0216002_詹昇 電腦安全_HW4

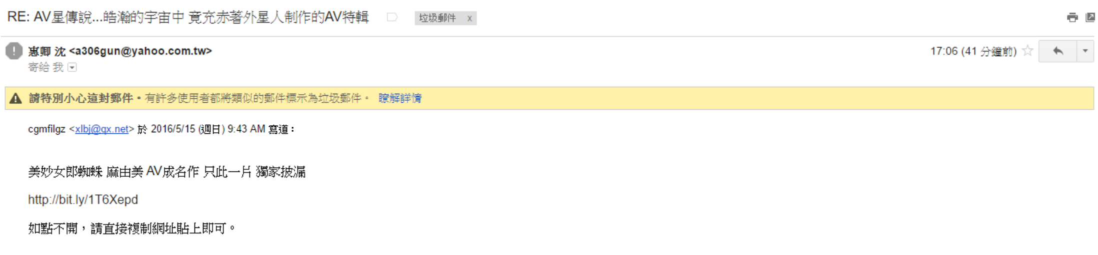
Homework #4 (chapters 6-8)

Due: 5/16 (Mon) in uploaded softcopy

(30 points)

1. Use all of WHOIS, Robtex, and PhishTank to trace back on a phishing email found in your mailbox. If you don't find one, create one email account and post the email address onto Web to solicit some. Show and discuss your findings.

我的釣魚信



RE: AV星傳說...皓瀚的宇宙中 竟充赤著外星人制作的AV特輯 垃圾郵件 x

惠卿 沈 <a306gun@yahoo.com.tw>
寄給 我

17:06 (41 分鐘前)

請特別小心這封郵件。有許多使用者都將類似的郵件標示為垃圾郵件。 瞭解詳情

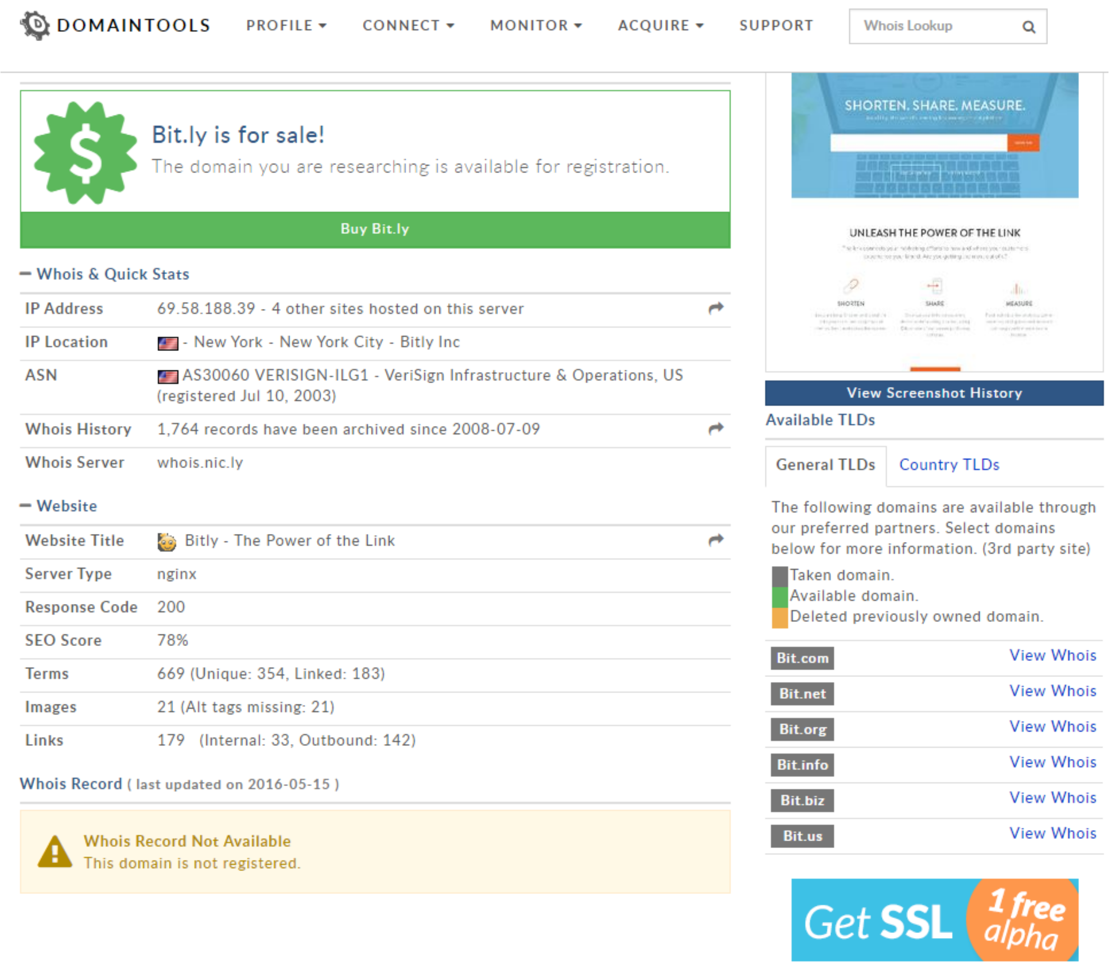
cgmfilgz <xlbj@qx.net> 於 2016/5/15 (週日) 9:43 AM 寫道：

美妙女郎蜘蛛 麻由美 AV成名作 只此一片 獨家披漏

http://bit.ly/1T6Xepd

如點不開，請直接複制網址貼上即可。

WHOIS



Bit.ly is for sale!

The domain you are researching is available for registration.

Buy Bit.ly

— Whois & Quick Stats

IP Address	69.58.188.39 - 4 other sites hosted on this server
IP Location	- New York - New York City - Bitly Inc
ASN	AS30060 VERISIGN-ILG1 - VeriSign Infrastructure & Operations, US (registered Jul 10, 2003)
Whois History	1,764 records have been archived since 2008-07-09
Whois Server	whois.nic.ly

— Website

Website Title	Bitly - The Power of the Link
Server Type	nginx
Response Code	200
SEO Score	78%
Terms	669 (Unique: 354, Linked: 183)
Images	21 (Alt tags missing: 21)
Links	179 (Internal: 33, Outbound: 142)

Whois Record (last updated on 2016-05-15)

Whois Record Not Available
This domain is not registered.

View Screenshot History

Available TLDs

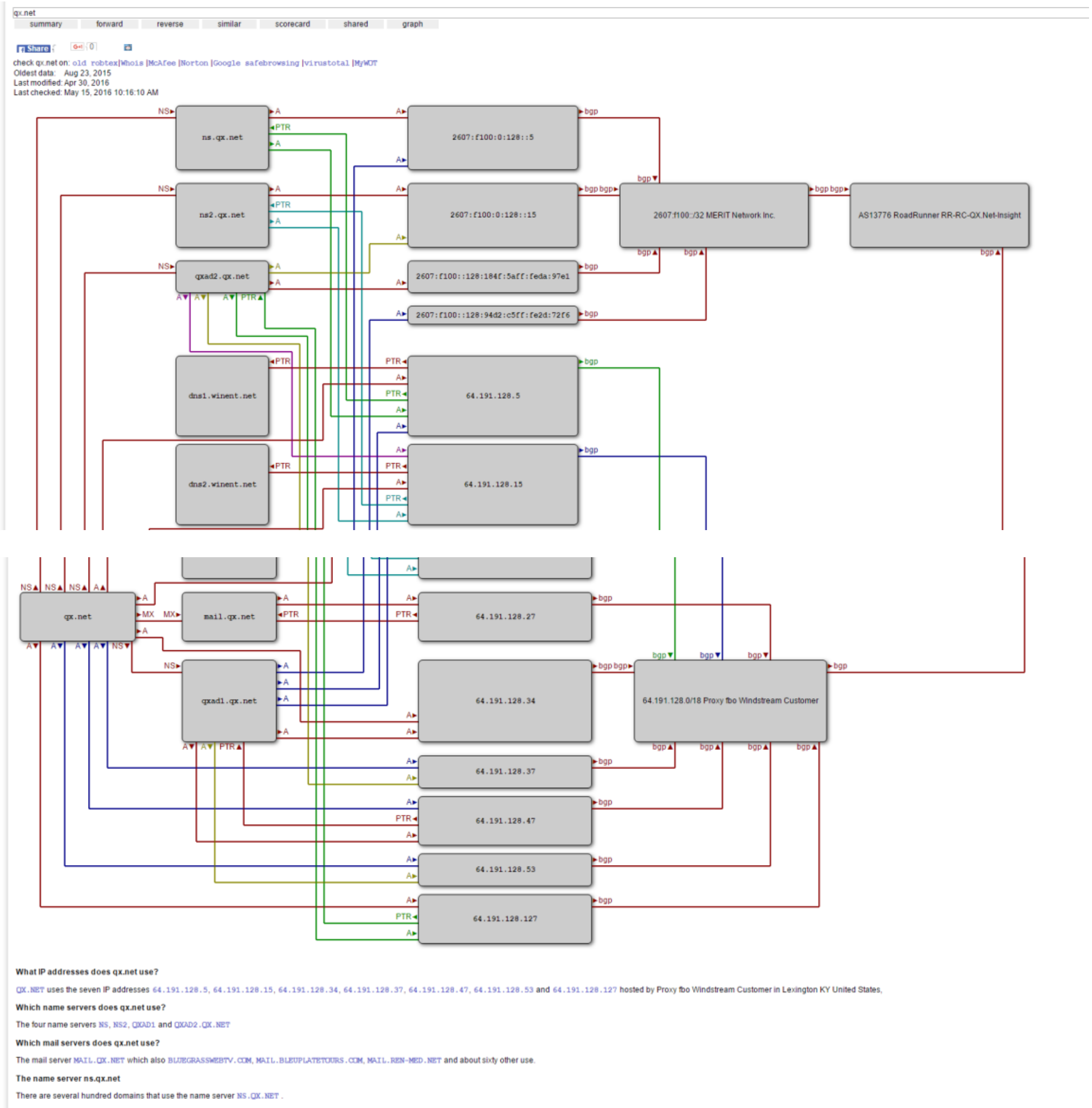
General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▨ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

Bit.com	View Whois
Bit.net	View Whois
Bit.org	View Whois
Bit.info	View Whois
Bit.biz	View Whois
Bit.us	View Whois

Robtex



check qx.net on: old robtex|Whois |McAfee |Norton |Google safebrowsing |virustotal |MyWOT
Oldest data: Aug 23, 2015
Last modified: Apr 30, 2016
Last checked: May 15, 2016 10:16:10 AM

What IP addresses does qx.net use?

QX.NET uses the seven IP addresses 64.191.128.5, 64.191.128.15, 64.191.128.34, 64.191.128.37, 64.191.128.47, 64.191.128.53 and 64.191.128.127 hosted by Proxy fbo Windstream Customer in Lexington KY United States,

Which name servers does qx.net use?

The four name servers NS, NS2, QXAD1 and QXAD2.QX.NET

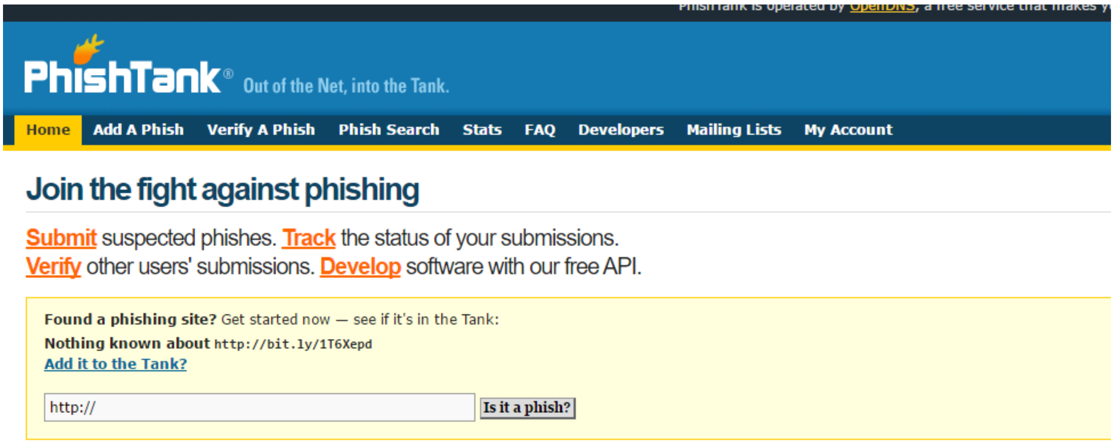
Which mail servers does qx.net use?

The mail server MAIL.QX.NET which also BLUEGRASSWEBTV.COM, MAIL.BLEUPLATETOURS.COM, MAIL.REN-MED.NET and about sixty other use.

The name server ns.qx.net

There are several hundred domains that use the name server NS.QX.NET .

PhishTank



Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

Nothing known about http://bit.ly/1T6Xepd

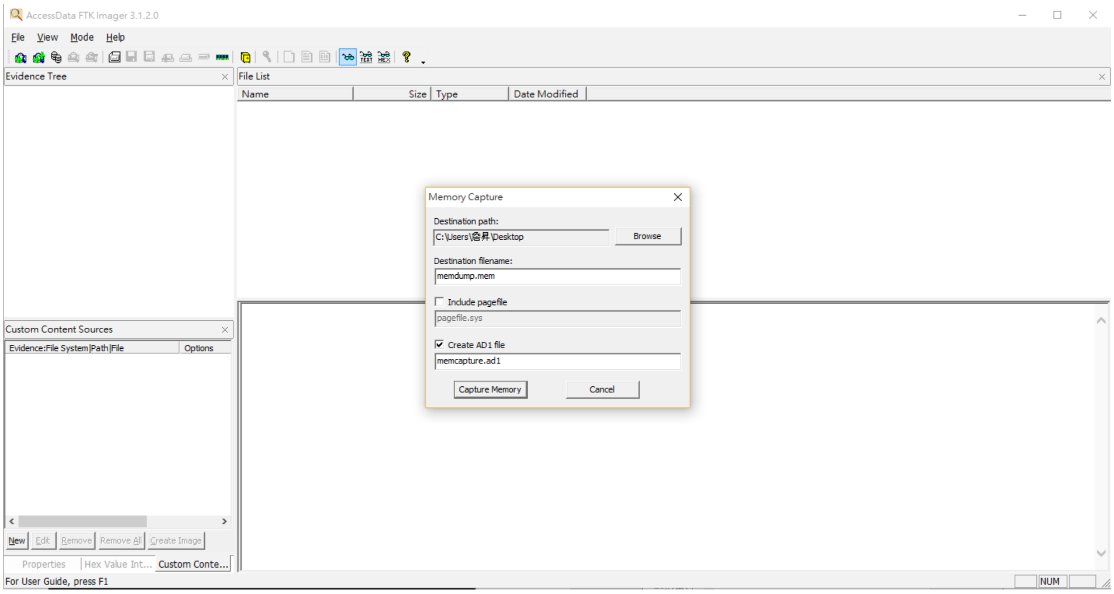
Add it to the Tank?

http://

使用 PhishTank 但似乎沒人貢獻到我要的資料

(30 points)

2. On Windows with some running processes connecting to the Internet, use FTK Imager to dump memory and then Volatility Framework to analyze the memory dump. Show processes with connections, and check whether they have DLLs.



Memory Capture

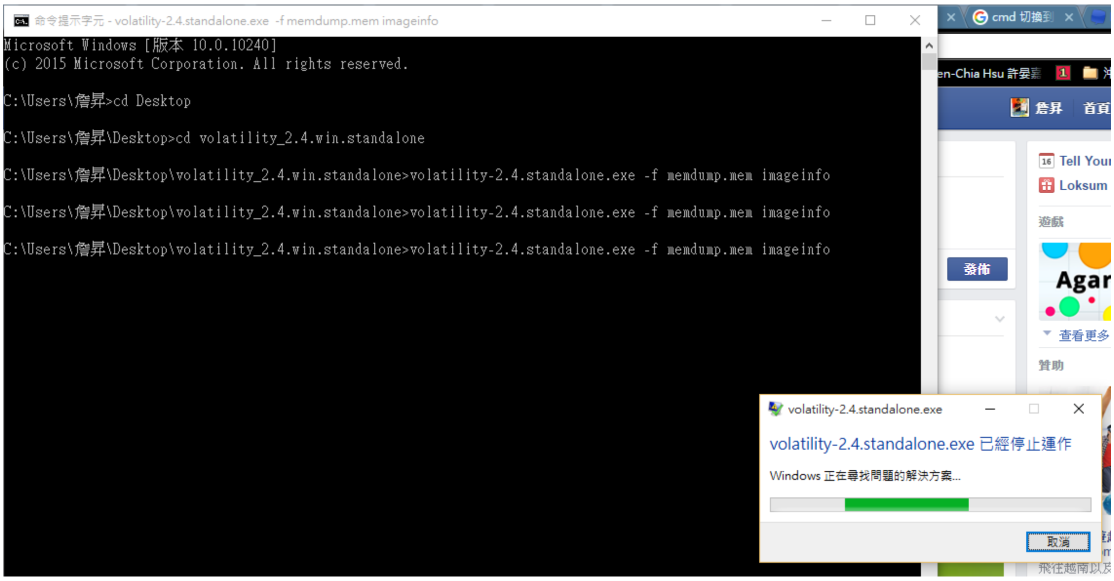
Destination path:
C:\Users\詹昇\Desktop
Browse

Destination filename:
memdump.mem

□ Include pagefile
pagefile.sys

☑ Create AD1 file
memcapture.ad1

Capture Memory
Cancel



```
Microsoft Windows [版本 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\詹昇>cd Desktop

C:\Users\詹昇\Desktop>cd volatility_2.4.win.standalone

C:\Users\詹昇\Desktop\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f memdump.mem imageinfo

C:\Users\詹昇\Desktop\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f memdump.mem imageinfo

C:\Users\詹昇\Desktop\volatility_2.4.win.standalone>volatility-2.4.standalone.exe -f memdump.mem imageinfo
```

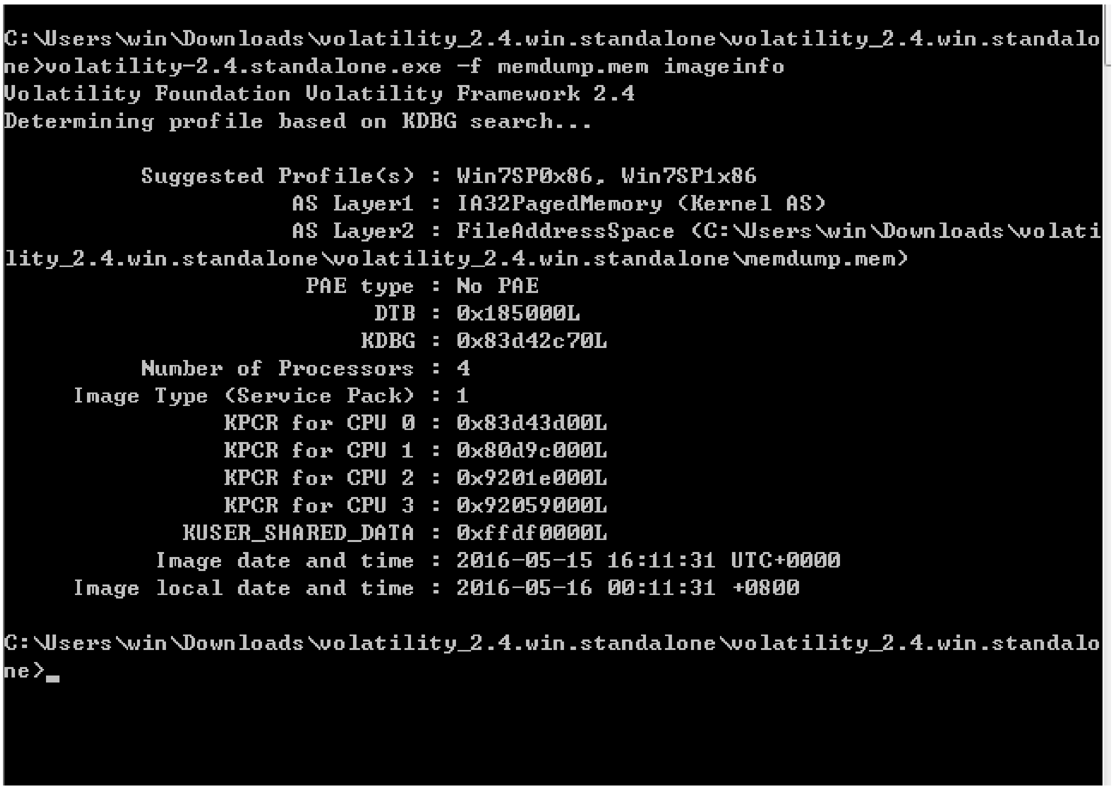
volatility-2.4.standalone.exe

volatility-2.4.standalone.exe 已經停止運作

Windows 正在尋找問題的解決方案...

取消

I can’t run volatility in my win10 so I run it on my win7 which is in Virtual Box

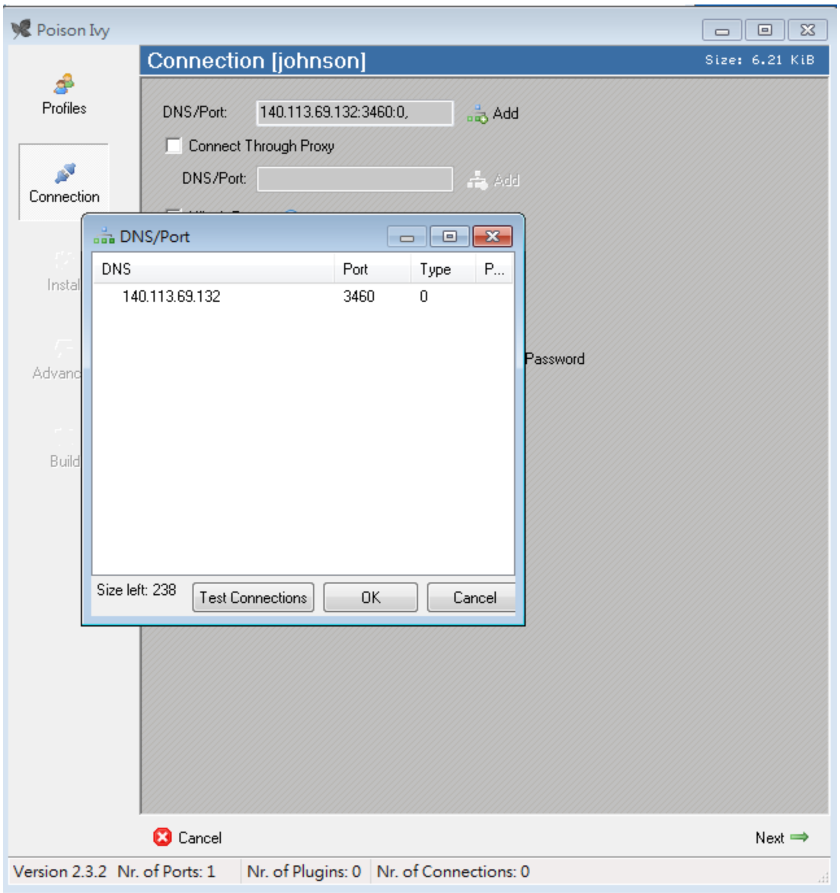


```
C:\Users\win\Downloads\volatility_2.4.win.standalone\volatility_2.4.win.standalo
ne>volatility-2.4.standalone.exe -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\win\Downloads\volati
lity_2.4.win.standalone\volatility_2.4.win.standalone\memdump.mem)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x83d42c70L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x83d43d00L
                KPCR for CPU 1 : 0x80d9c000L
                KPCR for CPU 2 : 0x9201e000L
                KPCR for CPU 3 : 0x92059000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-05-15 16:11:31 UTC+0000
     Image local date and time : 2016-05-16 00:11:31 +0800

C:\Users\win\Downloads\volatility_2.4.win.standalone\volatility_2.4.win.standalo
ne>_
```

(30 points)

3. Retrieve Poison Ivy RAT from the Internet. Use a program tracing tool you are familiar with to trace this RAT. Show how you trace the RAT with your tracing tool and summarize what modules this RAT contains.

0216002_詹昇 電腦安全_HW4



Connection [johnson]   Size: 6.21 KiB

DNS/Port: 140.113.69.132:3460:0,   Add

□ Connect Through Proxy

DNS/Port: Add

DNS/Port

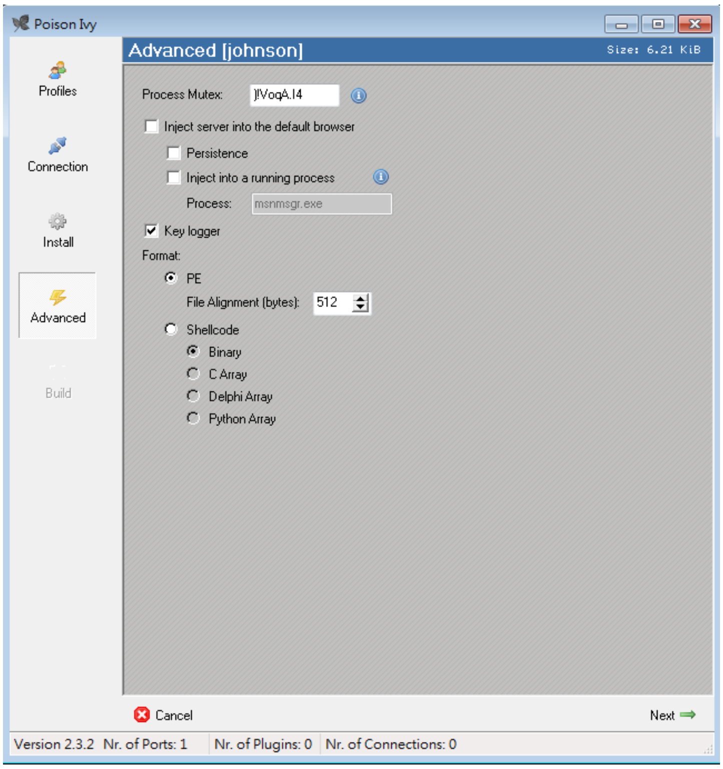
DNS	Port	Type	P...
140.113.69.132	3460	0	

Size left: 238   Test Connections   OK   Cancel

Password

Cancel   Next

Version 2.3.2   Nr. of Ports: 1   Nr. of Plugins: 0   Nr. of Connections: 0



Advanced [johnson]   Size: 6.21 KiB

Process Mutex:)!VoqA.I4

□ Inject server into the default browser

□ Persistence

□ Inject into a running process

Process: msnmsgr.exe

☑ Key logger

Format:

● PE

File Alignment (bytes): 512

○ Shellcode

● Binary

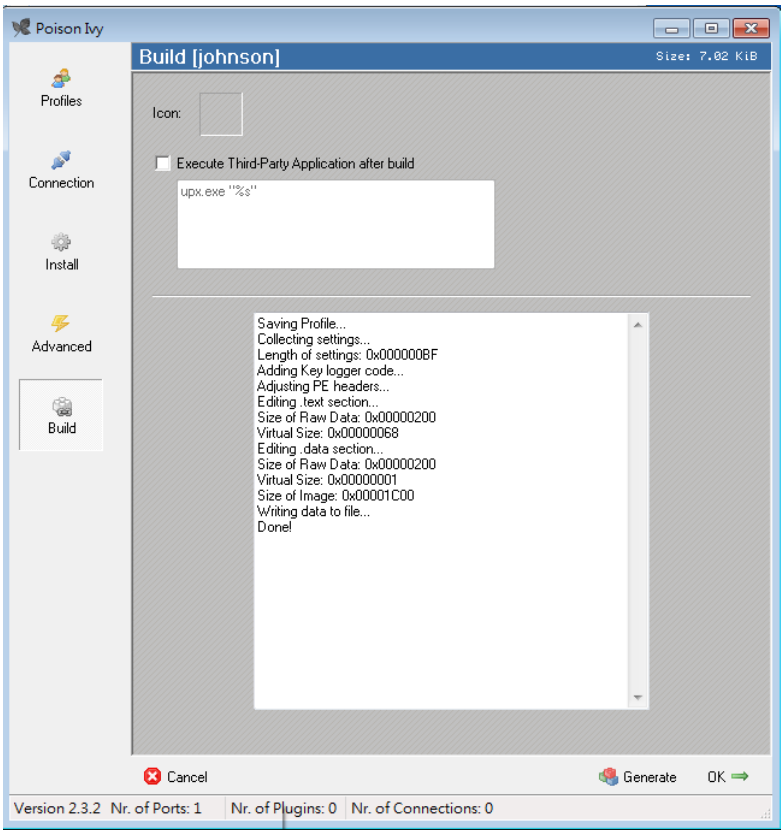
○ C Array

○ Delphi Array

○ Python Array

Cancel   Next

Version 2.3.2   Nr. of Ports: 1   Nr. of Plugins: 0   Nr. of Connections: 0



Build [johnson]   Size: 7.02 KiB

Icon:

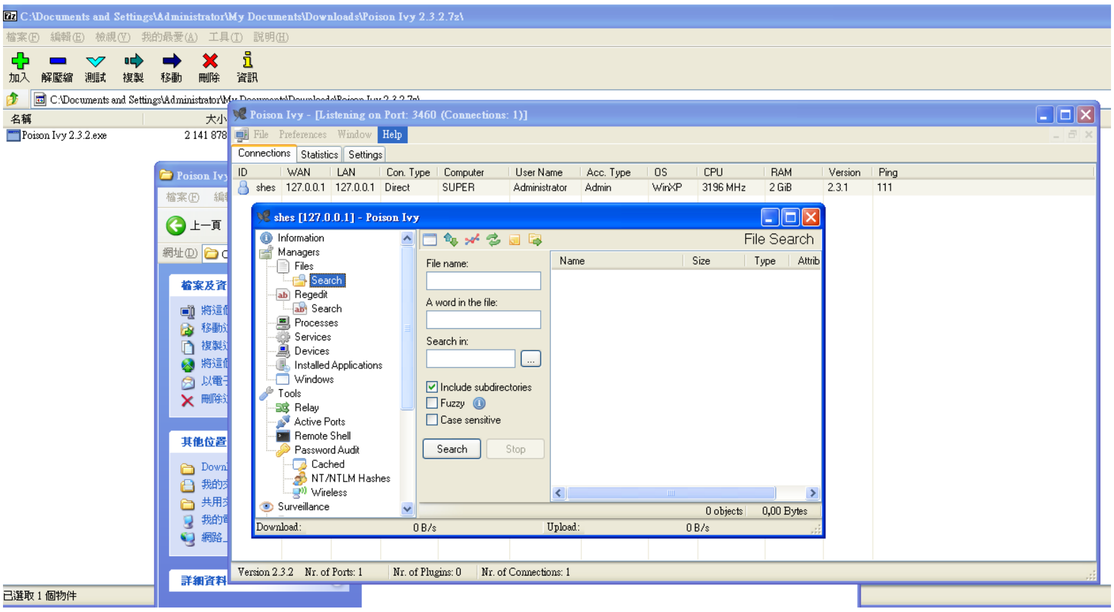
☐ Execute Third-Party Application after build

upx.exe "%s"

```
Saving Profile...
Collecting settings...
Length of settings: 0x000000BF
Adding Key logger code...
Adjusting PE headers...
Editing .text section...
Size of Raw Data: 0x00000200
Virtual Size: 0x00000068
Editing .data section...
Size of Raw Data: 0x00000200
Virtual Size: 0x00000001
Size of Image: 0x00001C00
Writing data to file...
Done!
```

Version 2.3.2   Nr. of Ports: 1   Nr. of Plugins: 0   Nr. of Connections: 0

後來改用 WINXP 繼續用



C:\Documents and Settings\Administrator\My Documents\Downloads\Poison Ivy 2.3.2.7z\

名稱	大小
Poison Ivy 2.3.2.exe	2 141 878

Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

ID	WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version	Ping
shes	127.0.0.1	127.0.0.1	Direct	SUPER	Administrator	Admin	WinXP	3196 MHz	2 GiB	2.3.1	111

shes [127.0.0.1] - Poison Ivy

File Search

File name:

A word in the file:

Search in:

☑ Include subdirectories
☐ Fuzzy
☐ Case sensitive

Name	Size	Type	Attrib

0 objects   0,00 Bytes

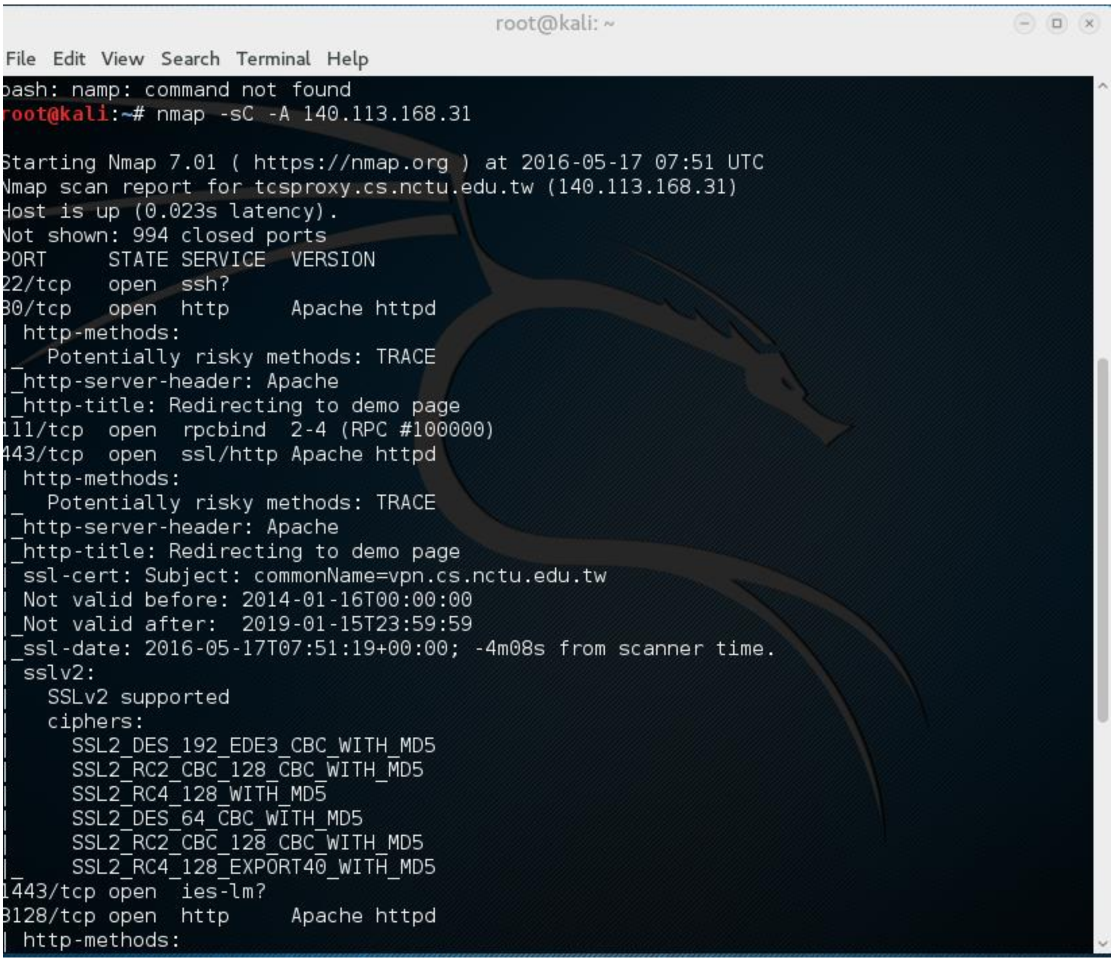
Download: 0 B/s   Upload: 0 B/s

Version 2.3.2   Nr. of Ports: 1   Nr. of Plugins: 0   Nr. of Connections: 1

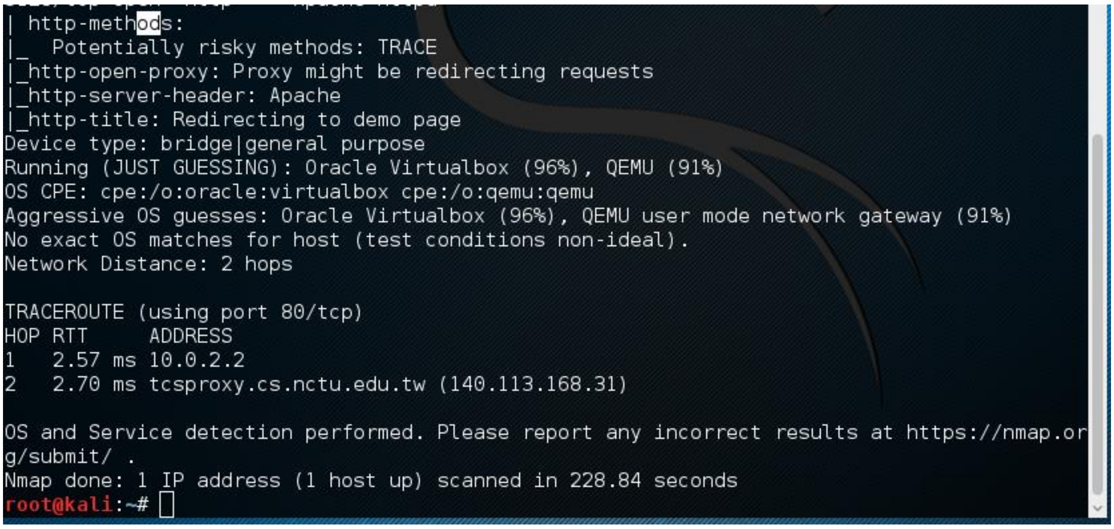
已選取 1 個物件

(20 points)

4. Use Nmap, NTA Monitor, IKEProbe to identify whether a target VPN server supports Aggressive mode. Screen dump “useful” results and explain.

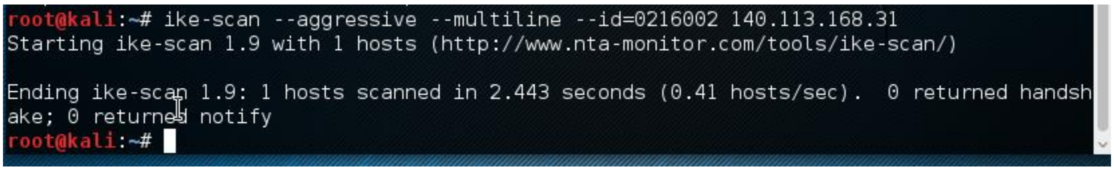


```
bash: namp: command not found
root@kali:~# nmap -sC -A 140.113.168.31

Starting Nmap 7.01 ( https://nmap.org ) at 2016-05-17 07:51 UTC
Nmap scan report for tcsproxy.cs.nctu.edu.tw (140.113.168.31)
Host is up (0.023s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh?
80/tcp   open  http     Apache httpd
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache
|_http-title: Redirecting to demo page
111/tcp  open  rpcbind  2-4 (RPC #100000)
443/tcp  open  ssl/http Apache httpd
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache
|_http-title: Redirecting to demo page
| ssl-cert: Subject: commonName=vpn.cs.nctu.edu.tw
| Not valid before: 2014-01-16T00:00:00
|_Not valid after:  2019-01-15T23:59:59
|_ssl-date: 2016-05-17T07:51:19+00:00; -4m08s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
1443/tcp open  ies-lm?
3128/tcp open  http     Apache httpd
| http-methods:
```



```
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache
|_http-title: Redirecting to demo page
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/o:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.57 ms 10.0.2.2
2   2.70 ms tcsproxy.cs.nctu.edu.tw (140.113.168.31)

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 228.84 seconds
root@kali:~# 
```

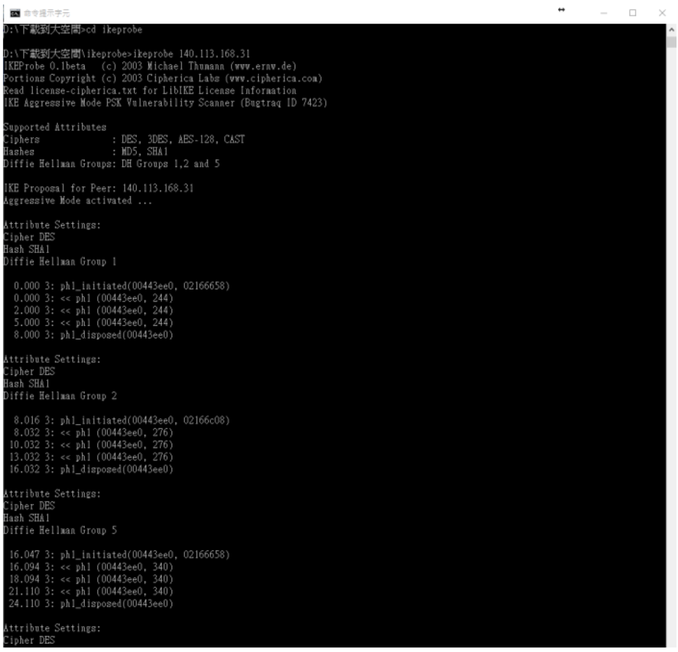
NTA monitor (parameter --aggressive) aggressive mode scan results :



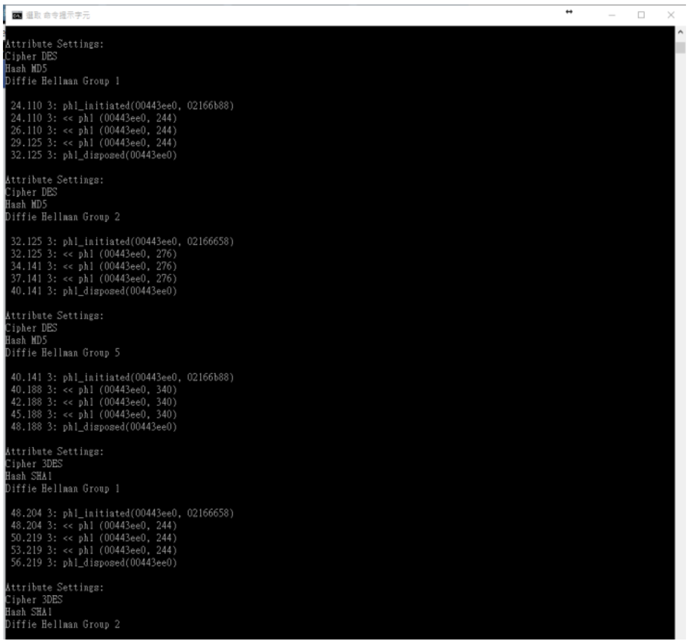
```
root@kali:~# ike-scan --aggressive --multiline --id=0216002 140.113.168.31
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

Ending ike-scan 1.9: 1 hosts scanned in 2.443 seconds (0.41 hosts/sec).  0 returned handsh
ake; 0 returned notify
root@kali:~# 
```

IKEProbe aggressive mode scan results :

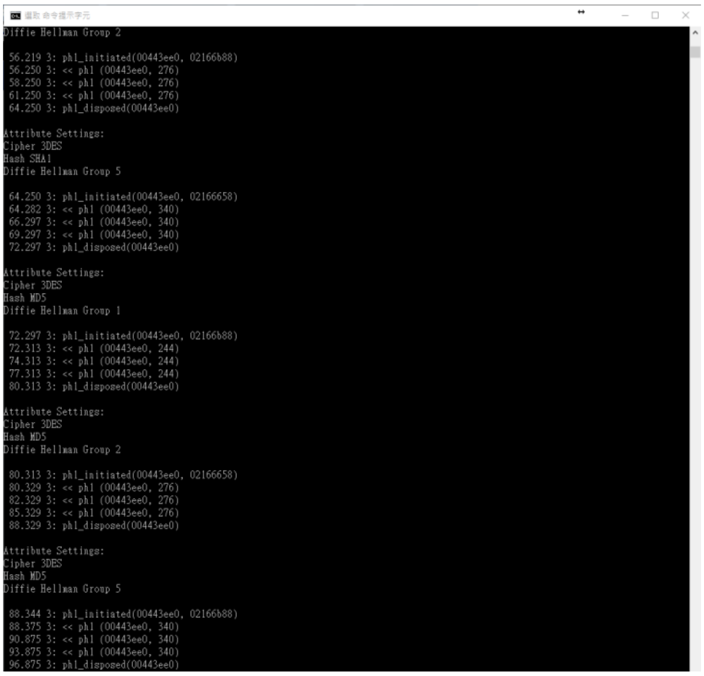
0216002_詹昇 電腦安全_HW4



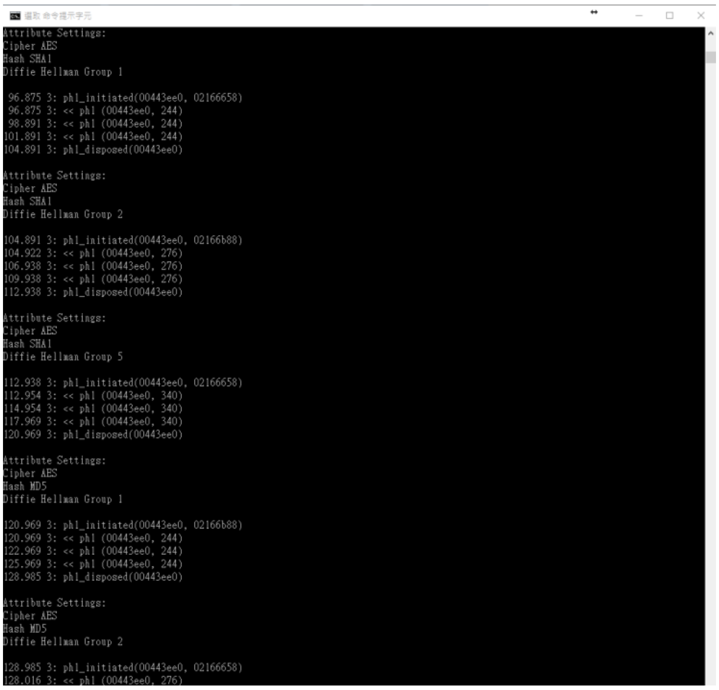
```
D:\下載到大空間>cd ikeprobe

D:\下載到大空間\ikeprobe>ikeprobe 140.113.168.31
IKEProbe 0.1beta   (c) 2003 Michael Thumann (www.ernw.de)
Portions Copyright (c) 2003 Cipherica Labs (www.cipherica.com)
Read license-cipherica.txt for LibIKE License Information
IKE Aggressive Mode PSK Vulnerability Scanner (Bugtraq ID 7423)

Supported Attributes
Ciphers             : DES, 3DES, AES-128, CAST
Hashes              : MD5, SHA1
Diffie Hellman Groups: DH Groups 1,2 and 5

IKE Proposal for Peer: 140.113.168.31
Aggressive Mode activated ...

Attribute Settings:
Cipher DES
Hash SHA1
Diffie Hellman Group 1

  0.000 3: ph1_initiated(00443ee0, 02166658)
  0.000 3: << ph1 (00443ee0, 244)
  2.000 3: << ph1 (00443ee0, 244)
  5.000 3: << ph1 (00443ee0, 244)
  8.000 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher DES
Hash SHA1
Diffie Hellman Group 2

  8.016 3: ph1_initiated(00443ee0, 02166c08)
  8.032 3: << ph1 (00443ee0, 276)
 10.032 3: << ph1 (00443ee0, 276)
 13.032 3: << ph1 (00443ee0, 276)
 16.032 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher DES
Hash SHA1
Diffie Hellman Group 5

 16.047 3: ph1_initiated(00443ee0, 02166658)
 16.094 3: << ph1 (00443ee0, 340)
 18.094 3: << ph1 (00443ee0, 340)
 21.110 3: << ph1 (00443ee0, 340)
 24.110 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher DES
```



```
Attribute Settings:
Cipher DES
Hash MD5
Diffie Hellman Group 1

 24.110 3: ph1_initiated(00443ee0, 02166b88)
 24.110 3: << ph1 (00443ee0, 244)
 26.110 3: << ph1 (00443ee0, 244)
 29.125 3: << ph1 (00443ee0, 244)
 32.125 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher DES
Hash MD5
Diffie Hellman Group 2

 32.125 3: ph1_initiated(00443ee0, 02166658)
 32.125 3: << ph1 (00443ee0, 276)
 34.141 3: << ph1 (00443ee0, 276)
 37.141 3: << ph1 (00443ee0, 276)
 40.141 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher DES
Hash MD5
Diffie Hellman Group 5

 40.141 3: ph1_initiated(00443ee0, 02166b88)
 40.188 3: << ph1 (00443ee0, 340)
 42.188 3: << ph1 (00443ee0, 340)
 45.188 3: << ph1 (00443ee0, 340)
 48.188 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash SHA1
Diffie Hellman Group 1

 48.204 3: ph1_initiated(00443ee0, 02166658)
 48.204 3: << ph1 (00443ee0, 244)
 50.219 3: << ph1 (00443ee0, 244)
 53.219 3: << ph1 (00443ee0, 244)
 56.219 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash SHA1
Diffie Hellman Group 2
```

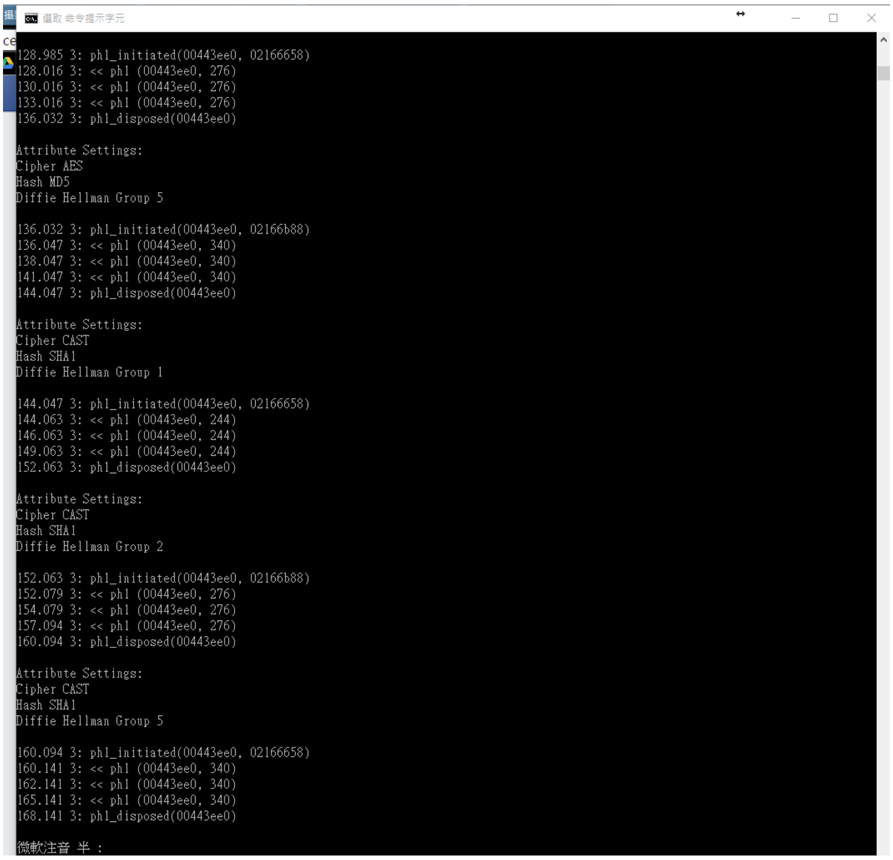


```
Diffie Hellman Group 2

 56.219 3: ph1_initiated(00443ee0, 02166b88)
 56.250 3: << ph1 (00443ee0, 276)
 58.250 3: << ph1 (00443ee0, 276)
 61.250 3: << ph1 (00443ee0, 276)
 64.250 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash SHA1
Diffie Hellman Group 5

 64.250 3: ph1_initiated(00443ee0, 02166658)
 64.282 3: << ph1 (00443ee0, 340)
 66.297 3: << ph1 (00443ee0, 340)
 69.297 3: << ph1 (00443ee0, 340)
 72.297 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash MD5
Diffie Hellman Group 1

 72.297 3: ph1_initiated(00443ee0, 02166b88)
 72.313 3: << ph1 (00443ee0, 244)
 74.313 3: << ph1 (00443ee0, 244)
 77.313 3: << ph1 (00443ee0, 244)
 80.313 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash MD5
Diffie Hellman Group 2

 80.313 3: ph1_initiated(00443ee0, 02166658)
 80.329 3: << ph1 (00443ee0, 276)
 82.329 3: << ph1 (00443ee0, 276)
 85.329 3: << ph1 (00443ee0, 276)
 88.329 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher 3DES
Hash MD5
Diffie Hellman Group 5

 88.344 3: ph1_initiated(00443ee0, 02166b88)
 88.375 3: << ph1 (00443ee0, 340)
 90.875 3: << ph1 (00443ee0, 340)
 93.875 3: << ph1 (00443ee0, 340)
 96.875 3: ph1_disposed(00443ee0)
```

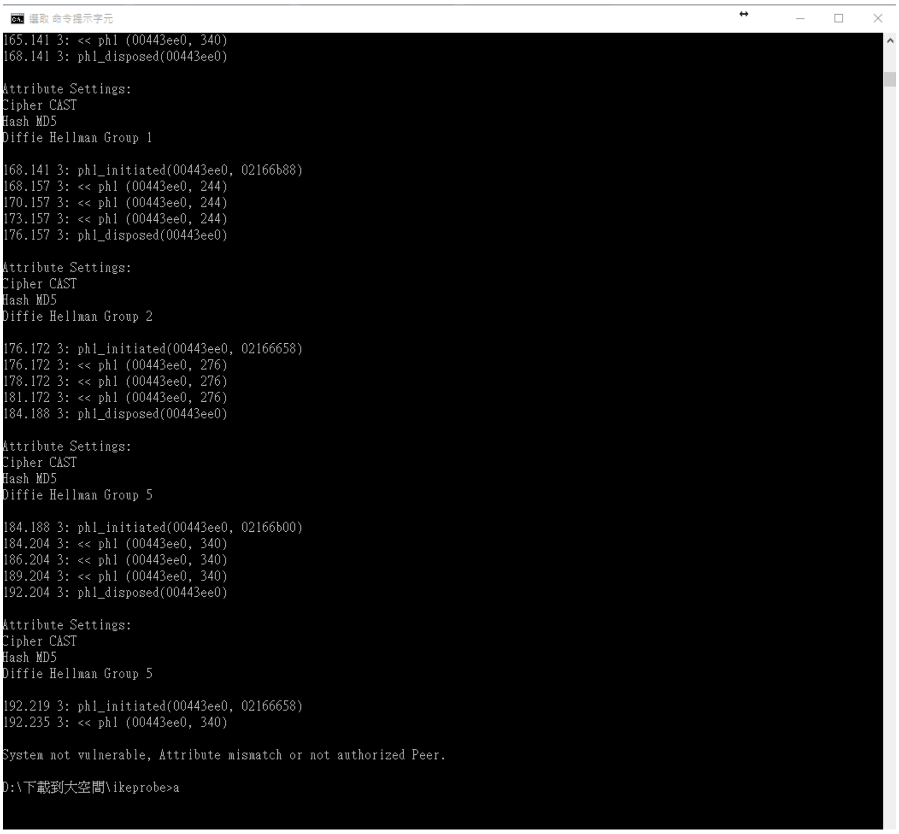


```
Attribute Settings:
Cipher AES
Hash SHA1
Diffie Hellman Group 1

 96.875 3: ph1_initiated(00443ee0, 02166658)
 96.875 3: << ph1 (00443ee0, 244)
 98.891 3: << ph1 (00443ee0, 244)
101.891 3: << ph1 (00443ee0, 244)
104.891 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher AES
Hash SHA1
Diffie Hellman Group 2

104.891 3: ph1_initiated(00443ee0, 02166b88)
104.922 3: << ph1 (00443ee0, 276)
106.938 3: << ph1 (00443ee0, 276)
109.938 3: << ph1 (00443ee0, 276)
112.938 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher AES
Hash SHA1
Diffie Hellman Group 5

112.938 3: ph1_initiated(00443ee0, 02166658)
112.954 3: << ph1 (00443ee0, 340)
114.954 3: << ph1 (00443ee0, 340)
117.969 3: << ph1 (00443ee0, 340)
120.969 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher AES
Hash MD5
Diffie Hellman Group 1

120.969 3: ph1_initiated(00443ee0, 02166b88)
120.969 3: << ph1 (00443ee0, 244)
122.969 3: << ph1 (00443ee0, 244)
125.969 3: << ph1 (00443ee0, 244)
128.985 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher AES
Hash MD5
Diffie Hellman Group 2

128.985 3: ph1_initiated(00443ee0, 02166658)
128.016 3: << ph1 (00443ee0, 276)
```

0216002_詹昇 電腦安全_HW4



```
128.985 3: ph1_initiated(00443ee0, 02166658)
128.016 3: << ph1 (00443ee0, 276)
130.016 3: << ph1 (00443ee0, 276)
133.016 3: << ph1 (00443ee0, 276)
136.032 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher AES
Hash MD5
Diffie Hellman Group 5

136.032 3: ph1_initiated(00443ee0, 02166b88)
136.047 3: << ph1 (00443ee0, 340)
138.047 3: << ph1 (00443ee0, 340)
141.047 3: << ph1 (00443ee0, 340)
144.047 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash SHA1
Diffie Hellman Group 1

144.047 3: ph1_initiated(00443ee0, 02166658)
144.063 3: << ph1 (00443ee0, 244)
146.063 3: << ph1 (00443ee0, 244)
149.063 3: << ph1 (00443ee0, 244)
152.063 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash SHA1
Diffie Hellman Group 2

152.063 3: ph1_initiated(00443ee0, 02166b88)
152.079 3: << ph1 (00443ee0, 276)
154.079 3: << ph1 (00443ee0, 276)
157.094 3: << ph1 (00443ee0, 276)
160.094 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash SHA1
Diffie Hellman Group 5

160.094 3: ph1_initiated(00443ee0, 02166658)
160.141 3: << ph1 (00443ee0, 340)
162.141 3: << ph1 (00443ee0, 340)
165.141 3: << ph1 (00443ee0, 340)
168.141 3: ph1_disposed(00443ee0)

微軟注音 半：
```

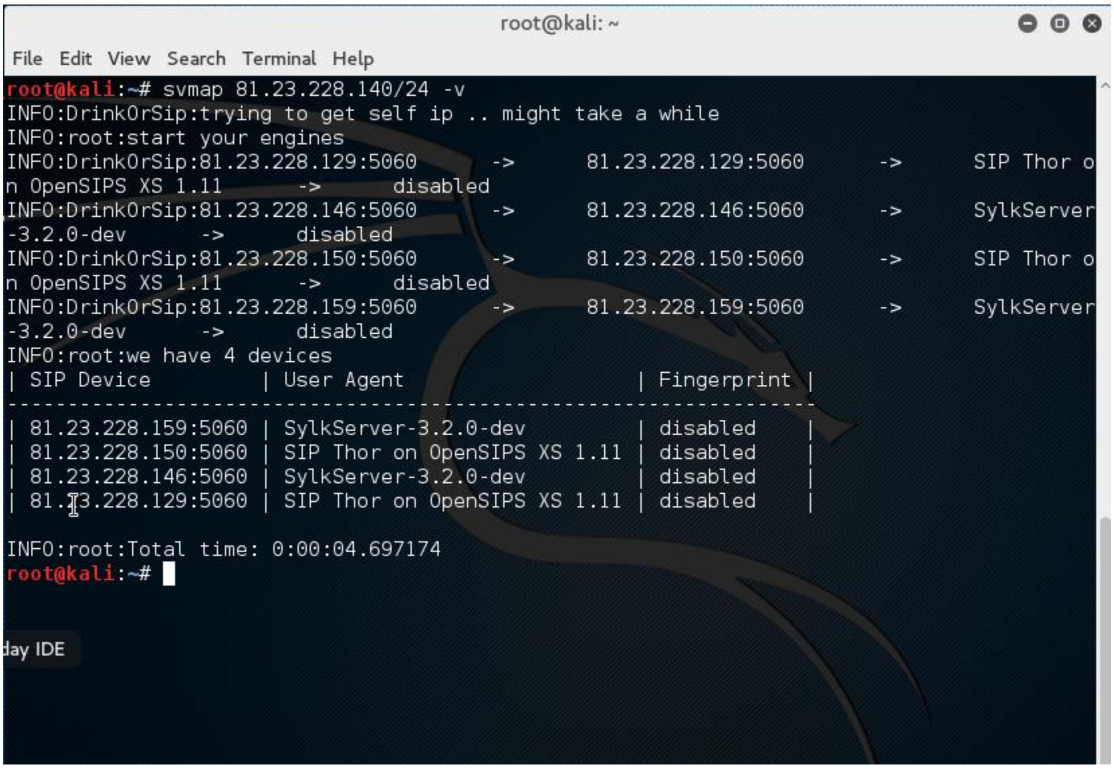


```
165.141 3: << ph1 (00443ee0, 340)
168.141 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 1

168.141 3: ph1_initiated(00443ee0, 02166b88)
168.157 3: << ph1 (00443ee0, 244)
170.157 3: << ph1 (00443ee0, 244)
173.157 3: << ph1 (00443ee0, 244)
176.157 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 2

176.172 3: ph1_initiated(00443ee0, 02166658)
176.172 3: << ph1 (00443ee0, 276)
178.172 3: << ph1 (00443ee0, 276)
181.172 3: << ph1 (00443ee0, 276)
184.188 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 5

184.188 3: ph1_initiated(00443ee0, 02166b00)
184.204 3: << ph1 (00443ee0, 340)
186.204 3: << ph1 (00443ee0, 340)
189.204 3: << ph1 (00443ee0, 340)
192.204 3: ph1_disposed(00443ee0)

Attribute Settings:
Cipher CAST
Hash MD5
Diffie Hellman Group 5

192.219 3: ph1_initiated(00443ee0, 02166658)
192.235 3: << ph1 (00443ee0, 340)

System not vulnerable, Attribute mismatch or not authorized Peer.

D:\下載到大空間\ikeprobe>a
```

From my observation,the target VPN server(NCTU CS VPN) does not support aggressive mode. Because no handshake be returned.

(20 points)

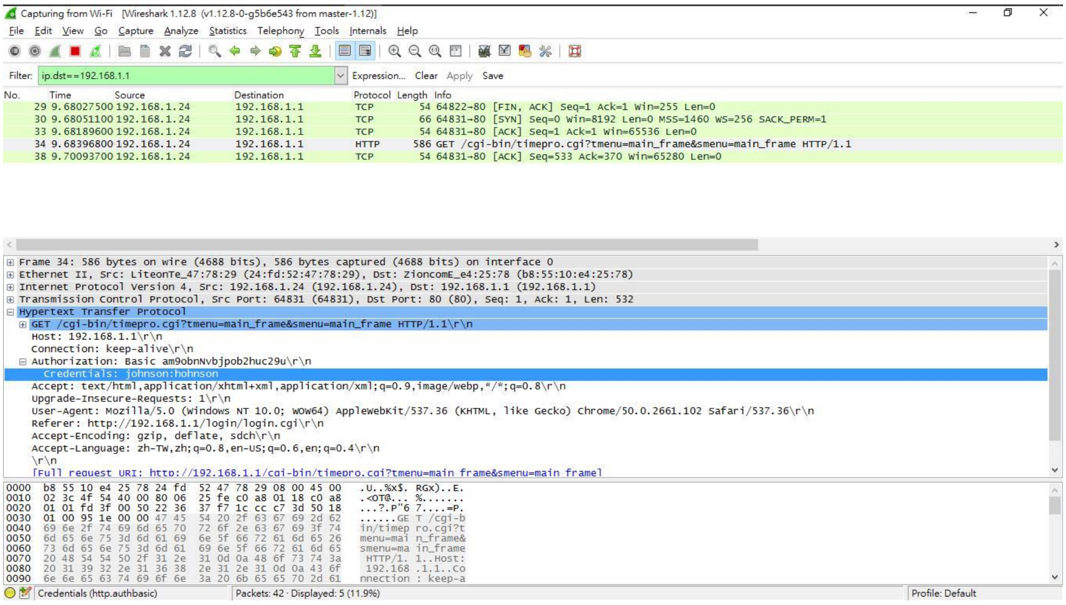
5. Use [redacted], SIPVicious to scan a public SIP server. Screen dump “useful” results and explain.



```
root@kali:~# svmap 81.23.228.140/24 -v
INFO:DrinkOrSip:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:DrinkOrSip:81.23.228.129:5060      ->      81.23.228.129:5060      ->      SIP Thor o
n OpenSIPS XS 1.11      ->      disabled
INFO:DrinkOrSip:81.23.228.146:5060      ->      81.23.228.146:5060      ->      SylkServer
-3.2.0-dev      ->      disabled
INFO:DrinkOrSip:81.23.228.150:5060      ->      81.23.228.150:5060      ->      SIP Thor o
n OpenSIPS XS 1.11      ->      disabled
INFO:DrinkOrSip:81.23.228.159:5060      ->      81.23.228.159:5060      ->      SylkServer
-3.2.0-dev      ->      disabled
INFO:root:we have 4 devices
| SIP Device           | User Agent                   | Fingerprint |
--------------------------------------------------------------------
| 81.23.228.159:5060 | SylkServer-3.2.0-dev         | disabled    |
| 81.23.228.150:5060 | SIP Thor on OpenSIPS XS 1.11 | disabled    |
| 81.23.228.146:5060 | SylkServer-3.2.0-dev         | disabled    |
| 81.23.228.129:5060 | SIP Thor on OpenSIPS XS 1.11 | disabled    |

INFO:root:Total time: 0:00:04.697174
root@kali:~# 
```

(30 points)

6. Setup your own client and an AP, or find an existing AP, running no encryption. Use wireshark or airodump-ng to sniff and decode data frames. Show and discuss your findings.



Capturing from Wi-Fi [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.dst==192.168.1.1

```
No.   Time       Source        Destination   Protocol Length Info
   29 9.68027500 192.168.1.24  192.168.1.1   TCP       54 64822→80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
   30 9.68051100 192.168.1.24  192.168.1.1   TCP       66 64831→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   33 9.68189600 192.168.1.24  192.168.1.1   TCP       54 64831→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   34 9.68396800 192.168.1.24  192.168.1.1   HTTP     586 GET /cgi-bin/timepro.cgi?tmenu=main_frame&smenu=main_frame HTTP/1.1
   38 9.70093700 192.168.1.24  192.168.1.1   TCP       54 64831→80 [ACK] Seq=533 Ack=370 Win=65280 Len=0
```

```
⊞ Frame 34: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on interface 0
⊞ Ethernet II, Src: LiteonTe_47:78:29 (24:fd:52:47:78:29), Dst: ZioncomE_e4:25:78 (b8:55:10:e4:25:78)
⊞ Internet Protocol Version 4, Src: 192.168.1.24 (192.168.1.24), Dst: 192.168.1.1 (192.168.1.1)
⊞ Transmission Control Protocol, Src Port: 64831 (64831), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 532
⊟ Hypertext Transfer Protocol
  ⊞ GET /cgi-bin/timepro.cgi?tmenu=main_frame&smenu=main_frame HTTP/1.1\r\n
    Host: 192.168.1.1\r\n
    Connection: keep-alive\r\n
  ⊟ Authorization: Basic am9obnNvbjpob2huc29u\r\n
      Credentials: johnson:hohnson
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36\r\n
    Referer: http://192.168.1.1/login/login.cgi\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4\r\n
    \r\n
    [Full request URI: http://192.168.1.1/cgi-bin/timepro.cgi?tmenu=main_frame&smenu=main_frame]
```

```
0000  b8 55 10 e4 25 78 24 fd  52 47 78 29 08 00 45 00   .U..%x$. RGx)..E.
0010  02 3c 4f 54 40 00 80 06  25 fe c0 a8 01 18 c0 a8   .<OT@... %.......
0020  01 01 fd 3f 00 50 22 36  37 f7 1c cc c7 3d 50 18   ...?.P"6 7....=P.
0030  01 00 95 1e 00 00 47 45  54 20 2f 63 67 69 2d 62   ......GE T /cgi-b
0040  69 6e 2f 74 69 6d 65 70  72 6f 2e 63 67 69 3f 74   in/timep ro.cgi?t
0050  6d 65 6e 75 3d 6d 61 69  6e 5f 66 72 61 6d 65 26   menu=mai n_frame&
0060  73 6d 65 6e 75 3d 6d 61  69 6e 5f 66 72 61 6d 65   smenu=ma in_frame
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0080  20 31 39 32 2e 31 36 38  2e 31 2e 31 0d 0a 43 6f    192.168 .1.1..Co
0090  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
```

Credentials (http.authbasic) | Packets: 42 · Displayed: 5 (11.9%) | Profile: Default

把 AP 加密調成沒有加密，再用 wireshark 監聽無線網卡的封包。

(50 points)

7. Setup your own client and an AP to run WEP. Use the aircrack-ng suite to crack the WEP key by running through the steps of frame capturing, fake authentication attack, ARP replay attack, and key cracking. Show and discuss the steps you run through.