HOMEWORK 1

GROUP NO. 10

A Atulya Sundaram (210001)
Dhiraj Pareek (231110012)
Akash Shivaji Varude (231110006)

QUESTION_1

a) Top 5 countries where devices or systems with OpenSSH run on non-default ports.

Shodan query: **OpenSSH !port:"22"**

Here's the list of the top 5 countries:

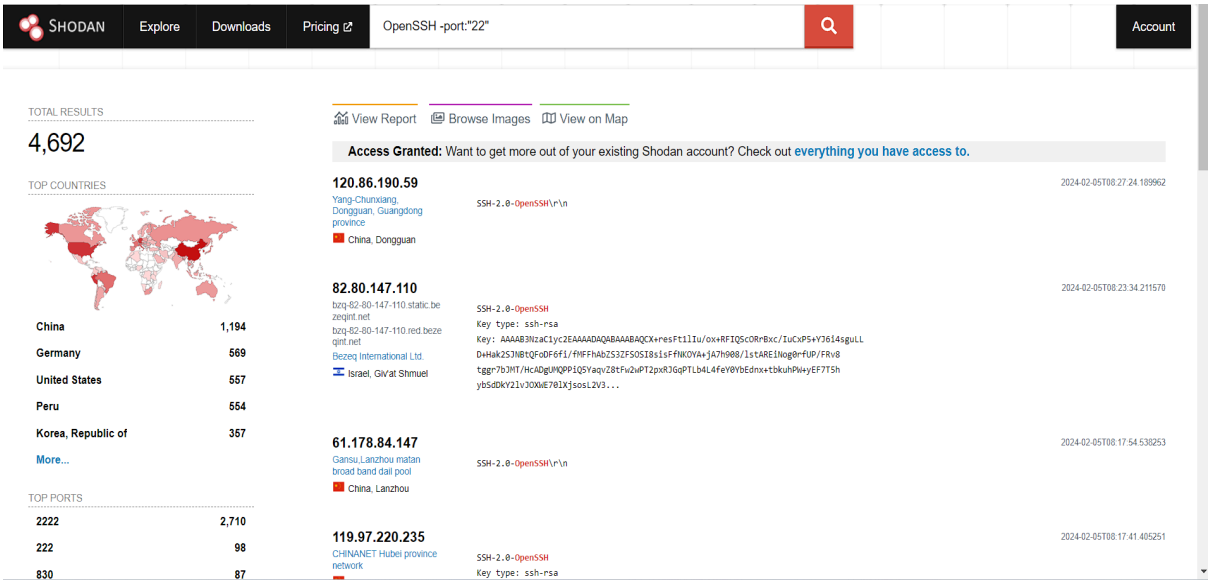
1.China

2. Germany

3. United States

4. Peru

5. Korea, Republic of Korea

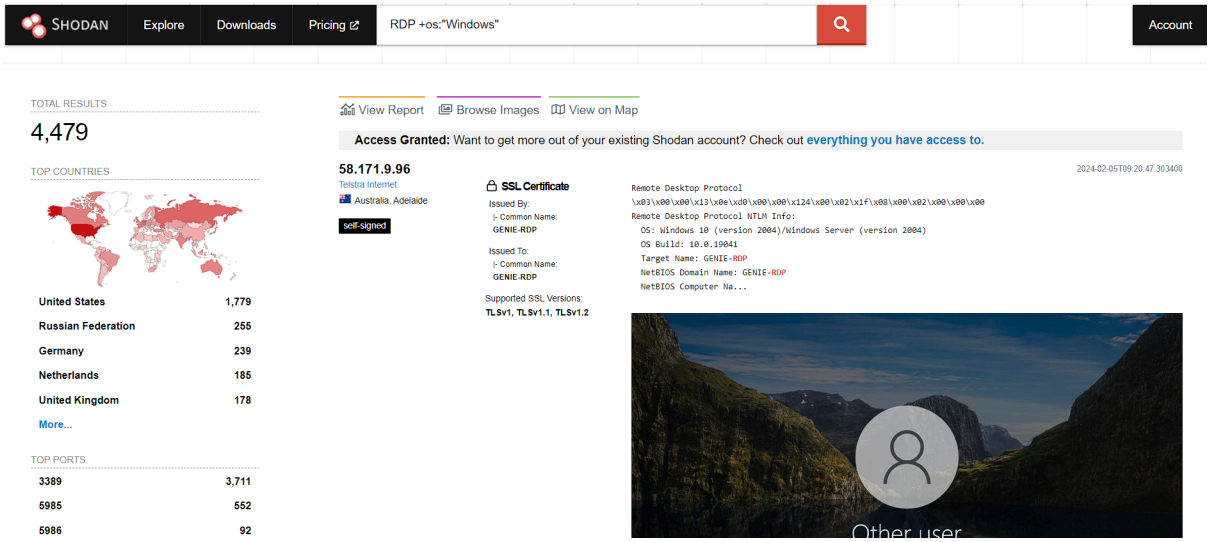


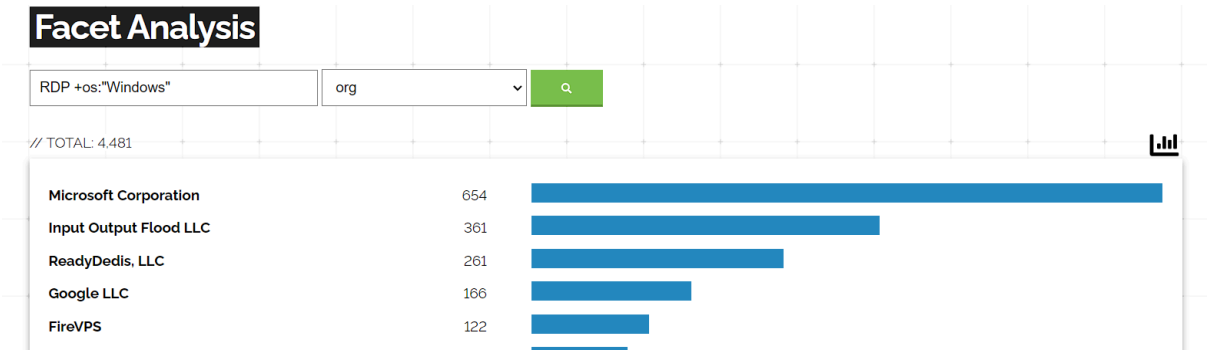
b) Top 5 organisations where RDP services are running on Windows operating systems.

Shodan query: **RDP +os:"Windows"**

Here's the list of the top 5 Organisations:

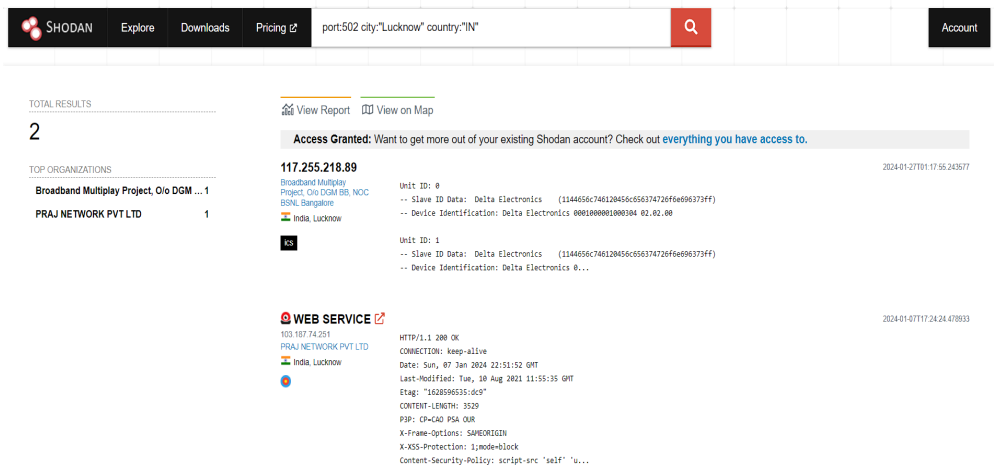
1. Microsoft Corporation
2. Input Output Flood LLc
3. ReadyDedis, LLC
4. Google LLC
5. FireVPS



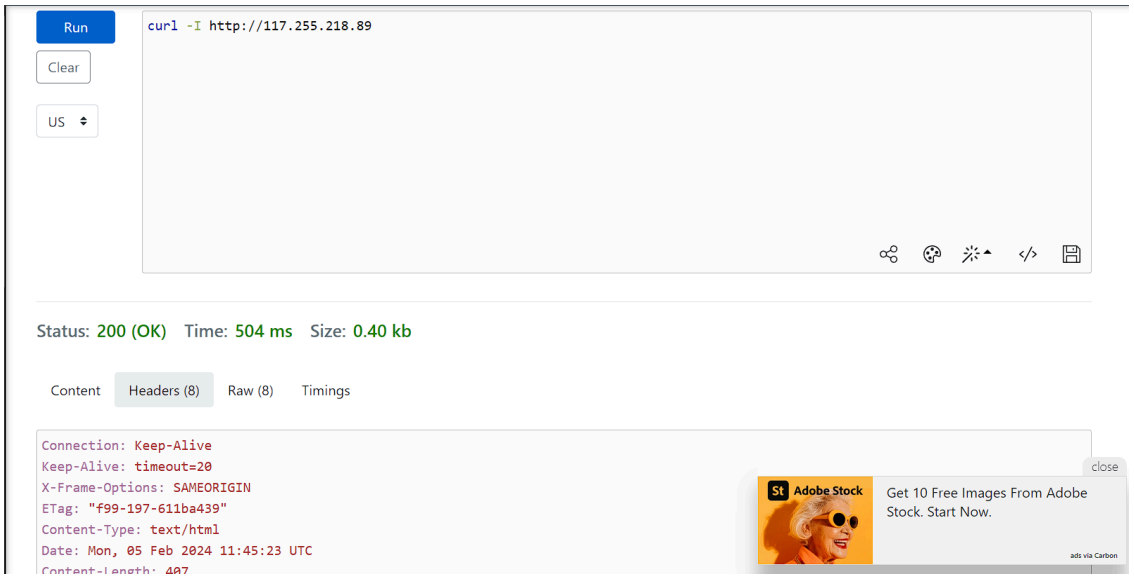


c) Search for devices in Lucknow, India, using the Modbus protocol and retrieve the Entity Tag header information in an HTTP response if you find any :

Shodan Query : **port:502 city:"Lucknow" country:"IN"**



Entity tag Header for **PRAJ NETWORK PVT LTD** is Etag: "1628596535:dc9" Entity tag for Broadband Multiplay Project is not present in Shodan but it can be found by sending http request on that IP address using curl .



Entity tag Header for **Broadband Multiplay Project** is Etag: "f99-197-611ba439"

QUESTION 2: CHECKING PERSISTANCE

1.exe :

1) Yes, File is persistent
2) **Reason:** We checked using RegShot as well as Task Manager. First of all there were no changes in the Task Manager. There were no persistent executables in the Task Manager once the executable (1.exe) finished executing.

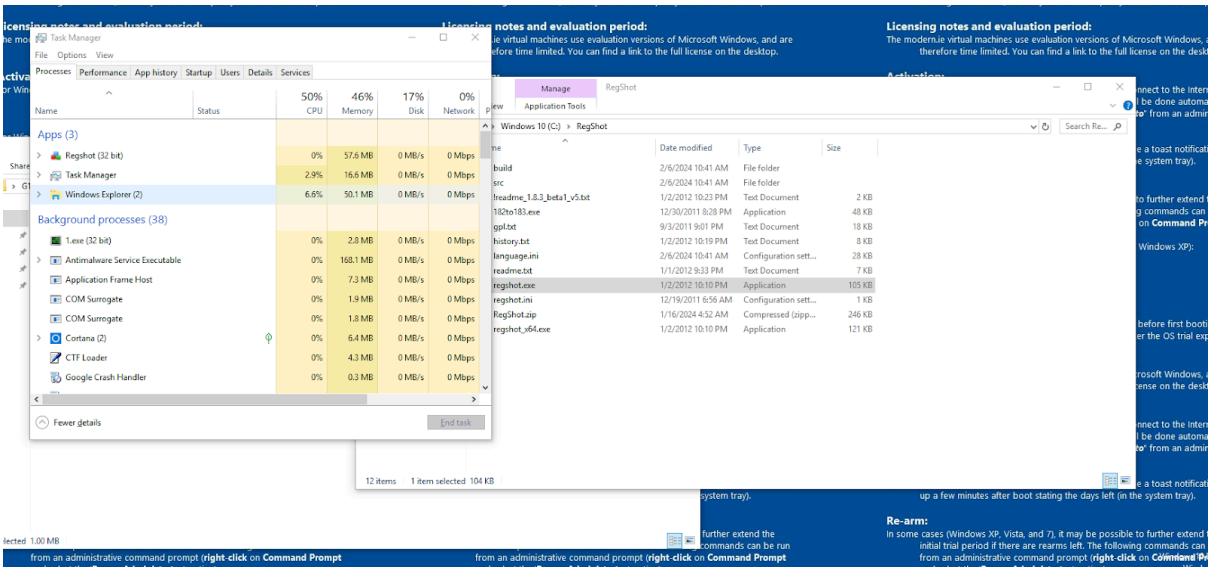


Fig. Before

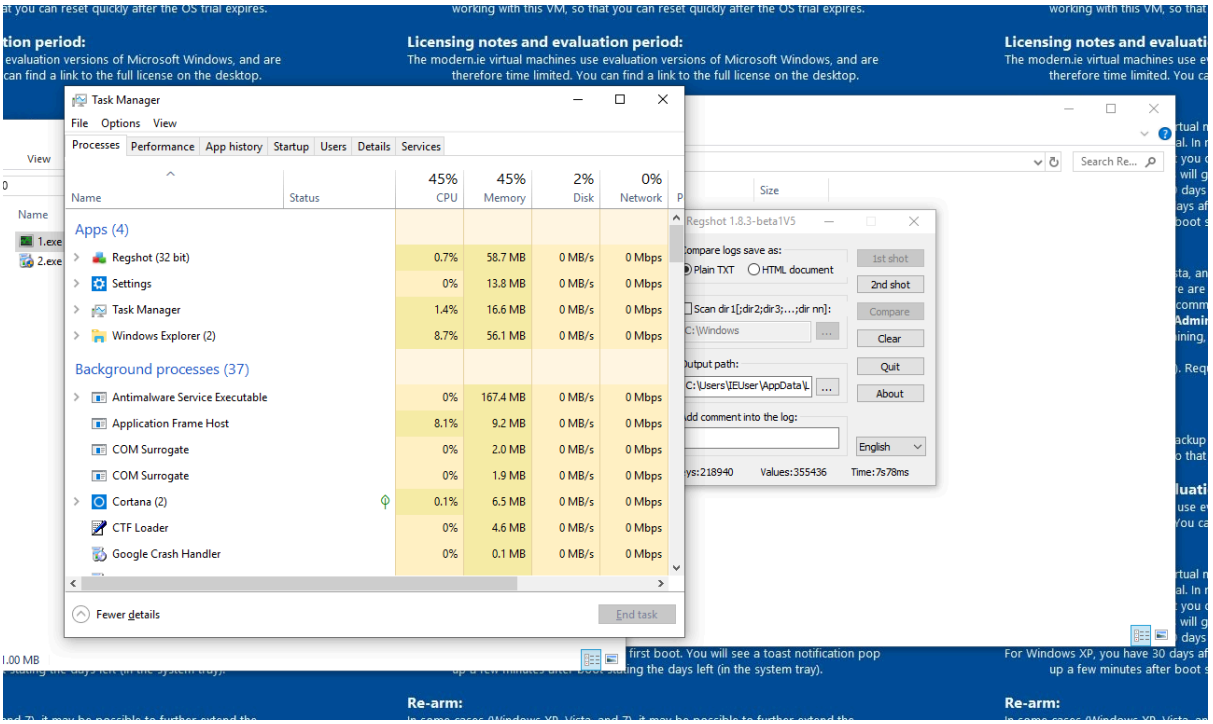
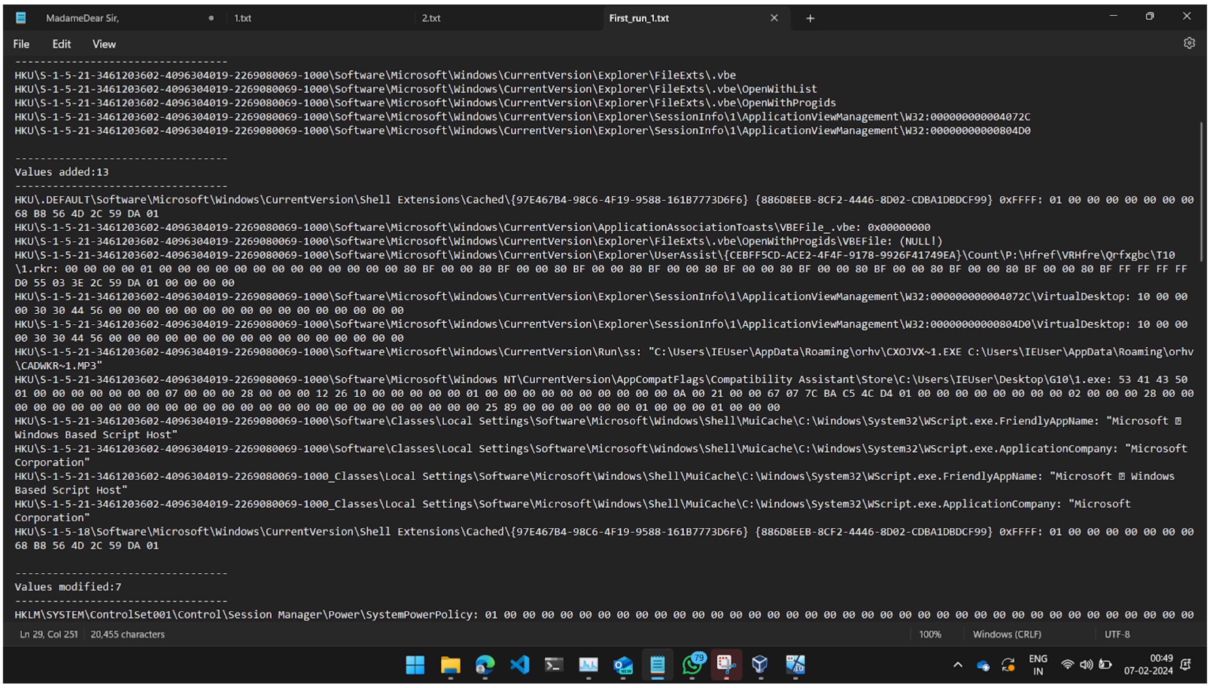


Fig. After

However, this is not sufficient to determine persistence. Thus, RegShot was used to check upon the Windows Registry.



Here, we find that the executable has been added to the Run registry. This is indicated by the following line:

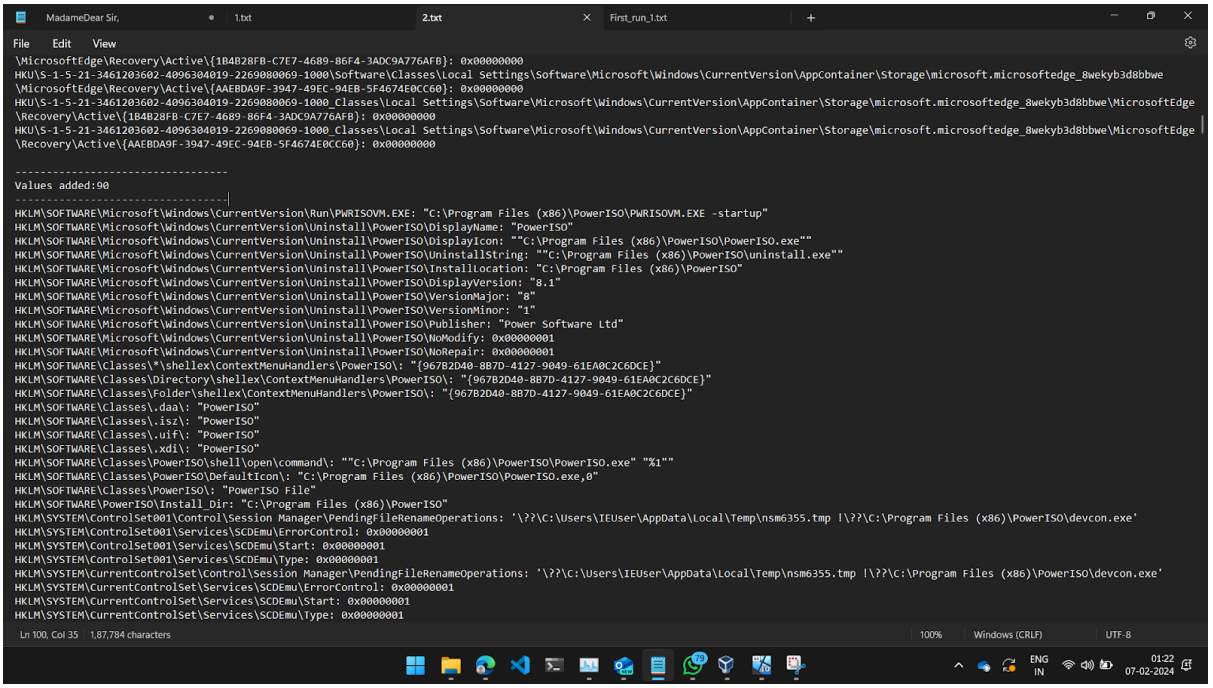
HKU\S-1-5-21-3461203602-4096304019-2269080069-1000\Software\Microsoft\Windows\CurrentVersion\Run\ss: "C:\Users\IEUser\AppData\Roaming\orhv\CXOJVX~1.EXE C:\Users\IEUser\AppData\Roaming\orhv\CADWKR~1.MP3"

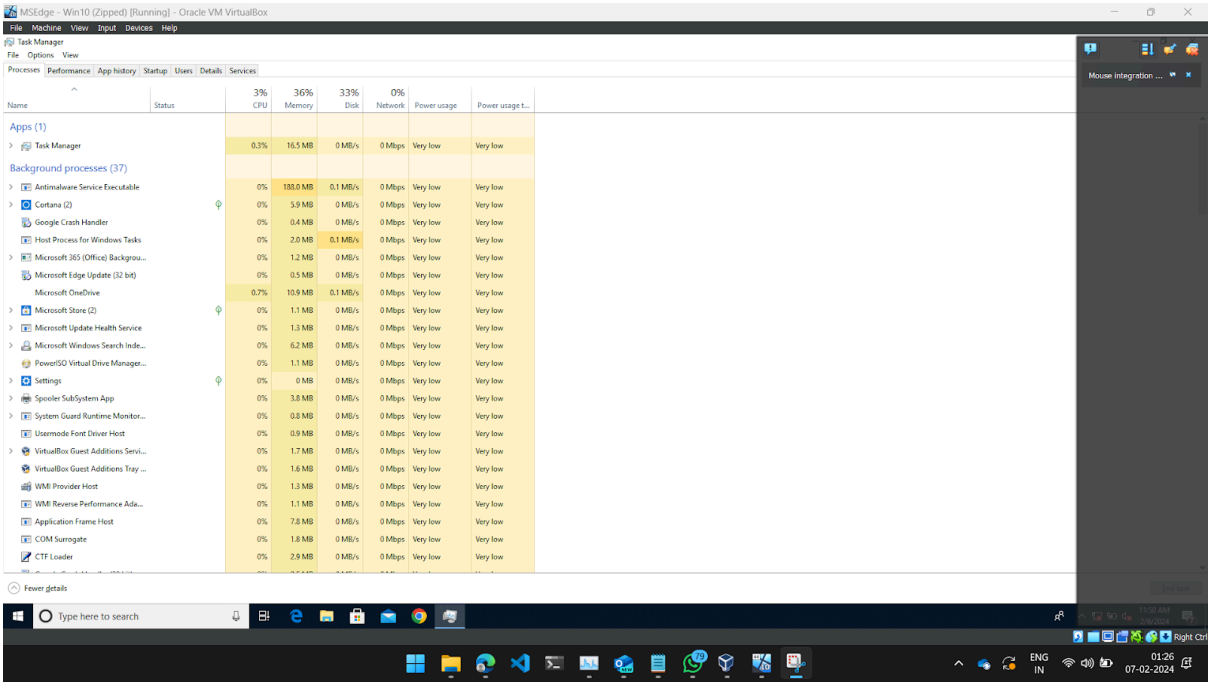
Upon checking what the Run Registry Key indicates, we see that Run registry key is used to make a program run when a user logs on, every time he/she logs on. This persists even after a reboot.

Hence the given malware is **persistent**.

2.exe:

1) Yes, it exhibits persistence of some kind
2) **Reason**: The given executable is the installation for POWERISO. Checking the RegShot Logs we can again see a similar value as above being added to the RUN command.





This time, the persistence is also visible in Task Manager (note PowerISO Virtual Drive Manager). The above has been taken after a reboot.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PWRISOVM.EXE: "C:\Program Files (x86)\PowerISO\PWRISOVM.EXE -startup"

The above line indicates **persistence.**

QUESTION 3: MALWARE ANALYSIS

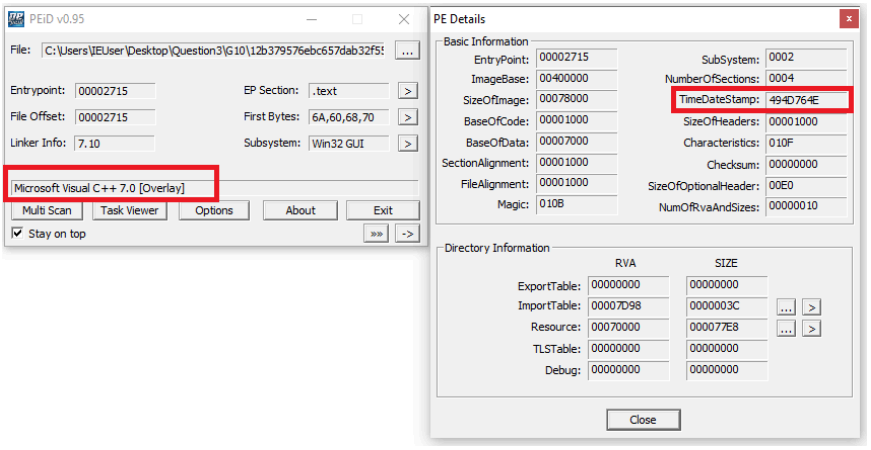
PART 1: ANALYSIS USING PEid TOOL

Executable No. 1) (The file of size 552kb)

a) Analyse the structure of executable files and identify the packers or compilers used in their creation (If any).

It appears the microsoft visual c++ 7.0 compiler is used

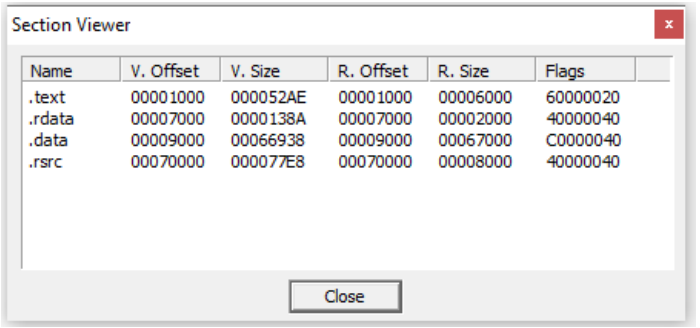
Also TimeDateStamp is 494D764E. If this is converted to human date and time format then it Date of creation is Saturday, December 20, 2008 10:48:46 PM



b) Find the following details from the EP Section: count the number of PE sections from the section viewer and also point out any suspicious PE section name with an explanation.

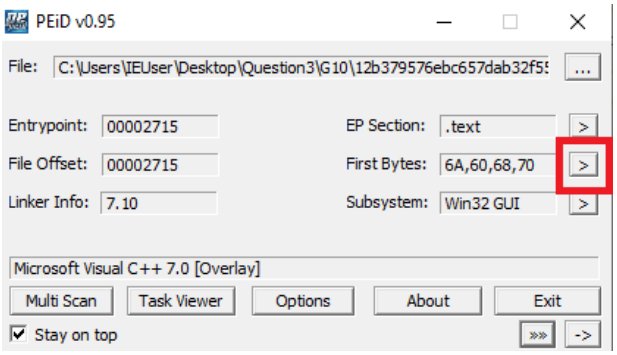
There are 4 PE Sections in Section Viewer. Namely ".text, .rdata, .data, .rsrc"

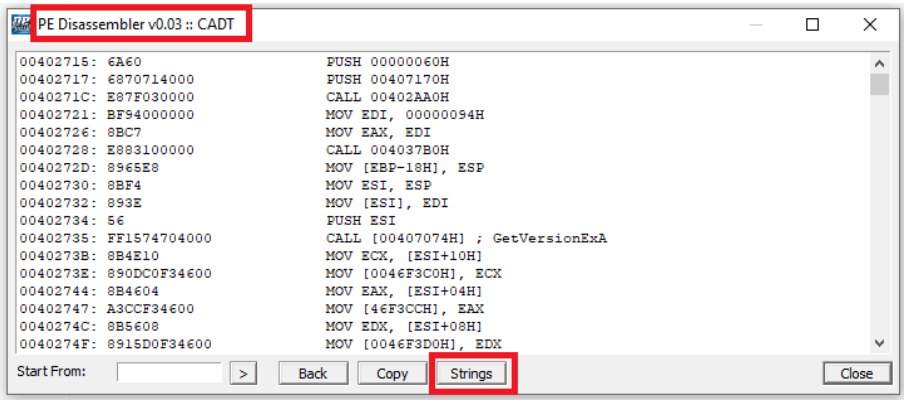
None of those appear to be suspicious



c) In which section of the PEid Tool will you find the PE disassembler and strings information?

I find out PE disassembler and strings information in 'by clicking on '>' which is in front of First Byte'

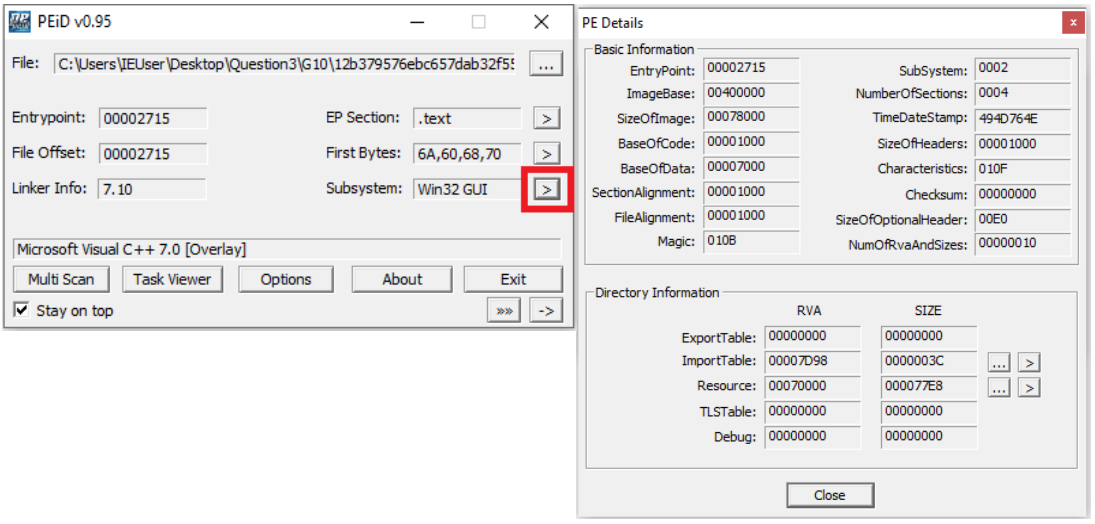




d) In which section of the PEid Tool will you find the PE details?

PE details like Entrypoint, File Offset, Linker Info, Subsystem are available in the analysis summary presented immediately after selecting the file for analysis

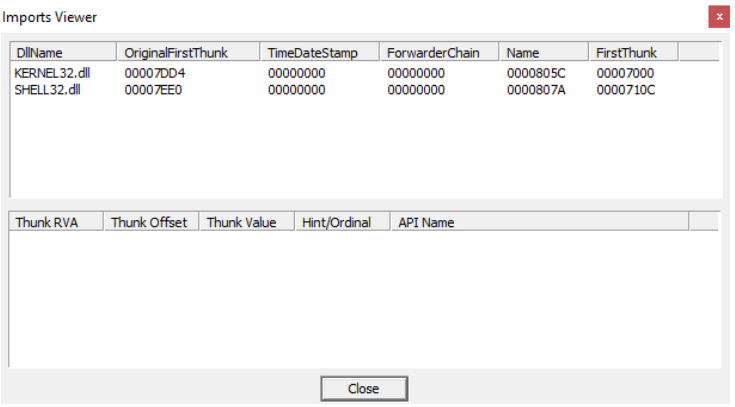
However more details are available in > in front of Subsystem



e) Count the number of DLL imports with the DLL names from the PE details

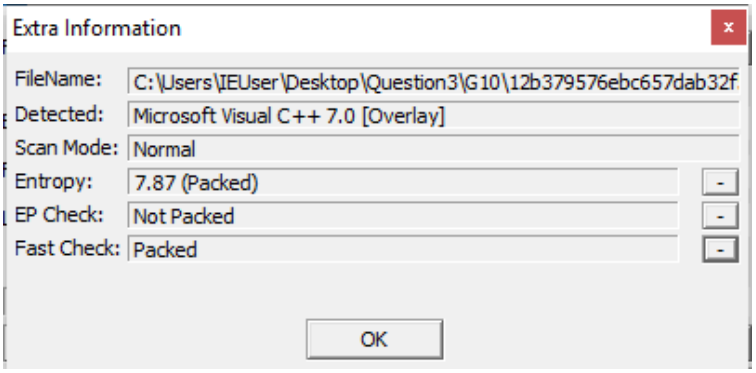
There are 2 DLL Imports

KERNEL32.dll and SHELL32.dll



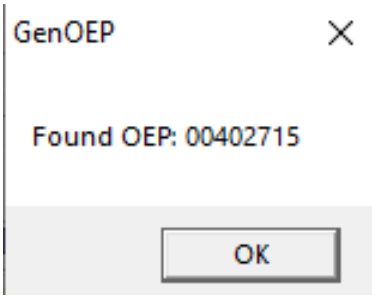
f) Goto Extra Information section of the PEid Tool, click on the (-) icon and calculate the Entropy, EP check output, and Fast check output.

Entropy: 7.87 (packed), EP Check : Not Packed, Fast Check: Packed



g) Goto plugin and find the Original Entry Point (OEP) of a packed executable, if any:

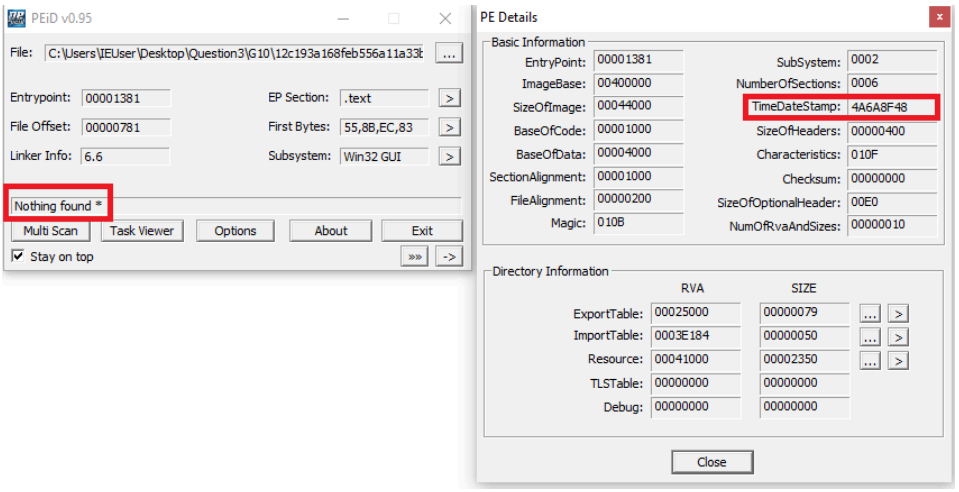
Found OEP: 00402715



Executable No. 2) (The file of size 133kb)

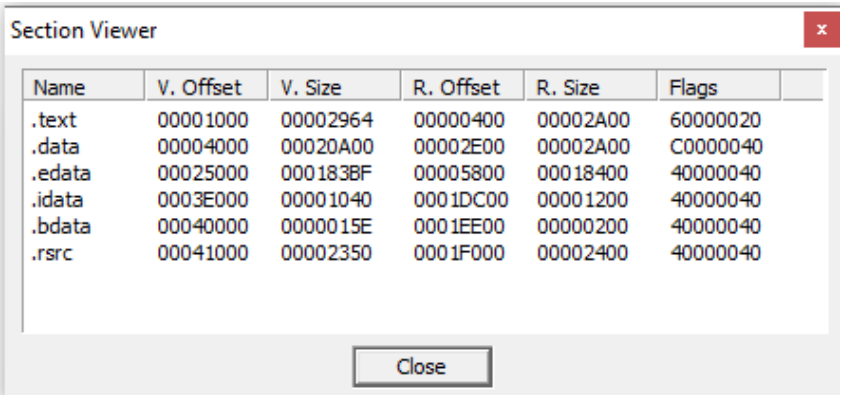
a. **Analyse the structure of executable files and identify the packers or compilers used in their creation (If any).**

Though we can see PEid can't detect compiler, there is still a linker info: 6.6
So compiler could be microsoft visual c++
DateTimeStamp is 4A6A8F48 which is Saturday, July 25, 2009 4:51:20 AM is time and date of creation



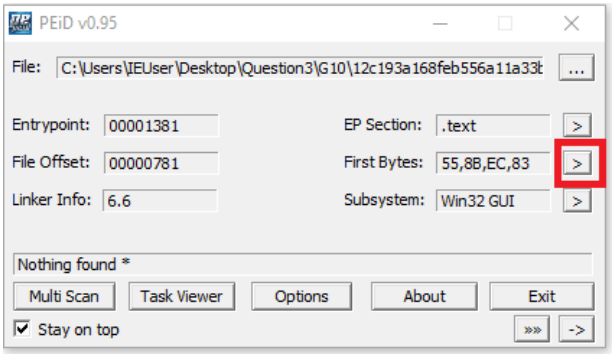
b. **Find the following details from the EP Section: count the number of PE sections from the section viewer and also point out any suspicious PE section name with an explanation.**

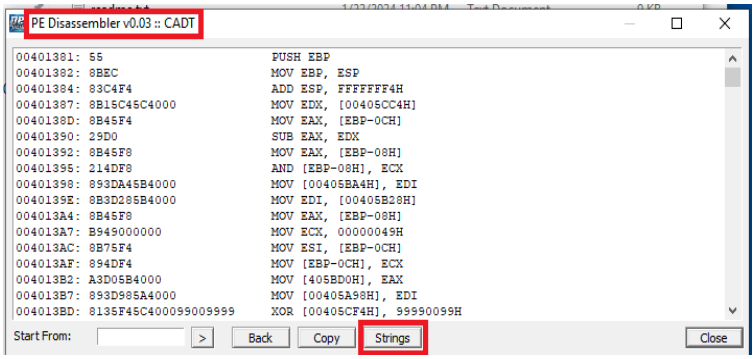
There are 6 PE Sections in Section Viewer. Namely ".text, .edata, .idata, .bdata, .data, .rsrc"
None of those appear to be suspicious



c. In which section of the PEid Tool will you find the PE disassembler and strings information?

I find out PE disassembler and strings information in 'by clicking on '>' which is in front of First Byte'

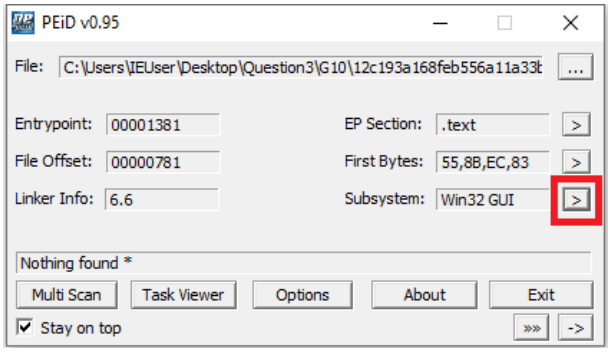


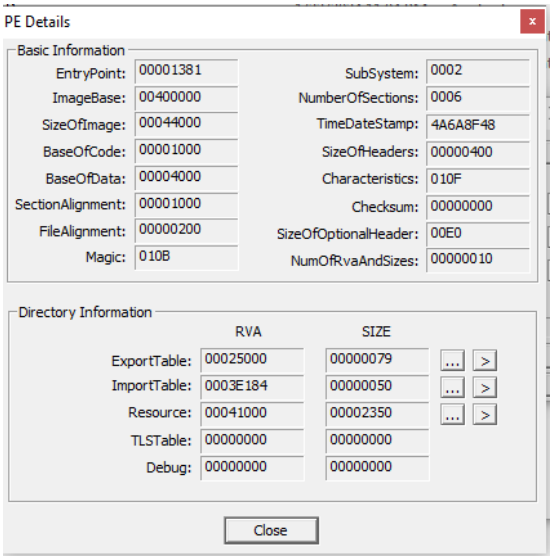


d. In which section of the PEid Tool will you find the PE details?

PE details like Entrypoint, File Offset, Linker Info, Subsystem are available in the analysis summary presented immediately after selecting the file for analysis

However more details are available in > in front of Subsystem

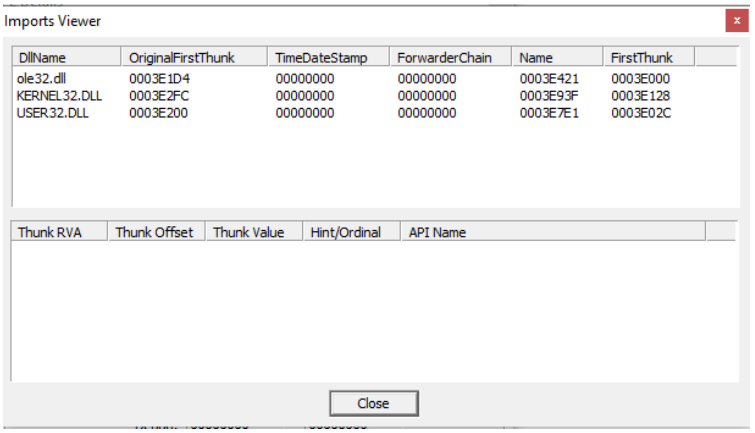




e. Count the number of DLL imports with the DLL names from the PE details

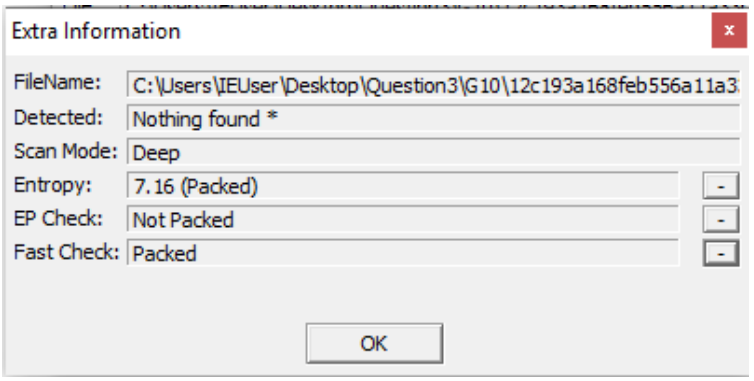
There are 3 DLL Imports

ole32.dll, KERNEL32.dll and USER32.dll



f. Goto Extra Information section of the PEid Tool, click on the (-) icon and calculate the Entropy, EP check output, and Fast check output.

Entropy: 7.16 (packed), EP Check : Not Packed, Fast Check: Packed



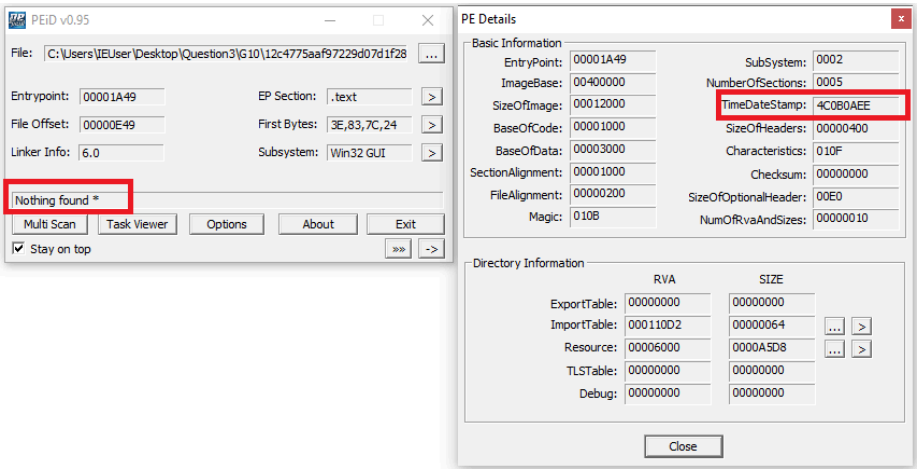
g. Goto plugin and find the Original Entry Point (OEP) of a packed executable, if any:

No OEP found

Executable No. 3) (The file of size 53kb)

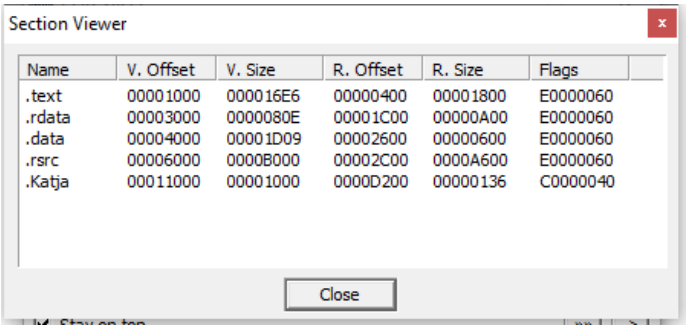
a) Analyse the structure of executable files and identify the packers or compilers used in their creation (If any).

Though we can see PEid can't detect compiler, there is still a linker info: 6.0
So compiler can be microsoft visual c++ with linker version 6.0
DateTimeStamp is 4C0B0AEE which is Saturday, Sunday, June 6, 2010 2:41:50 AM is time and date of creation



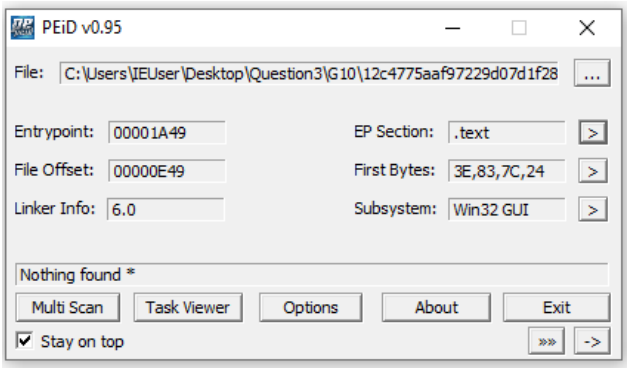
b) Find the following details from the EP Section: count the number of PE sections from the section viewer and also point out any suspicious PE section name with an explanation.

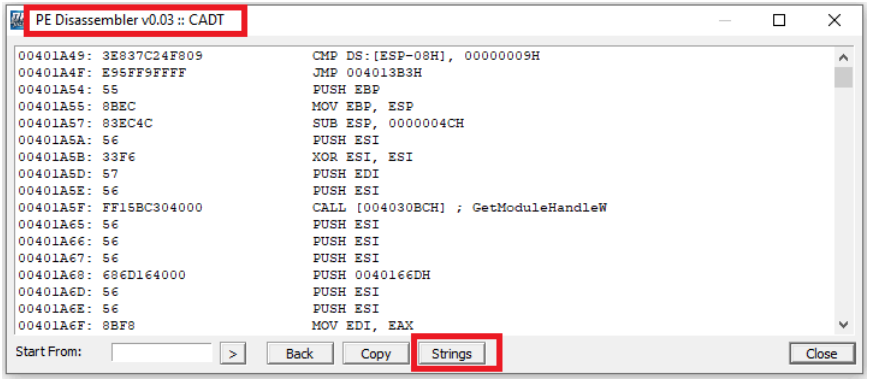
There are 5 PE Sections in Section Viewer. Namely ".text, .rdata, .data, .Katja, .rsrc"
None of those appear to be suspicious



c) In which section of the PEid Tool will you find the PE disassembler and strings information?

I find out PE disassembler and strings information in 'by clicking on '>' which is in front of First Byte'

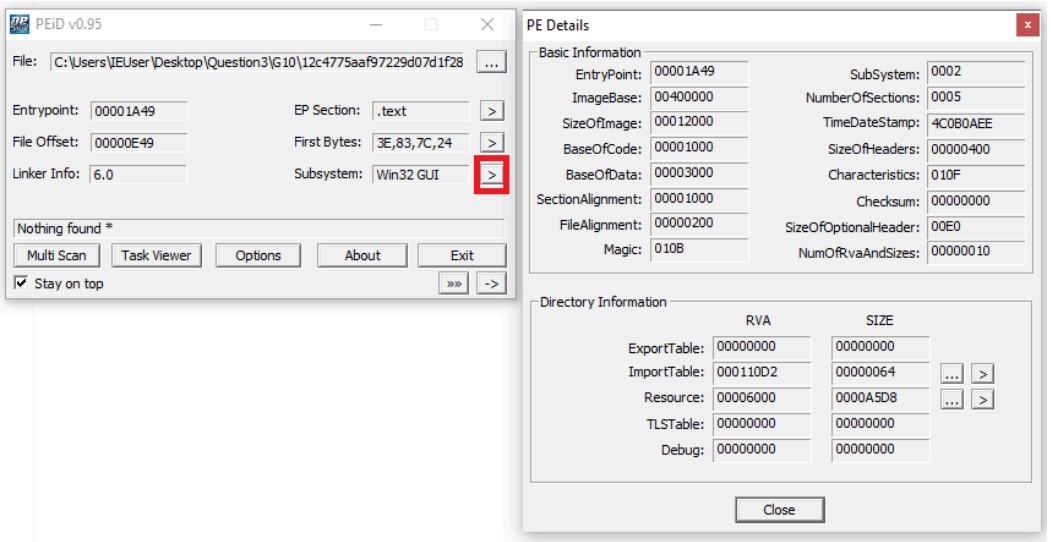




d) In which section of the PEid Tool will you find the PE details?

PE details like Entrypoint, File Offset, Linker Info, Subsystem are available in the analysis summary presented immediately after selecting the file for analysis

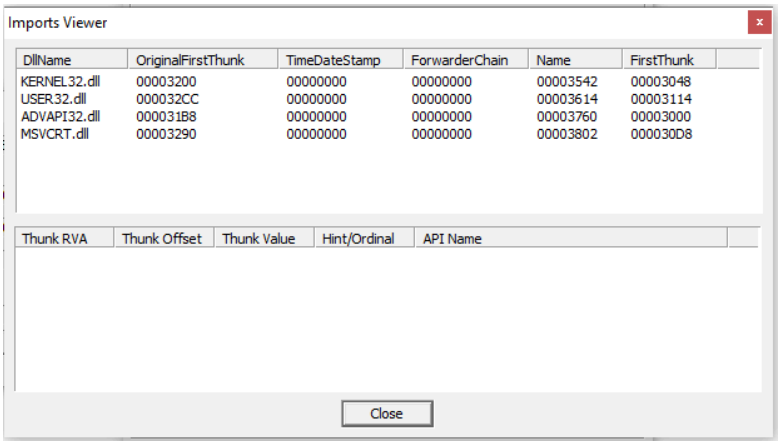
However more details are available in > in front of Subsystem



e) **Count the number of DLL imports with the DLL names from the PE details**

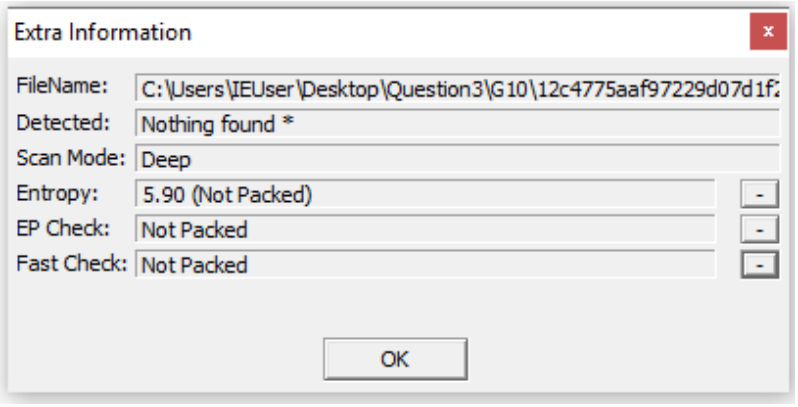
There are 4 DLL Imports

KERNEL32.dll , USER32.dll, ADVAPI32.dll, MSVCRT.dll



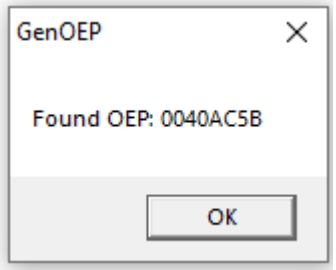
f) **Goto Extra Information section of the PEid Tool, click on the (-) icon and calculate the Entropy, EP check output, and Fast check output.**

Entropy: 5.90 (Not packed), EP Check : Not Packed, Fast Check: Packed



g) **Goto plugin and find the Original Entry Point (OEP) of a packed executable, if any:**

OEP found: 0040AC5B

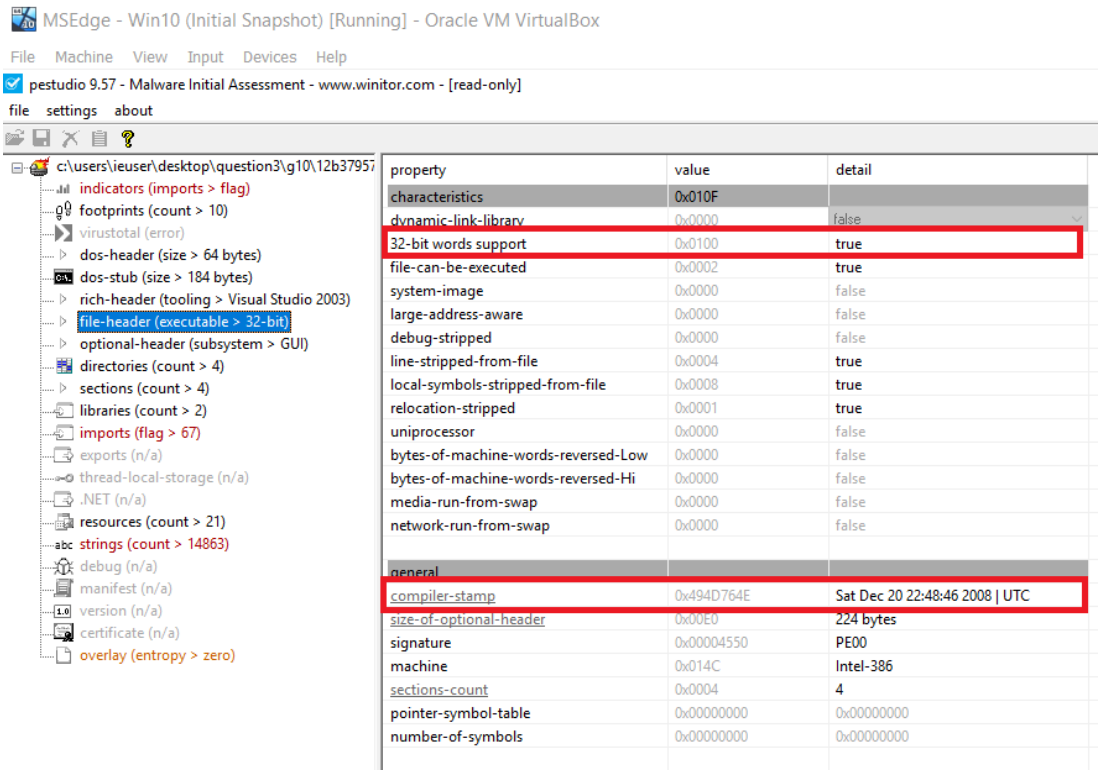


PART 2: ANALYSIS USING PESttudio

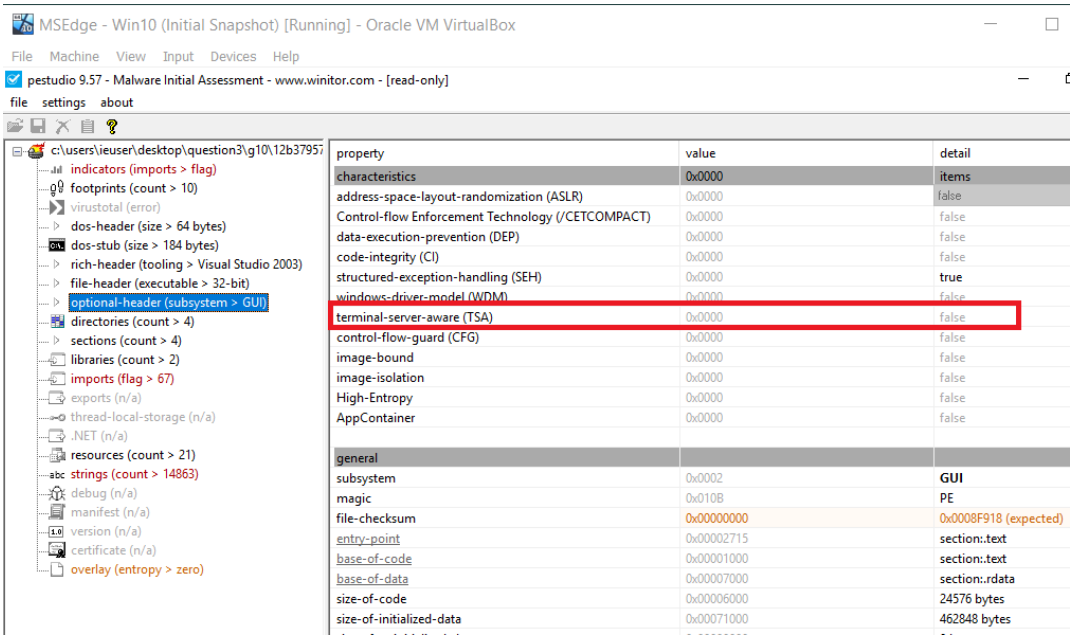
Executable No. 1 - (The file of size 552kb)

A. **Compiler-stamp** - Sat Dec 20 22:48:46 2008 | UTC

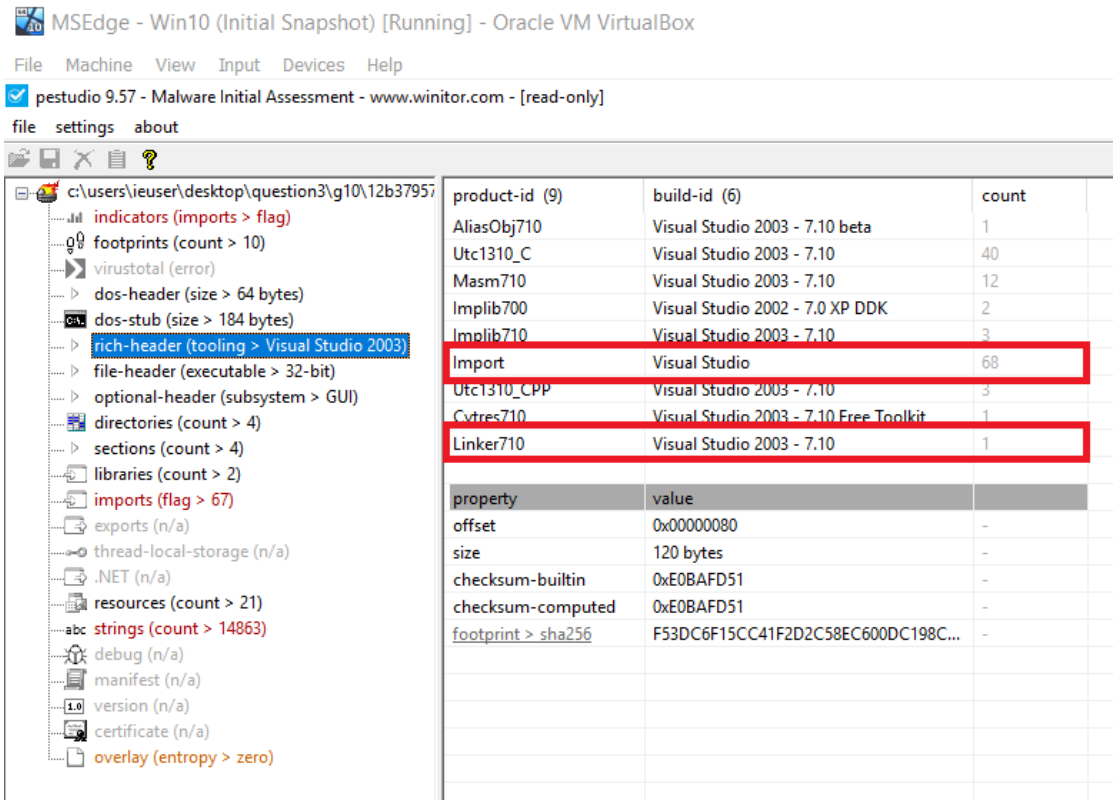
B. **Does the executable support 32-bit words?** Yes, the executable supports 32-bit words



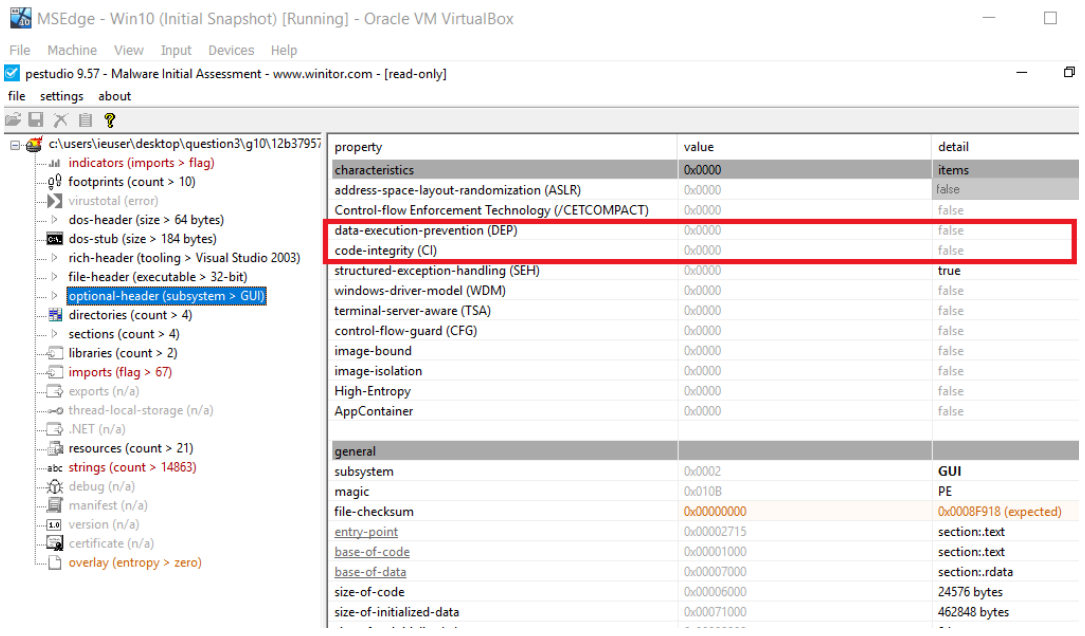
C. **Terminal server aware:** False



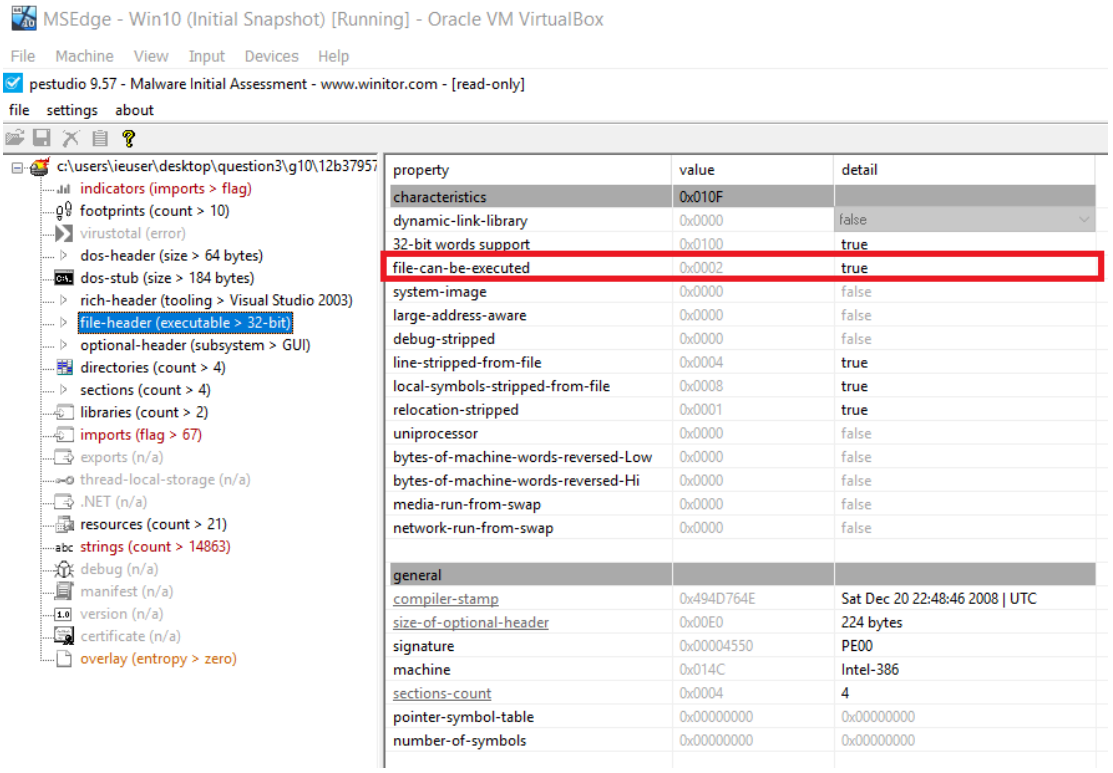
D. **Rich Header Info:** Yes, the executable contains rich header
Import: Visual Studio
Linker: Visual Studio 2003 - 7.10



E. **Data execution prevention (DEP):** False
F. **Code integrity:** False

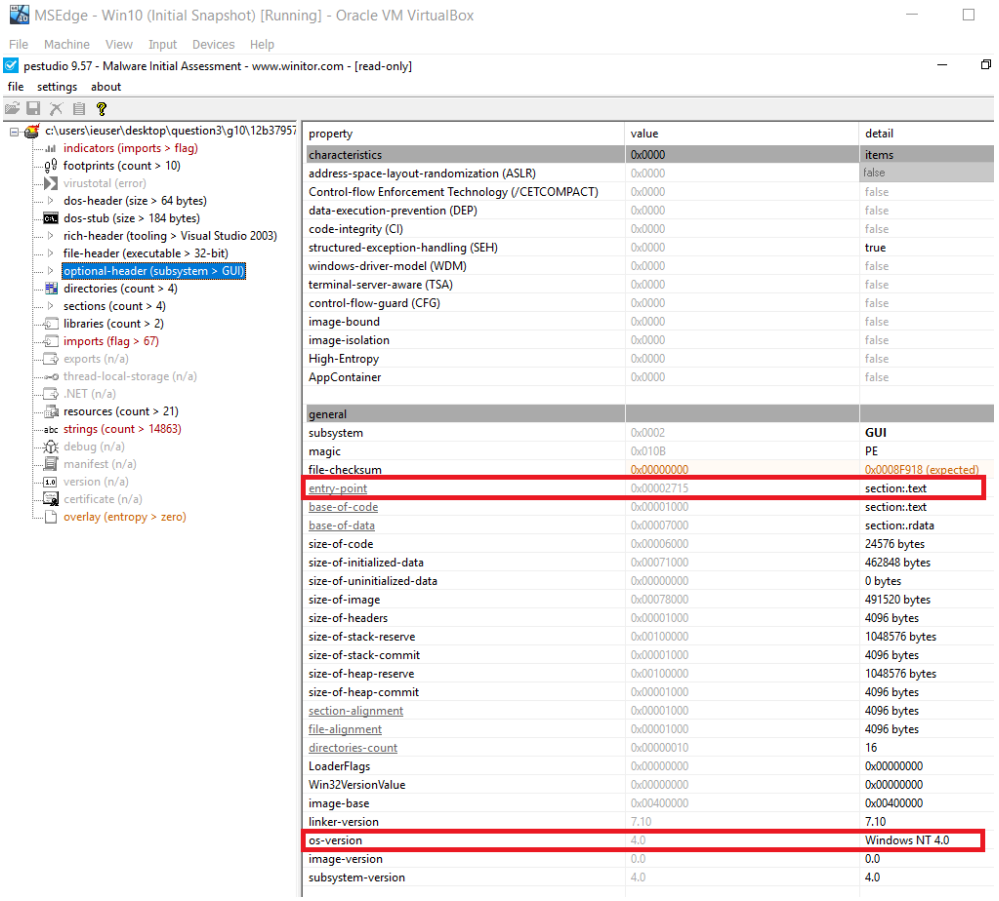


G. **Can the file be executed?:** Yes, file can be executed



H. **section's name, which is the executable's entry point:** Text

I. **What is the os-version:** Windows NT 4.0

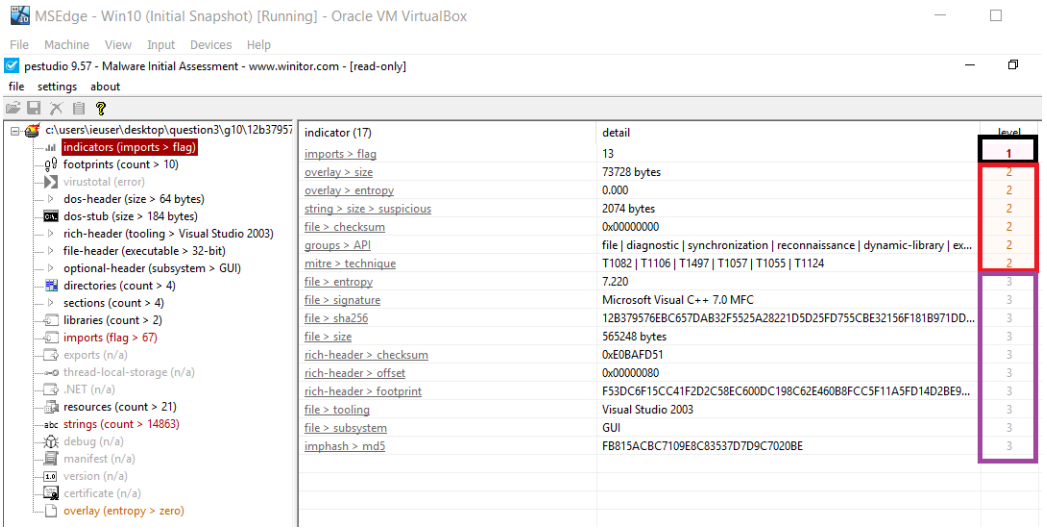


J. Count the number of indicators for each level: There are total 17 indicators

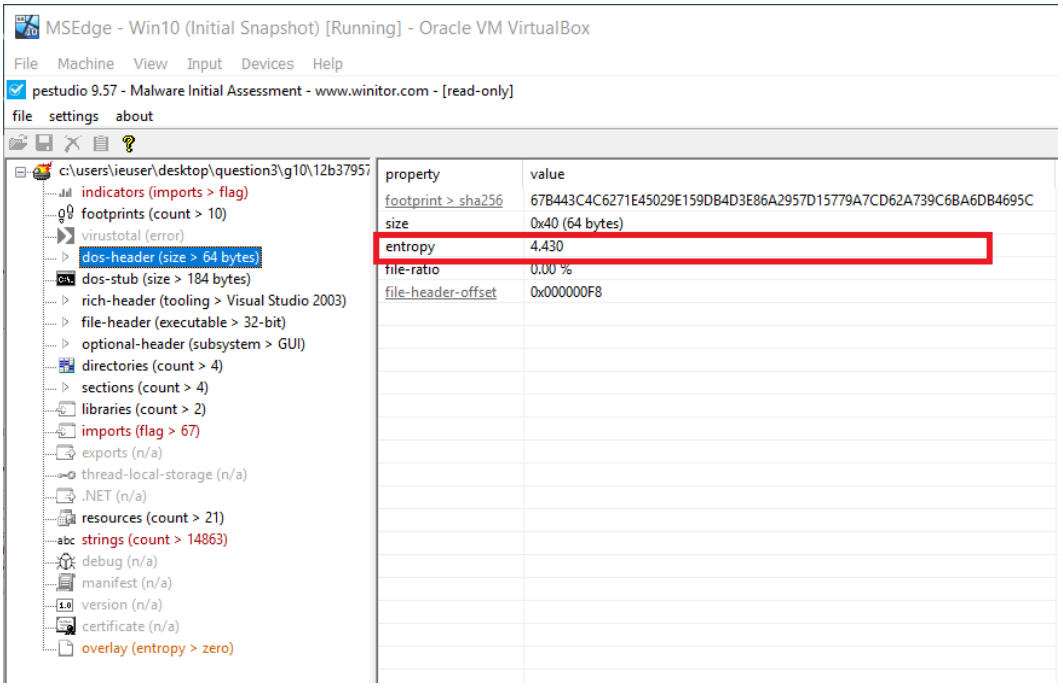
1 indicator in level 1

6 indicators in level 2

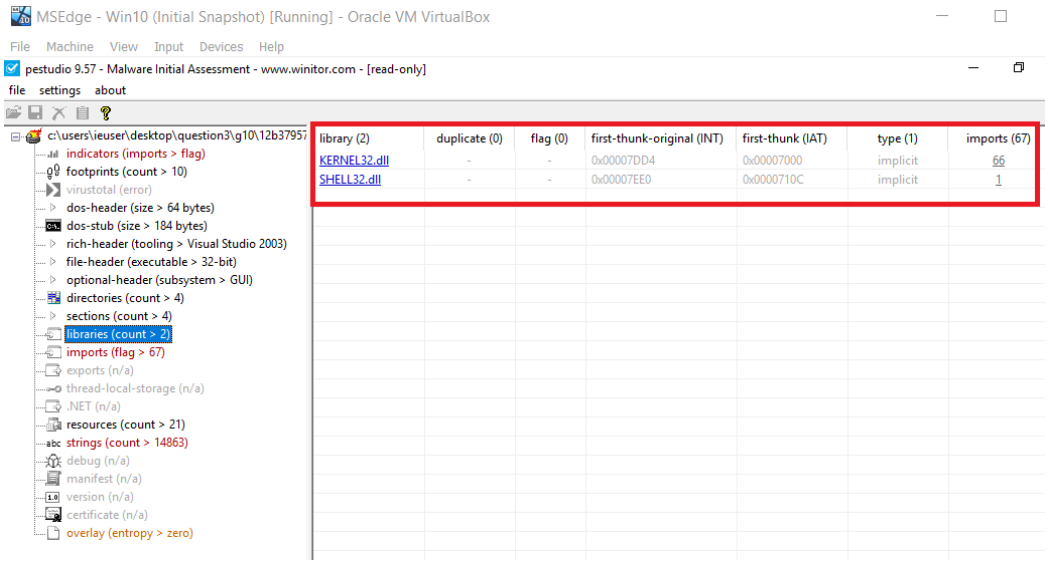
10 indicators in level 3



K. **What is the Dos-header entropy? :** 4.430



L. **Implicit type libraries:** There are 2. KERNEL32.dll and SHELL32.dll

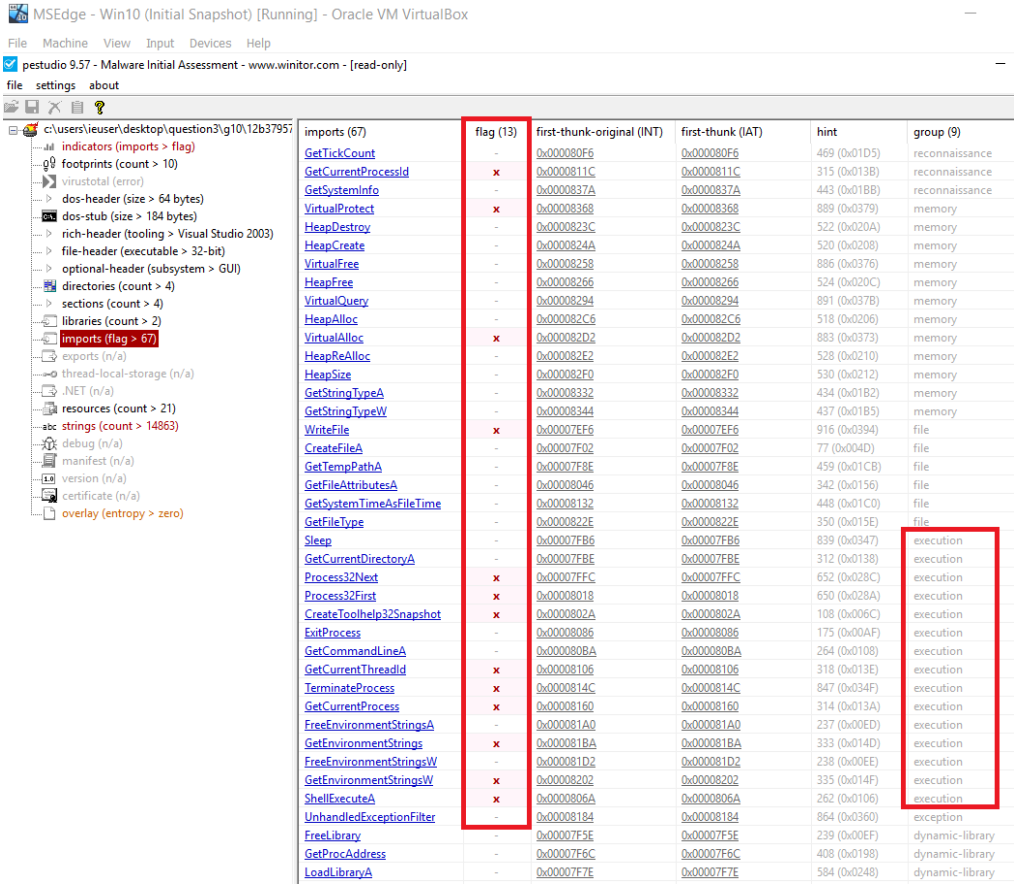


M. **Count the number of red flag imports:** 13

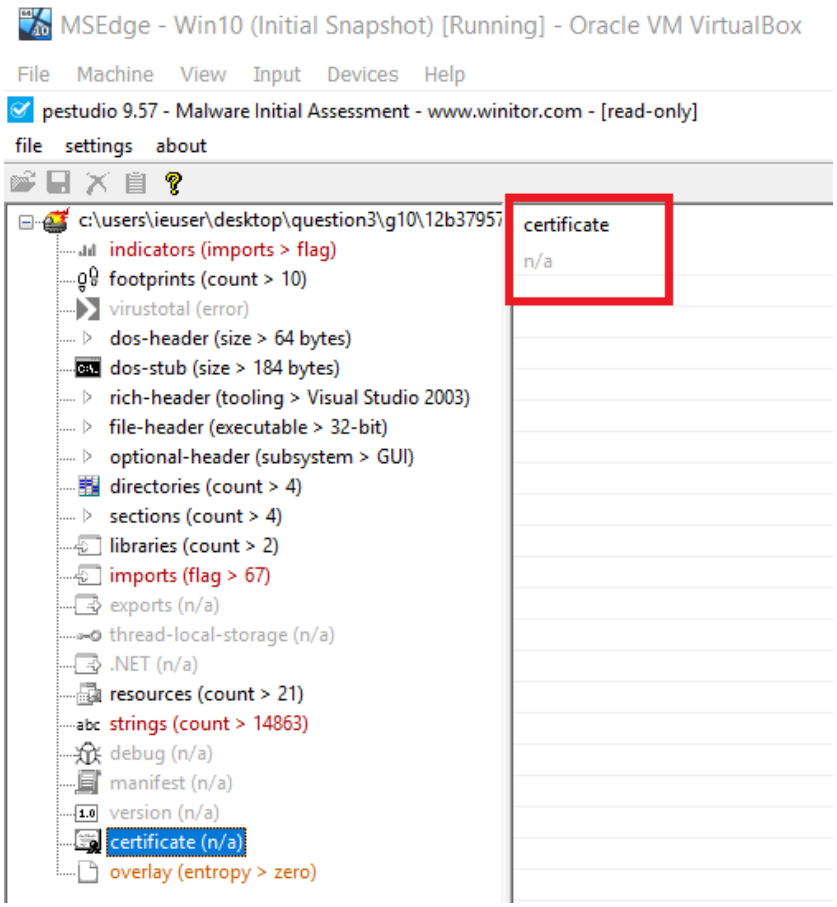
N. **Cryptography Group Imports**:0

Execution group imports: 15

Obfuscation group imports:0



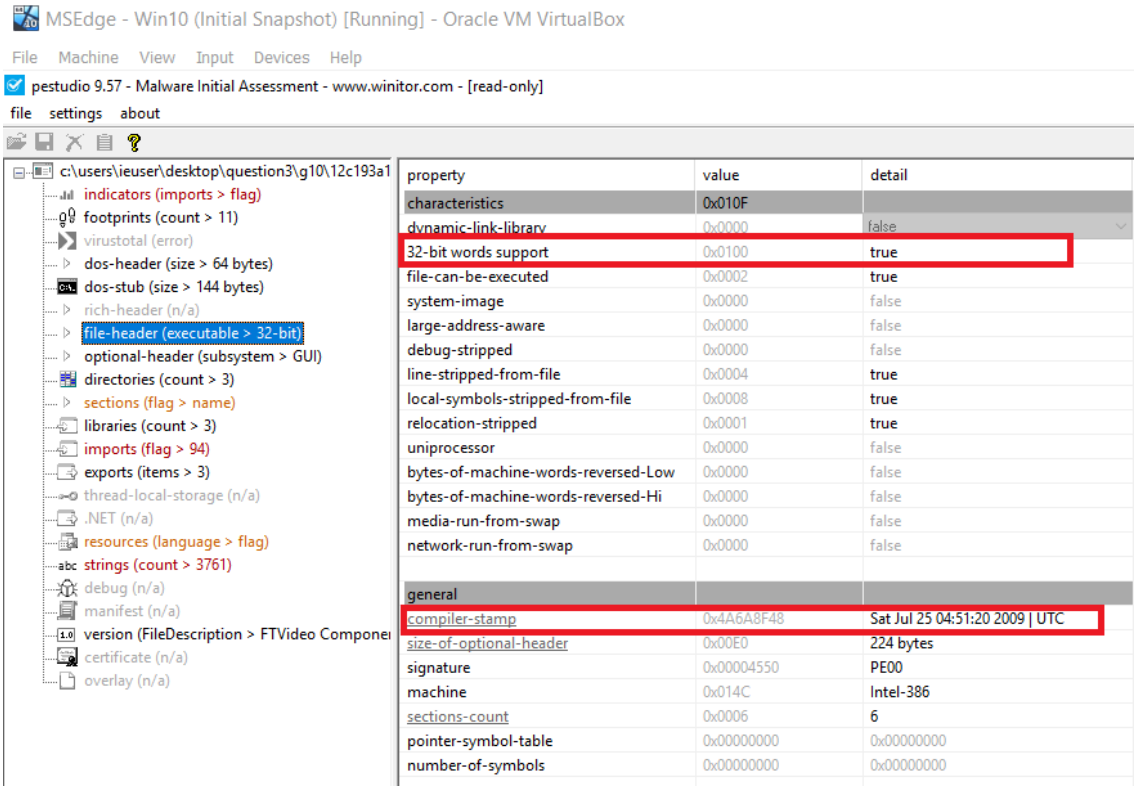
O. **Status of the certificate:** Invalid (n/a)



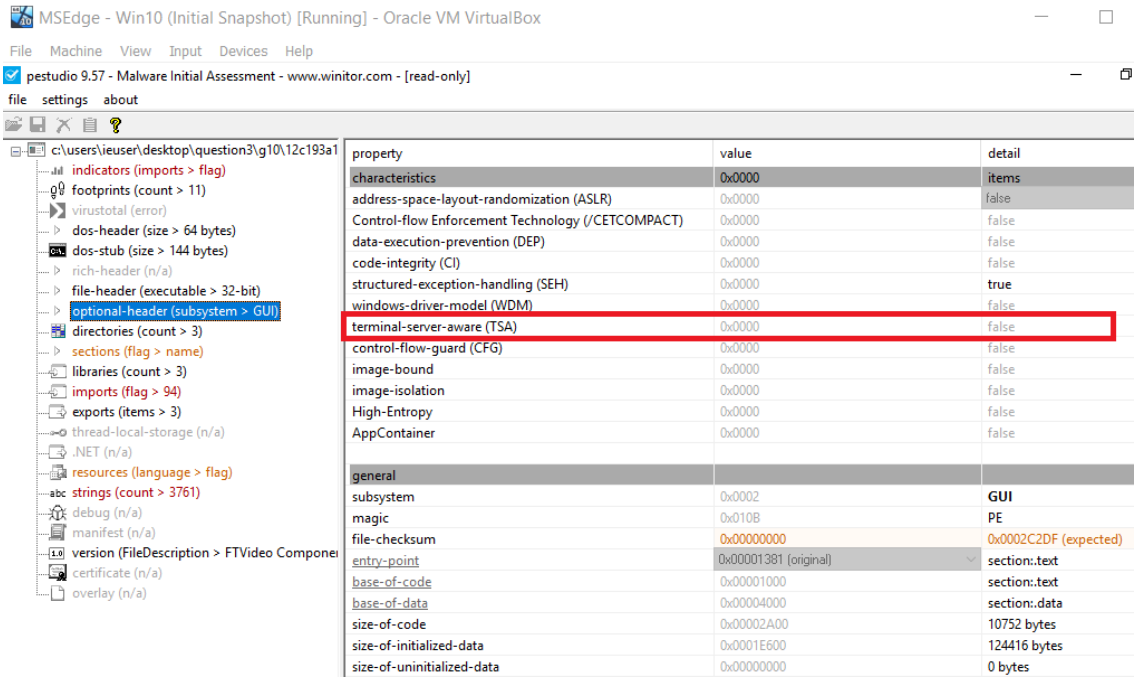
Executable number 2 - (The file of size 133kb)

a. **Compiler-stamp**: Sat Jul 25 04:51:20 2009 | UTC

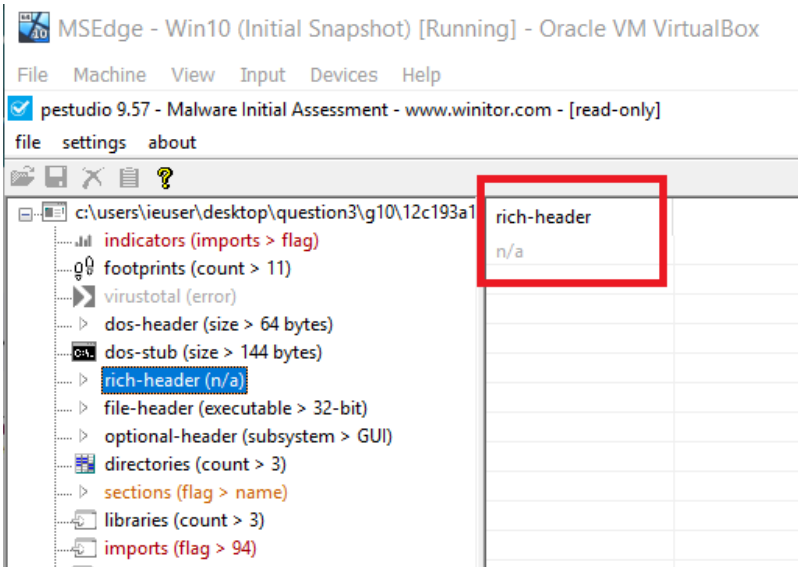
b. **Does the executable support 32-bit words?** True



c. **Terminal server aware**: False

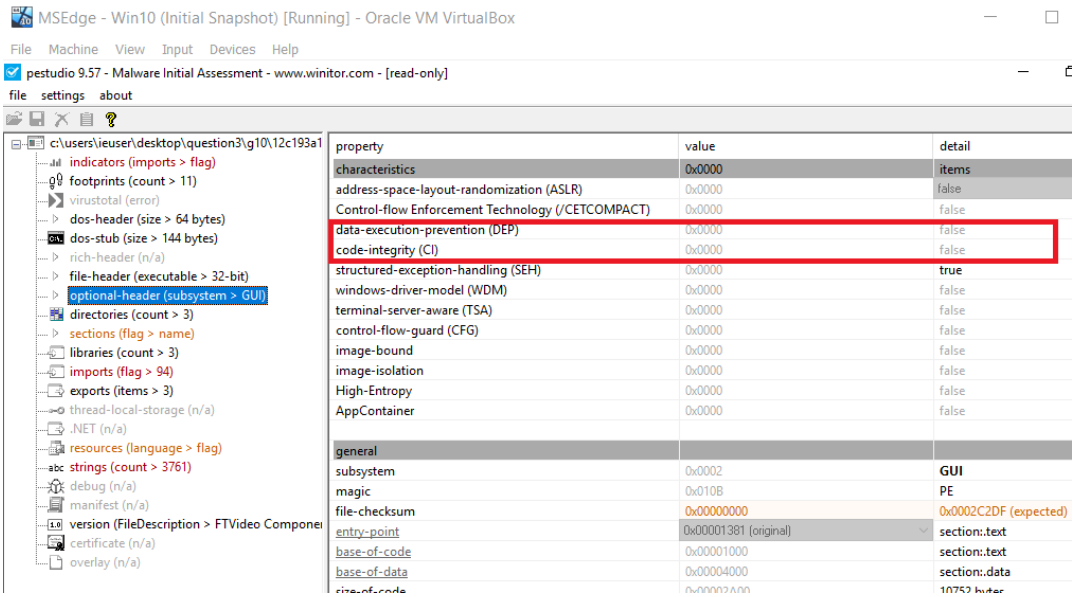


d. **Rich Header Info:** No, the executable does not contain rich header

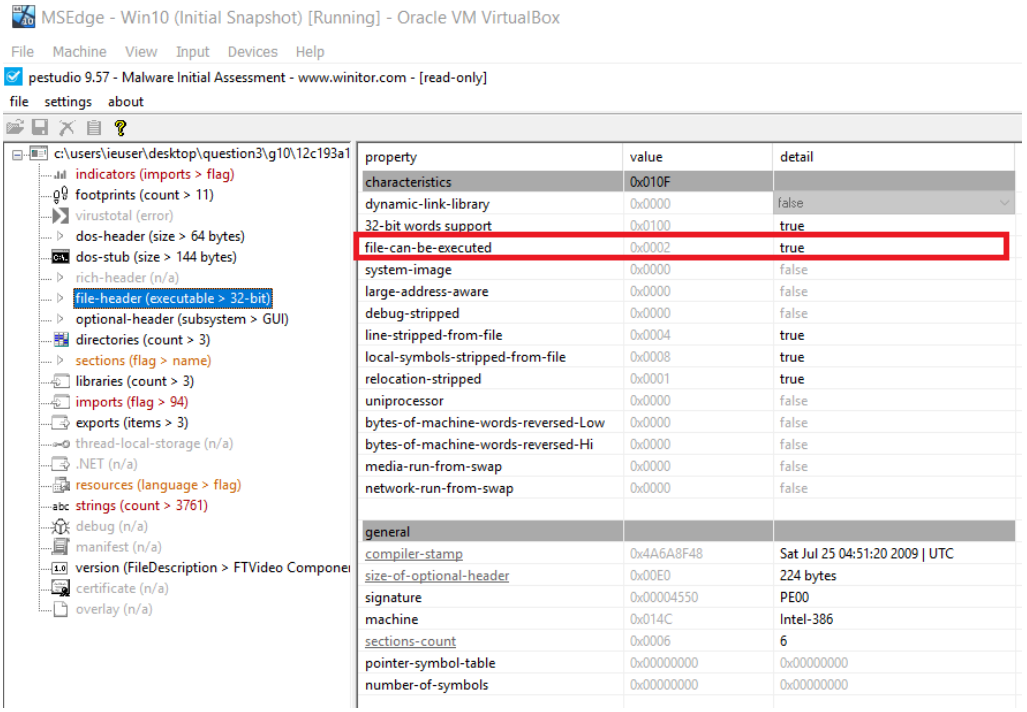


e. **Data execution prevention (DEP):** False

f. **Code integrity:** False

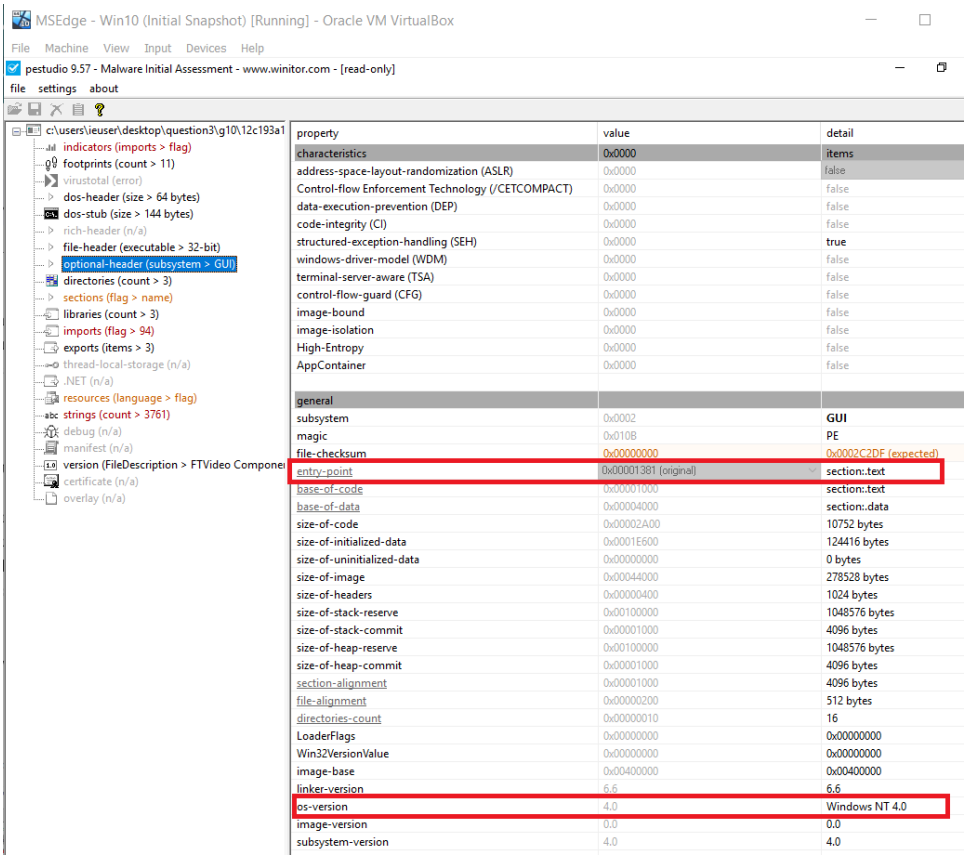


g. **Can the file be executed?:** Yes



h. **Section's name, which is the executable's entry point:** Text

i. **What is the os-version:** Windows NT 4.0



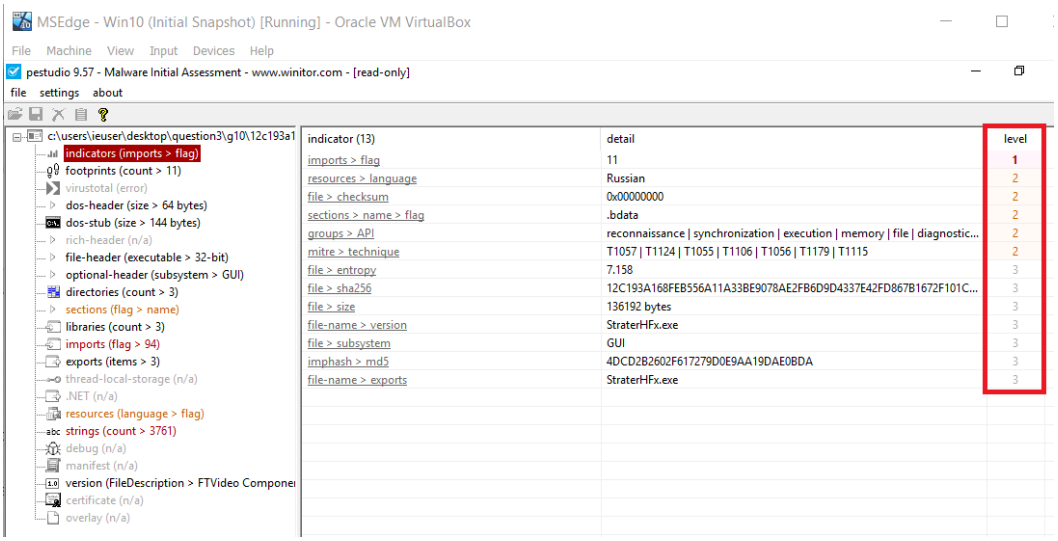
j. Count the number of indicators for each level:

There are 13 indicators

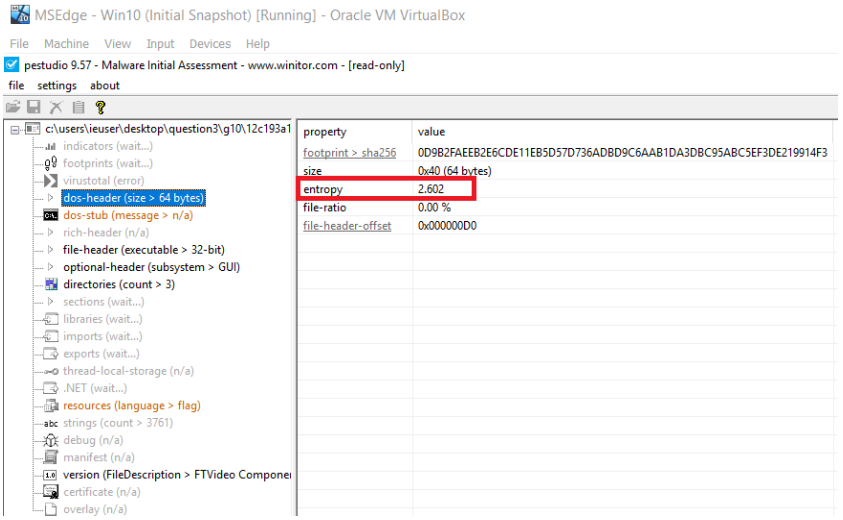
1 indicator in level 1

5 indicators in level 2

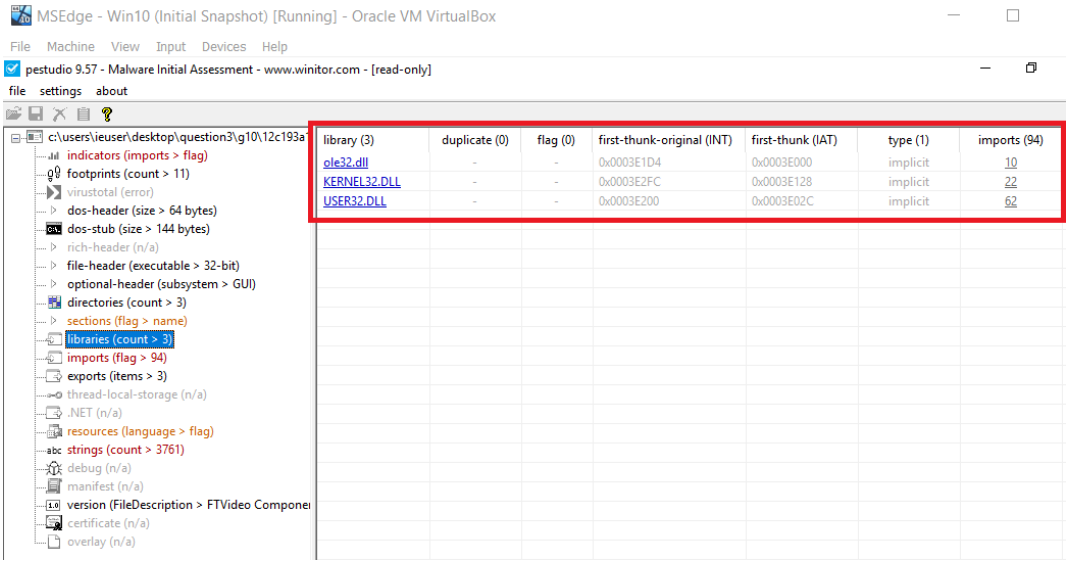
7 indicators in level 3



k. **What is the Dos-header entropy:** 2.602

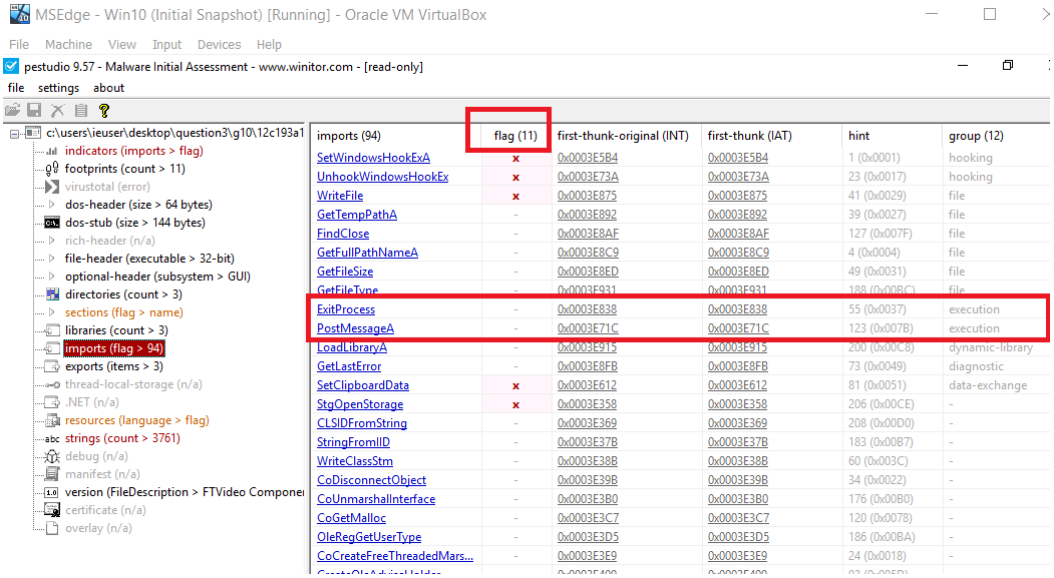


l. **Implicit type libraries:**
There are 3 implicit type libraries.
Ole32.dll, KERNEL32.dll and USER32.dll

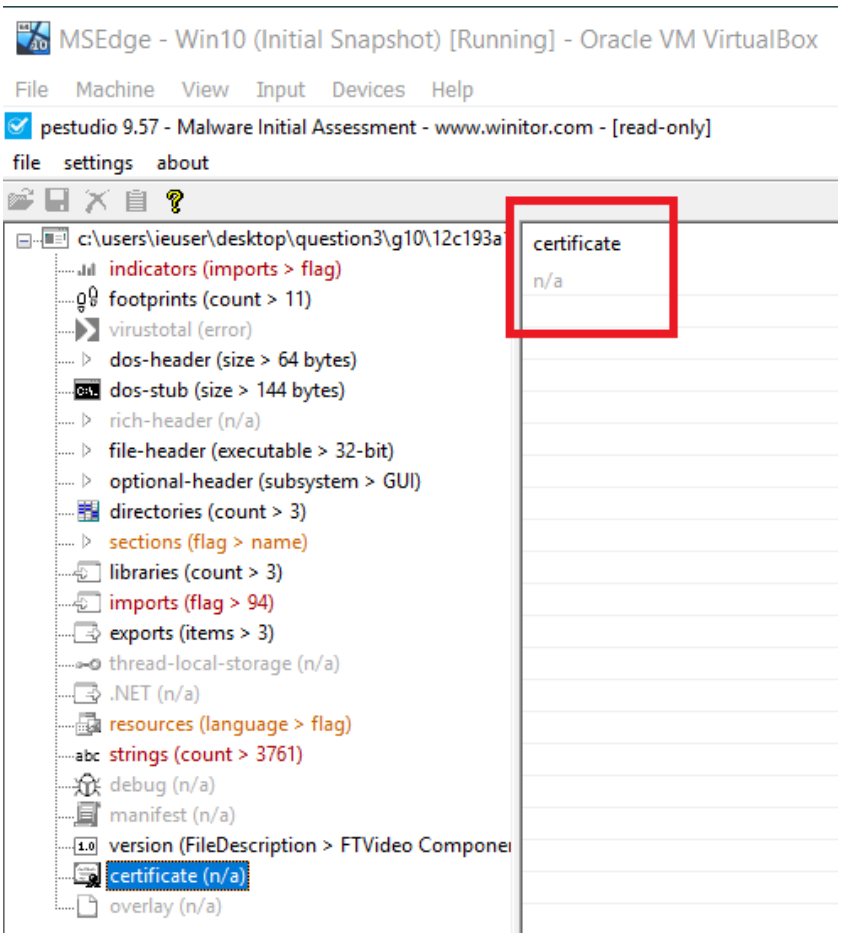


m. **Count the number of red flag imports:** 11

n. **Cryptography Group Imports:** 0
Execution group imports: 2
obfuscation group imports: 0



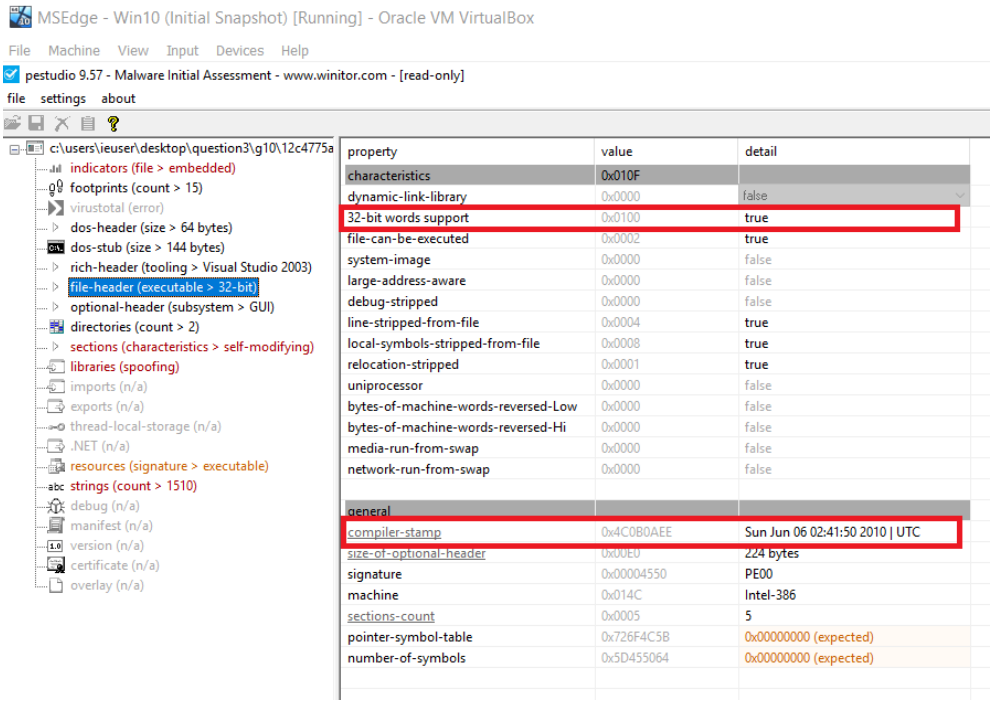
o. **Status of the certificate:** Invalid



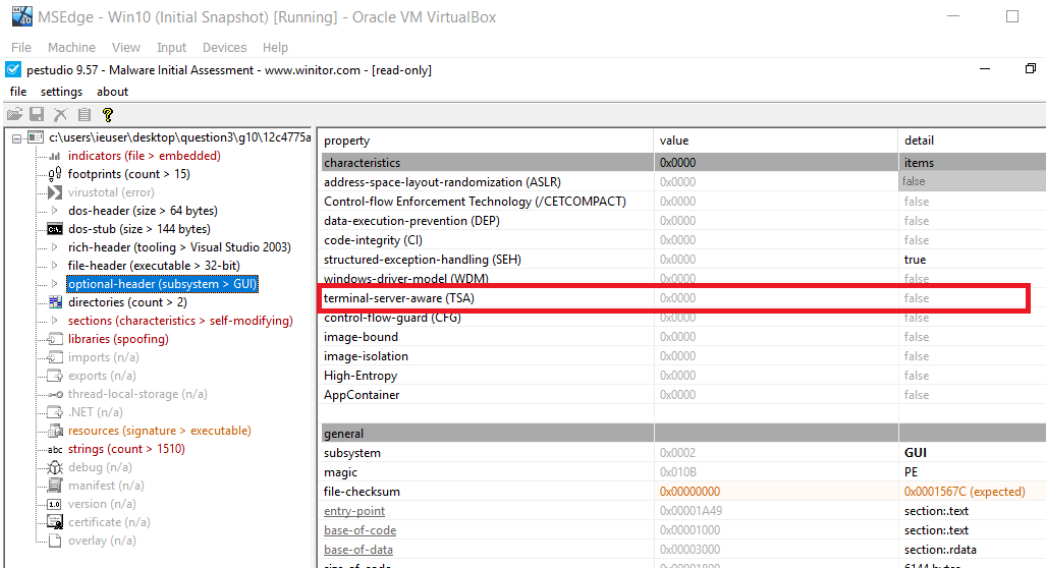
Executable no. 3 - (The file of size 53kb)

a) **Compiler-stamp**: Sun Jun 06 02:41:50 2010 | UTC

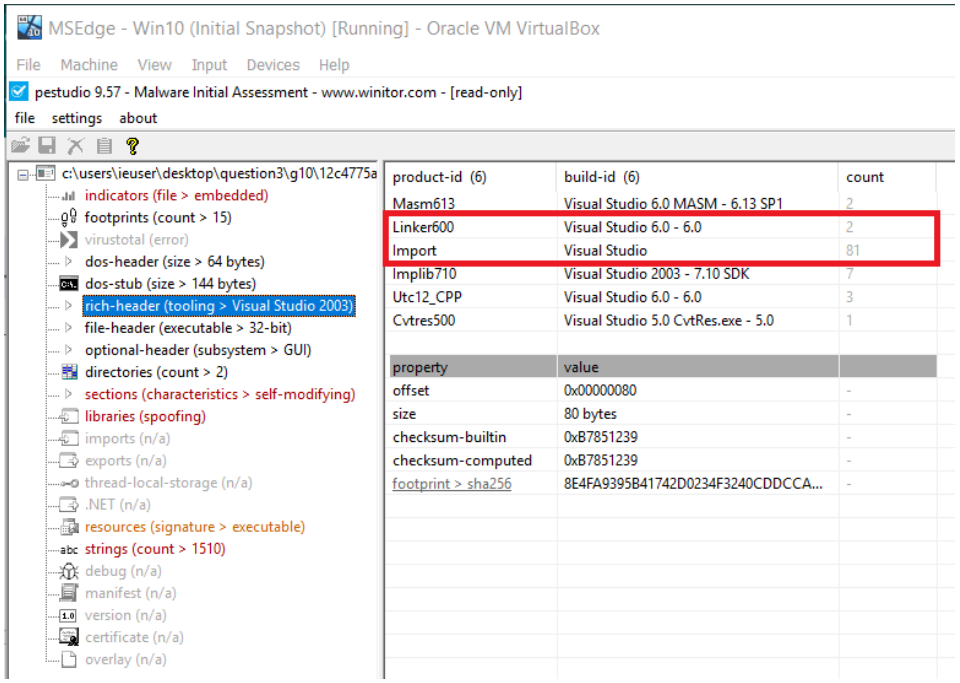
b) **Does the executable support 32-bit words?** True it supports



c) **Terminal server aware**: False (Terminal server is not aware)

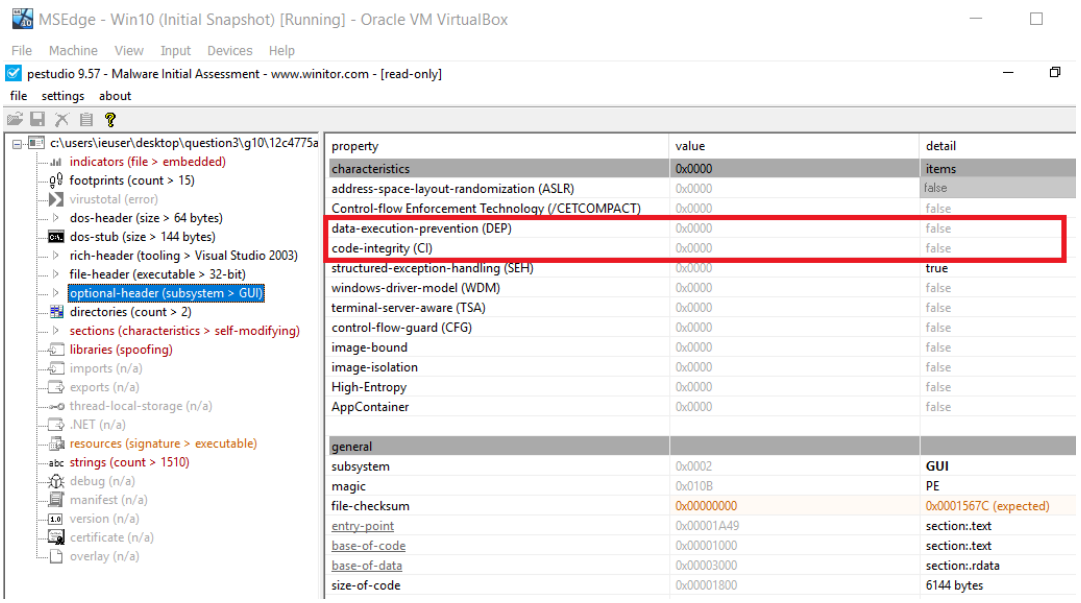


d) Rich Header Info: Yes, the executable contains rich header
Import: Visual Studio
Linker: Visual Studio 6.0 - 6.0

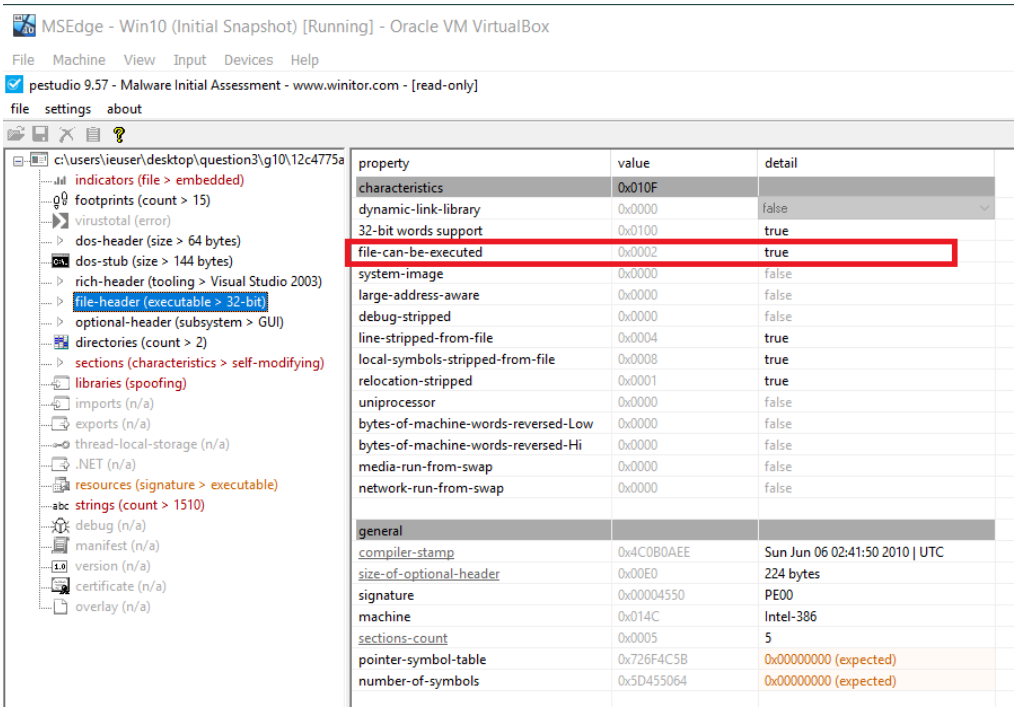


e) Data execution prevention (DEP): False

f) Code integrity: False

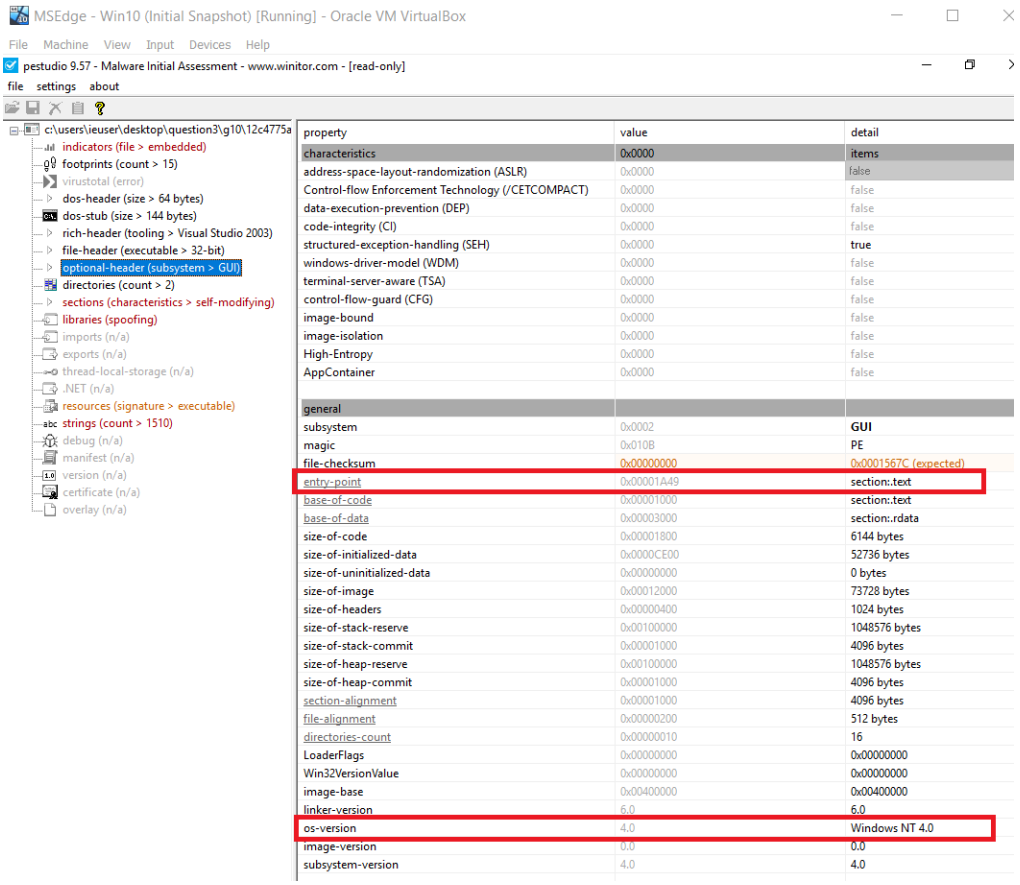


g) Can the file be executed?: Yes. The file can be executed



h) Section's name, which is the executable's entry point: Text

i) What is the os-version: Windows NT 4.0



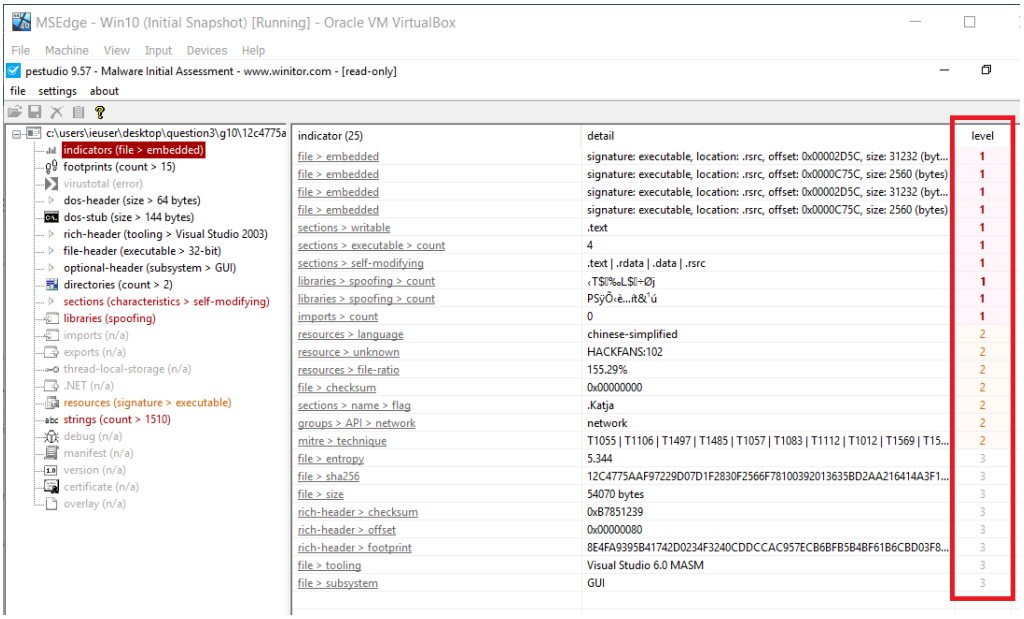
j) Count the number of indicators for each level:

Total 25 Indicators

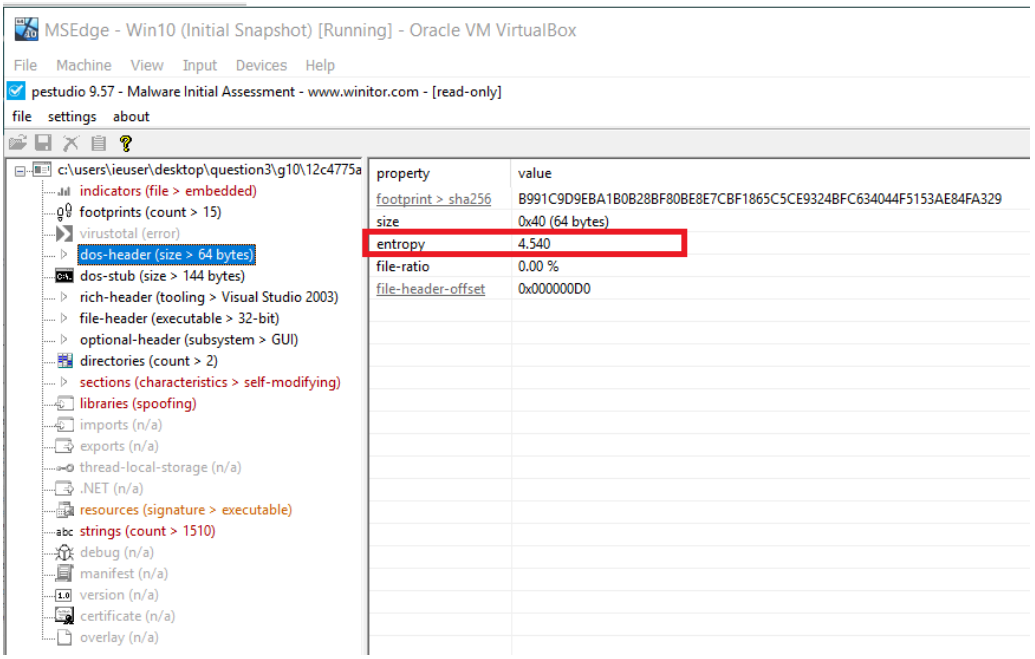
10 indicators in level 1

7 indicators in level 2

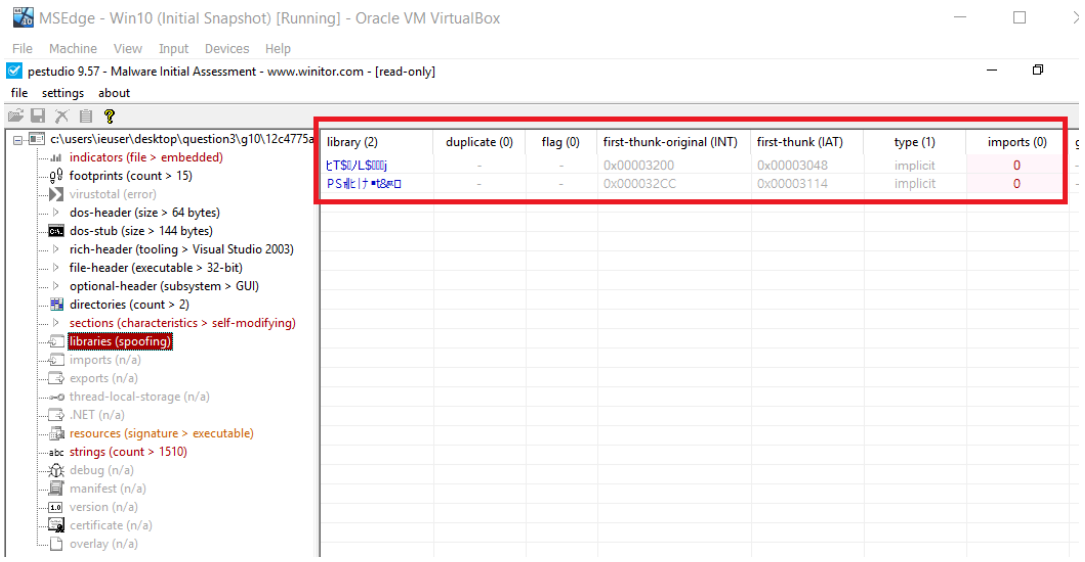
8 indicators in level 3



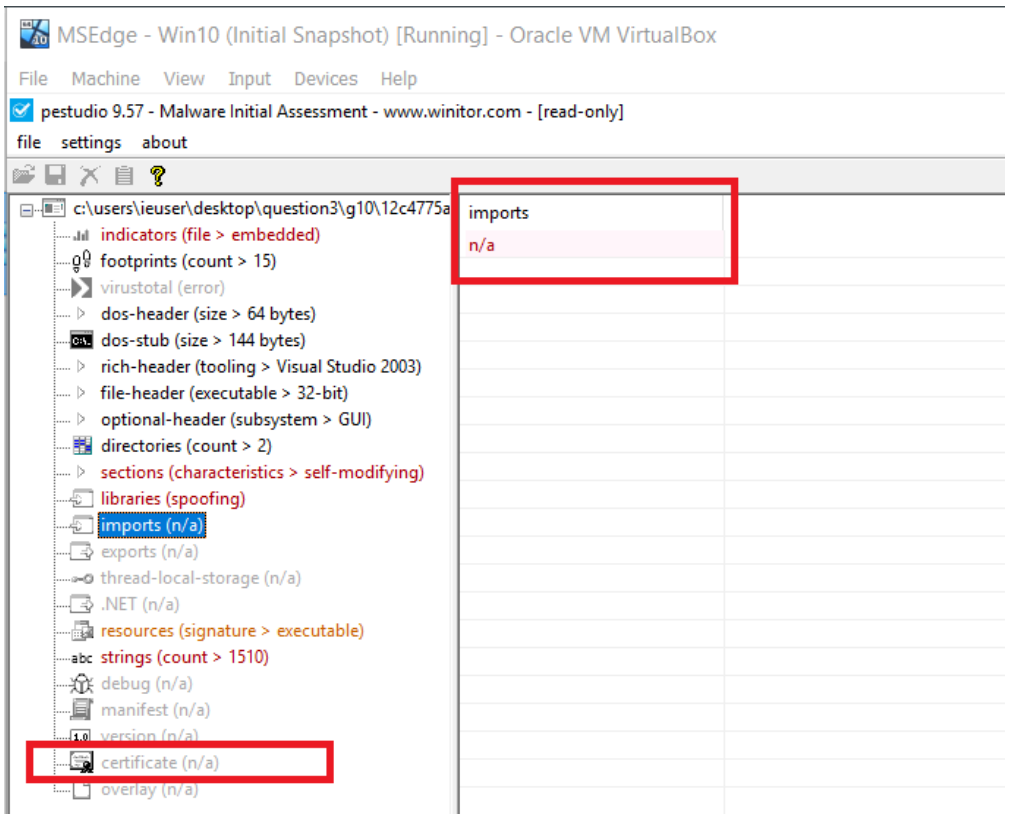
k) What is the Dos-header entropy: 4.540



l) **Implicit type libraries:**
There are 2 implicit type libraries.
‹T$‰L$÷Øj and PSÿÕ‹è…ít&¹ú (don't know in what language it is written or are those encrypted names. Screenshots are attached below)



m) **Count the number of red flag imports:** No imports
n) **No imports: Hence - Cryptography Group Imports**:0
Execution group imports: 0
obfuscation group imports: 0
o) **Status of the certificate:** Invalid (n/a)



QUESTION 4: RECONNAISSANCE

A Atulya Sundaram : 210001 **Assigned IP: 172.29.232.211**

The list of commands used for conducting the penetration test for the IP assigned i.e. **172.29.232.211**

1. **To get the list of open TCP ports:**
   The default nmap command returns which tcp ports are closed or open. We can see that port 21 is open with an FTP service running on it.

```
~ ❯ nmap 172.29.232.211
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 02:59 IST
Nmap scan report for 172.29.232.211
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

2. **To get the list of filtered TCP ports:**

   Filtered TCP ports indicate that there is a firewall blocking the port. Here we see that there is there is no firewall present blocking the packets.

```
~ ❯ sudo nmap -sA 172.29.232.211
[sudo] password for atulya:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 03:03 IST
Nmap scan report for 172.29.232.211
Host is up (0.0041s latency).
All 1000 scanned ports on 172.29.232.211 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

3. **Get the list of open UDP ports, services running on them and version**

```
~ ❯ sudo nmap -sU 172.29.232.211
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 03:05 IST
Nmap scan report for 172.29.232.211
Host is up (0.0061s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   filtered      dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf
```

```
~ 16m 50s ❯ sudo nmap -sUV 172.29.232.211
[sudo] password for atulya:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 04:07 IST
Nmap scan report for 172.29.232.211
Host is up (0.026s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE  VERSION
67/udp   open|filtered dhcps
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf
```

The basic scan shows that the above ports are either open or filtered. Interesting to note is that the UDP port **67** was not observed in the initial scan, however, it turns up while checking for the version. This is because version detection makes a deeper scan than simple UDP scanning. We conducted a deeper scan below. All the UDP scans were made at slightly different times. This might indicate that the remote is currently active and being used

```
~ ❯ sudo nmap -sUV -F 172.29.232.211

[sudo] password for atulya:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 11:45 IST
Warning: 172.29.232.211 giving up on port because retransmission cap
hit (10).
Nmap scan report for 172.29.232.211
Host is up (0.0072s latency).
Not shown: 92 closed ports
PORT      STATE         SERVICE        VERSION
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
445/udp   open|filtered microsoft-ds
631/udp   open|filtered ipp
5353/udp  open|filtered zeroconf
17185/udp open|filtered wdbrpc
32768/udp open|filtered omad
32771/udp open|filtered sometimes-rpc6
```

4. **Check the service and version number on the open tcp port**

```
~ ❯ sudo nmap -sV 172.29.232.211
[sudo] password for atulya:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 03:08 IST
Nmap scan report for 172.29.232.211
Host is up (0.0052s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix
```

This is the version for the service that is active on the port.

5. Getting the operating system of the device

```
~ ❯ sudo nmap -O 172.29.232.211
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 03:11 IST
Nmap scan report for 172.29.232.211
Host is up (0.0029s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/s
ubmit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/7%OT=21%CT=1%CU=42831%PV=Y%DS=2%DC=I%G=Y%TM=65C2A792
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M4E2ST11NW7%O2=M4E2ST11NW7%O3=M4E2NNT11NW7%O4=M4E2ST11NW7%O5=M4E2ST11
OS:NW7%O6=M4E2ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T
OS:=40%CD=S)

Network Distance: 2 hops
```

```
~ ❯ sudo nmap -O --fuzzy 172.29.232.211
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 03:43 IST
Nmap scan report for 172.29.232.211
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
Aggressive OS guesses: Linux 2.6.32 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 2
11 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%
), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10
 (92%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/su
bmit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/7%OT=21%CT=1%CU=40071%PV=Y%DS=2%DC=I%G=Y%TM=65C2AF30
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M4E2ST11NW7%O2=M4E2ST11NW7%O3=M4E2NNT11NW7%O4=M4E2ST11NW7%O5=M4E2ST11
OS:NW7%O6=M4E2ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 2 hops
```

The first command returned an uncertain answer. To get a guess estimate of the OS in use we used the --fuzzy tag. Thus we get that the host is probably a Linux based operating system. However, it is interesting that the fingerprint is not in the nmap database.

6. **Conducting the vulnerability test using the vuln script**

```
~ ❯ nmap 172.29.232.211 --script vuln

Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-07 12:00 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 172.29.232.211
Host is up (0.0062s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
```

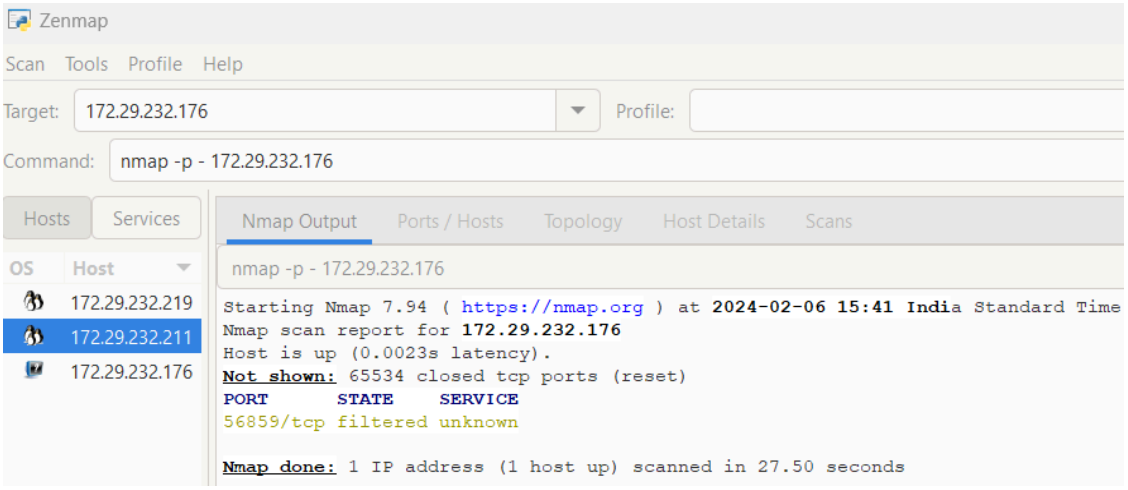
The debug scan was also conducted, however, the error was due to the inability to connect to SSL-VPN. Other than this, no other scripts showed any vulnerabilities.

The only vulnerability the given open tcp port 21 has is a remote denial of service attack (Using internet sources). No other major vulnerabilities were found.

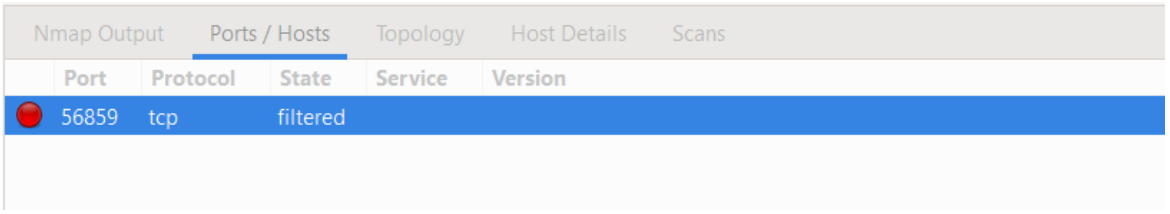
Dhiraj Pareek : 231110012 **Assigned IP: 172.29.232.176**

1) **Command: nmap -p - 172.29.232.176**

Rationale : This command in nmap is used to scan the target host (172.29.232.176) for open ports without specifying any particular port or range of ports to scan.

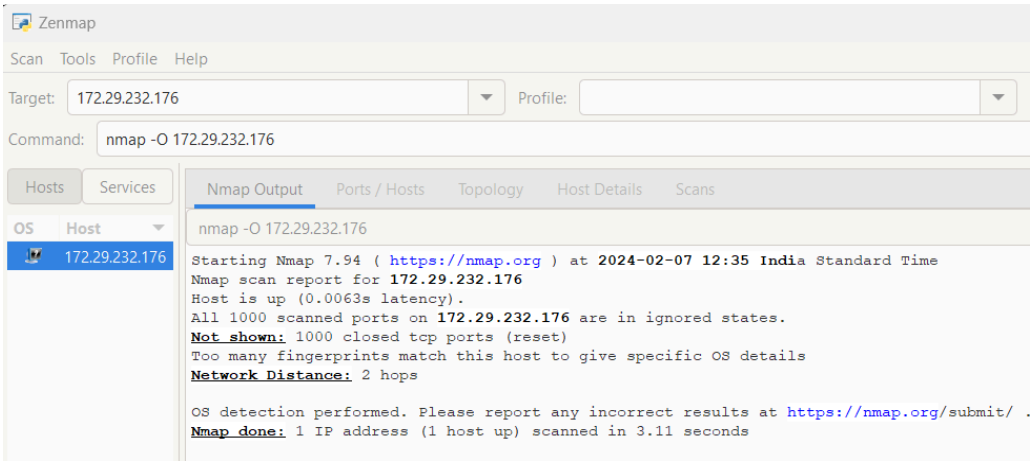


Result: Port 56859/tcp, is showing as **filtered.**
Which means that Nmap was unable to determine the state of this port due to various reasons such as firewall rules, packet filtering, or other network configurations.



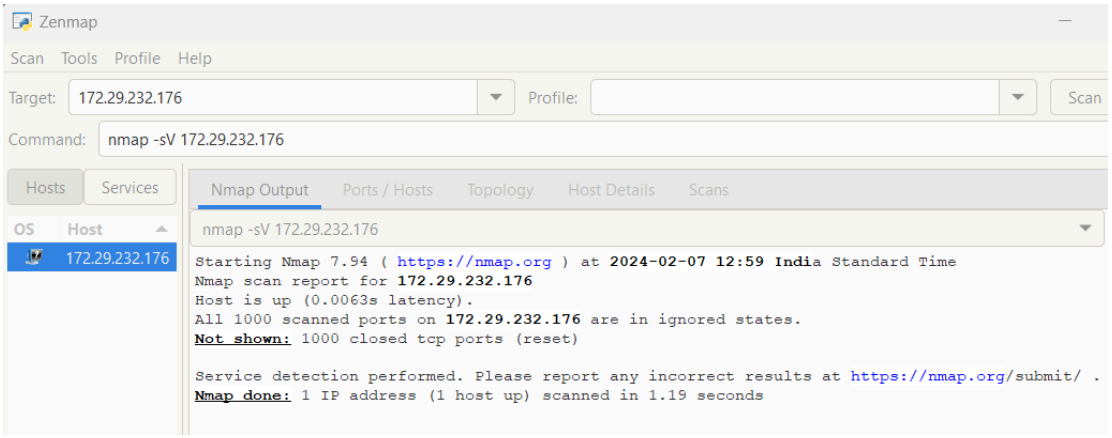
2) **Command**: **nmap -O 172.29.232.176**

Rationale : "-O" is used to perform OS detection against the target host with the IP address 172.29.232.176.



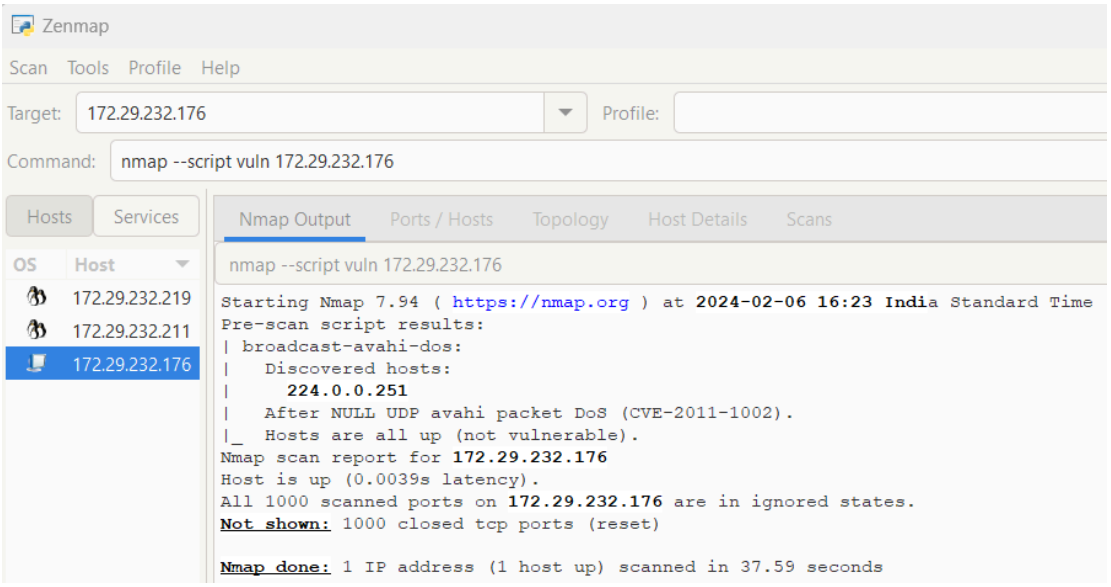
Result: OS Detection was unable to provide specific details about the OS which can be due to various reasons such as presence of multiple operating system fingerprints matching the host, or the host may be configured in a way that prevents accurate OS detection.

3) **Command**: **nmap -sV 172.29.232.176**
Rationale : **-sV** This option enables version detection, allowing Nmap to determine the versions of services running on open ports.



Result: service detection process did not yield any specific result regarding the services running on the target host's open ports due to certain conditions
such as firewall rules, packet filtering, or other network configurations.

4) **Command: nmap --script vuln 172.29.232.176**
Rationale : --script vuln This command is used to identify potential vulnerabilities in the services running on the target host



Result: Nmap ran a prescan script called "*broadcast-avahi-dos*" which checks for a vulnerability related to Avahi, a zeroconf service. It found a host at the IP address 224.0.0.251 but host is not vulnerable to the NULL UDP avahi packet Denial of Service (DoS) vulnerability.

Challenges: Open ports, service versions, and operating system inferences were not clear due to firewall or packet filtering which block or restrict Nmap's ability to scan ports and services.

Conclusions: The target host possesses at least one open port, specifically port 56859/tcp, which was marked as filtered. This status indicates that Nmap was unable to determine the state of the port due to various network configurations, such as firewall rules or packet filtering. The OS detection process failed to provide specific details about the operating system, which could be attributed to various factors including multiple operating system fingerprints or configurations designed to evade detection.Similarly, vulnerability detection scripts were unable to provide clear insights into the services and potential vulnerabilities present on the target host.

Akash Shivaji Varude: 231110006 Assigned IP: 172.29.233.230

1. **Command:** nmap -p- 172.29.233.230
   Reason to use: To find open ports in target system using nmap
   Result: The host is up. There are 65533 Closed ports and two open ports:
   1) Port 21/tcp is Open. It provides Service - FTP (File transfer protocol)
   2) Port 5900/tcp is Open. It provides Service - VNC (Virtual Network Computing)

```
C:\Users\akash>nmap -p- 172.29.233.230
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 18:48 India Standard Time
Nmap scan report for 172.29.233.230
Host is up (0.0042s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
5900/tcp open  vnc
```

2. **Command:** nmap -O 172.29.233.230
   Reason to Use: To perform scanning for OS detection
   Result: Network is 2 hops away (I scanned it from H14 room)
   Detected OS: No exact OS detected by CLI however by using –fuzzy in the command it detects OS as linux 4.15 - 5.8

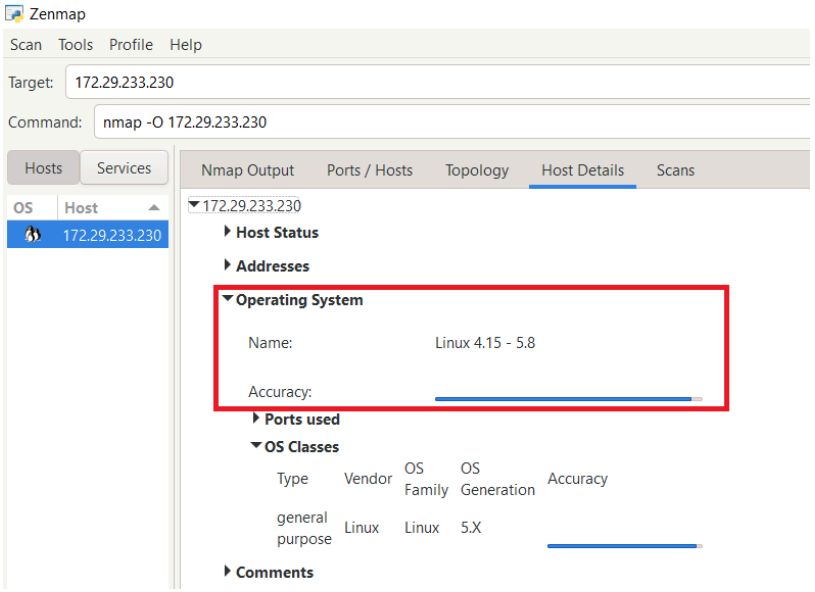
```
C:\Users\akash>nmap -O 172.29.233.230
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 16:00 India Standard Time
Nmap scan report for 172.29.233.230
Host is up (0.0048s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
5900/tcp open  vnc
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=2/7%OT=21%CT=1%CU=30267%PV=Y%DS=2%DC=I%G=Y%TM=65C35BCB
OS:%P=i686-pc-windows-windows)SEQ(CI=Z%II=I)SEQ(SP=107%GCD=1%ISR=105%TI=Z%C
OS:I=Z%II=I%TS=A)SEQ(SP=107%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=C)SEQ(SP=108%GC
OS:D=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M4E2ST11NW7%O2=M4E2ST11NW7%O3=M4E
OS:2NNT11NW7%O4=M4E2ST11NW7%O5=M4E2ST11NW7%O6=M4E2ST11)OPS(O1=NNT11%O2=NNT1
OS:1%O3=M4E2NNT11NW7%O4=M4E2ST11NW7%O5=M4E2ST11NW7%O6=M4E2ST11)OPS(O1=NNT11
OS:%O2=NNT11%O3=NNT11%O4=NNT11%O5=NNT11%O6=M4E2ST11)OPS(O1=NNT11%O2=NNT11%O
OS:3=NNT11%O4=NNT11%O5=NNT11%O6=NNT11)WIN(W1=1FD%W2=1FD%W3=1FD%W4=1FD%W5=1F
OS:D%W6=FE88)WIN(W1=1FD%W2=1FD%W3=FE88%W4=FE88%W5=FE88%W6=FE88)WIN(W1=FE88%
OS:W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=1F5%O=%CC=N%
OS:Q=)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=
OS:O%F=A%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=O%A=O%F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 2 hops
```

```
C:\Users\akash>nmap -O --fuzzy 172.29.233.230
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 16:41 India Standard Time
Nmap scan report for 172.29.233.230
Host is up (0.0047s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
5900/tcp open  vnc
Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux
3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), L
inux 3.16 (93%), Linux 5.0 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=2/7%OT=21%CT=1%CU=32763%PV=Y%DS=2%DC=I%G=Y%TM=65C3656C
OS:%P=i686-pc-windows-windows)SEQ(CI=Z%II=I)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%C
OS:I=Z%II=I%TS=9)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=104%GC
OS:D=1%ISR=10A%TI=Z%CI=Z%II=I%TS=C)SEQ(SP=108%GCD=1%ISR=109%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M4E2ST11NW7%O2=M4E2ST11NW7%O3=M4E2NNT11NW7%O4=M4E2ST11NW7%O5
OS:=M4E2ST11NW7%O6=M4E2ST11)OPS(O1=NNT11%O2=M4E2ST11NW7%O3=M4E2NNT11NW7%O4=
OS:M4E2ST11NW7%O5=M4E2ST11NW7%O6=M4E2ST11)OPS(O1=NNT11%O2=NNT11%O3=M4E2NNT1
OS:1NW7%O4=M4E2ST11NW7%O5=M4E2ST11NW7%O6=M4E2ST11)OPS(O1=NNT11%O2=NNT11%O3=
OS:NNT11%O4=NNT11%O5=NNT11%O6=NNT11)WIN(W1=1FD%W2=1FD%W3=1FD%W4=1FD%W5=1FD%
OS:W6=FE88)WIN(W1=1FD%W2=1FD%W3=FE88%W4=FE88%W5=FE88%W6=FE88)WIN(W1=1FD%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88
OS:%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=1F5%O=%CC=N%Q=)ECN(R=Y%DF=Y%T=40%W=
OS:FAF0%O=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=O%F=A%RD=0%Q=)T1(R=Y%DF
OS:=Y%T=40%S=O%A=O%F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%U
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.18 seconds
```



3. **Command:** nmap -sV 172.29.233.230
   Reason to use: To find open ports services running on open ports, their versions, and OS used
   Result: Port 21/tcp: Open, Service - FTP (version: vsftpd 3.0.3)
   Port 5900/tcp: Open, Service - VNC (Version: VNC (protocol 3.7))

```
C:\Users\akash>nmap -sV 172.29.233.230
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 18:42 India Standard Time
Nmap scan report for 172.29.233.230
Host is up (0.0065s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
5900/tcp open  vnc     VNC (protocol 3.7)
Service Info: OS: Unix
```

4. **Command:** nmap --script vuln 172.29.233.230
   Reason to use: To identify potential vulnerabilities on the target system
   Result: There is a potential vulnerability related to the SSL/TLS configuration on the FTP service.
   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability:
   State: Vulnerable
   Reason: It can lead to man-in-the-middle attacks.
   Diffie-Hellman Key Exchange Incorrectly Generated Group Parameters:
   State: Likely Vulnerable
   Reason: This TLS service appears to be using a modulus that is not a safe prime and does not correspond to any well-known DSA group for Diffie-Hellman key exchange.

```
C:\Users\akash>nmap --script vuln 172.29.233.230
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 19:29 India Standard Time
Nmap scan report for 172.29.233.230
Host is up (0.0050s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
5900/tcp open  vnc
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
|             Modulus Type: Non-safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Diffie-Hellman Key Exchange Incorrectly Generated Group Parameters
|     State: LIKELY VULNERABLE
|       This TLS service appears to be using a modulus that is not a safe prime
|       and does not correspond to any well-known DSA group for Diffie-Hellman
|       key exchange.
|       These parameters MAY be secure if:
|       - They were generated according to the procedure described in
|         FIPS 186-4 for DSA Domain Parameter Generation, or
|       - The generator g generates a subgroup of large prime order
|       Additional testing may be required to verify the security of these
|       parameters.
|     Check results:
|       NON-SAFE GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
|             Modulus Type: Non-safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
```

Challenges Faced: Firewall might have been configured to detect and respond to scanning activities and as aggressive scanning techniques might trigger firewall rules hence I couldn't use aggressive scanning. Due to which it might be possible that results I obtained could be partial or incomplete.