

# **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

The screenshot shows the Shodan search interface with the query "OpenSSH !port:'22'" entered. The results page displays a world map showing the distribution of found hosts. Below the map, a table lists the top countries and their counts: China (1,194), Germany (569), United States (557), Peru (554), and Korea, Republic of (357). Each entry includes the IP address, location, and a detailed technical card showing SSH version, key type, and key content. The results are paginated with a "More..." link.

- 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

**TOTAL RESULTS** 4,479

**TOP COUNTRIES**

Country	Count
United States	1,779
Russian Federation	255
Germany	239
Netherlands	185
United Kingdom	178
<a href="#">More...</a>	

**TOP PORTS**

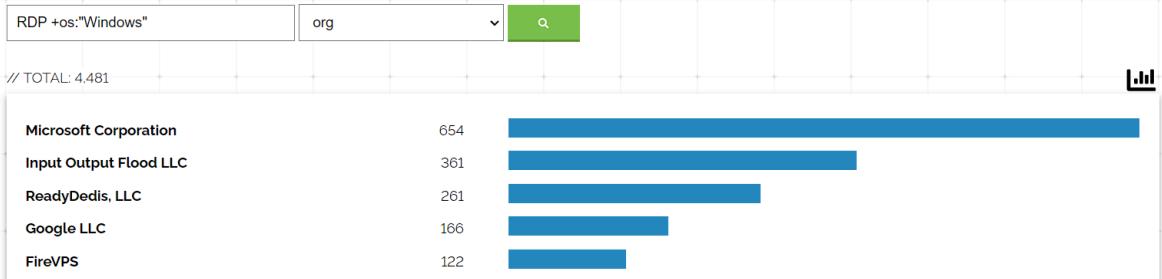
Port	Count
3389	3,711
5985	552
5986	92

**Access Granted:** Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

**58.171.9.96**  
Telstra Internet  
Australia, Adelaide  
 **SSL Certificate**  
Issued By: self-signed  
I-Common Name: GENIE-RDP  
Issued To: I-Common Name: GENIE-RDP  
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2  
Remote Desktop Protocol  
\x03\x00\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00  
Remote Desktop Protocol NTLM Info:  
OS: Windows 10 (version 2004)/Windows Server (version 2004)  
OS Build: 10.0.19041  
Target Name: GENIE-RDP  
NetBIOS Domain Name: GENIE-RDP  
NetBIOS Computer Na...  
2024-02-05T09:20:47.303400

Other user

## Facet Analysis



- 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"

**TOTAL RESULTS** 2

**TOP ORGANIZATIONS**

Organization	Count
Broadband Multiplex Project, O/o DGM ... 1	1
PRAJ NETWORK PVT LTD	1

**117.255.218.89**  
Broadband Multiplex Project, O/o DGM ... 1  
BSNL, Bangalore  
India, Lucknow  
 **WEB SERVICE**  
HTTP/1.1 200 OK  
Connection: keep-alive  
Date: Sun, 07 Jan 2024 22:51:52 GMT  
Last-Modified: Tue, 10 Aug 2021 11:55:35 GMT  
Etag: "1628946535:dc9"  
Content-Length: 3529  
P3P: CP=CAO PSA OUR  
X-Frame-Options: SAMEORIGIN  
X-XSS-Protection: 1;mode=block  
Content-Security-Policy: script-src 'self' ...  
2024-01-27T01:17:55.243577

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 .

```
Run      curl -I http://117.255.218.89
Clear
US ↴

Status: 200 (OK) Time: 504 ms Size: 0.40 kb
Content Headers (8) Raw (8) Timings

Connection: Keep-Alive
Keep-Alive: timeout=20
X-Frame-Options: SAMEORIGIN
ETag: "f99-197-611ba439"
Content-Type: text/html
Date: Mon, 05 Feb 2024 11:45:23 UTC
Content-Length: 447

close

Get 10 Free Images From Adobe Stock. Start Now.
ads via Carbon
```

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.

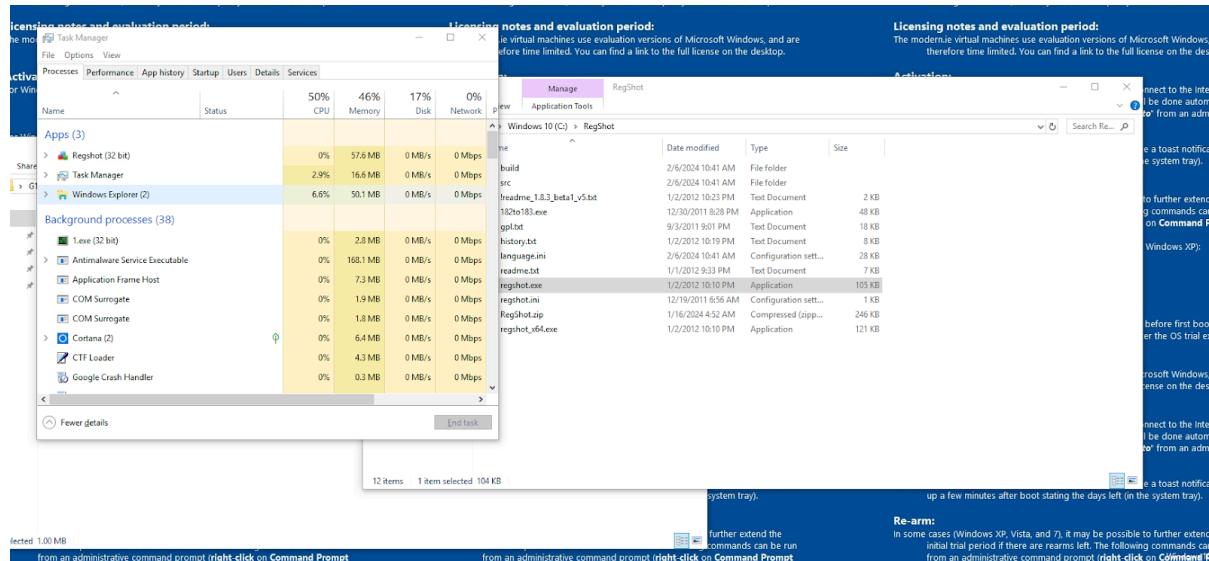


Fig. Before

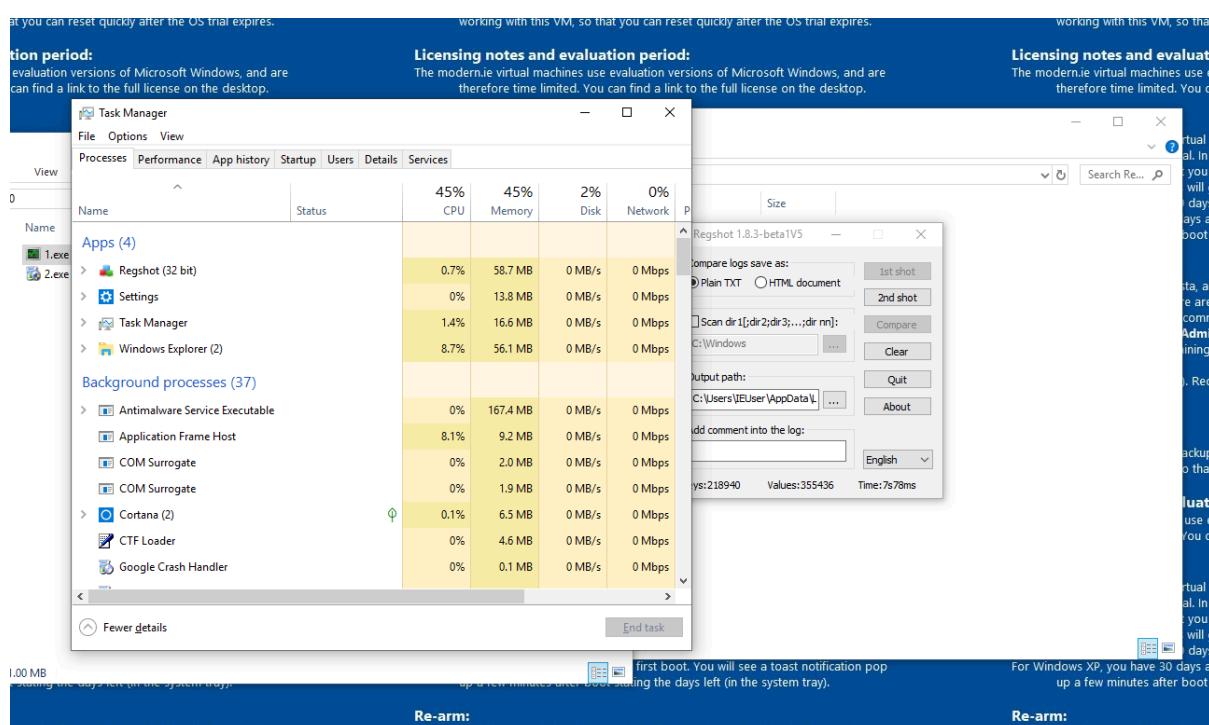


Fig. After

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

The screenshot shows the RegShot application interface comparing two registry snapshots. The left pane displays a list of registry changes, while the right pane shows the full registry key structure. Key differences highlighted in the left pane include:

- A new value entry under `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ss` pointing to `C:\Users\IEUser\AppData\Roaming\orhv\CXOJVX~1.EXE`.
- A new value entry under `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ss` pointing to `C:\Users\IEUser\AppData\Roaming\orhv\CADWKR~1.MP3`.
- Changes in the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ss` key itself, such as modifications to the `0x00000000000000000000000000000000` value.

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

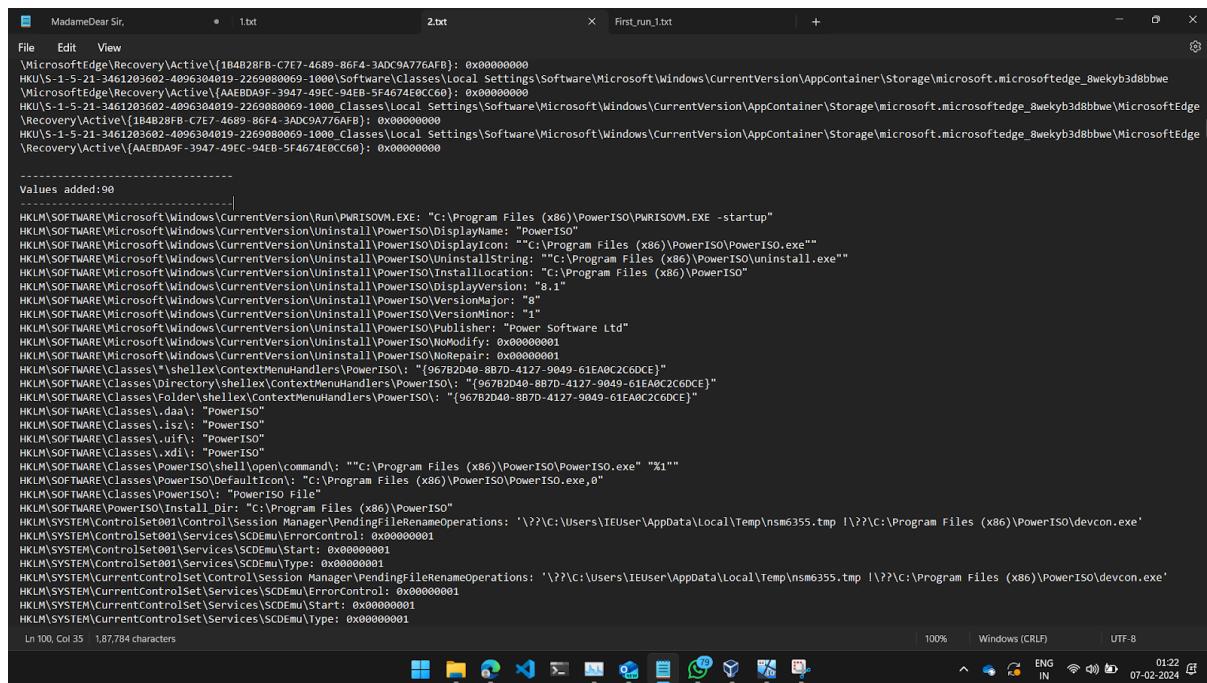
**HKU\S-1-5-21-3461203602-4096304019-2269080069-1000\Software\Microsoft\Windows\CurrentVersion\Run\ss: "C:\Users\IEUser\AppData\Roaming\orhv\CXOJVX~1.EXE C:\Users\IEUser\AppData\Roaming\orhv\CADWKR~1.MP3"**

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.

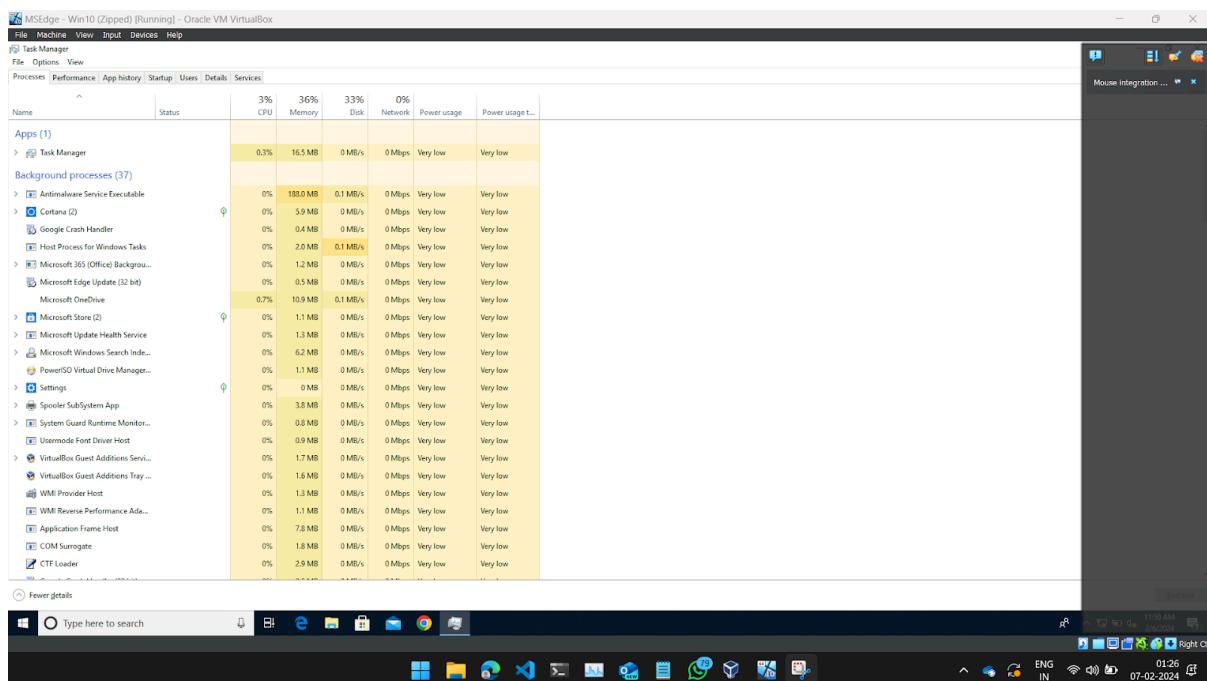
Hence the given malware is **persistent**.

## 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.



```
MadameDear Sir, 1.txt First_run_1.txt
File Edit View
\Microsoft\Edge\Recovery\Active\[1BA828FB-C7E7-4689-86FA-3ADC9A776AFB]: 0x00000000
HKEY\Software\Microsoft\Windows\CurrentVersion\Run\PWRISOVM.EXE: "C:\Program Files (x86)\PowerISO\PWRISOVM.EXE -startup"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO DisplayName: "PowerISO"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO DisplayIcon: "C:\Program Files (x86)\PowerISO\PowerISO.exe"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\UninstallString: "C:\Program Files (x86)\PowerISO\uninstall.exe"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\InstallLocation: "C:\Program Files (x86)\PowerISO"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\DisplayVersion: "8.1"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\VersionMajor: "8"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\VersionMinor: "1"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\Publisher: "Power Software Ltd"
HKEY\Software\Microsoft\Windows\CurrentVersion\Uninstall\PowerISO\NoRepair: 0x00000001
HKEY\Software\Windows\CurrentVersion\Uninstall\PowerISO\NoRepair: 0x00000001
HKEY\Software\Classes\shell\ContextMenuHandlers\PowerISO: "(967B2D40-887D-4127-9049-61EA0C2C6DCE)"
HKEY\Software\Classes\Directory\shell\ContextMenuHandlers\PowerISO: "(967B2D40-887D-4127-9049-61EA0C2C6DCE)"
HKEY\Software\Classes\Folder\shell\ContextMenuHandlers\PowerISO: "(967B2D40-887D-4127-9049-61EA0C2C6DCE)"
HKEY\Software\Classes\dll: "PowerISO"
HKEY\Software\Classes\isz: "PowerISO"
HKEY\Software\Classes\uiF: "PowerISO"
HKEY\Software\Classes\xdl: "PowerISO"
HKEY\Software\Classes\PowerISO\shell\open\command: "C:\Program Files (x86)\PowerISO\PowerISO.exe" "%1"
HKEY\Software\Classes\PowerISO\DefaultIcon: "C:\Program Files (x86)\PowerISO\PowerISO.exe,0"
HKEY\Software\PowerISO\Install_Dir: "C:\Program Files (x86)\PowerISO"
HKEY\SYSTEM\ControlSet001\control\Session Manager\PendingFileRenameOperations: '\??\C:\Users\IEUser\AppData\Local\Temp\nsm6355.tmp !\??\C:\Program Files (x86)\PowerISO\devcon.exe'
HKEY\SYSTEM\ControlSet001\services\SCDEmu\ErrorControl: 0x00000001
HKEY\SYSTEM\ControlSet001\services\SCDEmu\Start: 0x00000001
HKEY\SYSTEM\ControlSet001\services\SCDEmu\Type: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations: '\??\C:\Users\IEUser\AppData\Local\Temp\nsm6355.tmp !\??\C:\Program Files (x86)\PowerISO\devcon.exe'
HKEY\SYSTEM\CurrentControlSet\Services\SCDEmu\ErrorControl: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\SCDEmu\Start: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\SCDEmu\Type: 0x00000001
Ln 100, Col 35 1,877,784 characters
100% Windows (CRLE) UTF-8
0122 07-02-2024
```



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

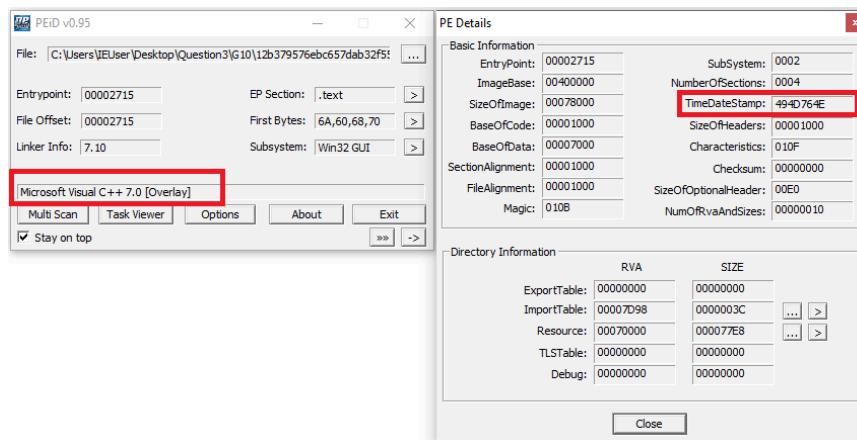
### PART 1: ANALYSIS USING PEID TOOL

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

Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	000052AE	00001000	00006000	60000020
.rdata	00007000	0000138A	00007000	00002000	40000040
.data	00009000	00066938	00009000	00067000	C0000040
.rsrc	00070000	000077E8	00070000	00008000	40000040

**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’

The screenshot shows two windows from the PEiD tool. The top window is the main analysis summary, displaying file details like Entrypoint (00002715), EP Section (.text), File Offset (00002715), First Bytes (6A,60,68,70), Linker Info (7.10), and Subsystem (Win32 GUI). The 'First Bytes' field has a red box around its '...' button. The bottom window is the 'PE Disassembler v0.03 :: CADT' window, showing assembly code. The 'Strings' button at the bottom of this window is also highlighted with a red box.

**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

This screenshot shows the PEiD interface with a detailed view of PE file information. The 'PE Details' section on the right lists various fields such as EntryPoint, ImageBase, SizeOfImage, BaseOfCode, BaseOfData, SectionAlignment, FileAlignment, and Magic. The 'SubSystem' field in the main summary has a red box around its '...' button. The 'Directory Information' section below lists ExportTable, ImportTable, Resource, TLSTable, and Debug, each with their corresponding RVA and SIZE values.

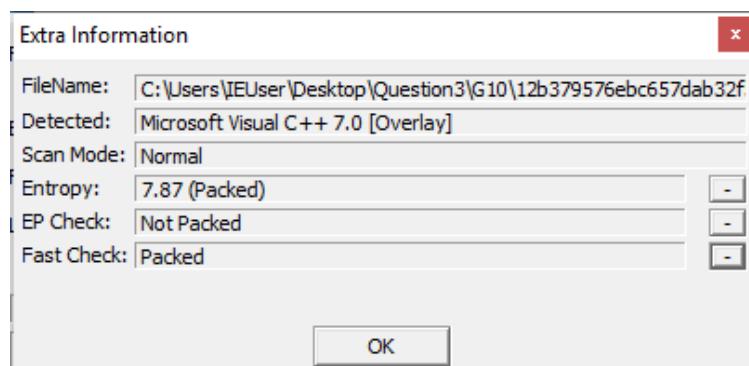
- e) Count the number of DLL imports with the DLL names from the PE details

There are 2 DLL Imports  
KERNEL32.dll and SHELL32.dll

Imports Viewer						
DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk	
KERNEL32.dll	00007D04	00000000	00000000	0000805C	00007000	
SHELL32.dll	00007EE0	00000000	00000000	0000807A	0000710C	

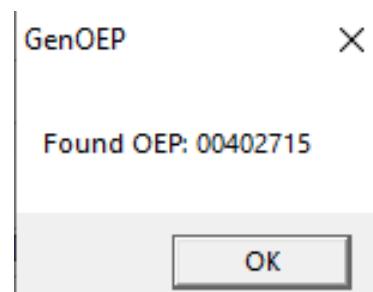
- f) Goto Extra Information section of the PEid Tool, click on the (-) icon and calculate the Entropy, EP check output, and Fast check output.

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



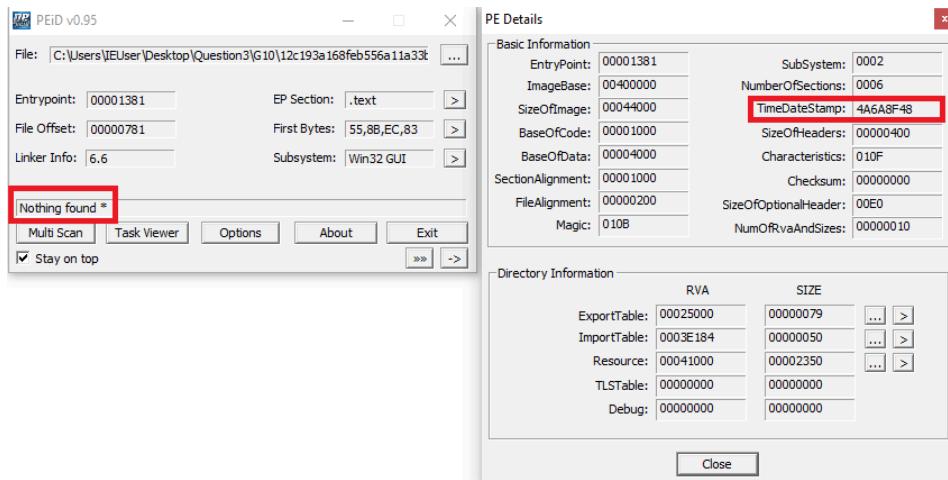
## Executable No. 2) (The file of size 133kb)

- 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.

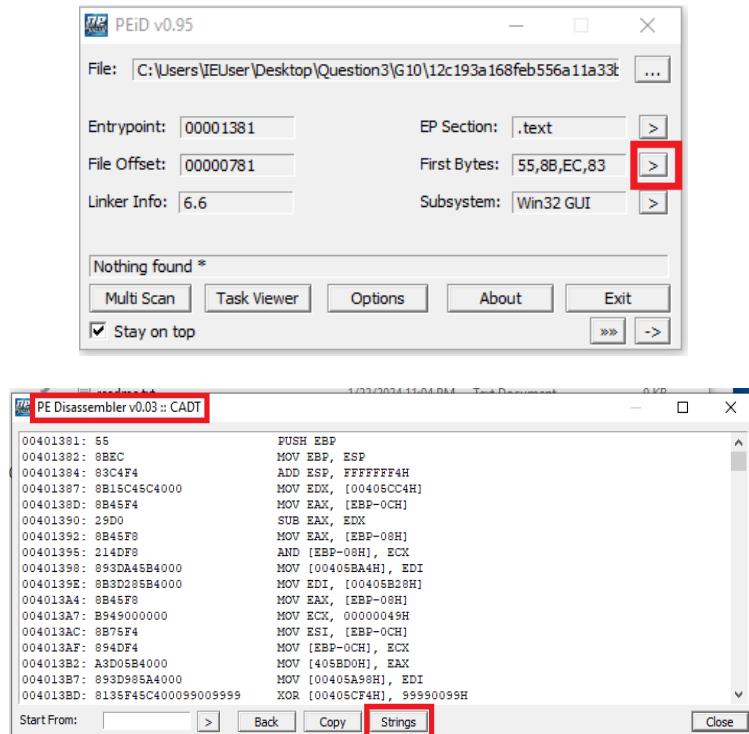
There are 6 PE Sections in Section Viewer. Namely ".text, .edata, .idata, .bdata, .data, .rsrc"

None of those appear to be suspicious

Section Viewer						
Name	V. Offset	V. Size	R. Offset	R. Size	Flags	
.text	00001000	00002964	00000400	00002A00	60000020	
.data	00004000	00020A00	00002E00	00002A00	C0000040	
.edata	00025000	000183BF	00005800	00018400	40000040	
.idata	0003E000	00001040	0001DC00	00001200	40000040	
.bdata	00040000	0000015E	0001EE00	00000200	40000040	
.rsrc	00041000	00002350	0001F000	00002400	40000040	

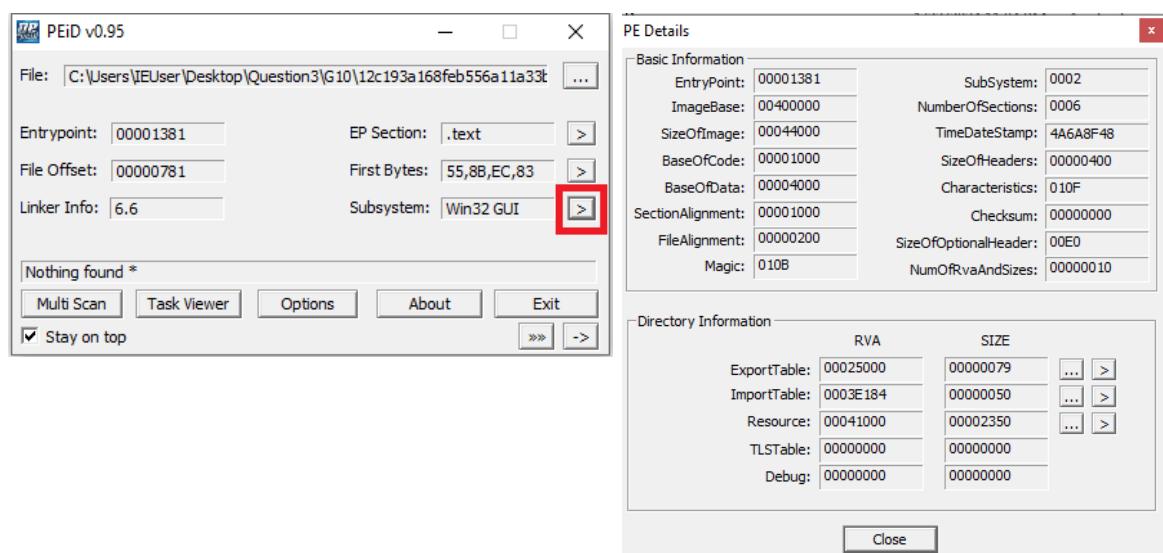
c. In which section of the PEid Tool will you find the PE disassembler and strings information?

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

Imports Viewer						
DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk	
ole32.dll	0003E1D4	00000000	00000000	0003E421	0003E000	
KERNEL32.DLL	0003E2FC	00000000	00000000	0003E93F	0003E128	
USER32.DLL	0003E200	00000000	00000000	0003E7E1	0003E02C	

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

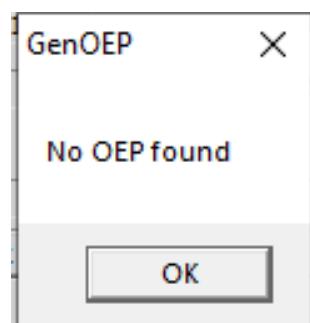
Extra Information

FileName:	C:\Users\IEUser\Desktop\Question3\G10\12c193a168feb556a11a3
Detected:	Nothing found *
Scan Mode:	Deep
Entropy:	7.16 (Packed)
EP Check:	Not Packed
Fast Check:	Packed

OK

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

No OEP found



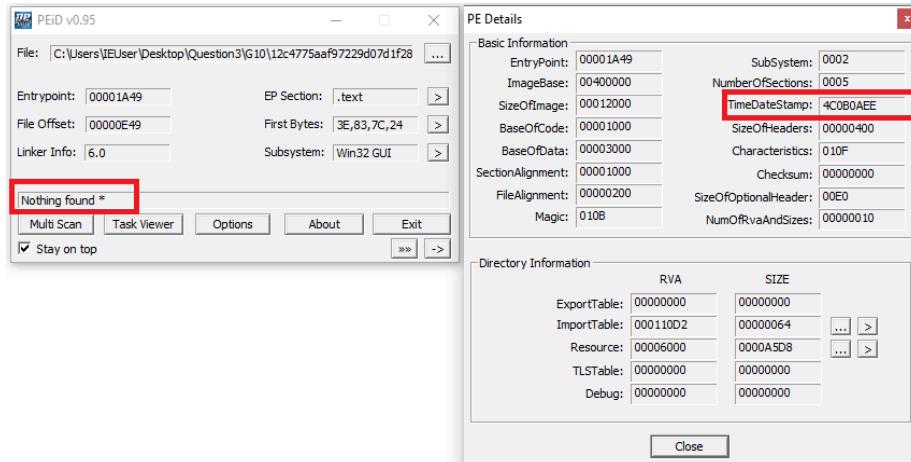
### Executable No. 3) (The file of size 53kb)

- 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



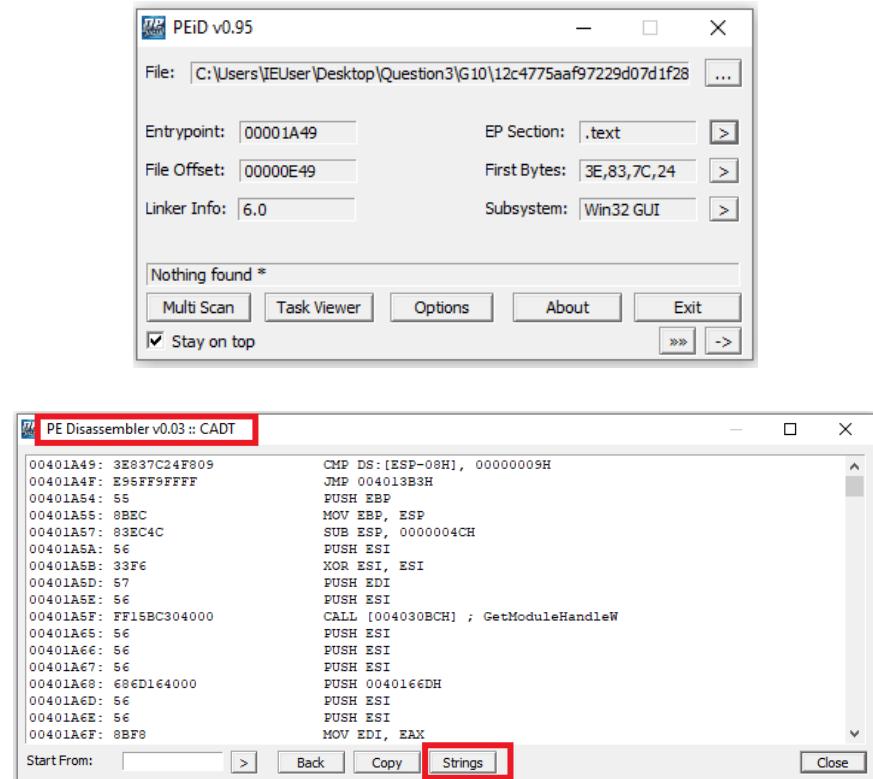
- b) Find the following details from the EP Section: count the number of PE sections from the section viewer and also point out any suspicious PE section name with an explanation.

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

Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	000016E6	00000400	00001800	E0000060
.rdata	00003000	0000080E	00001C00	00000A00	E0000060
.data	00004000	00001D09	00002600	00000600	E0000060
.rsrc	00006000	0000B000	00002C00	0000A600	E0000060
.Katja	00011000	00001000	0000D200	00000136	C0000040

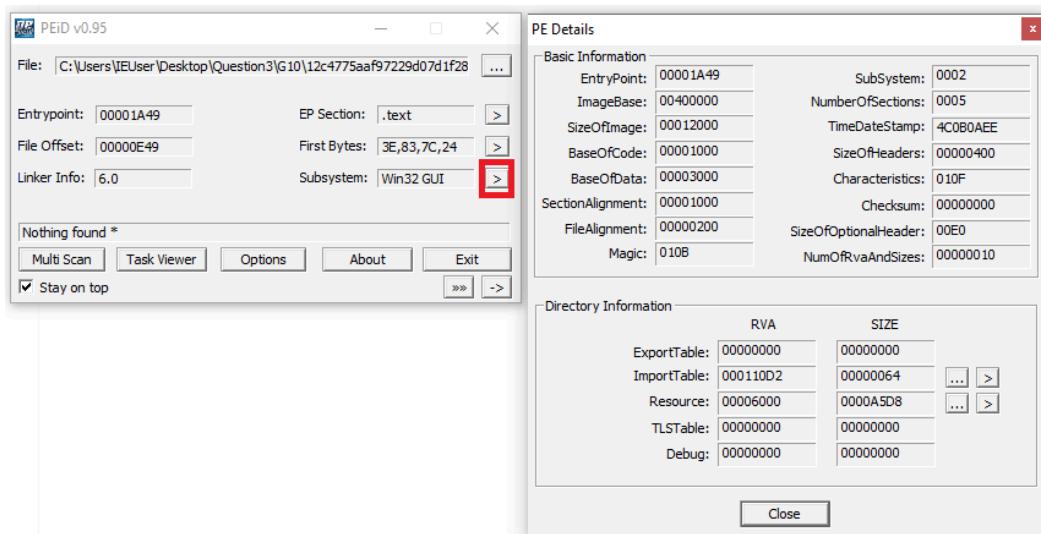
**c) In which section of the PEid Tool will you find the PE disassembler and strings information?**

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

Imports Viewer						
DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk	
KERNEL32.dll	00003200	00000000	00000000	00003542	00003048	
USER32.dll	000032CC	00000000	00000000	00003614	00003114	
ADVAPI32.dll	000031B8	00000000	00000000	00003760	00003000	
MSVCRT.dll	00003290	00000000	00000000	00003802	000030D8	

- 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

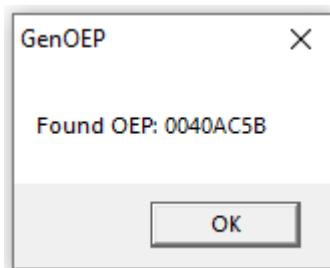
Extra Information

FileName:	C:\Users\IEUser\Desktop\Question3\G10\12c4775aa97229d07d1f;
Detected:	Nothing found *
Scan Mode:	Deep
Entropy:	5.90 (Not Packed)
EP Check:	Not Packed
Fast Check:	Not Packed

OK

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

OEP found: 0040AC5B



## PART 2: ANALYSIS USING PEStudio

### 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

property	value	detail
<u>characteristics</u>	0x010F	
dynamic-link-library	0x0000	false
<b>32-bit words support</b>	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
<b>general</b>		
<u>compiler-stamp</u>	0x494D764E	Sat Dec 20 22:48:46 2008   UTC
<u>size-of-optional-header</u>	0x00E0	224 bytes
<u>signature</u>	0x00004550	PE00
<u>machine</u>	0x014C	Intel-386
<u>sections-count</u>	0x0004	4
<u>pointer-symbol-table</u>	0x00000000	0x00000000
<u>number-of-symbols</u>	0x00000000	0x00000000

### C. Terminal server aware: False

property	value	detail
<u>characteristics</u>	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structured-exception-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
<b>terminal-server-aware (TSA)</b>	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
<b>general</b>		
<u>subsystem</u>	0x0002	GUI
<u>magic</u>	0x010B	PE
<u>file-checksum</u>	0x00000000	0x0008F918 (expected)
<u>entry-point</u>	0x00002715	section:text
<u>base-of-code</u>	0x00001000	section:text
<u>base-of-data</u>	0x00007000	section:rdata
<u>size-of-code</u>	0x00006000	24576 bytes
<u>size-of-initialized-data</u>	0x00071000	462848 bytes

D. **Rich Header Info:** Yes, the executable contains rich header

Import: Visual Studio

Linker: Visual Studio 2003 - 7.10

The screenshot shows the PEStudio interface with the file 'pestudio 9.57 - Malware Initial Assessment' open. The left pane displays a tree view of file sections and properties. The right pane contains two tables: one for 'product-id' and 'build-id', and another for file properties.

product-id (9)	build-id (6)	count
AliasObj710	Visual Studio 2003 - 7.10 beta	1
Utc1310_C	Visual Studio 2003 - 7.10	40
Masm710	Visual Studio 2003 - 7.10	12
Implib700	Visual Studio 2002 - 7.0 XP DDK	2
Implib710	Visual Studio 2003 - 7.10	3
<b>Import</b>	Visual Studio	68
Utc1310_CPP	Visual Studio 2003 - 7.10	3
Cvtres710	Visual Studio 2003 - 7.10 Free Toolkit	1
<b>Linker710</b>	Visual Studio 2003 - 7.10	1

property	value
offset	0x00000080
size	120 bytes
checksum-builtin	0xE0BAFD51
checksum-computed	0xE0BAFD51
footprint > sha256	F53DC6F15CC41F2D2C58EC600DC198C...

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

F. **Code integrity:** False

The screenshot shows the PEStudio interface with the same file open. The left pane shows the file structure. The right pane displays a table of file properties, with the 'characteristics' section highlighted by a red box.

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
<b>data-execution-prevention (DEP)</b>	0x0000	false
code-integrity (CI)	0x0000	false
structured-exception-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x0108	PE
file-checksum	0x00000000	0x0008F918 (expected)
entry-point	0x00002715	section:.text
base-of-code	0x00001000	section:.text
base-of-data	0x00007000	section:.rdata
size-of-code	0x00006000	24576 bytes
size-of-initialized-data	0x00071000	462848 bytes

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

MSEdge - Win10 (Initial Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

**c:\users\ieuser\Desktop\question3\g10\12b37957**

- indicators (imports > flag)
  - footprints (count > 10)
  - virusTotal (error)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 184 bytes)
  - rich-header (tooling > Visual Studio 2003)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 4)
  - sections (count > 4)
  - libraries (count > 2)
  - imports (flag > 67)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (n/a)
  - resources (count > 21)
  - strings (count > 14863)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (entropy > zero)

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x494D764E	Sat Dec 20 22:48:46 2008   UTC
size-of-optimal-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections-count	0x0004	4
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

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

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

MSEdge - Win10 (Initial Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

**c:\users\ieuser\Desktop\question3\g10\12b37957**

- indicators (imports > flag)
  - footprints (count > 10)
  - virusTotal (error)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 184 bytes)
  - rich-header (tooling > Visual Studio 2003)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 4)
  - sections (count > 4)
  - libraries (count > 2)
  - imports (flag > 67)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (n/a)
  - resources (count > 21)
  - strings (count > 14863)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (entropy > zero)

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structuredException-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00000000	0x0008F918 (expected)
entry-point	0x00002715	section:text
base-of-code	0x00001000	section:text
base-of-data	0x00007000	section:rdata
size-of-code	0x00006000	24576 bytes
size-of-initialized-data	0x000071000	462848 bytes
size-of-uninitialized-data	0x00000000	0 bytes
size-of-image	0x00078000	491520 bytes
size-of-header	0x00001000	4096 bytes
size-of-stack-reserve	0x00010000	1048576 bytes
size-of-stack-commit	0x00001000	4096 bytes
size-of-heap-reserve	0x00010000	1048576 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00001000	4096 bytes
file-alignment	0x00001000	4096 bytes
directories-count	0x00000010	16
LoaderFlags	0x00000000	0x00000000
Win32VersionValue	0x00000000	0x00000000
image-base	0x00400000	0x00400000
linker-version	7.10	7.10
os-version	4.0	Windows NT 4.0
image-version	0.0	0.0
subsystem-version	4.0	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

level
1
2
2
2
2
2
3
3
3
3
3
3
3
3
3
3
3
3

File Machine View Input Devices Help  
pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]  
file settings about

indicator (17)	detail
imports > flag	13
overlay > size	73728 bytes
overlay > entropy	0.000
string > suspicious	2074 bytes
file > checksum	0x00000000
groups > API	file   diagnostic   synchronization   reconnaissance   dynamic-library   ex...
mitre > technique	T1082   T1106   T1497   T1057   T1055   T1124
file > entropy	7.220
file > signature	Microsoft Visual C++ 7.0 MFC
file > sha256	12B379576EBC657DAB32F5525A28221D5D25FD755CBE32156F181B971DD...
file > size	565248 bytes
rich-header > checksum	0xE0BAFD51
rich-header > offset	0x00000080
rich-header > footprint	F53DC6F15CC41F2D2C58EC600DC198C62E460B8FCC5F11A5FD14D2BE9...
file > tooling	Visual Studio 2003
file > subsystem	GUI
imphash > md5	FB815ACBC7109E8C83537D7D9C7020BE

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

property	value
footprint > sha256	67B443C4C6271E45029E159DB4D3E86A2957D15779A7CD62A739C6BA6DB4695C
size	0x40 (64 bytes)
entropy	4.430
file-ratio	0.00 %
file-header-offset	0x000000F8

File Machine View Input Devices Help  
pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]  
file settings about

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

The screenshot shows the PEStudio interface with the file 'pestudio 9.57 - Malware Initial Assessment' open. The left pane displays the file structure of 'c:\users\ieuser\Desktop\question3\g10\12b3795'. The right pane is a table titled 'library (2)' showing imports for two DLLs:

library (2)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (67)
KERNEL32.dll	-	-	0x00007DD4	0x00007000	implicit	66
SHELL32.dll	-	-	0x00007E00	0x0000710C	implicit	1

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

## N. Cryptography Group Imports: 0

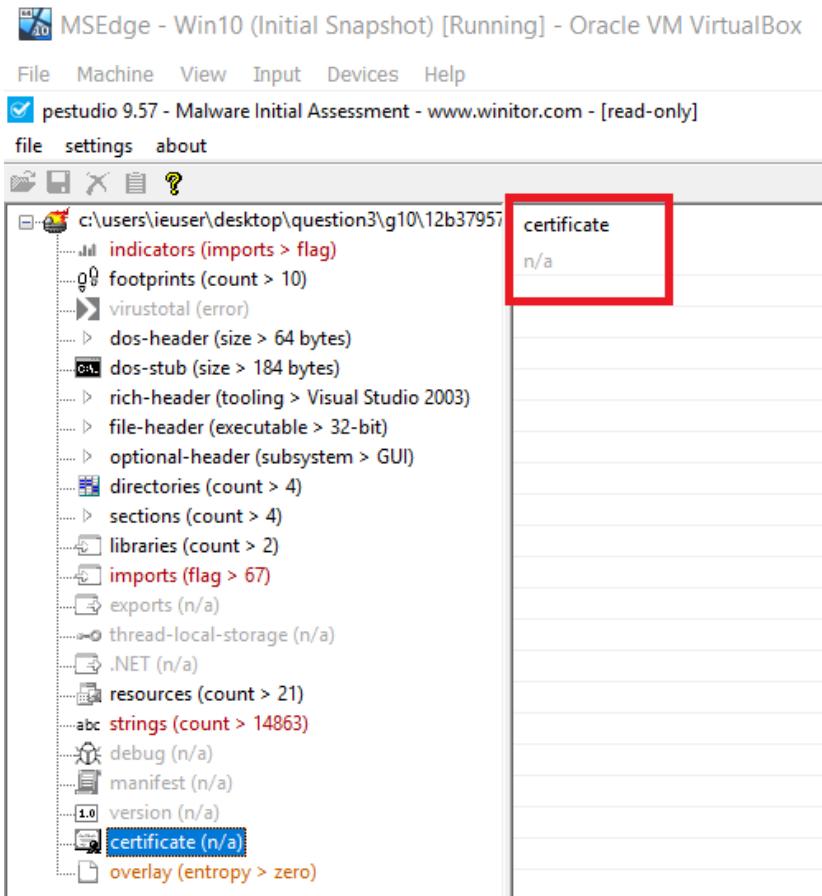
Execution group imports: 15

Obfuscation group imports: 0

The screenshot shows the PEStudio interface with the same file open. The left pane shows the file structure. The right pane is a detailed table of imports, with the 'flag (13)' column highlighted by a red box. This table includes columns for first-thunk-original (INT), first-thunk (IAT), hint, and group. The 'group (9)' column indicates the category of each import.

imports (67)	flag (13)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (9)
GetTickCount	-	0x000080F6	0x000080F6	469 (0x01D5)	reconnaissance
GetCurrentProcessId	x	0x0000811C	0x0000811C	315 (0x013B)	reconnaissance
GetSystemInfo	x	0x0000837A	0x0000837A	443 (0x01BB)	reconnaissance
VirtualProtect	x	0x00008368	0x00008368	889 (0x0379)	memory
VirtualAlloc	x	0x0000823C	0x0000823C	522 (0x020A)	memory
VirtualAllocEx	x	0x0000824A	0x0000824A	520 (0x0208)	memory
VirtualFree	-	0x00008258	0x00008258	886 (0x0376)	memory
VirtualFreeEx	-	0x00008266	0x00008266	524 (0x020C)	memory
VirtualQuery	-	0x00008294	0x00008294	891 (0x037B)	memory
HeapAlloc	-	0x000082C6	0x000082C6	518 (0x0206)	memory
VirtualAllocEx	x	0x000082D2	0x000082D2	883 (0x0373)	memory
HeapReAlloc	-	0x000082E2	0x000082E2	528 (0x0210)	memory
HeapSize	-	0x000082F0	0x000082F0	530 (0x0212)	memory
GetStringTypeA	-	0x00008332	0x00008332	434 (0x01B2)	memory
GetStringTypeW	x	0x00008344	0x00008344	437 (0x01B5)	memory
WriteFile	-	0x00007EF6	0x00007EF6	916 (0x0394)	file
CreateFileA	-	0x00007F02	0x00007F02	77 (0x004D)	file
GetTempPathA	-	0x00007F8E	0x00007F8E	459 (0x01CB)	file
GetFileAttributesA	-	0x00008046	0x00008046	342 (0x0156)	file
GetSystemTimeAsFileTime	-	0x00008132	0x00008132	448 (0x01C0)	file
GetFileType	-	0x0000822E	0x0000822E	350 (0x015E)	file
Sleep	-	0x00007FB6	0x00007FB6	839 (0x0347)	execution
GetCurrentDirectoryA	-	0x00007F8E	0x00007F8E	312 (0x013B)	execution
Process32Next	x	0x00007FFC	0x00007FFC	652 (0x028C)	execution
Process32First	x	0x00008018	0x00008018	650 (0x028A)	execution
CreateToolhelp32Snapshot	x	0x0000802A	0x0000802A	108 (0x006C)	execution
ExitProcess	-	0x00008086	0x00008086	175 (0x00AF)	execution
GetCommandLineA	-	0x0000808A	0x0000808A	264 (0x0108)	execution
GetCurrentThreadId	x	0x00008106	0x00008106	318 (0x013E)	execution
TerminateProcess	x	0x0000814C	0x0000814C	847 (0x034F)	execution
GetCurrentProcess	x	0x00008160	0x00008160	314 (0x013A)	execution
FreeEnvironmentStringsA	-	0x000081A0	0x000081A0	237 (0x00ED)	execution
GetEnvironmentStrings	x	0x000081BA	0x000081BA	333 (0x014D)	execution
FreeEnvironmentStringsW	-	0x000081D2	0x000081D2	238 (0x00EE)	execution
GetEnvironmentStringsW	x	0x00008202	0x00008202	335 (0x014F)	execution
ShellExecuteA	x	0x0000806A	0x0000806A	262 (0x0106)	execution
UnhandledExceptionFilter	-	0x00008184	0x00008184	864 (0x0360)	exception
FreeLibrary	-	0x00007F5E	0x00007F5E	239 (0x00EF)	dynamic-library
GetProcAddress	-	0x00007F6C	0x00007F6C	408 (0x0198)	dynamic-library
LoadLibraryA	-	0x00007F7E	0x00007F7E	584 (0x0248)	dynamic-library

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

MSEdge - Win10 (Initial Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

c:\users\ieuser\Desktop\question3\g10\12c193a1

indicators (imports > flag)

- footprints (count > 11)
- virusTotal (error)
- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 3)
- sections (flag > name)
- libraries (count > 3)
- imports (flag > 94)
- exports (items > 3)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (count > 3761)
- debug (n/a)
- manifest (n/a)

version (FileDescription > FTVideo Component)

certificate (n/a)

overlay (n/a)

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4A6A8F48	Sat Jul 25 04:51:20 2009   UTC
size-of-optimal-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections-count	0x0006	6
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

- c. Terminal server aware: False

MSEdge - Win10 (Initial Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

c:\users\ieuser\Desktop\question3\g10\12c193a1

indicators (imports > flag)

- footprints (count > 11)
- virusTotal (error)
- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 3)
- sections (flag > name)
- libraries (count > 3)
- imports (flag > 94)
- exports (items > 3)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (language > flag)
- strings (count > 3761)
- debug (n/a)
- manifest (n/a)

version (FileDescription > FTVideo Component)

certificate (n/a)

overlay (n/a)

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structured exception handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00000000	0x0002C2DF (expected)
entry-point	0x00001381 (original)	section:.text
base-of-code	0x00001000	section:.text
base-of-data	0x00004000	section:.data
size-of-code	0x00002A00	10752 bytes
size-of-initialized-data	0x0001E600	124416 bytes
size-of-uninitialized-data	0x00000000	0 bytes

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

MSEdge - Win10 (Initial Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

c:\users\ieuser\Desktop\question3\g10\12c193a1

- indicators (imports > flag)
- footprints (count > 11)
- virustotal (error)
- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (n/a) rich-header
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 3)
- sections (flag > name)
- libraries (count > 3)
- imports (flag > 94)

n/a

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

f. **Code integrity:** False

MSEdge - Win10 (Initial Snapshot) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

c:\users\ieuser\Desktop\question3\g10\12c193a1

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structured-exception-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00000000	0x0002C2DF (expected)
entry-point	0x00001381 [original]	section:text
base-of-code	0x00001000	section:text
base-of-data	0x00004000	section:data
size-of-code	0xffffffffffff	10752 bytes

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

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4A6A8F48	Sat Jul 25 04:51:20 2009   UTC
size-of-optimal-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections-count	0x0006	6
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

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

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

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structured-exception-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x10B	PE
file-checksum	0x00000000	0x0002C2DF (expected)
entry-point	0x00001381 (original)	section:text
base-of-code	0x00001000	section:text
base-of-data	0x00004000	section:data
size-of-code	0x00002A00	10752 bytes
size-of-initialized-data	0x0001E600	124416 bytes
size-of-uninitialized-data	0x00000000	0 bytes
size-of-image	0x00044000	278528 bytes
size-of-headers	0x00000400	1024 bytes
size-of-stack-reserve	0x00100000	1048576 bytes
size-of-stack-commit	0x00100000	4096 bytes
size-of-heap-reserve	0x00100000	1048576 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00001000	4096 bytes
file-alignment	0x00000200	512 bytes
directories-count	0x00000010	16
LoaderFlags	0x00000000	0x00000000
Win32VersionValue	0x00000000	0x00000000
image-base	0x00400000	0x00400000
linker-version	6.6	6.6
os-version	4.0	Windows NT 4.0
image-version	0.0	0.0
subsystem-version	4.0	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

	indicator (13)	detail	level
imports > flag	11		1
resources > language	Russian		2
file > checksum	0x00000000		2
sections > name > flag	.bdata		2
groups > API	reconnaissance   synchronization   execution   memory   file   diagnostic...		2
mitre > technique	T1057   T1124   T1055   T1106   T1056   T1179   T1115		2
file > entropy	7.158		3
file > sha256	12C193A168FEB556A11A33BE9078AE2FB6D9D4337E42FD867B1672F101C...		3
file > size	136192 bytes		3
file-name > version	StraterHF.exe		3
file > subsystem	GUI		3
imphash > md5	40CD2B2602F617279D0E9AA19DAE0BDA		3
file-name > exports	StraterHF.exe		3

k. What is the Dos-header entropy: 2.602

property	value
footprint > sha256	0D9B2FAEEB2E6CDE11EB5D57D736ADBD9C6AAB1DA3DBC95ABC5EF3DE219914F3
size	0x40 (64 bytes)
entropy	2.602
file-ratio	0.00 %
file-header-offset	0x000000D0

## 1. Implicit type libraries:

There are 3 implicit type libraries.

Ole32.dll, KERNEL32.dll and USER32.dll

library (3)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (94)
ole32.dll	-	-	0x0003E1D4	0x0003E000	implicit	10
KERNEL32.DLL	-	-	0x0003E2FC	0x0003E128	implicit	22
USER32.DLL	-	-	0x0003E200	0x0003E02C	implicit	62

m. Count the number of red flag imports: 11

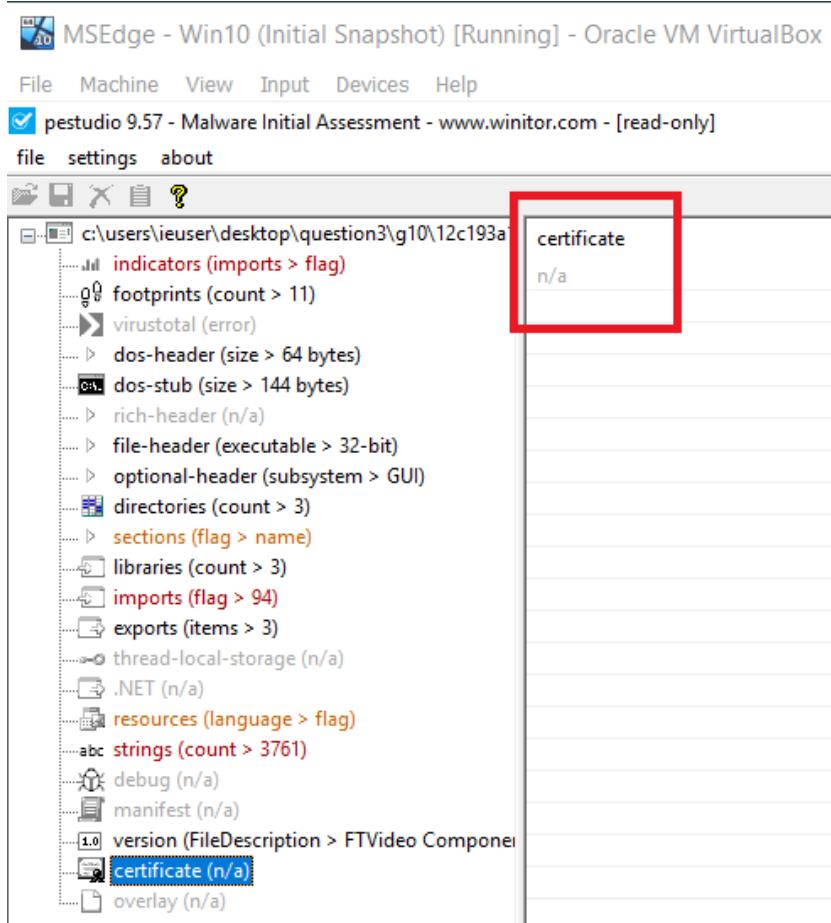
n. Cryptography Group Imports: 0

Execution group imports: 2

obfuscation group imports: 0

imports (94)	flag (11)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (12)
SetWindowsHookExA	x	0x0003E5B4	0x0003E5B4	1 (0x0001)	hooking
UnhookWindowsHookEx	x	0x0003E73A	0x0003E73A	23 (0x0017)	hooking
WriteFile	x	0x0003E875	0x0003E875	41 (0x0029)	file
GetTempPathA	-	0x0003E89A	0x0003E892	39 (0x0027)	file
FindClose	-	0x0003E8AF	0x0003E8AF	127 (0x007F)	file
GetFullPathNameA	-	0x0003E8C9	0x0003E8C9	4 (0x0004)	file
GetFileSize	-	0x0003E8ED	0x0003E8ED	49 (0x0031)	file
GetFileType	-	0x0003E931	0x0003E931	188 (0x00BC)	file
ExitProcess	-	0x0003E838	0x0003E838	55 (0x0037)	execution
PostMessageA	-	0x0003E71C	0x0003E71C	123 (0x007B)	execution
LoadLibraryA	-	0x0003E915	0x0003E915	200 (0x00C8)	dynamic-library
GetLastError	-	0x0003E8FB	0x0003E8FB	73 (0x0049)	diagnostic
SetClipboardData	x	0x0003E612	0x0003E612	81 (0x0051)	data-exchange
StOpenStorage	x	0x0003E358	0x0003E358	206 (0x00CE)	-
CLSIDFromString	-	0x0003E369	0x0003E369	208 (0x00D0)	-
StringFromID	-	0x0003E37B	0x0003E37B	183 (0x0087)	-
WriteClassStn	-	0x0003E38B	0x0003E38B	60 (0x003C)	-
CoDisconnectObject	-	0x0003E39B	0x0003E39B	34 (0x0022)	-
CoUnmarshalInterface	-	0x0003E3B0	0x0003E3B0	176 (0x00B0)	-
CoGetMalloc	-	0x0003E3C7	0x0003E3C7	120 (0x0078)	-
OleRegGetUserType	-	0x0003E3D5	0x0003E3D5	186 (0x00BA)	-
CoCreateFreeThreadedMars...	-	0x0003E3E9	0x0003E3E9	24 (0x0018)	-

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

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4C0B0AEE	Sun Jun 06 02:41:50 2010   UTC
size-of-optimal-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections-count	0x0005	5
pointer-symbol-table	0x726F4C5B	0x00000000 (expected)
number-of-symbols	0x5D455064	0x00000000 (expected)

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

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structured-exception-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00000000	0x0001567C (expected)
entry-point	0x00001A49	section:text
base-of-code	0x00001000	section:text
base-of-data	0x00003000	section:rdata

d) **Rich Header Info:** Yes, the executable contains rich header

Import: Visual Studio

Linker: Visual Studio 6.0 - 6.0

The screenshot shows the PEStudio interface with the file 'pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]' open. The left pane displays a tree view of file sections and characteristics, including indicators, footprints, virustotal, dos-header, dos-stub, rich-header, file-header, optional-header, directories, sections, libraries, imports, exports, thread-local-storage, .NET, resources, strings, debug, manifest, version, certificate, and overlay. The right pane contains two tables. The first table, titled 'product-id (6)', lists products and their build IDs and counts: Masm613 (Visual Studio 6.0 MASM - 6.13 SP1, count 2), Linker600 (Visual Studio 6.0 - 6.0, count 2), Import (Visual Studio, count 81), Implib710 (Visual Studio 2003 - 7.10 SDK, count 7), Utc12\_CPP (Visual Studio 6.0 - 6.0, count 3), and Cvtres500 (Visual Studio 5.0 CvtRes.exe - 5.0, count 1). The second table, titled 'property' (with columns 'property' and 'value'), lists properties like offset (0x00000080), size (80 bytes), checksum-builtin (0xB7851239), checksum-computed (0xB7851239), and footprint > sha256 (8E4FA9395B4174D0234F3240CDDCCA...).

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

f) **Code integrity:** False

The screenshot shows the PEStudio interface with the same file open. The left pane shows the same tree view of file sections and characteristics. The right pane displays a table titled 'characteristics' with columns 'property', 'value', and 'detail'. It lists various protection mechanisms: address-space-layout-randomization (ASLR) (0x0000, false), Control-flow Enforcement Technology (/CETCOMPACT) (0x0000, false), data-execution-prevention (DEP) (0x0000, false), code-integrity (CI) (0x0000, false), structured-exception-handling (SEH) (0x0000, true), windows-driver-model (WDM) (0x0000, false), terminal-server-aware (TSA) (0x0000, false), control-flow-guard (CFG) (0x0000, false), image-bound (0x0000, false), image-isolation (0x0000, false), High-Entropy (0x0000, false), and AppContainer (0x0000, false). Below this is another table titled 'general' with columns 'property', 'value', and 'detail'. It includes entries for subsystem (0x0002, GUI), magic (0x010B, PE), file-checksum (0x00000000, 0x0001567C (expected)), entry-point (0x00001A49, section:text), base-of-code (0x00001000, section:text), base-of-data (0x00003000, section:rdata), and size-of-code (0x00001800, 6144 bytes).

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

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4C0B0AEE	Sun Jun 06 02:41:50 2010   UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections-count	0x0005	5
pointer-symbol-table	0x726F4C5B	0x00000000 (expected)
number-of-symbols	0x5D455064	0x00000000 (expected)

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

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

property	value	detail
characteristics	0x0000	items
address-space-layout-randomization (ASLR)	0x0000	false
Control-flow Enforcement Technology (/CETCOMPACT)	0x0000	false
data-execution-prevention (DEP)	0x0000	false
code-integrity (CI)	0x0000	false
structured-exception-handling (SEH)	0x0000	true
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x0000	false
image-bound	0x0000	false
image-isolation	0x0000	false
High-Entropy	0x0000	false
AppContainer	0x0000	false
general		
subsystem	0x0002	GUI
magic	0x10B	PE
file-checksum	0x00000000	0x0001567C (expected)
entry-point	0x00091040	section:text
base-of-code	0x00001000	section:.text
base-of-data	0x00003000	section:.rdata
size-of-code	0x00001800	6144 bytes
size-of-initialized-data	0x0000CE00	52736 bytes
size-of-uninitialized-data	0x00000000	0 bytes
size-of-image	0x00012000	73728 bytes
size-of-headers	0x00000400	1024 bytes
size-of-stack-reserve	0x00010000	1048576 bytes
size-of-stack-commit	0x00001000	4096 bytes
size-of-heap-reserve	0x00000000	1048576 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00001000	4096 bytes
file-alignment	0x00000200	512 bytes
directories-count	0x00000010	16
LoaderFlags	0x00000000	0x00000000
Win32VersionValue	0x00000000	0x00000000
image-base	0x00400000	0x00400000
linker-version	6.0	6.0
os-version	4.0	Windows NT 4.0
image-version	0.0	0.0
subsystem-version	4.0	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

detail	level
signature: executable, location: .rsrc, offset: 0x00002D5C, size: 31232 (bytes)	1
signature: executable, location: .rsrc, offset: 0x0000C75C, size: 2560 (bytes)	1
signature: executable, location: .rsrc, offset: 0x00002D5C, size: 31232 (bytes)	1
signature: executable, location: .rsrc, offset: 0x0000C75C, size: 2560 (bytes)	1
.text	1
sections > executable > count	1
sections > self-modifying	1
libraries > spoofing > count	1
libraries > spoofing > count	1
imports > count	1
resources > language	2
resource > unknown	2
resources > file-ratio	2
file > checksum	2
sections > name > flag	2
groups > API > network	2
mrite > technique	2
file > entropy	2
file > sha256	3
file > size	3
rich-header > checksum	3
rich-header > offset	3
rich-header > footprint	3
file > tooling	3
file > subsystem	3

k) What is the Dos-header entropy: 4.540

property	value
footprint > sha256	B991C9D9EBA1B0B28BF80BE8E7CBF1865C5CE9324BFC634044F5153AE84FA329
size	0x40 (64 bytes)
entropy	4.540
file-ratio	0.00 %
file-header-offset	0x000000D0

## I) Implicit type libraries:

There are 2 implicit type libraries.

‘T\$%oL\$÷Øj and PSýØè...ít&ú (don't know in what language it is written or are those encrypted names. Screenshots are attached below)

library (2)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (0)
T\$%oL\$÷Øj	-	-	0x00003200	0x00003048	implicit	0
PSýØè...ít&ú	-	-	0x000032CC	0x00003114	implicit	0

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)

imports  
n/a

certificate (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 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/submit/).
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%02=M4E2ST11NW7%03=M4E2NNT11NW7%04=M4E2ST11NW7%05=M4E2ST11
OS:NW7%06=M4E2ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%0=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%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%0=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%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/submit/).
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%02=M4E2ST11NW7%03=M4E2NNT11NW7%04=M4E2ST11NW7%05=M4E2ST11
OS:NW7%06=M4E2ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%0=M4E2NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%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%0=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%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.

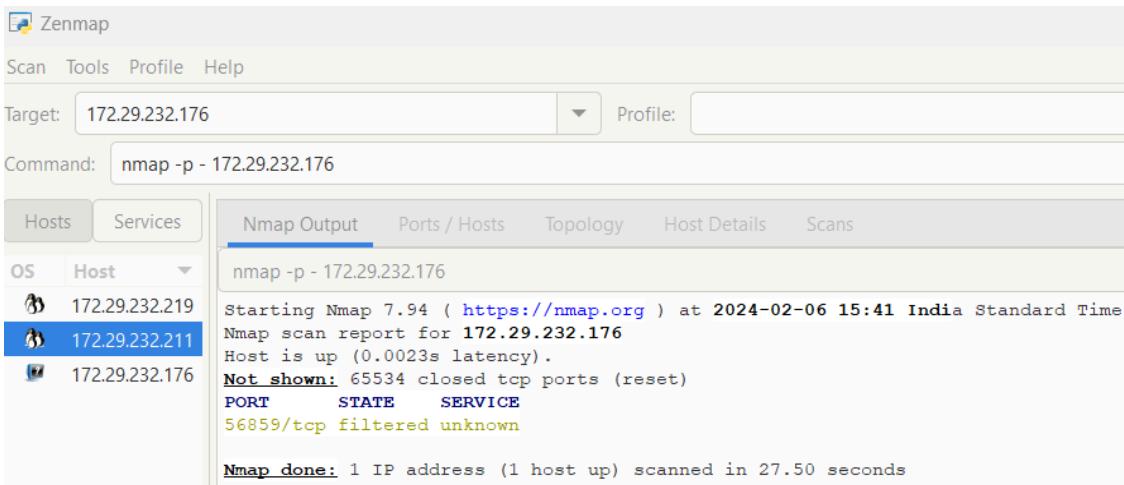
The only vulnerability the given open tcp port 21 has is a remote denial of service attack (Using internet sources). No other major vulnerabilities were found.

**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.



Zenmap

Scan Tools Profile Help

Target: 172.29.232.176 Profile:

Command: nmap -p - 172.29.232.176

Hosts Services

OS Host

172.29.232.219  
172.29.232.211  
**172.29.232.176**  
172.29.232.176

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -p - 172.29.232.176

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 15:41 India Standard Time

Nmap scan report for 172.29.232.176

Host is up (0.0023s latency).

Not shown: 65534 closed tcp ports (reset)

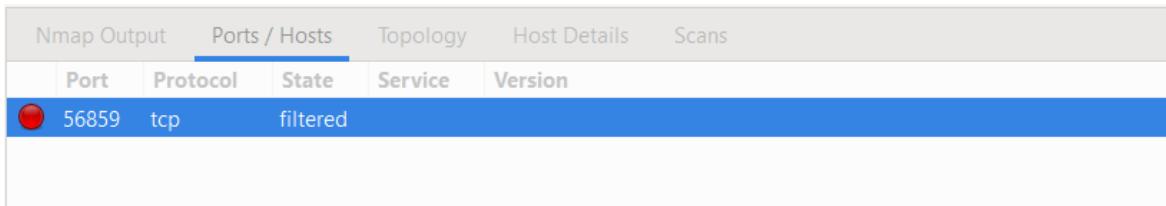
PORT STATE SERVICE

56859/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 27.50 seconds

**Result:** Port 56859/tcp, is showing as **filtered**.

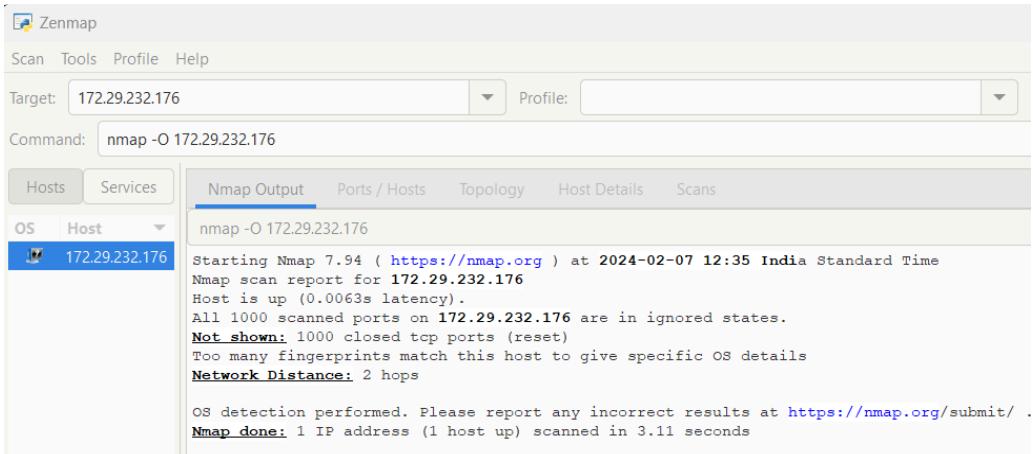
Which means that Nmap was unable to determine the state of this port due to various reasons such as firewall rules, packet filtering, or other network configurations.



Nmap Output Ports / Hosts Topology Host Details Scans					
Port	Protocol	State	Service	Version	
56859	tcp	filtered			

**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.



Zenmap

Scan Tools Profile Help

Target: 172.29.232.176 Profile:

Command: nmap -O 172.29.232.176

Hosts Services

OS Host

**172.29.232.176**

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -O 172.29.232.176

Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 12:35 India Standard Time

Nmap scan report for 172.29.232.176

Host is up (0.0063s latency).

All 1000 scanned ports on 172.29.232.176 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Too many fingerprints match this host to give specific OS details

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 3.11 seconds

**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.

The screenshot shows the Zenmap interface with the target set to 172.29.232.176. The command entered is nmap -sV 172.29.232.176. The Nmap Output tab is selected, displaying the following text:

```
nmap -sV 172.29.232.176
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-07 12:59 India Standard Time
Nmap scan report for 172.29.232.176
Host is up (0.0063s latency).
All 1000 scanned ports on 172.29.232.176 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
```

**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

The screenshot shows the Zenmap interface with the target set to 172.29.232.176. The command entered is nmap --script vuln 172.29.232.176. The Nmap Output tab is selected, displaying the following text:

```
nmap --script vuln 172.29.232.176
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-06 16:23 India Standard Time
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 172.29.232.176
Host is up (0.0039s latency).
All 1000 scanned ports on 172.29.232.176 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 37.59 seconds
```

**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.

**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%G
OS:D=1%SR=105%TI=Z%CI=Z%II=I%TS=A)OPS(01=M4E2ST11NW7%02=M4E2ST11NW7%03=M4E
OS:2NNT11NW7%04=M4E2ST11NW7%05=M4E2ST11NW7%06=M4E2ST11)OPS(01=NNT11%02=NNT1
OS:1%03=M4E2NNT11NW7%04=M4E2ST11NW7%05=M4E2ST11NW7%06=M4E2ST11)OPS(01=NNT11
OS:1%02=NNT11%03=NNT11%04=NNT11%05=NNT11%06=M4E2ST11)OPS(01=NNT11%02=NNT11%0
OS:3=NNT11%04=NNT11%05=NNT11%06=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=FAF%O=M4E2NNSN%W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=
OS:0%F=A%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=0%A=0%F=AS%RD=0%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:0%F=A%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
OS:(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%Q=)T7
OS:(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%IPPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=0%Q=)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) (95%), Linux 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=7.94E-4%D-2/%OT=21%CT=1%CU=32763%PV=Y%DS=2%DC=I%G=Y%TM=65C3656C
OS:>%P=1686_pc-windows-windows)SEQ(CI=Z%II=1)SEQ(SP=104%GC=1%ISR=10%A%TI=Z%C
OS:I=Z%II=I%TS=9)SEQ(SP=104%GC=1%ISR=10%A%TI=Z%II=I%TS=A)SEQ(SP=104%GC
OS:D=1%SR=10%A%TI=Z%CI=Z%II=1%TS=C)SEQ(SP=108%GC=1%SR=109%TI=Z%CI=Z%II=1%
OS:TS=A)OPS(O1=M4E2ST11NW7%02=M4E2ST11NW7%03=M4E2NNT11NW7%04=M4E2ST11NW7%05
OS:=M4E2ST11NW7%06=M4E2ST11)OPS(O1=NNT11%02=M4E2ST11NW7%03=M4E2NNT11NW7%04=
OS:M4E2ST11NW7%05=M4E2ST11NW7%06=M4E2ST11)OPS(O1=NNT11%02=NNT11%03-
OS:NNT11%04=NNT11%05=NNT11%06=NNT11)WIN(W1=1FD%W2=1FD%W3=1FD%W4=1FD%W5=1FD%
OS:W6=FE88)WIN(W1=1FD%W2=1FD%W3=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=%DF-%Y%T=40%W=1F5%0=%CC-N%Q=)ECN(R=%DF-%Y%T=40%W=
OS:5%AF=0%AE2NSNN7%C=Y%Q=)T1(R=%DF=%Y%T=40%W=0%A=0%-=A%RD=0%Q=)T1(R=%DF-
OS:=%Y%T=40%W=0%A=0%F=A%SRD=0%Q=)T1(R=%DF=%Y%T=40%W=0%A=1%F=A%SRD=0%Q=)T2(R
OS:=N)T3(R=%DF=%Y%T=40%W=0%S=A%A=2%F=R%O-XRD=0%Q=)T5(R=%DF=%Y%T=40%W
OS:=0%S=Z%A=S+F=AR%O-XRD=0%Q=)T6(R=%DF=%Y%T=40%W=0%S=A%A=Z%F=R%O-XRD=0%Q=)
OS:T7(R=%DF=%Y%T=40%W=0%S=Z%A=1%F=AR%O-XRD=0%Q=)U1(R=%DF=%Y%T=40%IPL=164%U
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=%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

Zenmap

Scan Tools Profile Help

Target: 172.29.233.230

Command: nmap -O 172.29.233.230

Hosts Services

OS Host

172.29.233.230

Nmap Output Ports / Hosts Topology Host Details Scans

▼ 172.29.233.230

▶ Host Status

▶ Addresses

▼ Operating System

Name: Linux 4.15 - 5.8

Accuracy: 100%

▶ Ports used

▼ OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Linux	Linux	5.X	100%

▶ Comments

### 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.