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

▼ 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

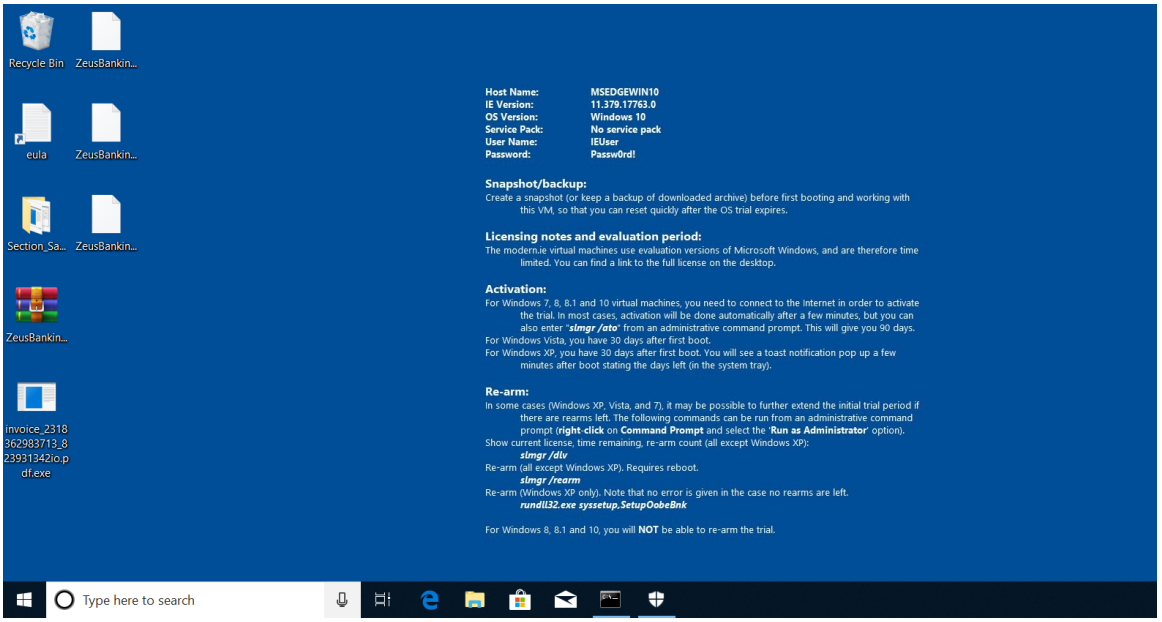
```
sudo apt install -y suricata
```

2. Check Version

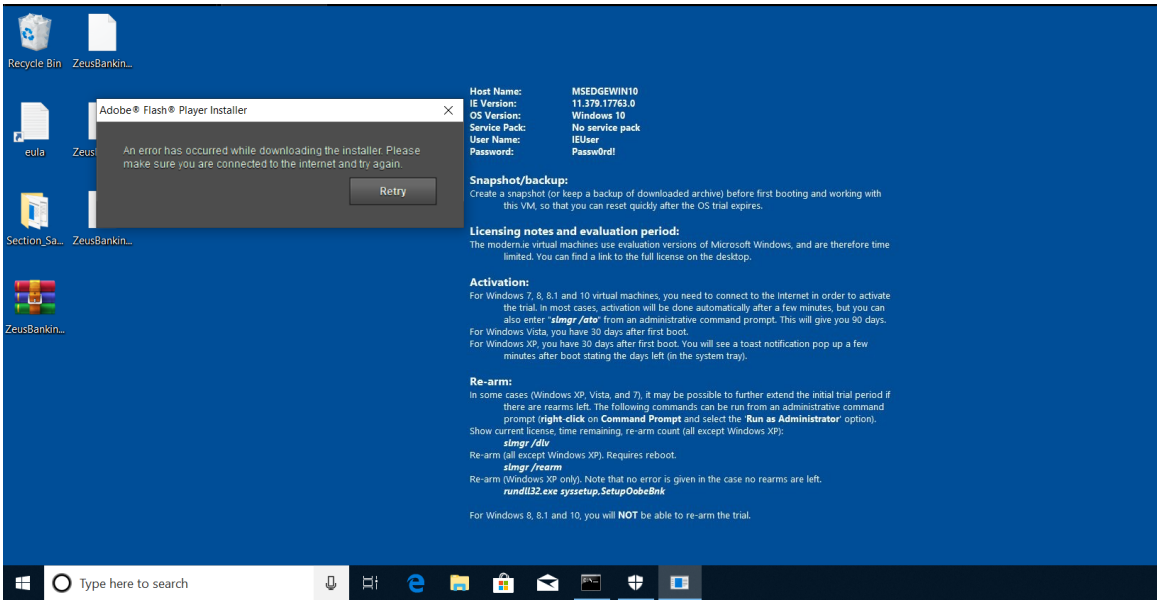
```
suricata -v
```

▼ Simulating Malware Execution

1. We Extracting The Zip file first

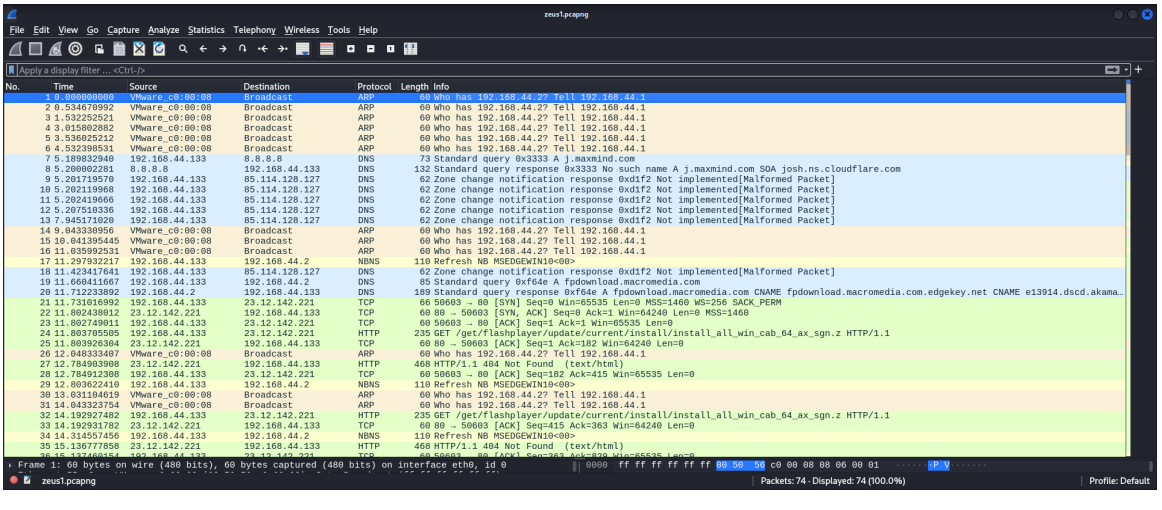


2. We Executing The Program

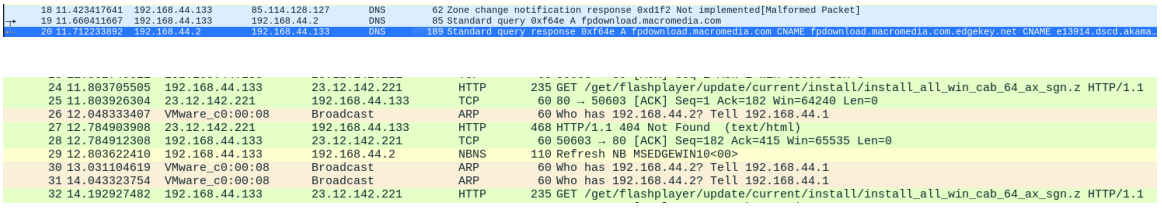


▼ Wireshark

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	11.423417641	192.168.44.133	85.114.128.127	DNS	62 Zone change notification response 0xd1f2 Not implemented[Malformed Packet]
19	11.660411667	192.168.44.133	192.168.44.2	DNS	85 Standard query 0xf64e A fpdownload.macromedia.com
20	11.712233892	192.168.44.2	192.168.44.133	DNS	189 Standard query response 0xf64e A fpdownload.macromedia.com CNAME fpdownload.macromedia.com.edgekey.net CNAME e13914.dscd.akama…

24	11.803705505	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	11.803926304	23.12.142.221	192.168.44.133	TCP	60 80 → 50603 [ACK] Seq=1 Ack=182 Win=64240 Len=0
26	12.048333407	VMware_c0:00:08	Broadcast	ARP	60 Who has 192.168.44.2? Tell 192.168.44.1
27	12.784903908	23.12.142.221	192.168.44.133	HTTP	468 HTTP/1.1 404 Not Found (text/html)
28	12.784912308	192.168.44.133	23.12.142.221	TCP	60 50603 → 80 [ACK] Seq=182 Ack=415 Win=65535 Len=0
29	12.803622410	192.168.44.133	192.168.44.2	NBNS	110 Refresh NB MSEDGEWIN10<00>
30	13.031104619	VMware_c0:00:08	Broadcast	ARP	60 Who has 192.168.44.2? Tell 192.168.44.1
31	14.043323754	VMware_c0:00:08	Broadcast	ARP	60 Who has 192.168.44.2? Tell 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.

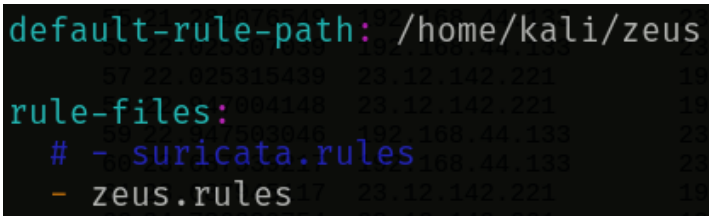
```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Fake Flash Player
http.uri;
content:"/get/flashplayer/update/current/install/install_all_win_cab_6
; http.method; content:"GET"; nocase; sid:1000001; rev:1;)
```

```
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,
```

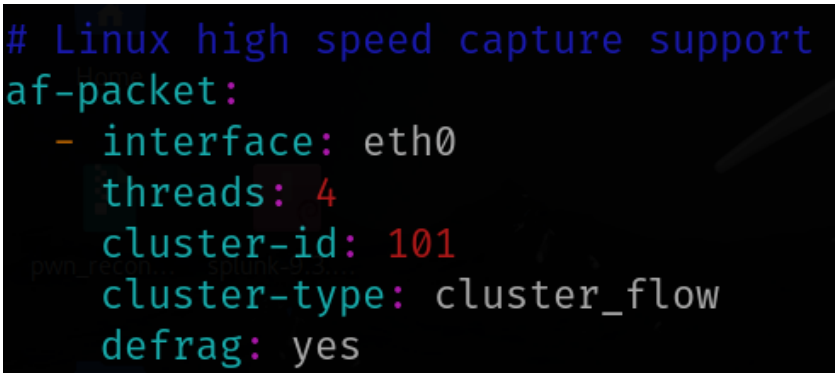
3.2. Configure "`/etc/suricata/suricata.yaml`".

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

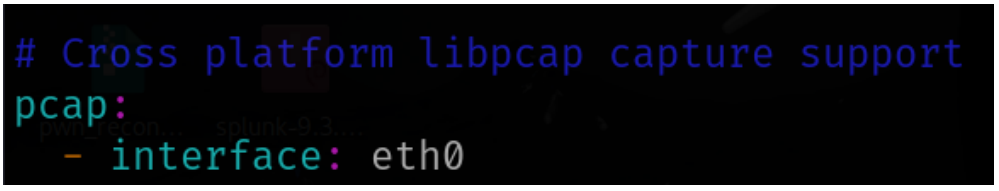
1. Configure `rule-path`: `/home/kali/zeus`
2. Configure `rule-files`: `zeus.rules`



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



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



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

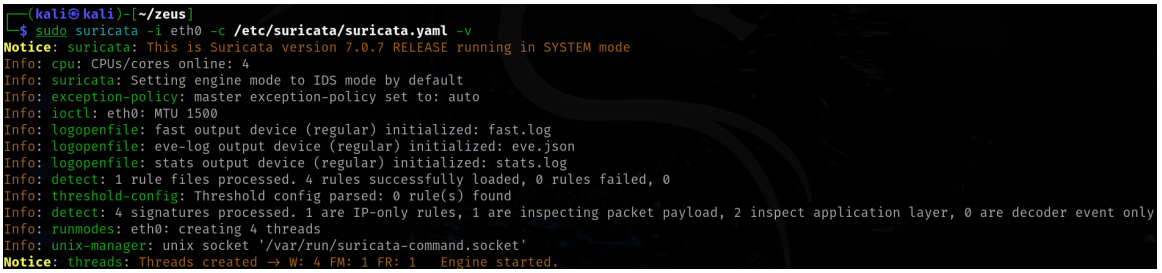
```
sudo systemctl start suricata
```

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
```



---

4. Logging

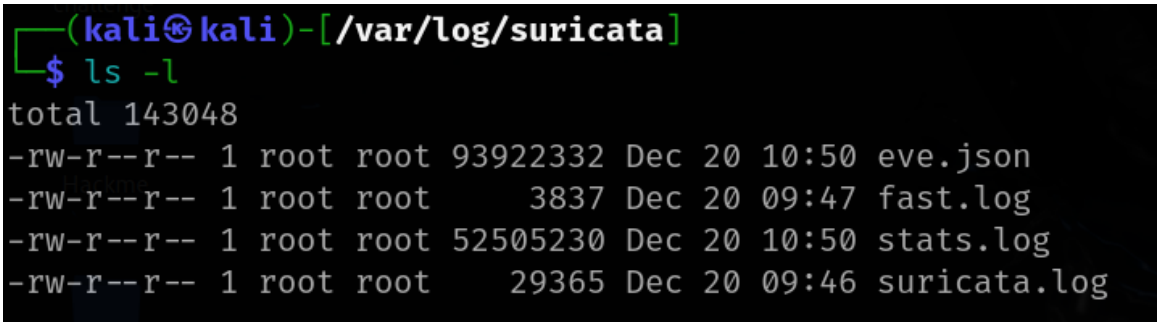
> After Executing The `Invoice` program on victim machine, we found logs in `/var/log/suricata`

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

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

4.2. We list all files in this directory

```
ls -l
```



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 'select(.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  [**] [1:100004:1] 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
```

`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: ioctl: 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 applicatio
n 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.

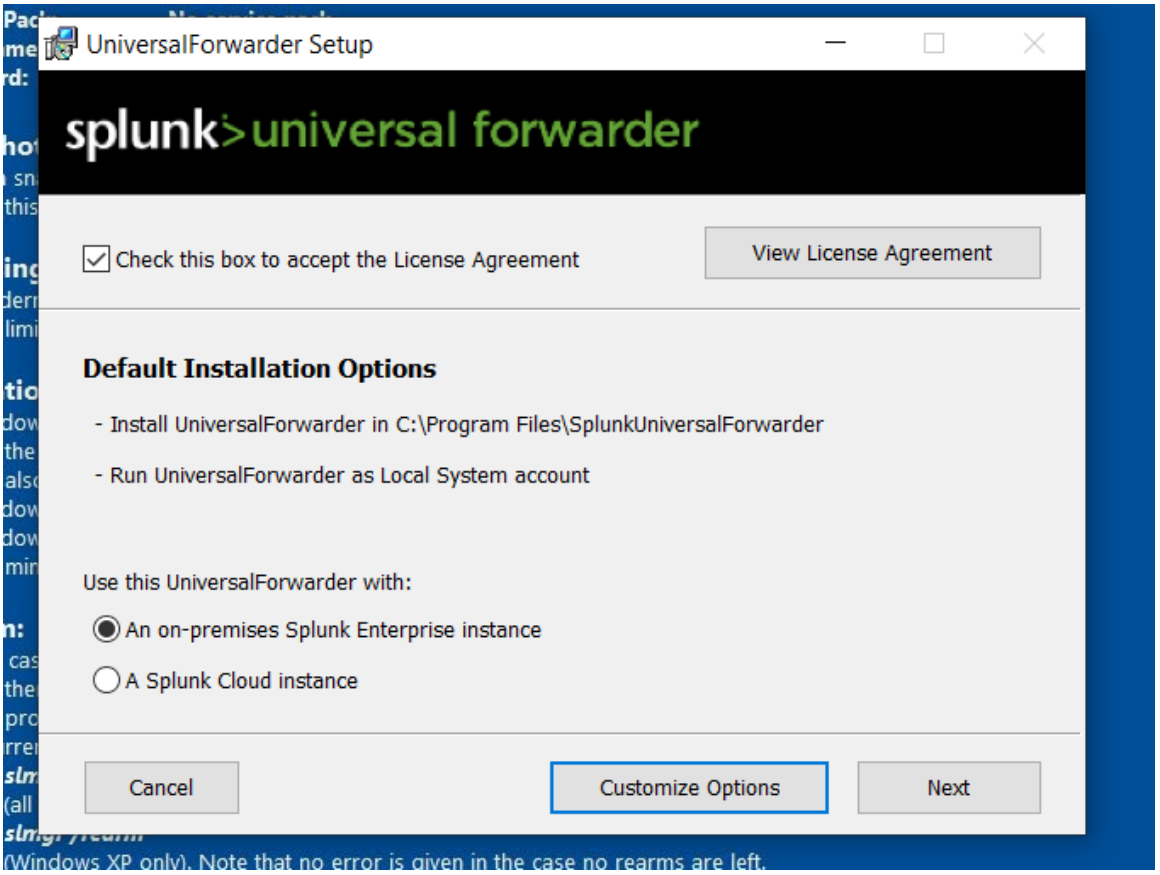
1. Download And Setup

1.1. Download Link

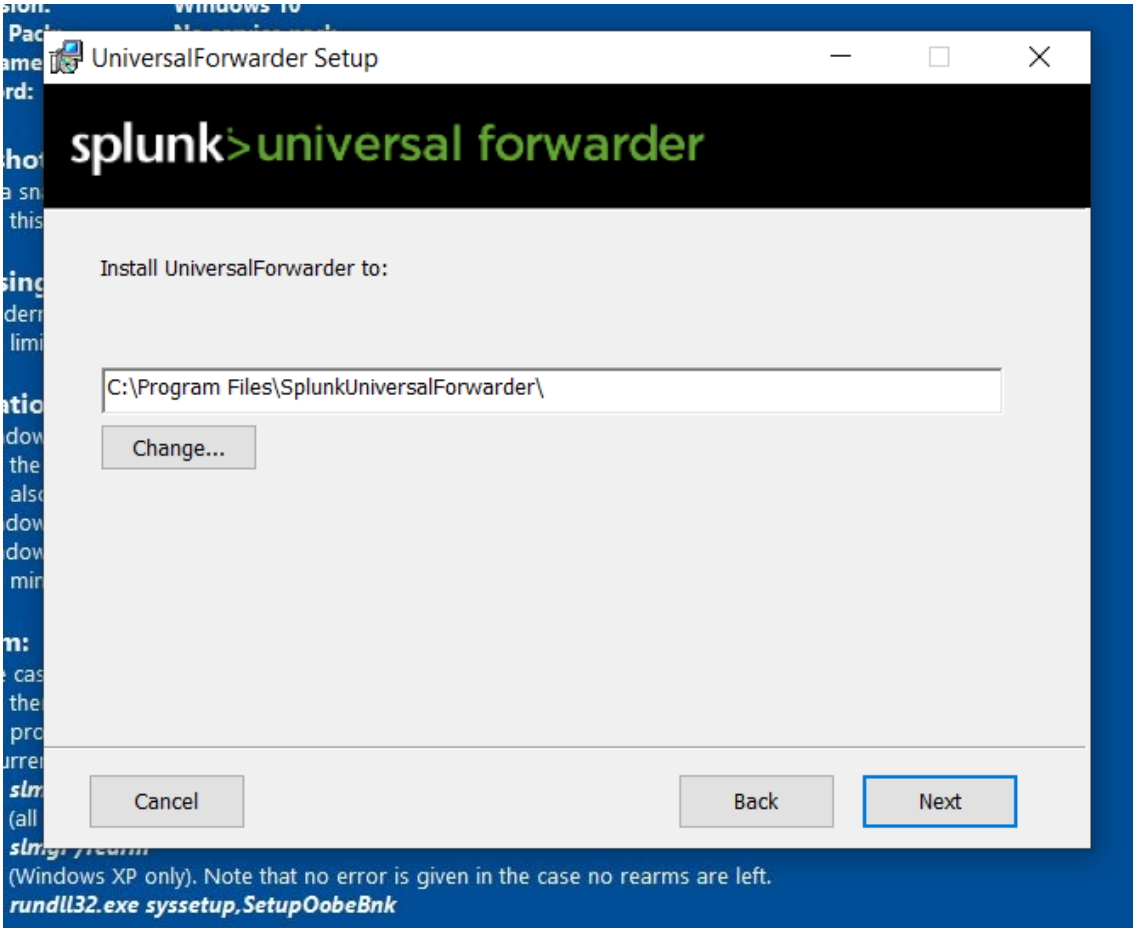
https://www.splunk.com/en_us/download/universal-forwarder.html

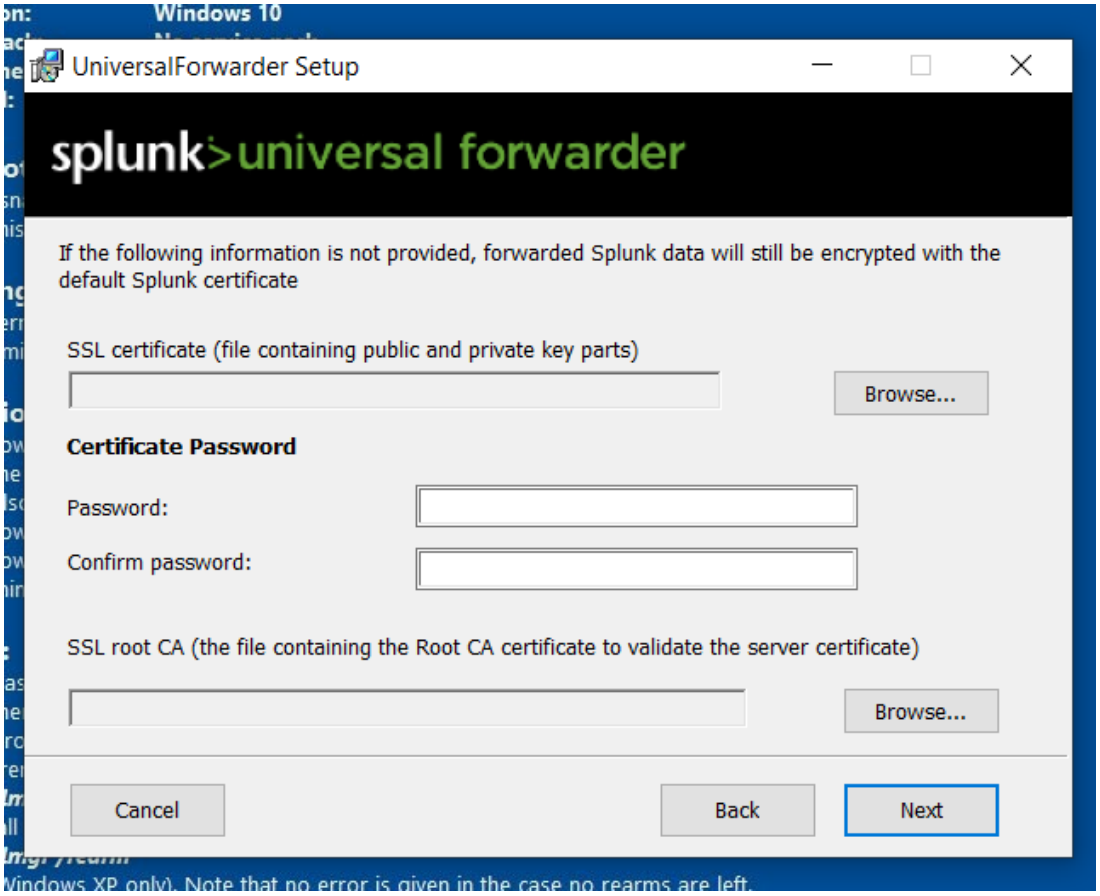
1.2. Setup

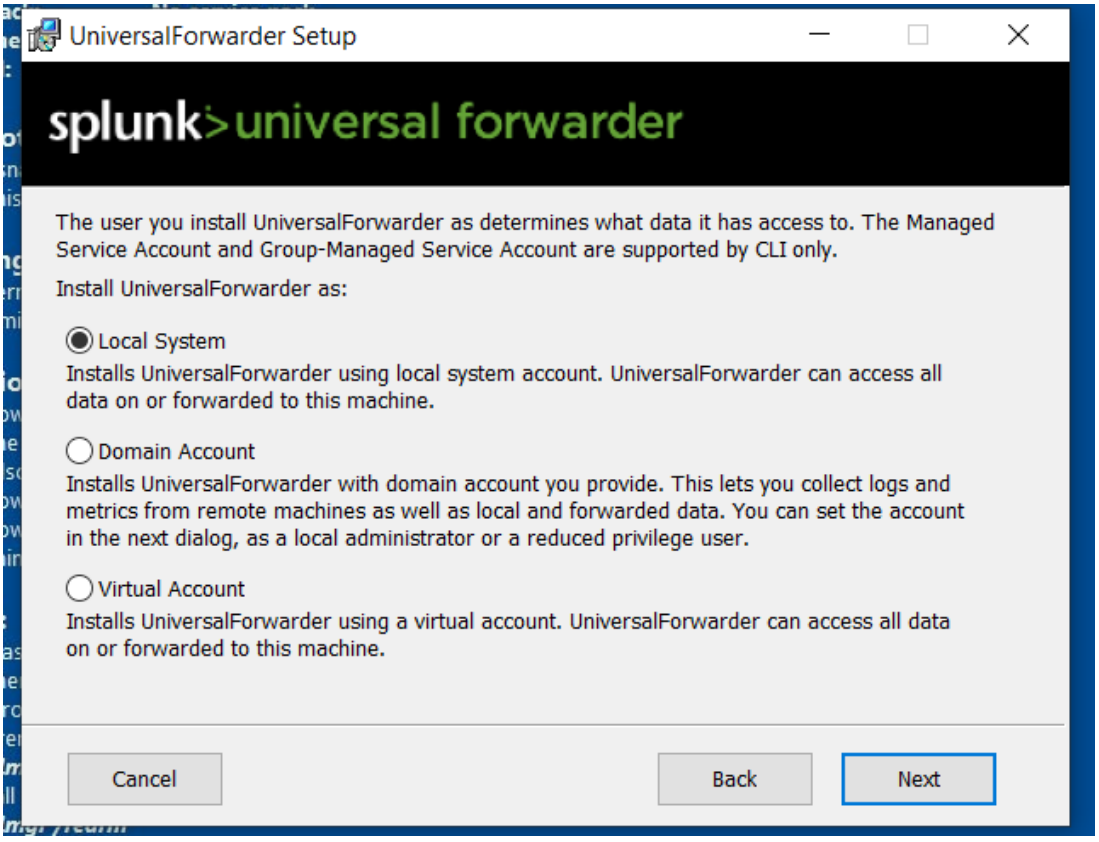
> First We execute the msi program



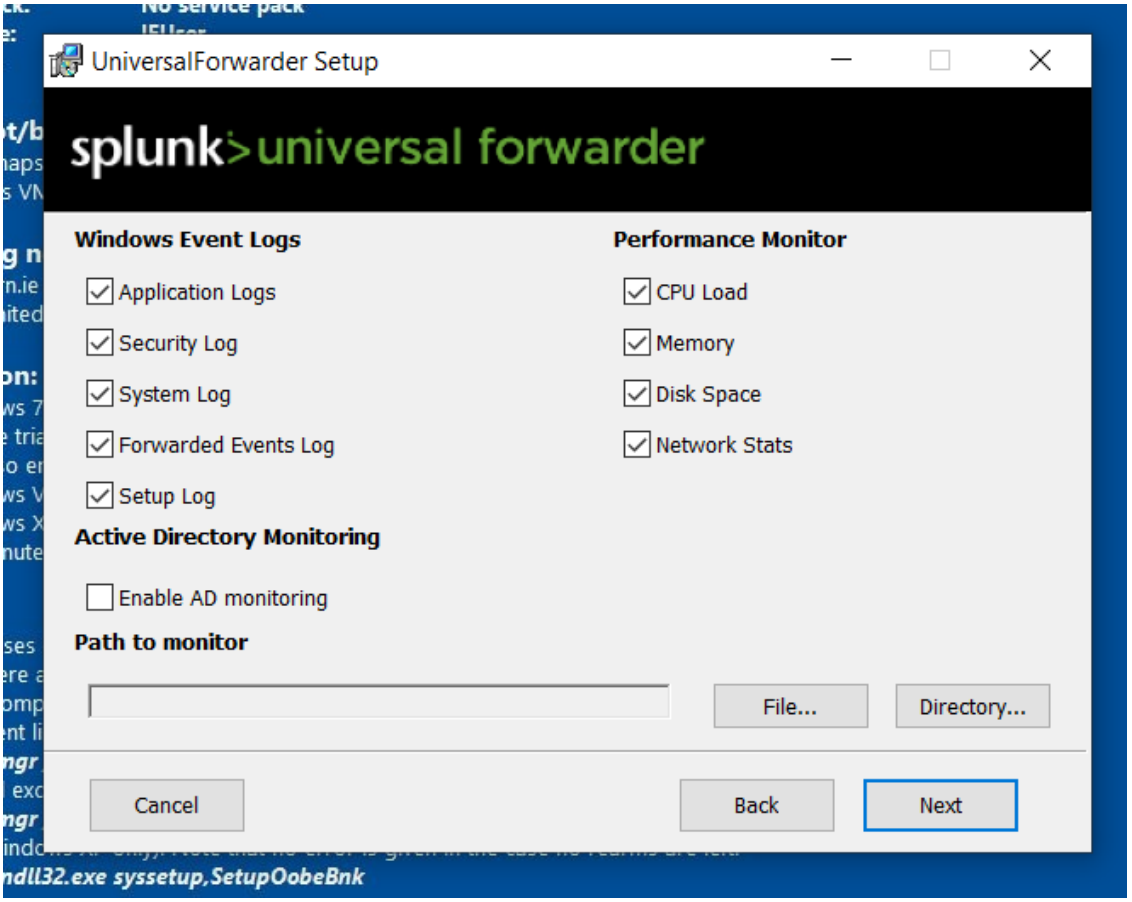
> Choose Customize options


UniversalForwarder Setup
splunk>universal forwarder
Install UniversalForwarder to:
C:\Program Files\SplunkUniversalForwarder\
Change...
Cancel
Back
Next
(Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

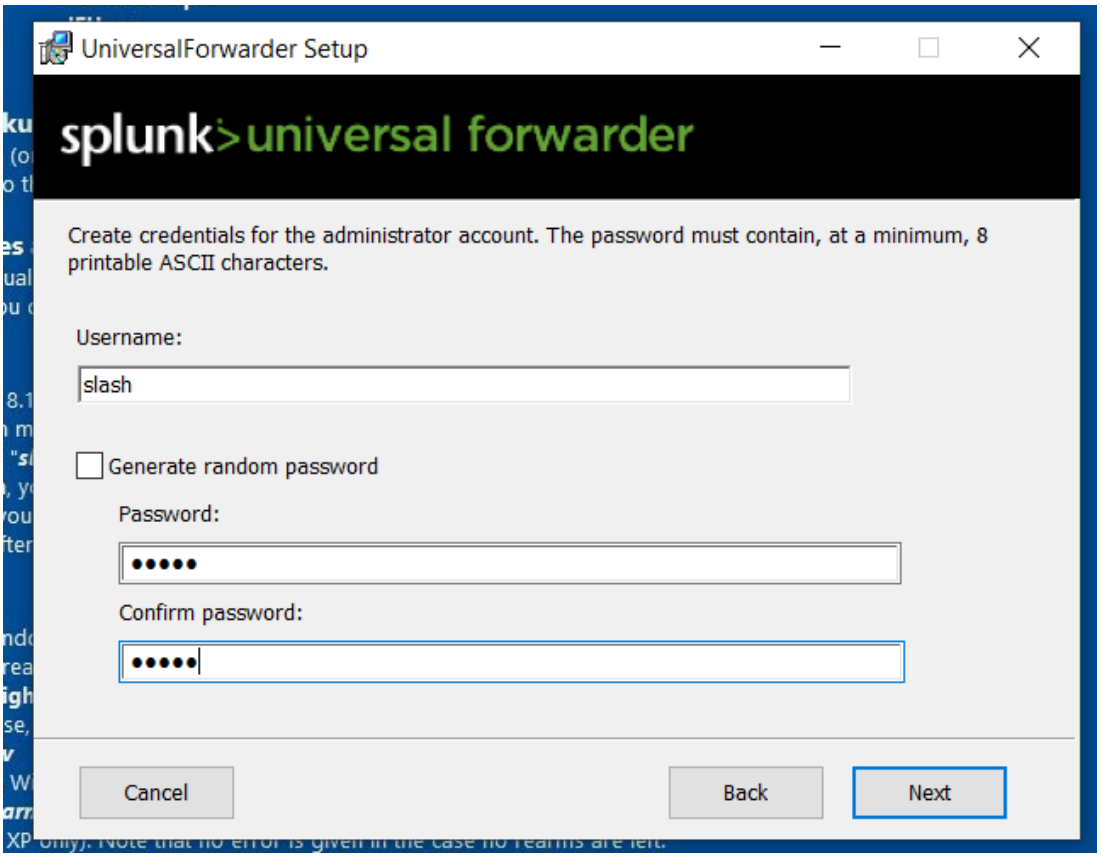

Windows 10
UniversalForwarder Setup
splunk>universal forwarder
If the following information is not provided, forwarded Splunk data will still be encrypted with the default Splunk certificate
SSL certificate (file containing public and private key parts)
Browse...
Certificate Password
Password:
Confirm password:
SSL root CA (the file containing the Root CA certificate to validate the server certificate)
Browse...
Cancel
Back
Next



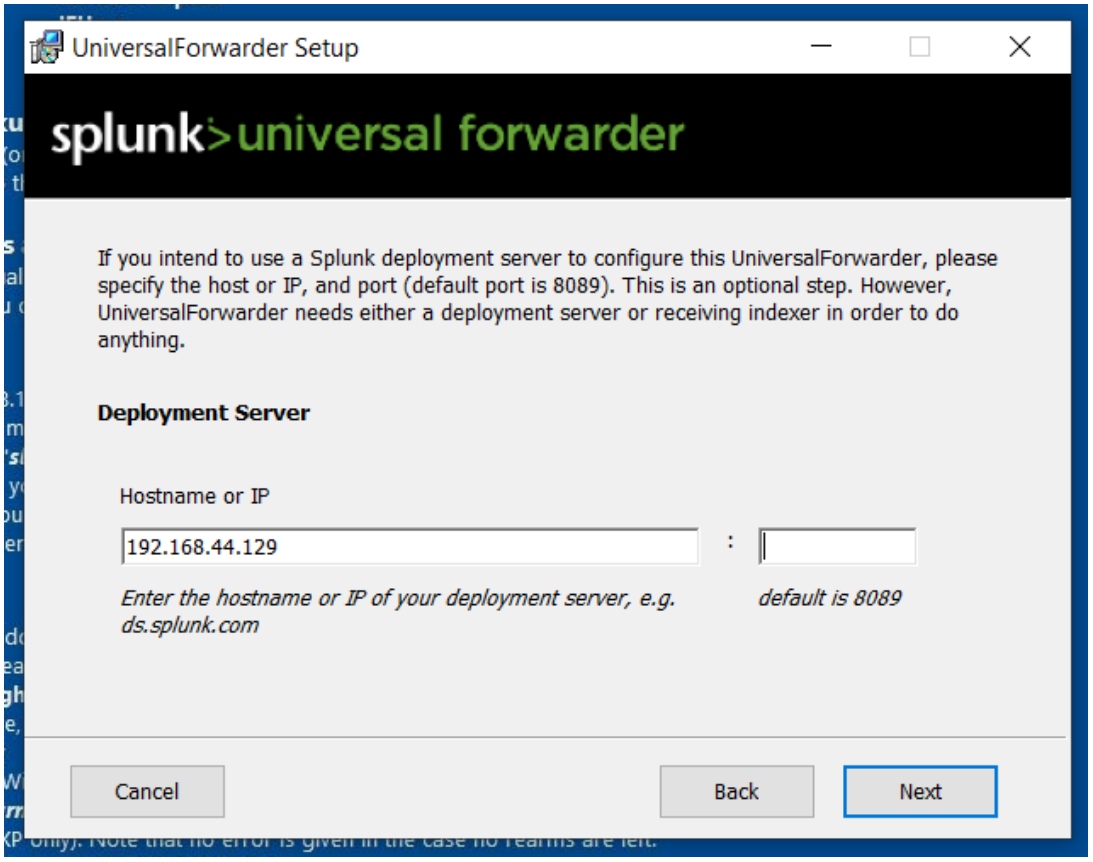
> Choose Local System



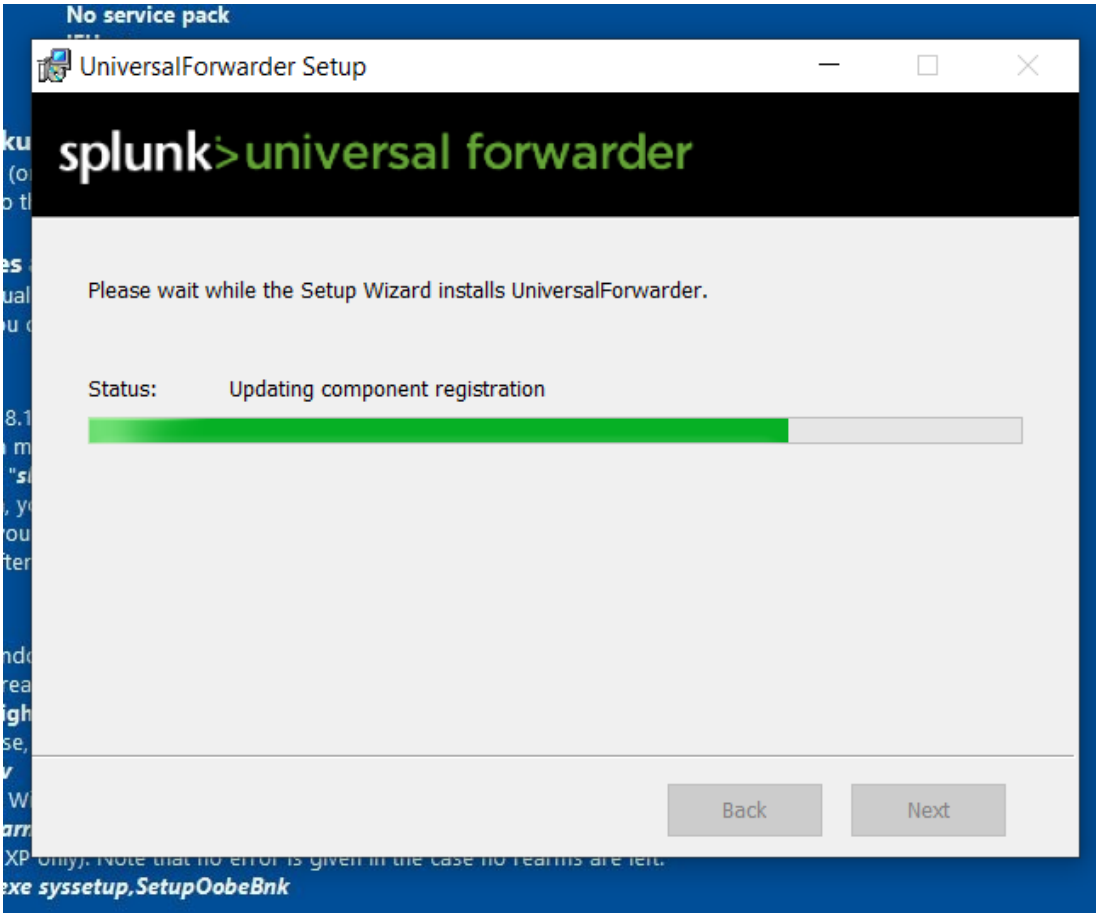
Check all select box except AD Monitoring



Create username and password

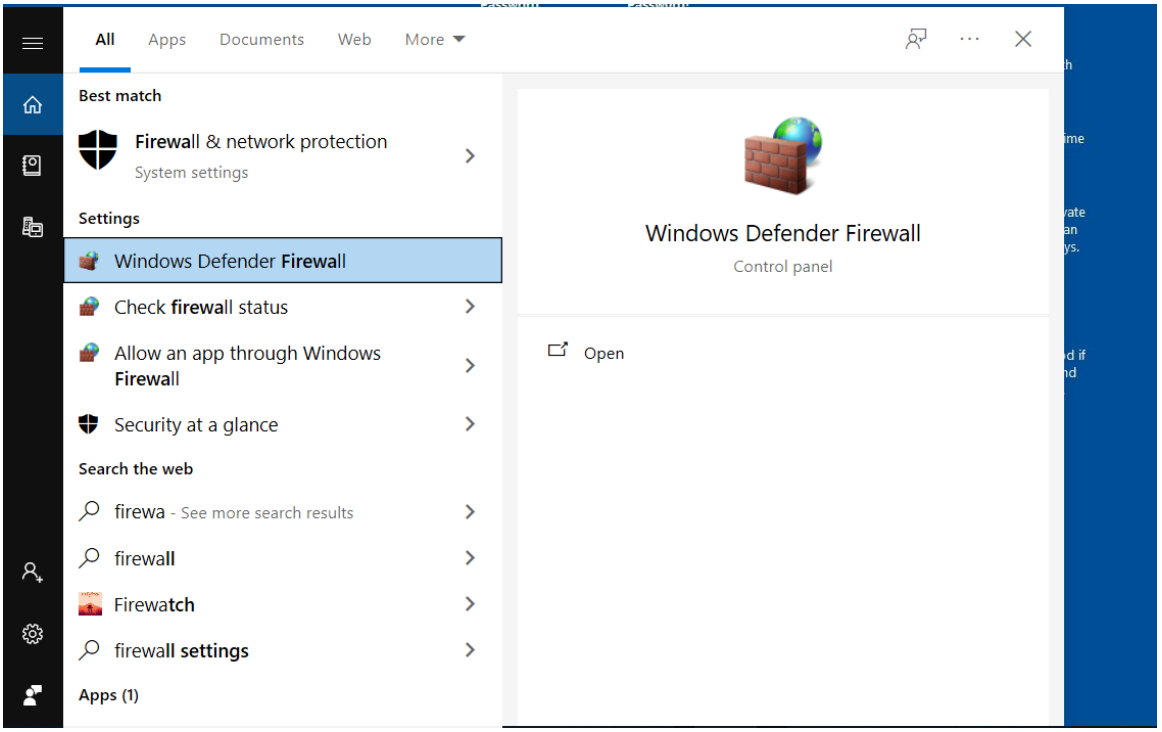


> Here we write IP of our Kali Linux machine and let port is default.

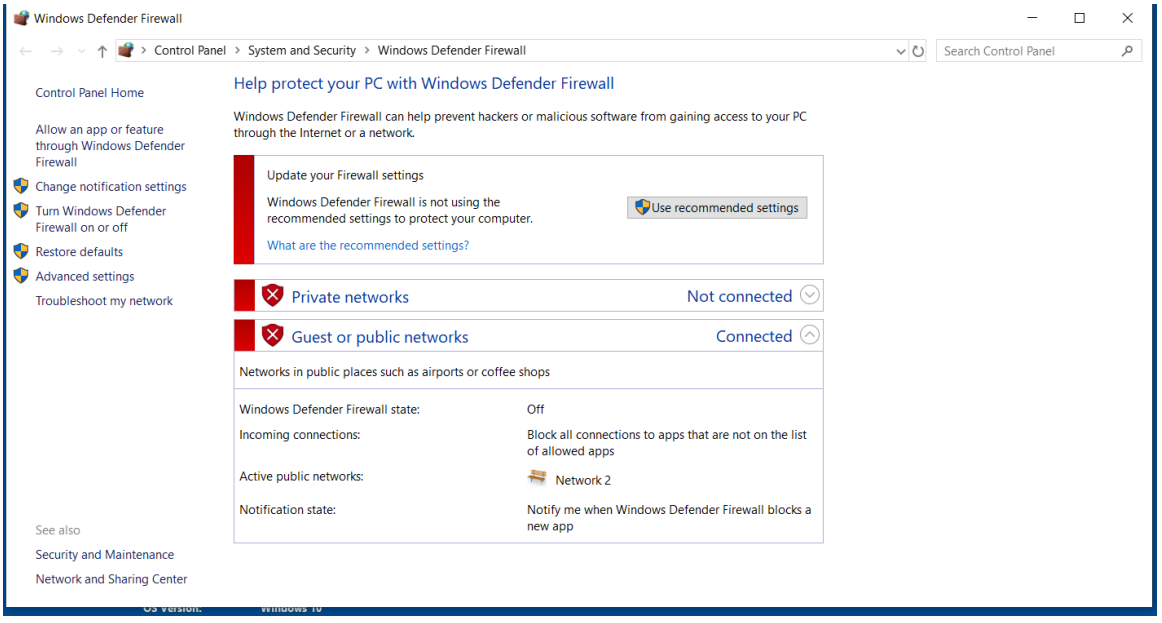


1.3. Configure Our Firewall rules

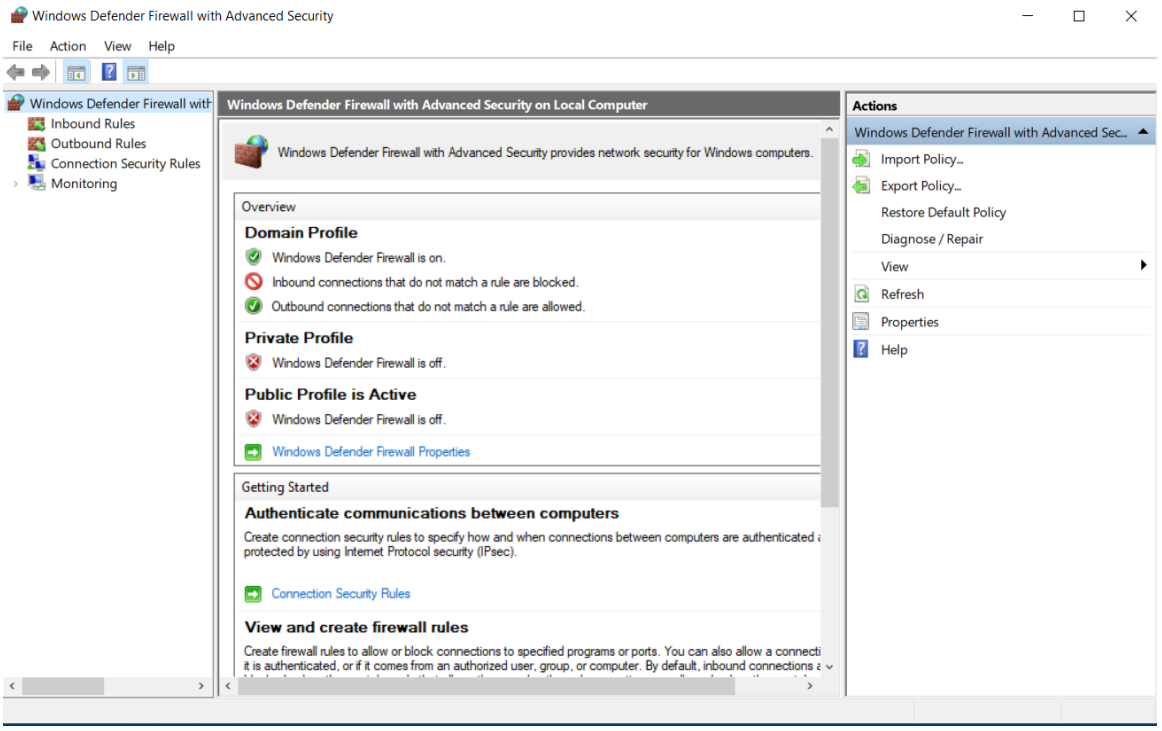
> First we search for firewall



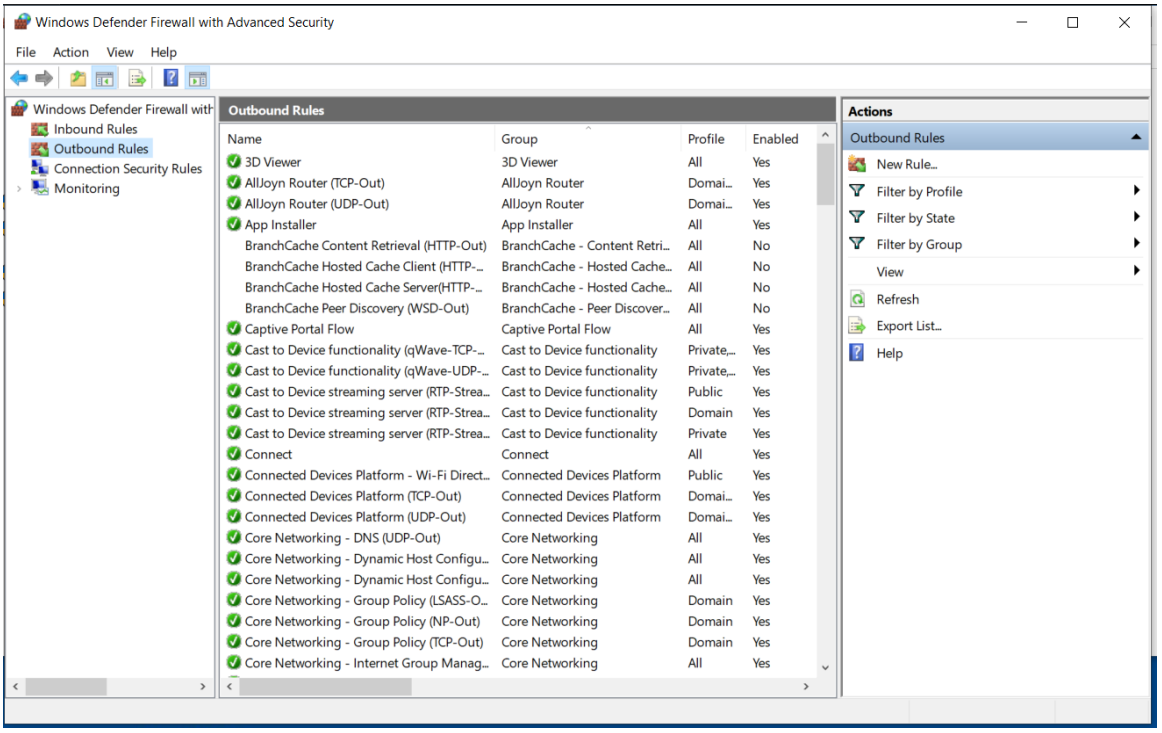
Open windows defender firewall



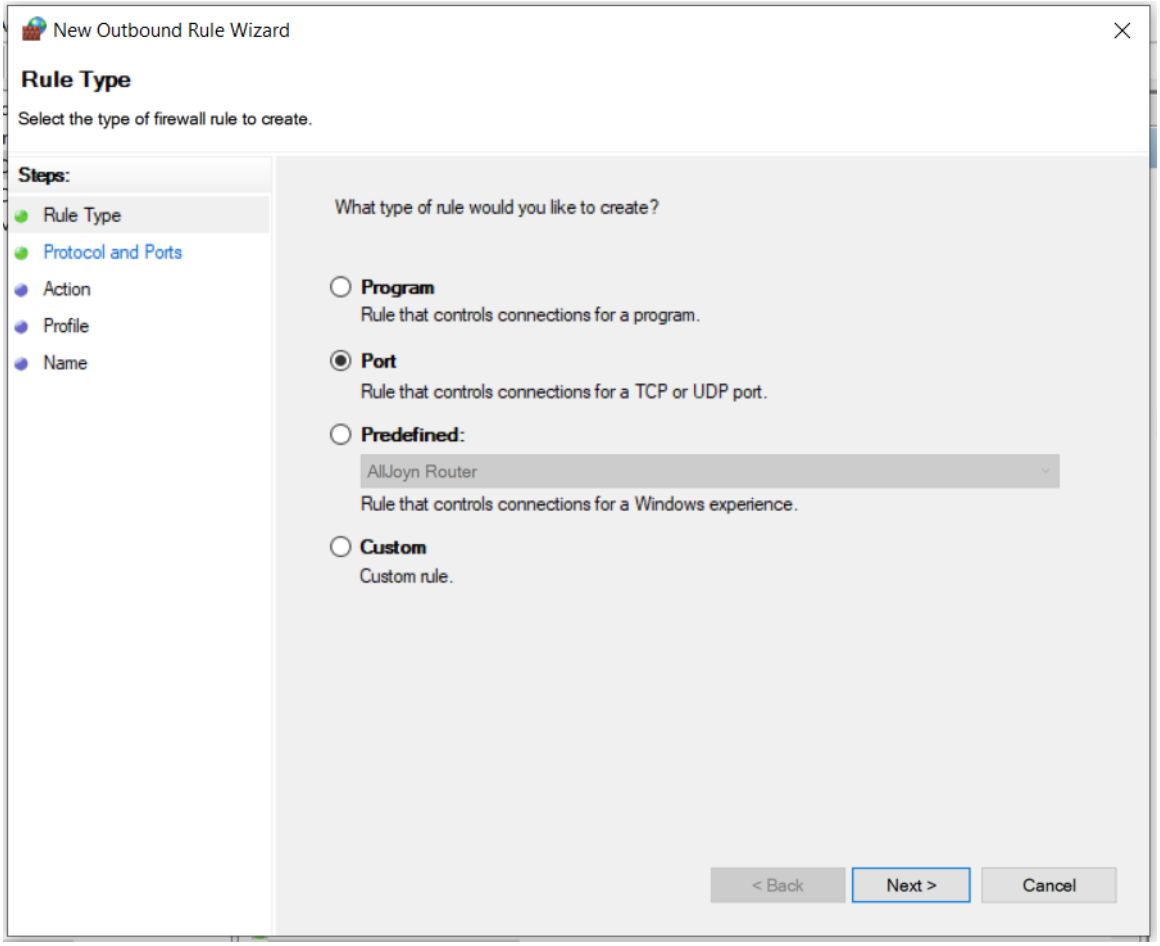
Navigate to advanced settings



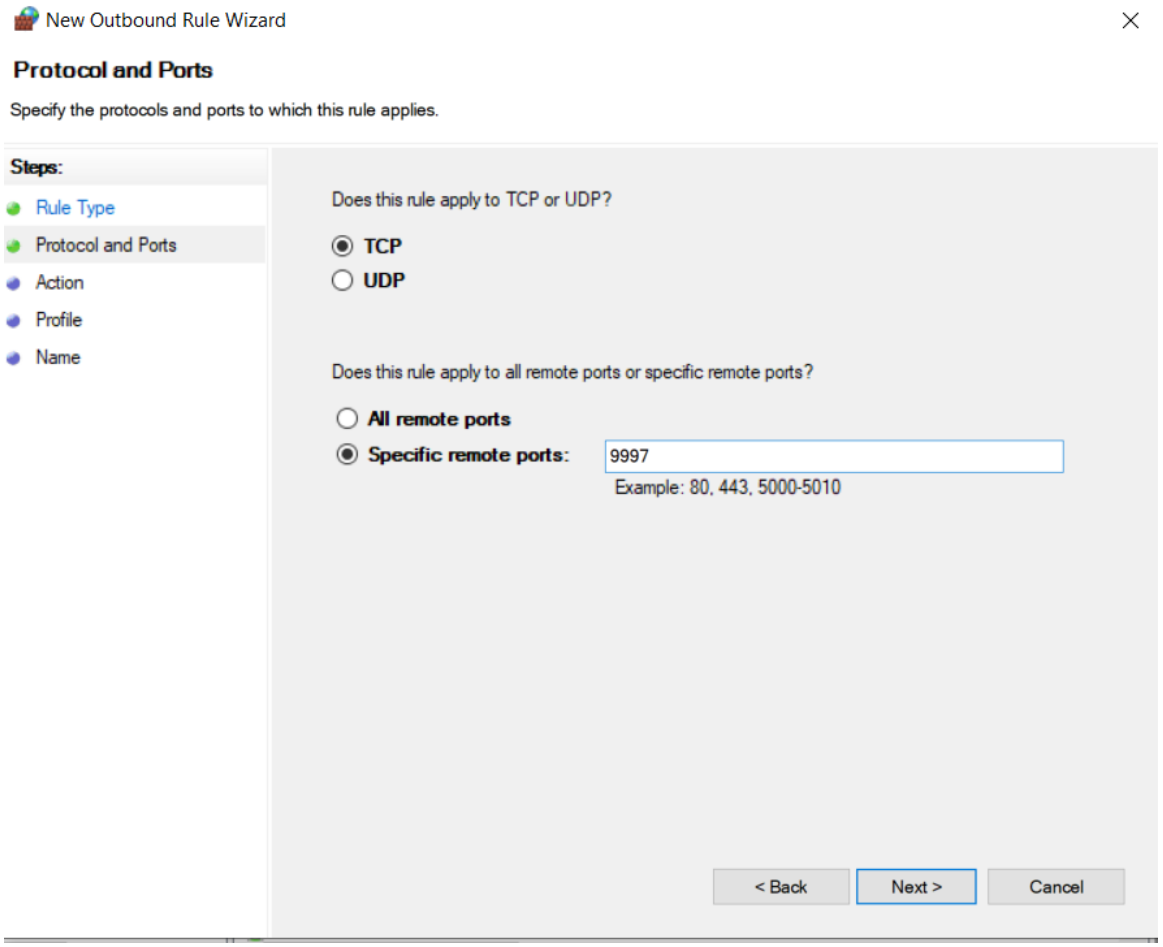
> Navigate to Outbound Rules



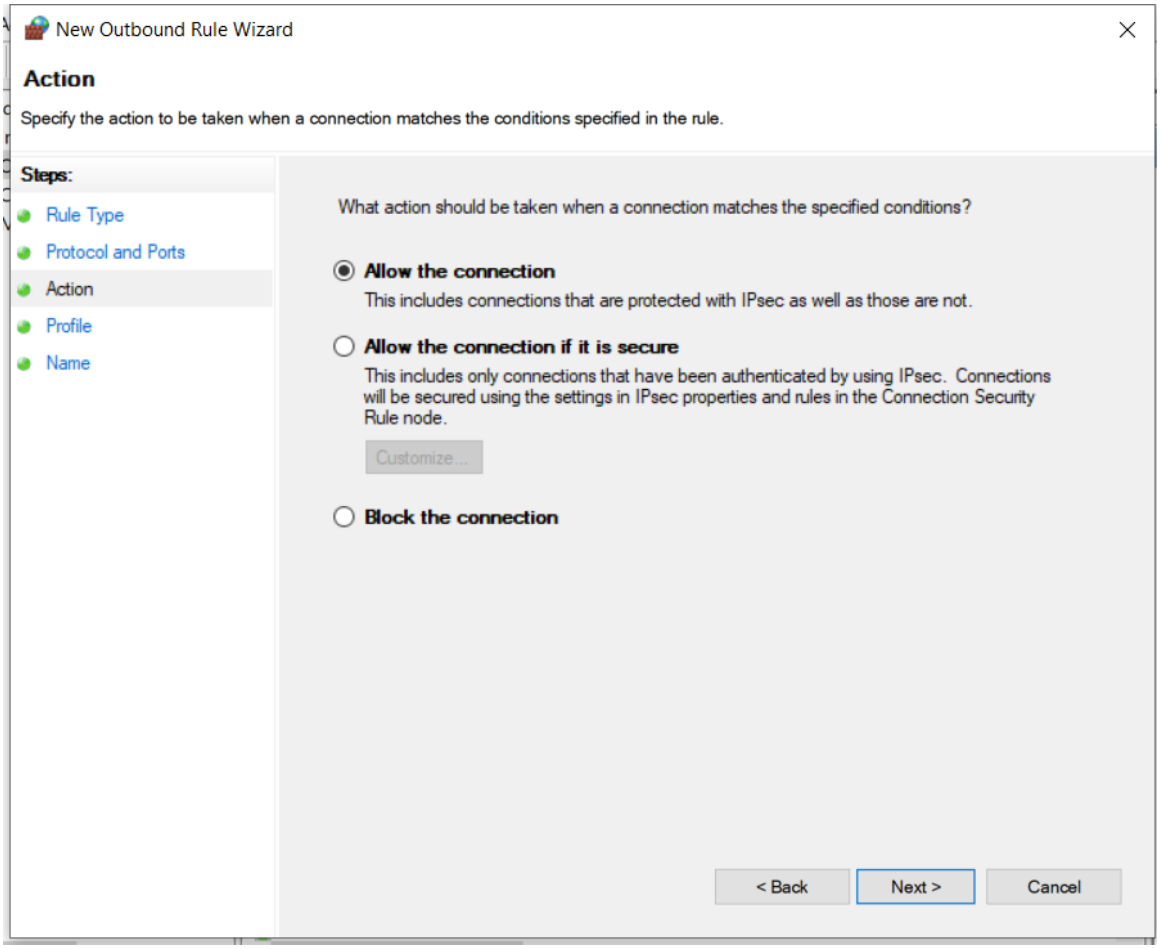
> Create New Rule.



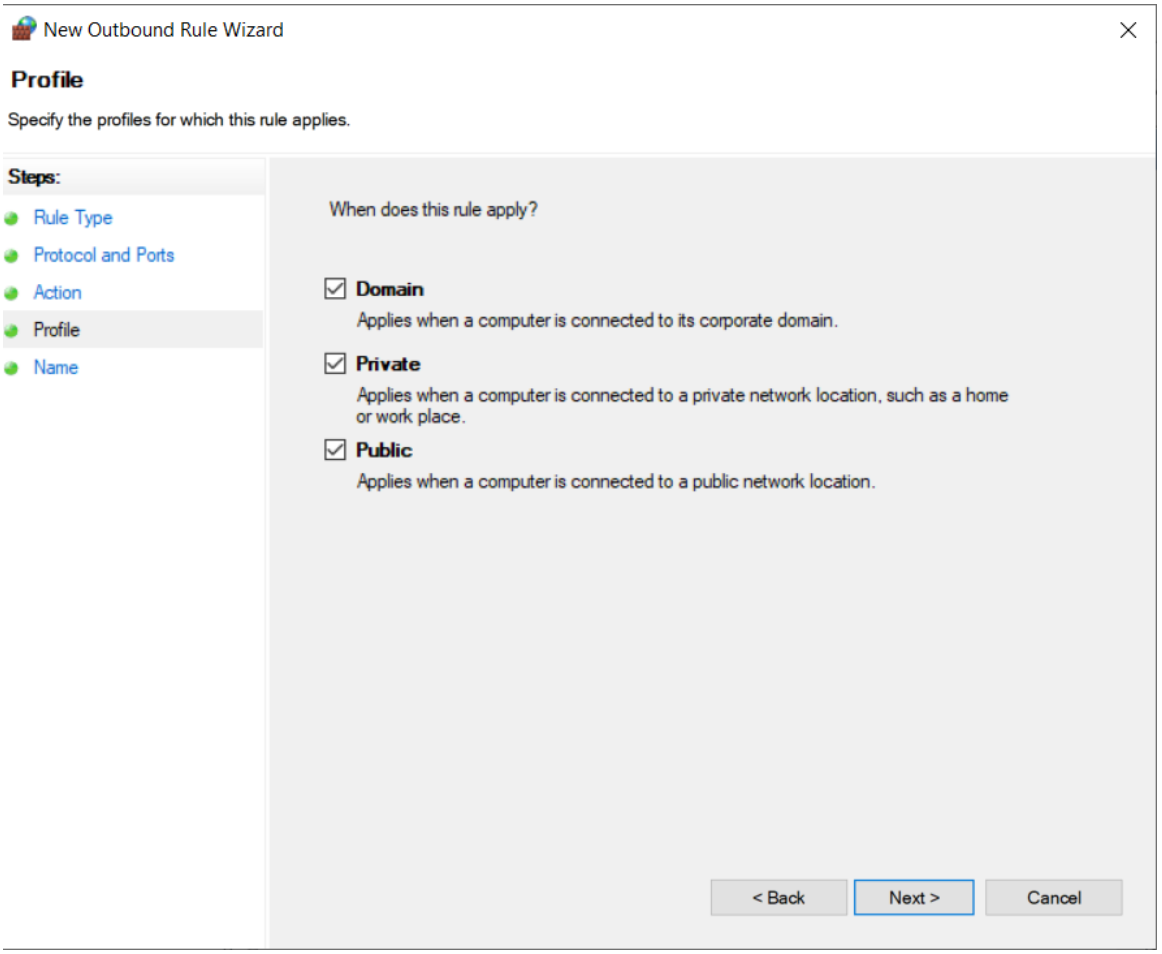
> We Choose Port → Next



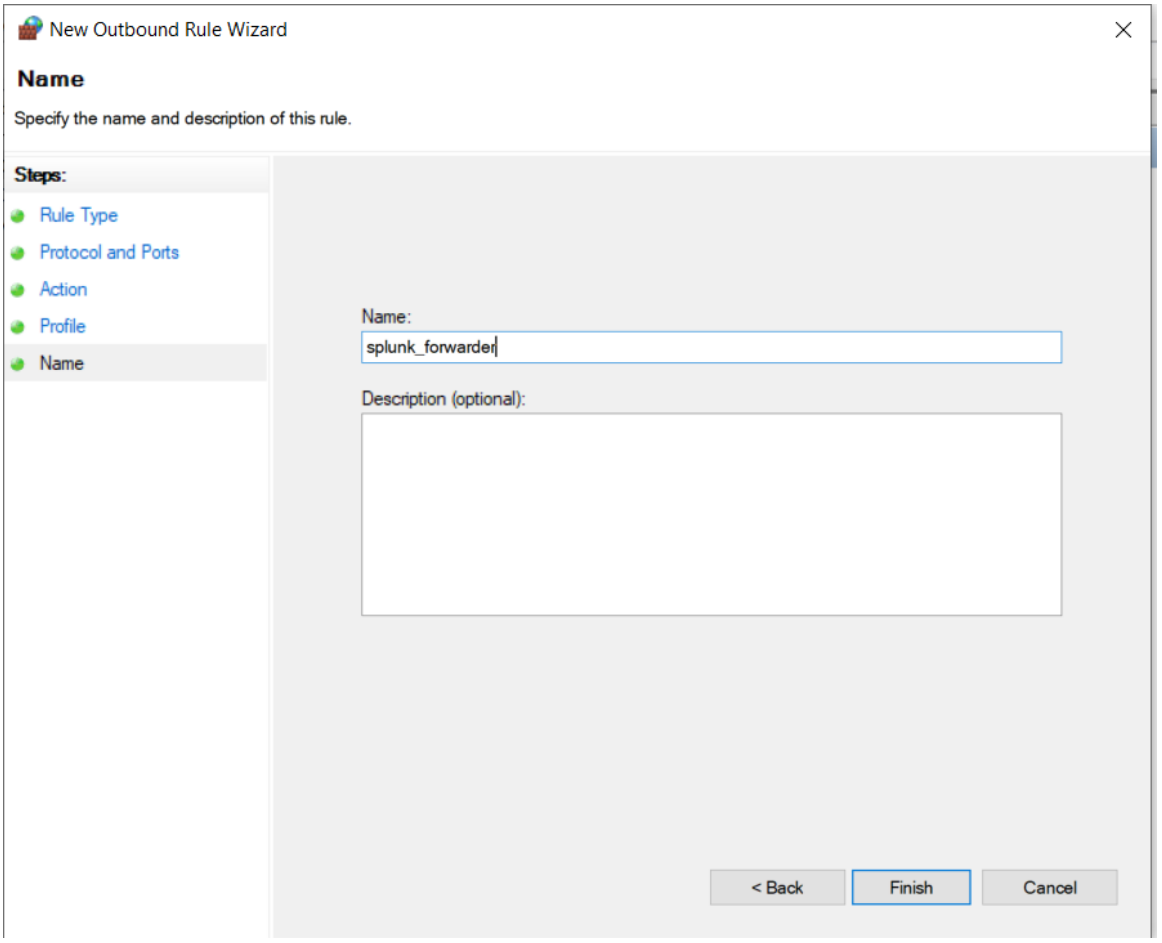
> We choose TCP and Specific remote ports and write default port that we let at the configuration → Next



> 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
```

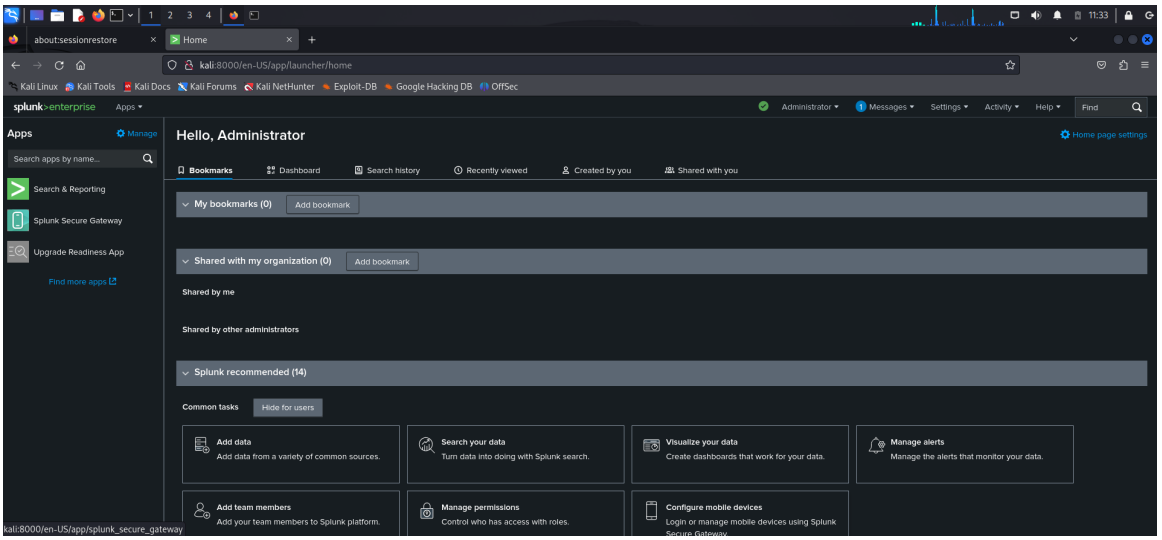
1.3. Start Splunk

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

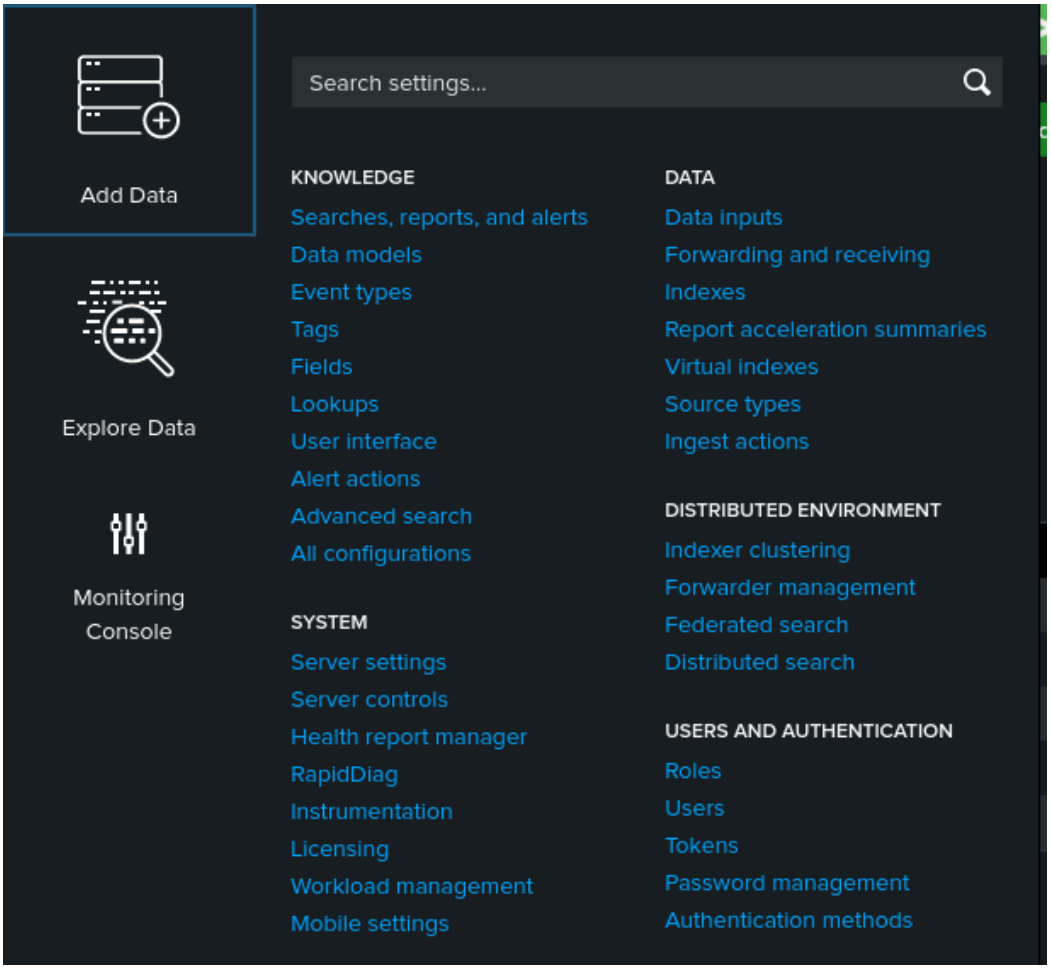
1.4. Login with your Credentials

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

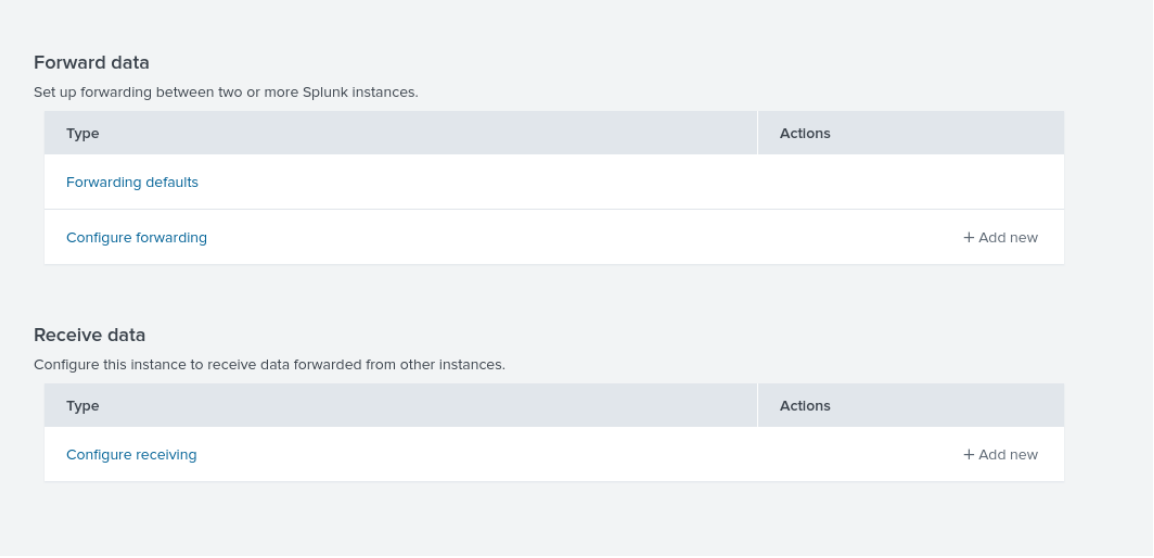
> After log in, you will see like this screen



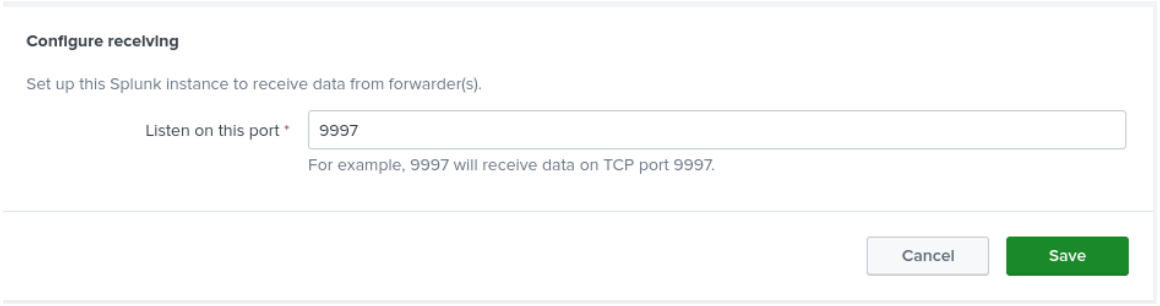
> Now we navigate to settings and from Data section choose forwarding and receiving.



> We use receive data and add new.

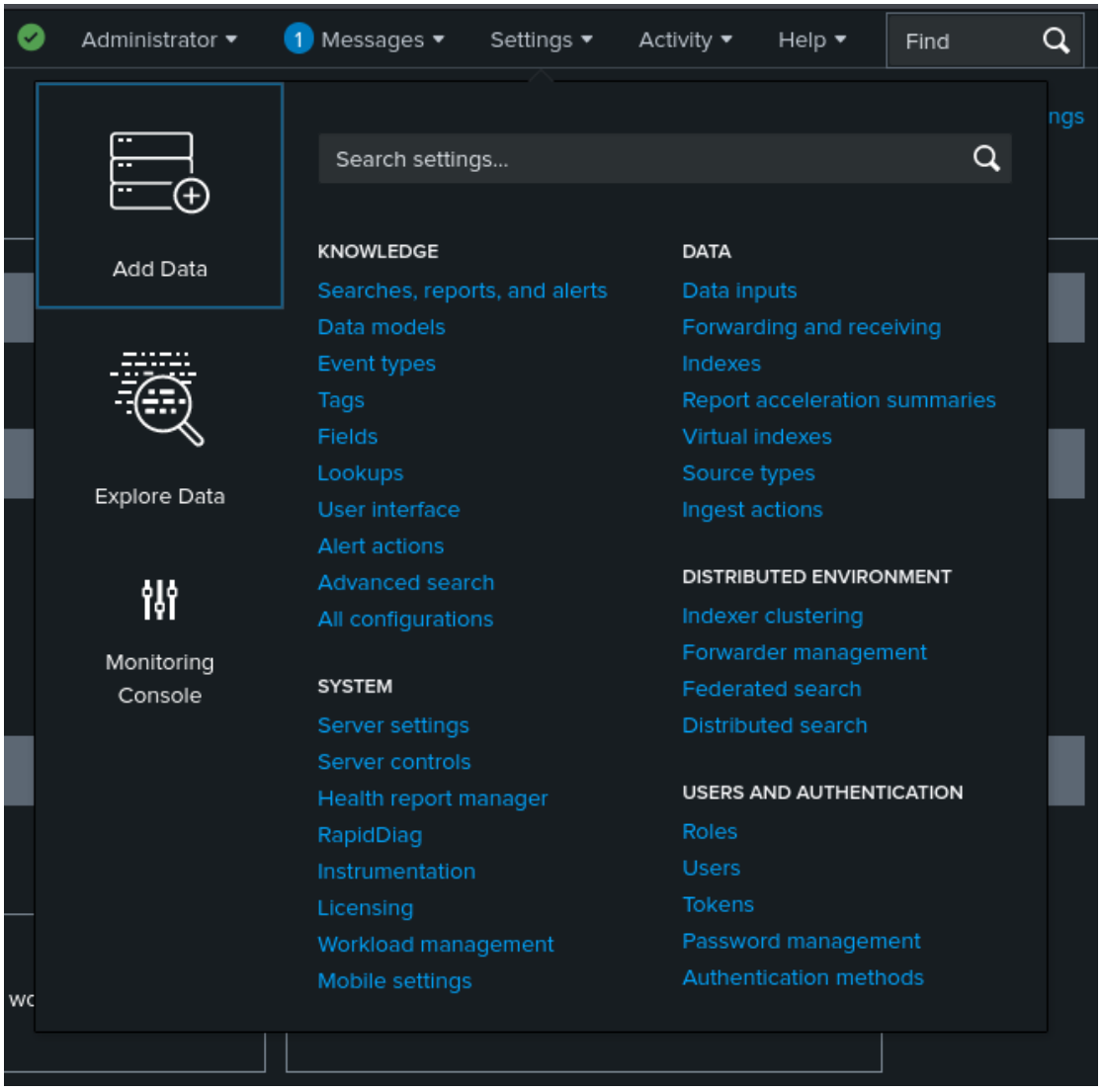


> We write default port of configuration of Splunk universal forwarder and click save.

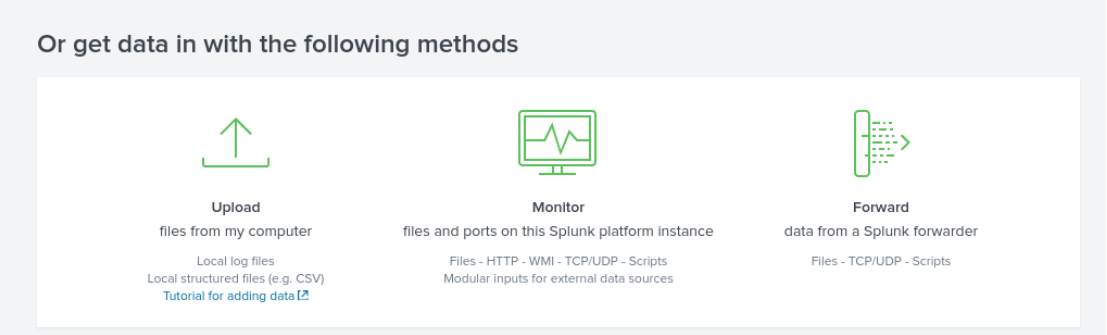


▼ STEPS TO USE SPLUNK FOR INVESTIGATION

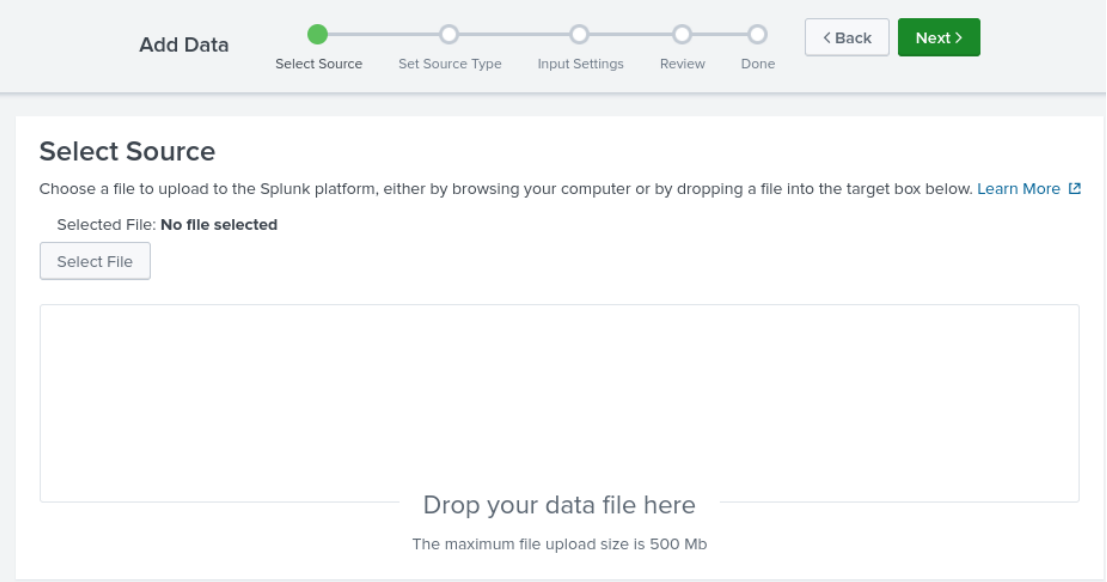
> We navigate to settings and Add Data.

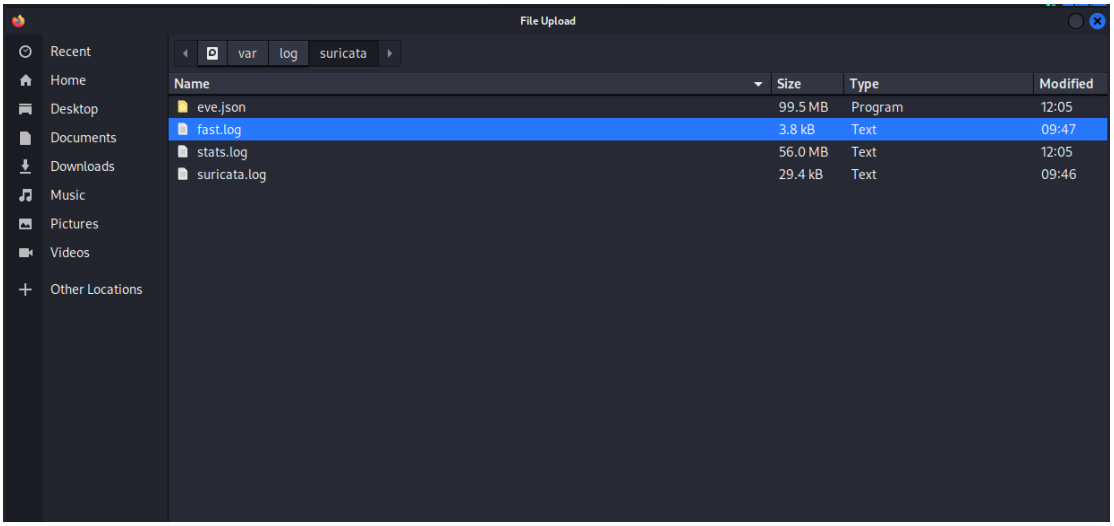


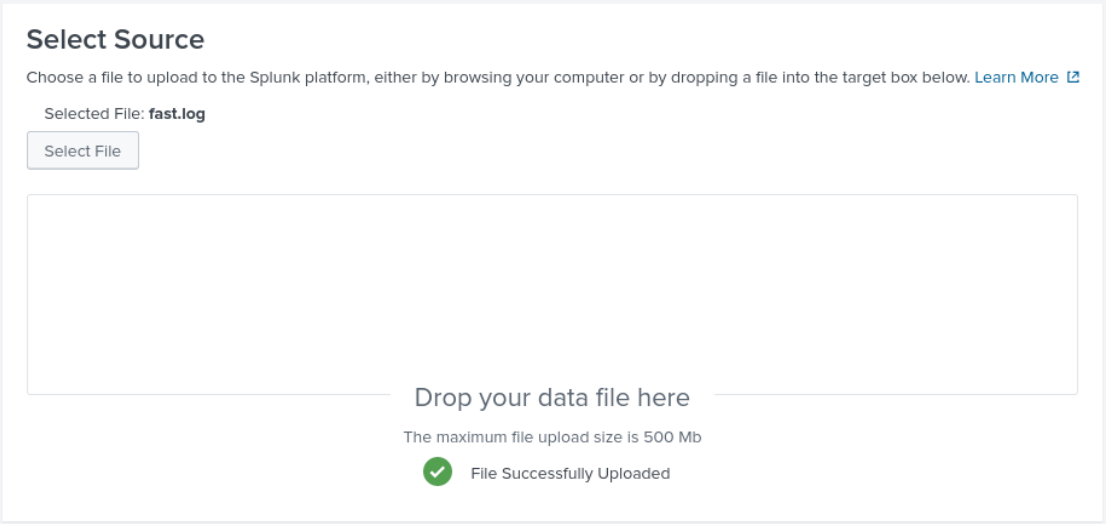
> We Choose upload



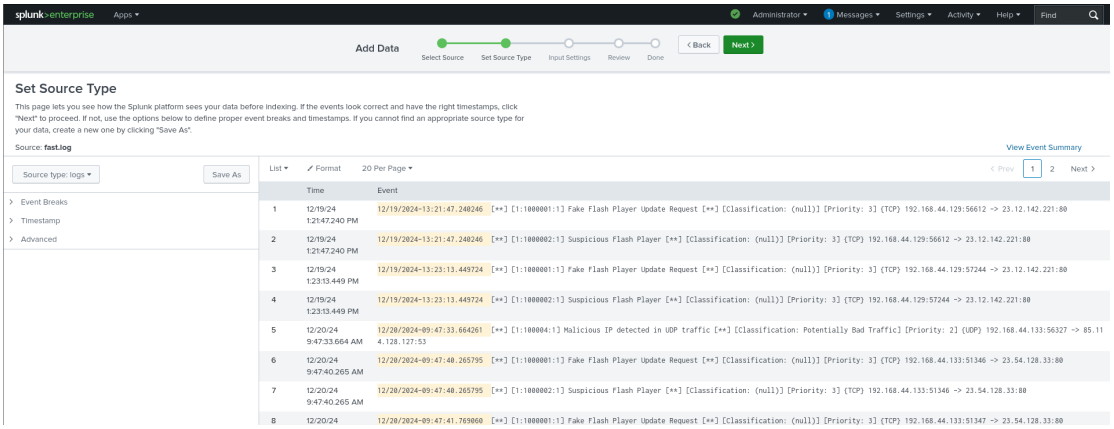
> We select file and upload our logs → `/var/log/suricata`



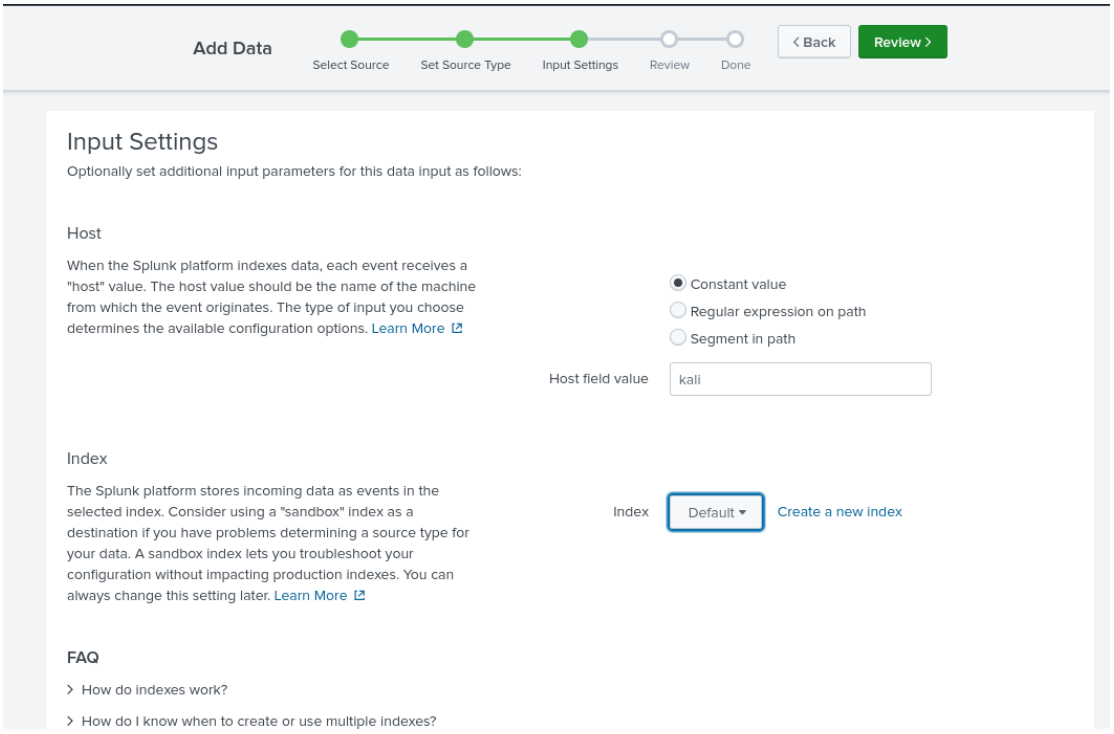




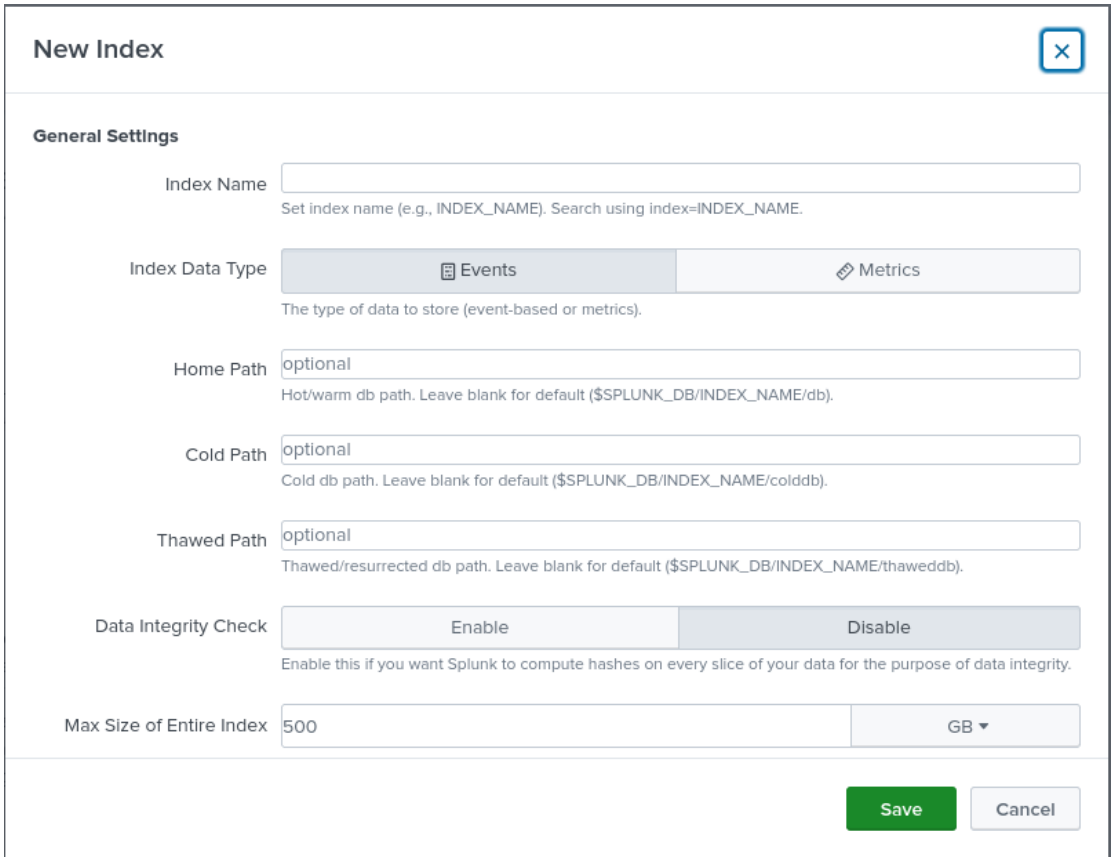
> Choose sourcetype: `logs` ⇒ Next



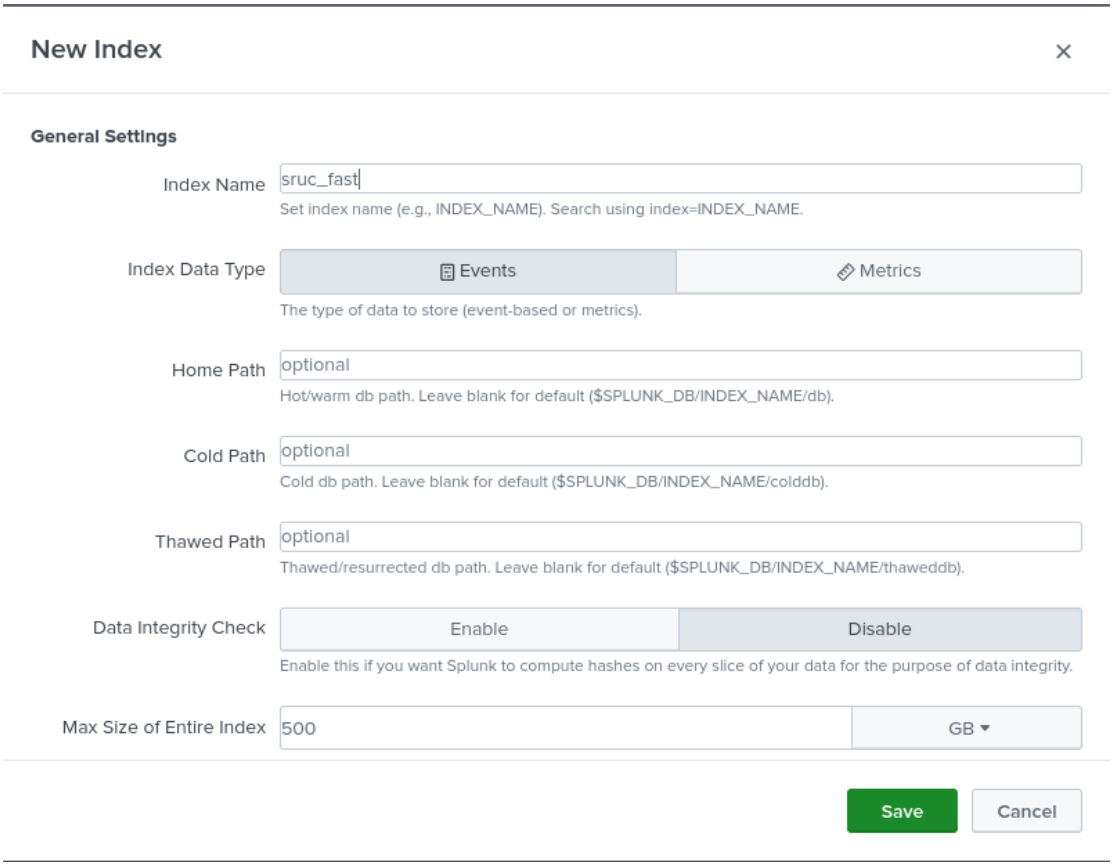
> We need to create an index to use in search



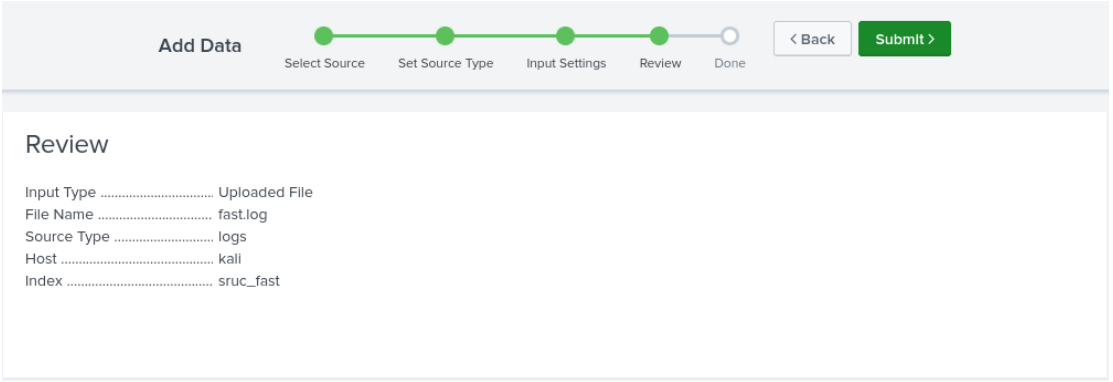
> Create a new index



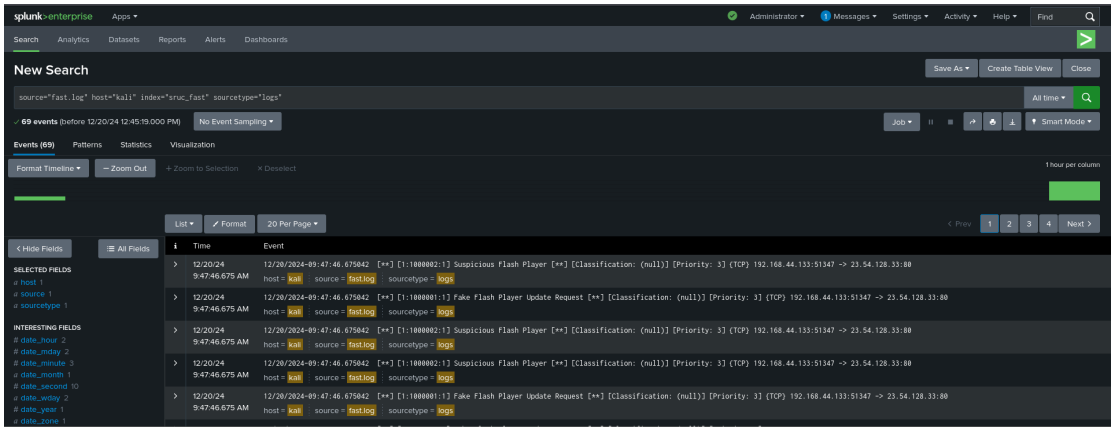
> Name your index as you like and click save.



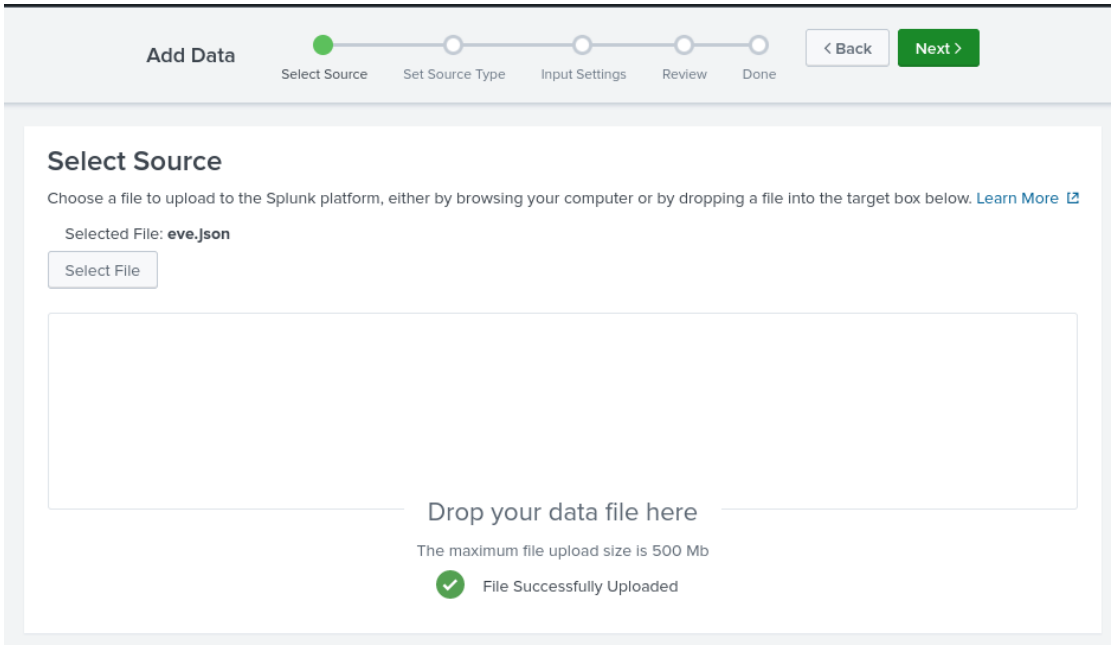
> Click Review



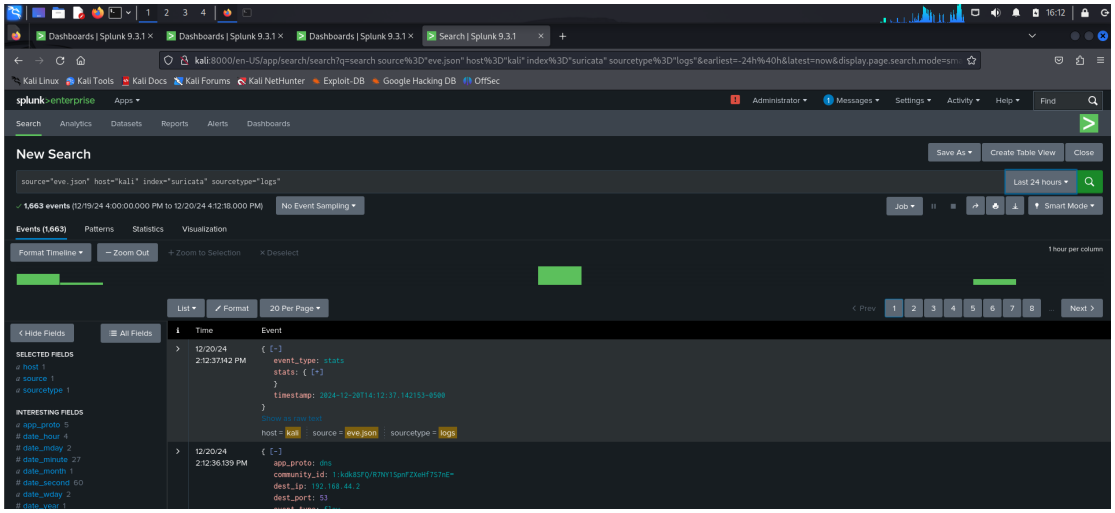
> Click Submit and Start Searching



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

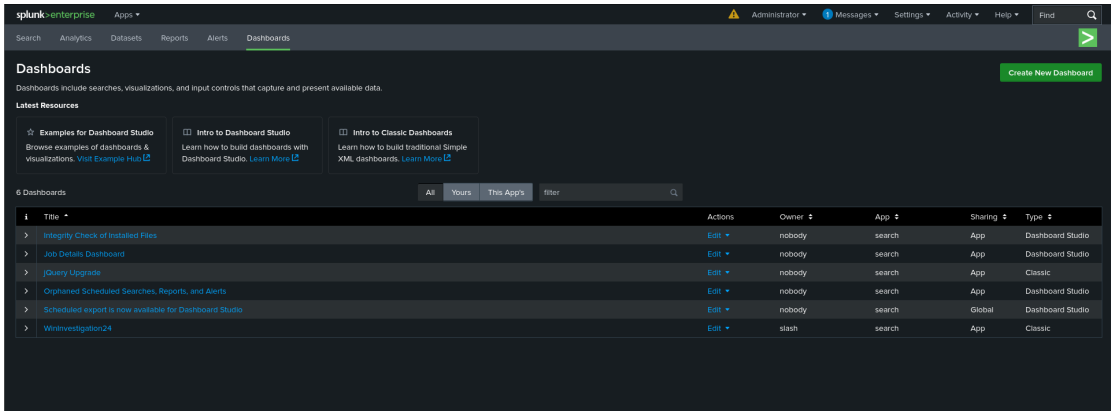


> After Uploading eve.json

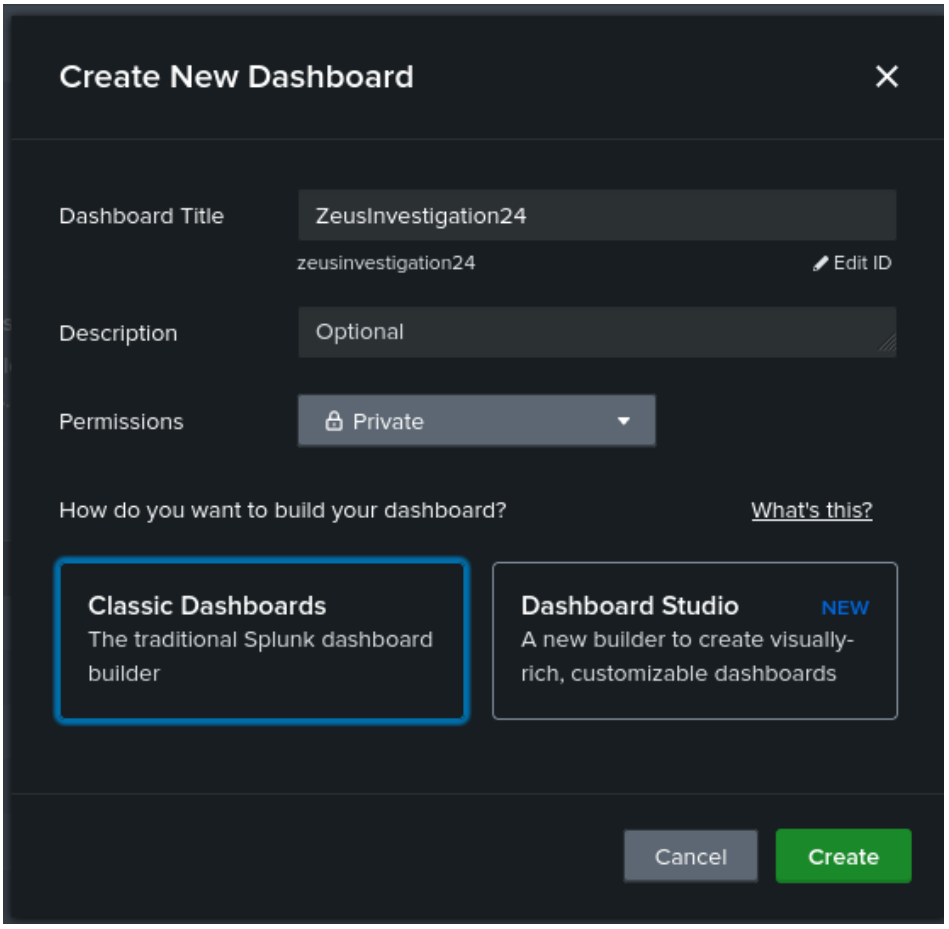


▼ Visualize With Splunk

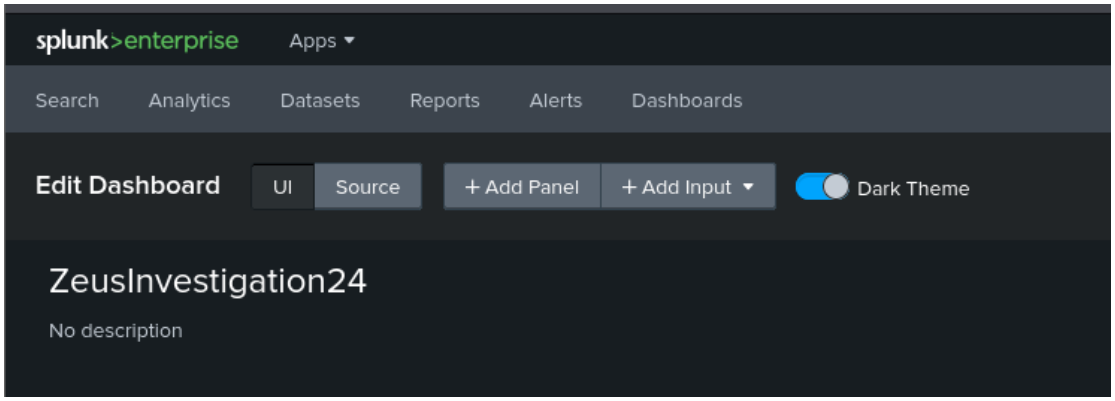
> Go To Dashboard

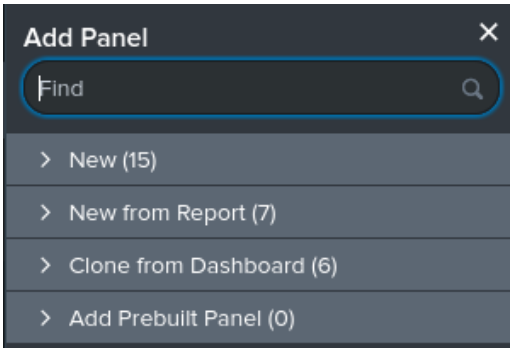


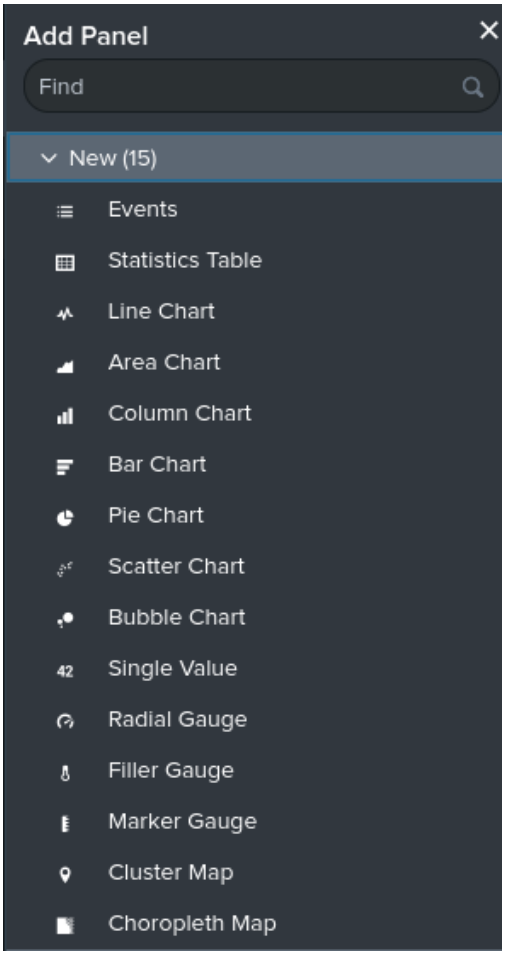
> Name Your Dashboard and choose classic Dashboards and click create.



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

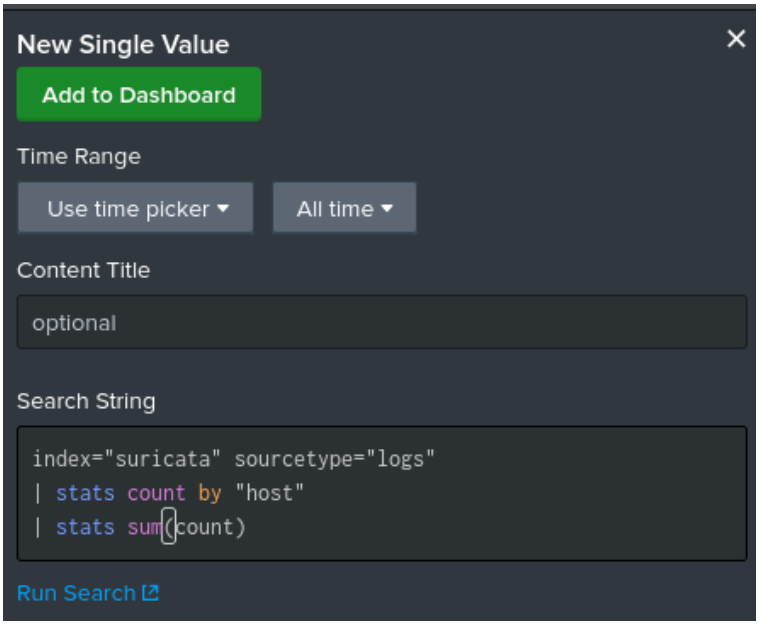




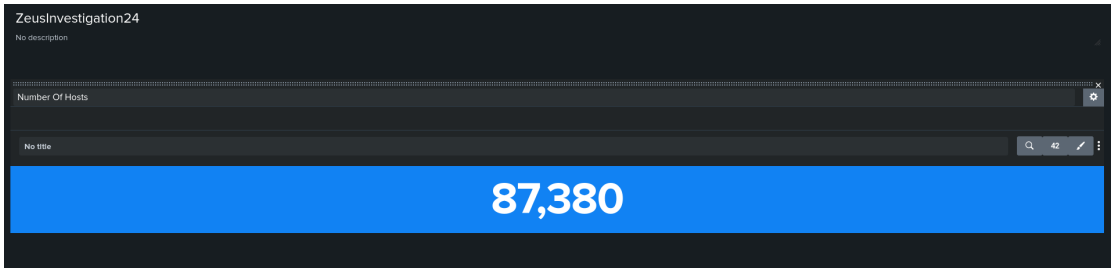


> We choose Single value and write our query

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



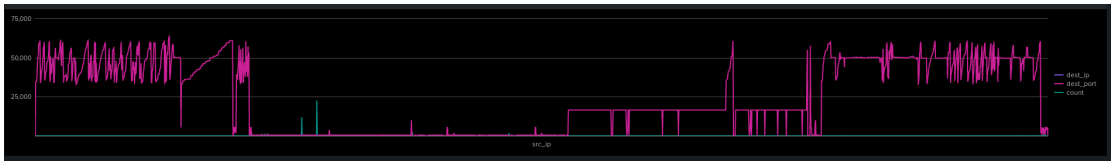
> Click all time and add to dashboard.



> We add some visualizations.

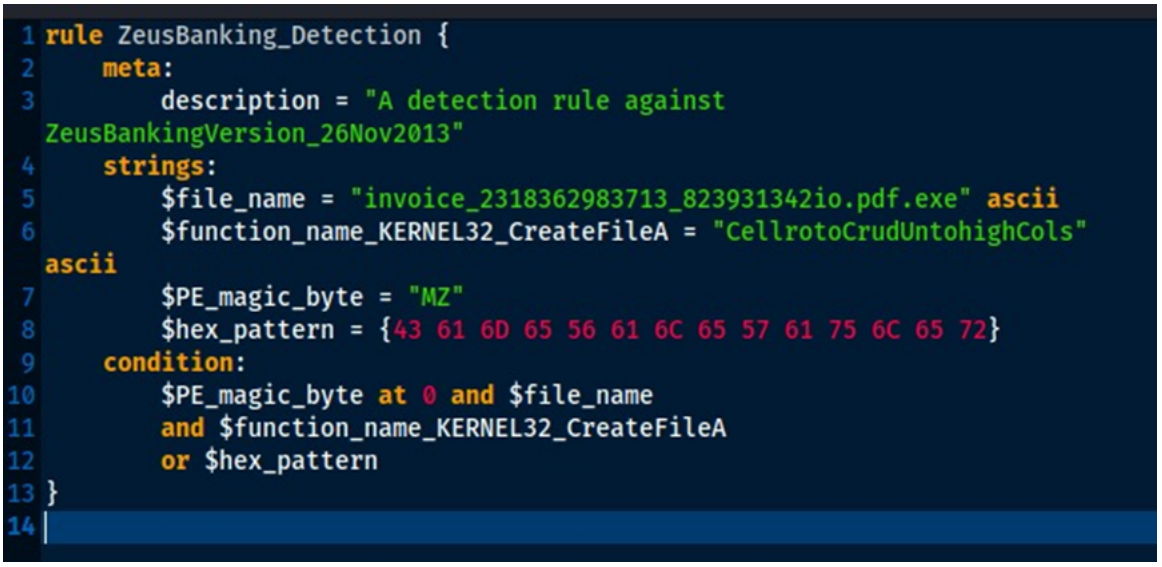
> Second Query

```
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
}
```



> 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

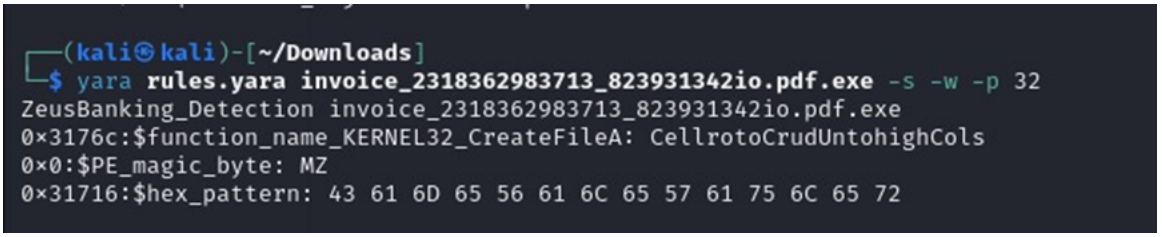
> **$file_name**: containing the suspicious file name
>
> **$function_name_KERNEL32_CreateFileA**: A string representing the name of a function, CellrotoCrudUntohighCols, which may be a part of obfuscated or custom function calls within the malware.
>
> **$PE_magic_byte:** The string "MZ" is the magic number at the start of Portable Executable (PE) files, which indicates that the file is an executable in the Windows PE format.
>
> **$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
```



> The output indicates that the rule ZeusBanking_Detection identified the file `invoice_2318362983713_8239313421o.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

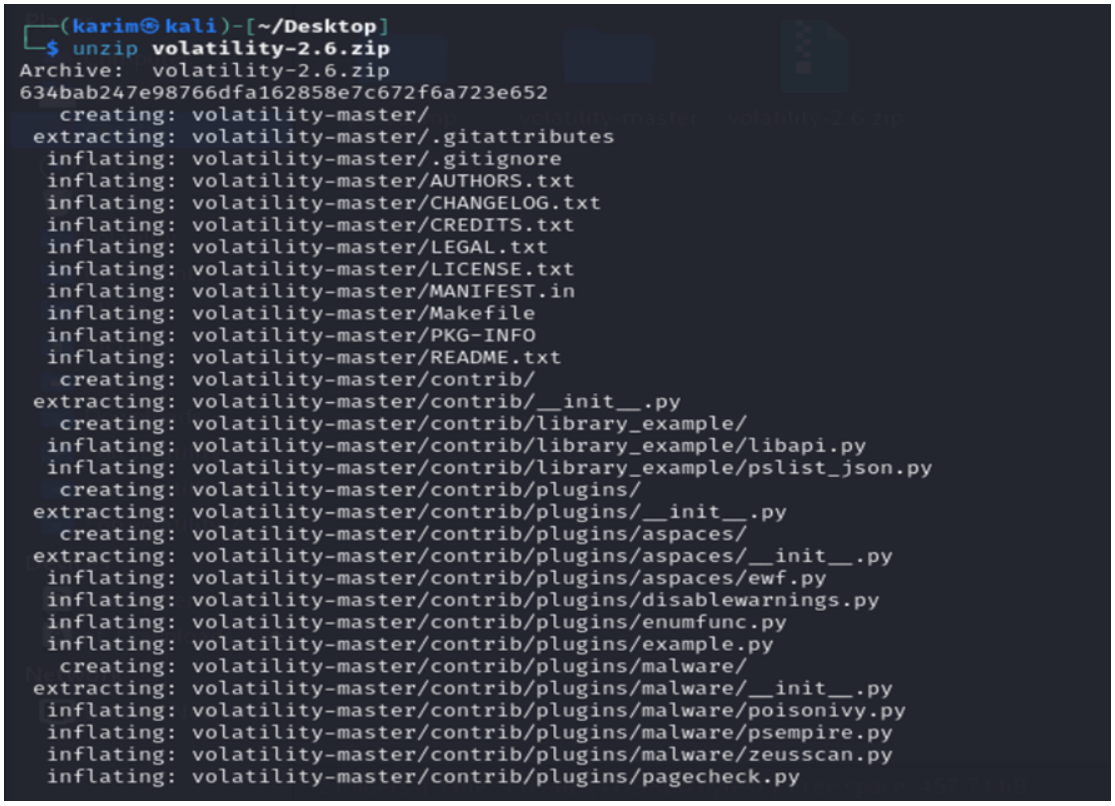
> We are going to use The Volatility tool that help us to investigate and analyze memory dumps and extract information about running processes, network connections, and potential malware.

▼ STEPS

1. Download And Setup

Link:
https://github.com/volatilityfoundation/volatility/releases/tag/2.6.1

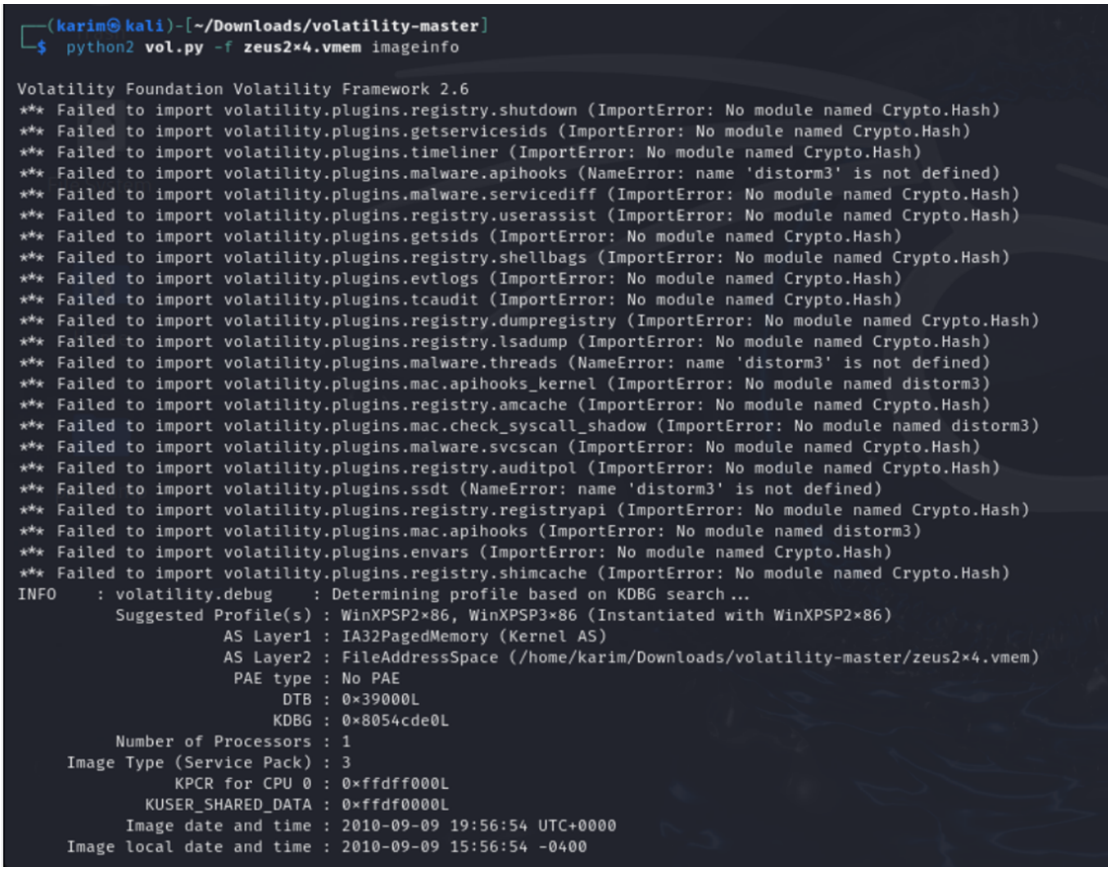
> then we are going to unzip the file after download it using (unzip volatility-master) command.



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 WinXSP2x86 as profile.



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.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)
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x0000000001e87da0 ihah.exe           3276   3772 0x1466b000 2010-09-09 19:56:32 UTC+0000
0x0000000001e8a368 alg.exe            2588    744 0x15058000 2010-09-02 12:25:44 UTC+0000
0x0000000001eab2f8 wuauclt.exe        3984   1084 0x173b7000 2010-09-09 19:52:45 UTC+0000
0x0000000001f4bb28 b98679df6defbb3    3772   2404 0x1f308000 2010-09-09 19:56:19 UTC+0000
0x0000000001ffb6d8 ImmunityDebugge    3788   1752 0x03e57000 2010-09-08 22:39:40 UTC+0000
0x0000000002001ad0 ImmunityDebugge    2972   1752 0x0e002000 2010-09-08 19:14:36 UTC+0000
0x000000000205dda0 wuauclt.exe         940   1084 0x1be36000 2010-09-02 12:26:40 UTC+0000
0x0000000002066478 ImmunityDebugge    2404   1752 0x0586f000 2010-09-09 19:56:19 UTC+0000
0x0000000002077da0 coherence.exe       572    744 0x15e5d000 2010-09-02 12:25:36 UTC+0000
0x000000000207bda0 nifek_locked.ex    2204   2972 0x1804d000 2010-09-08 19:14:36 UTC+0000
0x0000000002086798 prl_tools.exe       632    436 0x15e79000 2010-09-02 12:25:36 UTC+0000
0x0000000002089558 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
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x0000000001e87da0 ihah.exe           3276   3772 0x1466b000 2010-09-09 19:56:32 UTC+0000
0x0000000001e8a368 alg.exe            2588    744 0x15058000 2010-09-02 12:25:44 UTC+0000
0x0000000001eab2f8 wuauclt.exe        3984   1084 0x173b7000 2010-09-09 19:52:45 UTC+0000
0x0000000001f4bb28 b98679df6defbb3    3772   2404 0x1f308000 2010-09-09 19:56:19 UTC+0000
0x0000000001ffb6d8 ImmunityDebugge    3788   1752 0x03e57000 2010-09-08 22:39:40 UTC+0000
0x0000000002001ad0 ImmunityDebugge    2972   1752 0x0e002000 2010-09-08 19:14:36 UTC+0000
0x000000000205dda0 wuauclt.exe         940   1084 0x1be36000 2010-09-02 12:26:40 UTC+0000
0x0000000002066478 ImmunityDebugge    2404   1752 0x0586f000 2010-09-09 19:56:19 UTC+0000
0x0000000002077da0 coherence.exe       572    744 0x15e5d000 2010-09-02 12:25:36 UTC+0000
0x000000000207bda0 nifek_locked.ex    2204   2972 0x1804d000 2010-09-08 19:14:36 UTC+0000
0x0000000002086798 prl_tools.exe       632    436 0x15e79000 2010-09-02 12:25:36 UTC+0000
0x0000000002089558 jqs.exe             472    744 0x1598b000 2010-09-02 12:25:33 UTC+0000
0x000000000208abf0 sqlservr.exe        488    744 0x15a12000 2010-09-02 12:25:33 UTC+0000
0x0000000002095500 spoolsv.exe        1616    744 0x10a9d000 2010-09-02 12:25:24 UTC+0000
0x00000000020ee580 prl_cc.exe         1908   1752 0x11de1000 2010-09-02 12:25:25 UTC+0000
0x0000000002129370 svchost.exe         364    744 0x157c5000 2010-09-02 12:25:33 UTC+0000
0x000000000212ada0 jusched.exe        1936   1752 0x12010000 2010-09-02 12:25:26 UTC+0000
0x000000000213dda0 wscntfy.exe        2180   1084 0x1993a000 2010-09-02 12:25:41 UTC+0000
0x000000000214f488 svchost.exe        1192    744 0x10147000 2010-09-02 12:25:23 UTC+0000
0x0000000002150b90 svchost.exe         912    744 0x0e9ad000 2010-09-02 12:25:22 UTC+0000
0x0000000002151da0 svchost.exe        1084    744 0x0ef67000 2010-09-02 12:25:22 UTC+0000
0x00000000021521b0 svchost.exe        1140    744 0x0f13b000 2010-09-02 12:25:22 UTC+0000
0x0000000002189530 prl_tools_servi     436    744 0x15ce2000 2010-09-02 12:25:36 UTC+0000
0x000000000219e5c8 anaxu.exe          3508   3788 0x1a36a000 2010-09-08 22:39:40 UTC+0000
0x00000000021a5da0 services.exe        744    692 0x0e0d7000 2010-09-02 12:25:22 UTC+0000
0x00000000021aa7e8 sqlwriter.exe       660    744 0x15e67000 2010-09-02 12:25:36 UTC+0000
0x00000000021b2020 explorer.exe       1752   1720 0x10e31000 2010-09-02 12:25:25 UTC+0000
0x00000000021f2978 csrss.exe           668    596 0x0d5f0000 2010-09-02 12:25:21 UTC+0000
0x000000000221e278 iscsiexe.exe       1436    744 0x1090c000 2010-09-02 12:25:24 UTC+0000
0x000000000223c020 vaelh.exe           952   1932 0x1ee5a000 2010-09-08 19:23:02 UTC+0000
0x0000000002282380 ImmunityDebugge    1932   1752 0x18f4d000 2010-09-08 19:23:02 UTC+0000
0x0000000002292da0 smss.exe            596      4 0x0adcc000 2010-09-02 12:25:18 UTC+0000
0x00000000022b96c0 SharedIntApp.ex    1900   1752 0x11f33000 2010-09-02 12:25:25 UTC+0000
0x00000000022c09f8 winlogon.exe        692    596 0x0db75000 2010-09-02 12:25:22 UTC+0000
0x00000000022c8798 lsass.exe           756    692 0x0e121000 2010-09-02 12:25:22 UTC+0000
0x00000000022c8bf8 svchost.exe         992    744 0x0ed20000 2010-09-02 12:25:22 UTC+0000
0x0000000002311648 rundll32.exe       3768   1084 0x14502000 2010-09-09 19:56:33 UTC+0000
0x00000000023c8a00 System                4      0 0x00039000
```

3. List Active Processes Using psslist

```
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.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)
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c8a00 System                    4      0     57      671 ------      0
0x82292da0 smss.exe                596      4      3       19 ------      0 2010-09-02 12:25:18 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 iscsiexe.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
0x82292da0 smss.exe                596      4      3       19 ------      0 2010-09-02 12:25:18 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 iscsiexe.exe           1436    744      6       78      0      0 2010-09-02 12:25:24 UTC+0000
0x82095500 spoolsv.exe            1616    744     13      140      0      0 2010-09-02 12:25:24 UTC+0000
0x821b2020 explorer.exe           1752   1720     22      520      0      0 2010-09-02 12:25:25 UTC+0000
0x822b96c0 SharedIntApp.ex        1900   1752      3       75      0      0 2010-09-02 12:25:25 UTC+0000
0x820ee580 prl_cc.exe             1908   1752     14      133      0      0 2010-09-02 12:25:25 UTC+0000
0x8212ada0 jusched.exe            1936   1752      1       43      0      0 2010-09-02 12:25:26 UTC+0000
0x82129370 svchost.exe             364    744      4       88      0      0 2010-09-02 12:25:33 UTC+0000
0x82089558 jqs.exe                 472    744      5      146      0      0 2010-09-02 12:25:33 UTC+0000
0x8208abf0 sqlservr.exe            488    744     25      306      0      0 2010-09-02 12:25:33 UTC+0000
0x82077da0 coherence.exe           572    744      4       51      0      0 2010-09-02 12:25:36 UTC+0000
0x82189530 prl_tools_servi         436    744      3       78      0      0 2010-09-02 12:25:36 UTC+0000
0x82086798 prl_tools.exe           632    436      9      107      0      0 2010-09-02 12:25:36 UTC+0000
0x821aa7e8 sqlwriter.exe           660    744      4       84      0      0 2010-09-02 12:25:36 UTC+0000
0x8213dda0 wscntfy.exe            2180   1084      3       48      0      0 2010-09-02 12:25:41 UTC+0000
0x81e8a368 alg.exe                2588    744      6      107      0      0 2010-09-02 12:25:44 UTC+0000
0x8205dda0 wuauclt.exe             940   1084      4      126      0      0 2010-09-02 12:26:40 UTC+0000
0x82001ad0 ImmunityDebugge        2972   1752      2       87      0      0 2010-09-08 19:14:36 UTC+0000
0x8207bda0 nifek_locked.ex        2204   2972      2       38      0      0 2010-09-08 19:14:36 UTC+0000
0x82282380 ImmunityDebugge        1932   1752      2       86      0      0 2010-09-08 19:23:02 UTC+0000
0x8223c020 vaelh.exe               952   1932      2       40      0      0 2010-09-08 19:23:02 UTC+0000
0x81ffb6d8 ImmunityDebugge        3788   1752      2      103      0      0 2010-09-08 22:39:40 UTC+0000
0x8219e5c8 anaxu.exe              3508   3788      2       54      0      0 2010-09-08 22:39:40 UTC+0000
0x81eab2f8 wuauclt.exe            3984   1084      8      325      0      0 2010-09-09 19:52:45 UTC+0000
0x82066478 ImmunityDebugge        2404   1752      2       85      0      0 2010-09-09 19:56:19 UTC+0000
0x81f4bb28 b98679df6defbb3        3772   2404      1       46      0      0 2010-09-09 19:56:19 UTC+0000
0x81e87da0 ihah.exe               3276   3772      1       45      0      0 2010-09-09 19:56:32 UTC+0000
0x82311648 rundll32.exe           3768   1084      1       53      0      0 2010-09-09 19:56:33 UTC+0000
```

4. Scan Network Connectios

```
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 zeus2×4.vmem --profile WinXPSP2×86 connscan

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)
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0×020f5410 10.211.55.5:1427         65.54.81.89:80            1084
0×02125008 10.211.55.5:1423         207.46.21.123:80          1084
0×022ace08 10.211.55.5:1432         193.43.134.14:80          1752
```

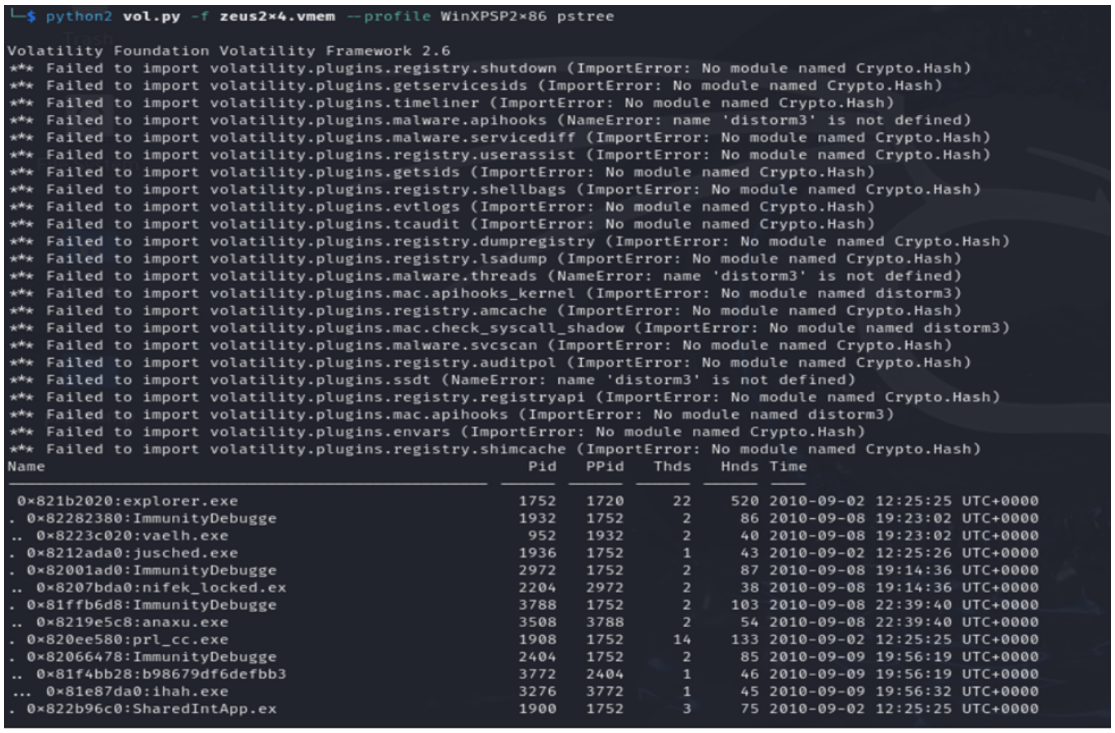
> Now we are going to scan this IP : `193.43.134.14` and we will find that this is the malicious ip with pid `1752`

5. Process Tree

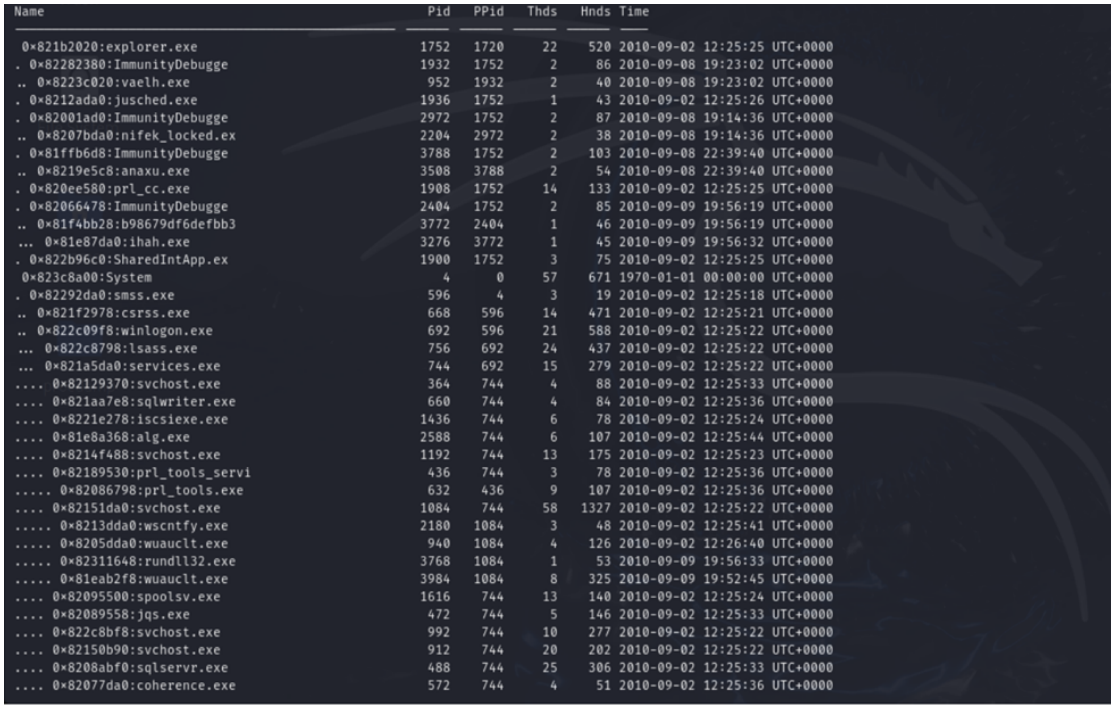
```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 pstree
```

> 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.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)
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.ex                        2204   2972      2     38 2010-09-08 19:14:36 UTC+0000
. 0x81ffb6d8: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.ex                         1900   1752      3     75 2010-09-02 12:25:25 UTC+0000
```

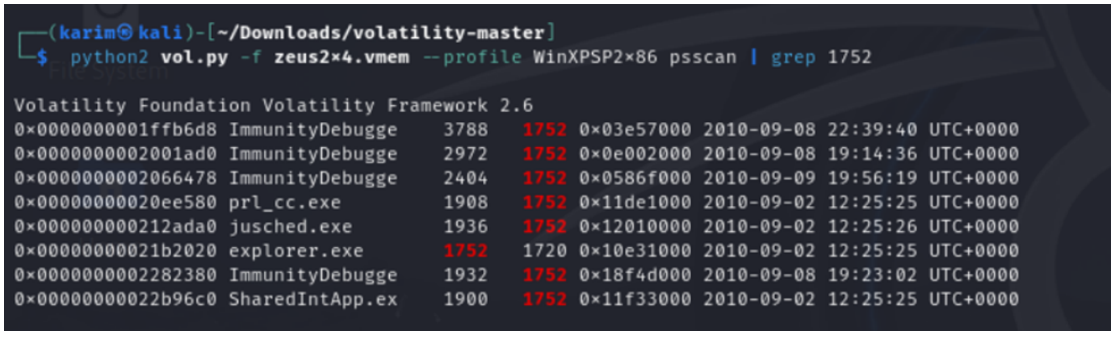


Name	Pid	PPid	Thds	Hnds	Time
0×821b2020:explorer.exe	1752	1720	22	520	2010-09-02 12:25:25 UTC+0000
. 0×82282380:ImmunityDebugge	1932	1752	2	86	2010-09-08 19:23:02 UTC+0000
.. 0×8223c020:vaelh.exe	952	1932	2	40	2010-09-08 19:23:02 UTC+0000
. 0×8212ada0:jusched.exe	1936	1752	1	43	2010-09-02 12:25:26 UTC+0000
. 0×82001ad0:ImmunityDebugge	2972	1752	2	87	2010-09-08 19:14:36 UTC+0000
.. 0×8207bda0:nifek_locked.ex	2204	2972	2	38	2010-09-08 19:14:36 UTC+0000
. 0×81ffb6d8:ImmunityDebugge	3788	1752	2	103	2010-09-08 22:39:40 UTC+0000
.. 0×8219e5c8:anaxu.exe	3508	3788	2	54	2010-09-08 22:39:40 UTC+0000
. 0×820ee580:prl_cc.exe	1908	1752	14	133	2010-09-02 12:25:25 UTC+0000
. 0×82066478:ImmunityDebugge	2404	1752	2	85	2010-09-09 19:56:19 UTC+0000
.. 0×81f4bb28:b98679df6defbb3	3772	2404	1	46	2010-09-09 19:56:19 UTC+0000
... 0×81e87da0:ihah.exe	3276	3772	1	45	2010-09-09 19:56:32 UTC+0000
. 0×822b96c0:SharedIntApp.ex	1900	1752	3	75	2010-09-02 12:25:25 UTC+0000
0×823c8a00:System	4	0	57	671	1970-01-01 00:00:00 UTC+0000
. 0×82292da0:smss.exe	596	4	3	19	2010-09-02 12:25:18 UTC+0000
.. 0×821f2978:csrss.exe	668	596	14	471	2010-09-02 12:25:21 UTC+0000
.. 0×822c09f8:winlogon.exe	692	596	21	588	2010-09-02 12:25:22 UTC+0000
... 0×822c8798:lsass.exe	756	692	24	437	2010-09-02 12:25:22 UTC+0000
... 0×821a5da0:services.exe	744	692	15	279	2010-09-02 12:25:22 UTC+0000
.... 0×82129370:svchost.exe	364	744	4	88	2010-09-02 12:25:33 UTC+0000
.... 0×821aa7e8:sqlwriter.exe	660	744	4	84	2010-09-02 12:25:36 UTC+0000
.... 0×8221e278:iscsiexe.exe	1436	744	6	78	2010-09-02 12:25:24 UTC+0000
.... 0×81e8a368:alg.exe	2588	744	6	107	2010-09-02 12:25:44 UTC+0000
.... 0×8214f488:svchost.exe	1192	744	13	175	2010-09-02 12:25:23 UTC+0000
.... 0×82189530:prl_tools_servi	436	744	3	78	2010-09-02 12:25:36 UTC+0000
..... 0×82086798:prl_tools.exe	632	436	9	107	2010-09-02 12:25:36 UTC+0000
.... 0×82151da0:svchost.exe	1084	744	58	1327	2010-09-02 12:25:22 UTC+0000
..... 0×8213dda0:wscntfy.exe	2180	1084	3	48	2010-09-02 12:25:41 UTC+0000
..... 0×8205dda0:wuauclt.exe	940	1084	4	126	2010-09-02 12:26:40 UTC+0000
..... 0×82311648:rundll32.exe	3768	1084	1	53	2010-09-09 19:56:33 UTC+0000
..... 0×81eab2f8:wuauclt.exe	3984	1084	8	325	2010-09-09 19:52:45 UTC+0000
.... 0×82095500:spoolsv.exe	1616	744	13	140	2010-09-02 12:25:24 UTC+0000
.... 0×82089558:jqs.exe	472	744	5	146	2010-09-02 12:25:33 UTC+0000
.... 0×822c8bf8:svchost.exe	992	744	10	277	2010-09-02 12:25:22 UTC+0000
.... 0×82150b90:svchost.exe	912	744	20	202	2010-09-02 12:25:22 UTC+0000
.... 0×8208abf0:sqlservr.exe	488	744	25	306	2010-09-02 12:25:33 UTC+0000
.... 0×82077da0: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 1
```

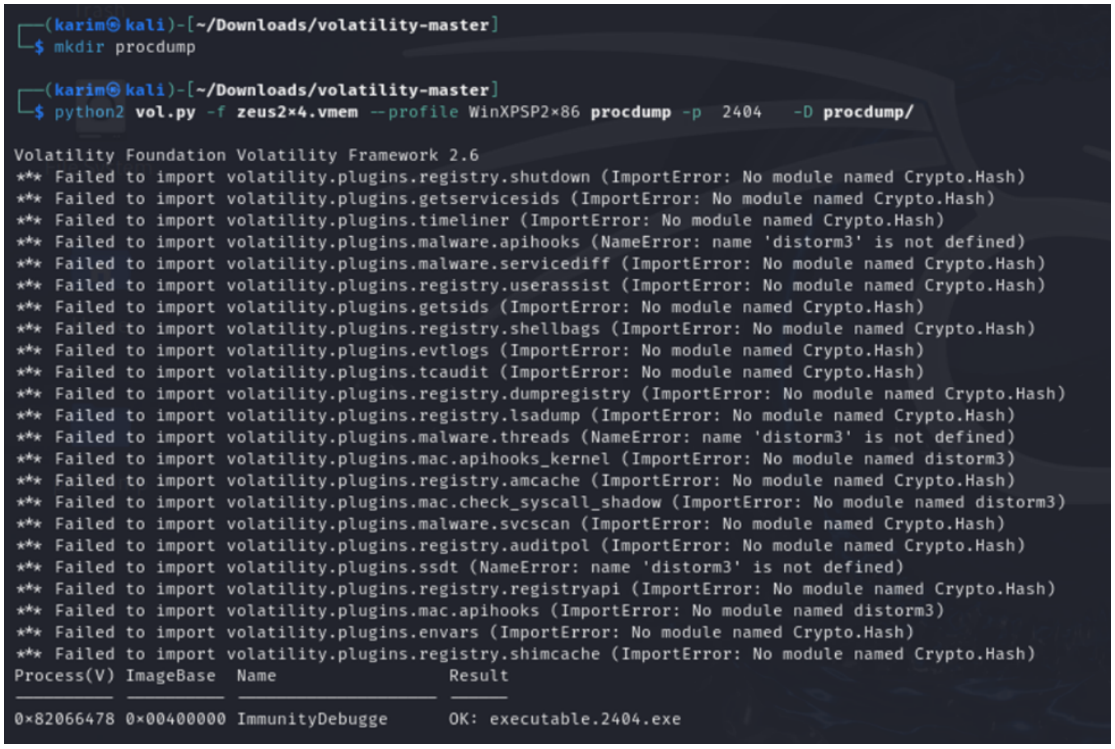


7. Dump Malicious Processes

> **First:** making directory for dumping (`mkdir procdump`).
> **Second:**
> we are going to dump the processes

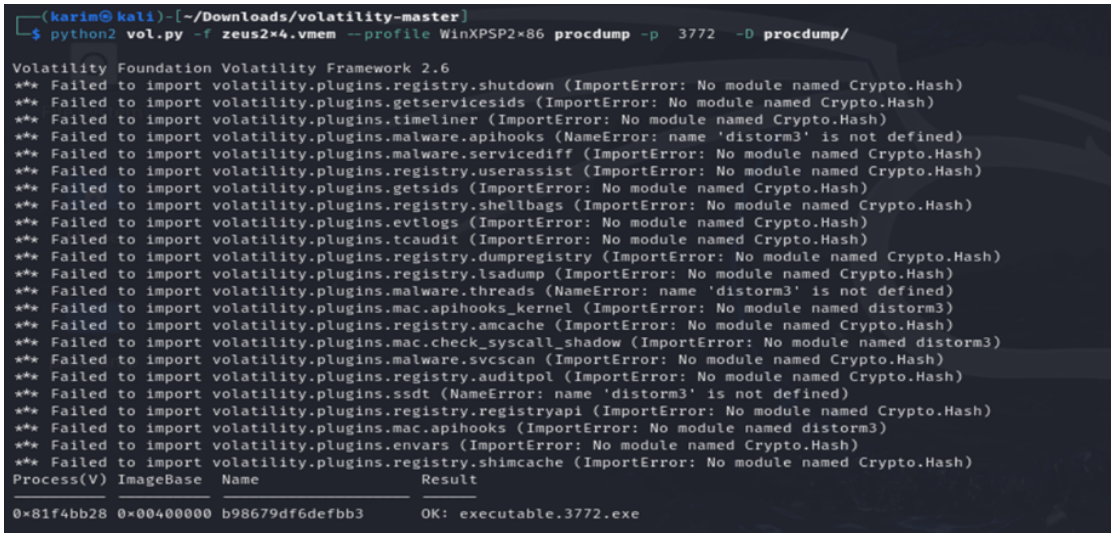
```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 procdump -p
2404   -D procdump/
```

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



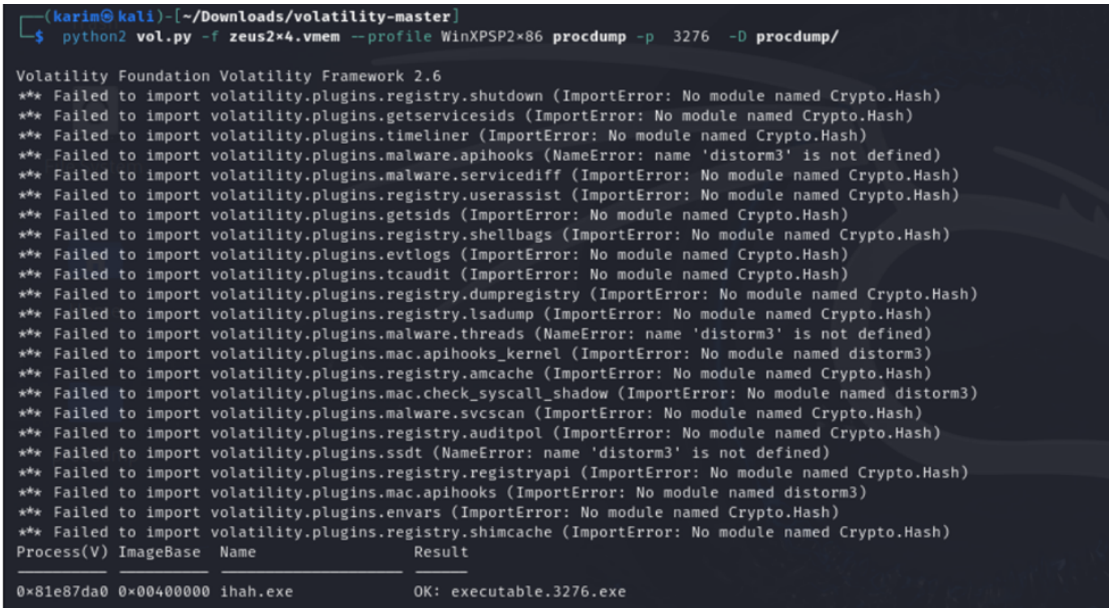
> Then we are going to dump process with pid `3772` which is `0x81f4bb28`:b98679df6defbb3 .

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



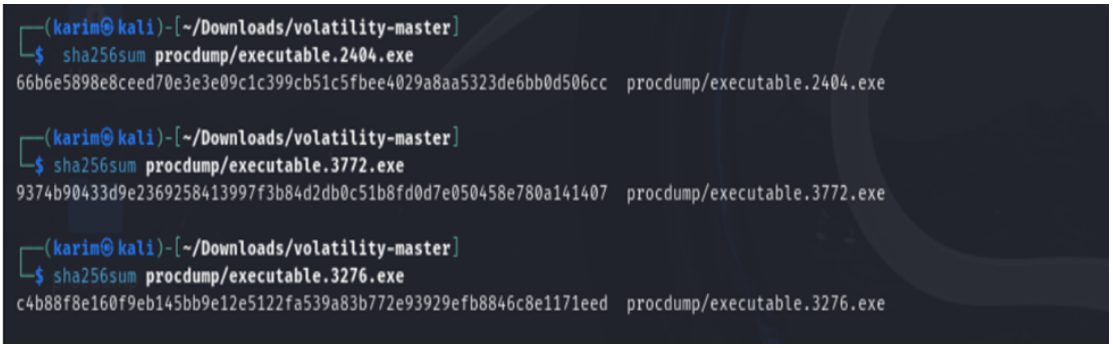
> Now and last process dump is process with pid `3276`

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

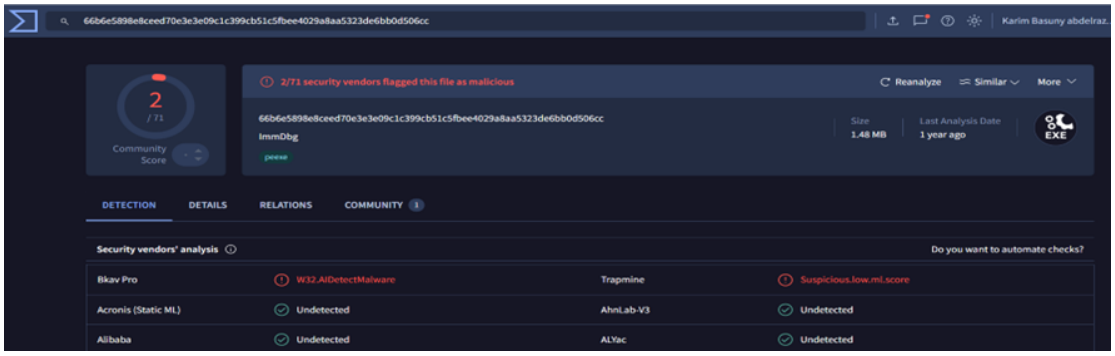


8. Getting the hash of dumped and check them on virus total.

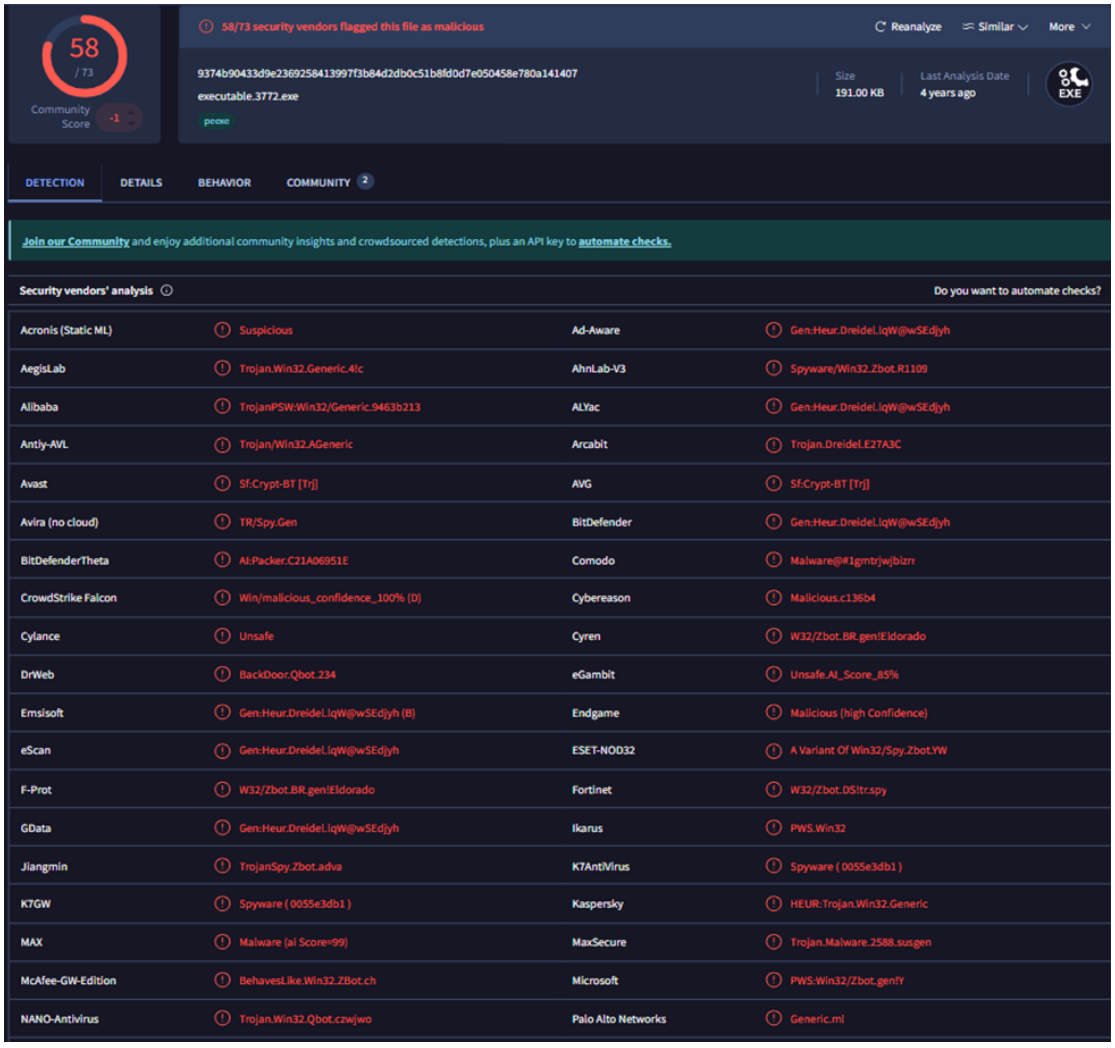
```
sha256sum procdump/executable.2404.exe
sha256sum procdump/executable.3772.exe
sha256sum procdump/executable.3276.exe
```



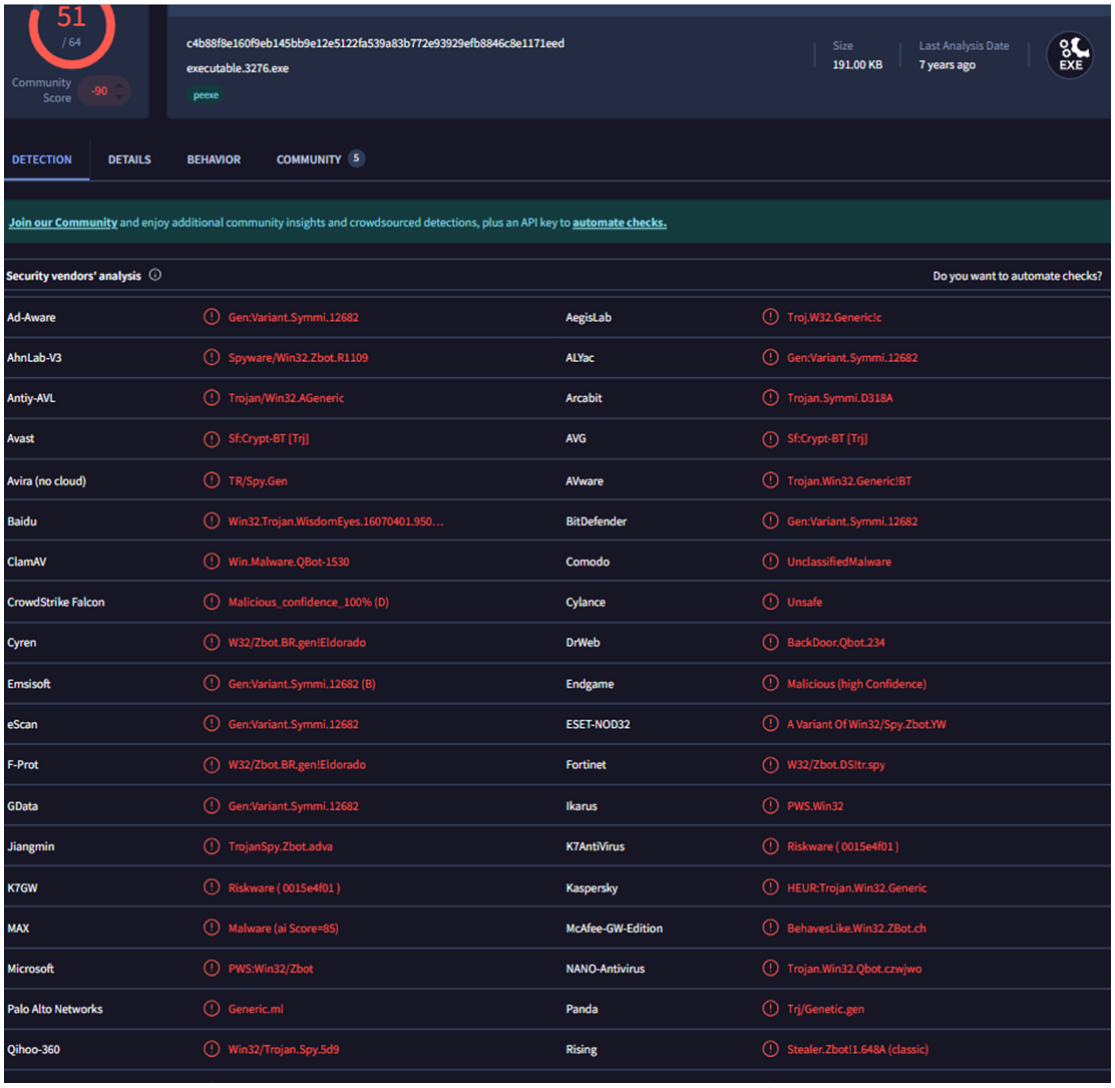
> First process of executable. `2404.exe`



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



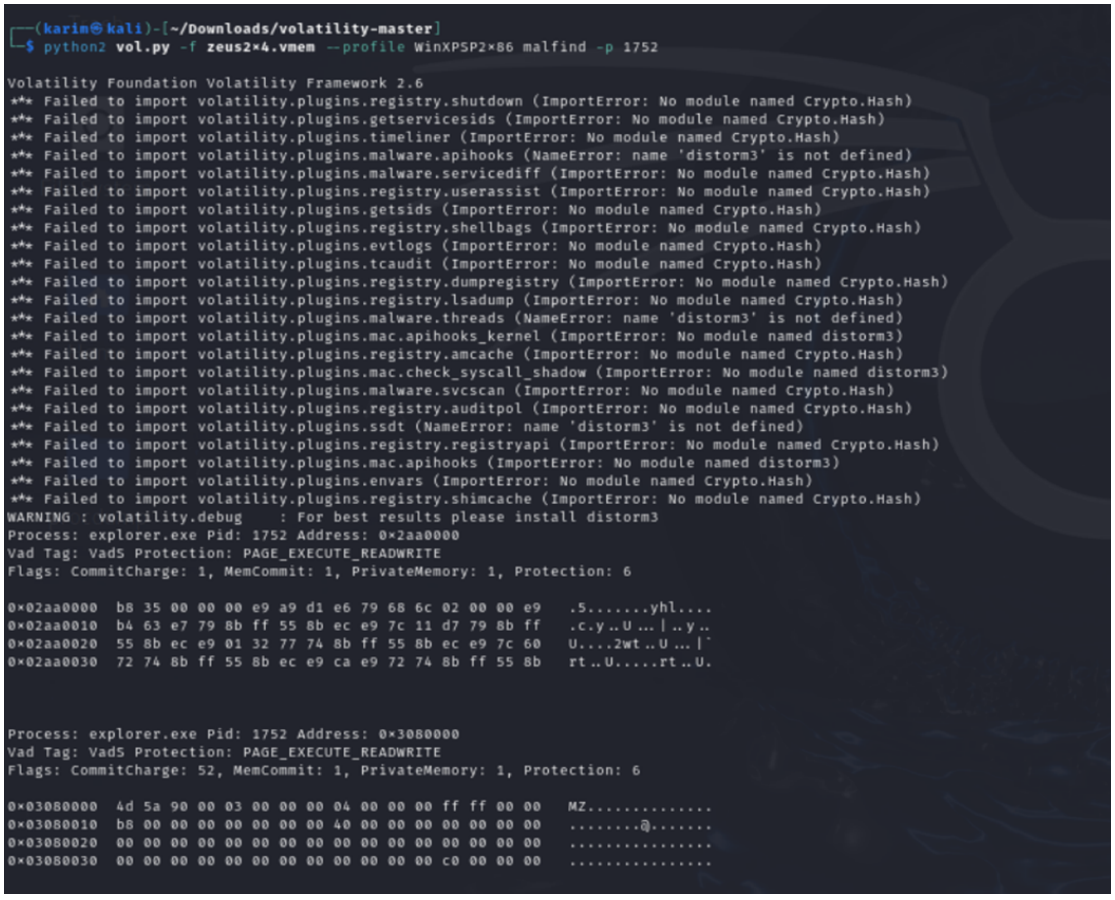
> Checking last hash of executable.3276.exe we will find that its also related to zbot.



9. Identifying Potential Malware

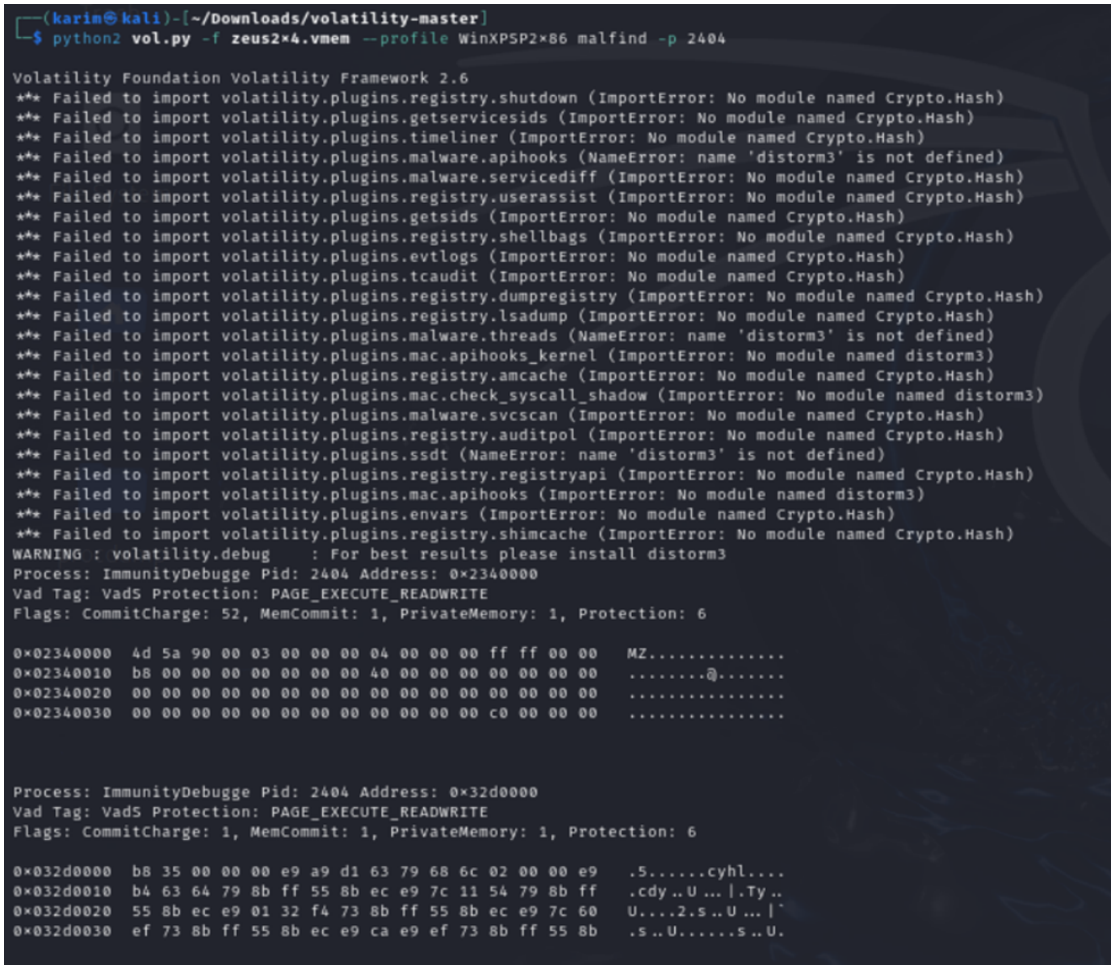
```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 175
```

> 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.



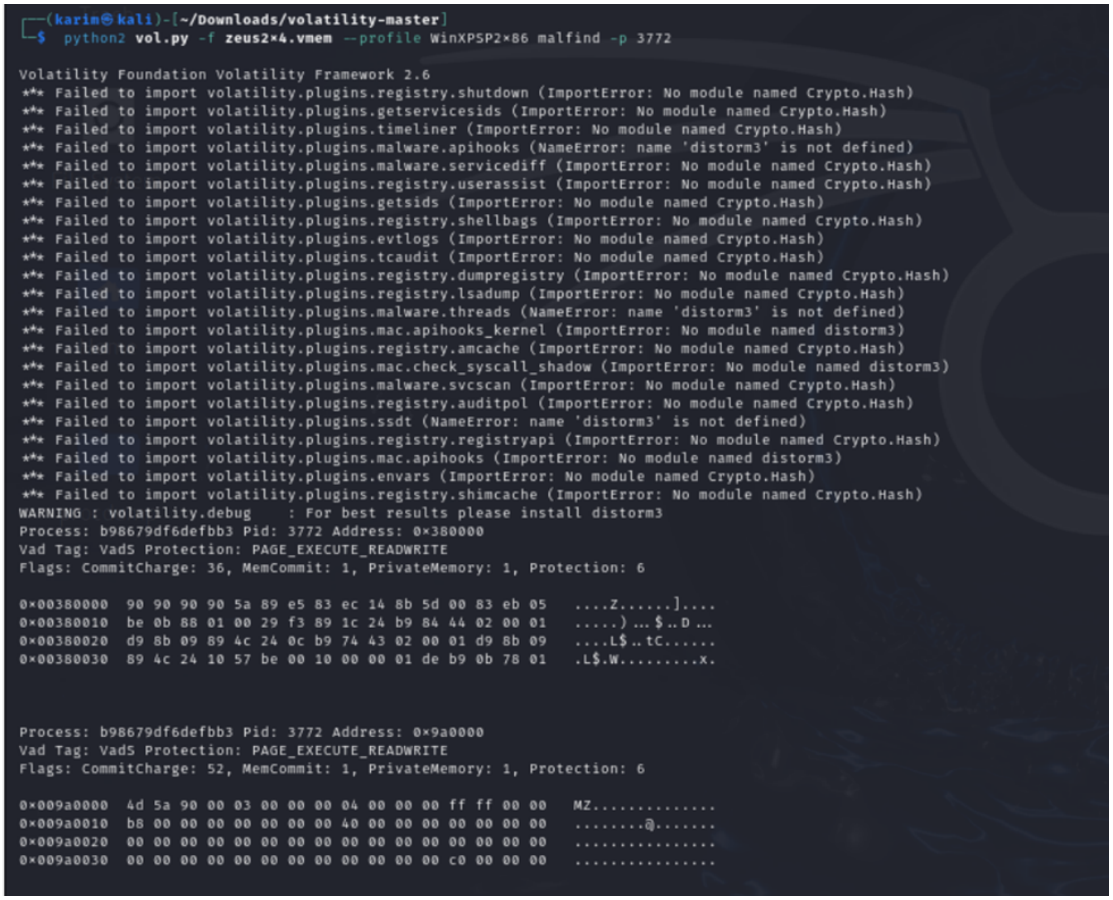
10. the same malfind but for pid `2404`

```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 240
```

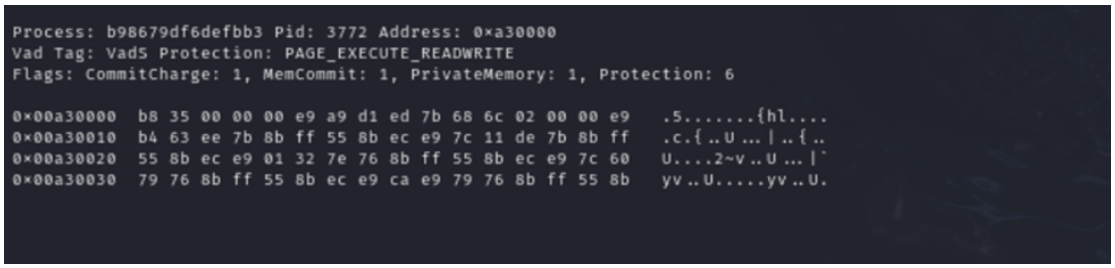


11. The same malfind but for pid `3772`

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



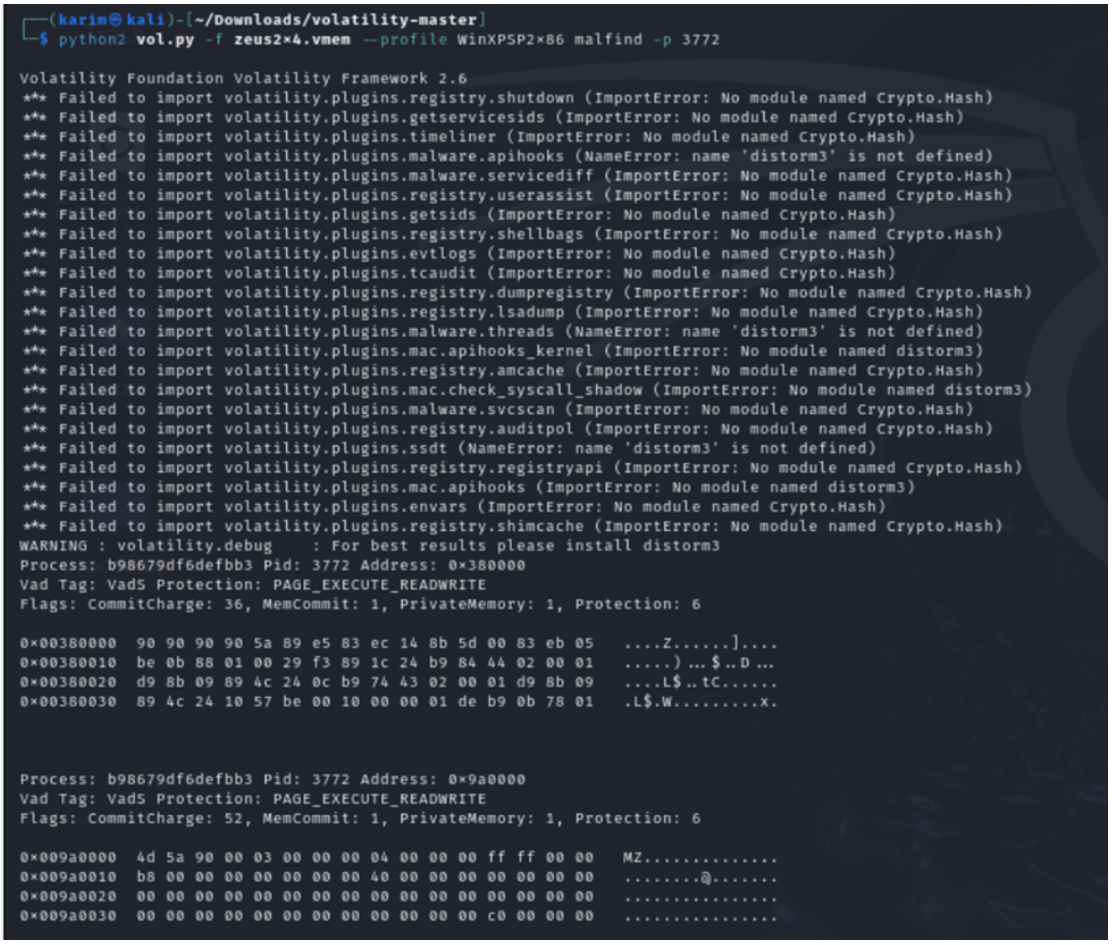
```
┌──(karim㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3772

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.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: VadS 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: 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 00 40 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   ................
```

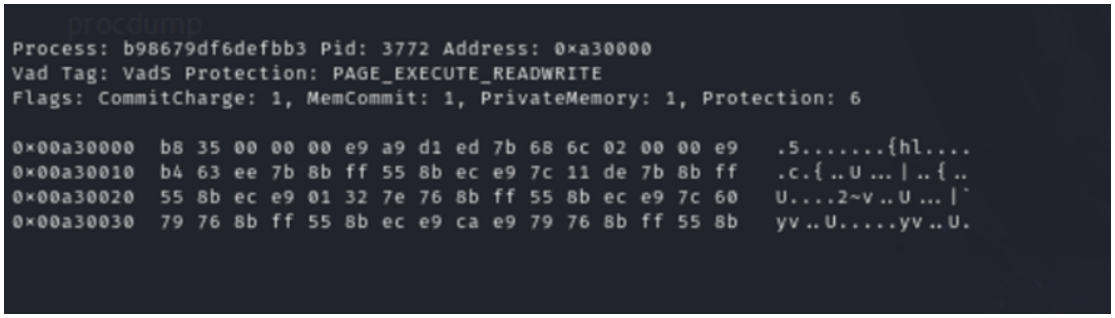


```
Process: b98679df6defbb3 Pid: 3772 Address: 0xa30000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

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
```





13. The same also but for pid `3772`

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

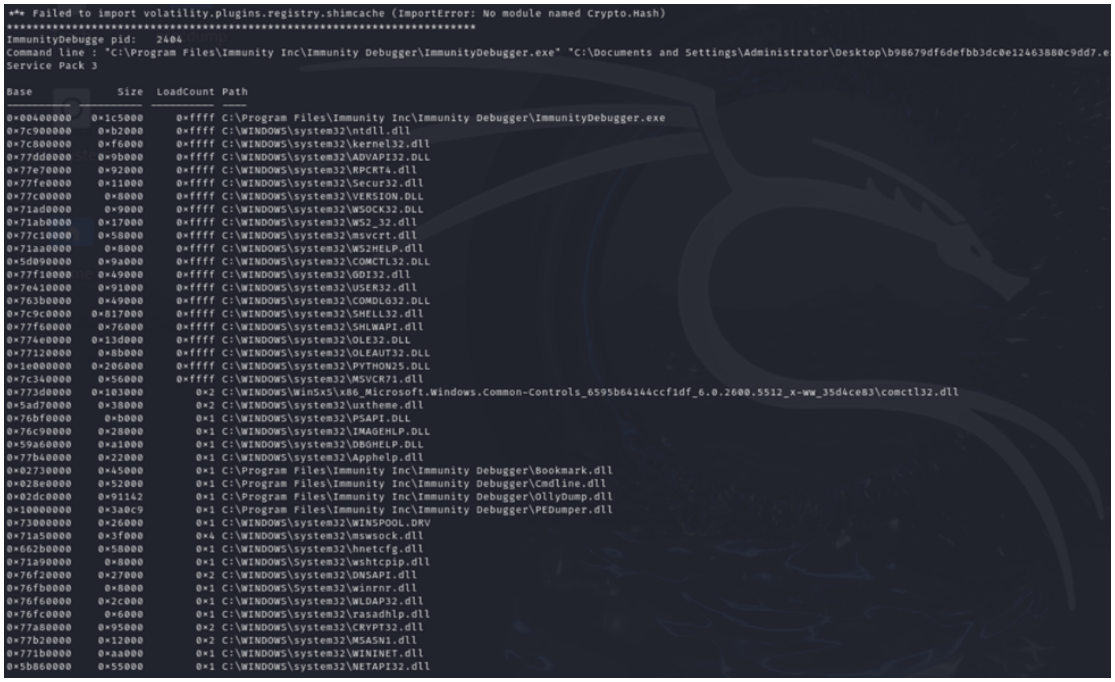
```
┌──(karim㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f zeus2×4.vmem --profile WinXPSP2×86 malfind -p 3276

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: ihah.exe Pid: 3276 Address: 0×380000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 37, MemCommit: 1, PrivateMemory: 1, Protection: 6

0×00380000  90 90 90 90 5a 89 e5 83 ec 14 8b 5d 00 83 eb 05   ....Z......]....
0×00380010  be 94 c2 00 00 29 f3 89 1c 24 b9 98 41 02 00 01   .....) … $ .. A …
0×00380020  d9 8b 09 89 4c 24 0c b9 30 46 02 00 01 d9 8b 09   ....L$ .. 0F......
0×00380030  89 4c 24 10 57 be 00 10 00 00 01 de b9 94 b2 00   .L$.W...........



Process: ihah.exe Pid: 3276 Address: 0×3f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0×003f0000  b8 35 00 00 00 e9 a9 d1 51 7c 68 6c 02 00 00 e9   .5......Q|hl....
0×003f0010  b4 63 52 7c 8b ff 55 8b ec e9 7c 11 42 7c 8b ff   .cR| .. U … |.B| ..
0×003f0020  55 8b ec e9 01 32 e2 76 8b ff 55 8b ec e9 7c 60   U....2.v .. U … |`
0×003f0030  dd 76 8b ff 55 8b ec e9 ca e9 dd 76 8b ff 55 8b   .v .. U......v .. U.
```

```
Process: ihah.exe Pid: 3276 Address: 0×9a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0×009a0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0×009a0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0×009a0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0×009a0030  00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00   ................
```

14. DLLIST scanning for processes

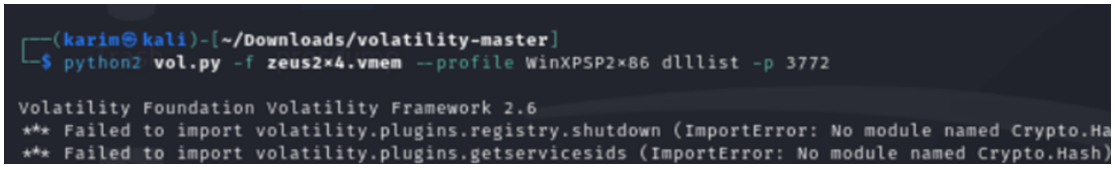
```
python2 vol.py -f zeus2x4.vmem --profile WinXPSP2x86 dlllist -p 240
```

```
┌──(karim㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f zeus2×4.vmem --profile WinXPSP2×86 dlllist -p 2404
```



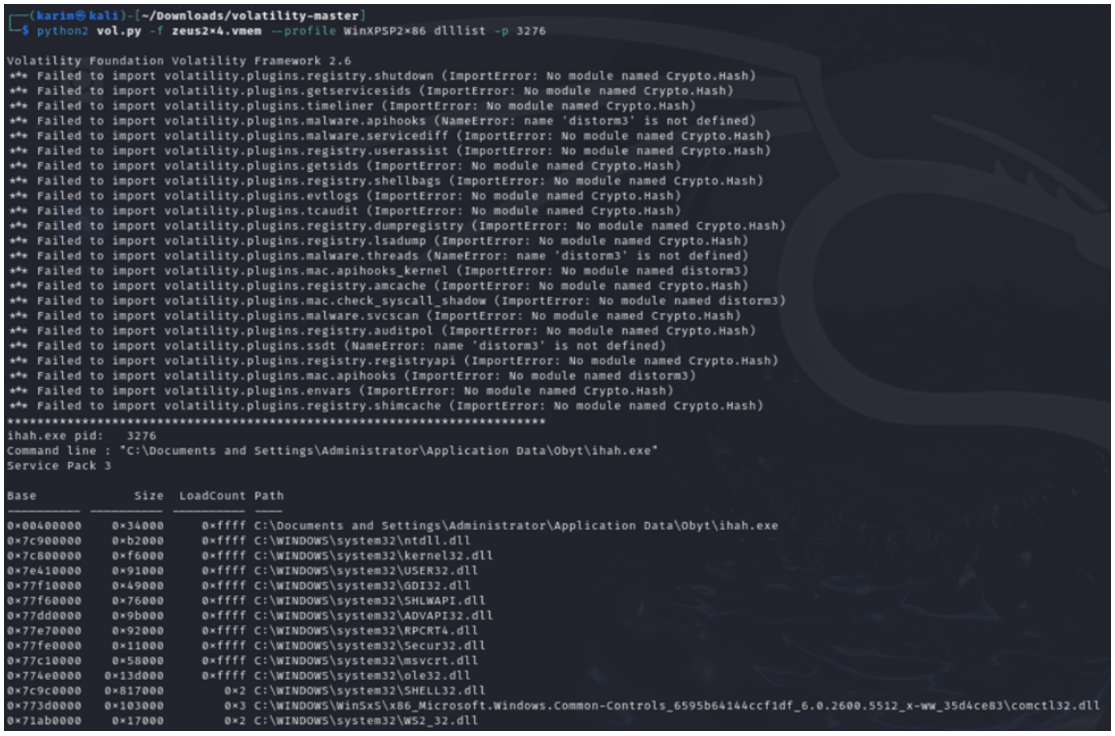
The same dlllist but for pid `3772`

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



The same dlllist but for pid `3276`:

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



> 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.