1/ Can you convert the number 42 (base 10) to binary (base 2)?

A: bin(42)

2/ This [garden](https://2019shell1.picoctf.com/static/3e1f573c9b18e87b6764ec3a36868b5a/garden.jpg) contains more than it seems. You can also find the file in /problems/glory-of-the-garden\_0\_25ece79ae00914856938a4b19d0e31af on the shell server.

A: hex editor online

A: cat <ten-file> | tail

3/ Kishor Balan tipped us off that the following code may need inspection: https://2019shell1.picoctf.com/problem/61676/ ([link](https://2019shell1.picoctf.com/problem/61676/)) or <http://2019shell1.picoctf.com:61676>

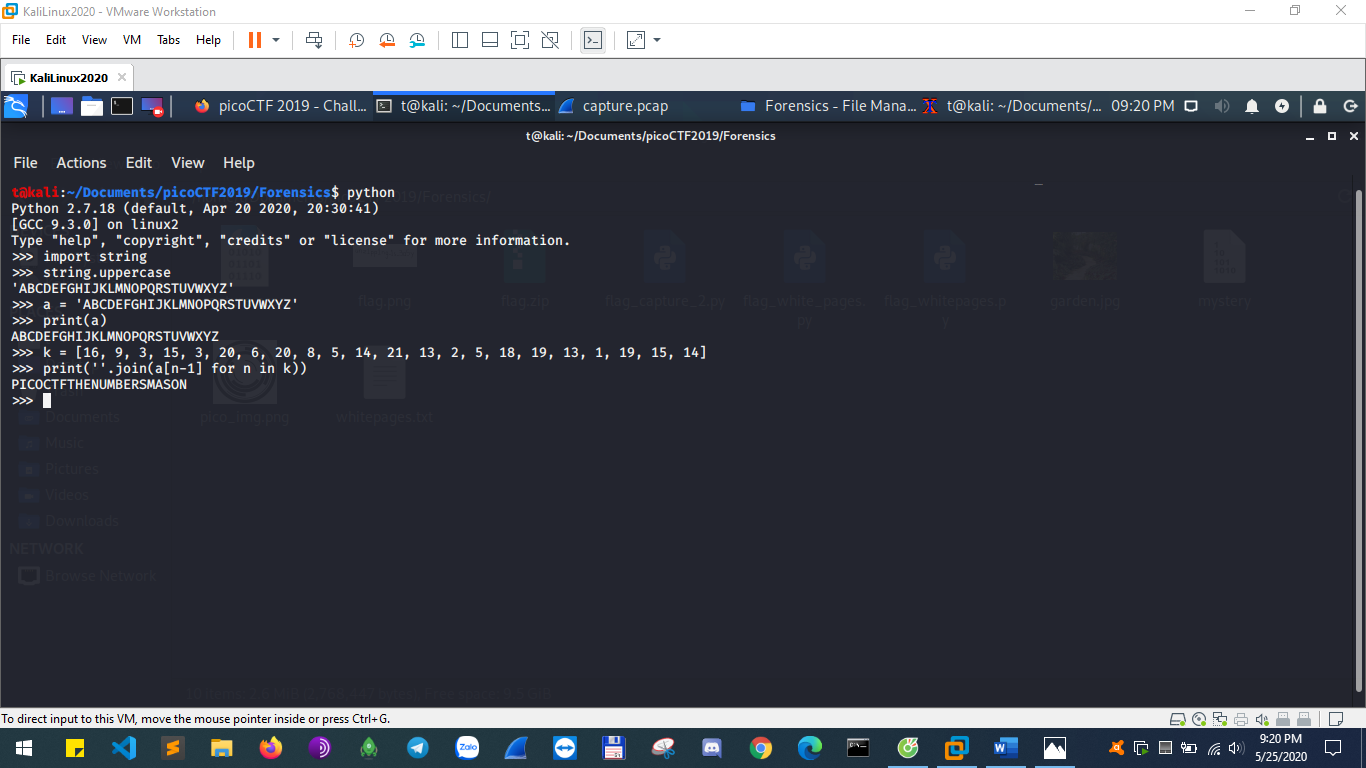
A: F12

4/ If I told you a word started with 0x70 in hexadecimal, what would it start with in ASCII?

A: man ascii

5/ The [numbers](https://2019shell1.picoctf.com/static/eb3589c566dd3f809908053460acb817/the_numbers.png)... what do they mean?

A: A = 1, B = 2, C = 3, …



6/ What is 0x3D (base 16) in decimal (base 10).

A: 0x3D (python)

7/ This [program](https://2019shell1.picoctf.com/static/3101ab62e47b525481217badc84a8c70/vuln) executes any shellcode that you give it. Can you spawn a shell and use that to read the flag.txt? You can find the program in /problems/handy-shellcode\_3\_1a2e95a810eefe4a5994631812c0b8af on the shell server. [Source](https://2019shell1.picoctf.com/static/3101ab62e47b525481217badc84a8c70/vuln.c).

A: minh ngu phan nay

8/ You're going to need to know how to run programs if you're going to get out of here. Navigate to /problems/practice-run-1\_0\_62b61488e896645ebff9b6c97d0e775e on the shell server and run this [program](https://2019shell1.picoctf.com/static/6eba3b66e7a2b786c6c9769711d85663/run_this) to receive a flag.

A: ./<ten-file>

9/ Can you unzip this [file](https://2019shell1.picoctf.com/static/37762a7e5774d7d6c1bc79e8e1758ef9/flag.zip) and get the flag?

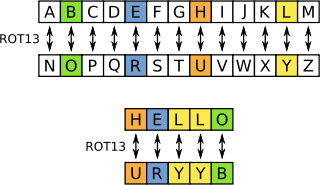
A: unzip <ten-file>

10/ Your mission is to enter Dr. Evil's laboratory and retrieve the blueprints for his Doomsday Project. The laboratory is protected by a series of locked vault doors. Each door is controlled by a computer and requires a password to open. Unfortunately, our undercover agents have not been able to obtain the secret passwords for the vault doors, but one of our junior agents obtained the source code for each vault's computer! You will need to read the source code for each level to figure out what the password is for that vault door. As a warmup, we have created a replica vault in our training facility. The source code for the training vault is here: [VaultDoorTraining.java](https://2019shell1.picoctf.com/static/56c37b7d53ba094dd5b05587ad27d3cf/VaultDoorTraining.java)

A: mo file ra doc thoi, hieu hay khon thi hen xui, :v

11/ Cryptography can be easy, do you know what ROT13 is? cvpbPGS{abg\_gbb\_onq\_bs\_n\_ceboyrz}

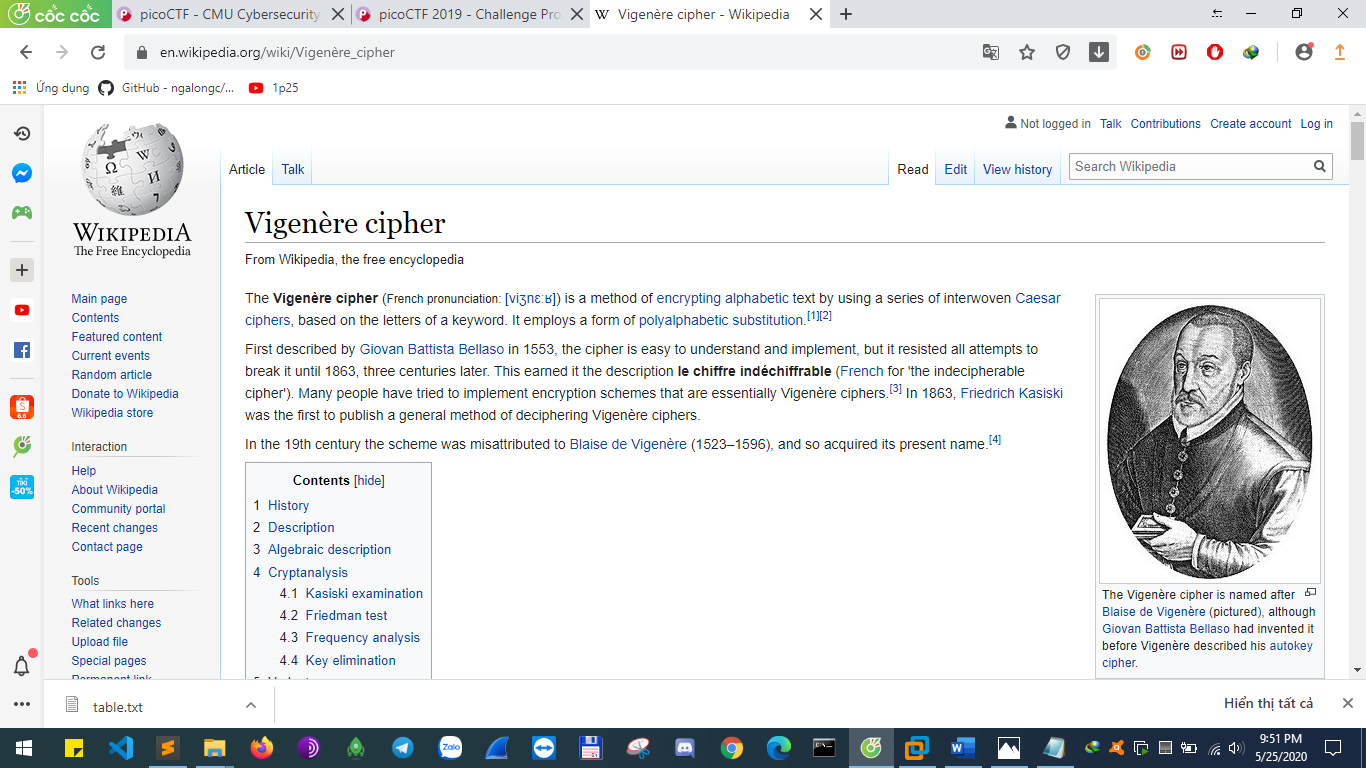
A: ROT13 online, de vl



12/ What does this bDNhcm5fdGgzX3IwcDM1 mean? I think it has something to do with bases.

A: base64 decode online

13/ The one time pad can be cryptographically secure, but not when you know the key. Can you solve this? We've given you the encrypted flag, key, and a table to help UFJKXQZQUNB with the key of SOLVECRYPTO. Can you use this [table](https://2019shell1.picoctf.com/static/30d4405c34cf6490b082e6cf8f56ac56/table.txt) to solve it?.



14/ Can you find the flag in [file](https://2019shell1.picoctf.com/static/3f6065eec2d3ed644932ada577a74334/file)? This would be really tedious to look through manually, something tells me there is a better way. You can also find the file in /problems/first-grep\_0\_93be1631acf1a93b98cdcc3e7b9fdc52 on the shell server.

A: mo bang sublime

A: cat <ten-file> | grep pico

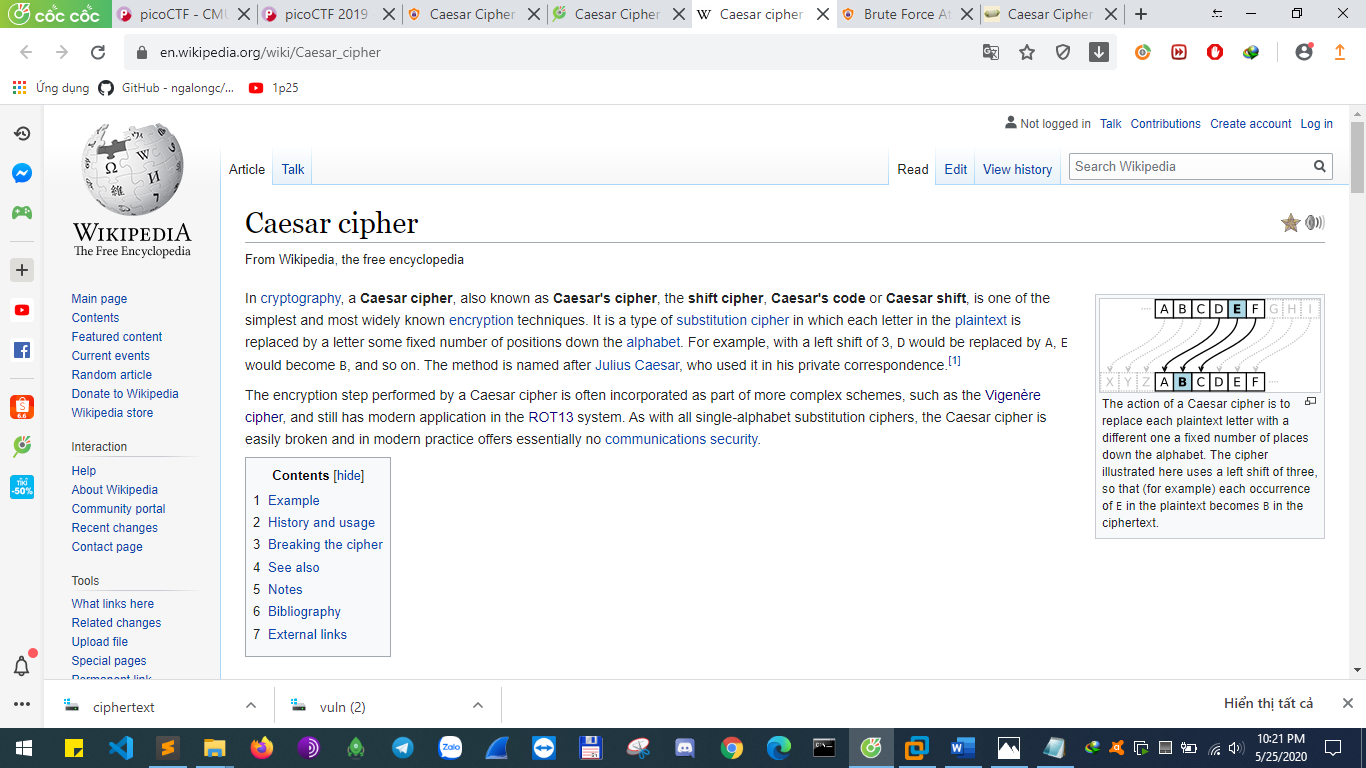
15/ This should be easy. Overflow the correct buffer in this [program](https://2019shell1.picoctf.com/static/8df893afa5d4ecda515901499b0fdd52/vuln) and get a flag. Its also found in /problems/overflow-0\_1\_54d12127b2833f7eab9758b43e88d3b7 on the shell server. [Source](https://2019shell1.picoctf.com/static/8df893afa5d4ecda515901499b0fdd52/vuln.c).

A: ./<ten-file> aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

16/ We put together a bunch of resources to help you out on our website! If you go over there, you might even find a flag! https://picoctf.com/resources ([link](https://picoctf.com/resources))

A: co link thi vo thoi, sao phai ngai

17/ Decrypt this [message](https://2019shell1.picoctf.com/static/61868db3838204e921e70dc9a883f0fe/ciphertext). You can find the ciphertext in /problems/caesar\_1\_4c9d445f770c71bd84ab0d822197a005 on the shell server.



18/ Can you break into this super secure portal? https://2019shell1.picoctf.com/problem/32259/ ([link](https://2019shell1.picoctf.com/problem/32259/)) or <http://2019shell1.picoctf.com:32259>

A: F12

19/ The factory is hiding things from all of its users. Can you login as logon and find what they've been looking at? https://2019shell1.picoctf.com/problem/12284/ ([link](https://2019shell1.picoctf.com/problem/12284/)) or <http://2019shell1.picoctf.com:12284>

A: EditThisCookie false thanh true

20/ Can you find the flag in [file](https://2019shell1.picoctf.com/static/d97e691ff0842819be9dfcb767c074d9/strings) without running it? You can also find the file in /problems/strings-it\_0\_b76c77672f6285e3a39c188481cdff99 on the shell server.

A: strings <ten-file>

21/