# CyberCamp{CTF2022} CheatSheet

**Intro:**

- Find flags that look like this: `CyberCamp{CTF2022}`
- They are hidden on the Cyber Range Windows Virtual Machines -- and possibly elsewhere on the internet.
- You may not "hack" the CTF server itself.

**General Advice:**

- When in doubt, Google commands and code.
- Be curious. Most things on the system are there for a reason. Explore. Read files, look at pictures, check out links -- and any other interesting corners of the system we discussed.
- **Base64:** Lots of things are *encoded* using base64. This is to make it slightly harder to search for text. There are plenty of websites that can help you decode base64.
  - It looks like this: `SGEhWW91VGhvdWdodFlvdUZvdW5kQUZsYWcuLi4=`
  - Note: It is composed of `a-z, A-Z, 0-9`, and 0-2 trailing = characters.
- Flag Text can and will be creatively structured. They are not space or case sensitive. They can be normal, backwards, with a bunch of spaces, or even arranged vertically. The flag should be put in the right order and any extra characters should be removed. Sometimes, you will need to insert curly braces.
  - `Q3liZXJDYW1we1RoaXNJc0FCYXNpYzY0RmxhZ30=`
  - ```
    C                a                r
    y                m                t
    b                p                i
    e                {                c
    r                V                a
    C                e                l
                                      }
    ```
- We gave you some code snippets on the desktop in the "Forensics Tools" folder. Modification likely required.
- You shouldn't have to brute force things except when you should. Don't do things manually.
- Strategy: some flags will take longer than others. This is about maximizing your flags per hour.
- **Other Tools**: Base64, Text Reverse, Stego

**Useful Linux Commands:**

- **Change Directory:** `cd "directory name"`
- **Search for text in all files in the directory**: `grep text *`
- **Show fill contents**: `cat`
- **Show file top**: `head`
    ```

- **Show file end**: `tail`
- **Show ALL files (including hidden ones)**: `ls -al`
- **Determine File Type**: `file *`
- **Base 64 decrypt**: `echo "base64 string here" | base64 -d`
- **Make a script executable**: `chmod +x file`
- **Execute a script**: `./scriptname`

**Python Code Snippets:** Check out the Forensics Tools Folder!

**SQL:**

- **Open Database:** `sqlite3 databasefile`
- **List Tables (SQLite only):** `SELECT name FROM sqlite_master WHERE type='table'`
- **Display Table**: `SELECT * FROM tableName`
- **Display Specific Table Rows**: `SELECT * FROM tableName WHERE stuff = 'thing'`
- **Display Results in Order**: `SELECT * FROM tableName ORDER BY fieldname`