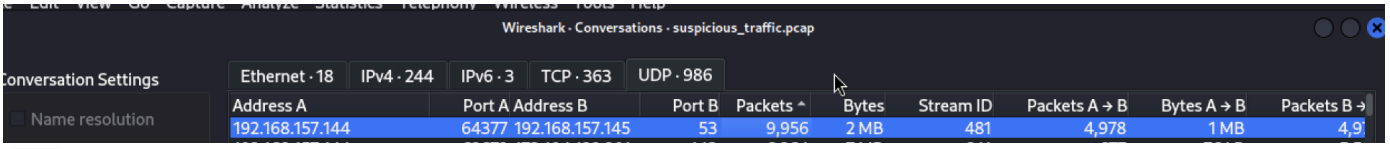
Litter,pcap(DNS 隧道)

```
Sherlock Scenario
Khalid has just logged onto a host that he and his team use as a testing host for many different purposes. It’s off their corporate network but has access to lots of resources on the network. The host is used as a dumping ground for a lot of people at the company, but it’s very useful, so no one has raised any issues. Little does Khalid know; the machine has been compromised and company information that should not have been on there has now been stolen — it’s up to you to figure out what has happened and what data has been taken.
* * *
About Litter
A commonly used off-network host, which serves as a testing ground for various purposes, has been breached. The host, while not on the corporate network, has extensive access to numerous resources, making it a significant vulnerability point. It has come to light that company information, which should not have been on this host, has been stolen. As the forensic investigator, your mission is multi-fold: you must unearth how this breach occurred, what company data has been exfiltrated, and whether the attacker employed any form of tunneling for the intrusion or data theft. This task demands your advanced understanding of cybersecurity, particularly network tunneling techniques, and your ability to perform thorough digital forensics to restore security and prevent further data loss.
```

文件：`suspicious_traffic.pcap`

Task 1

At a glance, what protocol seems to be suspect in this attack?



`DNS`

Task 2

There seems to be a lot of traffic between our host and another, what is the IP address of the suspect host?

同上

`192.168.157.145`

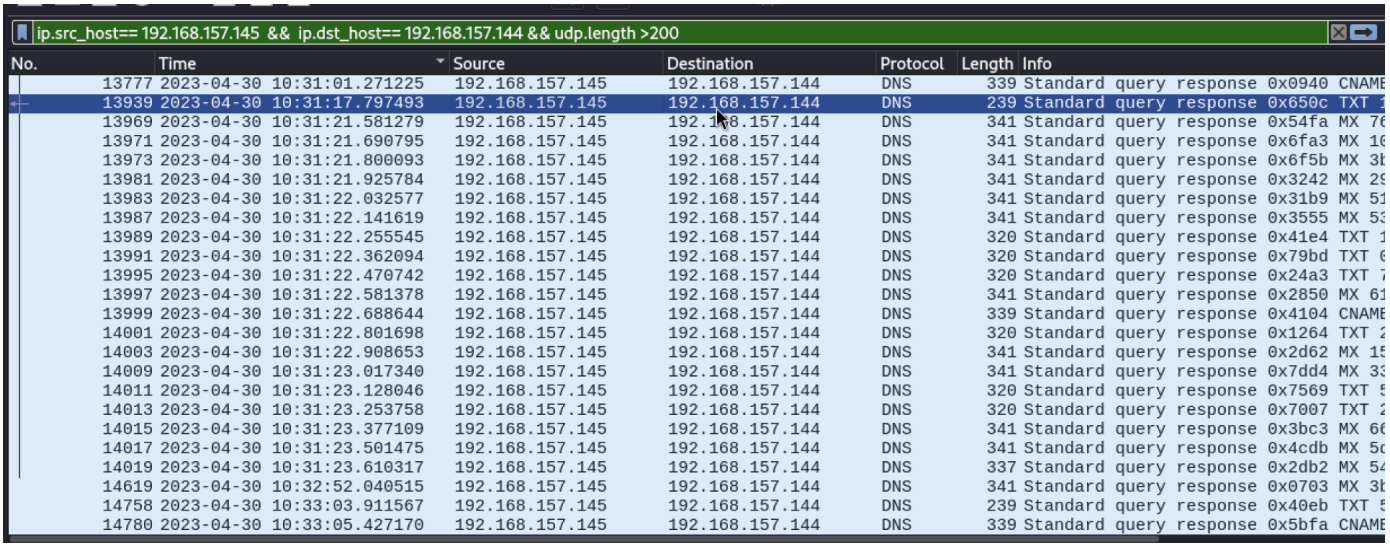
Task 3

What is the first command the attacker sends to the client?

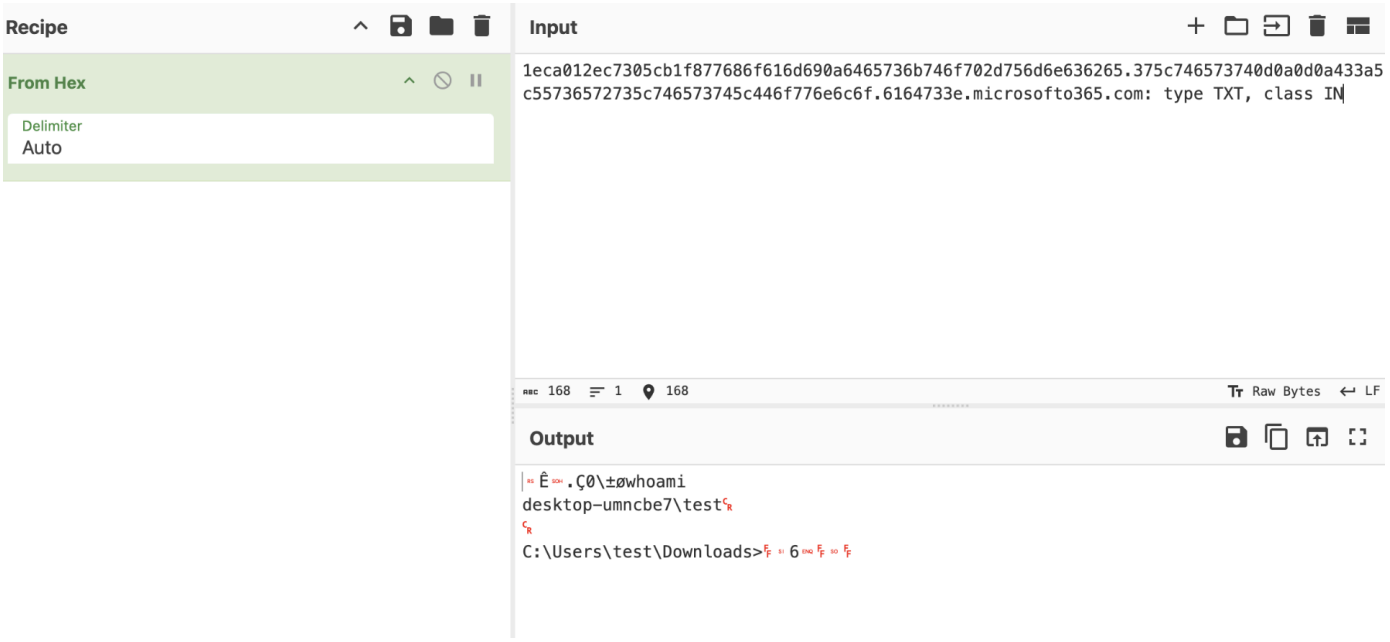
設定 udp.length > 200 是因為 UDP 封包的負載部分需要超過 200 個位元組才能包含足夠的資料來顯示文字內容。

```
ip.src_host== 192.168.157.145  &&  ip.dst_host== 192.168.157.144 &&
udp.length >200
```

進行時間排序，我找到第二個開始出入指令



需使用`gchq.github.io`轉換

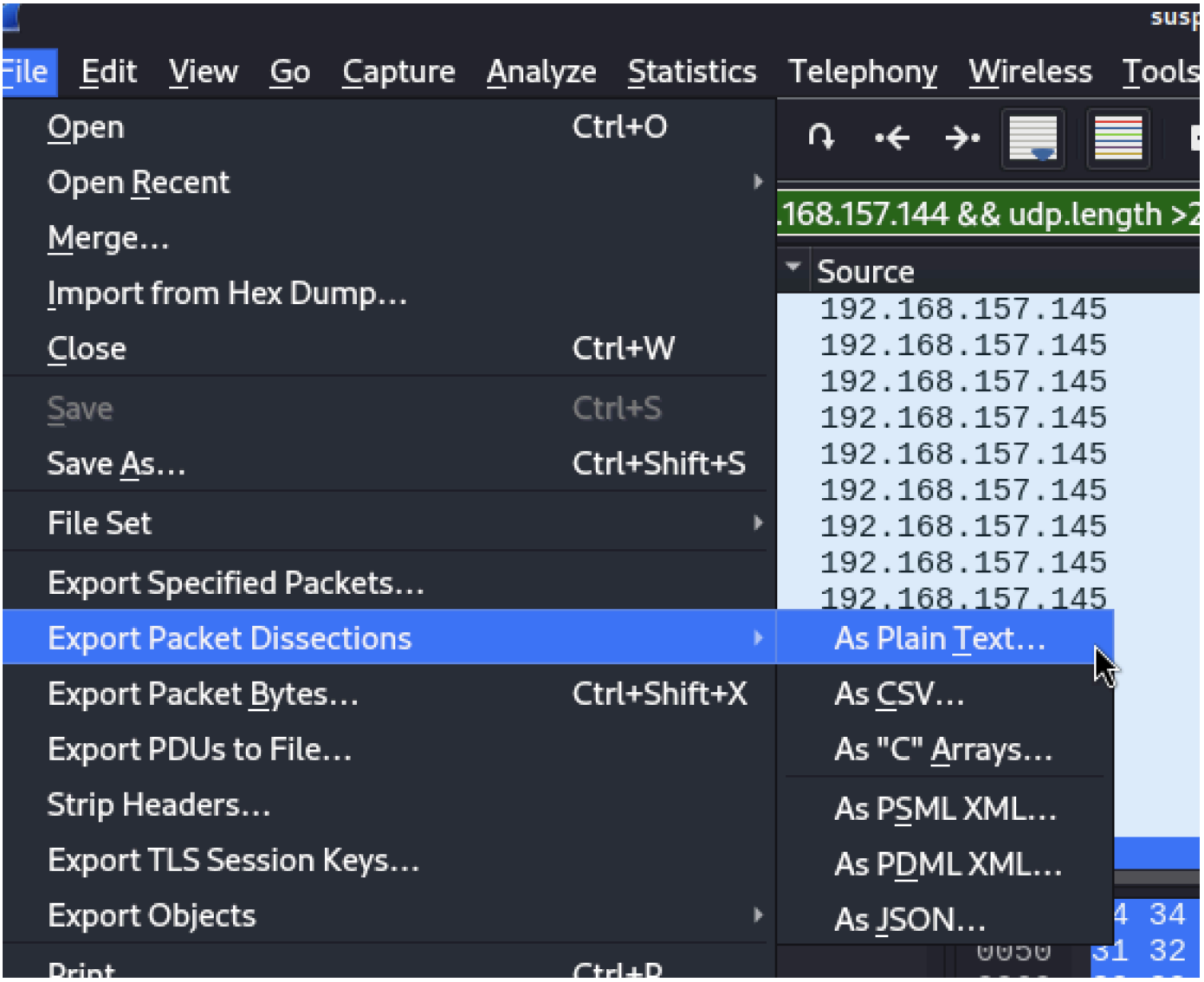


`whoami`

Task 4

What is the version of the DNS tunneling tool the attacker is using?

同上，使用另一個方式，存為文字



做法一：

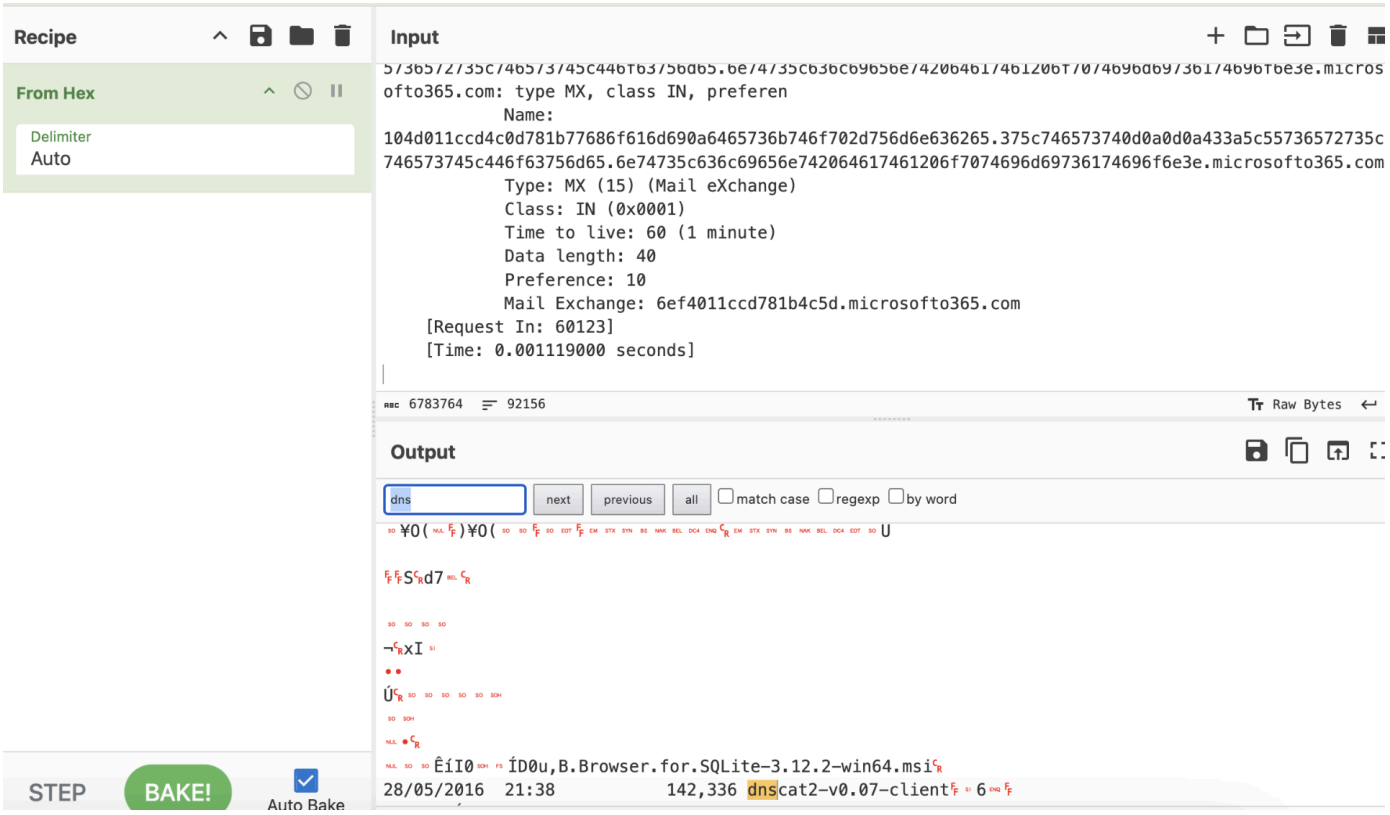
腳本：https://github.com/a6232283/HTB/blob/main/Sherlocks/wireshark_DNS.py

查詢DNS

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat 2.txt| grep dns
28/05/2016  21:38           142,336 dnscat2-v0.07-clientB.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016  21:38           142,336 dnscat2-v0.07-client-win32.exe
28/05/2016  21:38           142,336 dnscat2-v0.07-clientB.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016  21:38           142,336 dnscat2-v0.07-client-win32.exe
C:\Users\test\Downloads>ren ren dnscat2-v0.07-client-win32.exe
C:\Users\tren ren dnscat2-v0.07-client-win32.exe
C:\Users\tren ren 'dnscat2-v0.07-client-win32.exe' 'win_install.exe
The syntax of the command is incorrecren ren 'dnscat2-v0.07-client-win32.exe' 'win_install.exe
28/05/2016  21:38           142,336 dnscat2-v0.07-clientB.Browser.for.SQLite-3.12.2-win64.msi
28/05/2016  21:38           142,336 dnscat2-v0.07-client-win32.exe
C:\Users\test\Downloads>ren dnscat2-v0.07-client-win32.exe win_installer.exe
C:\Users\test\Downloads>ren dnscat2-v0.07-client-win32.exe win_installer.exe
```

做法二：

存為文字後，只接將文字轉換明文

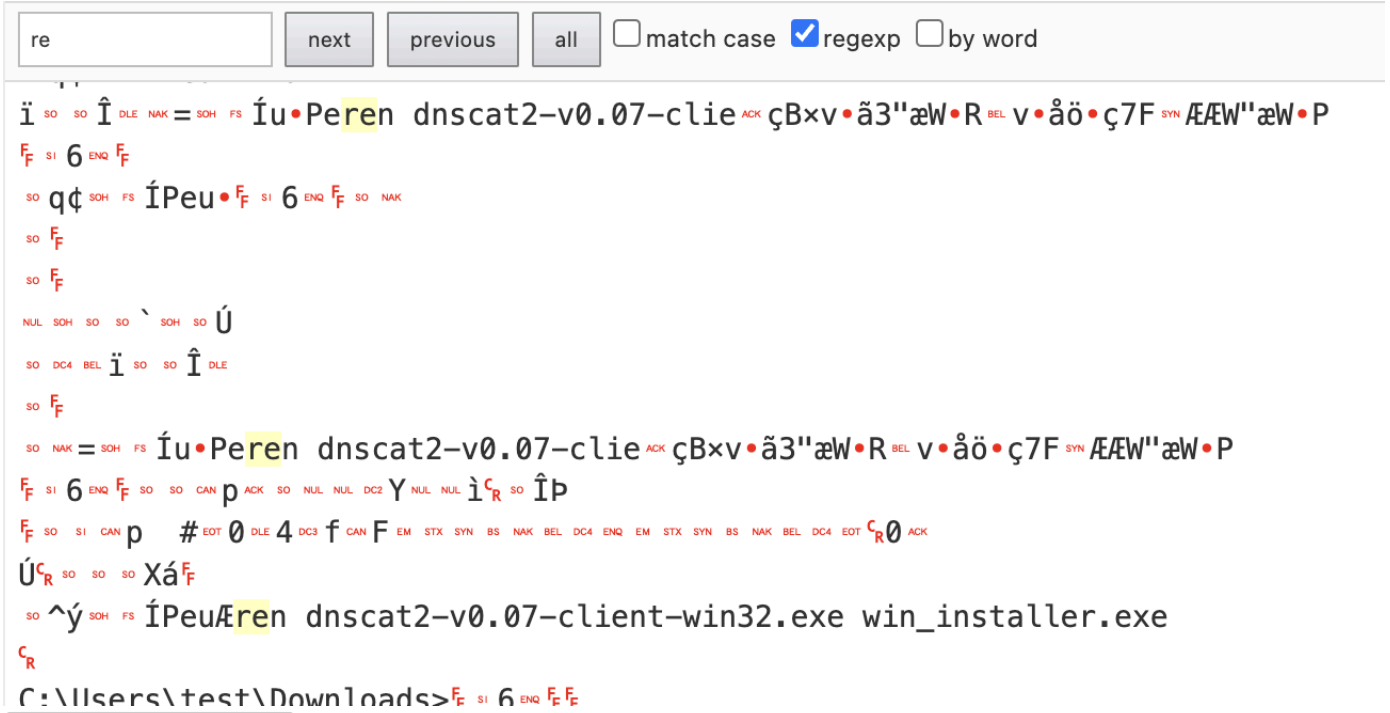


`0.07`

Task 5

The attackers attempts to rename the tool they accidentally left on the clients host. What do they name it to?

因為是windows所以指令為`ren`，前面一開始：`win_install.exe`是錯誤...



`win_installer.exe`

Task 6

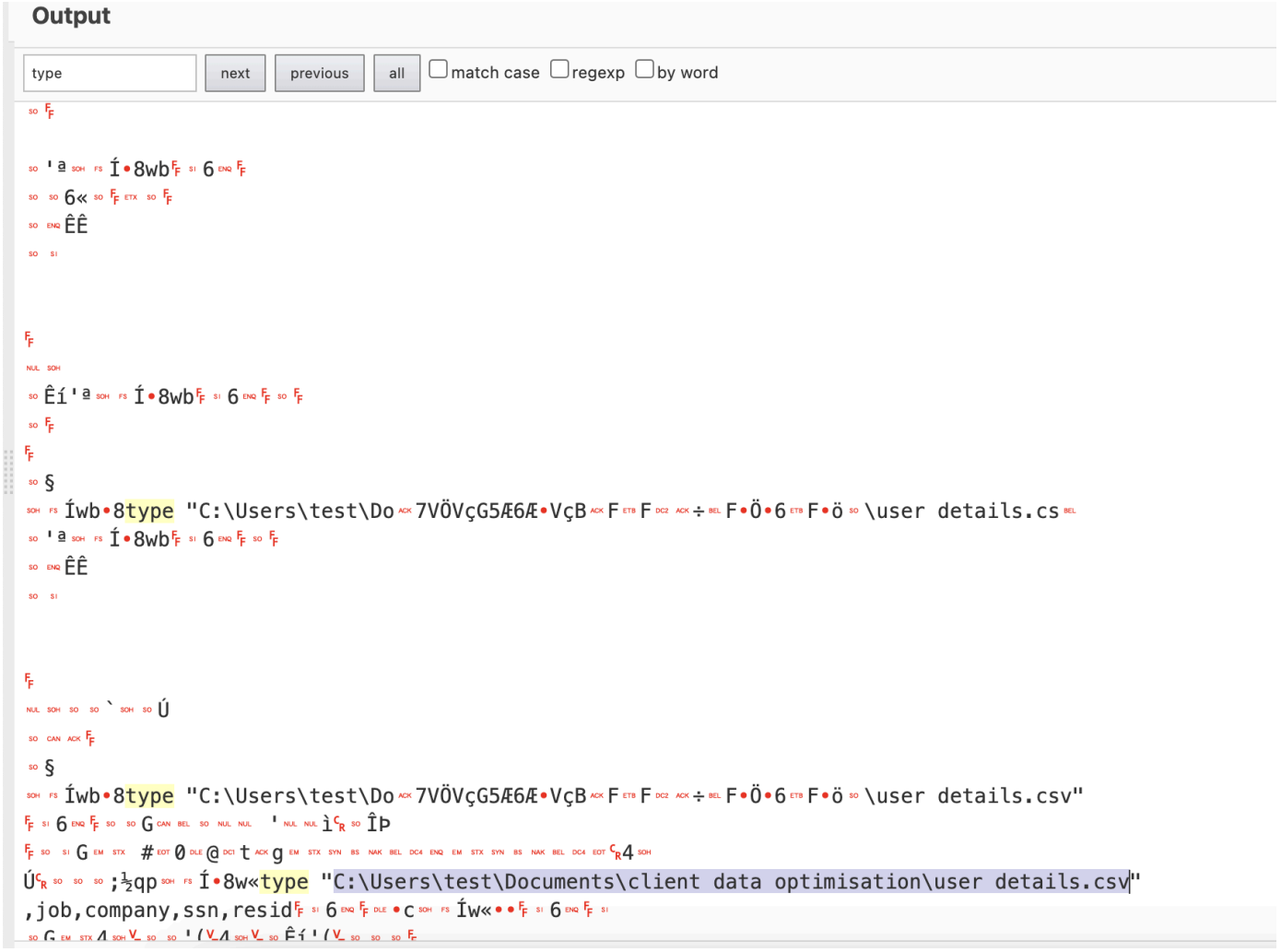
The attacker attempts to enumerate the users cloud storage. How many files do they locate in their cloud storage directory?

查詢各大公司、OneDrive都找不到
`0`

Task 7

What is the full location of the PII file that was stolen?

pll檔用途：儲存已編譯的函數或物件。
用查看`type`方式來尋找



`C:\Users\test\Documents\client data optimisation\user details.csv`

Task 8

Exactly how many customer PII records were stolen?

同上，開始第一數字為0最後為720
開始

```
,job,company,ssn,resid
qp Í•8w«type "C:\Users\test\Documents\client data optimisation\user details.csv"
,job,company,ssn,resid 6
@ï Î
•c Íw«•• 6 G Ì Îþ
G 2 .D5à Í••w$
0,Chief Tec 6
G 2 %`2 Êí%` Úzz
SRd7
¥Ö( )¥Ö(
Êí5à Í••$
0,Chief Tec 6
5à Í••w«ence,current_location,blood_group,website,username,name,sex,address,mail,birthdate
0,Chief Tec 6
"  «
Êí5à Í••w«ence,current_location,blood_group,website,username,name,sex,address,mail,birthdate
```

最後

```
ÊíW? Í–`w«",maria11@yahoo.com,1992-01-12
720,Ambulance person,"Smith, Collins and Brown",524-80-5753,"22 6
W? Í–`w«",maria11@yahoo.com,1992-01-12
720,Ambulance person,"Smith, Collins and Brown",524-80-5753,"22 6
```

721