**INTRODUCTION TO CRYPTIC HUNTS**

Do you exhibit great problem-solving skills? If yes, then cryptic hunts are for you.

For as long as humans have tried to communicate, they have also made sure some of the communication stays secretive. Cryptic hunts are online scavenger hunt-style competitions where a set of clues are given and you need to bring out your inner Sherlock coupled with prodigious wit and interminable foresight to go through a series of mind-bending puzzles to reach the final answer. The internet along with all its might is at your disposal while solving this.

If you have ever wondered what the Turing machine did? or what was the text at the end of gravity falls? The answer to both these questions is an encrypted message. If I have caught your interest I suggest you try finding out the meaning behind this encryption from gravity falls.

ZHOFRPH WR FRUH

**BASICS ABOUT CRYPTIC HUNTS**

* Cryptic hunts have a point system and all the top scorers are generally displayed on the site’s leaderboard.
* The levels generally start from level 0 or level 1 and they continue in a progressive manner.
* Each cryptic hunt has a specific duration. For example, [**Cryptocracy**](https://cryptichunt.com/) took place for 2 days i.e. 12:00 AM IST on 26th June 2020 to 11:59 AM IST on 27th June 2020.
* Usually, the hunt goes on until someone finishes the hunt or if the pre-announced time limit is over.
* Hunts are mainly of two types - a team hunt and an individual hunt;
  + In individual hunts, answer sharing and discussion among participants is forbidden.
* Mostly, all the hunts have unlimited tries on each level so you can try every answer that you can think of.
* There are some hunts with special formats which involve maps or tracks through which you can traverse through levels.
* There are some hunts that have a dynamic format which means that the number of points a level has, keeps decreasing as more and more people solve it.
* Hints are released throughout the hunt whenever the admins feel they are necessary.
* Many hunts have a system called Lead Confirmations - This is a certain time period in which you can ask the admins/moderators of the hunt to confirm if you are on the right track via personal messaging.

**DECODING MESSAGES**

* In cryptic hunt levels, there’s usually some form of a message encoded within texts, images, or even audio. There are several online tools to decode these ‘ciphers’ or encoding.
* Sometimes, you may have to code scripts in general languages like Python to decode, this is done to make things run faster. But remember, most of it can be done manually or through existing tools.
* Google is your best friend, you shall find what you seek.
* Subtle hints may be present in discord servers, docs, intro videos, social media pages even before the hunt starts! So make sure you keep a close check on everything.
* You should check if the level text has some texts that are not visible normally. For instance, uppercase letters, underlined letters, etc forming a different word  
  Sometimes, these clues are hidden in plain sight, with the text being of the same color as the background color.
* Hints can be present in the Page Titles as well.

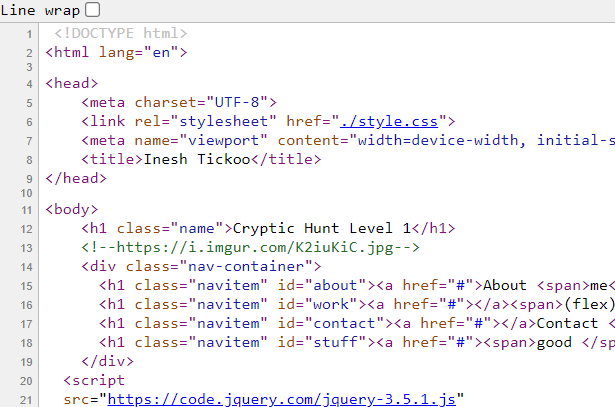
*This is an example of decoding a part of a level in a cryptic hunt:*  
Generally, in programming languages, comments may be displayed like this

<!-- comment text --> OR //comment text OR /\* comment text \*/

You can check the source code of a website, where you’ll find such comments which can be potential hints.

*Shortcuts for opening the source code are-*

Windows - Ctrl + U  
Mac - Command + Option + U  
Phone - view-source: before the URL of the website  
  
Generally a comment looks like this -



Upon seeing this comment, you may realize that the content of it is out of the blue. It looks like an image link - a potential hint to the answer! You would want to copy and paste this URL into your browser and see for yourself what this image may hint at.

Note that it’s not necessary that you’ll only find a link or an image as a hint, there may be other contents, like a ciphertext waiting to be decoded or a link to something within the website.

**Tools**  
Ciphers are well-defined instructions that help to encode or decode. Some ciphers also use keys as part of the formula. Some ciphers are - Caesar, Vigenere, Bifid, etc.  
You can also use certain online Cipher Identifiers when you need help identifying certain ciphers.

* [Decrypt a Message - Cipher Identifier - Online Code Recognizer](https://www.dcode.fr/cipher-identifier)
* [Cipher Identifier (online tool)](https://www.boxentriq.com/code-breaking/cipher-identifier)
* [CyberChef - The Cyber Swiss Army Knife](https://gchq.github.io/CyberChef/)
* [Cryptii](https://cryptii.com/)

Some encrypted texts or images have weird-looking symbols in them. Generally, they are some sort of symbol cipher.  
*eg.* 

*These symbols above represent the Dancing Men Cipher*

* A detailed list of symbol ciphers can be found here - [List of Symbols Cipher - Online Decoder, Translator](https://www.dcode.fr/symbols-ciphers)

Steganography refers to hiding a file within another file. This can be anything like audio, video, images, texts. You can use various websites available online to decode steganographic data.  
Some helpful sites are -   
  
<https://stylesuxx.github.io/steganography/><https://www.mobilefish.com/services/steganography/steganography.php><https://manytools.org/hacker-tools/steganography-encode-text-into-image/><https://aperisolve.fr/>  
LSB is another steganography technique in which you can hide messages by using the Least Significant Bits of an image. You can use this website to decode messages that are encoded through the LSB technique - <https://incoherency.co.uk/image-steganography/#unhide>  
  
  
**EXIF data** - (also sometimes referred to as **metadata**) contains information such as aperture, shutter speed, ISO, focal length, camera model, the date the photo was taken and much more. You can also include copyright information in your **EXIF data** when you register your camera through the manufacturer.  
  
You can use online tools like -<http://exif.regex.info/exif.cgi>  
  
Audio Files

If you have an audio file (.mp3, .wav) you can use tools like spectrum analyzer and certain steganography tools. You can also change the pitch of the audio or reverse it. Some helpful tools for this are -  
Steganographic Decoder - <https://futureboy.us/stegano/decinput.html>[Spectrum analyzer](https://academo.org/demos/spectrum-analyzer/)  
[Sonic audio visualizer](https://www.sonicvisualiser.org/)[Audacity](https://www.audacityteam.org/download/)

**Links and other tools**

URL Shorteners - These are special URLs that help us to use a shorter vision of the original URL. Common shorteners used in hunts are - [bit.ly](https://bitly.com/) [tinyurl.com](https://tinyurl.com/) [cutt.ly](https://cutt.ly/)   
Some cryptic hunts also have had custom shorteners like - eroc.ml quic.ml bhyi.tk

Common URLs - Some levels might have random strings in them which can be added to the back of common websites to get the right page.  
Examples are - YouTube, Google products (drive, docs, slides, forms) social media (Twitter Instagram), Pastebin, Hastebin, Imgur

*eg. you find a hint “K2iuKiC”, you can try it out with websites such as the above-mentioned, by just entering it in the backlink (bit.ly/backlink or bit.ly/K2iuKiC or quic.ml/K2iuKiC)*

* There are also certain *onion links*, which can be opened with [tor browser](https://www.torproject.org/)

URL Manipulation - Sometimes you need to put certain strings as a backlink to the hunt’s website itself. An example could be - play.cryptichunt.com/lethifold  
In this example, lethifold is the part (hint) that you will get from the level  
  
File Manipulation -When you receive a file from a level you can either open the file directly and if that doesn't work you need to make changes to that file. This includes renaming file formats to .txt .zip .jpg etc.  
To display these file extensions in the file explorer -

* Select the *View tab*.
* To display the extensions, deselect *Hide extensions for known file types*. Click on OK.

**Advanced**

Great! You’ve covered the basics of solving cryptic hunts. It’s now time to dive deeper.

Inspect element allows you to see the contents of the website, you can even edit the contents temporarily. The edits are temporary and don’t change the real website. You can use other developer tools such as the network tab or the console tab to try and get through the given level.  
Shortcuts are -   
Windows: Ctrl + Shift + J   
Mac: Cmd + Opt +J  
  
Cookies of a site - Cookies are messages that web servers pass to your web browser when you visit Internet sites. Sometimes they can have helpful information. Some levels might require you to change the contents of a certain cookie. This can be done using chrome extensions such as cookie editors.  
  
Changing user agent - User-agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with web content”. In some levels, you have to change the user agent to do the level. This can be done using extensions such as User-agent switcher.  
  
Linux Some levels require you to work on other operating systems like Linux. If you don't have one, then you can work on a Vmware workstation that runs along with your main host. There are some tools that are limited to only Linux like Stegsolve, Foremost, etc which can be used to solve levels.  
  
  
  
  
*Let’s now look at a level from* [*Cryptocracy 2020*](https://cryptichunt.com/)

Level Problem

"you can run but you can't hide, bi...!"  
[](https://imgur.com/a/d4lm1gz)  
  
  
Solution

As you can see, this is an image with a yellow man pointing towards the left. The person pointing towards the left hints towards something being there on the left side of the image. We find out that the image has LSB encoded ([Image Steganography Tool](https://incoherency.co.uk/image-steganography/)) another image in it, which has a string on the left- BTWSBTWSQCJSPTSMPT. Keeping the string aside, we look at the level text, the line is from Rick and Morty and is said by Scary Terry. Scary Terry and basketball present in the image give a basketball player named Terry Rozier, This hints us towards Rozier Cipher, The Imgur image name is titled MODI which is the key for Rozier cipher. After decoding BTWSBTWSQCJSPTSMPT with key MODI, we get 00119 which are the lyrics of a song named zungguzungguguzungguzeng which is the answer.  
  
Answer- **zungguzungguguzungguzeng**



Level Problem

Imgur/7557  
  
Solution

7557 is Hitarth Khurana’s discord tag, you will reach Hitarth's Imgur account by using the appropriate imgur search format. There you will find two pictures. A blank picture and a picture of a rock. The blank picture has lyrics of RIde out (from Furious 7). Both pictures have the title wassup. The blank image has steganographic data that can be decoded at [mobilefish.com](https://www.mobilefish.com/services/steganography/steganography.php) with the password wassup. The decoded text says strongholdonion/pgbpsu4hk/voeabd. stronghold onion refers to stronghold paste which is an onion website ( you can open onion links with tor browser). Onion paste's common link can be found on tor browser. when connected with the string at the end you reach the stronghold paste that is created on Tor browser. That paste has base64 encoded data that can be converted into an excel file by using websites that convert base64 to file online. the excel file has 8 letters written by dots(1 letter written over 6 rows and 6 columns), the 8 letter string when decoded by caesar cipher gives dustdust which can be understood as dust 2 which is a csgo map.   
  
  
Now the song ride out and the rock image (Dwayne Johnson) gives the movie F7(furious 7). there are map coordinates on the dust 2 map in csgo on *the loading screen* which can be found on the internet too.   
F7 on the map gives the location named ‘lower tunnel’.  
 Now there are two ways to go further  
1) In the excel file, in the last column and the last row, it was written r/ in the cell   
2) if the lyrics are compared to the original lyrics they have the difference of a ‘r’ and a ‘slash’.   
This gives us r/ which is how subreddits are resembled on Reddit.  
r/lowertunnel (does not exist anymore) gives a robotic arm image with the title free phone hack and it had a comment of a random string. Free phone hack and that robotic arm was a reference to an Elon Musk tweet(<https://twitter.com/elonmusk/status/1225488457667141633?s=20>) This leads us to WhatsApp. The string when put at the end of chat.whatsapp.com(format for WhatsApp group invite) joins a WhatsApp group. The WhatsApp group had /dbz in the description./dbz when put as a backlink to the hunt’s platform - [play.cryptichunt.com/dbz](http://play.cryptichunt.com/dbz) (link does not work now) downloads a zip file which has 5000 images all saying this is a fake answer. If you sort all the images by size we get two images (have to sort both ascending and descending). The first image says caulifla . The second image says kale. When searched on google it can be seen that both these characters are from the dragon ball franchise and they merge to form Kefla.  
  
Note: This level was one of the most difficult levels in cryptocracy 2020 and most participants found it quite tedious to reach the final answer. Thus, keep in mind that not all levels are like this, this has just been added to shed light on some important concepts at once.  
  
Answer **- Kefla**

**ARGs:**

* ARG stands for Alternate Reality Game.
* ARGs are generally a series of riddles and puzzles that go along with a storyline. Companies, TV shows, YouTubers generally host ARGs just to promote their products, and sometimes prizes are also involved.
* ARGs give a sense of the real world while being a virtual world revolving around cryptography.
* Some popular ARGs are -

Gravity Falls ARG: <https://youtu.be/QhuPJ20qNvM>  
Wilbur Soot ARG: <https://youtu.be/JoIgaJRHxVc>

Practice makes perfect.  
Doing more and more hunts will get you the gist of what you need to do and which resource you need to use at which point. So keep learning and improving!

*For any queries regarding the topic contact:*

Hitarth Khurana

Email**:** Hitarth2004@gmail.com

Instagram: @hitarthkhurana\_

Phone: 8130145877