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.

→ I tried hard, but I still cannot get any phishing email. So I use a phishing email database from www.millersmiles.co.uk. The phishing email I would like to trace is as follows.

content

.

Your access to usaa.com has been temporarily restricted because of suspicious activity on your USAA profile or account(s). Please review account Information.

Review Your Account

Thank you,
USAA

Date Reported: 16th May 2016 **Risk Level:** MEDIUM-HIGH

details

Email Subject: USAA Detected Suspicious Activity

Apparent Sender: USAA

Return Address: USAA.Customer.Service@mailcenter.usa.com

Email Format: HTML

URL of Web Content: http://admstestserver8.info/wp-admin/js/cp.php

Anchor text of URLs: 1) Review Your Account

Location: NEW YORK CITY, NEW YORK, UNITED STATES

Whois Record for AdMsTestServer8.info

Whois & Quick Stats

Email	admin@ausdms.com.au is associated with ~19 domains
Registrant Org	AUSTRALIAN DIGITAL MEDIA SOLUTIONS is associated with ~17 other domains
Dates	Created on 2015-06-19 - Expires on 2016-06-19 - Updated on 2016-01-07
IP Address	65.39.128.43 - 1,187 other sites hosted on this server
IP Location	- New York - New York City - Peer 1 Network (usa) Inc.
ASN	AS13768 PEER1 - Peer 1 Network (USA) Inc., US (registered Jun 10, 2002)
Domain Status	Registered And Active Website
Whois History	6 records have been archived since 2015-06-18
IP History	2 changes on 3 unique IP addresses over 1 years
Hosting History	2 changes on 3 unique name servers over 1 year
Whois Server	whois.afilias.net

Website

Website Title	None given.
Server Type	Apache

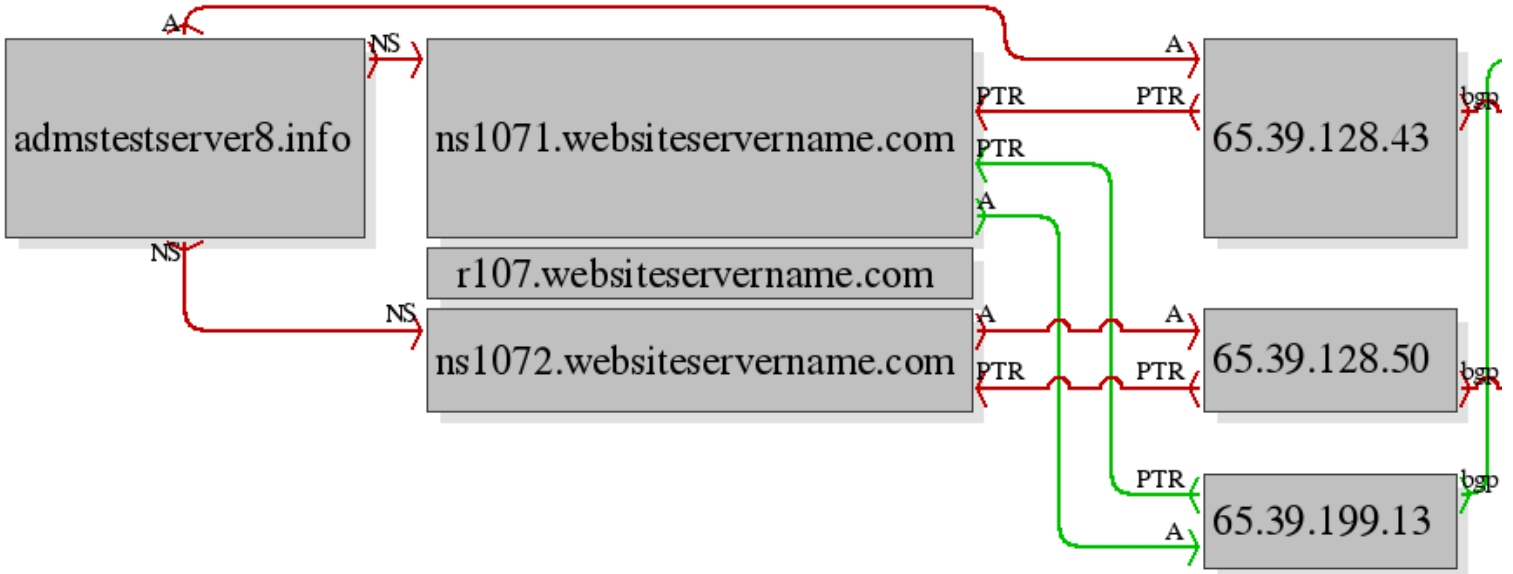
Whois Record (last updated on 2016-05-17)

DNS records found

Tue May 17 16:26:12 2016

MX 0 admstestserver8.info 65.39.128.43
United States NY New York Peer1 Route Object Network Inc. PEER1-BLK-06

NS ns1071.websiteservername.com 65.39.199.13
United States NY New York Peer1 Route Object Network Inc. PEER1-HOSTPAPA-04
SOA ns1071.websiteservername.com 65.39.199.13
NS ns1072.websiteservername.com 65.39.128.50
A 65.39.128.43



IP addresses of admstestserver8.info (1 shown)

What IP addresses does the hostname admstestserver8.info point to?

65.39.128.43

Mail servers of admstestserver8.info (1 shown)

admstestserver8.info

Names pointing to same IP address as admstestserver8.info (142 shown)

Which hostnames and domains point to the same IP address as admstestserver8.info?

northernbeachesrealestate.biz
steelsheds.biz
wollongongrealestate.biz
afmwebs.com
alampallam.com
andrew-reid.com
bennadaleenglishcockers.com
brandnew2market.com

Domains using the nameservers as admstestserver8.in

northernbeachesre
steelsheds.biz
wollongongrealest
afmwebs.com
alampallam.com
andrew-reid.com
brandnew2market.c
bzbhosting.com
chromatechnologie

Submission #4077272 is currently ONLINE

Submitted May 15th 2016 12:05 PM by dms (Current time: May 17th 2016 4:05 PM UTC)

http://admstestserver8.info/wp-admin/js/cp.php

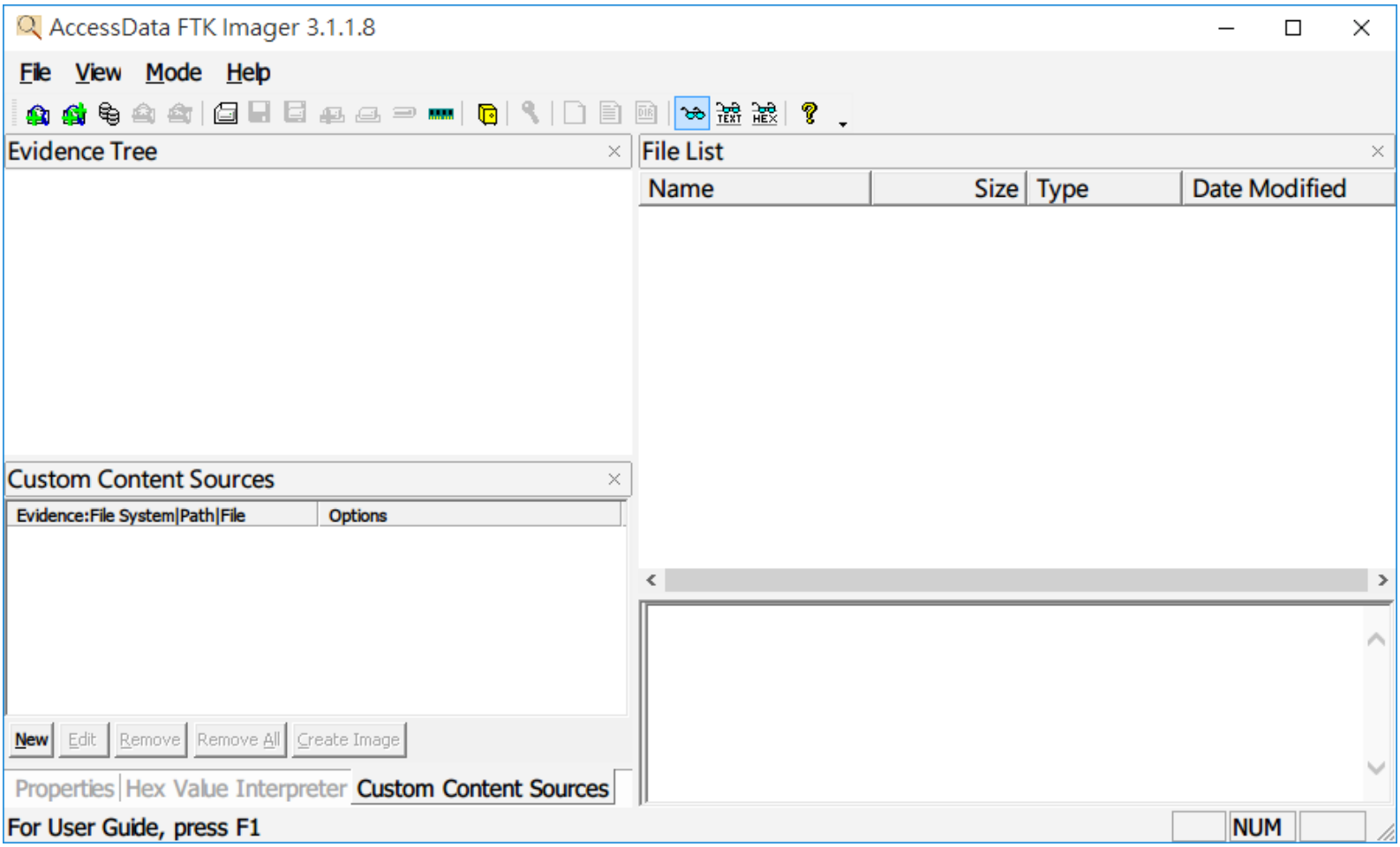
Sign in or Register to verify this submission.

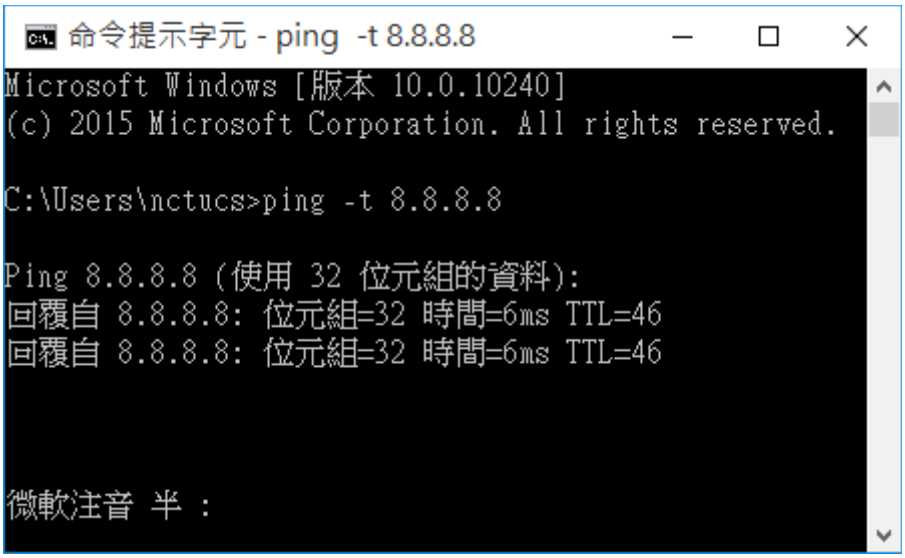
This submission needs more votes to be confirmed or denied.

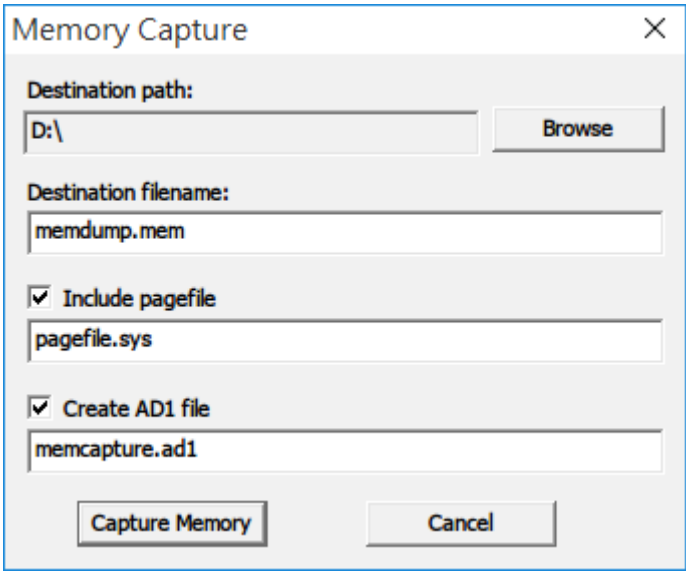
Screenshot of site | View site in frame | View technical details | View site in new window

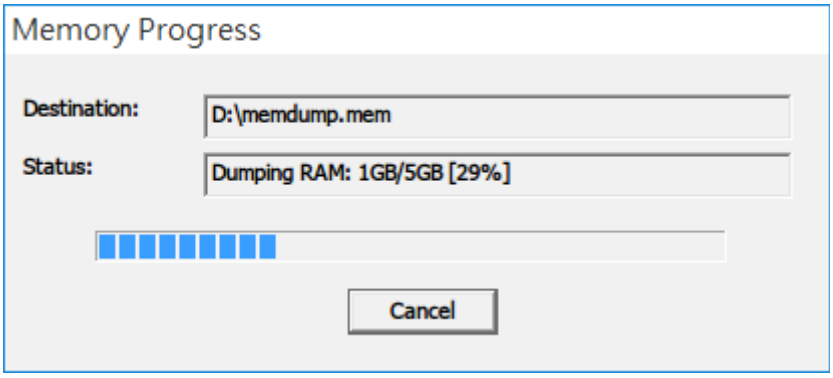
2. On Windows with some running processes connecting to the Internet, use FTK Imager to dump memory and then Volatility Framework to analyze the memory dump. Show processes with connections, and check whether they have DLLs.

→ Yes, the Ping.exe program has DLLs. Due to the limitation of Volatility Framework, I cannot list all processes with connections.




命令提示字元 - ping -t 8.8.8.8
Microsoft Windows [版本 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\nctucs>ping -t 8.8.8.8
Ping 8.8.8.8 (使用 32 位元組的資料):
回覆自 8.8.8.8: 位元組=32 時間=6ms TTL=46
回覆自 8.8.8.8: 位元組=32 時間=6ms TTL=46
微軟注音 半 :


Memory Capture
Destination path:
D:\
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel


Memory Progress
Destination:
D:\memdump.mem
Status:
Dumping RAM: 1GB/5GB [29%]
Cancel

```
C:\Users\nctucs\Downloads\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f D:\memdump.mem --profile=Win10x64 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffe0002f651840 System                    4      0    139        0 ------      0 2016-05-18 13:35:28 UTC+0000
0xffffe00031326440 smss.exe                348      4      2        0 ------      0 2016-05-18 13:35:28 UTC+0000
0xffffe00031b98380 csrss.exe               448    440     10        0      0      0 2016-05-18 13:35:36 UTC+0000
0xffffe00031d35080 csrss.exe               532    520     12        0      1      0 2016-05-18 13:35:37 UTC+0000
0xffffe00031d3b5c0 wininit.exe             572    440      1        0      0      0 2016-05-18 13:35:38 UTC+0000
0xffffe00031ddf080 winlogon.exe            608    520      2        0      1      0 2016-05-18 13:35:38 UTC+0000
0xffffe00031545080 services.exe            664    572      4        0      0      0 2016-05-18 13:35:38 UTC+0000
0xffffe00031557080 lsass.exe               684    572      6        0      0      0 2016-05-18 13:35:38 UTC+0000
0xffffe00031d32840 svchost.exe             768    664     19        0      0      0 2016-05-18 13:35:41 UTC+0000
0xffffe00031cf8840 svchost.exe             828    664     11        0      0      0 2016-05-18 13:35:41 UTC+0000
0xffffe00032015380 dwm.exe                 908    608      8        0      1      0 2016-05-18 13:35:41 UTC+0000
0xffffe000320a6780 svchost.exe            1020    664     38        0      0      0 2016-05-18 13:35:43 UTC+0000
0xffffe00031cf0840 svchost.exe             372    664     13        0      0      0 2016-05-18 13:35:43 UTC+0000
0xffffe00031cec840 svchost.exe             472    664     11        0      0      0 2016-05-18 13:35:43 UTC+0000
0xffffe00031cea840 svchost.exe             476    664     22        0      0      0 2016-05-18 13:35:43 UTC+0000
0xffffe00032144080 svchost.exe             736    664     15        0      0      0 2016-05-18 13:35:43 UTC+0000
0xffffe00031ce4840 WUDFHost.exe           1128    372      6        0      0      0 2016-05-18 13:35:45 UTC+0000
0xffffe00031ccf840 svchost.exe            1256    664     17        0      0      0 2016-05-18 13:35:45 UTC+0000
0xffffe00032355840 spoolsv.exe            1388    664     17        0      0      0 2016-05-18 13:35:45 UTC+0000
0xffffe0003231c580 svchost.exe            1412    664     23        0      0      0 2016-05-18 13:35:45 UTC+0000
0xffffe0003241f080 svchost.exe            1600    664     10        0      0      0 2016-05-18 13:35:46 UTC+0000
0xffffe000322b2840 OVRServiceLaun         1624    664      3        0      0      1 2016-05-18 13:35:46 UTC+0000
0xffffe00032435840 MacTray.exe            1692    664      5        0      0      1 2016-05-18 13:35:46 UTC+0000
0xffffe000322a8840 TeamViewer_Ser         1712    664     18        0      0      1 2016-05-18 13:35:46 UTC+0000
0xffffe0003246b840 svchost.exe            1732    664      6        0      0      0 2016-05-18 13:35:46 UTC+0000
0xffffe0003240d7c0 svchost.exe            1744    664     10        0      0      0 2016-05-18 13:35:46 UTC+0000
0xffffe00032461840 dasHost.exe            1852    372      3        0      0      0 2016-05-18 13:35:47 UTC+0000
0xffffe0003244f840 mt64agnt.exe            380   1692      1        0      0      0 2016-05-18 13:35:48 UTC+0000
0xffffe0003271c840 MsMpEng.exe            1240    664     37        0      0      0 2016-05-18 13:35:49 UTC+0000
0xffffe0002f85f840 NisSrv.exe             2228    664      8        0      0      0 2016-05-18 13:35:53 UTC+0000
0xffffe00032eb1840 taskhostw.exe          3204   1020     13        0      1      0 2016-05-18 13:36:36 UTC+0000
0xffffe00032ecb080 sihost.exe             3324   1020     12        0      1      0 2016-05-18 13:36:36 UTC+0000
0xffffe00032e61840 userinit.exe           3448    608      0 --------      1      0 2016-05-18 13:36:37 UTC+0000   2016-05-18 13:3
0xffffe00032e5f840 explorer.exe           3480   3448     65        0      1      0 2016-05-18 13:36:37 UTC+0000
0xffffe00032e5d840 OVRServer_x64.         3512   1624     10        0      1      0 2016-05-18 13:36:37 UTC+0000
0xffffe00032e5b840 conhost.exe            3532   3512      1        0      1      0 2016-05-18 13:36:37 UTC+0000
```

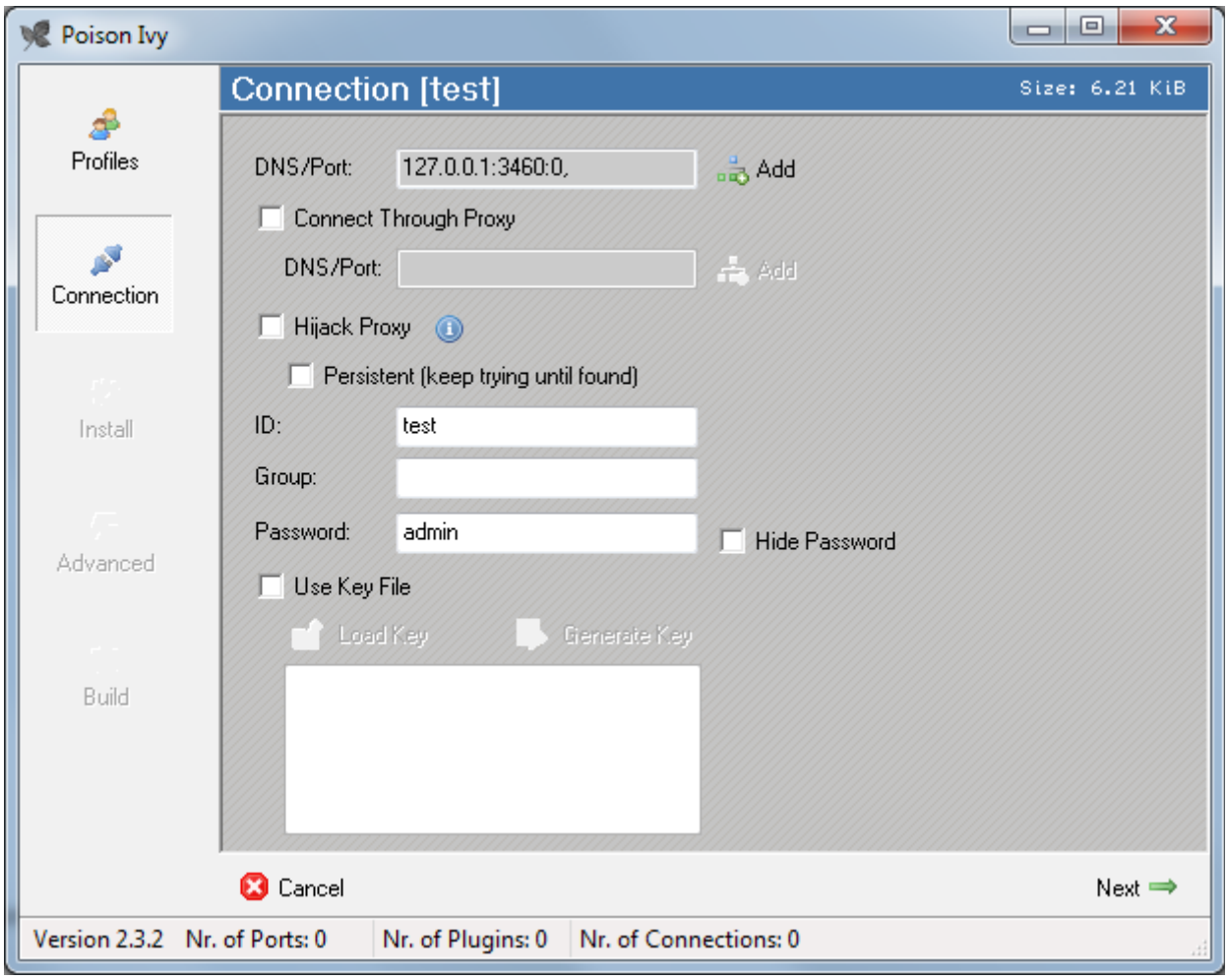
```
C:\Users\nctucs\Downloads\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f D:\memdump.mem --profile=Win10x64 dlllist
Volatility Foundation Volatility Framework 2.5
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    348
Command line : \SystemRoot\System32\smss.exe


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x00007ff676d40000            0x23000                0x0 \SystemRoot\System32\smss.exe
0x00007ffb402e0000           0x1c2000                0x0 C:\Windows\SYSTEM32\ntdll.dll
************************************************************************
csrss.exe pid:    448
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windo
f MaxRequestThreads=16


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x00007ff6c93b0000             0x7000                0x0 C:\Windows\system32\csrss.exe
0x00007ffb402e0000           0x1c2000                0x0 C:\Windows\SYSTEM32\ntdll.dll
0x00007ffb3ccb0000            0x15000                0x0 C:\Windows\system32\CSRSRV.dll
0x00007ffb3cc90000            0x14000                0x0 C:\Windows\system32\basesrv.DLL
0x00007ffb3cc50000            0x35000                0x0 C:\Windows\system32\winsrv.DLL
0x00007ffb3e6b0000           0x14e000                0x0 C:\Windows\system32\USER32.dll
0x00007ffb3d6d0000           0x1dd000                0x0 C:\Windows\system32\kernelbase.dll
0x00007ffb3eaa0000            0xad000                0x0 C:\Windows\system32\kernel32.dll
0x00007ffb3e180000           0x186000                0x0 C:\Windows\system32\GDI32.dll
0x00007ffb3cc40000             0xd000                0x0 C:\Windows\system32\sxssrv.DLL
0x00007ffb3cb60000            0x98000                0x0 C:\Windows\system32\sxs.dll
0x00007ffb3e370000           0x126000                0x0 C:\Windows\system32\RPCRT4.dll
0x00007ffb3caf0000            0x6b000                0x0 C:\Windows\system32\bcryptPrimitives.dll
************************************************************************
csrss.exe pid:    532
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windo
f MaxRequestThreads=16


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x00007ff6c93b0000             0x7000                0x0 C:\Windows\system32\csrss.exe
```

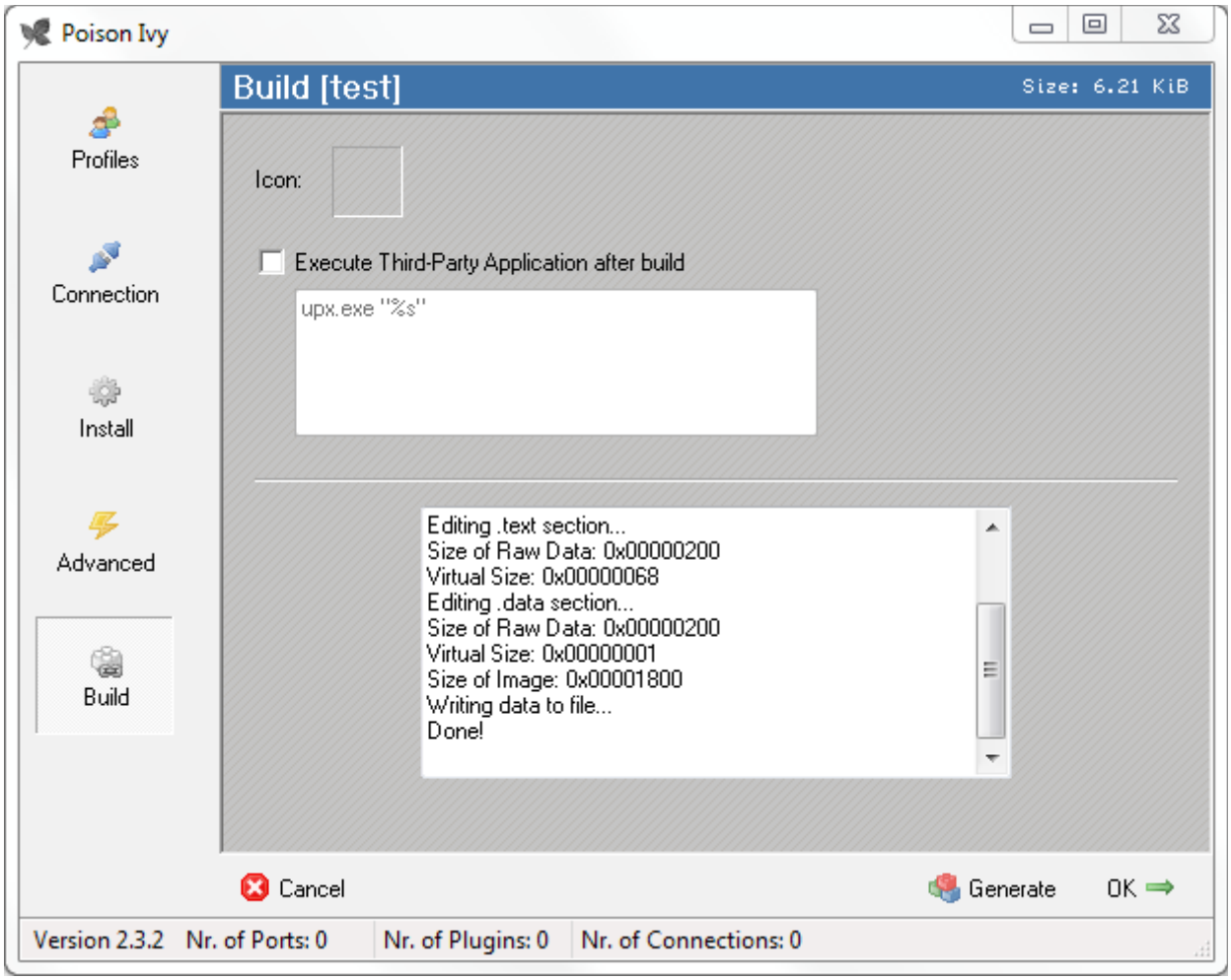
```
C:\Users\nctucs\Downloads\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f D:\memdump.mem --profile=Win10x64 --pid=2500 dlllist
Volatility Foundation Volatility Framework 2.5
************************************************************************
PING.EXE pid:   2500
Command line : ping  -t 8.8.8.8


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x00007ff7b0f00000             0xb000                0x0 C:\Windows\system32\PING.EXE
0x00007ffb402e0000            0x1c2000               0x0 C:\Windows\SYSTEM32\ntdll.dll
0x00007ffb3eaa0000             0xad000               0x0 C:\Windows\system32\KERNEL32.DLL
0x00007ffb3d6d0000            0x1dd000               0x0 C:\Windows\system32\KERNELBASE.dll
0x00007ffb3da60000             0x9d000               0x0 C:\Windows\system32\msvcrt.dll
0x00007ffb3dcb0000             0x69000               0x0 C:\Windows\system32\WS2_32.dll
0x00007ffb3e310000             0x5b000               0x0 C:\Windows\system32\sechost.dll
0x00007ffb37800000             0x38000               0x0 C:\Windows\system32\IPHLPAPI.DLL
0x00007ffb3e370000            0x126000               0x0 C:\Windows\system32\RPCRT4.dll
0x00007ffb3e4a0000              0x8000               0x0 C:\Windows\system32\NSI.dll
0x00007ffb377f0000              0xb000               0x0 C:\Windows\system32\WINNSI.DLL
0x0000000180000000             0xe7000               0x0 C:\Program Files (x86)\MacType\MacType64.dll
0x00007ffb3e6b0000            0x14e000               0x0 C:\Windows\system32\USER32.dll
0x00007ffb3e180000            0x186000               0x0 C:\Windows\system32\GDI32.dll
0x00007ffb3d9b0000             0xa6000               0x0 C:\Windows\system32\ADVAPI32.dll
0x00007ffb32d50000             0x21000               0x0 C:\Program Files (x86)\MacType\EasyHK64.dll
0x00007ffb3e4b0000              0x8000               0x0 C:\Windows\system32\PSAPI.DLL
0x00007ffb3d970000             0x36000               0x0 C:\Windows\system32\IMM32.DLL
0x00007ffb400c0000            0x15c000               0x0 C:\Windows\system32\MSCTF.dll
0x00007ffb3c4e0000             0x5d000               0x0 C:\Windows\system32\mswsock.dll
0x00007ffb35490000              0xa000               0x0 C:\Windows\system32\wshqos.dll
0x00007ffb35480000              0x8000               0x0 C:\Windows\system32\wshtcpip.DLL
0x00007ffb35470000              0x8000               0x0 C:\Windows\system32\wship6.dll
```

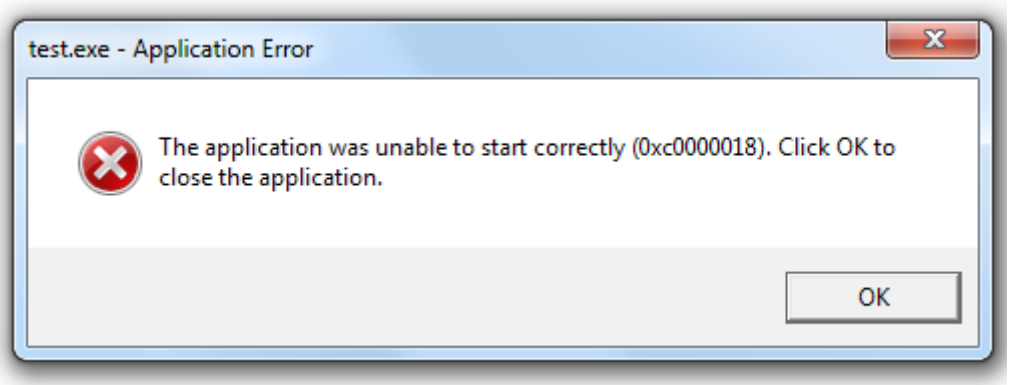
```
C:\Users\nctucs\Downloads\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f D:\memdump.mem --profile=Win10x64 connections
Volatility Foundation Volatility Framework 2.5
ERROR   : volatility.debug    : This command does not support the profile Win10x64
```

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.

→I failed to run the Trojan. I guess some of its dependencies is missing.




Poison Ivy
Build [test]
Size: 6.21 KiB
Profiles
Connection
Install
Advanced
Build
Icon:
Execute Third-Party Application after build
upx.exe "%s"
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: 0x00001800
Writing data to file...
Done!
Cancel
Generate
OK
Version 2.3.2
Nr. of Ports: 0
Nr. of Plugins: 0
Nr. of Connections: 0


test.exe - Application Error
The application was unable to start correctly (0xc0000018). Click OK to close the application.
OK

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

→ I tried 82.98.129.35. It only supports Main Mode. I don't have a real Windows so I cannot run IKEProbe.

```
~ sudo ike-scan 82.98.129.35
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
82.98.129.35    Main Mode Handshake returned HDR=(CKY-R=d120b594e773ce9e) SA=(Enc=3DES Hash=SHA1 Group=2:modp102
696fc77570100 (Dead Peer Detection v1.0) VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)

Ending ike-scan 1.9: 1 hosts scanned in 0.345 seconds (2.90 hosts/sec).  1 returned handshake; 0 returned notify
```

```
✗ ~ sudo ike-scan --aggressive 82.98.129.35
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
82.98.129.35    Notify message 24 (AUTHENTICATION-FAILED) HDR=(CKY-R=0b5c2d55feedb6b1, msgid=4556ead9)

Ending ike-scan 1.9: 1 hosts scanned in 0.343 seconds (2.91 hosts/sec).  0 returned handshake; 1 returned notify
```

```
~ sudo nmap -T4 -A -v 82.98.129.35

Starting Nmap 7.10 ( https://nmap.org ) at 2016-05-18 19:46 CST
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:46
Completed NSE at 19:46, 0.00s elapsed
Initiating NSE at 19:46
Completed NSE at 19:46, 0.00s elapsed
Initiating Ping Scan at 19:46
Scanning 82.98.129.35 [4 ports]
Completed Ping Scan at 19:46, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:46
```

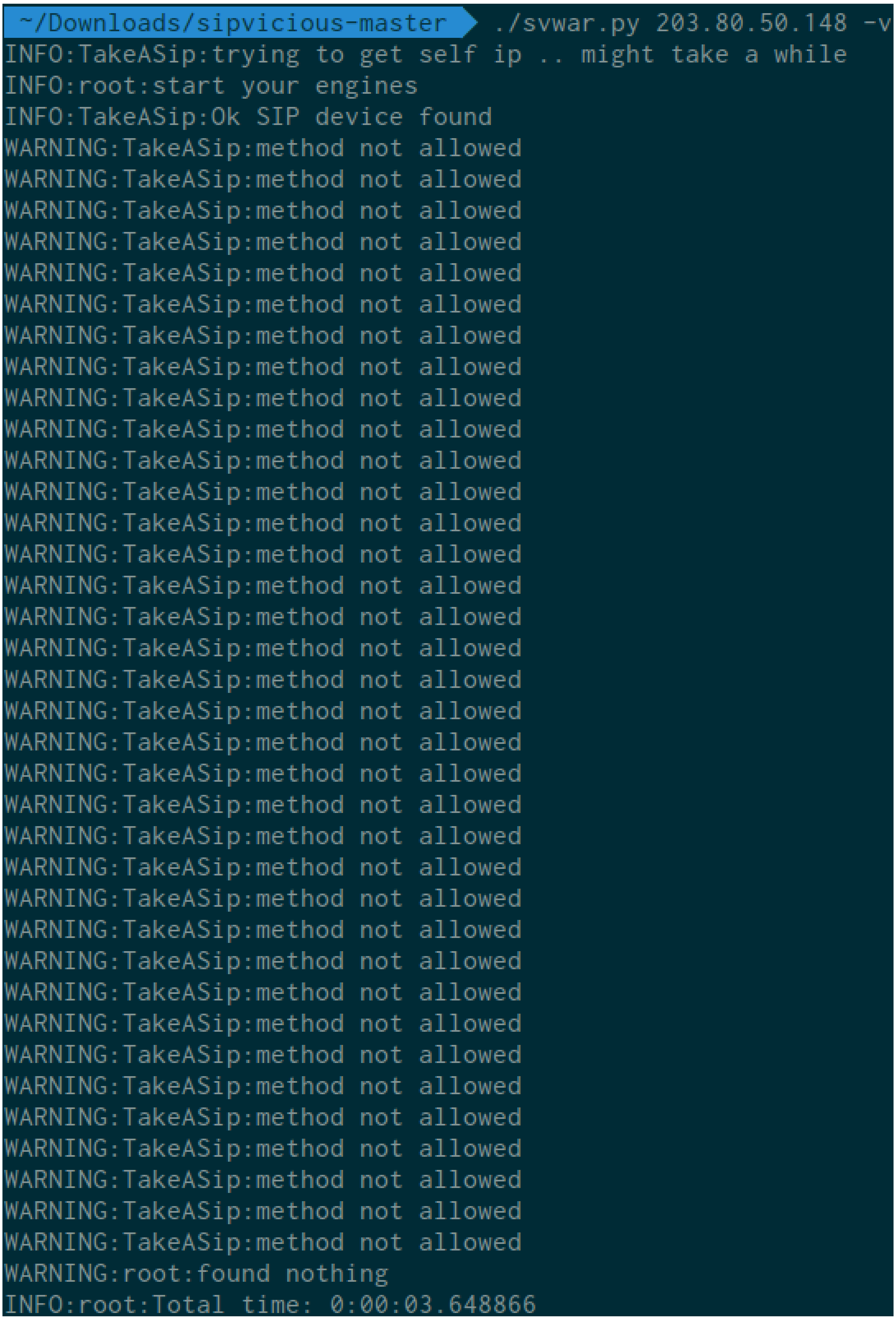
```
Completed NSE at 19:48, 0.00s elapsed
Nmap scan report for dl363.dinaserver.com (82.98.129.35)
Host is up (0.32s latency).
Not shown: 987 closed ports
PORT     STATE    SERVICE        VERSION
80/tcp   open     http
|_http-title: Site doesn't have a title.
111/tcp  filtered rpcbind
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1723/tcp open     pptp           linux (Firmware: 1)
2049/tcp filtered nfs
4000/tcp filtered remoteanything
4001/tcp filtered newoak
4002/tcp filtered mlchat-proxy
6666/tcp filtered irc
6667/tcp filtered irc
6668/tcp filtered irc
6669/tcp filtered irc
1 service unrecognized despite returning data. If you know the service/vers
SF-Port80-TCP:V=7.10%I=7%D=5/18%Time=573C562A%P=x86_64-redhat-linux-gnu%r(
SF:GetRequest,41,"HTTP/1\.1\x20403\x20Foribdden\r\nUpgrade:\x20websocket\r
SF:\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,41,"HTTP/1\.1\x20403\x20
SF:Foribdden\r\nUpgrade:\x20websocket\r\nConnection:\x20close\r\n\r\n")%r(
SF:FourOhFourRequest,41,"HTTP/1\.1\x20403\x20Foribdden\r\nUpgrade:\x20webs
SF:ocket\r\nConnection:\x20close\r\n\r\n");
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Uptime guess: 127.960 days (since Mon Jan 11 20:46:08 2016)
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: local

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
```

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

→ I tried 203.80.50.148. SIPVicious is unavailable.

```
~/Downloads/sipvicious-master  ./svmap.py --randomscan
q^CWARNING:root:caught your control^c - quiting
WARNING:root:could not remove .sipviciousrandomtmp
| SIP Device           | User Agent
-----------------------------------------------------------------------------
| 194.208.202.115:5060 | FRITZ!OS
| 188.109.35.79:5060   | FRITZ!OS
| 187.193.140.109:5060 | unknown
| 178.3.136.126:5060   | FRITZ!OS
| 192.92.205.143:5060  | FPBX-13.0.109(13.7.0)
| 2.245.117.12:5060    | FRITZ!OS
| 49.228.211.30:5060   | ZXHN H267N V1.0/V1.0.0T2_TH3
| 92.201.241.23:5060   | FRITZ!OS
| 12.213.5.71:64568    | Cisco-SIPGateway/IOS-15.2.1.T2
| 203.80.50.148:5060   | M5T SIP Stack/4.1.2.2
| 195.33.70.22:5060    | TANDBERG/4120 (X7.2.2)
| 187.228.19.135:5060  | unknown
| 78.49.101.163:5060   | FRITZ!OS
| 187.176.215.144:5060 | unknown
| 220.253.210.188:5060 | M5T SIP Stack/4.1.2.2
| 2.86.205.218:5060    | ZXDSL 931VII/V2.0.00.OTET06
| 121.98.101.64:5060   | unknown
| 111.99.54.54:5060    | unknown
| 188.251.89.59:5060   | Thomson TG784n Build 10.2.1.L
| 192.154.156.9:5060   | Linksys/SPA2102-5.2.12
| 84.191.197.159:5060  | FRITZ!OS
| 217.245.26.9:5060    | FRITZ!OS
| 188.109.189.39:5060  | FRITZ!OS
| 192.95.189.65:5060   | unknown
| 95.112.218.52:5060   | AVM FRITZ!Box Fon WLAN 7141 (UI) 40.04.77 TAL (Feb
```

```
~/Downloads/sipvicious-master  ./svmap.py 203.80.50.148 -v
INFO:DrinkOrSip:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:DrinkOrSip:203.80.50.148:5060      ->      203.80.50.148:5060      ->      M5T SIP Stack/4.1.2.2   ->      disabled
INFO:root:we have 1 devices
| SIP Device         | User Agent            | Fingerprint |
-------------------------------------------------------------
| 203.80.50.148:5060 | M5T SIP Stack/4.1.2.2 | disabled    |

INFO:root:Total time: 0:00:03.212437
```



```
 ~/Downloads/sipvicious-master  ./svwar.py 203.80.50.148 -v
INFO:TakeASip:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:TakeASip:Ok SIP device found
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:TakeASip:method not allowed
WARNING:root:found nothing
INFO:root:Total time: 0:00:03.648866
```

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.

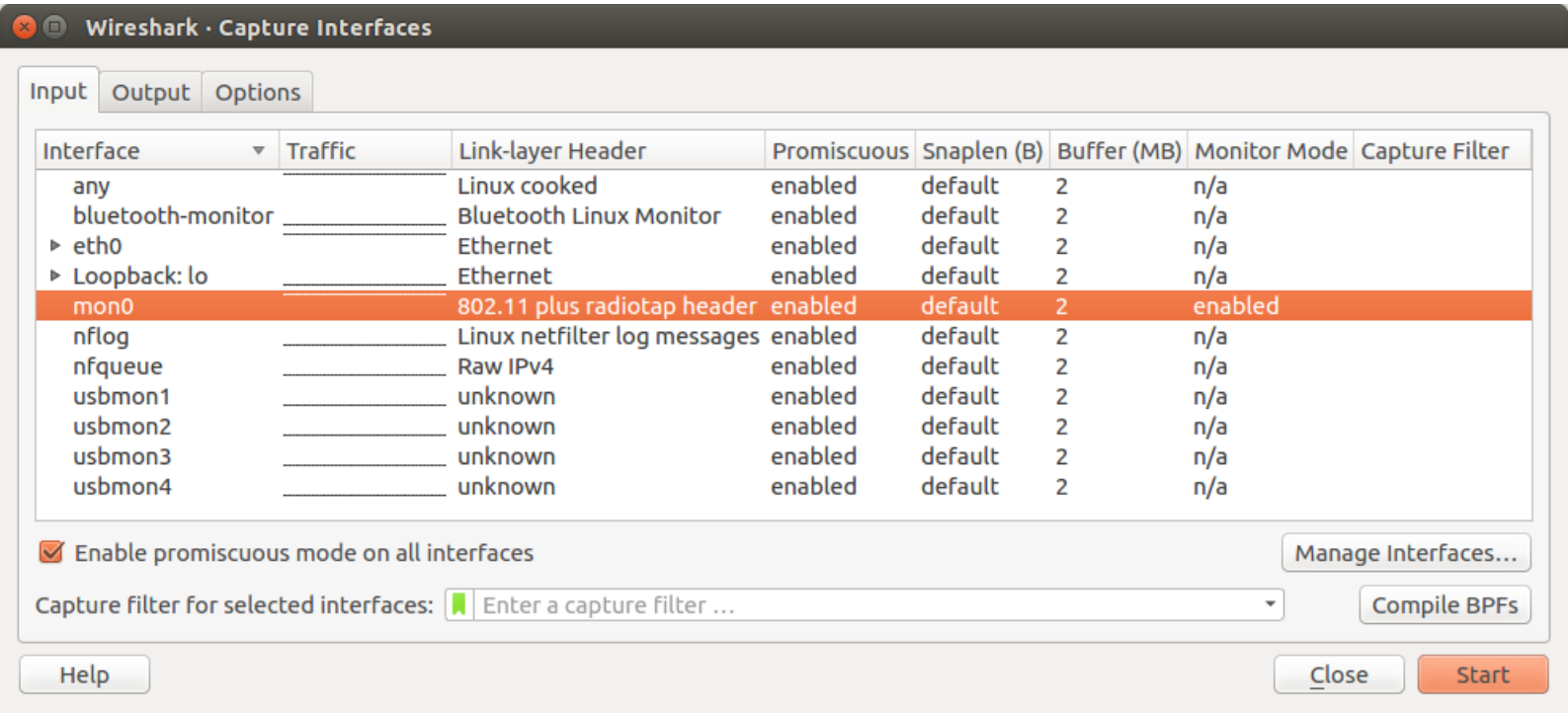
→ I followed the instructions on https://documentation.meraki.com/MR/Monitoring_and_Reporting/Capturing_Wireless_Traffic_from_a_Client_Machine. However, I cannot see any data frames. I heard that many Linux users have the same issue.

```
~/Downloads/sipvicious-master  sudo airmon-ng start wlan0
[sudo] password for yuwen41200:


Found 6 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
697     avahi-daemon
699     NetworkManager
775     avahi-daemon
825     wpa_supplicant
4653    dhclient
13039   dhclient
Process with PID 4653 (dhclient) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Unknown         rt2800pci - [phy0]SIOCSIFFLAGS: 網路上的名稱不是唯一的

                                (monitor mode enabled on mon0)

~/Downloads/sipvicious-master  sudo service avahi-daemon stop
```

```
~/Downloads/sipvicious-master  sudo kill 825
~/Downloads/sipvicious-master  sudo airmon-ng stop mon0


Interface       Chipset         Driver

mon0            Unknown         rt2800pci - [phy0] (removed)
wlan0           Unknown         rt2800pci - [phy0]

~/Downloads/sipvicious-master  sudo airmon-ng start wlan0


Interface       Chipset         Driver

wlan0           Unknown         rt2800pci - [phy0]
                                (monitor mode enabled on mon0)
```

```
~/Downloads/sipvicious-master  sudo airodump-ng mon0 --channel 1
```

```
CH  1 ][ Elapsed: 1 min ][ 2016-05-18 20:56

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

4C:E6:76:CC:FB:26  -51  93      605        0    0   1  54e. WPA  TKIP   PSK  Dorm212
10:C3:7B:D6:FE:4C  -75 100      574       43    0   1  54e  WPA2 CCMP   PSK  room109
9C:D6:43:69:1F:7D  -84  34      247        0    0   1  54e  WPA2 CCMP   PSK  ~QAQ~
10:FE:ED:AB:08:9A  -88  58      409        0    0   1  54e. WPA2 CCMP   PSK  TP-LINK_AB089A

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   24:0A:64:7D:49:8B  -59    0 - 1      0        2
(not associated)   28:C2:DD:C8:E0:97  -67    0 - 1      0        2
(not associated)   84:7A:88:43:D7:8C  -73    0 - 1      0        1
(not associated)   DC:85:DE:08:1D:40  -73    0 - 1      0        2
(not associated)   24:0A:64:25:5E:67  -79    0 - 1      0        2
(not associated)   68:5D:43:CB:58:27  -79    0 - 1      0        3  210-wifi
(not associated)   6C:71:D9:5F:B8:E7  -79    0 - 1      0        1
(not associated)   08:ED:B9:FA:C7:8D  -79    0 - 1      0        1
(not associated)   E8:03:9A:C7:F1:E5  -83    0 - 1     20        4
(not associated)   B8:EE:65:9E:6A:D8  -81    0 - 1      0        2
(not associated)   54:27:1E:75:3B:D9  -81    0 - 1      0        2
```



Source	Destination	Protocol	Length	Info
AsustekC_d6:fe:4c	Broadcast	802.11	295	Beacon frame, SN=2828, FN=0, Flags=....., BI=100, SSID=room109
BuffaloI_cc:fb:26	Broadcast	802.11	211	Beacon frame, SN=2251, FN=0, Flags=....., BI=100, SSID=Dorm212
Azurewav_14:a1:ee	Broadcast	802.11	65	Probe Request, SN=1648, FN=0, Flags=....., SSID=TAMIO
AsustekC_d6:fe:4c	Broadcast	802.11	295	Beacon frame, SN=2829, FN=0, Flags=....., BI=100, SSID=room109
Azurewav_14:a1:ee	Broadcast	802.11	65	Probe Request, SN=1649, FN=0, Flags=....., SSID=TAMIO
BuffaloI_cc:fb:26	Broadcast	802.11	211	Beacon frame, SN=2252, FN=0, Flags=....., BI=100, SSID=Dorm212
AsustekC_d6:fe:4c	Broadcast	802.11	295	Beacon frame, SN=2830, FN=0, Flags=....., BI=100, SSID=room109
D-LinkIn_69:1f:7d	Broadcast	802.11	326	Beacon frame, SN=3923, FN=0, Flags=....., BI=100, SSID=~QAQ~
Tp-LinkT_ab:08:9a	Broadcast	802.11	346	Beacon frame, SN=2093, FN=0, Flags=....., BI=100, SSID=TP-LINK_AB089A
BuffaloI_cc:fb:26	Broadcast	802.11	211	Beacon frame, SN=2253, FN=0, Flags=....., BI=100, SSID=Dorm212
AsustekC_d6:fe:4c	Broadcast	802.11	295	Beacon frame, SN=2831, FN=0, Flags=....., BI=100, SSID=room109
AsustekC_d6:fe:4c	Broadcast	802.11	295	Beacon frame, SN=2832, FN=0, Flags=....., BI=100, SSID=room109
AsustekC_d6:fe:4c	Spanning-...	802.11	96	Data, SN=66, FN=0, Flags=.p....F.
BuffaloI_cc:fb:26	Broadcast	802.11	211	Beacon frame, SN=2255, FN=0, Flags=....., BI=100, SSID=Dorm212
Tp-LinkT_ab:08:9a	Broadcast	802.11	346	Beacon frame, SN=2096, FN=0, Flags=....., BI=100, SSID=TP-LINK_AB089A
BuffaloI_cc:fb:26	Broadcast	802.11	211	Beacon frame, SN=2256, FN=0, Flags=, BI=100, SSID=Dorm212

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.

→N/A