

Unmasking the Zeus Banking Trojan Walkthrough: Tools and Techniques for Detection and Analysis

VMS

Tools

Configuration And Installation

Simulating Malware Execution

Wireshark

SURICATA

SPLUNK UNIVERSAL FORWARDER

SPLUNK

YARA

VOLATILITY

▼ VMs

1. Kali Linux

We Used Kali Linux as monitoring system to catch traffic and detect malware using various tools we cover it through this Write-up.

2. MS-Edge Windows 10

We Used Windows 10 as an environment to execute the malware

▼ Tools

1. Wireshark.
2. Suricata.
3. Splunk Universal Forwarder.
4. Splunk.
5. Yara Gen.
6. Volatility.

▼ Configuration And Installation

Suricata

1. Installation

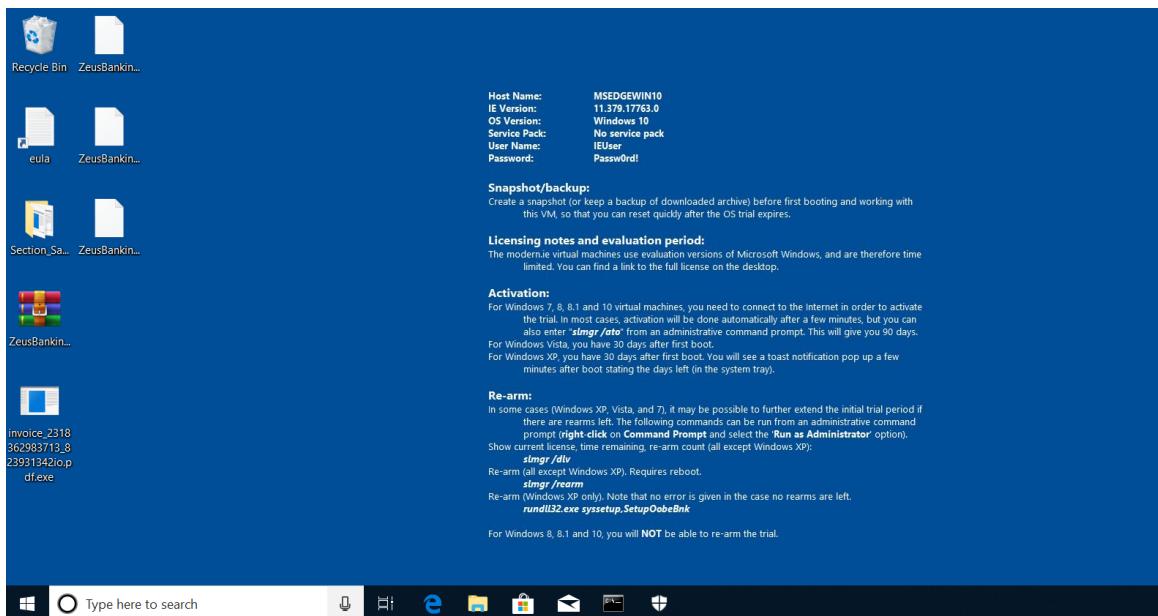
```
sudo apt install -y suricata
```

2. Check Version

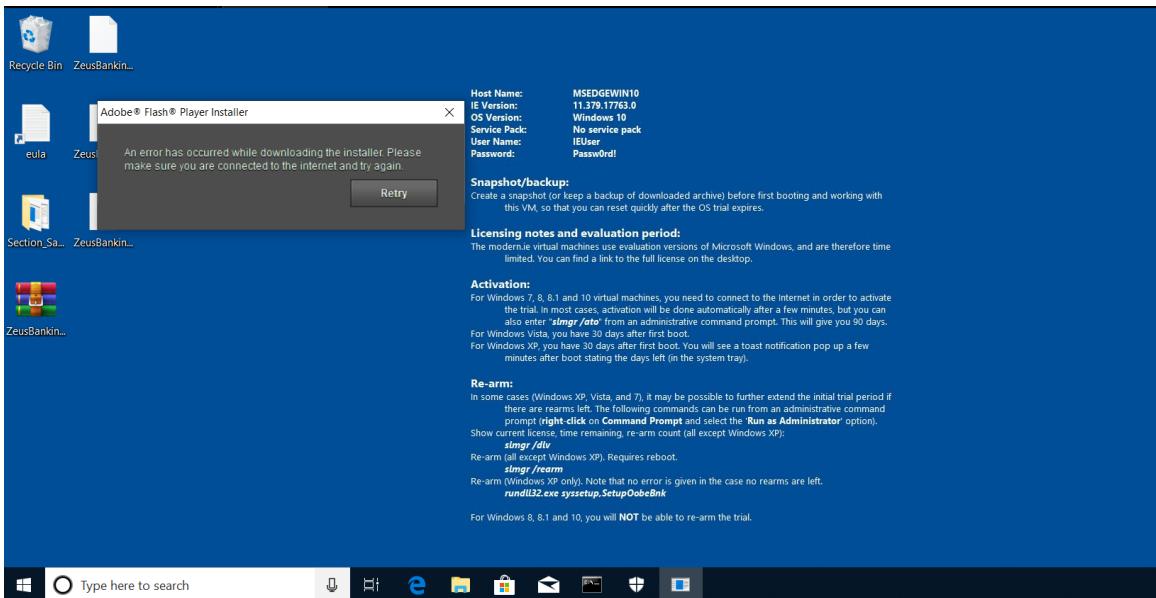
```
suricata -v
```

▼ Simulating Malware Execution

1. We Extracting The Zip file first

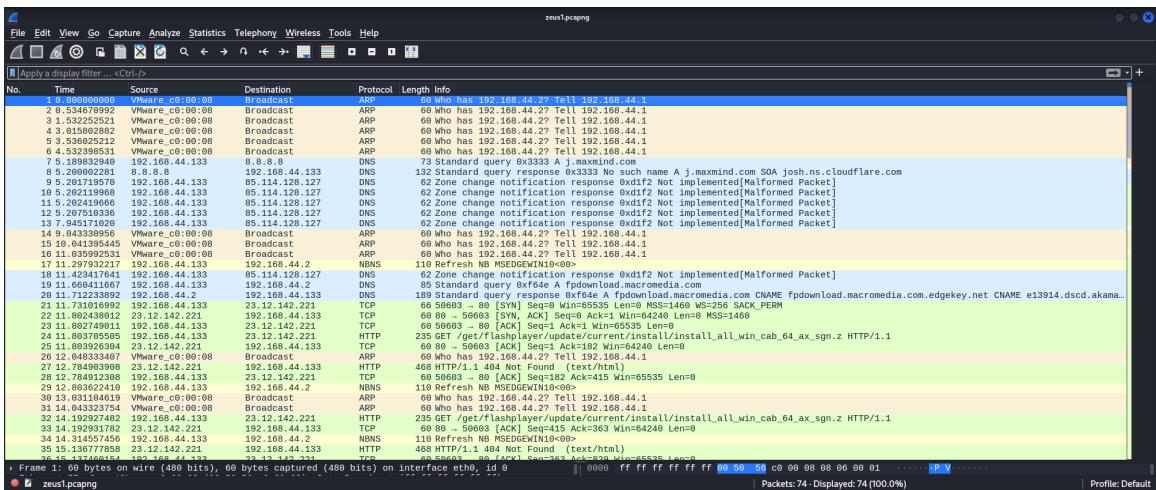


2. We Executing The Program



▼ Wireshark

1. Before we executing the program on victim machine, we start Wireshark to capture network traffic.



2. We see suspicious DNS at packet 20 and HTTP GET suspicious at packet 24.

18 11 _424217641	192.168.44.133	85.114.128.127	DNS	62 Zone change notification response 0x0fd2 Not implemented [Malformed Packet]
19 11 _664611667	192.168.44.133	192.168.44.2	DNS	85 Standard query response 0xf64e A fptdownload.macromedia.com
20 11 _712233892	192.168.44.2	192.168.44.133	DNS	189 Standard query response 0xf64e A fptdownload.macromedia.com CNAME edgekey.net CNAME e13914.dscl.akamai
24 11 _809705505	192.168.44.133	23.12.142.221	HTTP	235 GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1
25 11 _809705505	192.168.44.133	23.12.142.221	HTTP	60 80 50603 [ACK Seq=124 Win=240 Len=0
26 12 _404000007	192.168.44.133	192.168.44.1	ARP	60 Who has 192.168.44.1 Tel 192.168.44.1
27 12 _7840939098	23.12.142.221	192.168.44.133	HTTP	468 HTTP/1.1 404 Not Found (text/html)
28 12 _7849123098	192.168.44.133	23.12.142.221	TCP	60 50603 80 [ACK] Seq=102 Ack=415 Win=65535 Len=0
29 12 _803622410	192.168.44.133	192.168.44.2	NBNS	119 Refresh No MSEDGEWIN10@000
30 13 _031194619	VMware_c0:00:08	Broadcast	ARP	60 Who has 192.168.44.22 Tel 192.168.44.1
31 14 _044333354	VMware_c0:00:08	Broadcast	ARP	60 Who has 192.168.44.22 Tel 192.168.44.1
32 14 _192927482	192.168.44.133	23.12.142.221	HTTP	235 GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1

▼ SURICATA

1. We first update packages and install Suricata.

```
sudo apt install update
```

```
sudo apt install -y suricata
```

2. Check Suricata is installed success.

```
suricata -v
```

3. Enabling Promiscuous Mode

| Change interface to promiscuous mode to monitor traffic and capture it.

```
sudo ip link set eth0 promisc on
```

| Check Promiscuous Mode

```
ip link show eth0
```

3. Create Folder `zeus` that include all files of rules and logs.

3.1. Creating Suricata rules `"zeus.rules"`.

| We use Wireshark to inspect traffic and write Suricata rules to catch this trojan.

| After inspection we see a malicious IP

`85.114.128.127` DNS Query.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Fake Flash Player
http.uri;
content: "/get/flashplayer/update/current/install/install_all_win_cab_6
; http.method; content:"GET"; nocase; sid:1000001; rev:1;)
```

```

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Suspicious Flash P
http.user_agent; content:"Flash Player Seed/3.0"; nocase; sid:1000002;

alert udp any any -> 85.114.128.127 any (msg:"Malicious IP detected in
sid:100004; rev:1; classtype:bad-unknown; metadata:service udp;
reference:url,example.com; threshold: type limit,track by_src,count 1,

```

3.2. Configure “/etc/suricata/suricata.yaml”.

1. Configure \$HOME_NET : [192.168.44.0/24]
2. Configure \$EXTERNAL_NET : [!\$HOME_NET]

```

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.44.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"
    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

```

1. Configure rule-path : /home/kali/zeus
2. Configure rule-files : zeus.rules

```

default-rule-path: /home/kali/zeus
rule-files:
  # - suricata.rules
  - zeus.rules

```

3. Update the `af-packet` to match our end point network interface

```
# Linux high speed capture support
af-packet:
  - interface: eth0
    threads: 4
    cluster-id: 101
    cluster-type: cluster_flow
    defrag: yes
```

4. Change the `pcap` interface to our interface `eth0`.

```
# Cross platform libpcap capture support
pcap:
  - interface: eth0
```

5. Enable `community-id` by setting it to `true`.

```
# enable/disable the community id feature.
community-id: true
```

6. Update Suricata Configuration

```
sudo suricata-update
```

7. Verify Suricata Configuration File using the built-in test command

```
sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

8. Start Suricata

```
sudo systemctl start suricata
```

9. Verify Suricata Status

```
sudo systemctl status suricata
```

10. Use Suricata as Network Security Monitoring (Logging Only)

```
sudo suricata -i eth0 -c /etc/suricata/suricata.yaml -v
```

```
[kali㉿kali)-[~/zeus]
└─$ sudo suricata -i eth0 -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: ioctl: eth0: MTU 1500
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 4 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 4 signatures processed. 1 are IP-only rules, 1 are inspecting packet payload, 2 inspect application layer, 0 are decoder event only
Info: runmodes: eth0: creating 4 threads
Info: unix-manager: unix socket '/var/run/suricata-command.socket'
Notice: threads: Threads created -> W: 4 FM: 1 FR: 1 Engine started.
```

4. Logging

After Executing The `Invoice` program on victim machine, we found logs in `/var/log/suricata`

4.1. We change directory to `/var/log/suricata`

```
cd /var/log/suricata
```

4.2. We list all files in this directory

```
ls -l
```

```
[kali㉿kali)-[/var/log/suricata]
└─$ ls -l
total 143048
-rw-r--r-- 1 root root 93922332 Dec 20 10:50 eve.json
-rw-r--r-- 1 root root      3837 Dec 20 09:47 fast.log
-rw-r--r-- 1 root root 52505230 Dec 20 10:50 stats.log
-rw-r--r-- 1 root root     29365 Dec 20 09:46 suricata.log
```

4.3. As we see there are 4 files of logs:

1. `eve.json`

Suricata's recommended output.

2. `fast.log`

3. `stats.log`

Human-readable statistics log

4. `suricata.log`

`eve.json` output

```
(kali㉿kali)-[~/var/log/suricata]
└─$ cat eve.json | jq '.event_type = "alert"'
{
  "timestamp": "2024-12-19T13:21:47.240246-0500",
  "flow_id": 631716809528082,
  "in_iface": "eth0",
  "event_type": "alert",
  "src_ip": "192.168.44.129",
  "src_port": 56612,
  "dest_ip": "23.12.142.221",
  "dest_port": 80,
  "proto": "TCP",
  "pkt_src": "wire/pcap",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1000001,
    "rev": 1,
    "signature": "Fake Flash Player Update Request",
    "category": "",
    "severity": 3
  },
  "http": {
    "hostname": "fpdownload.macromedia.com",
    "url": "/get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z",
    "http_user_agent": "Flash Player Seed/3.0",
  }
}
```

fast.log output

```
(kali㉿kali)-[~/var/log/suricata]
└─$ cat fast.log
12/19/2024-13:21:47.240246 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.129:56612 → 23.12.142.221:80
12/19/2024-13:21:47.240246 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.129:56612 → 23.12.142.221:80
12/19/2024-13:23:13.449724 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.129:57244 → 23.12.142.221:80
12/19/2024-13:23:13.449724 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.129:57244 → 23.12.142.221:80
12/20/2024-09:47:33.664261 [**] [1:1000004:1] Malicious IP detected in UDP traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.44.133:56327 → 85.114.128.127:53
12/20/2024-09:47:40.265795 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51346 → 23.54.128.33:80
12/20/2024-09:47:40.265795 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51346 → 23.54.128.33:80
12/20/2024-09:47:41.769060 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 → 23.54.128.33:80
12/20/2024-09:47:41.769060 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 → 23.54.128.33:80
12/20/2024-09:47:42.649633 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 → 23.54.128.33:80
12/20/2024-09:47:42.649633 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 → 23.54.128.33:80
12/20/2024-09:47:43.308520 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 → 23.54.128.33:80
12/20/2024-09:47:43.308520 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 → 23.54.128.33:80
```

stats.log output

```
(kali㉿kali)-[~/var/log/suricata]
└─$ cat stats.log

Date: 12/17/2024 -- 09:05:06 (uptime: 0d, 00h 00m 08s)



| Counter                       | TM Name | Value  |
|-------------------------------|---------|--------|
| capture.kernel_packets        | Total   | 597    |
| capture.afpacket.polls        | Total   | 468    |
| capture.afpacket.poll_timeout | Total   | 176    |
| capture.afpacket.poll_data    | Total   | 292    |
| decoder.pkts                  | Total   | 706    |
| decoder.bytes                 | Total   | 787143 |
| decoder.ipv4                  | Total   | 702    |
| decoder.ethernet              | Total   | 706    |
| decoder.arp                   | Total   | 4      |
| decoder.tcp                   | Total   | 702    |
| decoder.avg_pkt_size          | Total   | 1114   |
| decoder.max_pkt_size          | Total   | 1514   |
| flow.total                    | Total   | 14     |
| flow.active                   | Total   | 14     |
| flow.tcp                      | Total   | 14     |
| flow.wrk.spare_sync_avg       | Total   | 100    |
| flow.wrk.spare_sync           | Total   | 4      |
| flow.mgr.rows_per_sec         | Total   | 6553   |
| flow.spare                    | Total   | 9600   |


```

suricata.log output

```
(kali㉿kali)-[~/var/log/suricata]
└─$ cat suricata.log

[872131 - Suricata-Main] 2024-12-17 09:03:55 Notice: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
[872131 - Suricata-Main] 2024-12-17 09:03:55 Info: cpu: CPUs/cores online: 4
[872131 - Suricata-Main] 2024-12-17 09:03:55 Info: suricata: Running suricata under test mode
[872131 - Suricata-Main] 2024-12-17 09:03:55 Info: suricata: Setting engine mode to IDS mode by default
[872131 - Suricata-Main] 2024-12-17 09:03:55 Info: exception-policy: master exception-policy set to: auto
[872131 - Suricata-Main] 2024-12-17 09:03:56 Info: logopenfile: fast output device (regular) initialized: fast.log
[872131 - Suricata-Main] 2024-12-17 09:03:56 Info: logopenfile: eve-log output device (regular) initialized: eve.json
[872131 - Suricata-Main] 2024-12-17 09:03:56 Info: logopenfile: stats output device (regular) initialized: stats.log
[872131 - Suricata-Main] 2024-12-17 09:03:56 Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
[872627 - Suricata-Main] 2024-12-17 09:04:57 Notice: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
[872627 - Suricata-Main] 2024-12-17 09:04:57 Info: cpu: CPUs/cores online: 4
[872627 - Suricata-Main] 2024-12-17 09:04:57 Info: suricata: Setting engine mode to IDS mode by default
[872627 - Suricata-Main] 2024-12-17 09:04:57 Info: exception-policy: master exception-policy set to: auto
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: ioclt: eth0: MTU 1500
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: logopenfile: fast output device (regular) initialized: fast.log
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: logopenfile: eve-log output device (regular) initialized: eve.json
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: logopenfile: stats output device (regular) initialized: stats.log
[872627 - Suricata-Main] 2024-12-17 09:04:58 Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
[872627 - Suricata-Main] 2024-12-17 09:04:58 Warning: detect: No rule files match the pattern /var/lib/suricata/rules/custom.rules
[872627 - Suricata-Main] 2024-12-17 09:04:58 Warning: detect: 2 rule files specified, but no rules were loaded!
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: threshold-config: Threshold config parsed: 0 rule(s) found
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: detect: 0 signatures processed. 0 are IP-only rules, 0 are inspecting packet payload, 0 inspect application layer, 0 are decoder event only
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: runmodes: eth0: creating 4 threads
[872627 - Suricata-Main] 2024-12-17 09:04:58 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
[872627 - Suricata-Main] 2024-12-17 09:04:58 Notice: threads: Threads created → W: 4 FM: 1 FR: 1 Engine started.
```

▼ SPLUNK UNIVERSAL FORWARDER

We use Splunk universal forwarder to forward logs of windows to our Kali Linux machine.

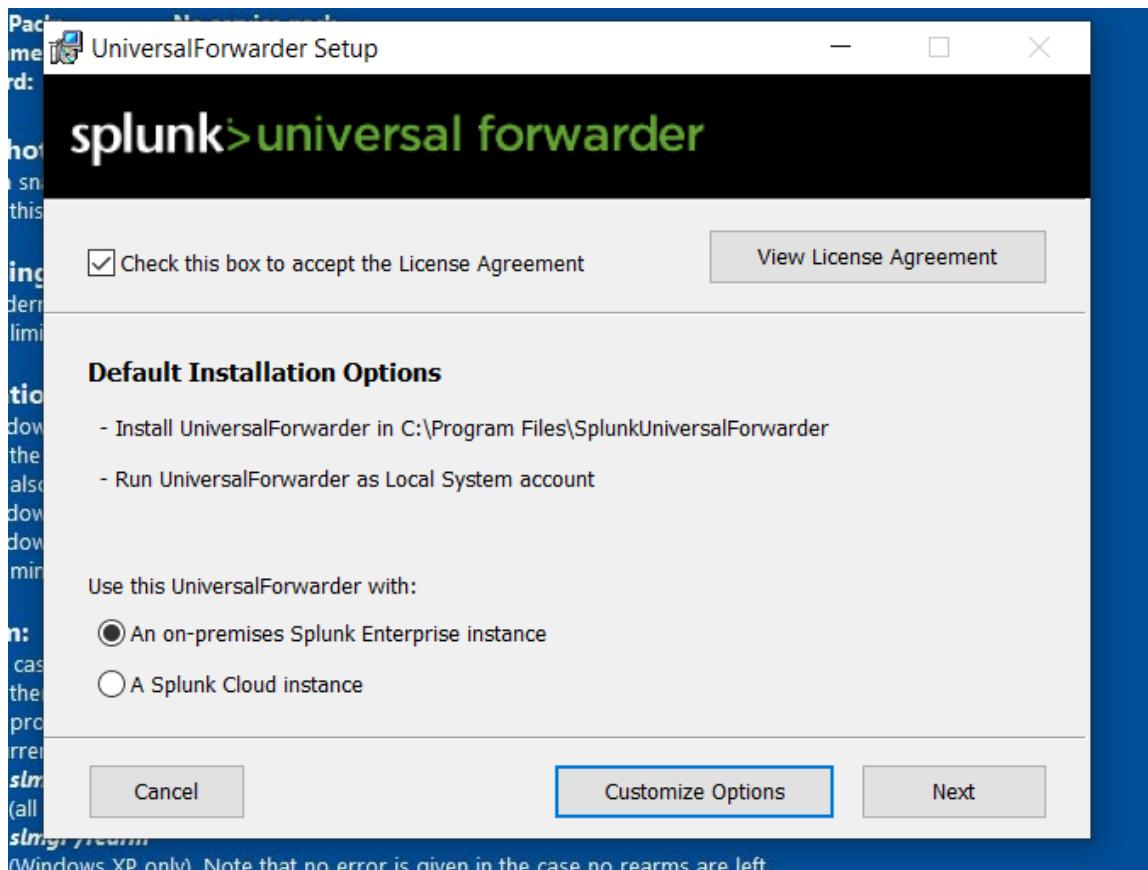
1. Download And Setup

1.1. Download Link

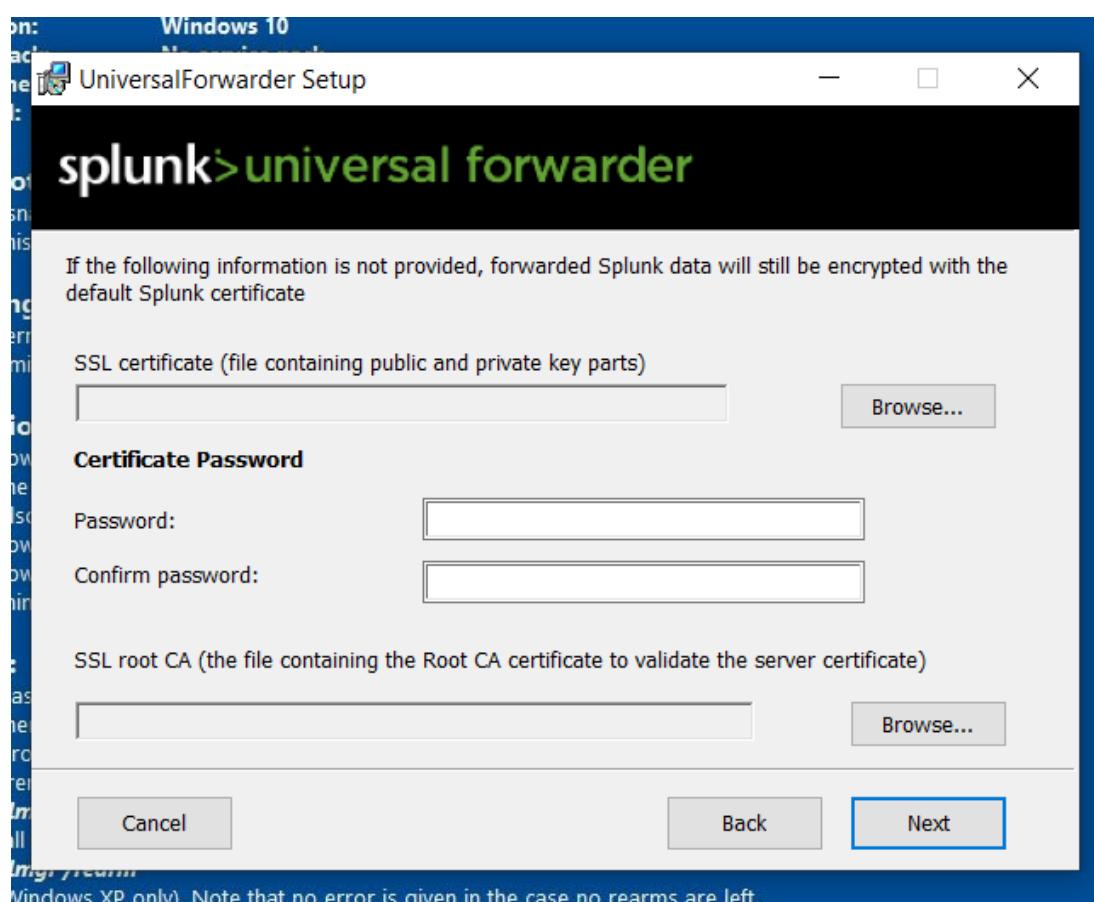
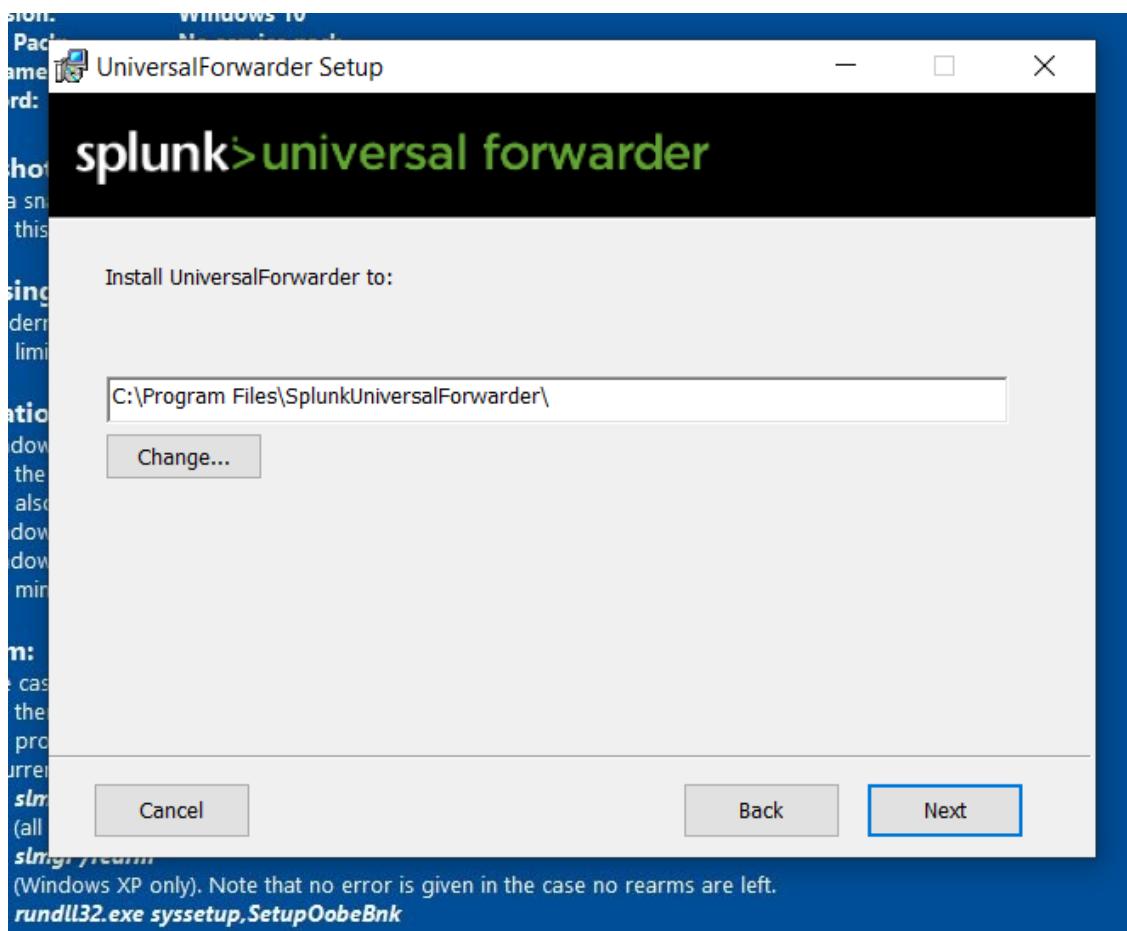
https://www.splunk.com/en_us/download/universal-forwarder.html

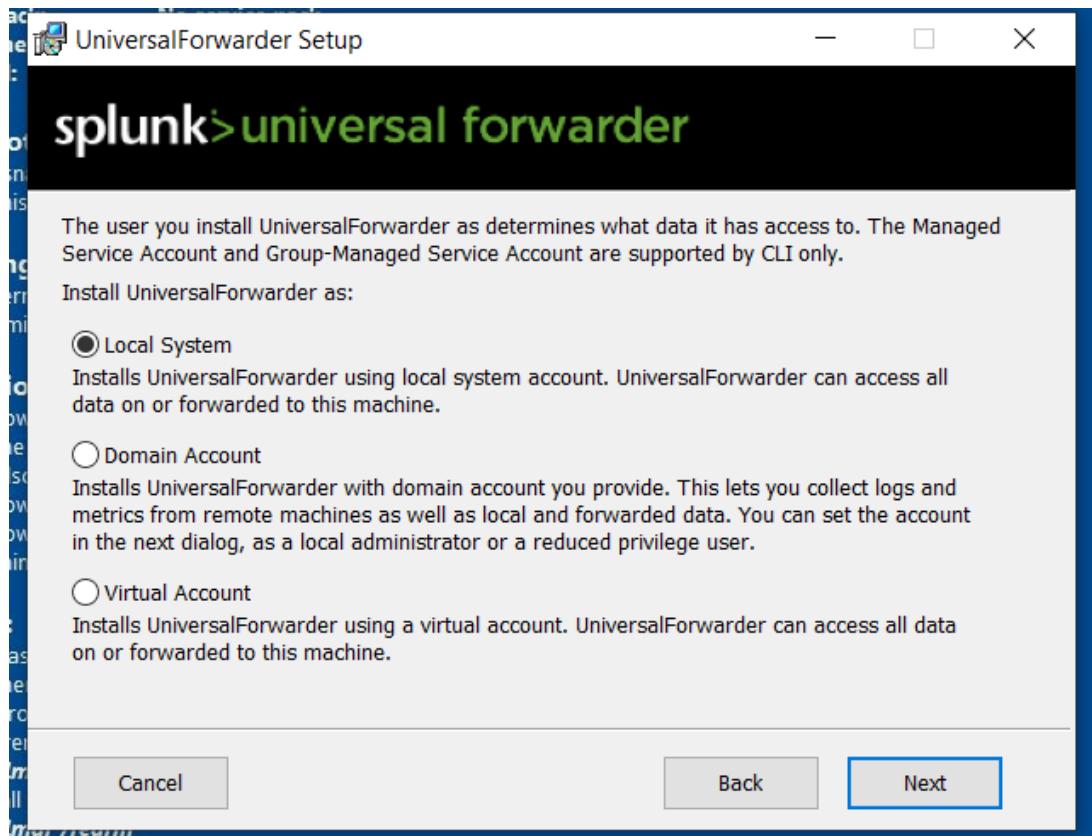
1.2. Setup

First We execute the msi program

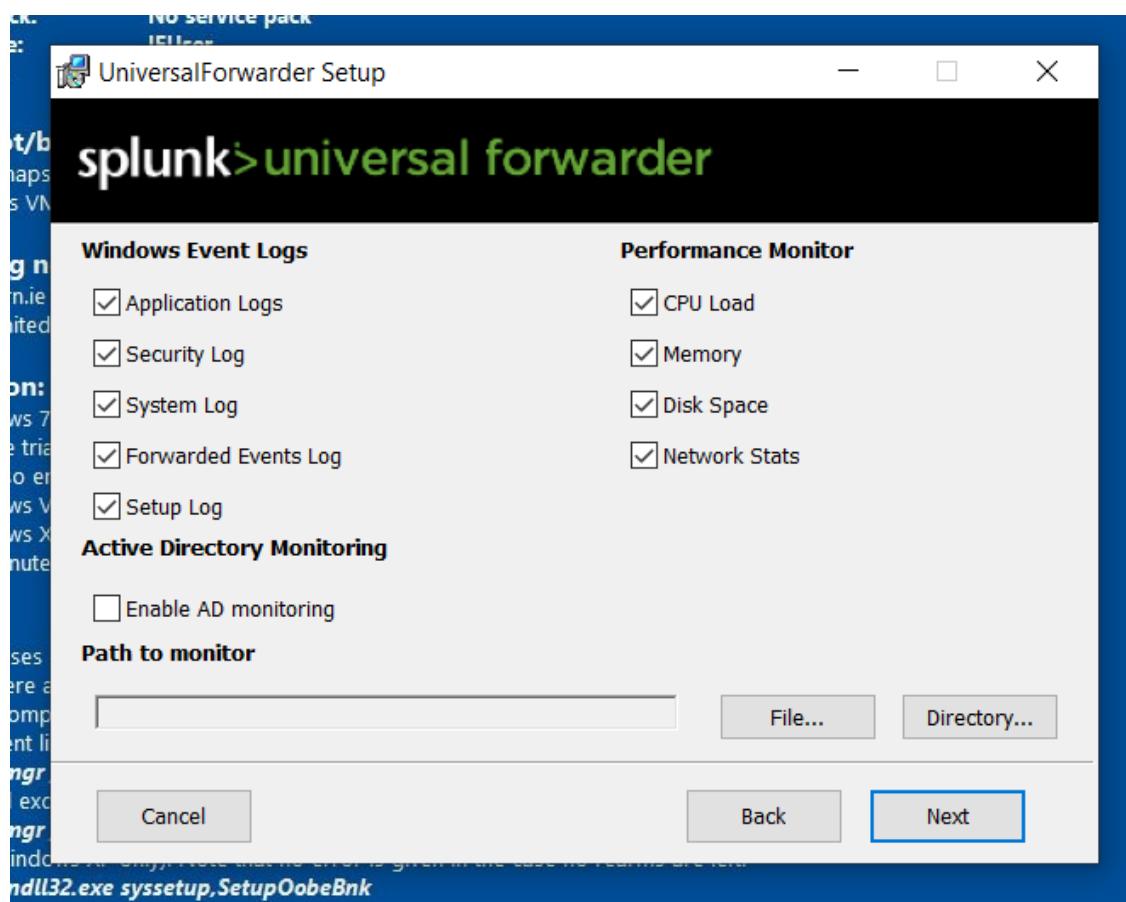


| Choose Customize options

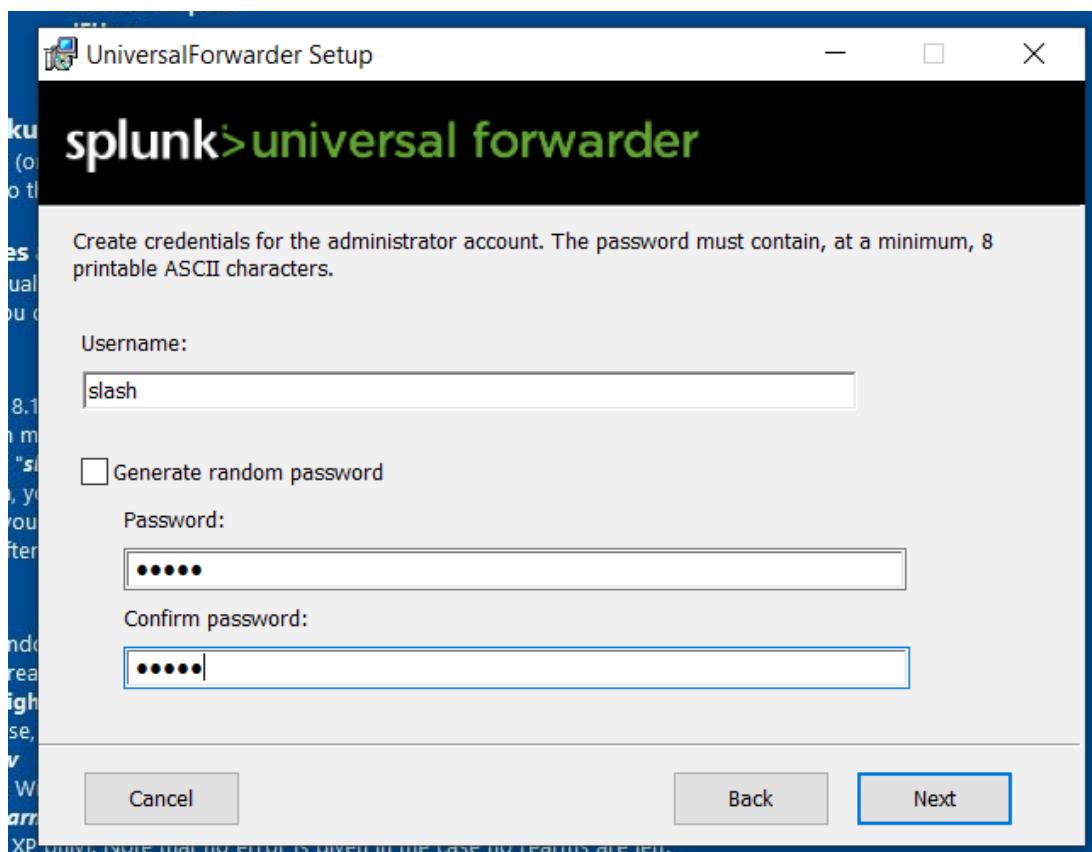




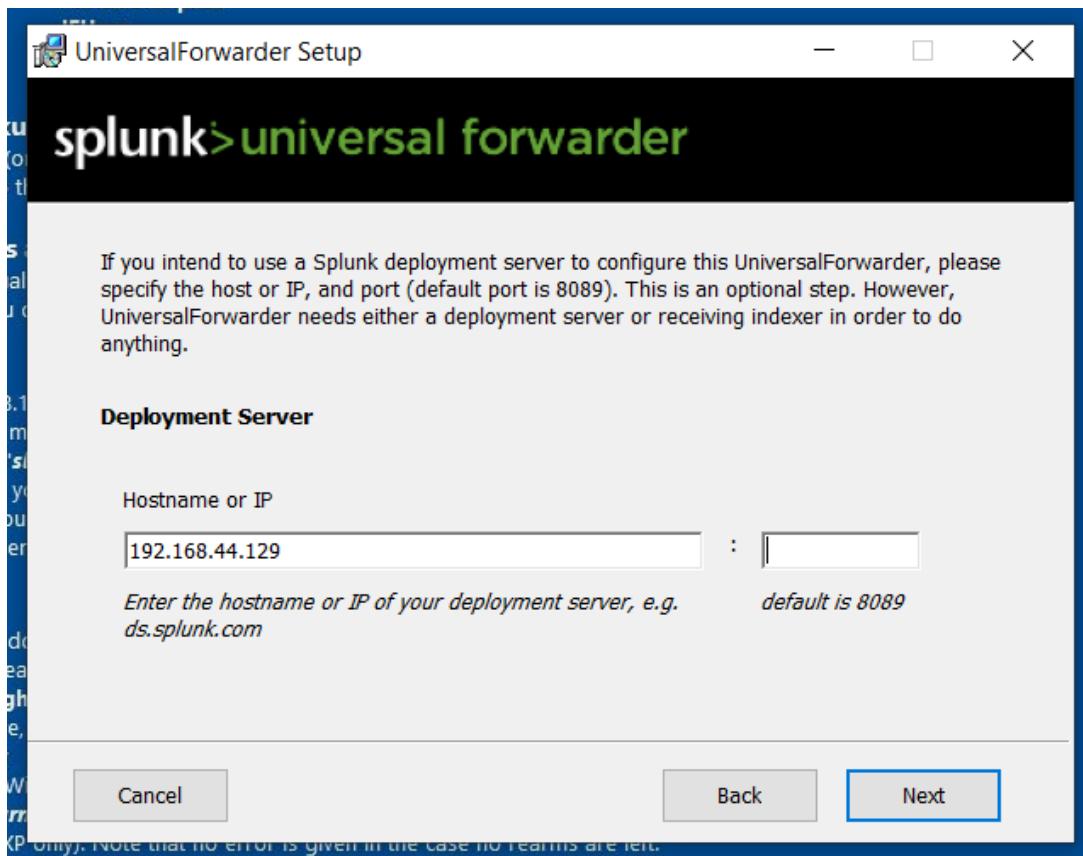
Choose Local System



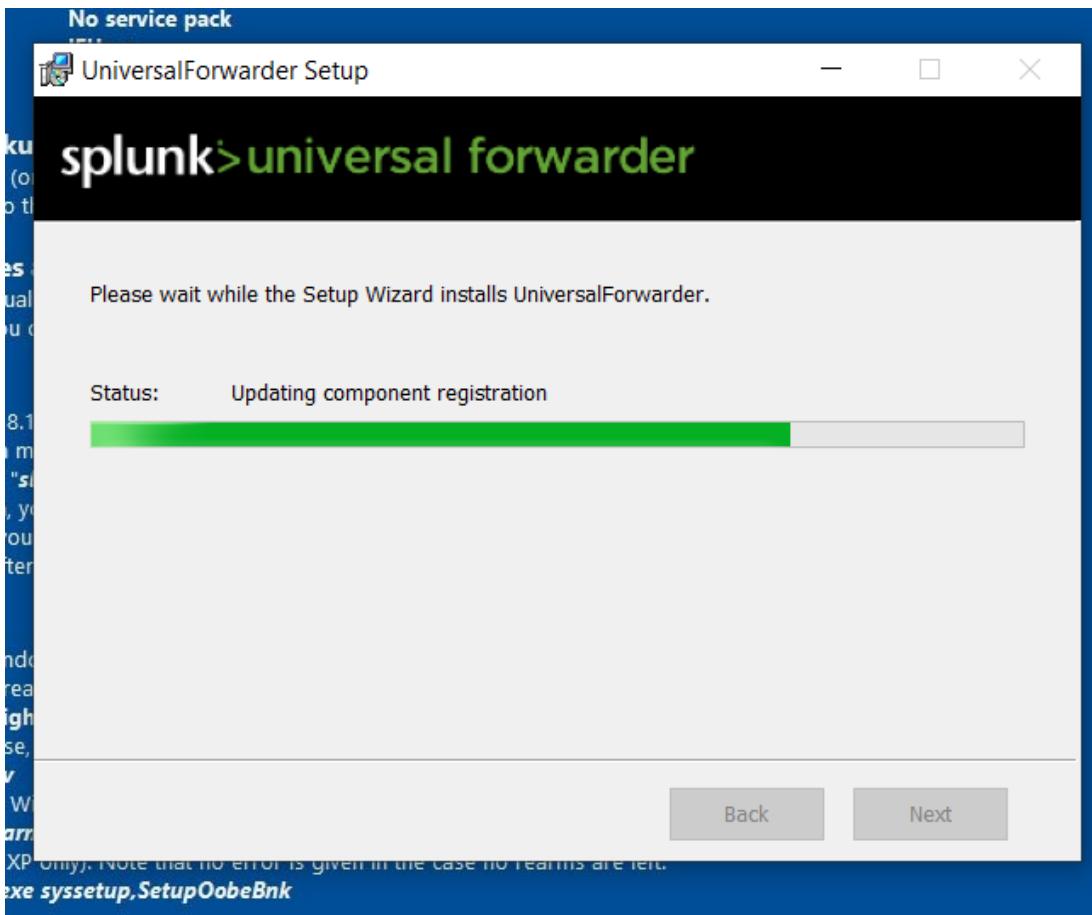
| Check all select box except AD Monitoring



| Create username and password

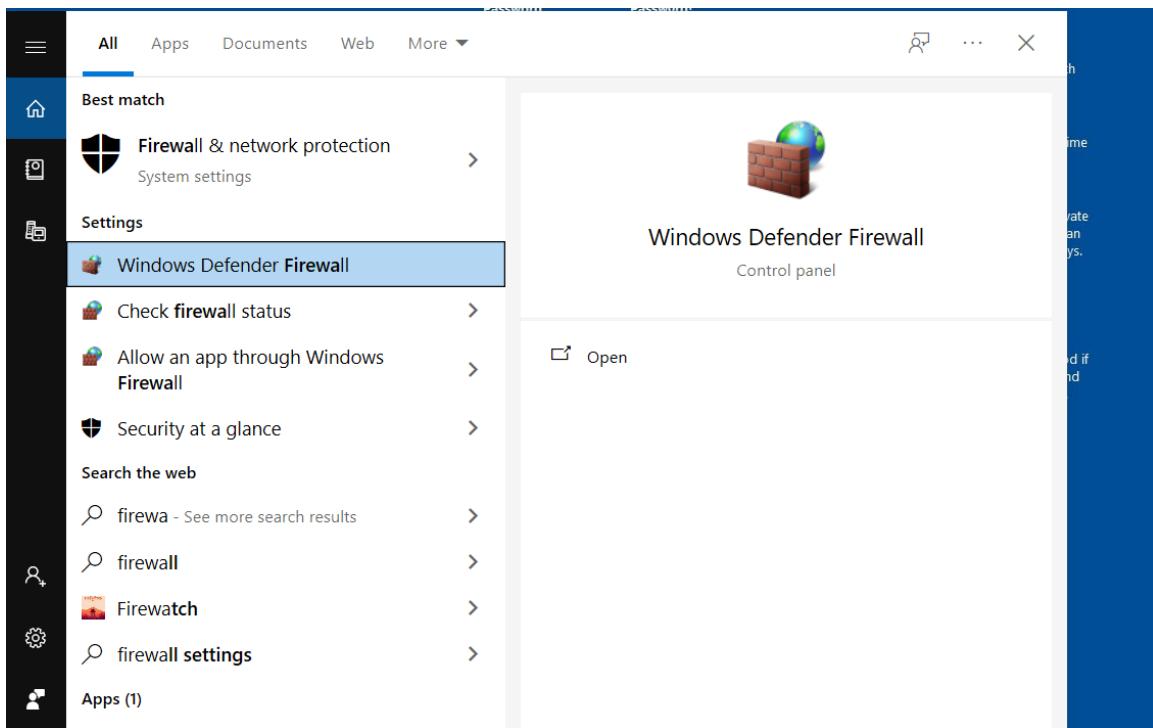


Here we write IP of our Kali Linux machine and let port is default.

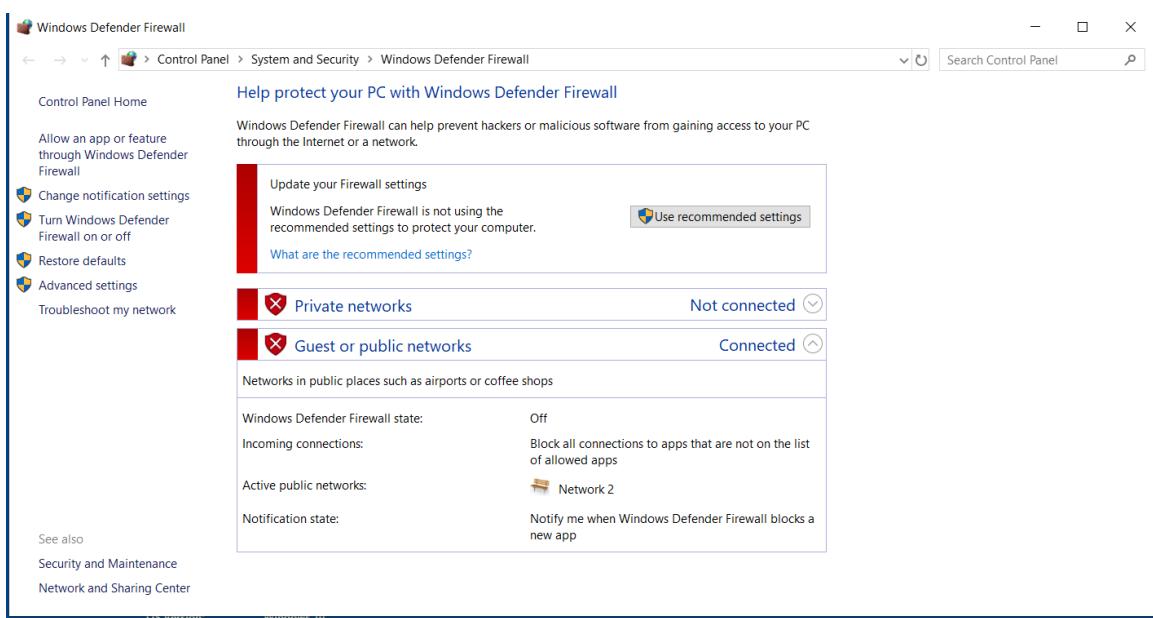


1.3. Configure Our Firewall rules

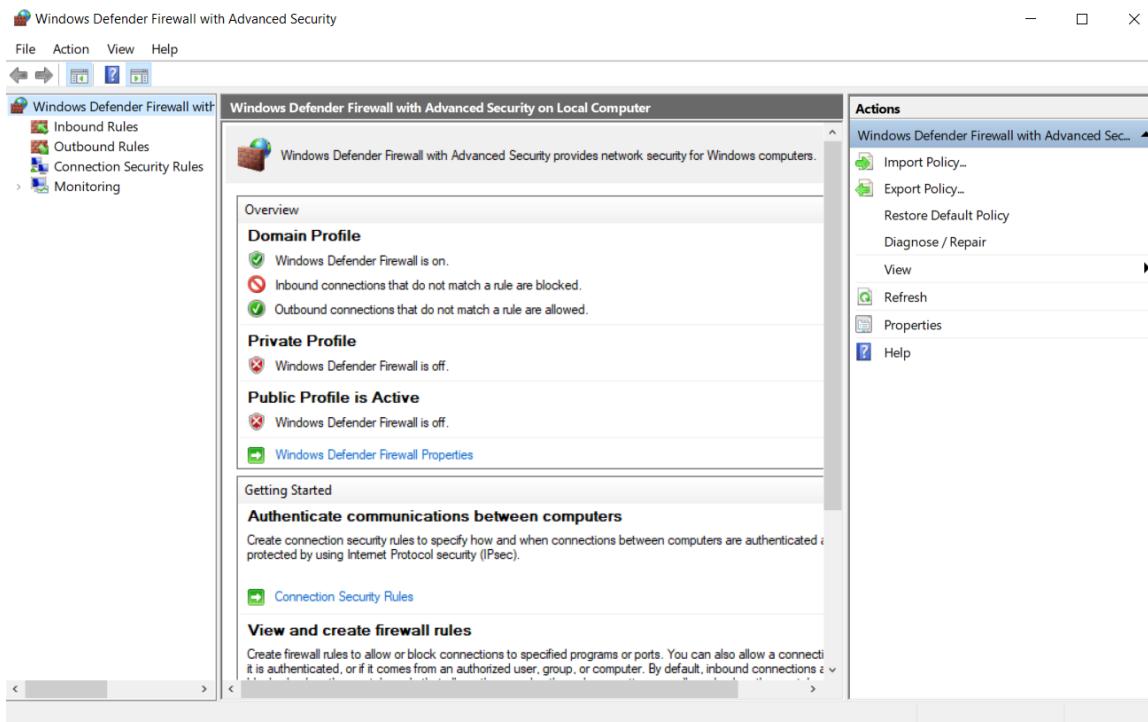
| First we search for firewall



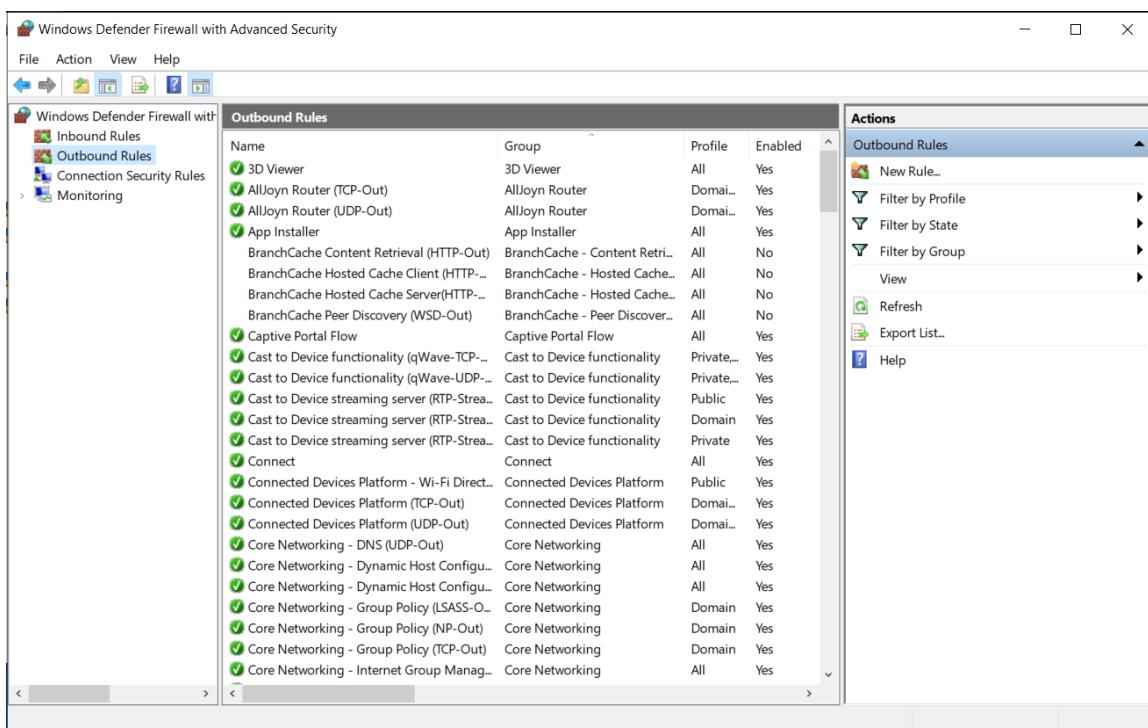
Open windows defender firewall



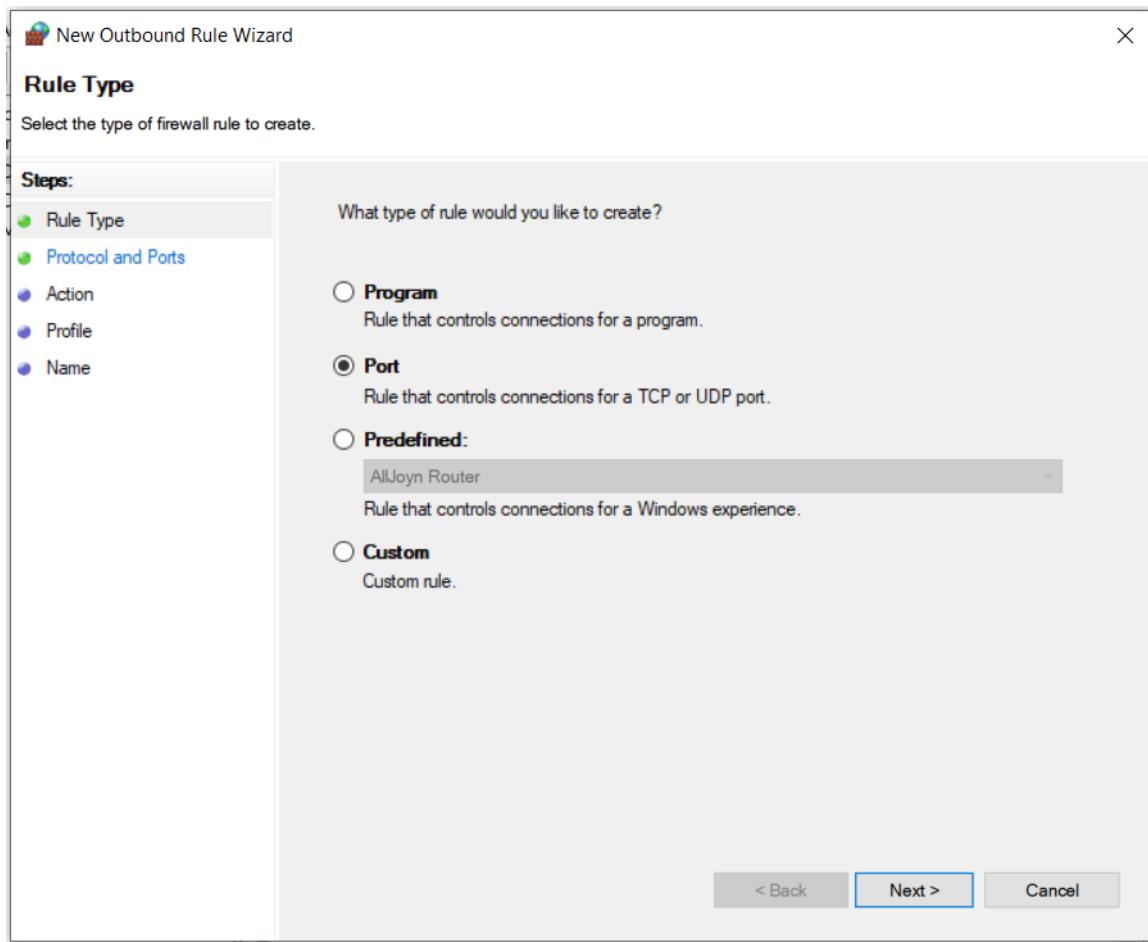
Navigate to advanced settings



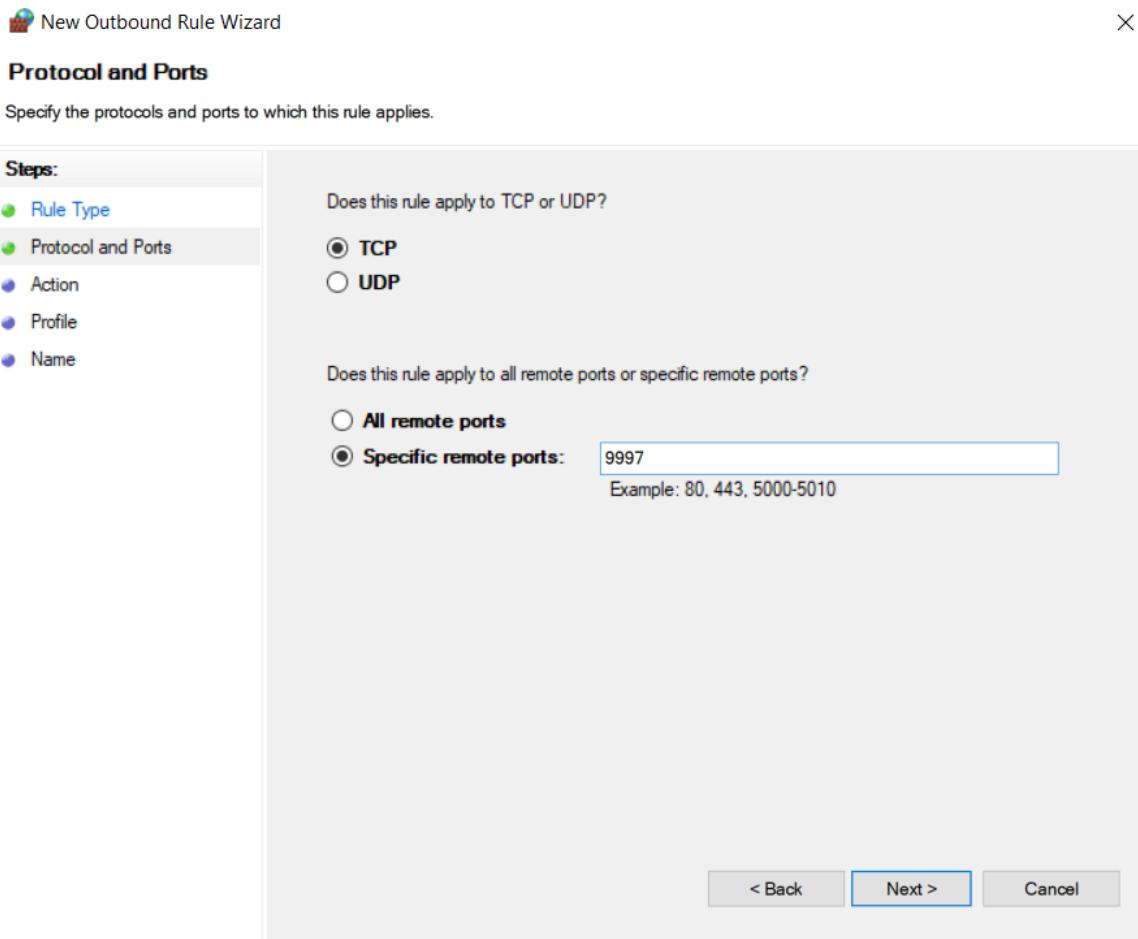
Navigate to Outbound Rules



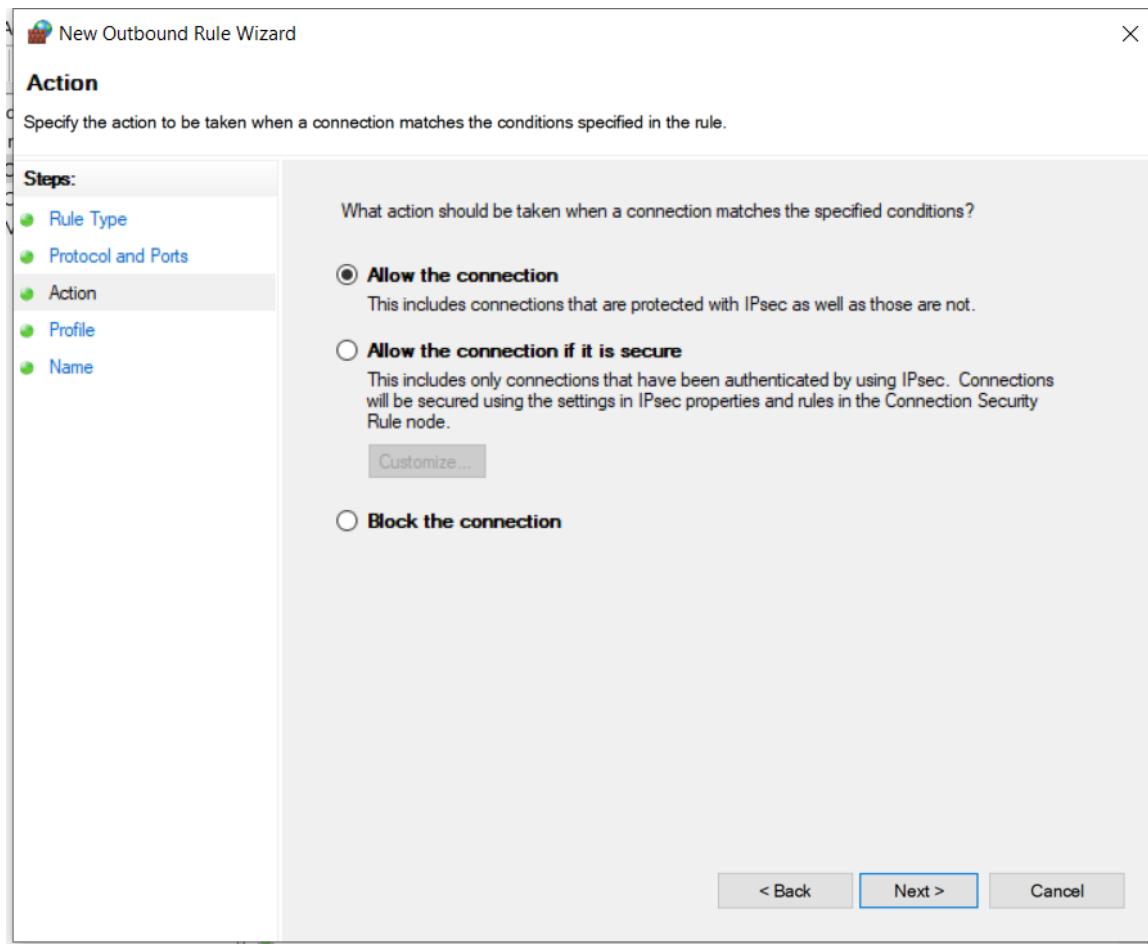
Create New Rule.



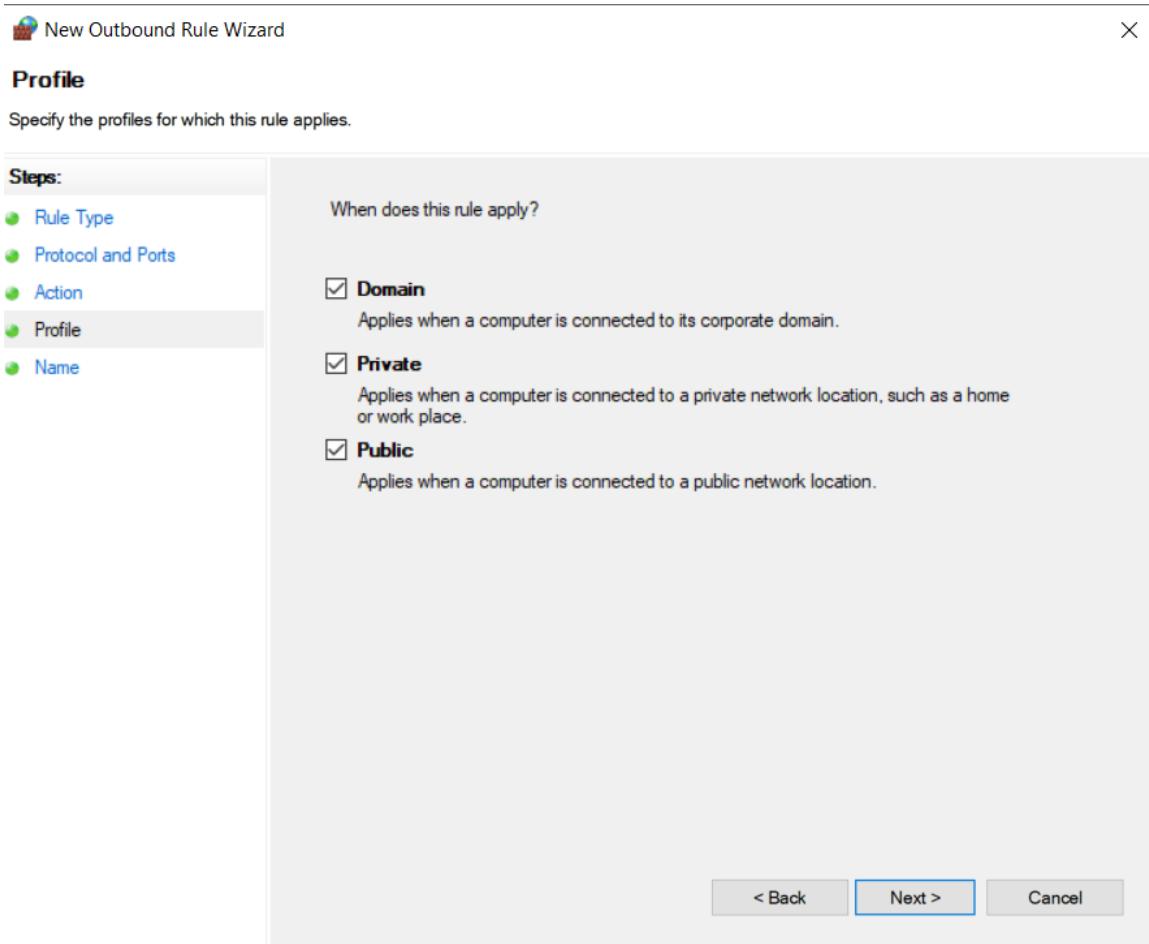
We Choose Port → Next



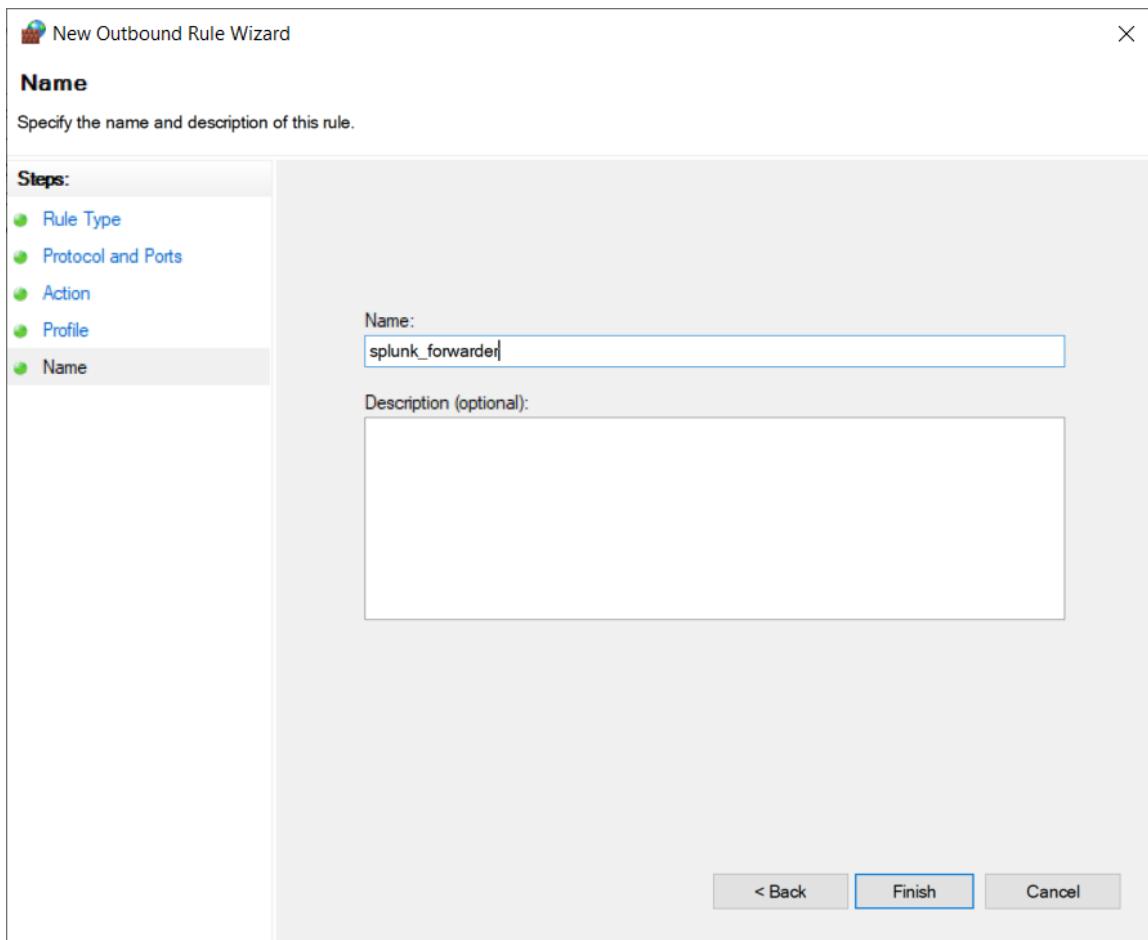
We choose TCP and Specific remote ports and write default port that we let at the configuration → Next



| Allow Connection → Next



| Select All → Next



| Name as you like → Next

▼ SPLUNK

1. Installation and Setup

1.1. We unpack the file “**Splunk.dep**”.

```
dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
```

1.2. Credentials Used.

```
username: slash  
password: 12345678
```

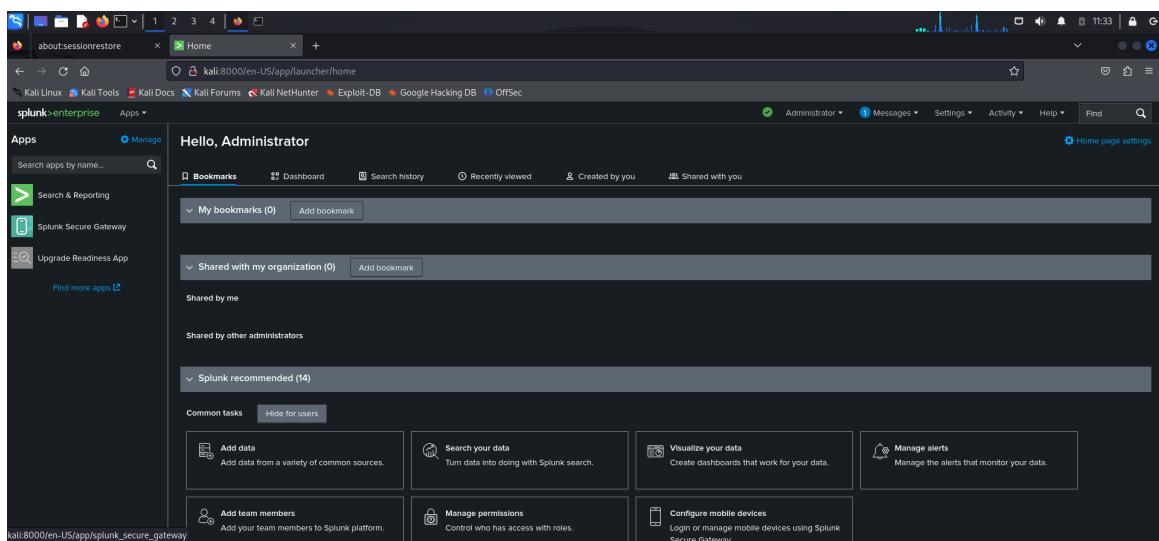
1.3. Start Splunk

```
sudo /opt/splunk/bin/splunk start
```

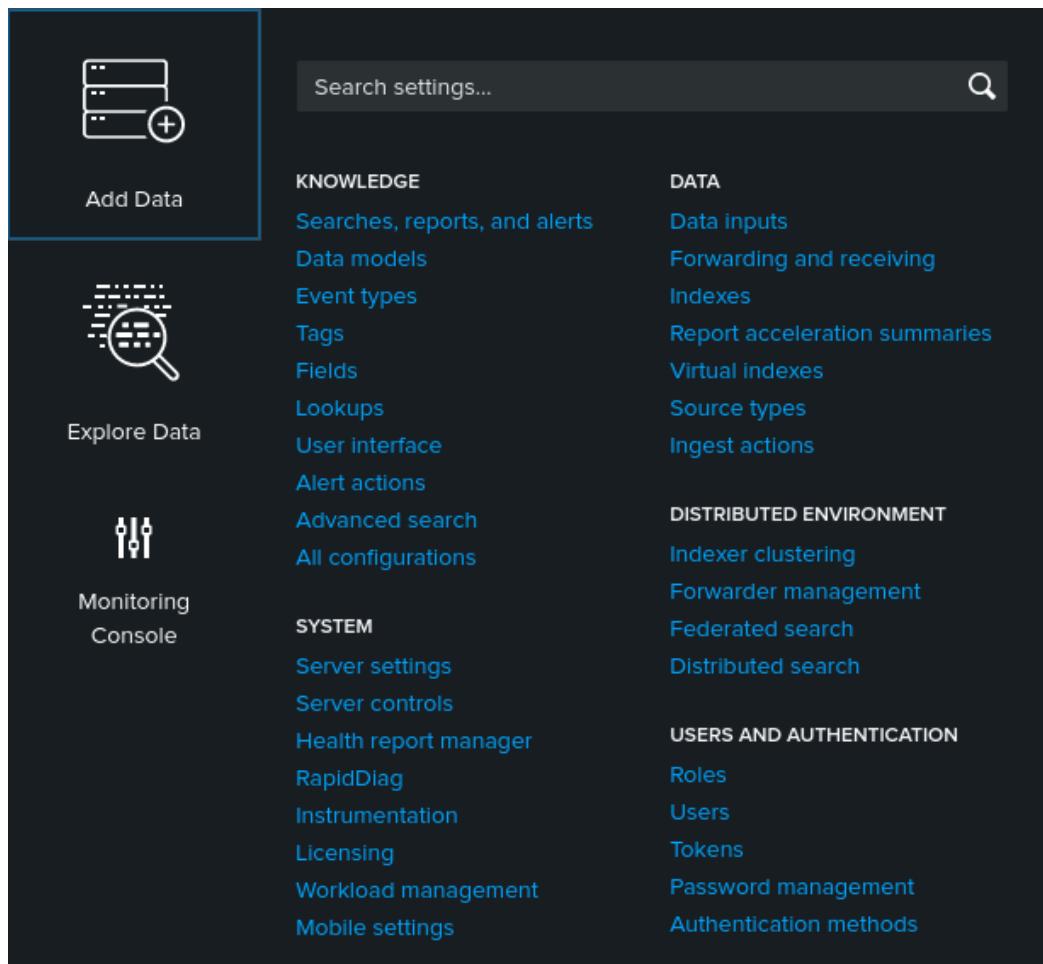
1.4. Login with your Credentials

You will see link in terminal click and open it and write your credentials.

After log in, you will see like this screen



Now we navigate to settings and from Data section choose forwarding and receiving.



We use receive data and add new.

The screenshot shows two configuration sections in the Splunk web interface:

Forward data

Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

We write default port of configuration of Splunk universal forwarder and click save.

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * 9997

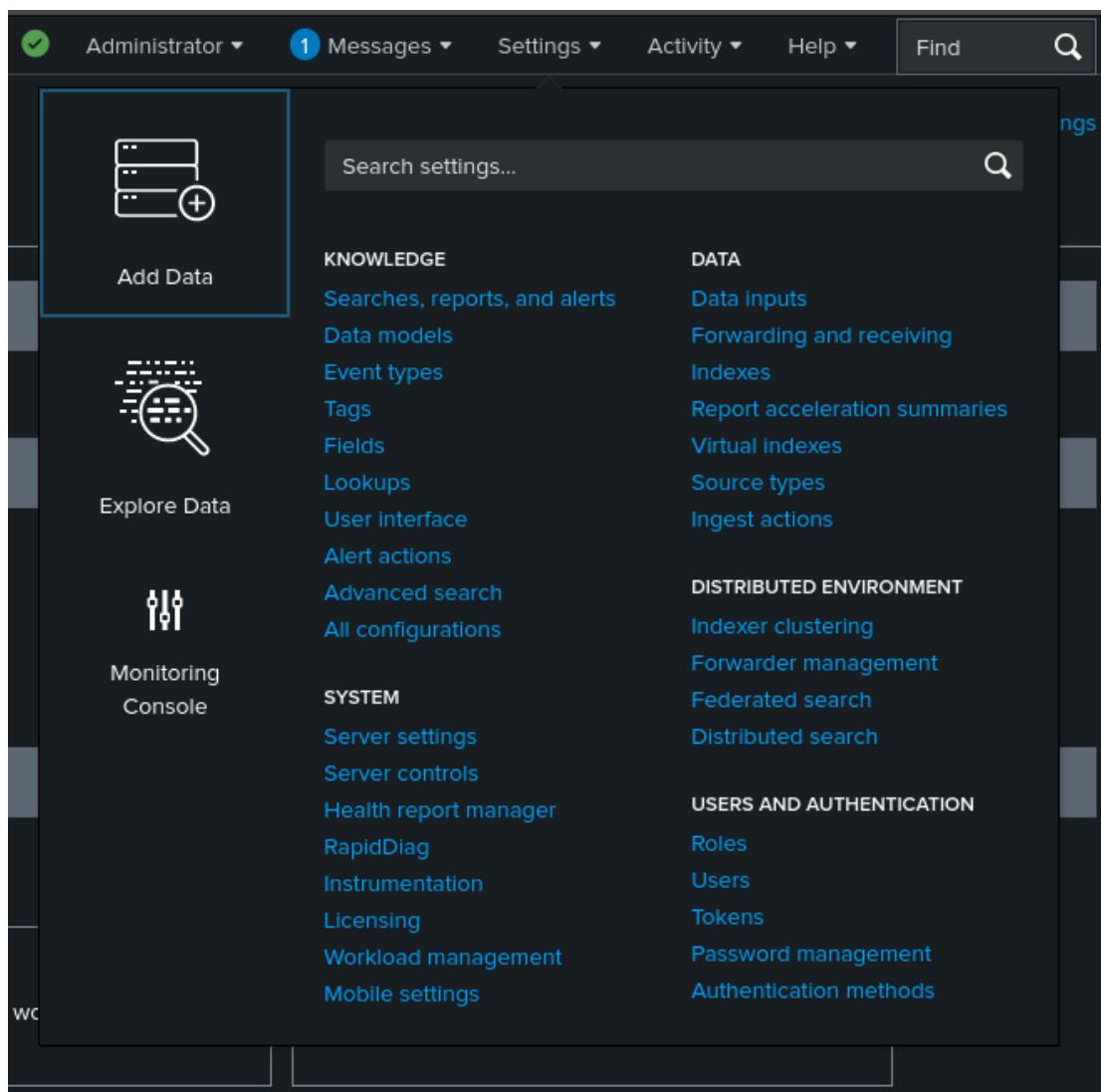
For example, 9997 will receive data on TCP port 9997.

Cancel

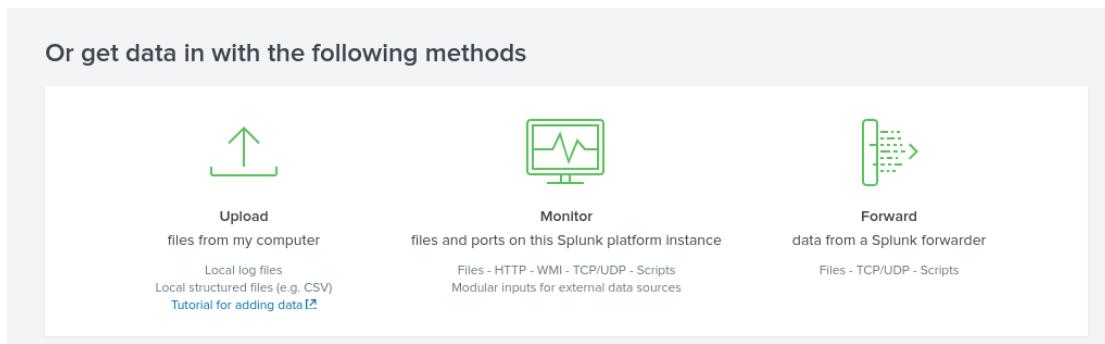
Save

▼ STEPS TO USE SPLUNK FOR INVESTIGATION

| We navigate to settings and Add Data.



| We Choose upload



We select file and upload our logs → `/var/log/suricata`

Add Data

Select Source Set Source Type Input Settings Review Done < Back **Next >**

Select Source

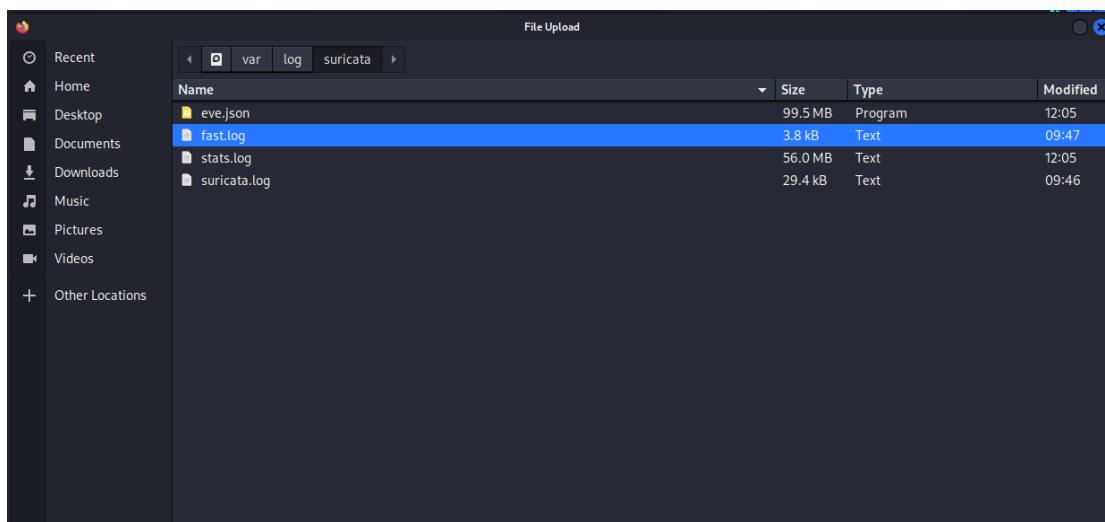
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: No file selected

Select File

Drop your data file here

The maximum file upload size is 500 Mb



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **fast.log**

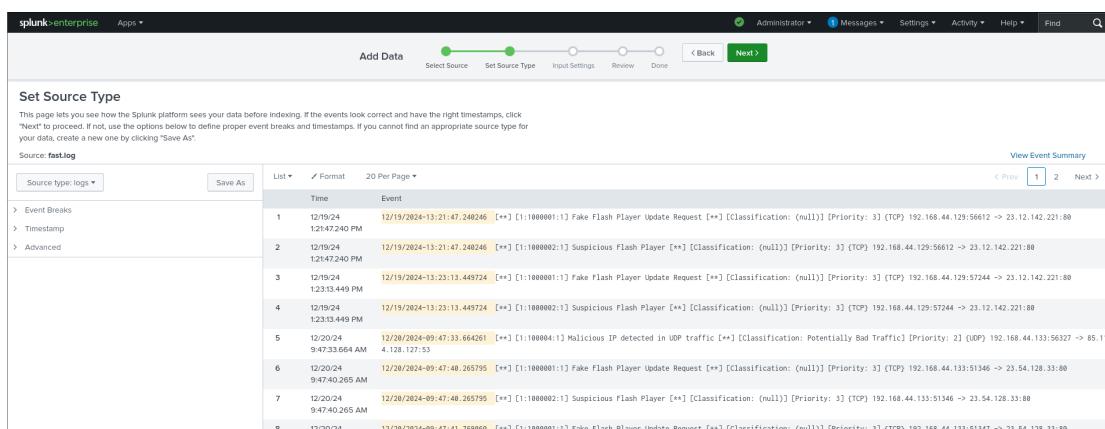
Select File

Drop your data file here

The maximum file upload size is 500 Mb

 File Successfully Uploaded

Choose sourcetype: **logs** ⇒ Next



Time	Event
12/19/24 1:25:47:240 PM	12/19/2024-13:21:47.240246 [+]Fake Flash Player Update Request [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.129:56612 -> 23.12.142.221:80
12/19/24 1:25:47:240 PM	12/19/2024-13:21:47.240246 [+]Suspicious Flash Player [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.129:56812 -> 23.12.142.221:80
12/19/24 1:25:13.449 PM	12/19/2024-13:23:13.449724 [+]Fake Flash Player Update Request [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.129:57244 -> 23.12.142.221:80
12/19/24 1:25:13.449 PM	12/19/2024-13:23:13.449724 [+]Suspicious Flash Player [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.129:57244 -> 23.12.142.221:80
12/20/24 9:47:33.664 AM	12/20/2024-09:47:33.664261 [+]Malicious IP detected in UDP traffic [+] [Classification: Potentially Bad Traffic] [Priority: 2] (UDP) 192.168.44.133:56327 -> 85.11.4.128.127:53
12/20/24 9:47:40.265 AM	12/20/2024-09:47:40.265795 [+]Fake Flash Player Update Request [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.133:51346 -> 23.54.128.33:80
12/20/24 9:47:40.265 AM	12/20/2024-09:47:40.265795 [+]Suspicious Flash Player [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.133:51346 -> 23.54.128.33:80
12/20/24 9:47:40.265 AM	12/20/2024-09:47:41.709600 [+]Fake Flash Player Update Request [+] [Classification: (null)] [Priority: 3] (TCP) 192.168.44.133:51347 -> 23.54.128.33:80

We need to create an index to use in search

Add Data

[Select Source](#) [Set Source Type](#) [Input Settings](#) [Review](#) [Done](#)

[Back](#) [Review >](#)

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index [Default](#) [Create a new index](#)

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

Create a new index

New Index [X](#)

General Settings

Index Name	<input type="text"/>	
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.		
Index Data Type	<input checked="" type="radio"/> Events	<input type="radio"/> Metrics
The type of data to store (event-based or metrics).		
Home Path	<input type="text" value="optional"/>	
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).		
Cold Path	<input type="text" value="optional"/>	
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).		
Thawed Path	<input type="text" value="optional"/>	
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).		
Data Integrity Check	<input type="radio"/> Enable	<input type="radio"/> Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.		
Max Size of Entire Index	<input type="text" value="500"/>	GB ▼
Save Cancel		

Name your index as you like and click save.

New Index

X

General Settings

Index Name Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB ▾

Save

Cancel

Click Review

Add Data Select Source Set Source Type Input Settings Review Done < Back Submit >

Review

Input Type Uploaded File
File Name fast.log
Source Type logs
Host kali
Index sruc_fast

Click Submit and Start Searching

Splunk>enterprise Apps ▾

New Search

source="fast.log" host="kali" index="sruc_fast" sourcetype="logs"

69 events (before 12/20/24 12:45:19.000 PM) No Event Sampling ▾

Events (69) Patterns Statistics Visualization

Format Timeline ▾ + Zoom Out + Zoom to Selection X Deselect

List ▾ Format 20 Per Page ▾

Time Event

Selected Fields: host=1, source=1, sourcetype=1

Interesting Fields: date_hour=2, date_minute=2, date_second=10, date_year=1, date_zone=1

Events:

- > 12/20/24 12/20/24:09:47:46.675842 [*] [1:1000002:1] Suspicious Flash Player [...] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 -> 23.54.128.33:80 host=kali source=fast.log sourcetype=logs
- > 12/20/24 12/20/24:09:47:46.675842 [*] [1:1000001:1] Fake Flash Player Update Request [...] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 -> 23.54.128.33:80 host=kali source=fast.log sourcetype=logs
- > 12/20/24 12/20/24:09:47:46.675842 [*] [1:1000002:1] Suspicious Flash Player [...] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 -> 23.54.128.33:80 host=kali source=fast.log sourcetype=logs
- > 12/20/24 12/20/24:09:47:46.675842 [*] [1:1000002:1] Suspicious Flash Player [...] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 -> 23.54.128.33:80 host=kali source=fast.log sourcetype=logs
- > 12/20/24 12/20/24:09:47:46.675842 [*] [1:1000002:1] Suspicious Flash Player [...] [Classification: (null)] [Priority: 3] {TCP} 192.168.44.133:51347 -> 23.54.128.33:80 host=kali source=fast.log sourcetype=logs

Now we upload `eve.json` with same steps of the `fast.log`.

Add Data

Select Source Set Source Type Input Settings Review Done < Back Next >

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: eve.json

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

After Uploading `eve.json`

Splunk>enterprise Apps ▾

New Search

source="eve.json" host="kali" index="sruc_eve" sourcetype="logs"

1,663 events (2/19/24 4:00:00:00 PM to 12/20/24 4:12:18.000 PM) No Event Sampling ▾

Events (1,663) Patterns Statistics Visualization

Format Timeline ▾ + Zoom Out + Zoom to Selection X Deselect

List ▾ Format 20 Per Page ▾

Time Event

Selected Fields: host=1, source=1, sourcetype=1

Interesting Fields: date_hour=3, date_minute=27, date_month=1, date_second=60, date_year=7, date_zone=1

Events:

- > 12/20/24 2:12:37142 PM [{ ... } event_type: stats \$stats: [{ ... }] timestamp: 2024-12-20T14:12:37.142155-0500] Show as raw text host=kali source=eve.json sourcetype=logs
- > 12/20/24 2:12:36139 PM [{ ... } app_proto: dns community_id: 1:kdk3FQfR7NY1SpnfZxeHf757nE dest_ip: 192.168.44.1 dest_port: 53 source_ip: 23.54.128.33 dest_port: 53] Show as raw text host=kali source=eve.json sourcetype=logs

▼ Visualize With Splunk

| Go To Dashboard

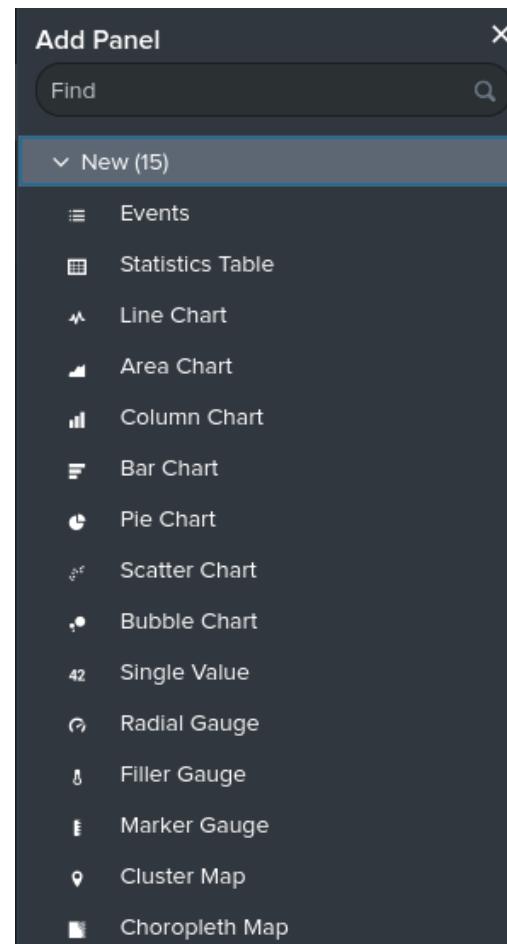
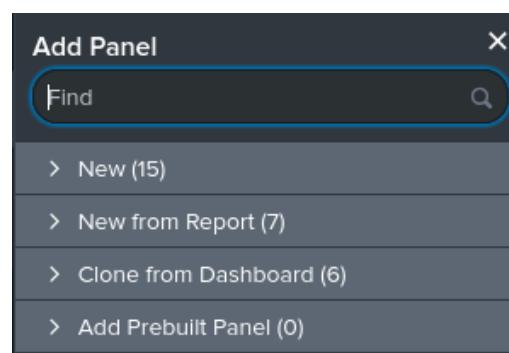
The screenshot shows the Splunk Enterprise interface with the 'Dashboards' tab selected. At the top, there are several informational cards: 'Examples for Dashboard Studio', 'Intro to Dashboard Studio', and 'Intro to Classic Dashboards'. Below this is a table listing six existing dashboards, each with columns for Actions, Owner, App, Sharing, and Type. The dashboards listed are: 'Integrity Check of Installed Files', 'Job Details Dashboard', 'jQuery Upgrade', 'Orphaned Scheduled Searches, Reports, and Alerts', 'Scheduled export is now available for Dashboard Studio', and 'WinInvestigation24'. A green button at the top right says 'Create New Dashboard'.

| Name Your Dashboard and choose classic Dashboards and click create.

The dialog box has a title 'Create New Dashboard' and a close button. It contains three main input fields: 'Dashboard Title' with the value 'ZeusInvestigation24', 'Description' with the value 'Optional', and 'Permissions' set to 'Private'. Below these fields is a question 'How do you want to build your dashboard?' with a 'What's this?' link. Two options are shown: 'Classic Dashboards' (selected) and 'Dashboard Studio' (NEW). Both options have descriptions below them. At the bottom are 'Cancel' and 'Create' buttons.

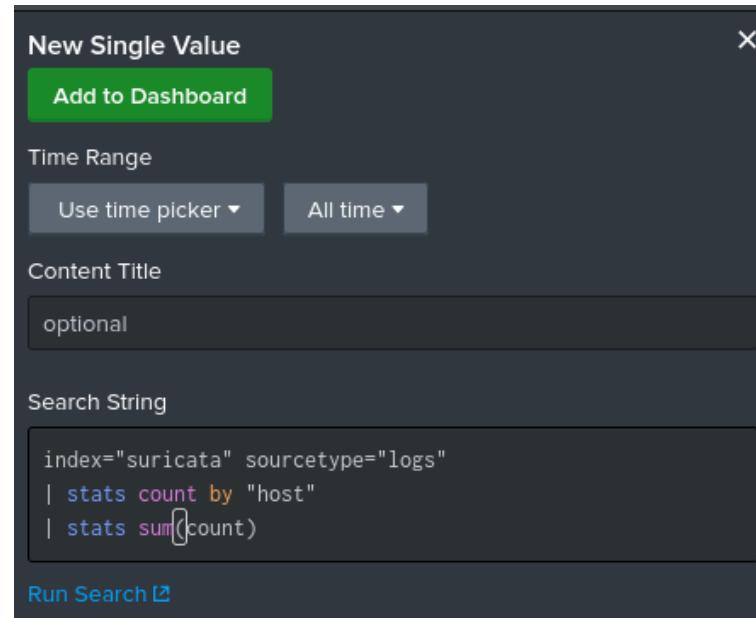
| Now, we click on add panel → choose new form and choose your chart visualization.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps ▾'. Below it is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A toolbar below these includes 'Edit Dashboard' (highlighted in blue), 'UI', 'Source', '+ Add Panel', '+ Add Input ▾', and a 'Dark Theme' toggle switch. The main content area is titled 'ZeusInvestigation24' and has a sub-section 'No description'. The overall theme is dark.

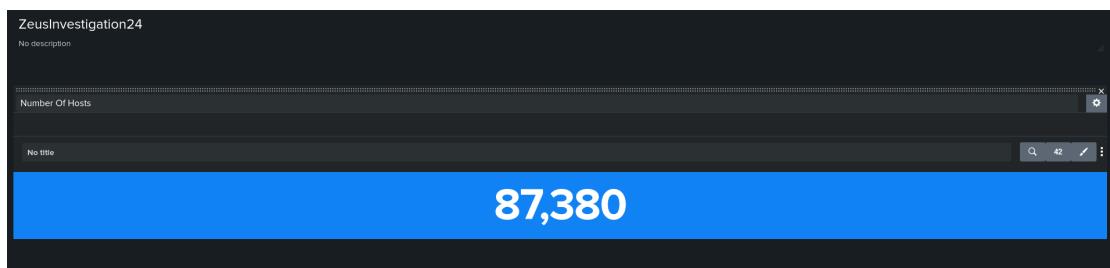


We choose Single value and write our query

```
index="suricata" sourcetype="logs"
| stats count by "host"
| stats sum(count)
```



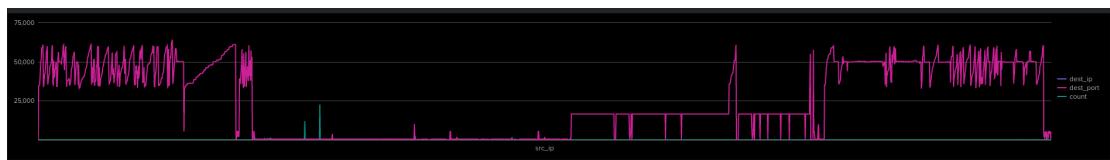
| Click all time and add to dashboard.



| We add some visualizations.

| Second Query

```
index="suricata" sourcetype="logs"
| stats count by src_ip,dest_ip,dest_port
```



▼ YARA

```
rule ZeusBanking_Detection {  
    meta:  
        description = "A detection rule against ZeusBankingVersion_26N  
    strings:  
        $file_name = "invoice_2318362983713_823931342io.pdf.exe" ascii  
        $function_name_KERNEL32_CreateFileA = "CellrotoCrudUntohighCol  
        $PE_magic_byte = "MZ"  
        $hex_pattern = {43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72}  
    condition:  
        $PE_magic_byte at 0 and $file_name  
        and $function_name_KERNEL32_CreateFileA  
        or $hex_pattern  
}
```

```
1 rule ZeusBanking_Detection {  
2     meta:  
3         description = "A detection rule against  
ZeusBankingVersion_26Nov2013"  
4     strings:  
5         $file_name = "invoice_2318362983713_823931342io.pdf.exe" ascii  
6         $function_name_KERNEL32_CreateFileA = "CellrotoCrudUntohighCols"  
7         ascii  
8             $PE_magic_byte = "MZ"  
9             $hex_pattern = {43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72}  
10        condition:  
11            $PE_magic_byte at 0 and $file_name  
12            and $function_name_KERNEL32_CreateFileA  
13            or $hex_pattern  
14 }
```

This yara rule is used for identifying zeus malware, here is a breakdown of the rule:

Meta Section

provide descriptive info about the rule

Strings Section

specifies the patterns that the rule will look for in the scanned file

\$file_name: containing the suspicious file name

\$function_name_KERNEL32_CreateFileA: A string representing the name of a function, CellrotoCrudUntohighCols, which may be a part of obfuscated or custom function calls within the malware.

\$PE_magic_byte: The string "MZ" is the magic number at the start of Portable Executable (PE) files, which indicates that the file is an executable in the Windows PE format.

\$hex_pattern: A hex string {43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72} representing a specific sequence translates to the ASCII string (CameValeWarner), which may be a marker or unique identifier within the malware.

Condition Section

\$PE_magic_byte at 0: Checks if the string \$PE_magic_byte ("MZ") is located at offset 0, which confirms that the file is a PE file.

And \$file_name: Ensures that the suspicious file name pattern \$file_name is present in the file.

And \$function_name_KERNEL32_CreateFileA: Confirms that the string \$function_name_KERNEL32_CreateFileA appears in the file, potentially indicating a call to a suspicious or obfuscated function.

or \$hex_pattern: Allows the rule to match files containing the specific byte sequence \$hex_pattern even if other conditions are not met.

Running the yara command for scanning:

```
yara rules.yara invoice_2318362983713_823931342io.pdf.exe -s -w -p 32
```

```
(kali㉿kali)-[~/Downloads]$ yara rules.yara invoice_2318362983713_823931342io.pdf.exe -s -w -p 32
ZeusBanking_Detection invoice_2318362983713_823931342io.pdf.exe
0x3176c:$function_name_KERNEL32_CreateFileA: CellrotoCrudUntohighCols
0x0:$PE_magic_byte: MZ
0x31716:$hex_pattern: 43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72
```

The output indicates that the rule `ZeusBanking_Detection` identified the file `invoice_2318362983713_823931342io.pdf.exe` as malicious based on its conditions.

Matched Strings

`$function_name_KERNEL32_CreateFileA:` Found at offset `0x3176C`. The matched string is `CellrotoCrudUntohighCols`, which corresponds to a suspicious function call in the file.

`$PE_magic_byte:` Found at offset 0. This confirms that the file starts with the magic bytes `MZ`, indicating it is a Windows Portable Executable (PE) file.

`$hex_pattern:` Found at offset `0x31716`. This matched the specific sequence of bytes `{43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72}` defined in the rule.

▼ VOLATILITY

We are going to use The Volatility tool that help us to investigate and analyze memory dumps and extract information about running processes, network connections, and potential malware.

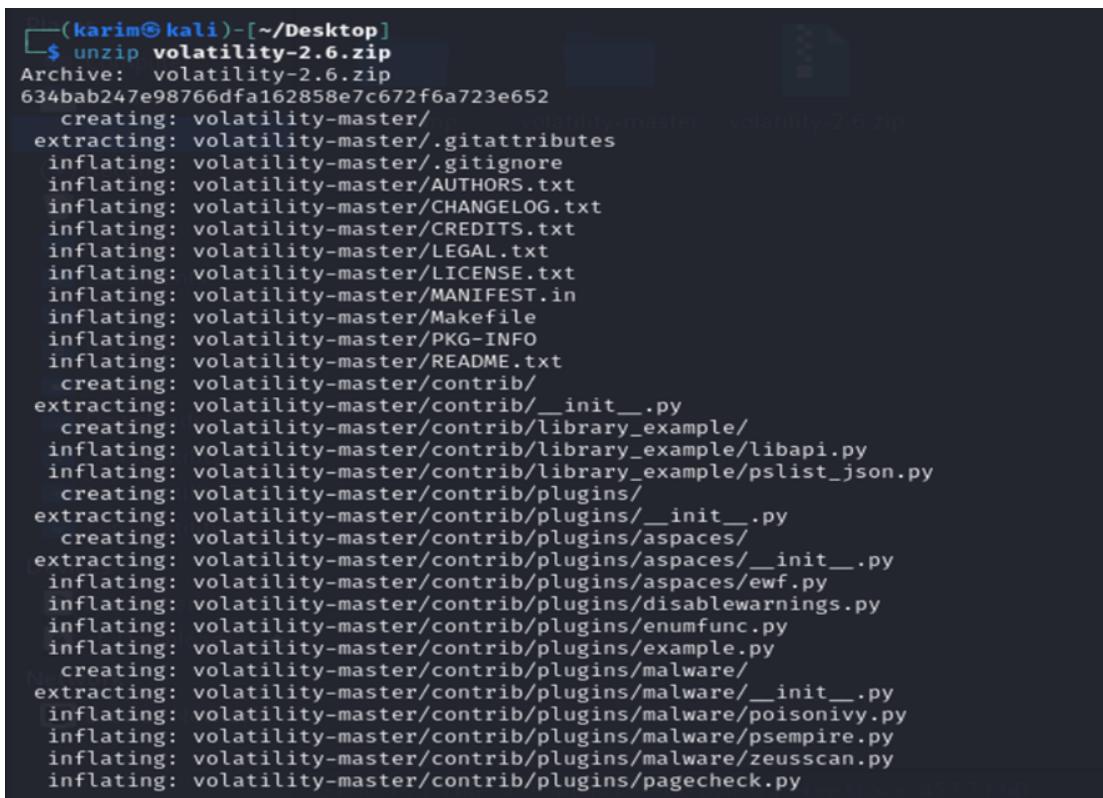
▼ STEPS

1. Download And Setup

Link:

<https://github.com/volatilityfoundation/volatility/releases/tag/2.6.1>

then we are going to unzip the file after download it using (unzip volatility-master) command.



```
(karim㉿kali)-[~/Desktop]$ unzip volatility-2.6.zip
Archive:  volatility-2.6.zip
634bab247e98766dfa162858e7c672f6a723e652
  creating: volatility-master/
  extracting: volatility-master/.gitattributes
  inflating: volatility-master/.gitignore
  inflating: volatility-master/AUTHORS.txt
  inflating: volatility-master/CHANGELOG.txt
  inflating: volatility-master/CREDITS.txt
  inflating: volatility-master/LEGAL.txt
  inflating: volatility-master/LICENSE.txt
  inflating: volatility-master/MANIFEST.in
  inflating: volatility-master/Makefile
  inflating: volatility-master/PKG-INFO
  inflating: volatility-master/README.txt
  creating: volatility-master/contrib/
  extracting: volatility-master/contrib/__init__.py
  creating: volatility-master/contrib/library_example/
  inflating: volatility-master/contrib/library_example/libapi.py
  creating: volatility-master/contrib/plugins/
  extracting: volatility-master/contrib/plugins/__init__.py
  creating: volatility-master/contrib/plugins/aspaces/
  extracting: volatility-master/contrib/plugins/aspaces/__init__.py
  inflating: volatility-master/contrib/plugins/aspaces/ewf.py
  inflating: volatility-master/contrib/plugins/disablewarnings.py
  inflating: volatility-master/contrib/plugins/enumfunc.py
  inflating: volatility-master/contrib/plugins/example.py
  creating: volatility-master/contrib/plugins/malware/
  extracting: volatility-master/contrib/plugins/malware/__init__.py
  inflating: volatility-master/contrib/plugins/malware/poisonivy.py
  inflating: volatility-master/contrib/plugins/malware/psemprise.py
  inflating: volatility-master/contrib/plugins/malware/zeuscan.py
  inflating: volatility-master/contrib/plugins/pagecheck.py
```

1. Get Image Information

```
python2 vol.py -f zeus2x4.vmem imageinfo
```

The command give us details about the memory image and profiles(**WinXPSP2x86**, **WinXPSP3x86**), the number of processors, and the image's date and time. And we are going to use **WinXPSP2x86** as profile.

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem imageinfo

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

INFO    : volatility.debug    : Determining profile based on KDBG search ...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                      AS Layer1 : IA32PagedMemory (Kernel AS)
                      AS Layer2 : FileAddressSpace (/home/karim/Downloads/volatility-master/zeus2x4.vmem)
                      PAE type : No PAE
                      DTB : 0x39000L
                      KDBG : 0x8054cde0L
                      Number of Processors : 1
Image Type (Service Pack) : 3
                      KPCR for CPU 0 : 0xffdff000L
                      KUSER_SHARED_DATA : 0xfffff0000L
                      Image date and time : 2010-09-09 19:56:54 UTC+0000
Image local date and time : 2010-09-09 15:56:54 -0400
```

2. Process Scan

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 psscan
```

The command scans memory for process-related structures using signature-based search techniques. And we will see all the processes we have.

```
(karim@kali)[-~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 psscan

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

Offset(P) Name PID PPID PDB Time created Time exited
-----
0x00000000001e87da0 ihah.exe 3276 3772 0x1466b000 2010-09-09 19:56:32 UTC+0000
0x00000000001e8a368 alg.exe 2588 744 0x15058000 2010-09-02 12:25:44 UTC+0000
0x00000000001eb2f8 wuauclt.exe 3984 1084 0x173b7000 2010-09-09 19:52:45 UTC+0000
0x00000000001f4bb28 b98679df6defbb3 3772 2404 0x1f308000 2010-09-09 19:56:19 UTC+0000
0x00000000001ffb6d8 ImmunityDebugge 3788 1752 0x03e57000 2010-09-08 22:39:40 UTC+0000
0x00000000002001ad0 ImmunityDebugge 2972 1752 0x0e002000 2010-09-08 19:14:36 UTC+0000
0x0000000000205dda0 wuauclt.exe 940 1084 0x1be36000 2010-09-02 12:26:40 UTC+0000
0x00000000002066478 ImmunityDebugge 2404 1752 0x0586f000 2010-09-09 19:56:19 UTC+0000
0x00000000002077da0 coherence.exe 572 744 0x15e5d000 2010-09-02 12:25:36 UTC+0000
0x0000000000207bda0 nife_k_locked.ex 2204 2972 0x1804d000 2010-09-08 19:14:36 UTC+0000
0x00000000002086798 prl_tools.exe 632 436 0x15e79000 2010-09-02 12:25:36 UTC+0000
0x00000000002089558 jqs.exe 472 744 0x1598b000 2010-09-02 12:25:33 UTC+0000
```

```
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Offset(P) Name PID PPID PDB Time created Time exited
-----
0x00000000001e87da0 ihah.exe 3276 3772 0x1466b000 2010-09-09 19:56:32 UTC+0000
0x00000000001e8a368 alg.exe 2588 744 0x15058000 2010-09-02 12:25:44 UTC+0000
0x00000000001eb2f8 wuauclt.exe 3984 1084 0x173b7000 2010-09-09 19:52:45 UTC+0000
0x00000000001f4bb28 b98679df6defbb3 3772 2404 0x1f308000 2010-09-09 19:56:19 UTC+0000
0x00000000001ffb6d8 ImmunityDebugge 3788 1752 0x03e57000 2010-09-08 22:39:40 UTC+0000
0x00000000002001ad0 ImmunityDebugge 2972 1752 0x0e002000 2010-09-08 19:14:36 UTC+0000
0x0000000000205dda0 wuauclt.exe 940 1084 0x1be36000 2010-09-02 12:26:40 UTC+0000
0x00000000002066478 ImmunityDebugge 2404 1752 0x0586f000 2010-09-09 19:56:19 UTC+0000
0x00000000002077da0 coherence.exe 572 744 0x15e5d000 2010-09-02 12:25:36 UTC+0000
0x0000000000207bda0 nife_k_locked.ex 2204 2972 0x1804d000 2010-09-08 19:14:36 UTC+0000
0x00000000002086798 prl_tools.exe 632 436 0x15e79000 2010-09-02 12:25:36 UTC+0000
0x00000000002089558 jqs.exe 472 744 0x1598b000 2010-09-02 12:25:33 UTC+0000
0x0000000000208abf0 sqlserver.exe 488 744 0x15a12000 2010-09-02 12:25:33 UTC+0000
0x00000000002095500 spoolsv.exe 1616 744 0x10a9d000 2010-09-02 12:25:24 UTC+0000
0x000000000020ee580 prl_cc.exe 1908 1752 0x11de1000 2010-09-02 12:25:25 UTC+0000
0x00000000002129370 svchost.exe 364 744 0x157c5000 2010-09-02 12:25:33 UTC+0000
0x0000000000212ada0 jusched.exe 1936 1752 0x12010000 2010-09-02 12:25:26 UTC+0000
0x0000000000213ddaa0 wscntfy.exe 2180 1084 0x1993a000 2010-09-02 12:25:41 UTC+0000
0x00000000002147488 svchost.exe 1192 744 0x10147000 2010-09-02 12:25:23 UTC+0000
0x00000000002150b90 svchost.exe 912 744 0x0e9ad000 2010-09-02 12:25:22 UTC+0000
0x00000000002151da0 svchost.exe 1084 744 0x0ef67000 2010-09-02 12:25:22 UTC+0000
0x000000000021521b0 svchost.exe 1140 744 0x0f13b000 2010-09-02 12:25:22 UTC+0000
0x00000000002189530 prl_tools_servi 436 744 0x15ce2000 2010-09-02 12:25:36 UTC+0000
0x0000000000219e6c8 anaxuu.exe 3508 3788 0x1a36a000 2010-09-08 22:39:40 UTC+0000
0x000000000021a5da0 services.exe 744 692 0x0e0d7000 2010-09-02 12:25:22 UTC+0000
0x000000000021aa7e8 sqlwriter.exe 660 744 0x15e67000 2010-09-02 12:25:36 UTC+0000
0x000000000021b2020 explorer.exe 1752 1720 0x10e31000 2010-09-02 12:25:25 UTC+0000
0x000000000021f2978 csrss.exe 668 596 0x0d5f0000 2010-09-02 12:25:21 UTC+0000
0x0000000000221e278 iscsieexe.exe 1436 744 0x1090c000 2010-09-02 12:25:24 UTC+0000
0x0000000000223c020 vaelh.exe 952 1932 0x1ee5a000 2010-09-08 19:23:02 UTC+0000
0x00000000002282380 ImmunityDebugge 1932 1752 0x18f4d000 2010-09-08 19:23:02 UTC+0000
0x00000000002292da0 smss.exe 596 4 0x0adcc000 2010-09-02 12:25:18 UTC+0000
0x000000000022b96c0 SharedIntlApp.ex 1900 1752 0x11f33000 2010-09-02 12:25:25 UTC+0000
0x000000000022c09f8 winlogon.exe 692 596 0x0db75000 2010-09-02 12:25:22 UTC+0000
0x000000000022c8798 lsass.exe 756 692 0x0e121000 2010-09-02 12:25:22 UTC+0000
0x000000000022c8bf8 svchost.exe 992 744 0x0ed20000 2010-09-02 12:25:22 UTC+0000
0x00000000002311648 rundll32.exe 3768 1084 0x14502000 2010-09-09 19:56:33 UTC+0000
0x000000000023c8a00 System 4 0 0x00039000
```

3. List Active Processes Using pslist

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 pslist
```

command provided a detailed list of active processes, including their thread counts and handles.

```
(karim@kali) -~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 pslist

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtxlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.ma.apiohooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apiohooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0x823c8a00 System 4 0 57 671 — 0 0 2010-09-02 12:25:18 UTC+0000
0x82292da0 smss.exe 596 4 3 19 — 0 0 2010-09-02 12:25:21 UTC+0000
0x821f2978 csrss.exe 668 596 14 471 0 0 2010-09-02 12:25:21 UTC+0000
0x822c09f8 winlogon.exe 692 596 21 588 0 0 2010-09-02 12:25:22 UTC+0000
0x821a5da0 services.exe 744 692 15 279 0 0 2010-09-02 12:25:22 UTC+0000
0x822c8798 lsass.exe 756 692 24 437 0 0 2010-09-02 12:25:22 UTC+0000
0x82150b90 svchost.exe 912 744 20 202 0 0 2010-09-02 12:25:22 UTC+0000
0x822c8bf8 svchost.exe 992 744 10 277 0 0 2010-09-02 12:25:22 UTC+0000
0x82151da0 svchost.exe 1084 744 58 1327 0 0 2010-09-02 12:25:22 UTC+0000
0x821521b0 svchost.exe 1140 744 6 81 0 0 2010-09-02 12:25:22 UTC+0000
0x8214f488 svchost.exe 1192 744 13 175 0 0 2010-09-02 12:25:23 UTC+0000
0x8221e278 iscsieexe.exe 1436 744 6 78 0 0 2010-09-02 12:25:24 UTC+0000
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x823c8a00	System	4	0	57	671	—	0	0 2010-09-02 12:25:18 UTC+0000	
0x82292da0	smss.exe	596	4	3	19	—	0	0 2010-09-02 12:25:21 UTC+0000	
0x821f2978	csrss.exe	668	596	14	471	0	0	0 2010-09-02 12:25:21 UTC+0000	
0x822c09f8	winlogon.exe	692	596	21	588	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x821a5da0	services.exe	744	692	15	279	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x822c8798	lsass.exe	756	692	24	437	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x82150b90	svchost.exe	912	744	20	202	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x822c8bf8	svchost.exe	992	744	10	277	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x82151da0	svchost.exe	1084	744	58	1327	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x821521b0	svchost.exe	1140	744	6	81	0	0	0 2010-09-02 12:25:22 UTC+0000	
0x8214f488	svchost.exe	1192	744	13	175	0	0	0 2010-09-02 12:25:23 UTC+0000	
0x8221e278	iscsieexe.exe	1436	744	6	78	0	0	0 2010-09-02 12:25:24 UTC+0000	
0x82095500	spoolsv.exe	1616	744	13	140	0	0	0 2010-09-02 12:25:24 UTC+0000	
0x821b2020	explorer.exe	1752	1720	22	520	0	0	0 2010-09-02 12:25:25 UTC+0000	
0x822b96c0	SharedIntApp.exe	1900	1752	3	75	0	0	0 2010-09-02 12:25:25 UTC+0000	
0x820ee580	prl_cc.exe	1988	1752	14	133	0	0	0 2010-09-02 12:25:25 UTC+0000	
0x8212ada0	jusched.exe	1936	1752	1	43	0	0	0 2010-09-02 12:25:26 UTC+0000	
0x82129370	svchost.exe	364	744	4	88	0	0	0 2010-09-02 12:25:33 UTC+0000	
0x82089558	jqs.exe	472	744	5	146	0	0	0 2010-09-02 12:25:33 UTC+0000	
0x8208abf0	sqlservr.exe	488	744	25	306	0	0	0 2010-09-02 12:25:33 UTC+0000	
0x82077da0	coherence.exe	572	744	4	51	0	0	0 2010-09-02 12:25:36 UTC+0000	
0x82189530	prl_tools_servi	436	744	3	78	0	0	0 2010-09-02 12:25:36 UTC+0000	
0x82086798	prl_tools.exe	632	436	9	107	0	0	0 2010-09-02 12:25:36 UTC+0000	
0x821aa7e8	sqlwriter.exe	660	744	4	84	0	0	0 2010-09-02 12:25:36 UTC+0000	
0x8213ddaa	wscntrfy.exe	2180	1084	3	48	0	0	0 2010-09-02 12:25:41 UTC+0000	
0x81e8a368	alg.exe	2588	744	6	107	0	0	0 2010-09-02 12:25:44 UTC+0000	
0x8205ddaa	wuauctl.exe	940	1084	4	126	0	0	0 2010-09-02 12:26:40 UTC+0000	
0x82001ad0	ImmunityDebugge	2972	1752	2	87	0	0	0 2010-09-08 19:14:36 UTC+0000	
0x8207bda0	nifek_locked.ex	2204	2972	2	38	0	0	0 2010-09-08 19:14:36 UTC+0000	
0x82282380	ImmunityDebugge	1932	1752	2	86	0	0	0 2010-09-08 19:23:02 UTC+0000	
0x8223c020	vaelh.exe	952	1932	2	40	0	0	0 2010-09-08 19:23:02 UTC+0000	
0x81ff66d8	ImmunityDebugge	3788	1752	2	103	0	0	0 2010-09-08 22:39:40 UTC+0000	
0x8219e5c8	anaxu.exe	3508	3788	2	54	0	0	0 2010-09-08 22:39:40 UTC+0000	
0x81cab2f8	wuauctl.exe	3984	1084	8	325	0	0	0 2010-09-09 19:52:45 UTC+0000	
0x82066478	ImmunityDebugge	2404	1752	2	85	0	0	0 2010-09-09 19:56:19 UTC+0000	
0x81f4bb28	b98679df6defbb3	3772	2404	1	46	0	0	0 2010-09-09 19:56:19 UTC+0000	
0x81e87da0	iiah.exe	3276	3772	1	45	0	0	0 2010-09-09 19:56:32 UTC+0000	
0x82311648	rundll32.exe	3768	1084	1	53	0	0	0 2010-09-09 19:56:33 UTC+0000	

4. Scan Network Connections

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 connscan
```

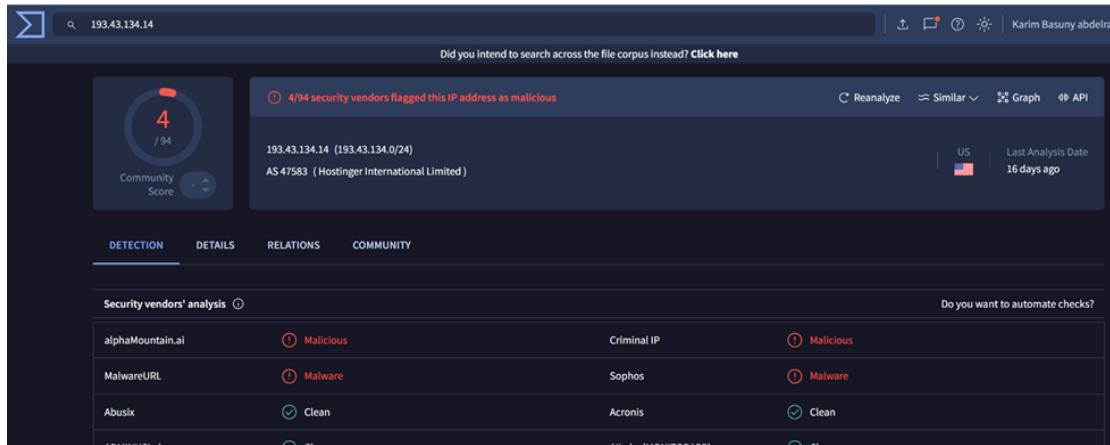
The command shows us the suspicious network activity it gives us 3 addresses with pid then we are going to take these Ips to virus total.

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 connscan

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicendiff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.environvars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

Offset(P) Local Address           Remote Address         Pid
_____
0x020f5410 10.211.55.5:1427      65.54.81.89:80        1084
0x02125008 10.211.55.5:1423      207.46.21.123:80     1084
0x022ace08 10.211.55.5:1432      193.43.134.14:80     1752
```

Now we are going to scan this IP : [193.43.134.14](#) and we will find that this is the malicious ip with pid [1752](#)



5. Process Tree

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 pstree
```

This command will display parent and child relationships of processes.

We will find that these processes connected to each other:

```
0x82066478 :ImmunityDebugge          pid: 2404 , ppid:  
1752  
  
0x81f4bb28 :b98679df6defbb3          pid: 3772 ,  
ppid: 2404  
  
0x81e87da0 :ihah.exe  
pid: 3276 , ppid: 3772
```

```
└$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 pstree  
Volatility Foundation Volatility Framework 2.6  
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.apihooks (NameError: name 'distorm3' is not defined)  
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.evtdlogs (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)  
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)  
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)  
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)  
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)  
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)  
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)  
Name          Pid  PPid  Thds  Hnds  Time  
-----  
0x821b2020:explorer.exe           1752  1720  22   520 2010-09-02 12:25:25 UTC+0000  
. 0x82282380:ImmunityDebugge      1932  1752  2    86 2010-09-08 19:23:02 UTC+0000  
.. 0x8223c020:vaelh.exe          952   1932  2    40 2010-09-08 19:23:02 UTC+0000  
. 0x8212ada0:jusched.exe        1936  1752  1    43 2010-09-02 12:25:26 UTC+0000  
. 0x82001ad0:ImmunityDebugge      2972  1752  2    87 2010-09-08 19:14:36 UTC+0000  
.. 0x8207bda0:nifek_locked.exe  2204  2972  2    38 2010-09-08 19:14:36 UTC+0000  
. 0x81fb6d8:ImmunityDebugge      3788  1752  2   103 2010-09-08 22:39:40 UTC+0000  
.. 0x8219e5c8:anaxu.exe          3508  3788  2    54 2010-09-08 22:39:40 UTC+0000  
. 0x820ee580:prl_cc.exe         1908  1752  14   133 2010-09-02 12:25:25 UTC+0000  
. 0x82066478:ImmunityDebugge      2404  1752  2    85 2010-09-09 19:56:19 UTC+0000  
.. 0x81f4bb28:b98679df6defbb3  3772  2404  1    46 2010-09-09 19:56:19 UTC+0000  
... 0x81e87da0:ihah.exe          3276  3772  1    45 2010-09-09 19:56:32 UTC+0000  
. 0x822b96c0:SharedIntApp.exe    1900  1752  3    75 2010-09-02 12:25:25 UTC+0000
```

Name	Pid	PPid	Thds	Hnds	Time
0x821b2020:explorer.exe	1752	1720	22	520	2010-09-02 12:25:25 UTC+0000
. 0x82282380:ImmunityDebugge	1932	1752	2	86	2010-09-08 19:23:02 UTC+0000
.. 0x8223c20:vaclh.exe	952	1932	2	40	2010-09-08 19:23:02 UTC+0000
. 0x8212ada0:jusched.exe	1936	1752	1	43	2010-09-02 12:25:26 UTC+0000
. 0x82001ad0:ImmunityDebugge	2972	1752	2	87	2010-09-08 19:14:36 UTC+0000
.. 0x8207bda0:nifek_locked.exe	2204	2972	2	38	2010-09-08 19:14:36 UTC+0000
. 0x81fb6d8:ImmunityDebugge	3788	1752	2	103	2010-09-08 22:39:40 UTC+0000
.. 0x8219e5c8:anaxu.exe	3508	3788	2	54	2010-09-08 22:39:40 UTC+0000
. 0x820ee580:prl_cc.exe	1908	1752	14	133	2010-09-02 12:25:25 UTC+0000
. 0x82066478:ImmunityDebugge	2404	1752	2	85	2010-09-09 19:56:19 UTC+0000
.. 0x81f4bb28:998679df6defbd3	3772	2404	1	46	2010-09-09 19:56:19 UTC+0000
... 0x81e87da0:ihah.exe	3276	3772	1	45	2010-09-09 19:56:32 UTC+0000
. 0x822b96c0:SharedIntApp.ex	1900	1752	3	75	2010-09-02 12:25:25 UTC+0000
0x823c8a00:system	4	0	57	671	1970-01-01 00:00:00 UTC+0000
. 0x82292da0:smss.exe	596	4	3	19	2010-09-02 12:25:18 UTC+0000
.. 0x821f2978:csrss.exe	668	596	14	471	2010-09-02 12:25:21 UTC+0000
.. 0x822c09f8:winlogon.exe	692	596	21	588	2010-09-02 12:25:22 UTC+0000
.. 0x822c8798:lsass.exe	756	692	24	437	2010-09-02 12:25:22 UTC+0000
... 0x821a5da0:services.exe	744	692	15	279	2010-09-02 12:25:22 UTC+0000
.... 0x82129370:svchost.exe	364	744	4	88	2010-09-02 12:25:33 UTC+0000
.... 0x821aa7e8:sqlwriter.exe	660	744	4	84	2010-09-02 12:25:36 UTC+0000
.... 0x8212e278:icscexe.exe	1436	744	6	78	2010-09-02 12:25:24 UTC+0000
.... 0x81e8a368:alg.exe	2588	744	6	107	2010-09-02 12:25:44 UTC+0000
.... 0x8214f488:svchost.exe	1192	744	13	175	2010-09-02 12:25:23 UTC+0000
.... 0x82189530:prl_tools_servi	436	744	3	78	2010-09-02 12:25:36 UTC+0000
.... 0x82086798:prl_tools.exe	632	436	9	107	2010-09-02 12:25:36 UTC+0000
.... 0x82151da0:svchost.exe	1084	744	58	1327	2010-09-02 12:25:22 UTC+0000
.... 0x8213d00:wsrndfy.exe	2180	1084	3	48	2010-09-02 12:25:41 UTC+0000
.... 0x8205dd0:wuaclt.exe	940	1084	4	126	2010-09-02 12:26:40 UTC+0000
.... 0x82311648:rundll32.exe	3768	1084	1	53	2010-09-09 19:56:33 UTC+0000
.... 0x81eab2f8:wuaclt.exe	3984	1084	8	325	2010-09-09 19:52:45 UTC+0000
.... 0x82095500:spoolsv.exe	1616	744	13	140	2010-09-02 12:25:24 UTC+0000
.... 0x82089558:jqs.exe	472	744	5	146	2010-09-02 12:25:33 UTC+0000
.... 0x822c8bf8:svchost.exe	992	744	10	277	2010-09-02 12:25:22 UTC+0000
.... 0x82150b90:svchost.exe	912	744	20	202	2010-09-02 12:25:22 UTC+0000
.... 0x8208abf0:sqlservr.exe	488	744	25	306	2010-09-02 12:25:33 UTC+0000
.... 0x8207da0:coherence.exe	572	744	4	51	2010-09-02 12:25:36 UTC+0000

6. Scanning Process

With focusing on processes with pid `1752`.

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 psscan | grep :
```

```
(karim@kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 psscan | grep 1752

Volatility Foundation Volatility Framework 2.6
0x00000000001ffbd8 ImmunityDebugge 3788 1752 0x03e57000 2010-09-08 22:39:40 UTC+0000
0x00000000002001ad0 ImmunityDebugge 2972 1752 0x0e002000 2010-09-08 19:14:36 UTC+0000
0x00000000002066478 ImmunityDebugge 2404 1752 0x0586f000 2010-09-09 19:56:19 UTC+0000
0x000000000020ee580 prl_cc.exe 1908 1752 0x11de1000 2010-09-02 12:25:25 UTC+0000
0x0000000000212ada0 jusched.exe 1936 1752 0x12010000 2010-09-02 12:25:26 UTC+0000
0x000000000021b2020 explorer.exe 1752 1720 0x10e31000 2010-09-02 12:25:25 UTC+0000
0x00000000002282380 ImmunityDebugge 1932 1752 0x18f4d000 2010-09-08 19:23:02 UTC+0000
0x000000000022b96c0 SharedIntApp.ex 1900 1752 0x11f33000 2010-09-02 12:25:25 UTC+0000
```

7. Dump Malicious Processes

First: making directory for dumping (`mkdir procdump`).

Second:

we are going to dump the processes

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p
2404 -D procdump/
```

This dumps the process with pid -p 2404 which is 0x82066478 :ImmunityDebugge .

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ mkdir procdump

(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p 2404 -D procdump/

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

Process(V) ImageBase Name Result
----- -----
0x82066478 0x00400000 ImmunityDebugge OK: executable.2404.exe
```

Then we are going to dump process with pid 3772 which is 0x81f4bb28 :b98679df6defbb3 .

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p 3772 -D procdump/
```

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p 3772 -D procdump/

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

Process(V) ImageBase Name Result
----- -----
0x81f4bb28 0x00400000 b98679df6defbb3 OK: executable.3772.exe
```

Now and last process dump is process with pid 3276

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p 3276 -D procdump/
```

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p 3276 -D procdump/

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Process(V) ImageBase Name Result
----- -----
0x81e87da0 0x00400000 ihah.exe OK: executable.3276.exe
```

8. Getting the hash of dumped and check them on virus total.

```
sha256sum procdump/executable.2404.exe
sha256sum procdump/executable.3772.exe
sha256sum procdump/executable.3276.exe
```

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ sha256sum procdump/executable.2404.exe
66b6e5898e8ceed70e3e09c1c399cb51c5fbe4029a8aa5323de6bb0d506cc procdump/executable.2404.exe

(karim㉿kali)-[~/Downloads/volatility-master]
$ sha256sum procdump/executable.3772.exe
9374b90433d9e2369258413997f3b84d2db0c51b8fd0d7e050458e780a141407 procdump/executable.3772.exe

(karim㉿kali)-[~/Downloads/volatility-master]
$ sha256sum procdump/executable.3276.exe
c4b88f8e160f9eb145bb9e12e5122fa539a83b772e93929efb8846c8e1171eed procdump/executable.3276.exe
```

First process of executable. 2404.exe

Second: checking the process executable.3772.exe we will find its related to zbot

Checking last hash of executable.3276.exe we will find that its also related to zbot.

Security vendors' analysis				Do you want to automate checks?
Ad-Aware	Gen:Variant.Symmi.12682	AegisLab	Troj.W32.Generic!c	
AhnLab-V3	Spyware/Win32.Zbot.R1109	ALYac	Gen:Variant.Symmi.12682	
AntiAVL	Trojan/Win32.AGeneric	Arcabit	Trojan.Symmi.D318A	
Avast	Sf:Crypt-BT [Trj]	AVG	Sf:Crypt-BT [Trj]	
Avira (no cloud)	TR/Spy.Gen	AVware	Trojan.Win32.Generic!BT	
Baidu	Win32.Trojan.WisdomEyes.16070401.950...	BitDefender	Gen:Variant.Symmi.12682	
ClamAV	Win.Malware.QBot-1530	Comodo	UnclassifiedMalware	
CrowdStrike Falcon	Malicious_confidence_100% (D)	Cylance	Unsafe	
Cyren	W32/Zbot.BR.gen Eldorado	DrWeb	BackDoor.Qbot.234	
Emsisoft	Gen:Variant.Symmi.12682 (B)	Endgame	Malicious (high Confidence)	
eScan	Gen:Variant.Symmi.12682	ESET-NOD32	A Variant Of Win32/Spy.Zbot.YW	
F-Prot	W32/Zbot.BR.gen Eldorado	Fortinet	W32/Zbot.DS1tr.spy	
GData	Gen:Variant.Symmi.12682	Ikarus	PWS.Win32	
Jiangmin	TrojanSpy.Zbot.adva	K7Antivirus	Riskware (0015e4f01)	
K7GW	Riskware (0015e4f01)	Kaspersky	HEUR:Trojan.Win32.Generic	
MAX	Malware (ai Score=85)	McAfee-GW-Edition	BehavesLike.Win32.Zbot.ch	
Microsoft	PWS:Win32/Zbot	NANO-Antivirus	Trojan.Win32.Qbot.czwjwo	
Palo Alto Networks	Generic.ml	Panda	Trj/Genetic.gen	
Qihoo-360	Win32/Trojan.Spy.5d9	Rising	Stealer.Zbot!I.648A (classic)	

9. Identifying Potential Malware

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 1752
```

This command: scan the memory of the process for malicious activity, such as code injections or memory regions with executable permissions. Contains finding a PE header in a process's memory (MZ) can indicate a loaded executable or a malicious injection.

```

[karim@kali:[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 1752

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug : For best results please install distorm3
Process: explorer.exe Pid: 1752 Address: 0x2aa0000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02aa0000 b8 35 00 00 00 e9 a9 d1 e6 79 68 6c 02 00 e9 .5.....yhl...
0x02aa0010 b4 63 e7 79 8b ff 55 8b ec e9 7c 11 d7 79 8b ff .c.y..U...|..y..
0x02aa0020 55 8b ec e9 01 32 77 74 8b ff 55 8b ec e9 7c 60 U....2wt..U...|
0x02aa0030 72 74 8b ff 55 8b ec e9 ca e9 72 74 8b ff 55 8b rt..U.....rt..U.

Process: explorer.exe Pid: 1752 Address: 0x3080000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x03080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x03080010 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x03080020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....0.....
0x03080030 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 .....
```

10. the same malfind but for pid 2404

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 2404
```

```

└─$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 2404

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)

WARNING : volatility.debug : For best results please install distorm3
Process: ImmunityDebugge Pid: 2404 Address: 0x2340000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02340000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x02340010 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00  ..@.....
0x02340020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x02340030 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00  .....

Process: ImmunityDebugge Pid: 2404 Address: 0x32d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x032d0000 b8 35 00 00 00 e9 a9 d1 63 79 68 6c 02 00 00 e9  .5.....cyhl...
0x032d0010 b4 63 64 79 8b ff 55 8b ec e9 7c 11 54 79 8b ff  .cdy..U...|.Ty..
0x032d0020 55 8b ec e9 01 32 f4 73 8b ff 55 8b ec e9 7c 60  U...2.s..U...|`.
0x032d0030 ef 73 8b ff 55 8b ec e9 ca e9 ef 73 8b ff 55 8b  .s..U.....s..U.
```

11. The same malfind but for pid 3772

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3772
```

```

[karim@kali:~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3772

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug : For best results please install distorm3
Process: b98679df6defbb3 Pid: 3772 Address: 0x380000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 36, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00380000  90 90 90 90 5a 89 e5 83 ec 14 8b 5d 00 83 eb 05  ....Z.....]...
0x00380010  be 0b 88 01 00 29 f3 89 1c 24 b9 84 44 02 00 01  ....) ...$..D ...
0x00380020  d9 8b 09 89 4c 24 0c b9 74 43 02 00 01 d9 8b 09  ....L$..tC.....
0x00380030  89 4c 24 10 57 be 00 10 00 00 01 de b9 0b 78 01  .L$.W.....x.

Process: b98679df6defbb3 Pid: 3772 Address: 0x9a0000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x009a0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x009a0010  b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00  ....@.....
0x009a0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x009a0030  00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00  .....

Process: b98679df6defbb3 Pid: 3772 Address: 0xa30000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00a30000  b8 35 00 00 00 e9 a9 d1 ed 7b 68 6c 02 00 00 e9  .5.....{hl...
0x00a30010  b4 63 ee 7b 8b ff 55 8b ec e9 7c 11 de 7b 8b ff  .c.{..U...|..{..
0x00a30020  55 8b ec e9 01 32 7e 76 8b ff 55 8b ec e9 7c 60  U....2~v..U...|`.
0x00a30030  79 76 8b ff 55 8b ec e9 ca e9 79 76 8b ff 55 8b  yv..U.....yv..U.

```

12. The same also but for pid 3772

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3772
```

```

[karim@kali:~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3772

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcsan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.environ (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug : For best results please install distorm3
Process: b98679df6defbb3 Pid: 3772 Address: 0x380000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 36, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00380000  90 90 90 90 5a 89 e5 83 ec 14 8b 5d 00 83 eb 05  ....Z.....].
0x00380010  be 0b 88 01 00 29 f3 89 1c 24 b9 84 44 02 00 01  ....) ...$..D...
0x00380020  d9 8b 09 89 4c 24 0c b9 74 43 02 00 01 d9 8b 09  ....L$..tC.....
0x00380030  89 4c 24 10 57 be 00 10 00 00 01 de b9 0b 78 01  .L$.W.....x.

Process: b98679df6defbb3 Pid: 3772 Address: 0x9a0000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x009a0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x009a0010  b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00  .....@...
0x009a0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..... .
0x009a0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

```

Process: b98679df6defbb3 Pid: 3772 Address: 0xa30000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00a30000  b8 35 00 00 00 e9 a9 d1 ed 7b 68 6c 02 00 00 e9  .5.....{hl...
0x00a30010  b4 63 ee 7b 8b ff 55 8b ec e9 7c 11 de 7b 8b ff  .c.{...u...|..{..
0x00a30020  55 8b ec e9 01 32 7e 76 8b ff 55 8b ec e9 7c 60  U....2~v..U...|`.
0x00a30030  79 76 8b ff 55 8b ec e9 ca e9 79 76 8b ff 55 8b  yv ..U.....yv..U.
```

13. The same also but for pid 3772

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3276
```

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3276
[...]
Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug : For best results please install distorm3
Process: iahh.exe Pid: 3276 Address: 0x380000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 37, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00380000 90 90 90 90 5a b9 e5 b3 ec 14 8b 5d 00 83 eb 05  ....Z.....]...
0x00380010 be 94 c2 00 00 29 f3 b9 1c 24 b9 98 41 02 00 01  ....) ... $..A...
0x00380020 d9 8b 09 89 4c 24 0c b9 30 46 02 00 01 d9 8b 09  ....L$..@F.....
0x00380030 89 4c 24 10 57 be 00 10 00 00 01 de b9 94 b2 00  .L$.W.....
[...]
Process: iahh.exe Pid: 3276 Address: 0x3f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x003f0000 b8 35 00 00 00 e9 a9 d1 51 7c 68 6c 02 00 00 e9  .5.....Q|h...
0x003f0010 b4 63 52 7c b8 ff 55 8b ec e9 7c 11 42 7c 8b ff  .cR| ..U ... |B| ..
0x003f0020 55 8b ec e9 01 32 e2 76 8b ff 55 8b ec e9 7c 60  U....2.v..U ... |`...
0x003f0030 dd 76 8b ff 55 8b ec e9 ca e9 dd 76 8b ff 55 8b  .v..U.....v..U.
[...]
```

```
Process: iahh.exe Pid: 3276 Address: 0x9a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6
[...]
0x009a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x009a0010 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00  ....@....
0x009a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x009a0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00  .....
[...]
```

14. DLLIST scanning for processes

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 2404
```

```
(karim㉿kali)-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 2404
```

```

*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*****
ImmunityDebugger pid: 2404
Command line : "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C:\Documents and Settings\Administrator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe"
Service Pack 3

Base      Size  LoadCount Path
0x00400000 0x1c5000 0xfffff C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe
0x7c900000 0xb2000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77d00000 0x9b000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x92000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x77c00000 0x8000 0xfffff C:\WINDOWS\system32\VERSION.dll
0x71a00000 0x9000 0xfffff C:\WINDOWS\system32\WSOCK32.dll
0x71b00000 0x17000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x77f10000 0x58000 0xfffff C:\WINDOWS\system32\WSOCKHELP.dll
0x71a00000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x5d000000 0x70000 0xfffff C:\WINDOWS\system32\COMCTL32.dll
0x77f10000 0x49000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x76410000 0x91000 0xfffff C:\WINDOWS\system32\USER32.dll
0x76300000 0x49000 0xfffff C:\WINDOWS\system32\COMDLG32.dll
0x77c90000 0x817000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x77f50000 0x76000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x77e40000 0x13d000 0xfffff C:\WINDOWS\system32\OLE32.dll
0x77120000 0x8b000 0xfffff C:\WINDOWS\system32\PYTHON25.dll
0x1e000000 0x206000 0xfffff C:\WINDOWS\system32\comctl32.dll
0x7c340000 0x56000 0xfffff C:\WINDOWS\system32\MSVCR71.dll
0x773d0000 0x103000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5ad70000 0x38000 0x2 C:\WINDOWS\System32\RPC.dll
0x70b10000 0xb000 0x4 C:\WINDOWS\System32\RPCRT4.dll
0x77e70000 0x30000 0x1 C:\WINDOWS\System32\IMAGEHLP.dll
0x59a10000 0x13000 0x1 C:\WINDOWS\System32\OBDAHELP.dll
0x77b00000 0x22000 0x1 C:\WINDOWS\System32\Apphelp.dll
0x02730000 0x45000 0x1 C:\Program Files\Immunity Inc\Immunity Debugger\Bookmark.dll
0x028e0000 0x52000 0x1 C:\Program Files\Immunity Inc\Immunity Debugger\Cmdline.dll
0x02dc0000 0x91142 0x1 C:\Program Files\Immunity Inc\Immunity Debugger\ollyDump.dll
0x10000000 0x3a0c9 0x1 C:\Program Files\Immunity Inc\Immunity Debugger\PEDumper.dll
0x73000000 0x26000 0x1 C:\WINDOWS\System32\WINSPPOOL.DRV
0x71a50000 0x3f000 0x4 C:\WINDOWS\System32\mswsock.dll
0x662b0000 0x58000 0x1 C:\WINDOWS\System32\hnetcfg.dll
0x71a90000 0x8000 0x1 C:\WINDOWS\System32\wshttp.dll
0x76f20000 0x27000 0x2 C:\WINDOWS\System32\DNSAPI.dll
0x76fb0000 0x8000 0x1 C:\WINDOWS\System32\wininet.dll
0x77f10000 0x2c000 0x1 C:\WINDOWS\System32\RPCRT4.dll
0x77f50000 0x10000 0x1 C:\WINDOWS\System32\rsasdh.dll
0x77a80000 0x95000 0x2 C:\WINDOWS\System32\CRYPT32.dll
0x77b20000 0x12000 0x2 C:\WINDOWS\System32\MSASN1.dll
0x771b0000 0x3aa000 0x1 C:\WINDOWS\System32\WININET.dll
0x5b860000 0x55000 0x1 C:\WINDOWS\System32\NETAPI32.dll

```

The same dlllist but for pid 3772

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 3772
```

```

[karim@kali]-[~/Downloads/volatility-master]
$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 3772

Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)

***** 
b98679df6defbb3 pid: 3772
Command line : "C:\Documents and Settings\Administrator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe"
Service Pack 3

Base      Size  LoadCount Path
0x00400000 0x34000 0xfffff C:\Documents and Settings\Administrator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe
0x7c900000 0xb2000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0x6f000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77d00000 0x9b000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x76000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x77f6f0000 0x76000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x77f1a0000 0x49000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x76a10000 0x91000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c10000 0x58000 0xfffff C:\WINDOWS\system32\msvcr7.dll
0x77a4e0000 0x13d000 0xfffff C:\WINDOWS\system32\ole32.dll
0x77c9c0000 0x817000 0x2 C:\WINDOWS\System32\SHLWAPI.dll
0x773d0000 0x103000 0x3 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x71ab0000 0x17000 0x2 C:\WINDOWS\System32\WS2_32.dll
0x71aa0000 0x8000 0x2 C:\WINDOWS\System32\WS2HELP.dll
0x77a80000 0x95000 0x4 C:\WINDOWS\System32\CRYPT32.dll
0x77b20000 0x12000 0x4 C:\WINDOWS\System32\MSASN1.dll
0x771b0000 0x3aa000 0x2 C:\WINDOWS\System32\WININET.dll
0x77120000 0xb8000 0x4 C:\WINDOWS\System32\OLEAUT32.dll
0x5b860000 0x55000 0x2 C:\WINDOWS\System32\NETAPI32.dll
0x77b40000 0x22000 0x1 C:\WINDOWS\System32\Apphelp.dll

```

The same dlllist but for pid 3276 :

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 3276
```

```

[karim@kali]~/Downloads/volatility-master]
└$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 3276

Volatility Foundation Volatility Framework 2.6
** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.lsacache (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
** Failed to import volatility.plugins.malware.svscan (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*****
ihah.exe pid: 3276
Command line : "C:\Documents and Settings\Administrator\Application Data\Obyt\ihah.exe"
Service Pack 3

Base          Size    LoadCount Path
=====
0x00400000  0x34000   0xffff C:\Documents and Settings\Administrator\Application Data\Obyt\ihah.exe
0x7c900000  0xb2000   0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000  0xf6000   0xffff C:\WINDOWS\system32\kernel32.dll
0x7e100000  0x91000   0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000  0x49000   0xffff C:\WINDOWS\system32\GDI32.dll
0x77f60000  0x76000   0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x77dd0000  0x9b000   0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000  0x92000   0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000  0x11000   0xffff C:\WINDOWS\system32\Secur32.dll
0x77c10000  0x58000   0xffff C:\WINDOWS\system32\msvcrt.dll
0x77ae0000  0x13d000  0xffff C:\WINDOWS\system32\ole32.dll
0x7c9c0000  0x817000   0x2 C:\WINDOWS\system32\SHELL32.dll
0x773d0000  0x103000  0x3 C:\WINDOWS\Win32\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-wm_35d4ce83\comctl32.dll
0x71ab0000  0x17000   0x2 C:\WINDOWS\system32\WS2_32.dll

```

The `dlllist` lists the dynamic link libraries (DLLs) loaded into a process's memory. It provides details such as the base address, size, load count, and file path of each loaded DLL. This information helps identify potentially suspicious or malicious DLLs running within a process. It is commonly used in memory forensics to trace the behavior and dependencies of processes. By analyzing the DLLs, investigators can uncover anomalies or malware running in memory.