import Iterator, List

TEMP_OUTPUT_FILE = 'temp-output.txt'
OUTPUT_FILE = 'output.txt'
LEET_TRANSLATIONS = str.maketrans('oOaAeEiIsS', '0044331155')


def init_argparse() -> argparse.ArgumentParser:
    """
    Define and manage arguments passed to Wordlister via terminal.

    :return argparse.ArgumentParser
    """

    parser = argparse.ArgumentParser(
        description='A simple wordlist generator and mangler written in python.')
    required = parser.add_argument_group('required arguments')
    # Required arguments
    required.add_argument('--input', help='Input file name', required=True)
    required.add_argument('--perm', help='Max number of words to be combined on the same line',
                          required=True, type=int)
    required.add_argument('--min', help='Minimum generated password length', required=True,
                          type=int)
    required.add_argument('--max', help='Maximum generated password length', required=True,
                          type=int)
    # Optional arguments
    parser.add_argument('--test', help='Output first N iterations (single process/core)',
                        required=False, type=int)
    parser.add_argument('--cores',
                        help='Manually specify processes/cores pool that you want to use',
                        required=False, type=int)
```

This is a list which includes all personal information of the user given in the profile.



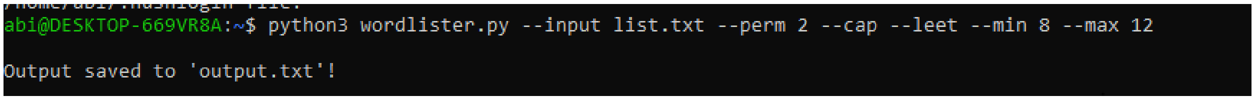
```
abi@DESKTOP-669VR8A:~$ cat list.txt
harry
james
potter
july
1980
godrics
hollow
quidditch
defensegainstthedarkarts
remus
lupin
iamawizard
```

Now, possible passwords can be generated. The following arguments can be used for this purpose:



```
~# python3 wordlister.py -h

usage: wordlister.py [-h] --input INPUT --perm PERM --min MIN --max MAX
                     [--test TEST] [--cores CORES] [--leet] [--cap] [--up]
                     [--append APPEND] [--prepend PREPEND]

A simple wordlist generator and mangler written in python.

optional arguments:
  -h, --help          show this help message and exit
  --test TEST         Output first N iterations (single process/core)
  --cores CORES       Manually specify processes/cores pool that you want to
                      use
  --leet              Activate l33t mutagen
  --cap               Activate capitalize mutagen
  --up                Activate uppercase mutagen
  --append APPEND     Append chosen word (append 'word' to all passwords)
  --prepend PREPEND   Append chosen word (prepend 'word' to all passwords)

required arguments:
  --input INPUT       Input file name
  --perm PERM         Max number of words to be combined on the same line
  --min MIN           Minimum generated password length
  --max MAX           Maximum generated password length
```

Since the hint says “The Wizarding World's password policy states that passwords must contain at least 8 characters and maximum 12 characters and should contain at least 1 number.”, the player can use these arguments accordingly.



```
abi@DESKTOP-669VR8A:~$ python3 wordlister.py --input list.txt --perm 2 --cap --leet --min 8 --max 12

Output saved to 'output.txt'!
```

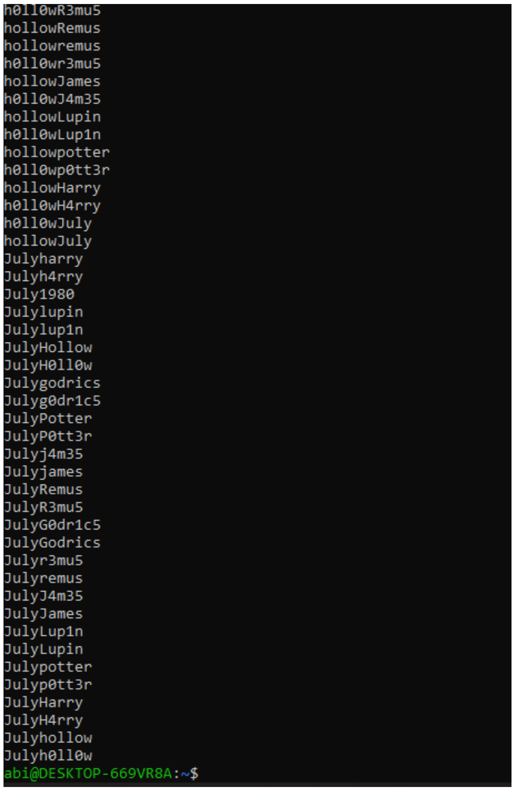
Since the maximum number of characters is 12, two permutations can be used as follows:

--leet used to transform any letters into numbers

--min 8 = minimum number of characters is 8

--max 12 = maximum number of characters 12

These are the generated passwords. There are 483 passwords here. The player can use manual brute forcing or a brute forcing tool to try passwords till they get the message saying flag is correct.

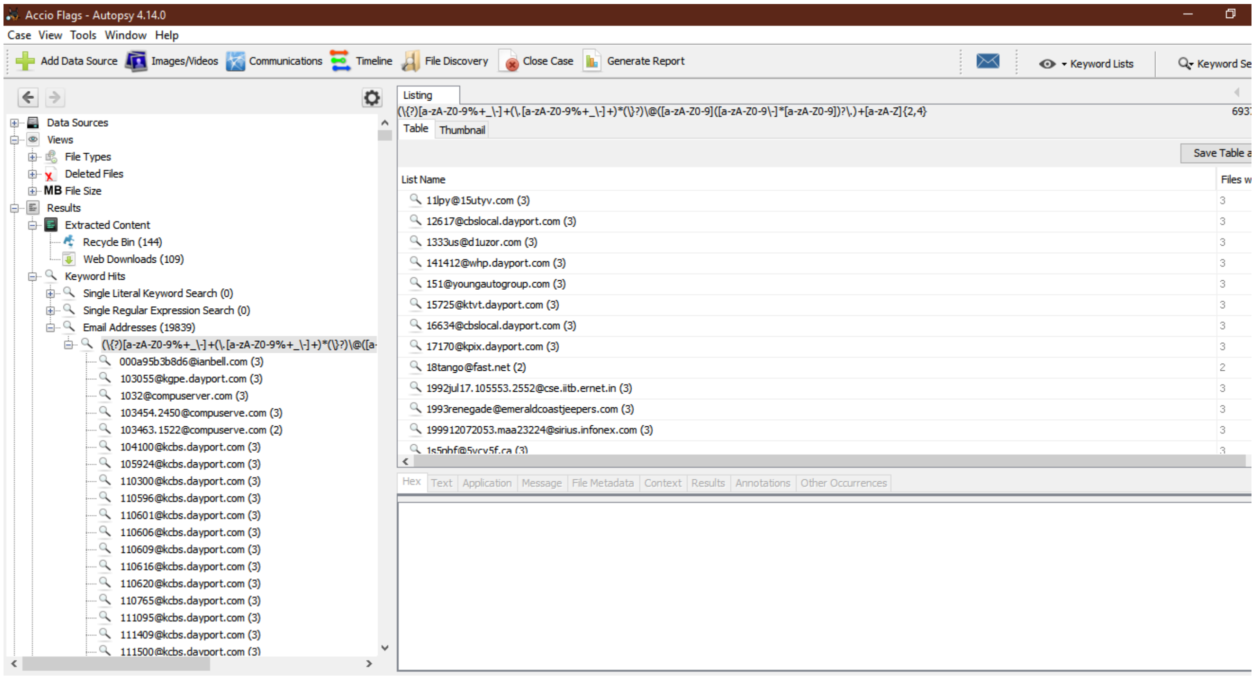


```
h0ll0wR3mu5
hollowRemus
hollowremus
h0ll0wr3mu5
hollowJames
h0ll0wJ4m35
hollowLupin
h0ll0wLup1n
hollowpotter
h0ll0wp0tt3r
hollowHarry
h0ll0wH4rry
h0ll0wJuly
hollowJuly
Julyharry
Julyh4rry
July1980
Julylupin
Julylup1n
JulyHollow
JulyH0ll0w
Julygodrics
Julyg0dr1c5
JulyPotter
JulyP0tt3r
Julyj4m35
Julyjames
JulyRemus
JulyR3mu5
JulyG0dr1c5
JulyGodrics
Julyr3mu5
Julyremus
JulyJ4m35
JulyJames
JulyLup1n
JulyLupin
Julypotter
Julyp0tt3r
JulyHarry
JulyH4rry
Julyhollow
Julyh0ll0w
abi@DESKTOP-669VR8A:~$
```

**FLAG: g0dr1c5r3mu5**

## LEVEL 12

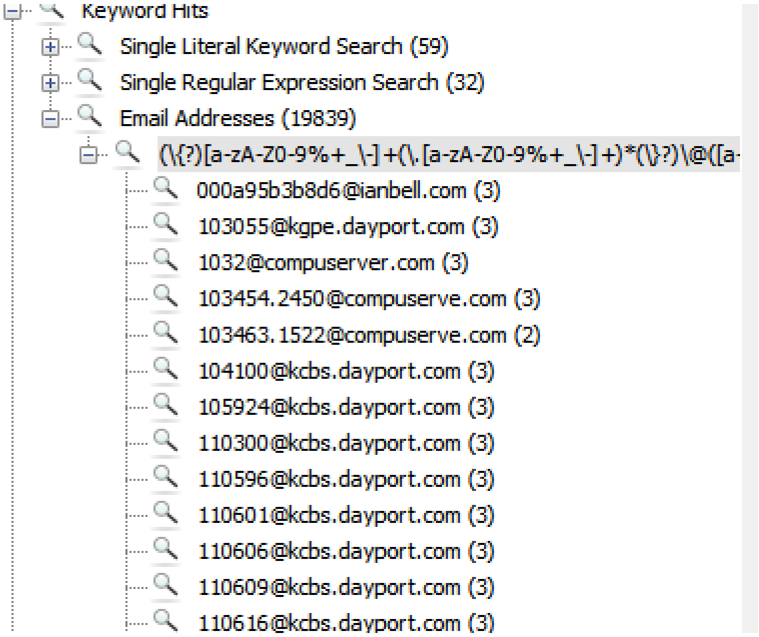
The player is given a .vhd file to download once they click on the link provided. The Virtual Hard Disk needs to be opened by Autopsy and analyzed for suspicious material. The player can use the plugins in Autopsy to search through the contents on the .vhd file for emails. The following image shows the emails found:



```
Data Sources
Views
    File Types
    Deleted Files
    MB File Size
Results
    Extracted Content
        Recycle Bin (144)
        Web Downloads (109)
    Keyword Hits
        Single Literal Keyword Search (0)
        Single Regular Expression Search (0)
        Email Addresses (19839)
            (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-
                000a95b3b8d6@ianbell.com (3)
                103055@kgpe.dayport.com (3)
                1032@compuserver.com (3)
                103454.2450@compuserve.com (3)
                103463.1522@compuserve.com (2)
                104100@kcbs.dayport.com (3)
                105924@kcbs.dayport.com (3)
                110300@kcbs.dayport.com (3)
                110596@kcbs.dayport.com (3)
                110601@kcbs.dayport.com (3)
                110606@kcbs.dayport.com (3)
                110609@kcbs.dayport.com (3)
                110616@kcbs.dayport.com (3)
                110620@kcbs.dayport.com (3)
                110765@kcbs.dayport.com (3)
                111095@kcbs.dayport.com (3)
                111409@kcbs.dayport.com (3)
                111500@kcbs.dayport.com (3)
```

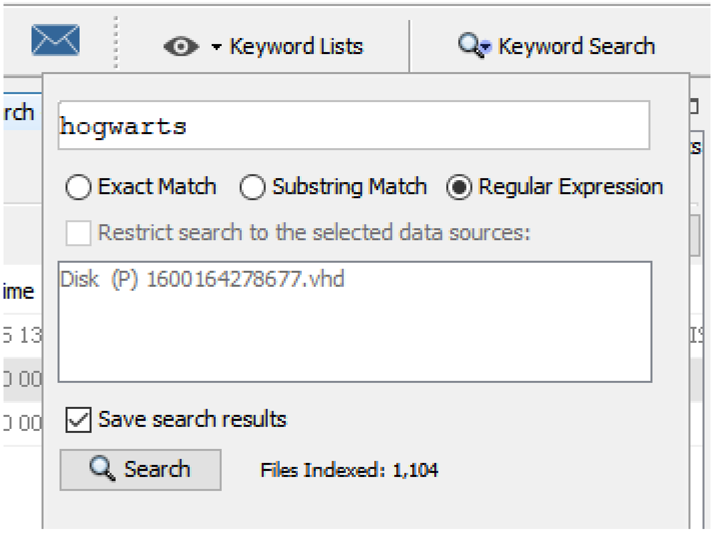
(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4} 693

| List Name | Files w |
|---|---|
| 11lpy@15utyv.com (3) | 3 |
| 12617@cbslocal.dayport.com (3) | 3 |
| 1333us@d1uzor.com (3) | 3 |
| 141412@whp.dayport.com (3) | 3 |
| 151@youngautogroup.com (3) | 3 |
| 15725@ktvt.dayport.com (3) | 3 |
| 16634@cbslocal.dayport.com (3) | 3 |
| 17170@kpix.dayport.com (3) | 3 |
| 18tango@fast.net (2) | 2 |
| 1992jul17.105553.2552@cse.iitb.ernet.in (3) | 3 |
| 1993renegade@emeraldcoastjeepers.com (3) | 3 |
| 199912072053.maa23224@sirius.infonex.com (3) | 3 |
| 1s5pbf@5vcv5f.ca (3) | 3 |



```
Keyword Hits
    Single Literal Keyword Search (59)
    Single Regular Expression Search (32)
    Email Addresses (19839)
        (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-
            000a95b3b8d6@ianbell.com (3)
            103055@kgpe.dayport.com (3)
            1032@compuserver.com (3)
            103454.2450@compuserve.com (3)
            103463.1522@compuserve.com (2)
            104100@kcbs.dayport.com (3)
            105924@kcbs.dayport.com (3)
            110300@kcbs.dayport.com (3)
            110596@kcbs.dayport.com (3)
            110601@kcbs.dayport.com (3)
            110606@kcbs.dayport.com (3)
            110609@kcbs.dayport.com (3)
            110616@kcbs.dayport.com (3)
```

There are 19, 839 emails in this file. It would be time consuming to try each and every email address to find the correct flag. However, since the email belongs to a former employee at Hogwarts, it is likely that the email takes the format username@hogwarts.com or username@hogwarts.edu. Therefore, the player can use the keyword search to search for the expression "hogwarts".



hogwarts

○ Exact Match ○ Substring Match ● Regular Expression

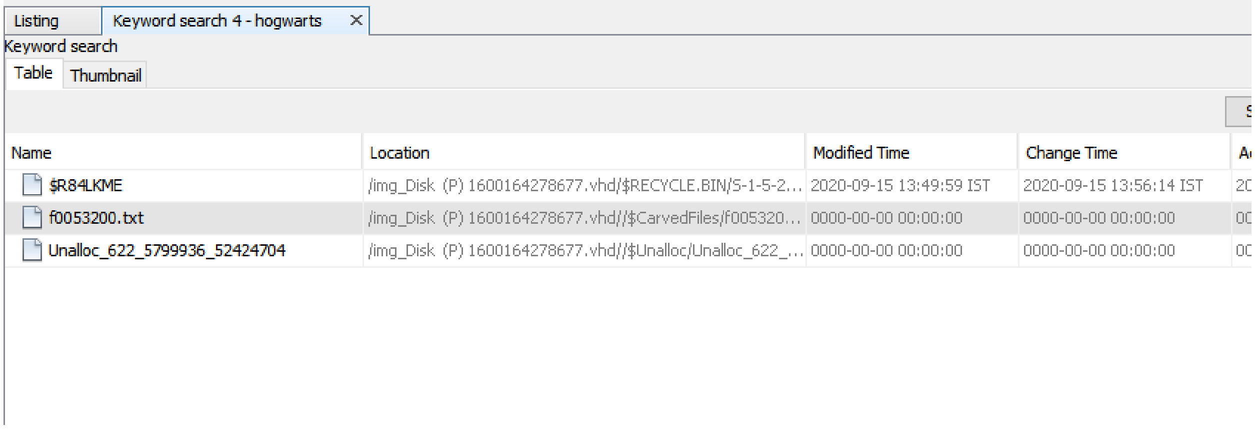
□ Restrict search to the selected data sources:

Disk (P) 1600164278677.vhd

☑ Save search results

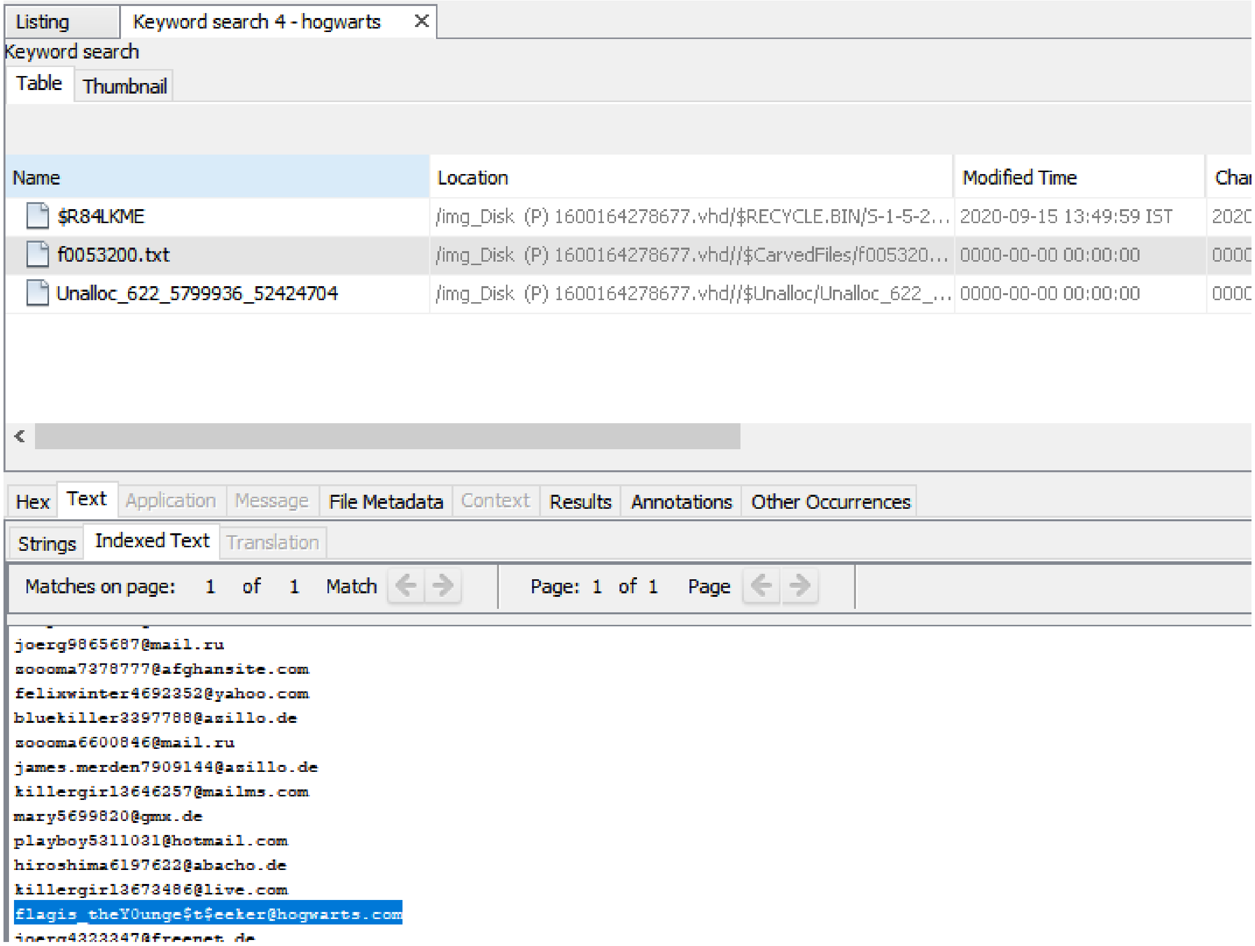
Files Indexed: 1,104

There are 3 results:



| Name | Location | Modified Time | Change Time | A |
|---|---|---|---|---|
| $R84LKME | /img_Disk (P) 1600164278677.vhd/$RECYCLE.BIN/S-1-5-2... | 2020-09-15 13:49:59 IST | 2020-09-15 13:56:14 IST | 20 |
| f0053200.txt | /img_Disk (P) 1600164278677.vhd//$CarvedFiles/f005320... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 00 |
| Unalloc_622_5799936_52424704 | /img_Disk (P) 1600164278677.vhd//$Unalloc/Unalloc_622_... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 00 |

The player can now check the .txt file.



| Name | Location | Modified Time | Char |
|---|---|---|---|
| $R84LKME | /img_Disk (P) 1600164278677.vhd/$RECYCLE.BIN/S-1-5-2… | 2020-09-15 13:49:59 IST | 2020 |
| f0053200.txt | /img_Disk (P) 1600164278677.vhd//$CarvedFiles/f005320… | 0000-00-00 00:00:00 | 0000 |
| Unalloc_622_5799936_52424704 | /img_Disk (P) 1600164278677.vhd//$Unalloc/Unalloc_622_… | 0000-00-00 00:00:00 | 0000 |

Matches on page: 1 of 1 Match

Page: 1 of 1 Page

```
joerg9865687@mail.ru
sooomа7378777@afghansite.com
felixwinter4692352@yahoo.com
bluekiller3397788@asillo.de
sooomа6600846@mail.ru
james.merden7909144@asillo.de
killergirl3646257@mailms.com
mary5699820@gmx.de
playboy5311031@hotmail.com
hiroshima6197622@abacho.de
killergirl3673486@live.com
flagis_theY0unge$t$eeker@hogwarts.com
joerg4323347@freenet.de
```

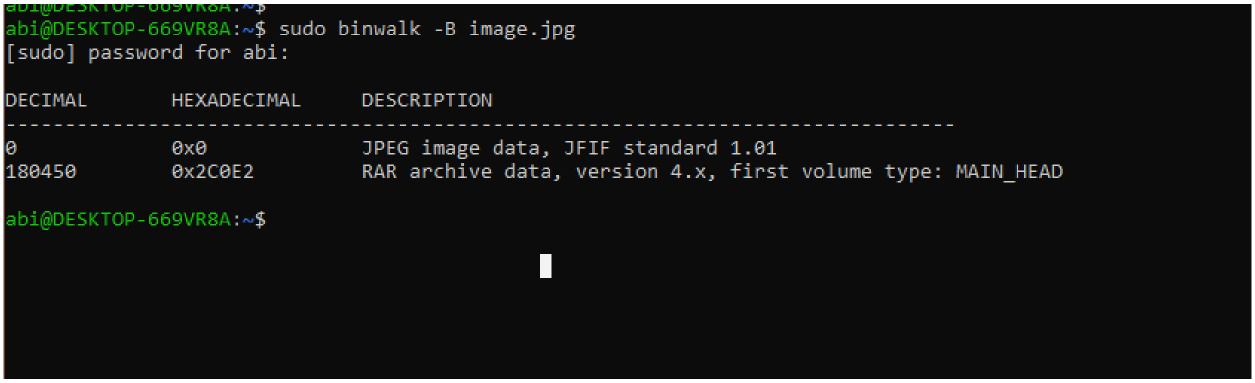
The player can see that there is an email that looks very much like the flag.

**FLAG: flagis_theY0unge$t$eeker@hogwarts.com**

## LEVEL 13

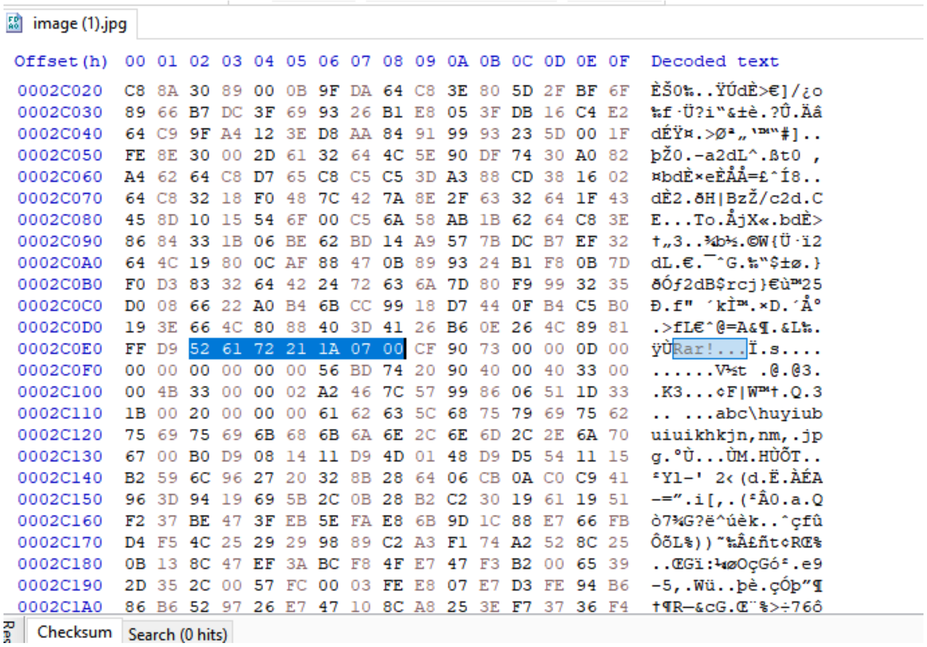
The players need to follow the mega.nz link given and download the image file. It is a simple .jpeg file containing an image of Julius Caesar. Although the image looks random it will be needed to find the flag.

Since image files can be used to hide files, the first step is to scan the file for known file signatures. For that Binwalk tool can be used



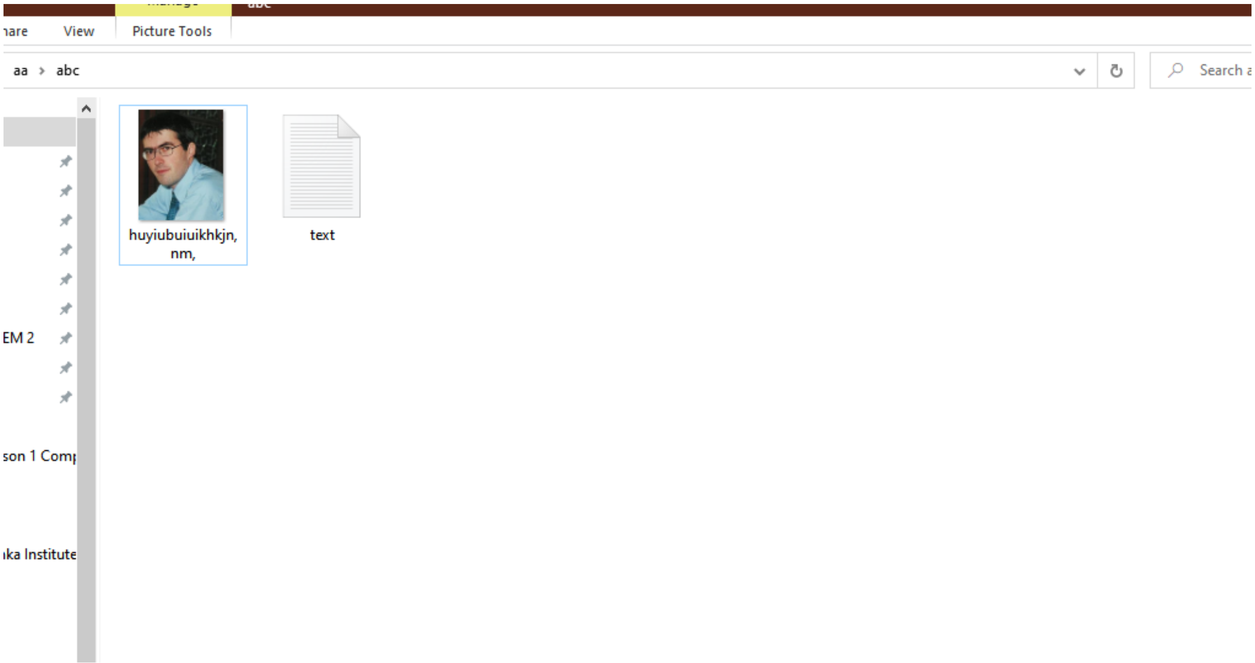
```
abi@DESKTOP-669VR8A:~$
abi@DESKTOP-669VR8A:~$ sudo binwalk -B image.jpg
[sudo] password for abi:

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
180450        0x2C0E2         RAR archive data, version 4.x, first volume type: MAIN_HEAD

abi@DESKTOP-669VR8A:~$
```

The scan says that there is .rar archive data inside the image file. Another method to find this is by examining the file through a hex editor. When searching for known file signature hex values, players can find out the value for .rar files which is 52 61 72 21 1A 07 00.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

0002C020  C8 8A 30 89 00 0B 9F DA 64 C8 3E 80 5D 2F BF 6F  ÈŠ0‰..ŸÚdÈ>€]/¿o
0002C030  89 66 B7 DC 3F 69 93 26 B1 E8 05 3F DB 16 C4 E2  ‰f·Ü?i“&±è.?Û.Äâ
0002C040  64 C9 9F A4 12 3E D8 AA 84 91 99 93 23 5D 00 1F  dÉŸ¤.>Øª„‘™“#]..
0002C050  FE 8E 30 00 2D 61 32 64 4C 5E 90 DF 74 30 A0 82  þŽ0.-a2dL^.ßt0 ‚
0002C060  A4 62 64 C8 D7 65 C8 C5 C5 3D A3 88 CD 38 16 02  ¤bdÈ×eÈÅÅ=£ˆÍ8..
0002C070  64 C8 32 18 F0 48 7C 42 7A 8E 2F 63 32 64 1F 43  dÈ2.ðH|BzŽ/c2d.C
0002C080  45 8D 10 15 54 6F 00 C5 6A 58 AB 1B 62 64 C8 3E  E...To.ÅjX«.bdÈ>
0002C090  86 84 33 1B 06 BE 62 BD 14 A9 57 7B DC B7 EF 32  †„3..¾b½.©W{Ü·ï2
0002C0A0  64 4C 19 80 0C AF 88 47 0B 89 93 24 B1 F8 0B 7D  dL.€.¯ˆG.‰“$±ø.}
0002C0B0  F0 D3 83 32 64 42 24 72 63 6A 7D 80 F9 99 32 35  ðÓƒ2dB$rcj}€ù™25
0002C0C0  D0 08 66 22 A0 B4 6B CC 99 18 D7 44 0F B4 C5 B0  Ð.f" ´kÌ™.×D.´Å°
0002C0D0  19 3E 66 4C 80 88 40 3D 41 26 B6 0E 26 4C 89 81  .>fL€ˆ@=A&¶.&L‰.
0002C0E0  FF D9 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00  ÿÙRar!...Ï.s....
0002C0F0  00 00 00 00 00 00 56 BD 74 20 90 40 00 40 33 00  ......V½t .@.@3.
0002C100  00 4B 33 00 00 02 A2 46 7C 57 99 86 06 51 1D 33  .K3...¢F|W™†.Q.3
0002C110  1B 00 20 00 00 00 61 62 63 5C 68 75 79 69 75 62  .. ...abc\huyiub
0002C120  75 69 75 69 6B 68 6B 6A 6E 2C 6E 6D 2C 2E 6A 70  uiuikhkjn,nm,.jp
0002C130  67 00 B0 D9 08 14 11 D9 4D 01 48 D9 D5 54 11 15  g.°Ù...ÙM.HÙÕT..
0002C140  B2 59 6C 96 27 20 32 8B 28 64 06 CB 0A C0 C9 41  ²Yl–' 2‹(d.Ë.ÀÉA
0002C150  96 3D 94 19 69 5B 2C 0B 28 B2 C2 30 19 61 19 51  –=”.i[,.(²Â0.a.Q
0002C160  F2 37 BE 47 3F EB 5E FA E8 6B 9D 1C 88 E7 66 FB  ò7¾G?ë^úèk..ˆçfû
0002C170  D4 F5 4C 25 29 29 98 89 C2 A3 F1 74 A2 52 8C 25  ÔõL%))˜‰Â£ñt¢RŒ%
0002C180  0B 13 8C 47 EF 3A BC F8 4F E7 47 F3 B2 00 65 39  ..ŒGï:¼øOçGó².e9
0002C190  2D 35 2C 00 57 FC 00 03 FE E8 07 E7 D3 FE 94 B6  -5,.Wü..þè.çÓþ”¶
0002C1A0  86 B6 52 97 26 E7 47 10 8C A8 25 3E F7 37 36 F4  †¶R—&çG.Œ¨%>÷76ô
```

Now, the player can open this using WINRAR or any other archive extracting tools.



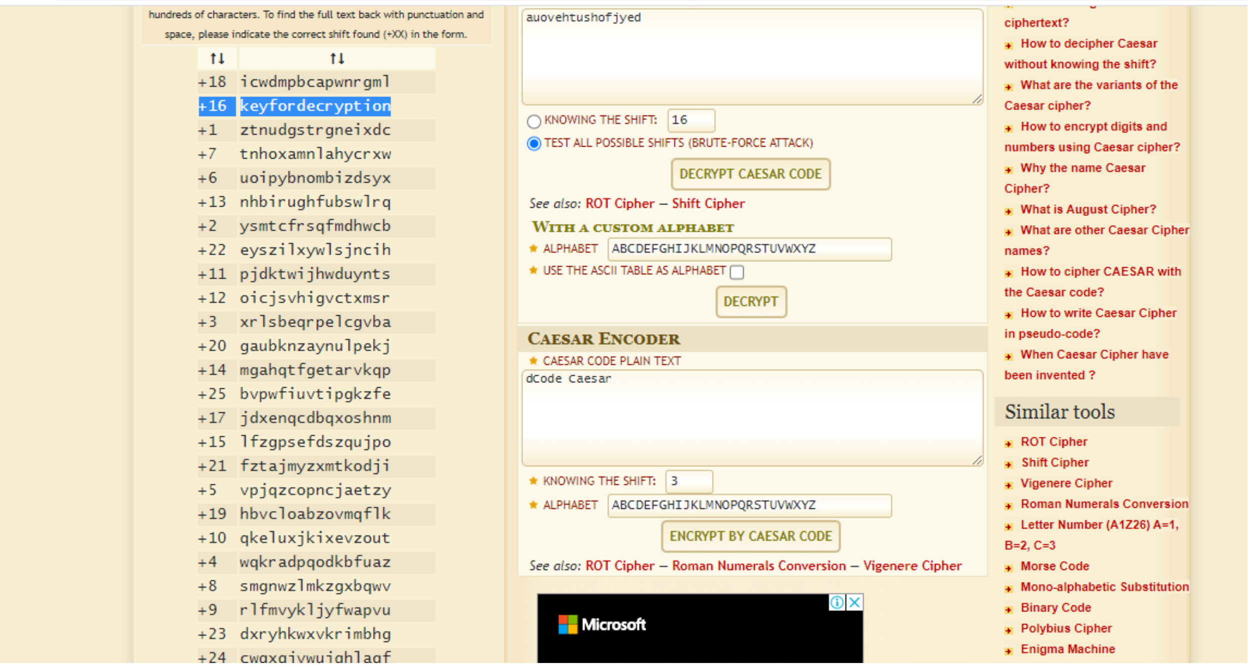
There are 2 files inside the .rar file. One is an image file. By doing a reverse image search, it can be found out that it is an image of Joan Daemen who is the founder of AES. This is a hint that should be noted.

The text file has 2 strings:

**82MXpG3RMdIW+Lc7r+ulLw==**

**Auovehtushofjyed**

The first string is a cipher text encrypted with AES, hence the hint was given by providing Joan Daemen's photo. The second string is encrypted using Caesar cipher and hence Caesar's image was given as a hint. The player can brute force Caesar cipher encrypted string and find the plaintext.



hundreds of characters. To find the full text back with punctuation and space, please indicate the correct shift found (+XX) in the form.

| ↑↓ | ↑↓ |
|---|---|
| +18 | icwdmpbcapwnrgml |
| +16 | keyfordecryption |
| +1 | ztnudgstrgneixdc |
| +7 | tnhoxamnlahycrxw |
| +6 | uoipybnombizdsyx |
| +13 | nhbirughfubswlrq |
| +2 | ysmtcfrsqfmdhwcb |
| +22 | eyszilxywlsjncih |
| +11 | pjdktwijhwduynts |
| +12 | oicjsvhigvctxmsr |
| +3 | xrlsbeqrpelcgvba |
| +20 | gaubknzaynulpekj |
| +14 | mgahqtfgetarvkqp |
| +25 | bvpwfiuvtipgkzfe |
| +17 | jdxenqcdbqxoshnm |
| +15 | lfzgpsefdszqujpo |
| +21 | fztajmyzxmtkodji |
| +5 | vpjqzcopncjaetzy |
| +19 | hbvcloabzovmqflk |
| +10 | qkeluxjkixevzout |
| +4 | wqkradpqodkbfuaz |
| +8 | smgnwzlmkzgxbqwv |
| +9 | rlfmvykljyfwapvu |
| +23 | dxryhkwxvkrimbhg |
| +24 | cwqxgivwuighlagf |

auovehtushofjyed

○ KNOWING THE SHIFT: 16

● TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)

DECRYPT CAESAR CODE

*See also:* ROT Cipher – Shift Cipher

**With a custom alphabet**

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ USE THE ASCII TABLE AS ALPHABET □

DECRYPT

**Caesar Encoder**

★ CAESAR CODE PLAIN TEXT

dCode Caesar

★ KNOWING THE SHIFT: 3

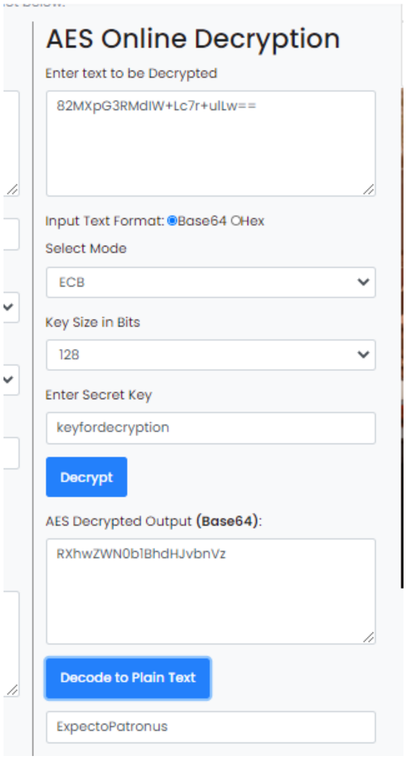
★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

ENCRYPT BY CAESAR CODE

*See also:* ROT Cipher – Roman Numerals Conversion – Vigenere Cipher

Microsoft
ciphertext?
How to decipher Caesar without knowing the shift?
What are the variants of the Caesar cipher?
How to encrypt digits and numbers using Caesar cipher?
Why the name Caesar Cipher?
What is August Cipher?
What are other Caesar Cipher names?
How to cipher CAESAR with the Caesar code?
How to write Caesar Cipher in pseudo-code?
When Caesar Cipher have been invented ?
Similar tools
ROT Cipher
Shift Cipher
Vigenere Cipher
Roman Numerals Conversion
Letter Number (A1Z26) A=1, B=2, C=3
Morse Code
Mono-alphabetic Substitution
Binary Code
Polybius Cipher
Enigma Machine

The key is **keyfordecryption**. This is the 128-bit key to be used for AES decryption



AES Online Decryption

Enter text to be Decrypted

82MXpG3RMdIW+Lc7r+uILw==

Input Text Format: ● Base64 ○ Hex

Select Mode

ECB

Key Size in Bits

128

Enter Secret Key

keyfordecryption

Decrypt

AES Decrypted Output (**Base64**):

RXhwZWN0b1BhdHJvbnVz

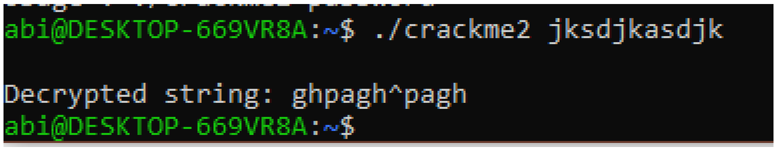
Decode to Plain Text

ExpectoPatronus

**FLAG: ExpectoPatronus**

## LEVEL 14

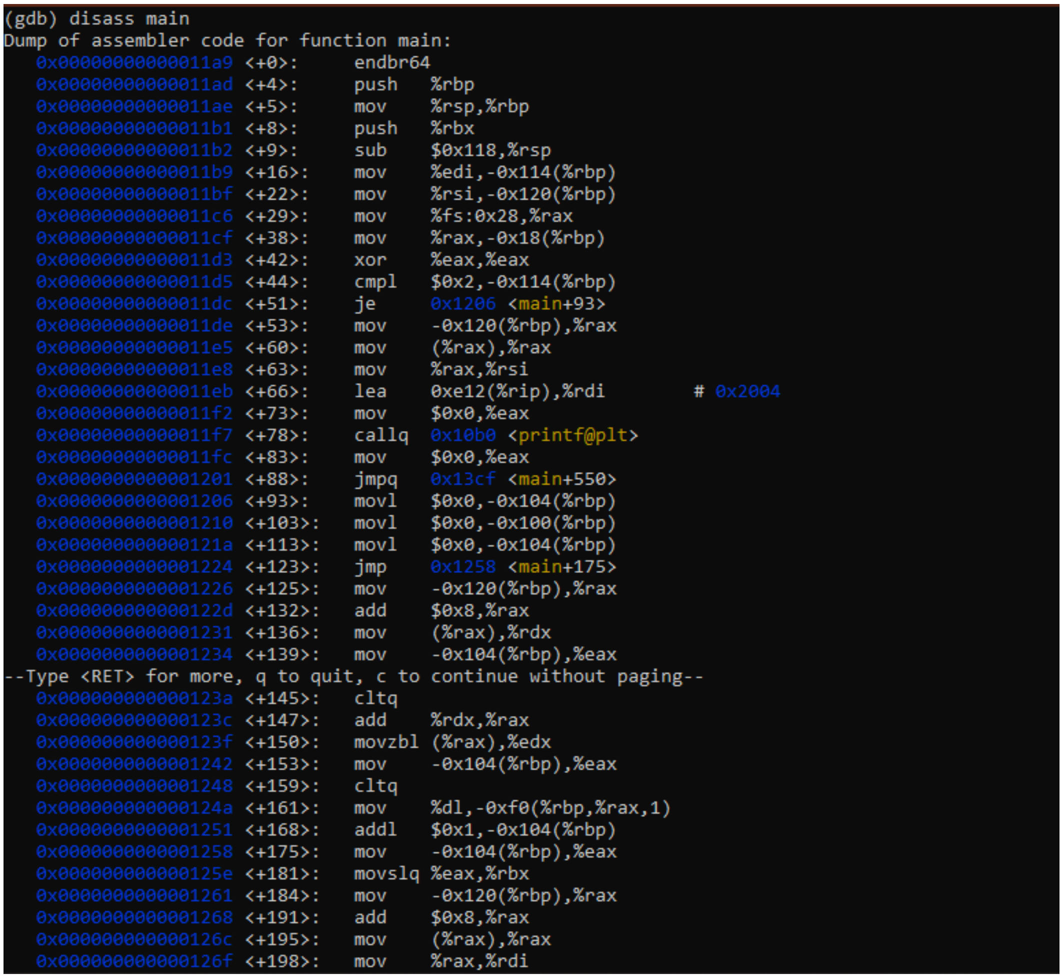
The player is given an executable C file which need 1 argument to be passed at execution.



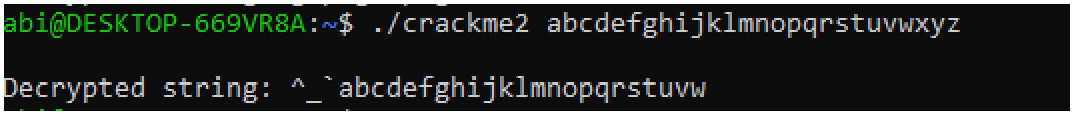
```
abi@DESKTOP-669VR8A:~$ ./crackme2 jksdjkasdjk

Decrypted string: ghpagh^pagh
abi@DESKTOP-669VR8A:~$
```

It can be seen that when a string is entered, the decrypted string is given as the output. There are several methods to solve this. Players can use decompilers such as ghidra or use GDB debugger and analyze the code in assembly and recreate the original program functions. This is time consuming.

The easiest way however, is to observe the output for several inputs.

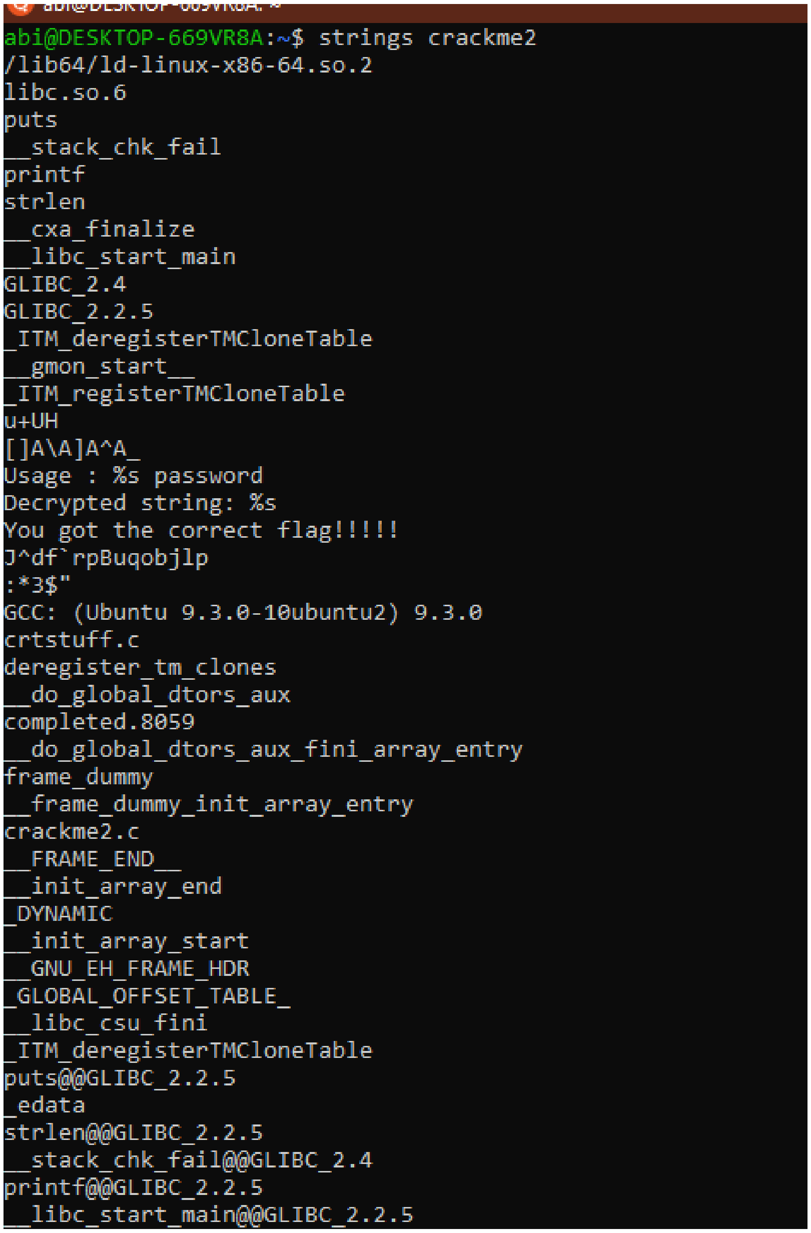


```
(gdb) disass main
Dump of assembler code for function main:
   0x00000000000011a9 <+0>:     endbr64
   0x00000000000011ad <+4>:     push   %rbp
   0x00000000000011ae <+5>:     mov    %rsp,%rbp
   0x00000000000011b1 <+8>:     push   %rbx
   0x00000000000011b2 <+9>:     sub    $0x118,%rsp
   0x00000000000011b9 <+16>:    mov    %edi,-0x114(%rbp)
   0x00000000000011bf <+22>:    mov    %rsi,-0x120(%rbp)
   0x00000000000011c6 <+29>:    mov    %fs:0x28,%rax
   0x00000000000011cf <+38>:    mov    %rax,-0x18(%rbp)
   0x00000000000011d3 <+42>:    xor    %eax,%eax
   0x00000000000011d5 <+44>:    cmpl   $0x2,-0x114(%rbp)
   0x00000000000011dc <+51>:    je     0x1206 <main+93>
   0x00000000000011de <+53>:    mov    -0x120(%rbp),%rax
   0x00000000000011e5 <+60>:    mov    (%rax),%rax
   0x00000000000011e8 <+63>:    mov    %rax,%rsi
   0x00000000000011eb <+66>:    lea    0xe12(%rip),%rdi        # 0x2004
   0x00000000000011f2 <+73>:    mov    $0x0,%eax
   0x00000000000011f7 <+78>:    callq  0x10b0 <printf@plt>
   0x00000000000011fc <+83>:    mov    $0x0,%eax
   0x0000000000001201 <+88>:    jmpq   0x13cf <main+550>
   0x0000000000001206 <+93>:    movl   $0x0,-0x104(%rbp)
   0x0000000000001210 <+103>:   movl   $0x0,-0x100(%rbp)
   0x000000000000121a <+113>:   movl   $0x0,-0x104(%rbp)
   0x0000000000001224 <+123>:   jmp    0x1258 <main+175>
   0x0000000000001226 <+125>:   mov    -0x120(%rbp),%rax
   0x000000000000122d <+132>:   add    $0x8,%rax
   0x0000000000001231 <+136>:   mov    (%rax),%rdx
   0x0000000000001234 <+139>:   mov    -0x104(%rbp),%eax
--Type <RET> for more, q to quit, c to continue without paging--
   0x000000000000123a <+145>:   cltq
   0x000000000000123c <+147>:   add    %rdx,%rax
   0x000000000000123f <+150>:   movzbl (%rax),%edx
   0x0000000000001242 <+153>:   mov    -0x104(%rbp),%eax
   0x0000000000001248 <+159>:   cltq
   0x000000000000124a <+161>:   mov    %dl,-0xf0(%rbp,%rax,1)
   0x0000000000001251 <+168>:   addl   $0x1,-0x104(%rbp)
   0x0000000000001258 <+175>:   mov    -0x104(%rbp),%eax
   0x000000000000125e <+181>:   movslq %eax,%rbx
   0x0000000000001261 <+184>:   mov    -0x120(%rbp),%rax
   0x0000000000001268 <+191>:   add    $0x8,%rax
   0x000000000000126c <+195>:   mov    (%rax),%rax
   0x000000000000126f <+198>:   mov    %rax,%rdi
```



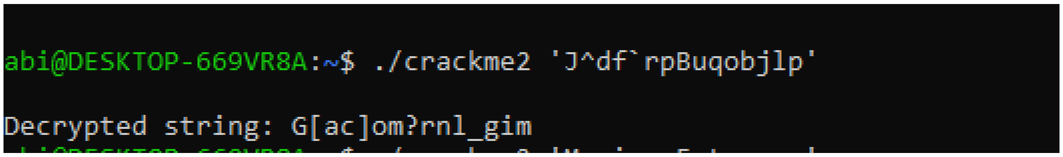
```
abi@DESKTOP-669VR8A:~$ ./crackme2 abcdefghijklmnopqrstuvwxyz

Decrypted string: ^_`abcdefghijklmnopqrstuvw
```

When the whole alphabet is passed as the argument, the above output can be observed. Characters have been shifted 3 positions to the right. For example, letter “a” which took the 1st position in the input has now taken the 3rd position in the output. Now, the player needs to find the correct string to enter to get the decrypted string which could be the flag.



```
abi@DESKTOP-669VR8A:~$ strings crackme2
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__stack_chk_fail
printf
strlen
__cxa_finalize
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Usage : %s password
Decrypted string: %s
You got the correct flag!!!!!
J^df`rpBuqobjlp
:*3$"
GCC: (Ubuntu 9.3.0-10ubuntu2) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8059
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
crackme2.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
puts@@GLIBC_2.2.5
_edata
strlen@@GLIBC_2.2.5
__stack_chk_fail@@GLIBC_2.4
printf@@GLIBC_2.2.5
__libc_start_main@@GLIBC_2.2.5
```

Using the “strings” command, the player can observe the following results. It also shows the strings which are printed and the defined variables. There is a suspicious string “**J^df`rpBuqobjlp**” which can be tried as the argument to be passed.



```
abi@DESKTOP-669VR8A:~$ ./crackme2 'J^df`rpBuqobjlp'

Decrypted string: G[ac]om?rnl_gim
```

If the player tries entering the output as the flag in the challenge page it can be seen that this is not the correct flag. However, this could be a clue.

Initially, it was found out that the shift cipher is used in this challenge. Therefore, in order to get the correct flag, the player needs to use the algorithm used in the program which is shift cipher on the string was found.

| | | |
|---|---|---|
| 1 | a | ^ |
| 2 | b | _ |
| 3 | c | ` |
| 4 | d | a |
| 5 | e | b |
| 6 | f | c |
| 7 | g | d |
| 8 | h | e |
| 9 | i | f |
| 10 | j | g |
| 11 | k | h |
| 12 | l | i |

| | | |
|---|---|---|
| 13 | m | j |
| 14 | n | k |
| 15 | o | l |
| 16 | p | m |
| 17 | q | n |
| 18 | r | o |
| 19 | s | p |
| 20 | t | q |
| 21 | u | r |
| 22 | v | s |
| 23 | w | t |
| 24 | x | u |
| 25 | y | v |
| 26 | z | w |

By looking at this table, the characters in **J^df`rpBuqobjlp** can be matched to the alphabet as follows:

J→M

^→a

d→g

f→i

`→c

r→u

p→s

B→E

u→x

q→t

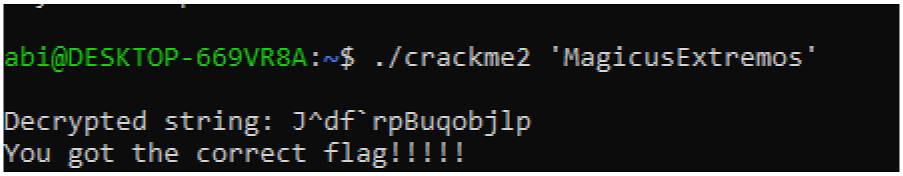
o→r

b→e

j→m

l→o

p→s

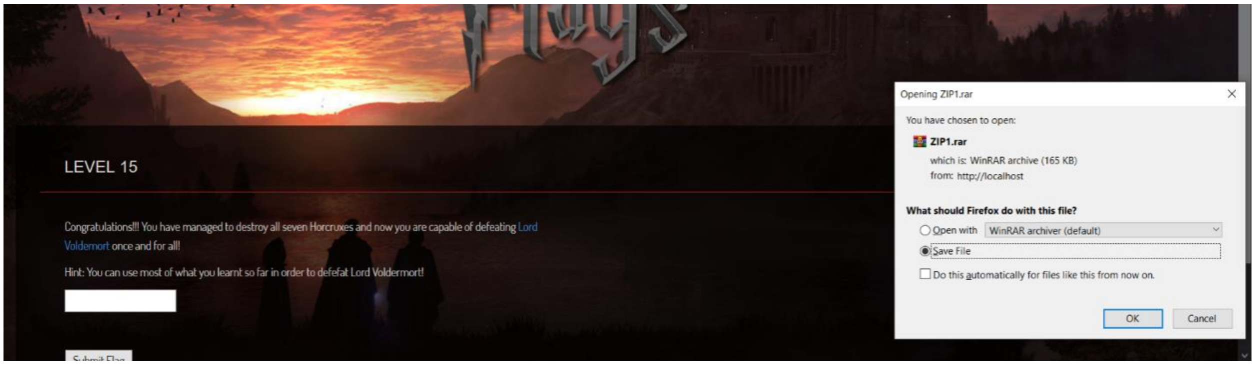


```
abi@DESKTOP-669VR8A:~$ ./crackme2 'MagicusExtremos'

Decrypted string: J^df`rpBuqobjlp
You got the correct flag!!!!!
```

**FLAG: MagicusExtremos**

## LEVEL 15

Once the player clicks on the link, a .zip file will be downloaded.



LEVEL 15

Congratulations!!! You have managed to destroy all seven Horcruxes and now you are capable of defeating Lord Voldemort once and for all!

Hint: You can use most of what you learnt so far in order to defeat Lord Voldermort!

Opening ZIP1.rar

You have chosen to open:

ZIP1.rar

which is: WinRAR archive (165 KB)

from: http://localhost

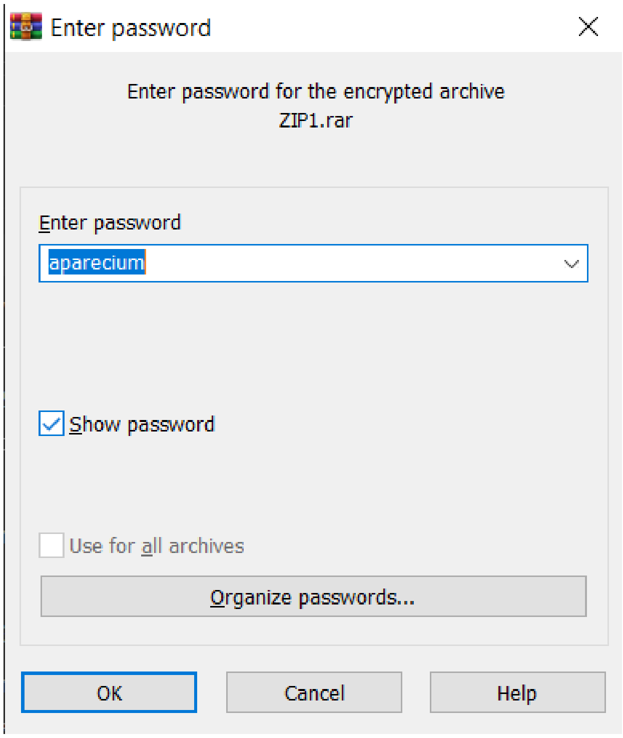
What should Firefox do with this file?

○ Open with WinRAR archiver (default)

● Save File

□ Do this automatically for files like this from now on.

The player could use the hint given in an earlier level and use the spell “**aparecium**” as the password in order to reveal what is in the .zip file.



Enter password

Enter password for the encrypted archive ZIP1.rar

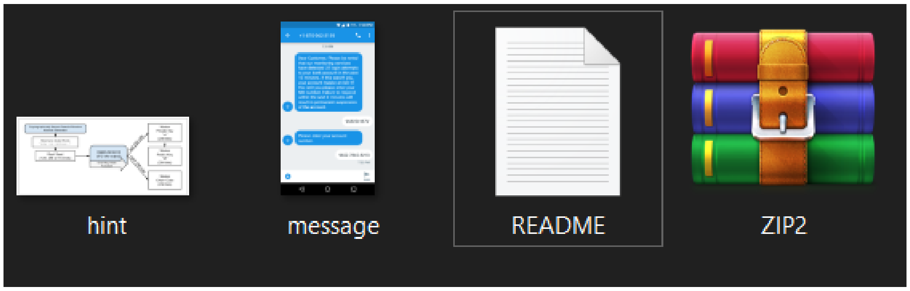
Enter password

aparecium

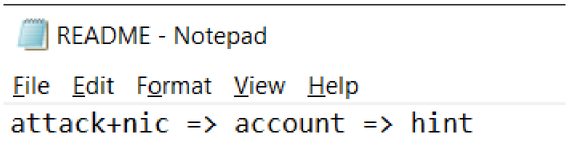
☑ Show password

□ Use for all archives

The contents of the extracted folder will be as follows:

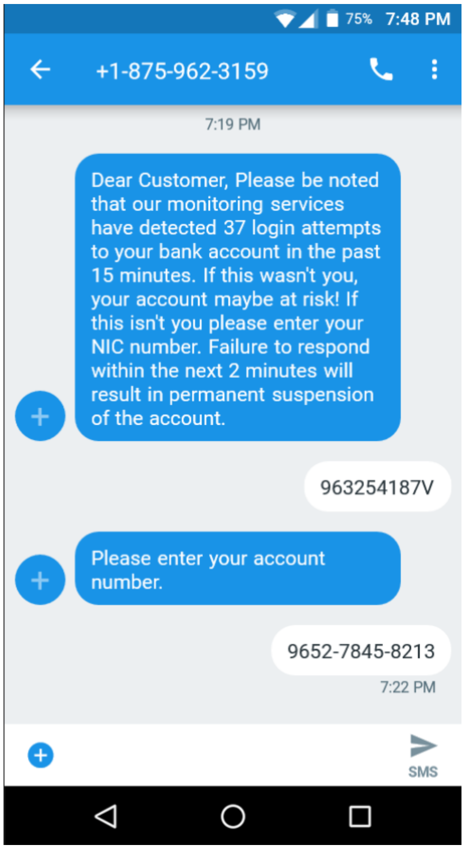


The README file would give the hint in order to open the .zip file.



```
attack+nic => account => hint
```

This means that the player has to check the attack given in message.png and combine it with the details given with relevance to the hint as follows:



7:19 PM

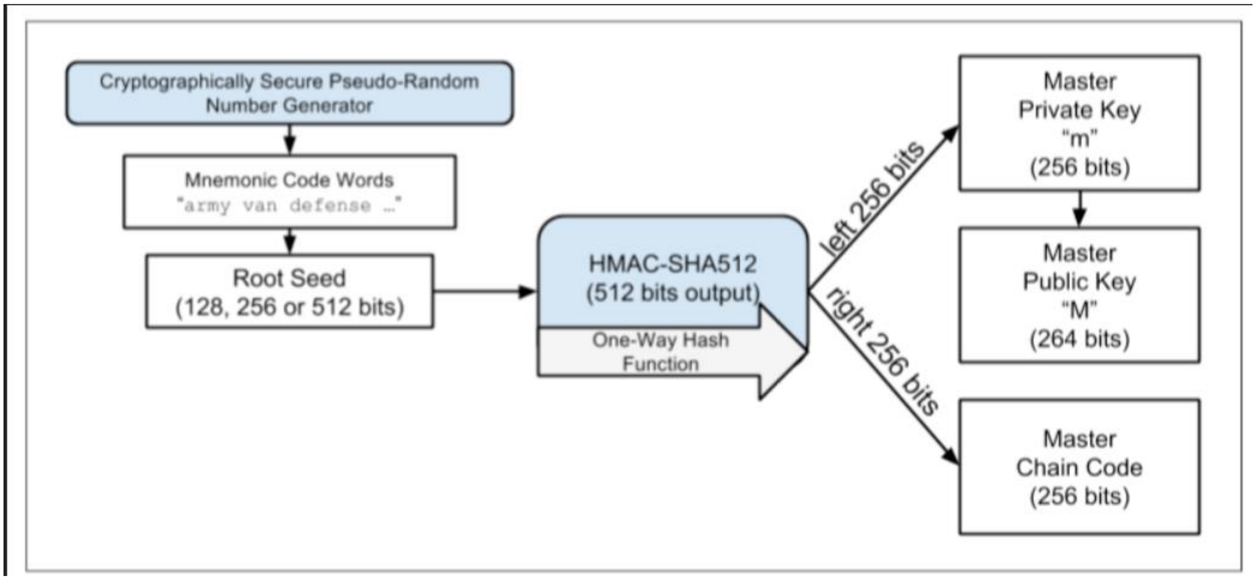
Dear Customer, Please be noted that our monitoring services have detected 37 login attempts to your bank account in the past 15 minutes. If this wasn't you, your account maybe at risk! If this isn't you please enter your NIC number. Failure to respond within the next 2 minutes will result in permanent suspension of the account.

963254187V

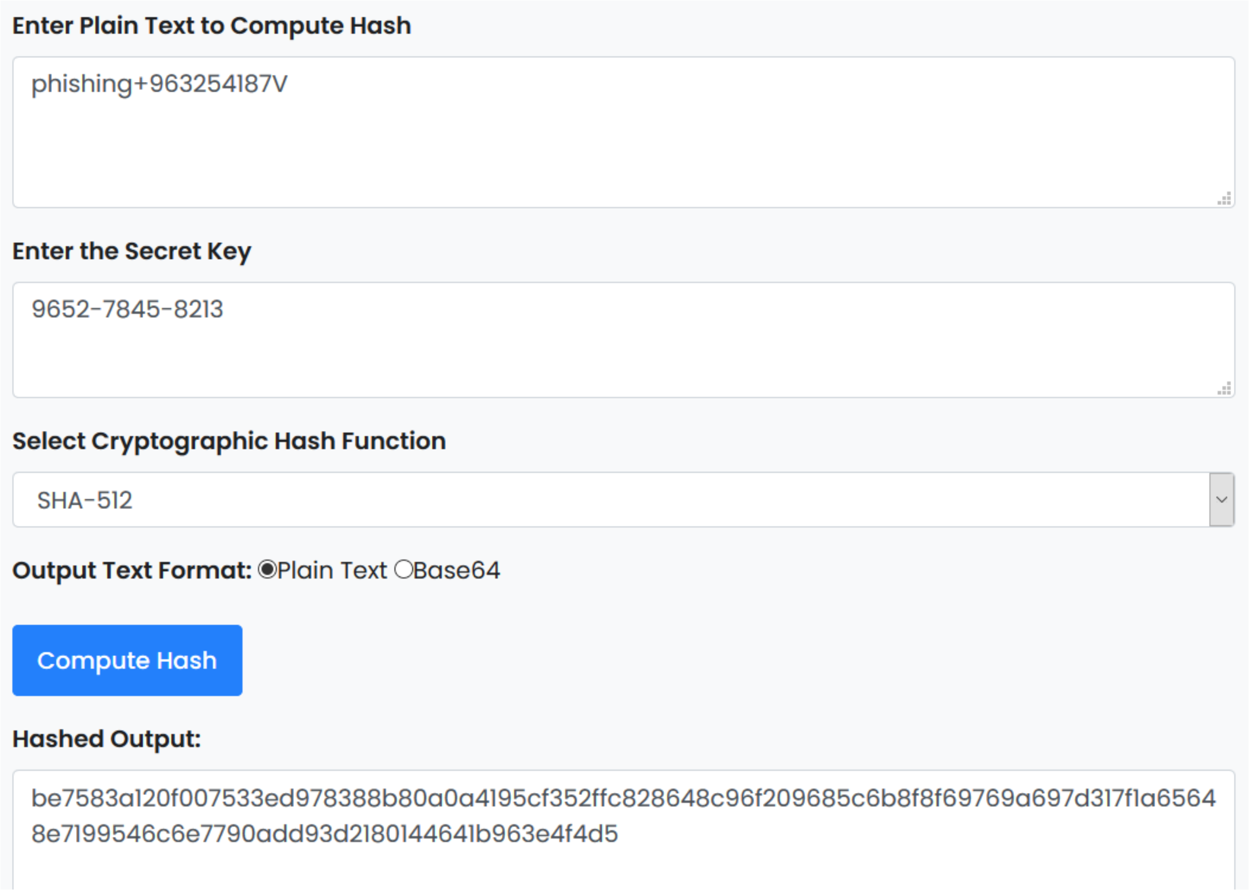
Please enter your account number.

9652-7845-8213

7:22 PM



Therefore, the password to the .zip file will be as follows:



**Enter Plain Text to Compute Hash**

phishing+963254187V

**Enter the Secret Key**

9652-7845-8213

**Select Cryptographic Hash Function**

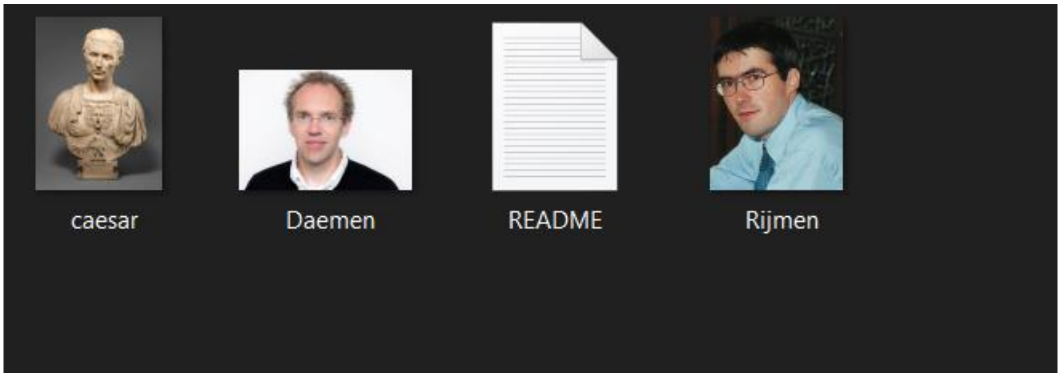
SHA-512

**Output Text Format:** ● Plain Text ○ Base64

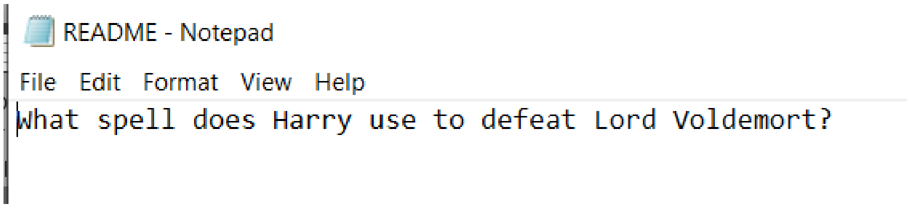
**Hashed Output:**

```
be7583a120f007533ed978388b80a0a4195cf352ffc828648c96f209685c6b8f8f69769a697d317f1a6564
8e7199546c6e7790add93d2180144641b963e4f4d5
```

The contents of the .zip file will be as follows:

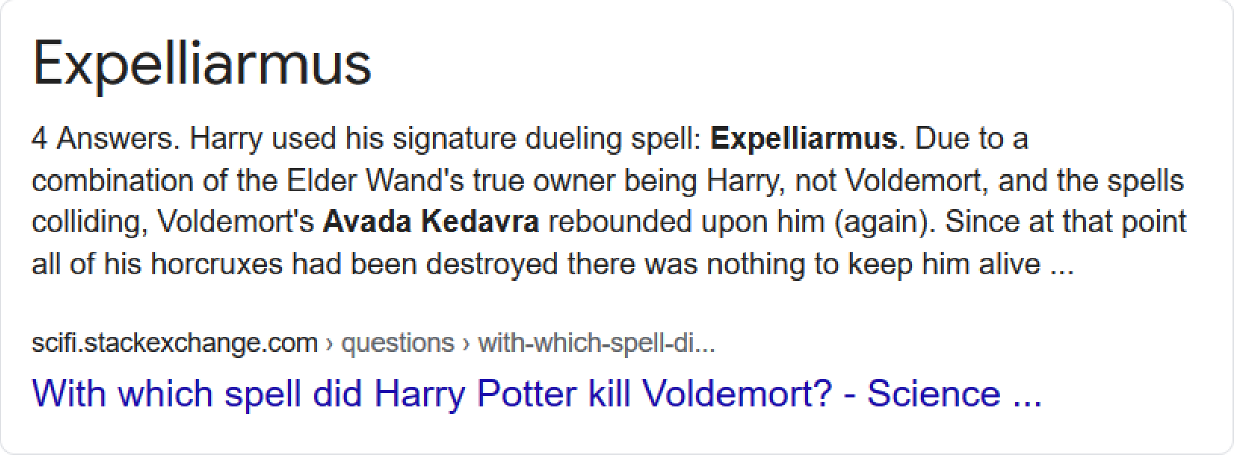


The README file shows the following details:



```
What spell does Harry use to defeat Lord Voldemort?
```

If the player googles this information, they will obtain a result as follows:



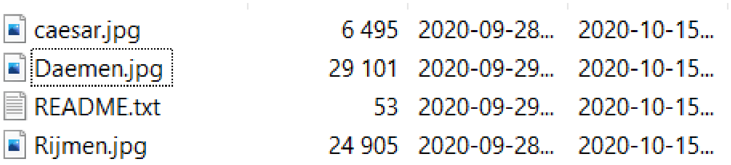
Expelliarmus

4 Answers. Harry used his signature dueling spell: **Expelliarmus**. Due to a combination of the Elder Wand's true owner being Harry, not Voldemort, and the spells colliding, Voldemort's **Avada Kedavra** rebounded upon him (again). Since at that point all of his horcruxes had been destroyed there was nothing to keep him alive ...

scifi.stackexchange.com › questions › with-which-spell-di...

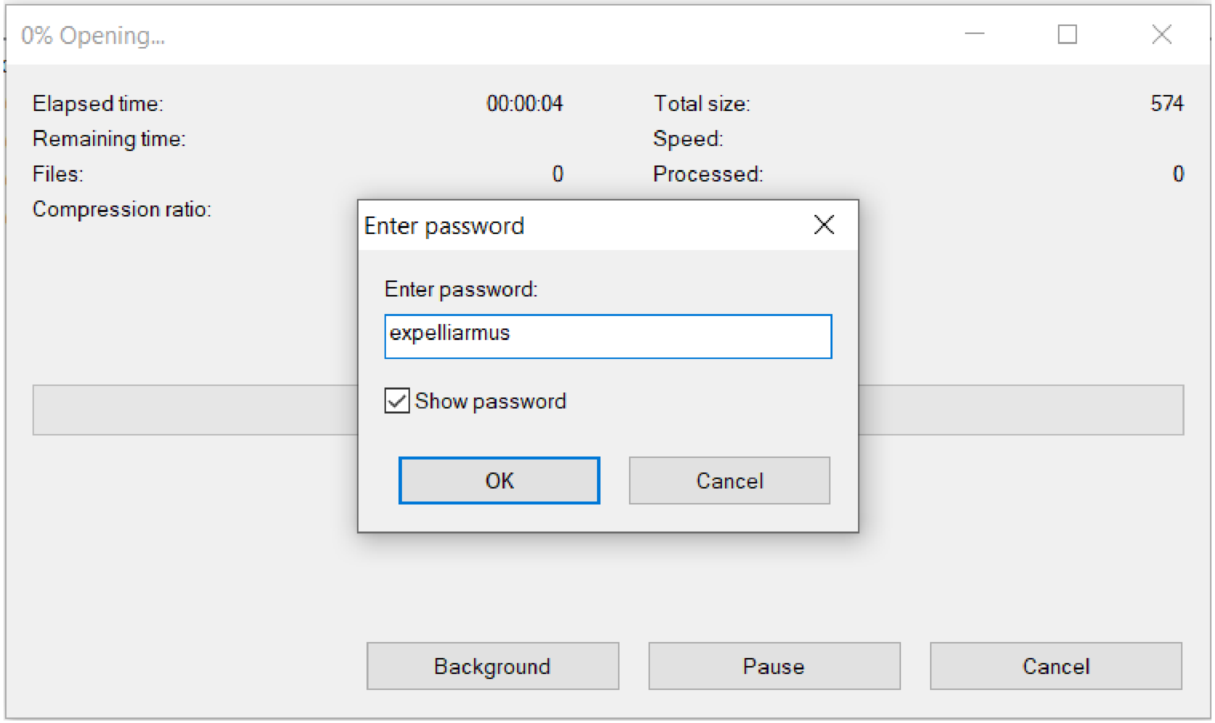
With which spell did Harry Potter kill Voldemort? - Science ...

But this will not be the flag. Hence, if the player uses 7-zip File Manager, they will be able to see the following details:



| | | | |
|---|---|---|---|
| caesar.jpg | 6 495 | 2020-09-28... | 2020-10-15... |
| Daemen.jpg | 29 101 | 2020-09-29... | 2020-10-15... |
| README.txt | 53 | 2020-09-29... | 2020-10-15... |
| Rijmen.jpg | 24 905 | 2020-09-28... | 2020-10-15... |

If the player opens, Daemen.jpg, it will prompt a password. For this, the player can use the spell obtained earlier as "**expelliarmus**".



0% Opening...

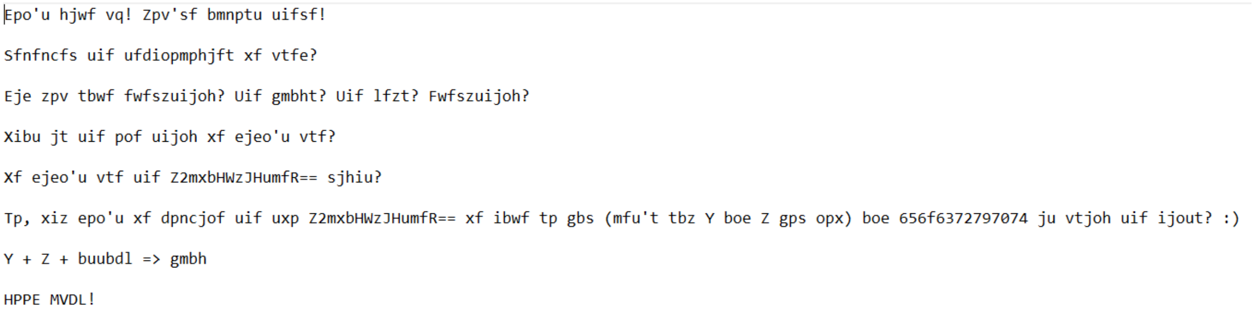
Elapsed time: 00:00:04
Remaining time:
Files: 0
Compression ratio:
Total size: 574
Speed:
Processed: 0

Enter password

Enter password: expelliarmus

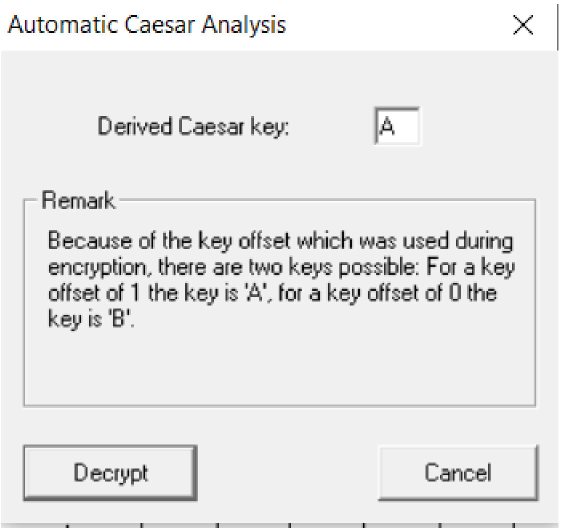
☑ Show password

When the player opens the extracted .zip folder, there will be a text document that gives the following details:



```
Epo'u hjwf vq! Zpv'sf bmnptu uifsf!

Sfnfncfs uif ufdiopmphjft xf vtfe?

Eje zpv tbwf fwfszuijoh? Uif gmbht? Uif lfzt? Fwfszuijoh?

Xibu jt uif pof uijoh xf ejeo'u vtf?

Xf ejeo'u vtf uif Z2mxbHWzJHumfR== sjhiu?

Tp, xiz epo'u xf dpncjof uif uxp Z2mxbHWzJHumfR== xf ibwf tp gbs (mfu't tbz Y boe Z gps opx) boe 656f6372797074 ju vtjoh uif ijout? :)

Y + Z + buubdl => gmbh

HPPE MVDL!
```

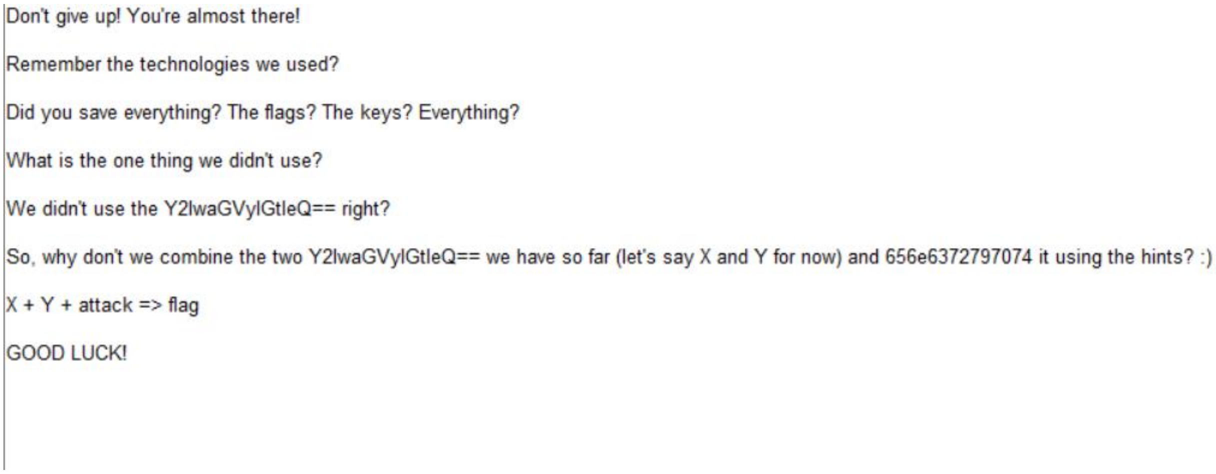
The player could perform a letter frequency analysis using the Caesar Cipher and get the following details:



Derived Caesar key: A

Remark

Because of the key offset which was used during encryption, there are two keys possible: For a key offset of 1 the key is 'A', for a key offset of 0 the key is 'B'.



Don't give up! You're almost there!

Remember the technologies we used?

Did you save everything? The flags? The keys? Everything?

What is the one thing we didn't use?

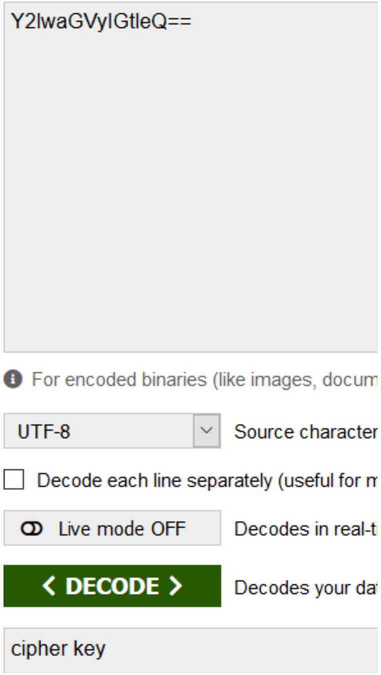
We didn't use the Y2lwaGVyIGtleQ== right?

So, why don't we combine the two Y2lwaGVyIGtleQ== we have so far (let's say X and Y for now) and 656e6372797074 it using the hints? :)

X + Y + attack => flag

GOOD LUCK!

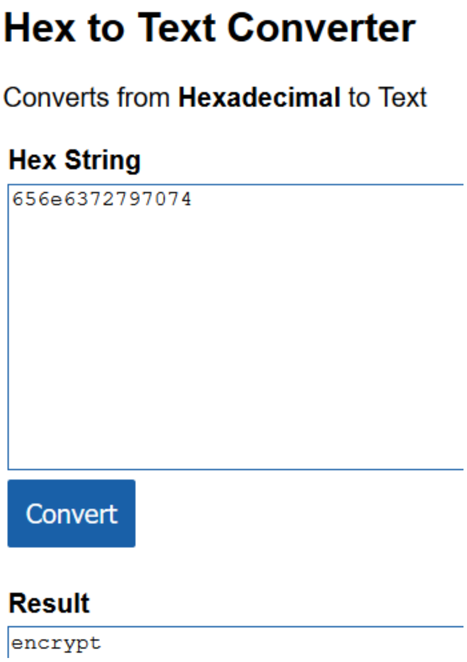
The player could decode the text obtained from this file as follows:



Y2lwaGVyIGtleQ==

For encoded binaries (like images, docum
UTF-8
Source character
□ Decode each line separately (useful for m
Live mode OFF
Decodes in real-t
< DECODE >
Decodes your da

cipher key



Hex to Text Converter

Converts from **Hexadecimal** to Text

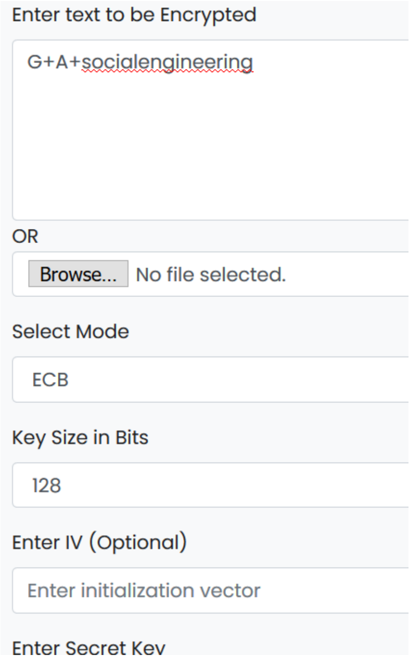
Hex String

```
656e6372797074
```

Result

```
encrypt
```

Now, the cipher keys obtained in this level as well as in Level 8 could be combined and encrypted via AES encryption algorithm and given as the flag.



Enter text to be Encrypted: G+A+socialengineering

OR

Select Mode: ECB

Key Size in Bits: 128

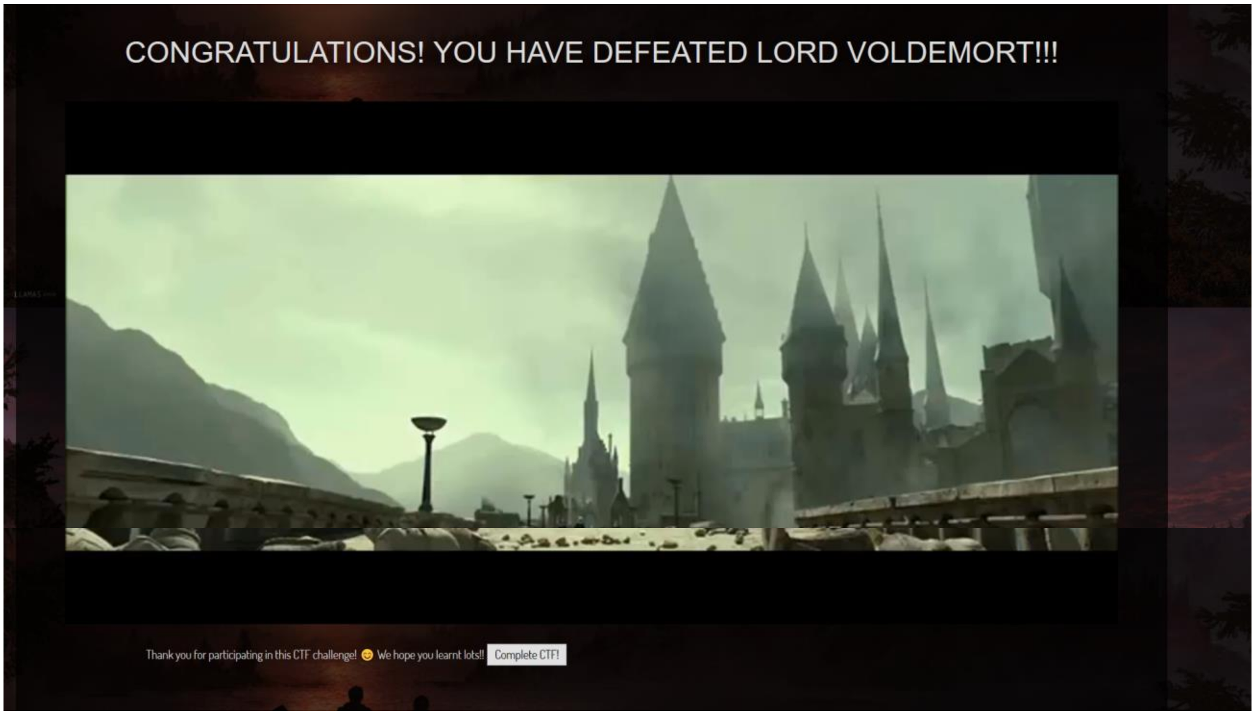
Enter IV (Optional): Enter initialization vector

Enter Secret Kev

**FLAG: OhaLNHTbiZhTHWi1cmMg4Vxhs9Pvevzxy5VGu2MR4Po=**

## CTF COMPLETION

After successful completion of Level 15, the player will be navigated to the following page where the ending scene of the Harry Potter series is played.



CONGRATULATIONS! YOU HAVE DEFEATED LORD VOLDEMORT!!!

Thank you for participating in this CTF challenge! 😊 We hope you learnt lots!!

The players are welcome to leave any feedback in order to further improve this CTF!

## WALKTHROUGH VIDEO

A video of the walkthrough could be found at:

https://mysliit-my.sharepoint.com/:v:/g/personal/it18120462_my_sliit_lk/EQ_loBipuWNHrYlsVV0Vu6UB7oymZkwqG-kb_U8fdUoEuA?e=0xheTF