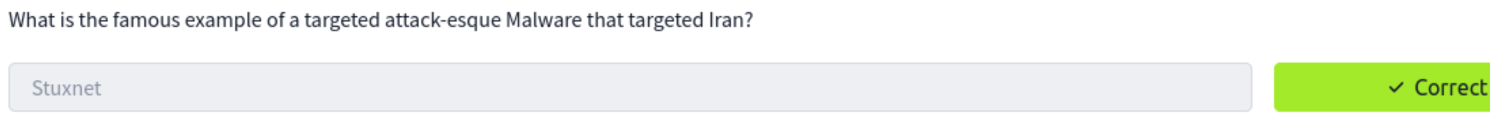
MAL: Malware Introductory

Introduction

Malware is a prevalent topic within cybersecurity and often an unfortunately recurring theme in global news today. Not only is malware analysis a form of incident response, but it also helps in understanding how the behaviors of different malware variants lead to their categorization. This room will serve as a practical introduction to the techniques and tools used in malware analysis. Although brief, it aims to provide a foundation that will be expanded upon in future discussions.

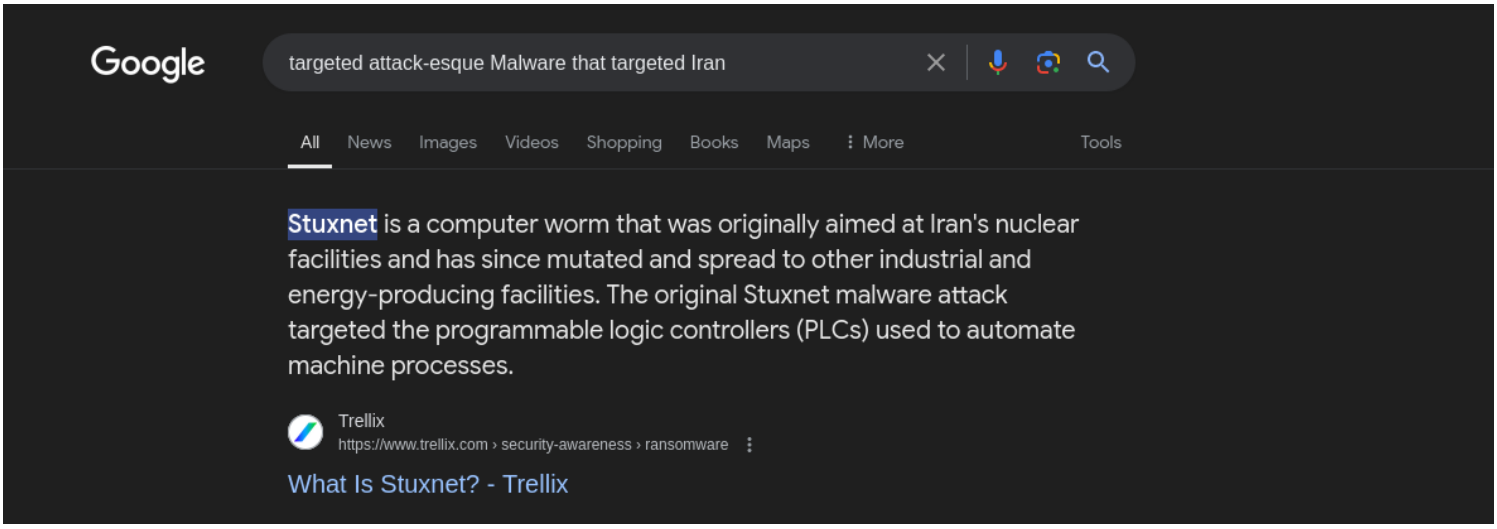
The first few tasks just involve some reading and or Googling. The last few tasks are hands on. If I skip a Task here it's because all you have to do is hit a button, there's no answer needed.
On an admin note, I have been having issues with TryHackMe's US VPN servers lately. OpenVPN would connect, then immediately show an error code. TryHackMe's website would show me as connected but I couldn't even ping THM's VM
Despite all that, I managed to solve every task in this room. Lets get started.



What is the famous example of a targeted attack-esque Malware that targeted Iran?

Stuxnet

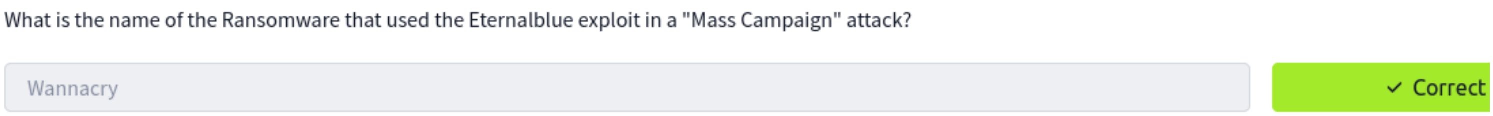
For this task I did a quick google search as shown in the image below.



Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes.

Trellix
https://www.trellix.com › security-awareness › ransomware

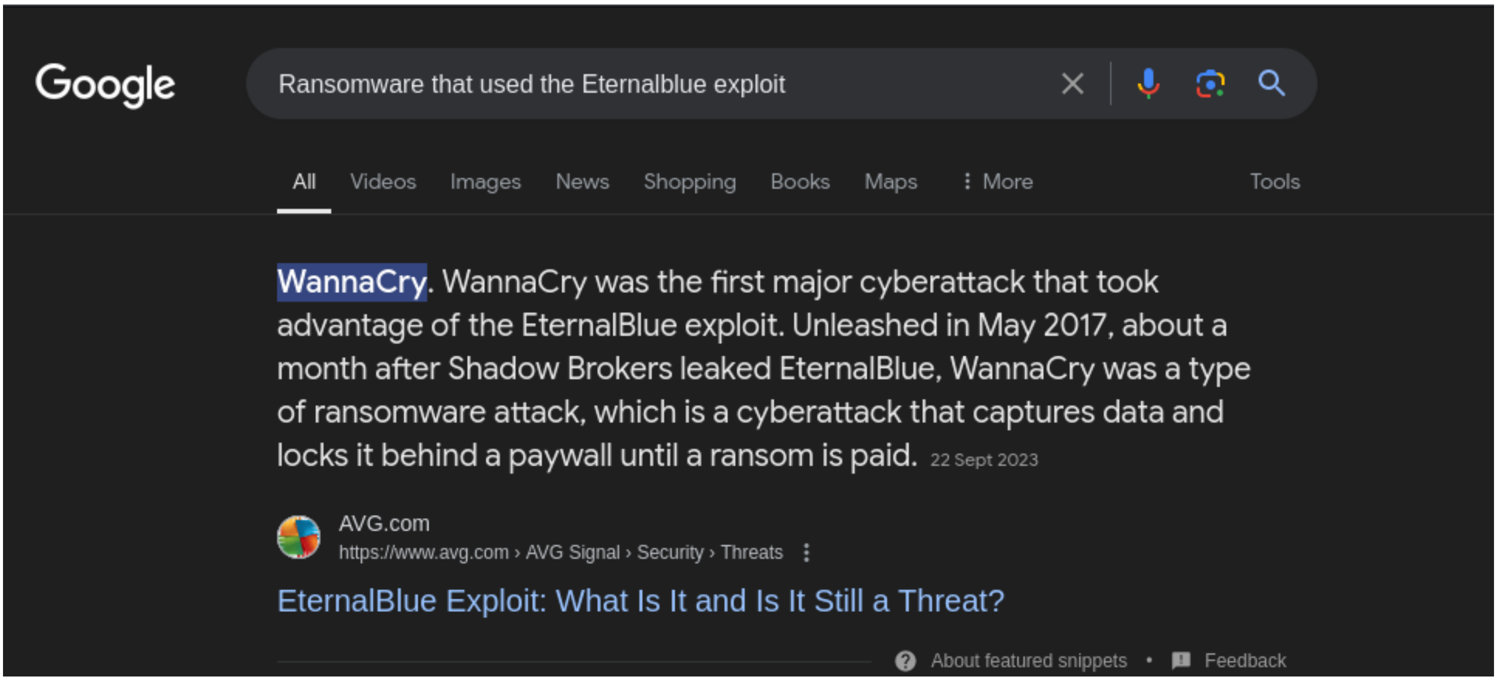
What Is Stuxnet? - Trellix



What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?

Wannacry

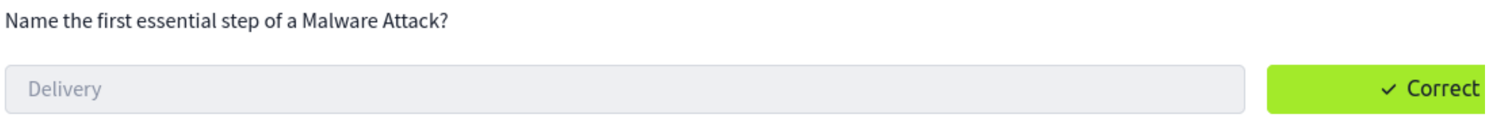
For this task I did a quick google search as shown in the image below.



WannaCry. WannaCry was the first major cyberattack that took advantage of the EternalBlue exploit. Unleashed in May 2017, about a month after Shadow Brokers leaked EternalBlue, WannaCry was a type of ransomware attack, which is a cyberattack that captures data and locks it behind a paywall until a ransom is paid. 22 Sept 2023

AVG.com
https://www.avg.com › AVG Signal › Security › Threats

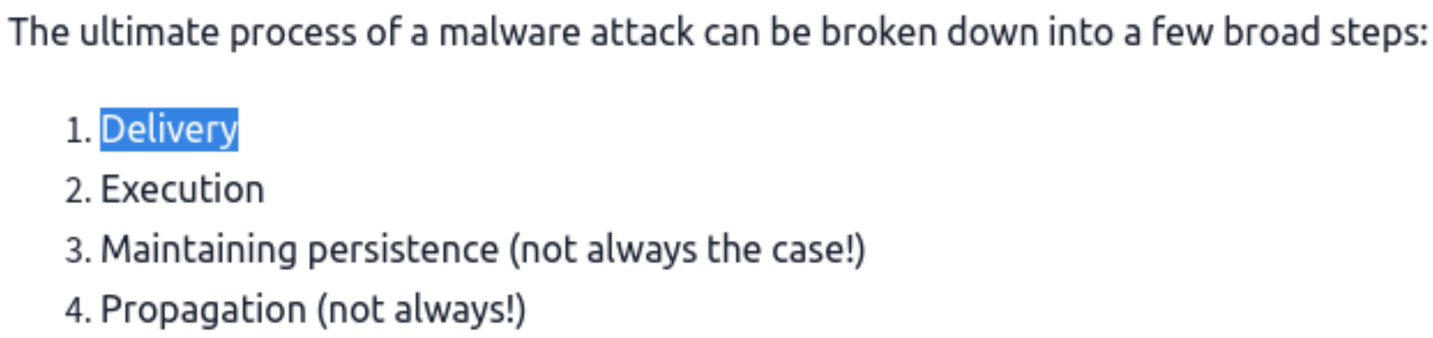
EternalBlue Exploit: What Is It and Is It Still a Threat?



Name the first essential step of a Malware Attack?

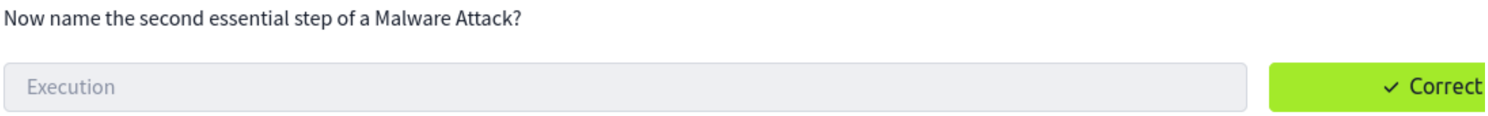
Delivery

For this task, the answer could be retrieved from the notes as shown in the image below.



The ultimate process of a malware attack can be broken down into a few broad steps:

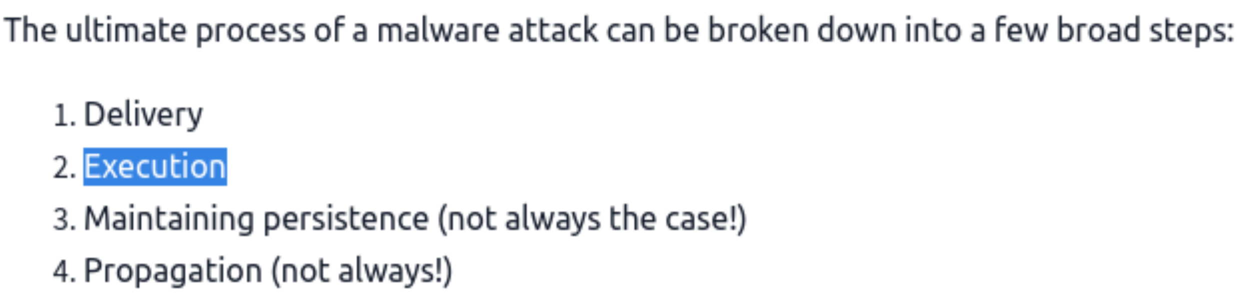
1. Delivery
2. Execution
3. Maintaining persistence (not always the case!)
4. Propagation (not always!)



Now name the second essential step of a Malware Attack?

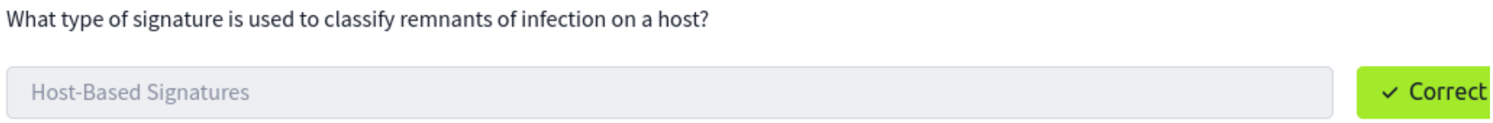
Execution

For this task, the answer could be retrieved from the notes as shown in the image below.



The ultimate process of a malware attack can be broken down into a few broad steps:

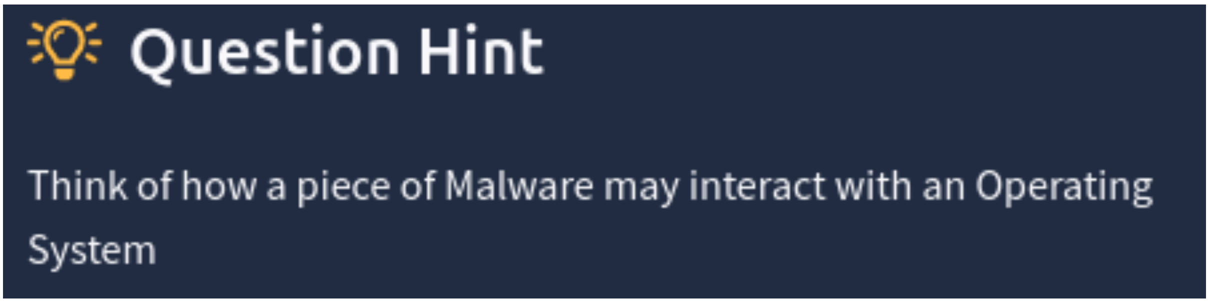
1. Delivery
2. Execution
3. Maintaining persistence (not always the case!)
4. Propagation (not always!)



What type of signature is used to classify remnants of infection on a host?

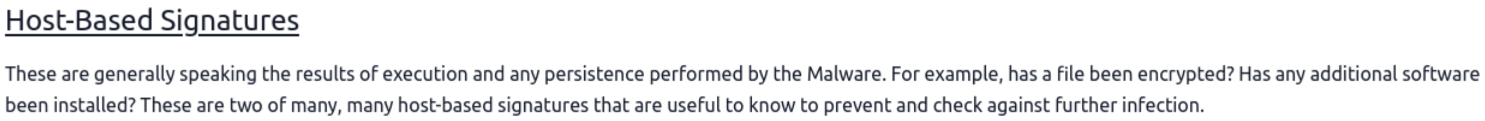
Host-Based Signatures

From reading and understanding the notes together with the hint given in this task, I was able to find the answer.



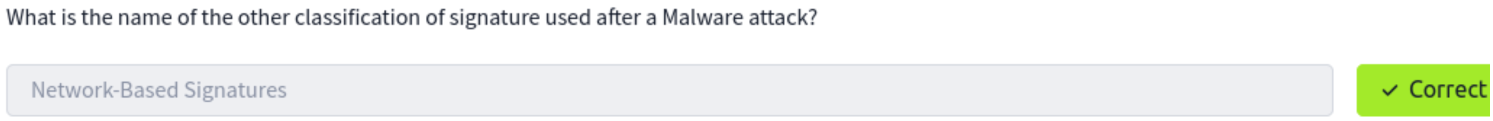
Question Hint

Think of how a piece of Malware may interact with an Operating System



Host-Based Signatures

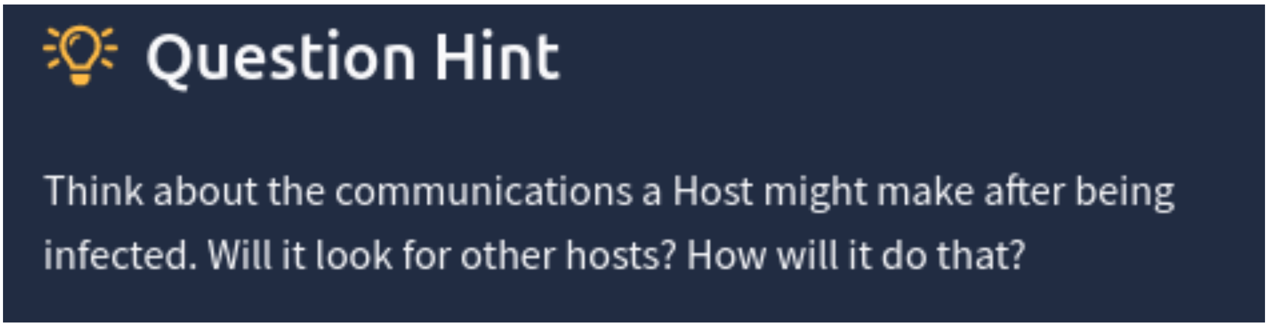
These are generally speaking the results of execution and any persistence performed by the Malware. For example, has a file been encrypted? Has any additional software been installed? These are two of many, many host-based signatures that are useful to know to prevent and check against further infection.



What is the name of the other classification of signature used after a Malware attack?

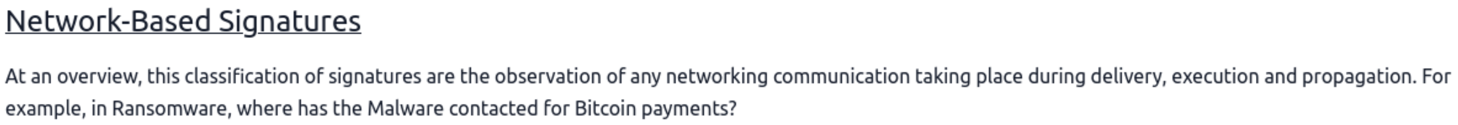
Network-Based Signatures

From reading and understanding the notes together with the hint given in this task, I was able to find the answer.



Question Hint

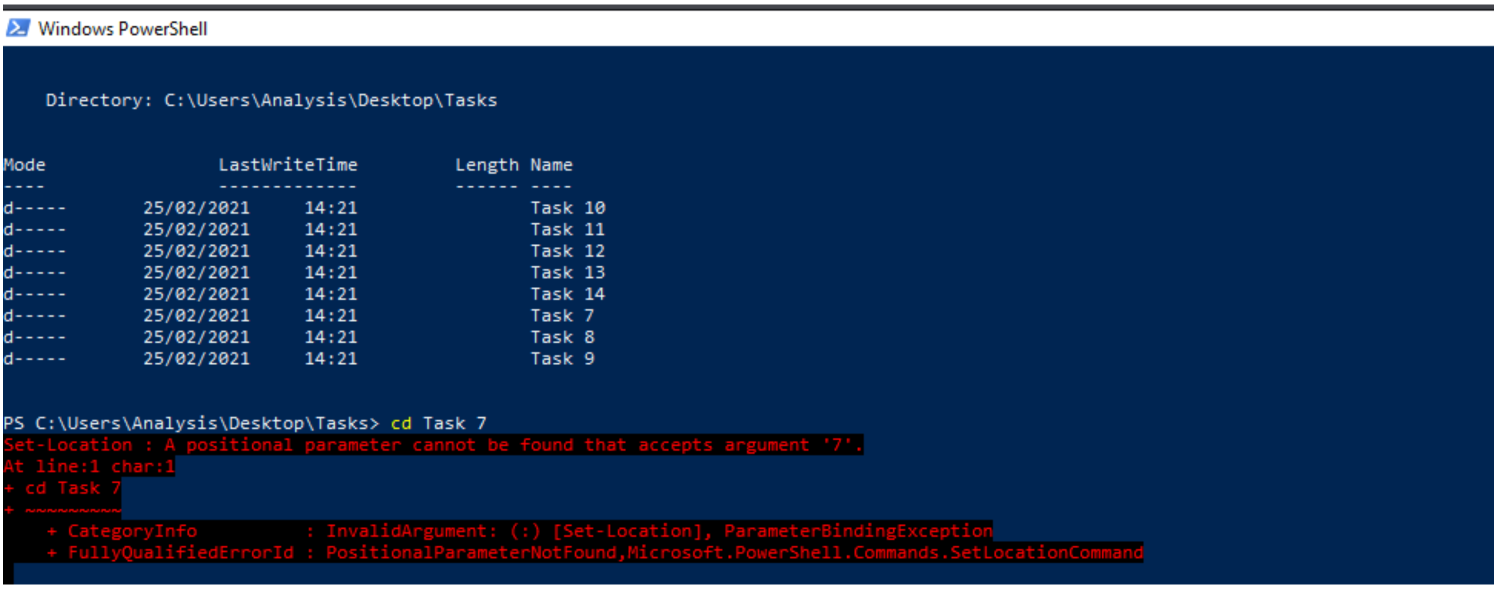
Think about the communications a Host might make after being infected. Will it look for other hosts? How will it do that?



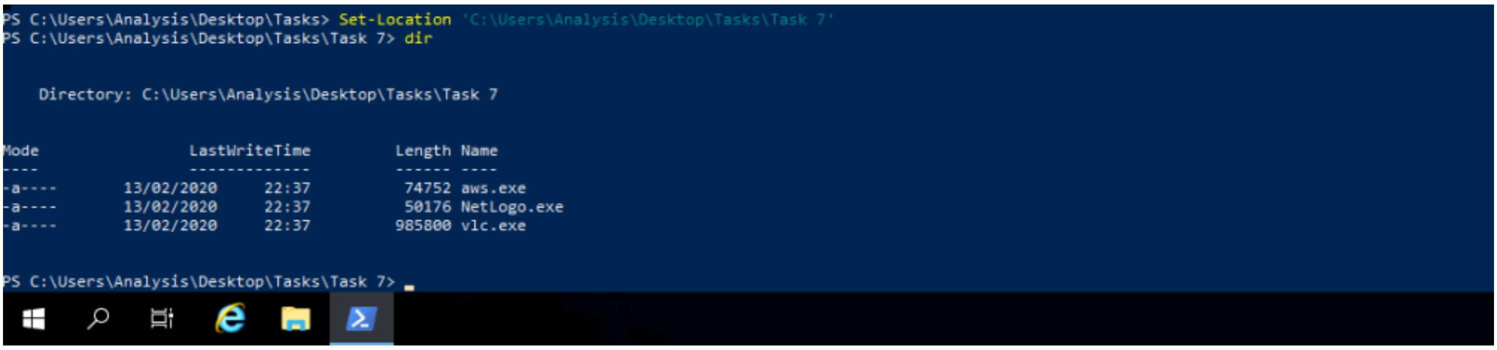
Network-Based Signatures

At an overview, this classification of signatures are the observation of any networking communication taking place during delivery, execution and propagation. For example, in Ransomware, where has the Malware contacted for Bitcoin payments?

For the remaining tasks, I was required to get my hands dirty.
So I first started the machine. However for me I used the web-based windows machine which I had issues to connect with due to network issues from my end, though in the long run a stable connection was established.
In most cases I prefer CLI to GUI. So mostly I will operate from the powershell and command promt.
After opening the windows powershell, I cd to task 7 dir but encountered an error that required me to set location for this directory. After setting the location as required, I was able to read the content inside this directory.

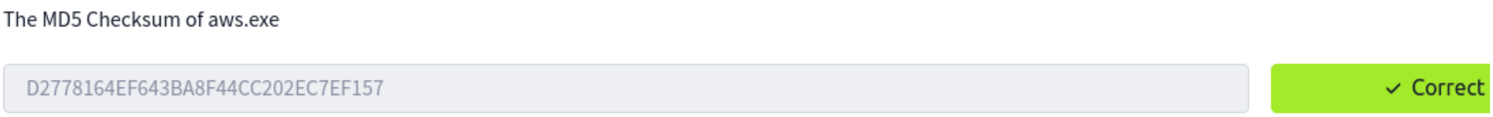


```
    Directory: C:\Users\Analysis\Desktop\Tasks


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       25/02/2021     14:21                Task 10
d-----       25/02/2021     14:21                Task 11
d-----       25/02/2021     14:21                Task 12
d-----       25/02/2021     14:21                Task 13
d-----       25/02/2021     14:21                Task 14
d-----       25/02/2021     14:21                Task 7
d-----       25/02/2021     14:21                Task 8
d-----       25/02/2021     14:21                Task 9


PS C:\Users\Analysis\Desktop\Tasks> cd Task 7
Set-Location : A positional parameter cannot be found that accepts argument '7'.
At line:1 char:1
+ cd Task 7
+ ~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
```



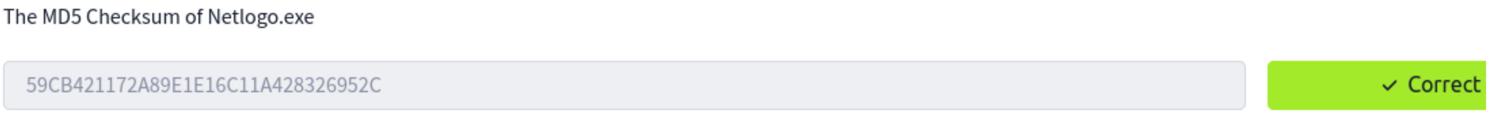
```
PS C:\Users\Analysis\Desktop\Tasks> Set-Location 'C:\Users\Analysis\Desktop\Tasks\Task 7'
PS C:\Users\Analysis\Desktop\Tasks\Task 7> dir


    Directory: C:\Users\Analysis\Desktop\Tasks\Task 7


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       13/02/2020     22:37          74752 aws.exe
-a----       13/02/2020     22:37          50176 NetLogo.exe
-a----       13/02/2020     22:37         985800 vlc.exe


PS C:\Users\Analysis\Desktop\Tasks\Task 7> _
```

From the mode tab in the image above, '-a---- ' :The file has the A attribute (Archive), indicating it has been changed since the last backup.



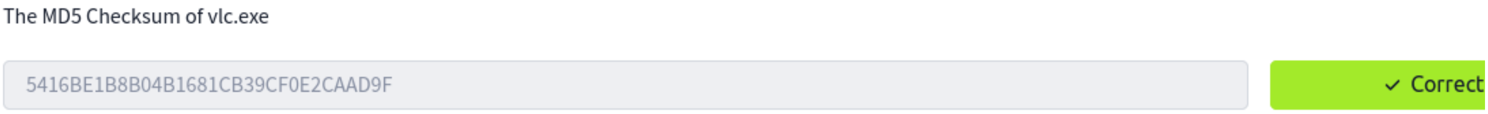
The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202EC7EF157



The MD5 Checksum of Netlogo.exe

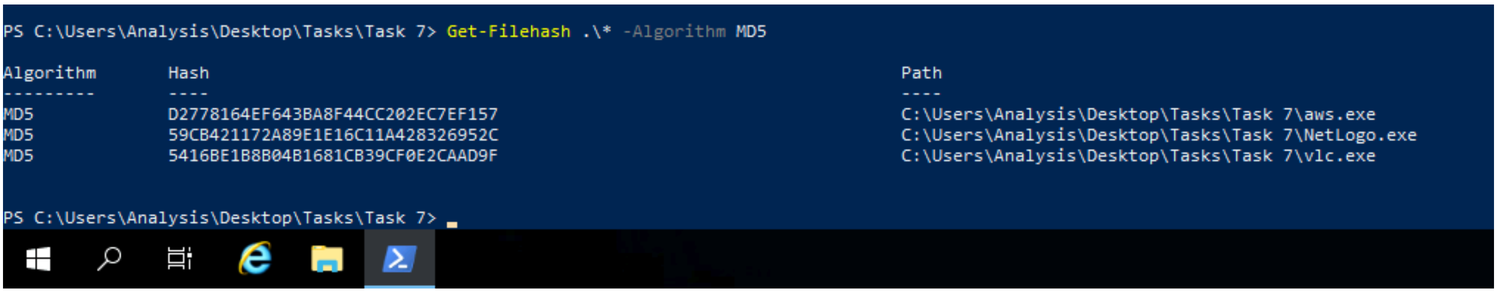
59CB421172A89E1E16C11A428326952C



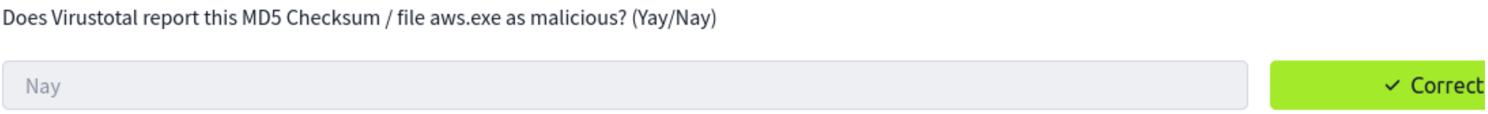
The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF0E2CAAD9F

For the three tasks above, I used the powershell cmd "Get-Filehash" to retrieve all the hashes of the files in the current dir. I specified the hash alg as MD5 and successfully retrieved the file hashes as it can be seen in the image below.



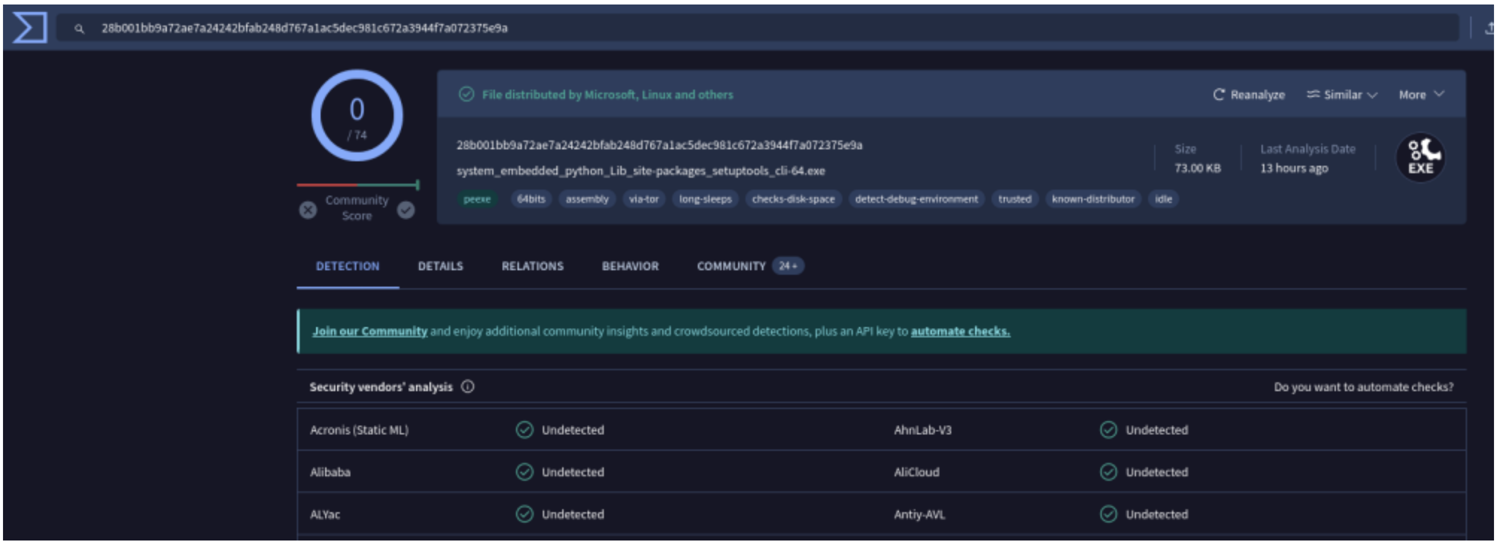
```
PS C:\Users\Analysis\Desktop\Tasks\Task 7> Get-Filehash .\* -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             D2778164EF643BA8F44CC202EC7EF157                                       C:\Users\Analysis\Desktop\Tasks\Task 7\aws.exe
MD5             59CB421172A89E1E16C11A428326952C                                       C:\Users\Analysis\Desktop\Tasks\Task 7\NetLogo.exe
MD5             5416BE1B8B04B1681CB39CF0E2CAAD9F                                       C:\Users\Analysis\Desktop\Tasks\Task 7\vlc.exe


PS C:\Users\Analysis\Desktop\Tasks\Task 7> _
```



Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)

Nay

I visited the virus total webpage and pasted the filehash to aws.exe, however it was not reported as malicious. This is evident in the image below.



28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a

File distributed by Microsoft, Linux and others

28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
system_embedded_python_Lib_site-packages_setuptools_cli-64.exe

peexe 64bits assembly via-tor long-sleeps checks-disk-space detect-debug-environment trusted known-distributor idle

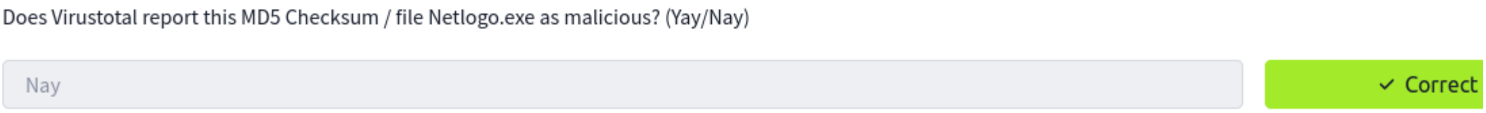
Size: 73.00 KB
Last Analysis Date: 13 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

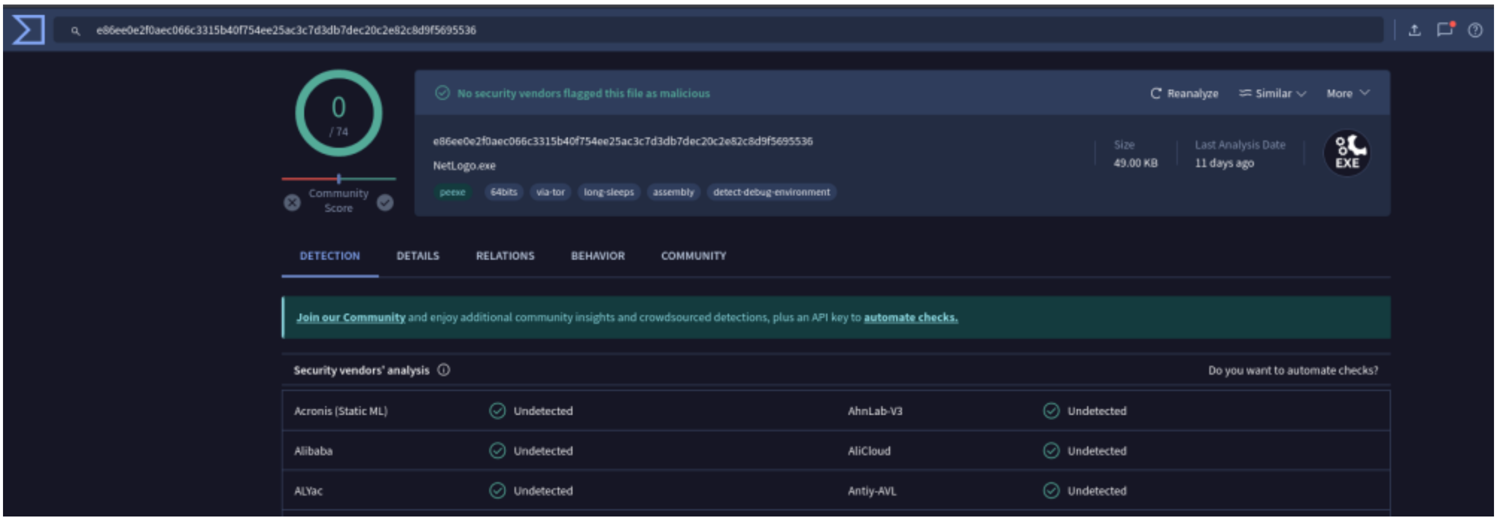
Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected



Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)

Nay

I visited the virus total webpage and pasted the filehash to Netlogo.exe, however it was not reported as malicious. This is evident in the image below.



e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536

No security vendors flagged this file as malicious

e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
NetLogo.exe

peexe 64bits via-tor long-sleeps assembly detect-debug-environment

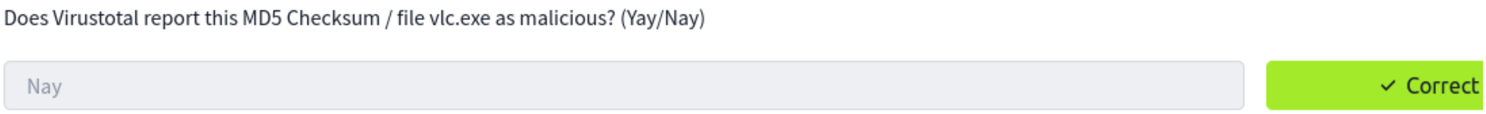
Size: 49.00 KB
Last Analysis Date: 11 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

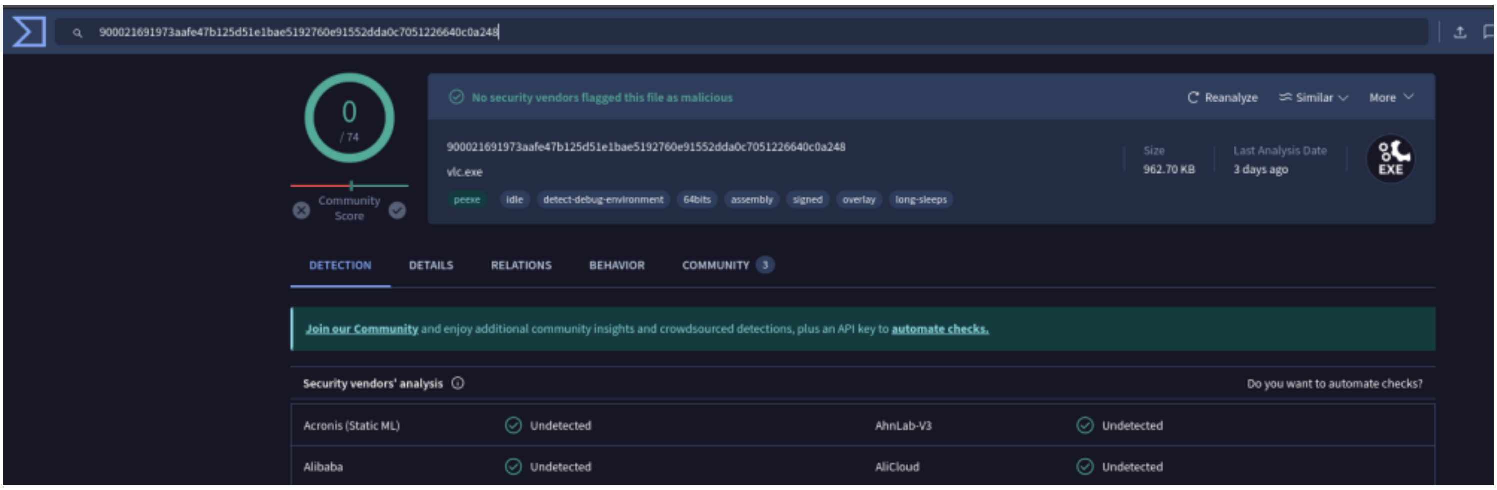
Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected



Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)

Nay

I visited the virus total webpage and pasted the filehash to vlc.exe, however it was not reported as malicious. This is evident in the image below.



900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248

0 / 74

No security vendors flagged this file as malicious

900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248
vlc.exe

peexe idle detect-debug-environment 64bits assembly signed overlay long-sleeps

Size 962.70 KB

Last Analysis Date 3 days ago

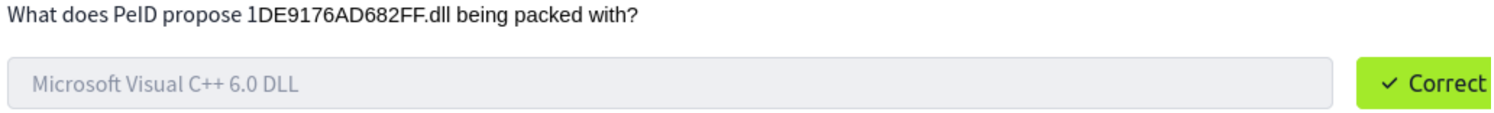
EXE

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

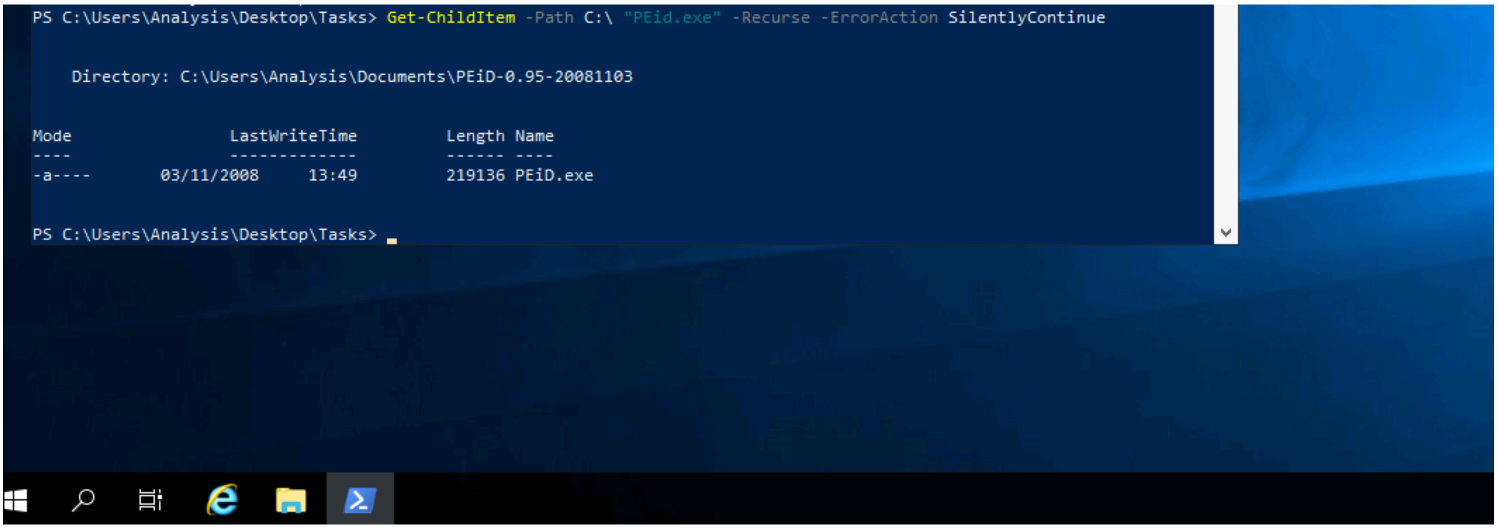
Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected



What does PeID propose 1DE9176AD682FF.dll being packed with?

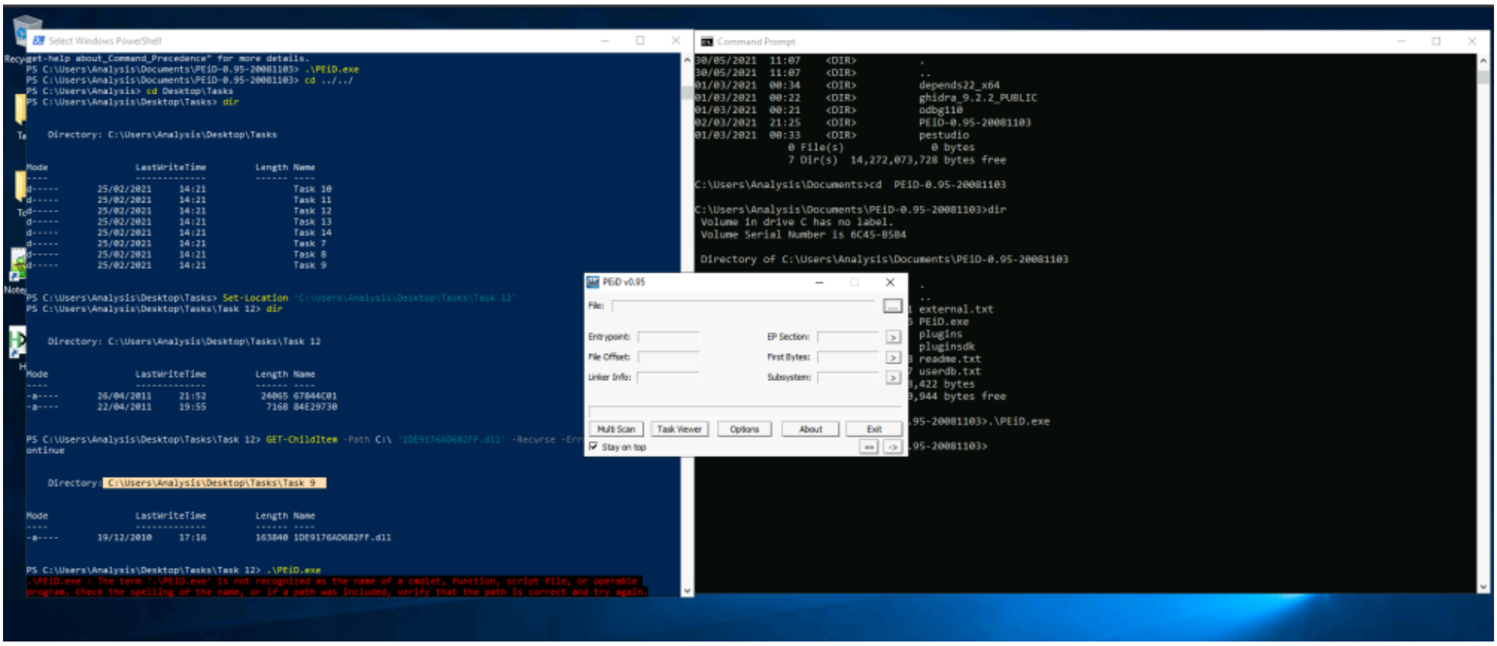
Microsoft Visual C++ 6.0 DLL

I had to search for PeID as THM didn't mention where it was saved.
The command in the image below is used to search for a file named `PEid.exe` throughout the entire `C:\` drive and to suppress any error messages that might occur during the search.
This can be seen below, and I successfully found the path to this executable.



```
PS C:\Users\Analysis\Desktop\Tasks> Get-ChildItem -Path C:\ "PEid.exe" -Recurse -ErrorAction SilentlyContinue


    Directory: C:\Users\Analysis\Documents\PEiD-0.95-20081103


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       03/11/2008     13:49         219136 PEiD.exe


PS C:\Users\Analysis\Desktop\Tasks> _
```

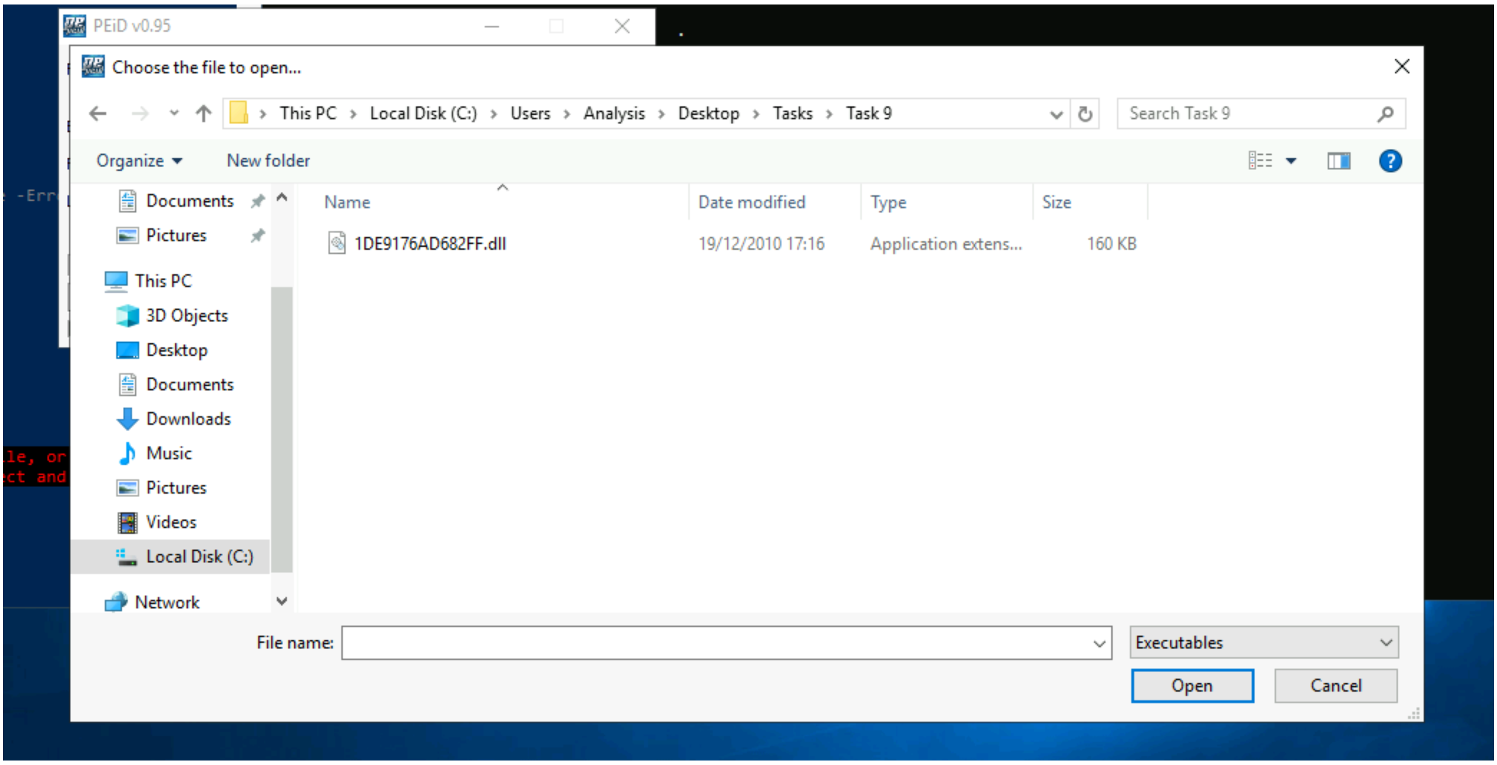
The .exe file succfully launched as seen in the image below.
Using the "Get-ChildItem" on the powershell terminal, I located the path to the .dll file as instructed in the task.



```
get-help about_Command_Precedence" for more details.
PS C:\Users\Analysis\Documents\PEiD-0.95-20081103> .\PEiD.exe
PS C:\Users\Analysis\Documents\PEiD-0.95-20081103> cd ../../
PS C:\Users\Analysis> cd Desktop\Tasks
PS C:\Users\Analysis\Desktop\Tasks> dir


    Directory: C:\Users\Analysis\Desktop\Tasks


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        25/02/2021     14:21                Task 10
d-----        25/02/2021     14:21                Task 11
d-----        25/02/2021     14:21                Task 12
d-----        25/02/2021     14:21                Task 13
d-----        25/02/2021     14:21                Task 14
d-----        25/02/2021     14:21                Task 7
d-----        25/02/2021     14:21                Task 8
d-----        25/02/2021     14:21                Task 9


PS C:\Users\Analysis\Desktop\Tasks> Set-Location 'C:\Users\Analysis\Desktop\Tasks\Task 12'
PS C:\Users\Analysis\Desktop\Tasks\Task 12> dir


    Directory: C:\Users\Analysis\Desktop\Tasks\Task 12


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        26/04/2011     21:52          24065 67844C01
-a----        22/04/2011     19:55           7168 84E29730


PS C:\Users\Analysis\Desktop\Tasks\Task 12> GET-ChildItem -Path C:\ '1DE9176AD682FF.dll' -Recurse -Err
ontinue


    Directory: C:\Users\Analysis\Desktop\Tasks\Task 9


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        19/12/2010     17:16         163840 1DE9176AD682FF.dll


PS C:\Users\Analysis\Desktop\Tasks\Task 12> .\PEiD.exe
.\PEiD.exe : The term '.\PEiD.exe' is not recognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
```

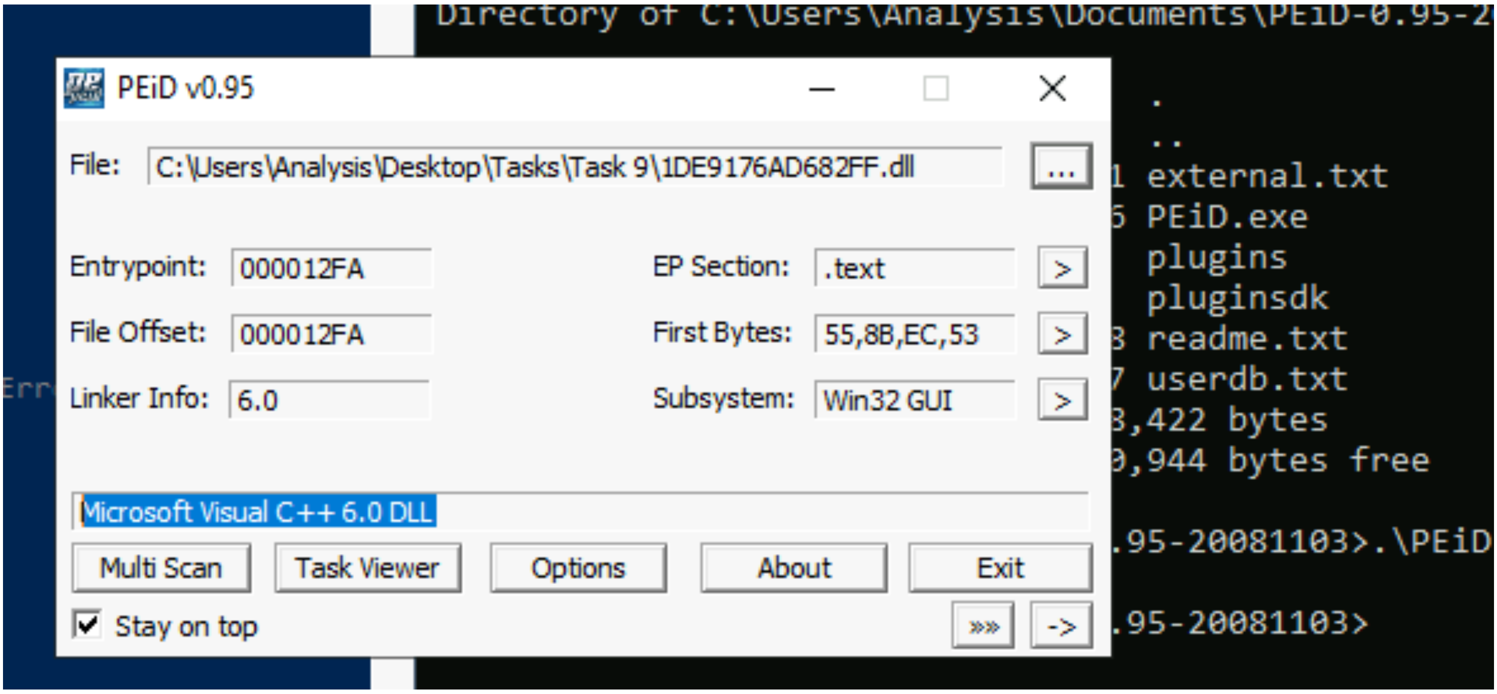
```
30/05/2021  11:07    <DIR>          .
30/05/2021  11:07    <DIR>          ..
01/03/2021  00:34    <DIR>          depends22_x64
01/03/2021  00:22    <DIR>          ghidra_9.2.2_PUBLIC
01/03/2021  00:21    <DIR>          odbg110
02/03/2021  21:25    <DIR>          PEiD-0.95-20081103
01/03/2021  00:33    <DIR>          pestudio
               0 File(s)              0 bytes
               7 Dir(s)  14,272,073,728 bytes free

C:\Users\Analysis\Documents>cd  PEiD-0.95-20081103

C:\Users\Analysis\Documents\PEiD-0.95-20081103>dir
 Volume in drive C has no label.
 Volume Serial Number is 6C45-8584

 Directory of C:\Users\Analysis\Documents\PEiD-0.95-20081103

                                    .
                                    ..
                                  1 external.txt
                                  5 PEiD.exe
                                    plugins
                                    pluginsdk
                                  3 readme.txt
                                  7 userdb.txt
                                  3,422 bytes
                                  3,944 bytes free

.95-20081103>.\PEiD.exe

.95-20081103>
```

Having the path to the .dll file, I navigated and chose it as seen in the image below.



Name	Date modified	Type	Size
1DE9176AD682FF.dll	19/12/2010 17:16	Application extens...	160 KB

After successfully opening, I was able to see Microsoft Visual C++ 6.0 DLL was used to pack this .dll file. This can be seen in the image below.



PEiD v0.95

File: C:\Users\Analysis\Desktop\Tasks\Task 9\1DE9176AD682FF.dll

Entrypoint: 000012FA

EP Section: .text

File Offset: 000012FA

First Bytes: 55,8B,EC,53

Linker Info: 6.0

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL

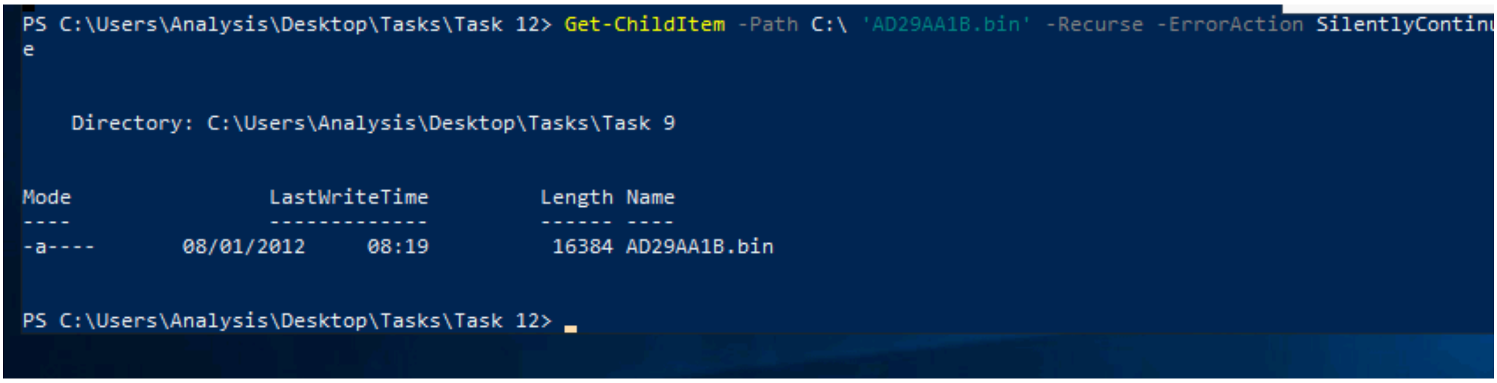
☑ Stay on top

```
 Directory of C:\Users\Analysis\Documents\PEiD-0.95-2
.
..
1 external.txt
5 PEiD.exe
  plugins
  pluginsdk
3 readme.txt
7 userdb.txt
3,422 bytes
9,944 bytes free
.95-20081103>.\PEiD
.95-20081103>
```

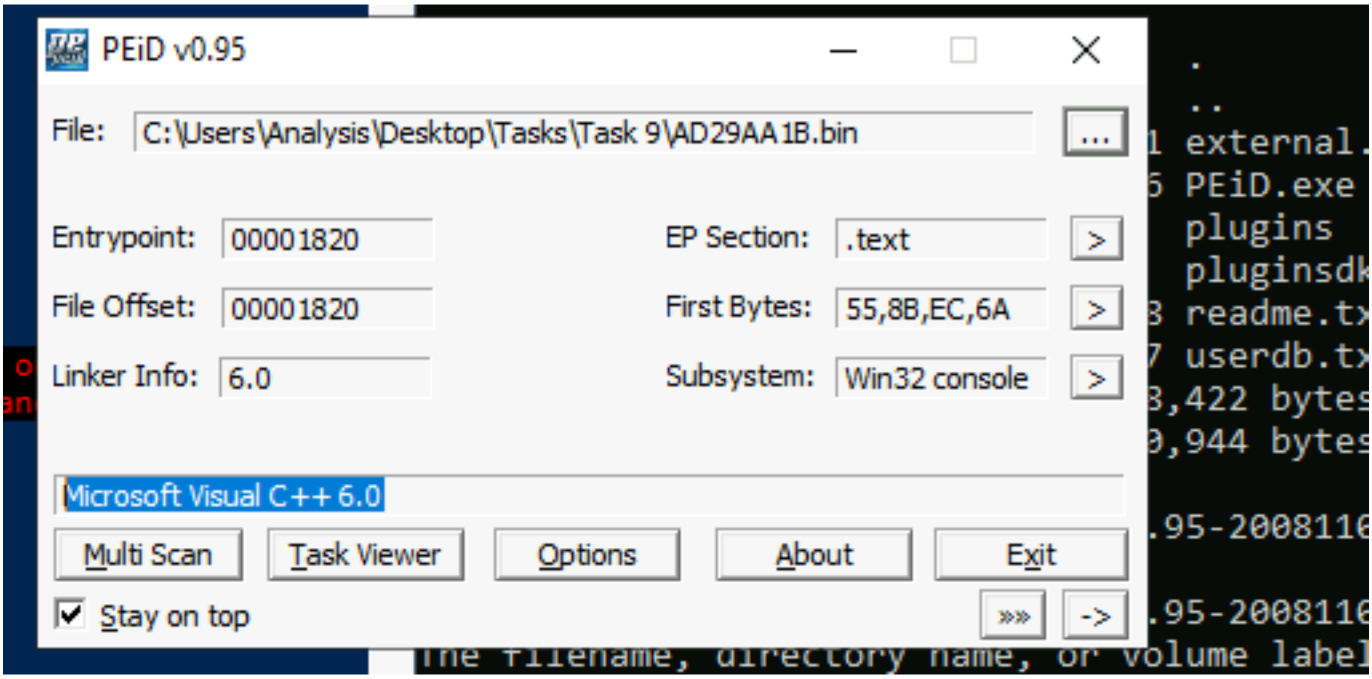
What does PeID propose AD29AA1B.bin being packed with?

Microsoft Visual C++ 6.0 ✓ Correct

Using the steps from the previous task, I also did the same for the .bin file which was found in task 9.



```
PS C:\Users\Analysis\Desktop\Tasks\Task 12> Get-ChildItem -Path C:\ 'AD29AA1B.bin' -Recurse -ErrorAction SilentlyContinu
e


    Directory: C:\Users\Analysis\Desktop\Tasks\Task 9


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       08/01/2012     08:19          16384 AD29AA1B.bin


PS C:\Users\Analysis\Desktop\Tasks\Task 12> _
```



PEiD v0.95

File: C:\Users\Analysis\Desktop\Tasks\Task 9\AD29AA1B.bin

Entrypoint: 00001820

EP Section: .text

File Offset: 00001820

First Bytes: 55,8B,EC,6A

Linker Info: 6.0

Subsystem: Win32 console

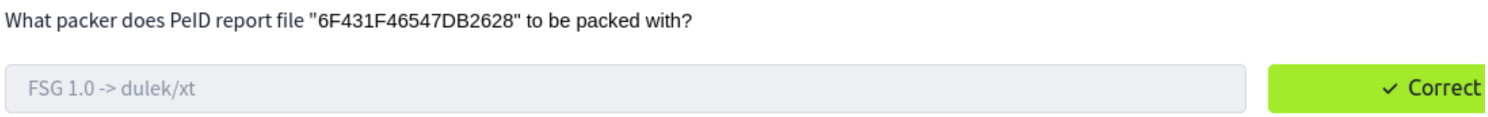
Microsoft Visual C++ 6.0

☑ Stay on top

```
.
..
1 external.
5 PEiD.exe
  plugins
  pluginsdk
3 readme.tx
7 userdb.tx
3,422 bytes
9,944 bytes
.95-2008110
.95-2008110
The filename, directory name, or volume label
```

TAKE AWAY:

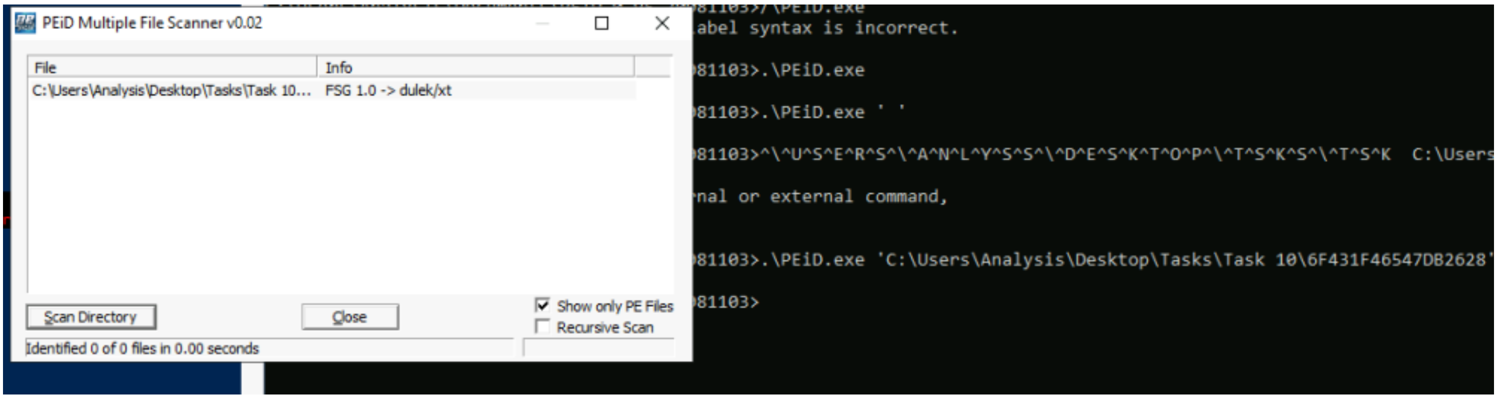
In the context of software and particularly malware analysis, a “packer” refers to a tool or software that can compress, encrypt, or obfuscate executable files. When run, the packed executable unpacks or decrypts itself in memory before executing the original code. While packers can be used legitimately to reduce file size or **protect intellectual property**, in malware, they’re used to **evade detection and hinder analysis**. The packed file contains a “**loader**” to handle this unpacking or decryption. **Packers challenge signature-based malware detection** and make reverse engineering more difficult.



What packer does PeID report file "6F431F46547DB2628" to be packed with?

FSG 1.0 -> dulek/xt

Following the steps in the above task, I was able to find the packer used for the file specified in this task as it can be seen in the image below.



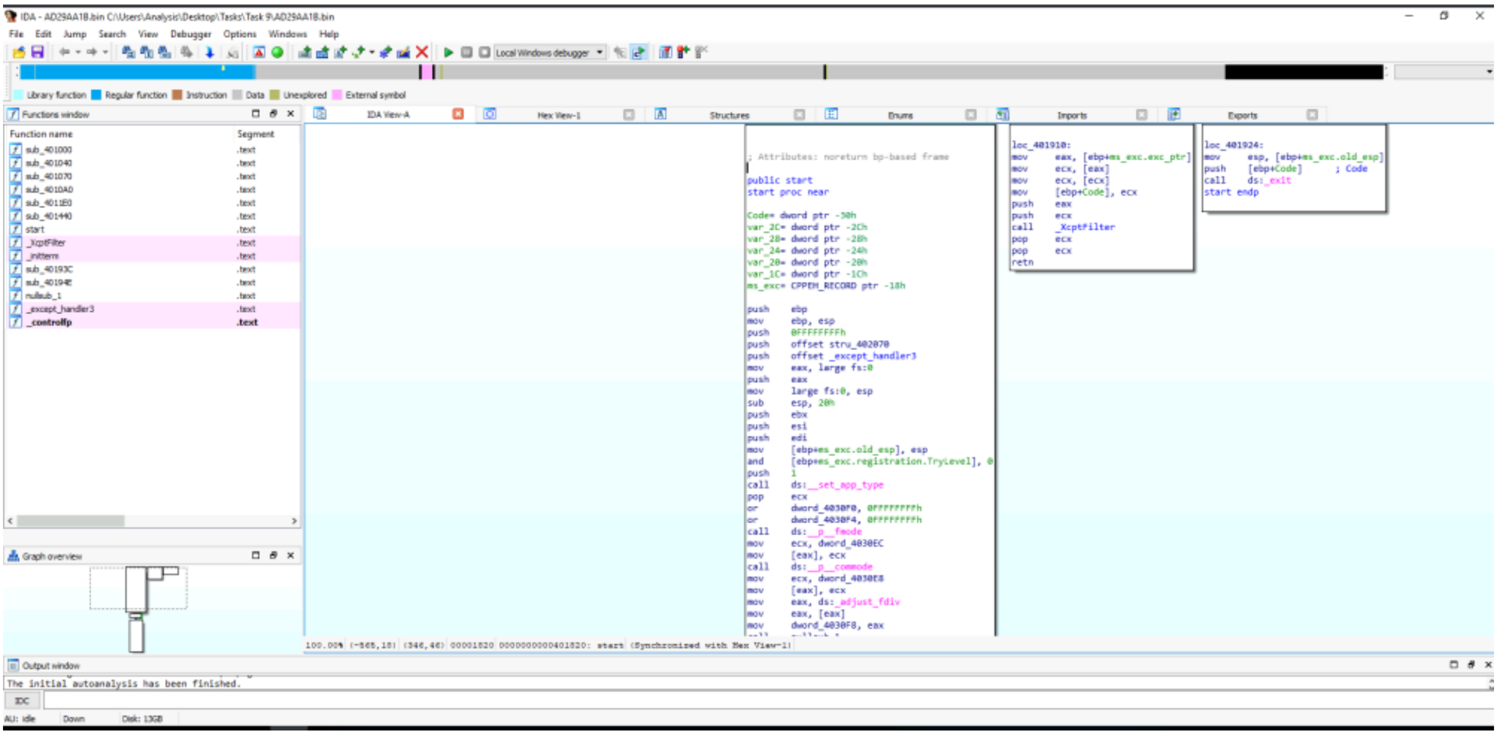
File	Info
C:\Users\Analysis\Desktop\Tasks\Task 10...	FSG 1.0 -> dulek/xt

Identified 0 of 0 files in 0.00 seconds

```
81103>/\PEiD.exe
abel syntax is incorrect.

81103>.\PEiD.exe

81103>.\PEiD.exe ' '

81103>^\^U^S^E^R^S^\^A^N^L^Y^S^S^\^D^E^S^K^T^O^P^\^T^S^K^S^\^T^S^K  C:\Users

rnal or external command,

81103>.\PEiD.exe 'C:\Users\Analysis\Desktop\Tasks\Task 10\6F431F46547DB2628'

81103>
```

For the images below, they pertain to a task with which no answer was needed though I tried as instructed in the notes and have an experience of my own.

So I opened the IDA freeware tool as seen below. Loaded the .bin file to be examined.



IDA - AD29AA18.bin C:\Users\Analysis\Desktop\Tasks\Task 9\AD29AA18.bin

Function name	Segment
sub_401000	.text
sub_401040	.text
sub_401070	.text
sub_4010A0	.text
sub_4011E0	.text
sub_401440	.text
start	.text
_XcptFilter	.text
_initterm	.text
sub_40193C	.text
sub_40194E	.text
nullsub_1	.text
_except_handler3	.text
_controlfp	.text

```
; Attributes: noreturn bp-based frame

public start
start proc near

Code= dword ptr -30h
var_2C= dword ptr -2Ch
var_28= dword ptr -28h
var_24= dword ptr -24h
var_20= dword ptr -20h
var_1C= dword ptr -1Ch
ms_exc= CPPEH_RECORD ptr -18h

push    ebp
mov     ebp, esp
push    0FFFFFFFFh
push    offset stru_402070
push    offset _except_handler3
mov     eax, large fs:0
push    eax
mov     large fs:0, esp
sub     esp, 20h
push    ebx
push    esi
push    edi
mov     [ebp+ms_exc.old_esp], esp
and     [ebp+ms_exc.registration.TryLevel], 0
push    1
call    ds:__set_app_type
pop     ecx
or      dword_4030F0, 0FFFFFFFFh
or      dword_4030F4, 0FFFFFFFFh
call    ds:__p__fmode
mov     ecx, dword_4030EC
mov     [eax], ecx
call    ds:__p__commode
mov     ecx, dword_4030E8
mov     [eax], ecx
mov     eax, ds:_adjust_fdiv
mov     eax, [eax]
mov     dword_4030F8, eax
```

```
loc_401910:
mov     eax, [ebp+ms_exc.exc_ptr]
mov     ecx, [eax]
mov     ecx, [ecx]
mov     [ebp+Code], ecx
push    eax
push    ecx
call    _XcptFilter
pop     ecx
pop     ecx
retn
```

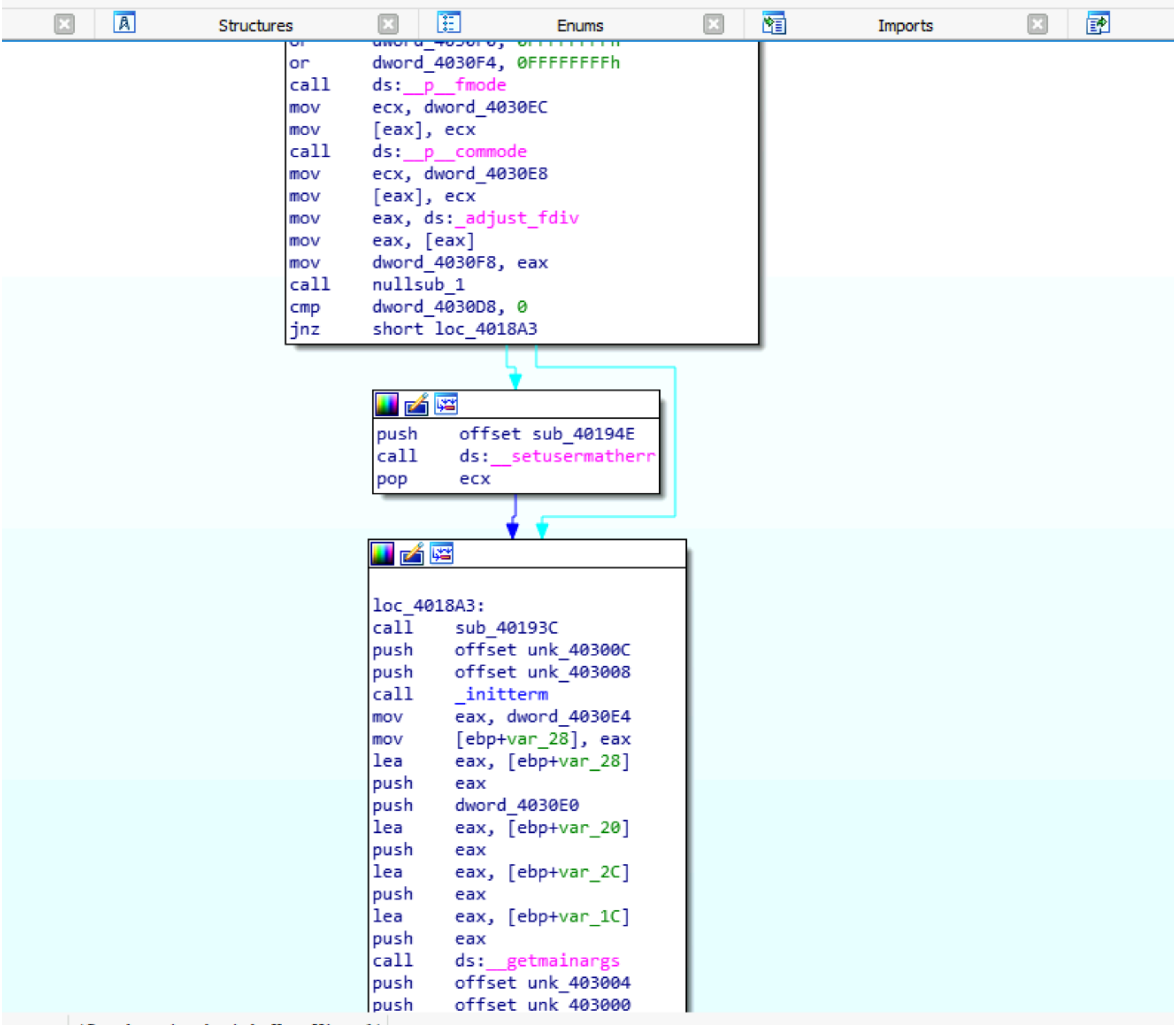
```
loc_401924:
mov     esp, [ebp+ms_exc.old_esp]
push    [ebp+Code]      ; Code
call    ds:_exit
start endp
```

```
100.00% (-565,18) (346,46) 00001820 0000000000401820: start (Synchronized with Hex View-1)
```

```
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 13GB

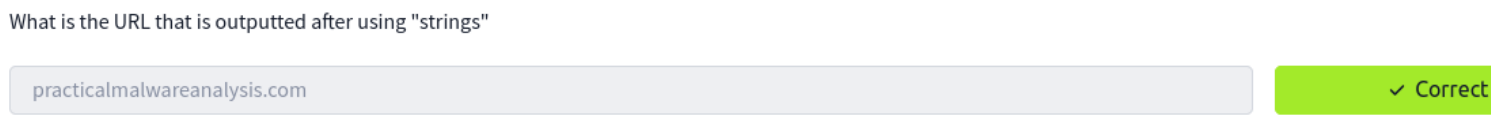
But essentially, we can see the flow of how the program executes - indicated by the arrows. The problem? There's very little here! There are a few more characteristics that indicate its packed.



```
or      dword_4030F4, 0FFFFFFFFh
call    ds:__p__fmode
mov     ecx, dword_4030EC
mov     [eax], ecx
call    ds:__p__commode
mov     ecx, dword_4030E8
mov     [eax], ecx
mov     eax, ds:_adjust_fdiv
mov     eax, [eax]
mov     dword_4030F8, eax
call    nullsub_1
cmp     dword_4030D8, 0
jnz     short loc_4018A3
```

```
push    offset sub_40194E
call    ds:__setusermatherr
pop     ecx
```

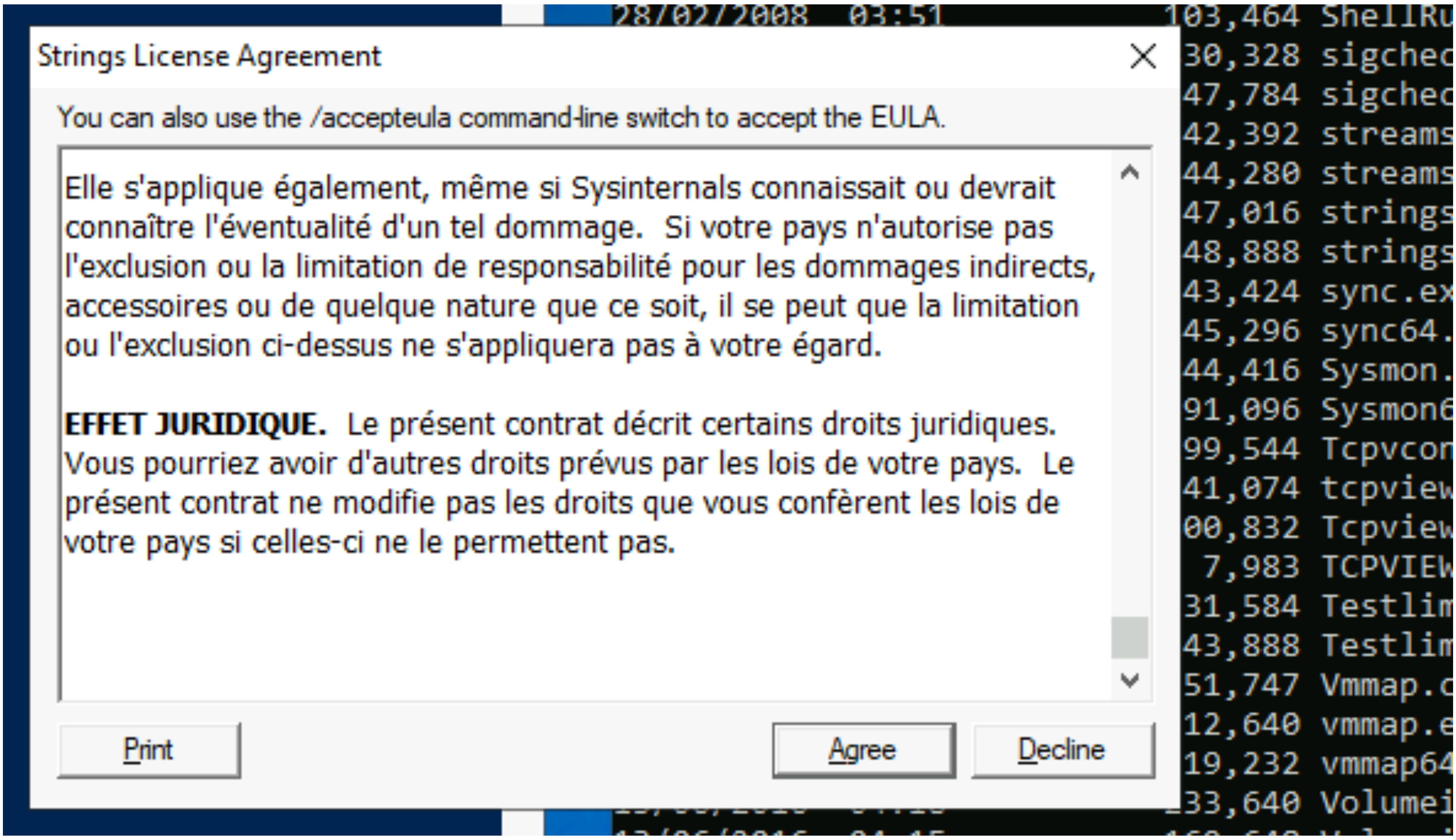
```
loc_4018A3:
call    sub_40193C
push    offset unk_40300C
push    offset unk_403008
call    _initterm
mov     eax, dword_4030E4
mov     [ebp+var_28], eax
lea     eax, [ebp+var_28]
push    eax
push    dword_4030E0
lea     eax, [ebp+var_20]
push    eax
lea     eax, [ebp+var_2C]
push    eax
lea     eax, [ebp+var_1C]
push    eax
call    ds:__getmainargs
push    offset unk_403004
push    offset unk_403000
```


What is the URL that is outputted after using "strings"

practicalmalwareanalysis.com

✓ Correct

Strings.exe refused to run properly in PowreShell_ISE, so I had to use command prompt instead.



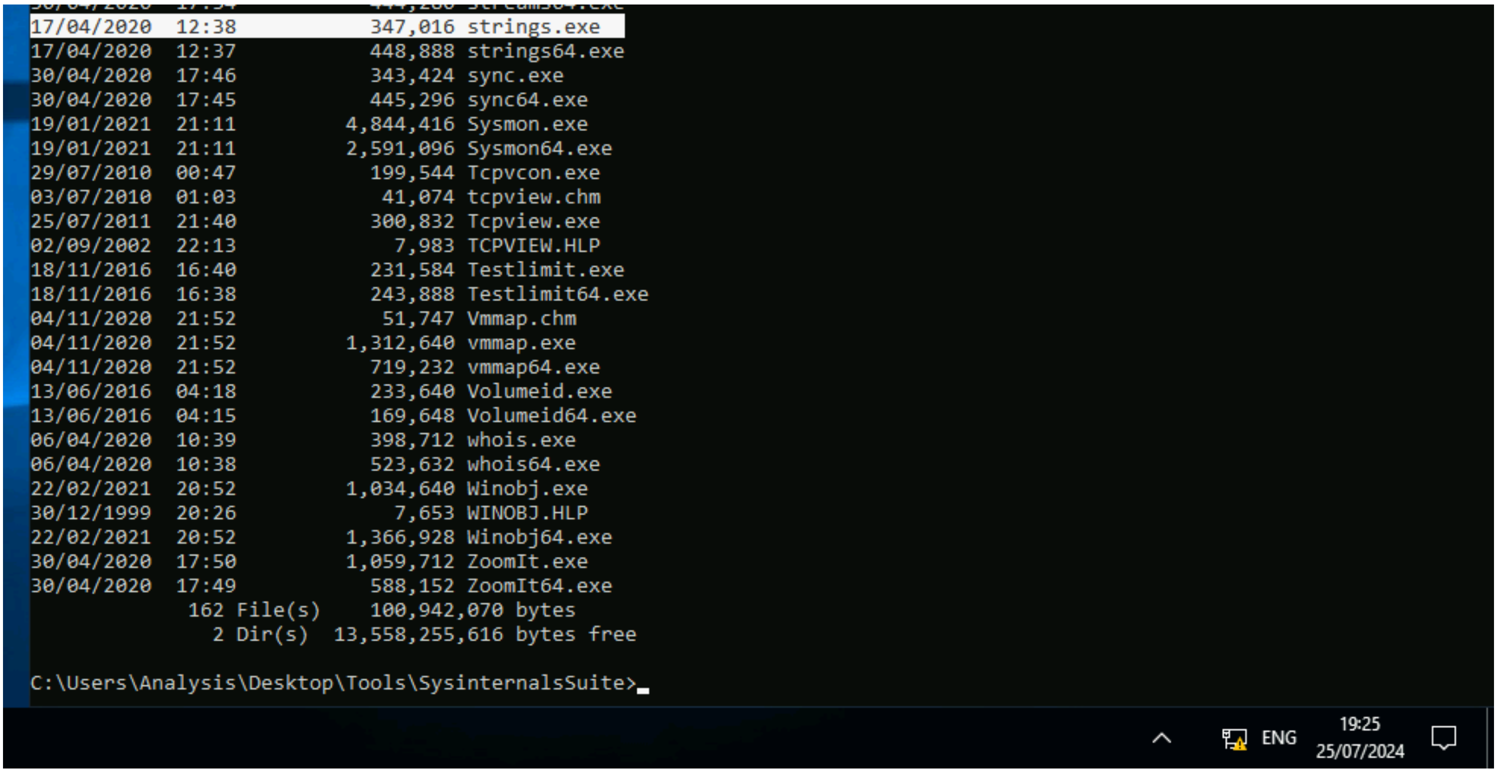
You can also use the /accepteula command-line switch to accept the EULA.

Elle s'applique également, même si Sysinternals connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

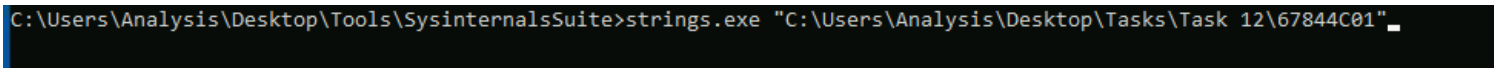
```
28/02/2008  03:51      103,464 ShellRu
                        30,328 sigchec
                        47,784 sigchec
                        42,392 streams
                        44,280 streams
                        47,016 strings
                        48,888 strings
                        43,424 sync.ex
                        45,296 sync64.
                        44,416 Sysmon.
                        91,096 Sysmon6
                        99,544 Tcpvcon
                        41,074 tcpview
                        00,832 Tcpview
                         7,983 TCPVIEW
                        31,584 Testlim
                        43,888 Testlim
                        51,747 Vmmap.c
                        12,640 vmmap.e
                        19,232 vmmap64
                        33,640 Volumei
```

I first had to find and navigate to C:\> cd C:\Users\Analysis\Desktop\Tools\SysinternalsSuite where strings.exe was located.



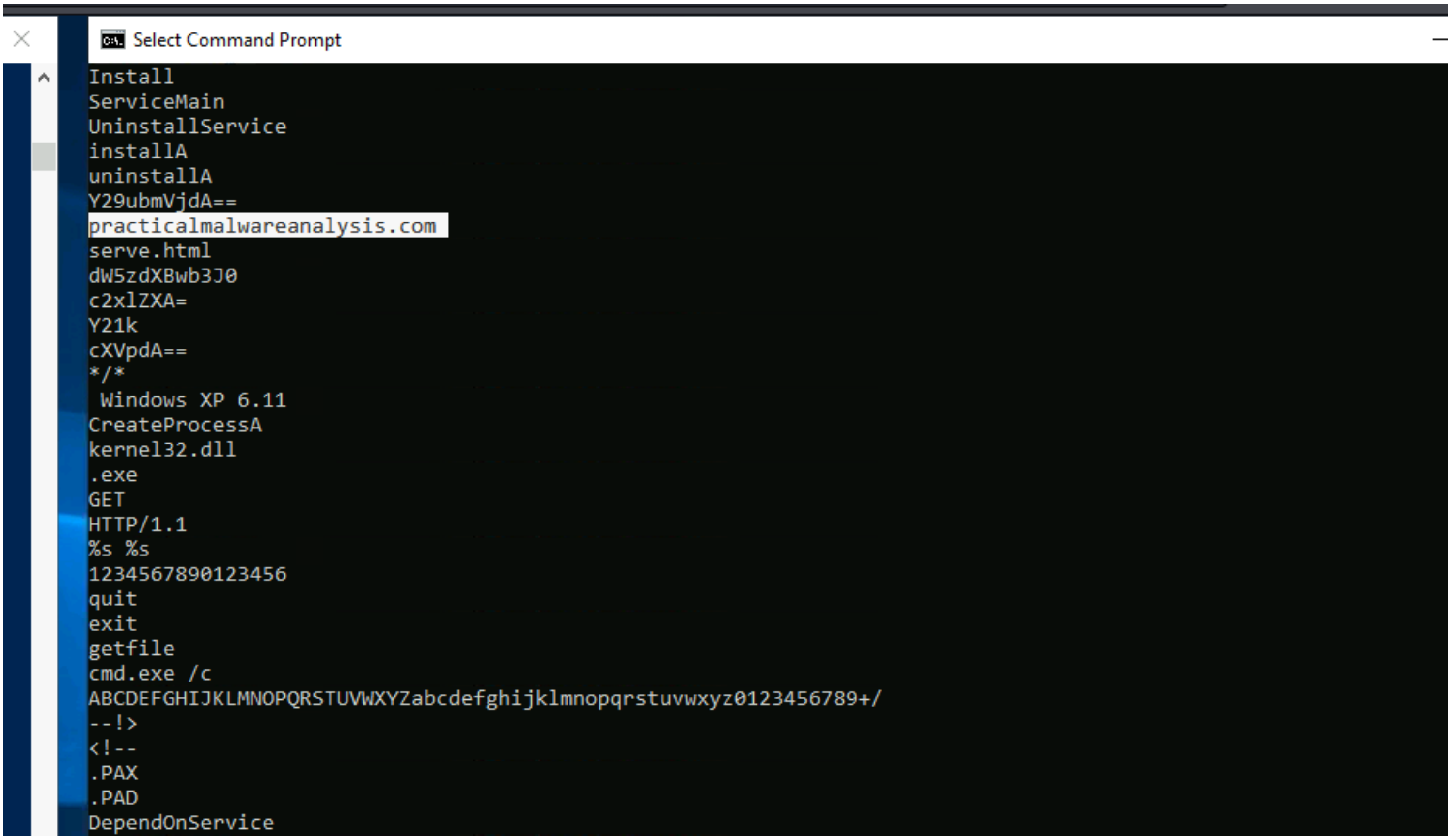
```
17/04/2020  12:38           347,016 strings.exe
17/04/2020  12:37           448,888 strings64.exe
30/04/2020  17:46           343,424 sync.exe
30/04/2020  17:45           445,296 sync64.exe
19/01/2021  21:11         4,844,416 Sysmon.exe
19/01/2021  21:11         2,591,096 Sysmon64.exe
29/07/2010  00:47           199,544 Tcpvcon.exe
03/07/2010  01:03            41,074 tcpview.chm
25/07/2011  21:40           300,832 Tcpview.exe
02/09/2002  22:13             7,983 TCPVIEW.HLP
18/11/2016  16:40           231,584 Testlimit.exe
18/11/2016  16:38           243,888 Testlimit64.exe
04/11/2020  21:52            51,747 Vmmap.chm
04/11/2020  21:52         1,312,640 vmmap.exe
04/11/2020  21:52           719,232 vmmap64.exe
13/06/2016  04:18           233,640 Volumeid.exe
13/06/2016  04:15           169,648 Volumeid64.exe
06/04/2020  10:39           398,712 whois.exe
06/04/2020  10:38           523,632 whois64.exe
22/02/2021  20:52         1,034,640 Winobj.exe
30/12/1999  20:26             7,653 WINOBJ.HLP
22/02/2021  20:52         1,366,928 Winobj64.exe
30/04/2020  17:50         1,059,712 ZoomIt.exe
30/04/2020  17:49           588,152 ZoomIt64.exe
             162 File(s)    100,942,070 bytes
               2 Dir(s)  13,558,255,616 bytes free

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>
```

I executed the command below, and there were a lot of information display on the command promt, some made sense while others didn't.



```
C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>strings.exe "C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01"
```

I went through the output and managed to locate the url asked in this task. However, there are a lot of string to go through with a human eye. The `findstr` command is a Windows `grep` equivalent in a Windows command-line prompt (CMD).



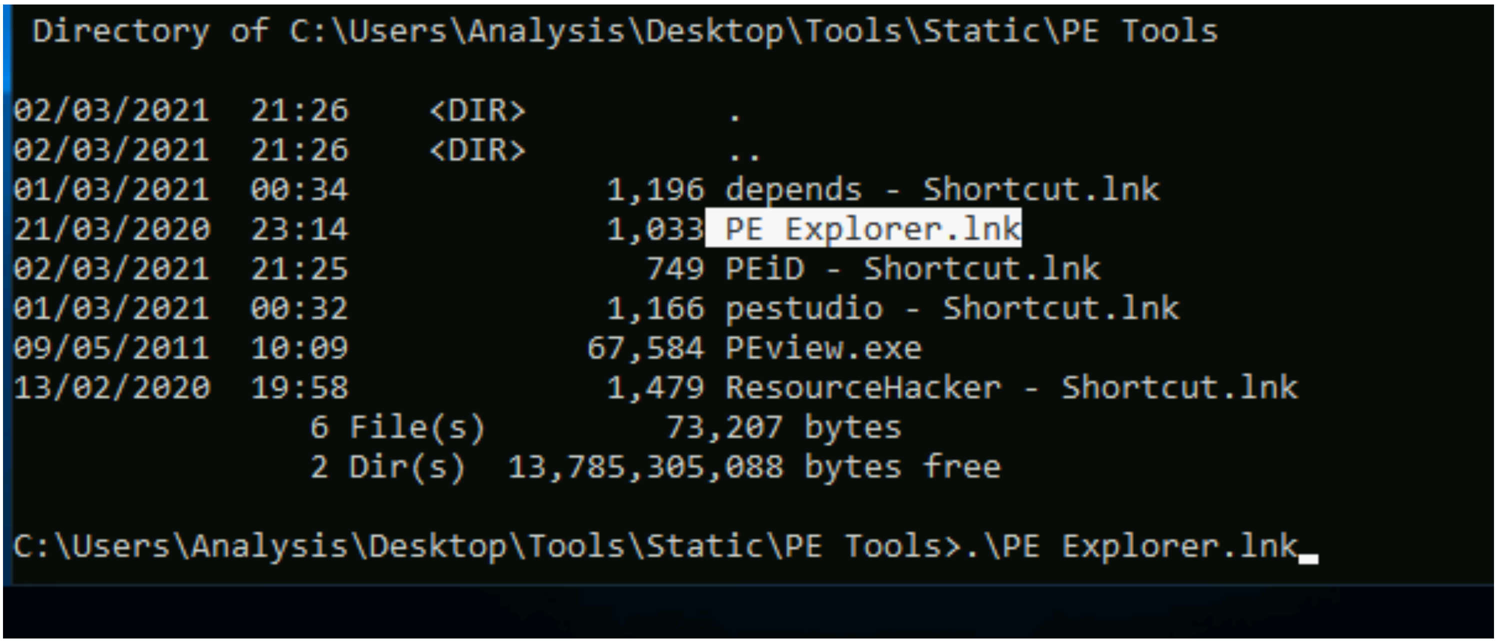
```
Install
ServiceMain
UninstallService
installA
uninstallA
Y29ubmVjdA==
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2xlZXA=
Y21k
cXVpdA==
*/*
 Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
--!>
<!--
.PAX
.PAD
DependOnService
```

How many **unique** "Imports" are there?

5

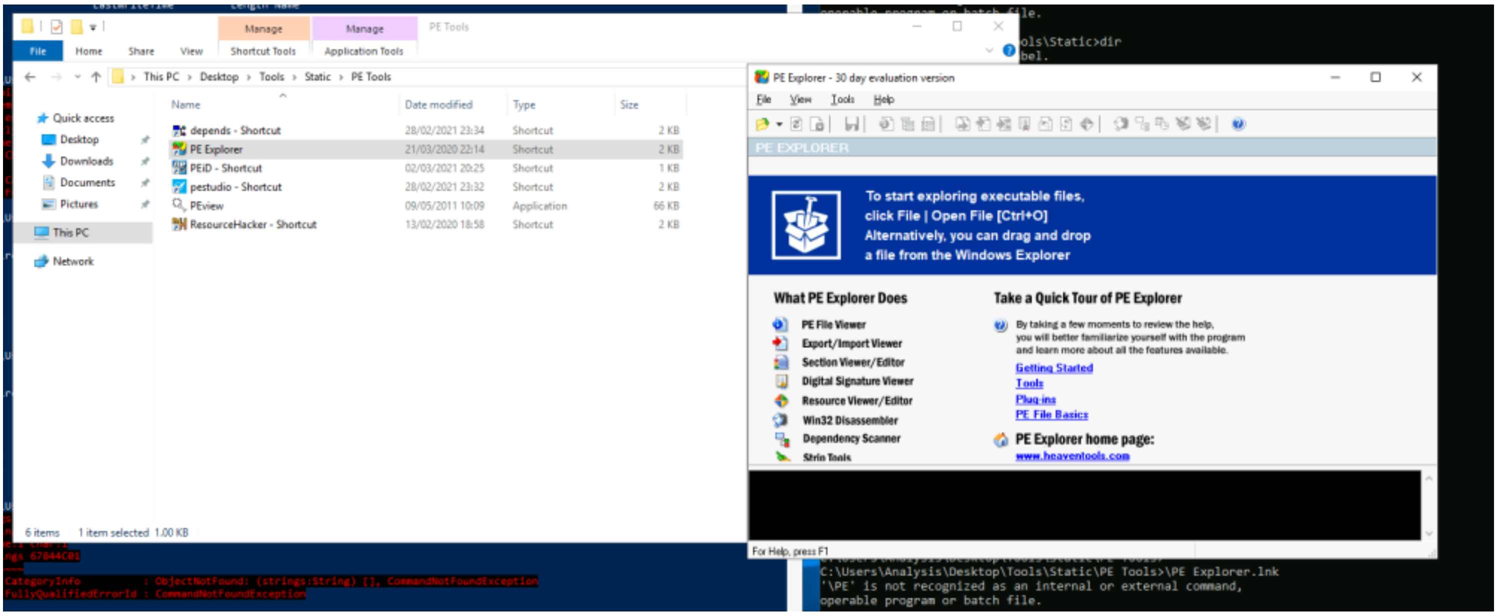
✓ Correct

First I located the path to the PE Explorer.



```
 Directory of C:\Users\Analysis\Desktop\Tools\Static\PE Tools

02/03/2021  21:26    <DIR>          .
02/03/2021  21:26    <DIR>          ..
01/03/2021  00:34             1,196 depends - Shortcut.lnk
21/03/2020  23:14             1,033 PE Explorer.lnk
02/03/2021  21:25               749 PEiD - Shortcut.lnk
01/03/2021  00:32             1,166 pestudio - Shortcut.lnk
09/05/2011  10:09            67,584 PEview.exe
13/02/2020  19:58             1,479 ResourceHacker - Shortcut.lnk
               6 File(s)         73,207 bytes
               2 Dir(s)  13,785,305,088 bytes free

C:\Users\Analysis\Desktop\Tools\Static\PE Tools>.\PE Explorer.lnk
```

I now navigated to this file from the file explorer and launched an instance as seen below.



This PC › Desktop › Tools › Static › PE Tools

Name	Date modified	Type	Size
depends - Shortcut	28/02/2021 23:34	Shortcut	2 KB
PE Explorer	21/03/2020 22:14	Shortcut	2 KB
PEiD - Shortcut	02/03/2021 20:25	Shortcut	1 KB
pestudio - Shortcut	28/02/2021 23:32	Shortcut	2 KB
PEview	09/05/2011 10:09	Application	66 KB
ResourceHacker - Shortcut	13/02/2020 18:58	Shortcut	2 KB

6 items 1 item selected 1.00 KB

```
CategoryInfo          : ObjectNotFound: (strings:String) [], CommandNotFoundException
FullyQualifiedErrorId : CommandNotFoundException
```

PE Explorer - 30 day evaluation version

PE EXPLORER

To start exploring executable files,
click File | Open File [Ctrl+O]
Alternatively, you can drag and drop
a file from the Windows Explorer

What PE Explorer Does
- PE File Viewer
- Export/Import Viewer
- Section Viewer/Editor
- Digital Signature Viewer
- Resource Viewer/Editor
- Win32 Disassembler
- Dependency Scanner
- Strip Tools

Take a Quick Tour of PE Explorer

By taking a few moments to review the help, you will better familiarize yourself with the program and learn more about all the features available.

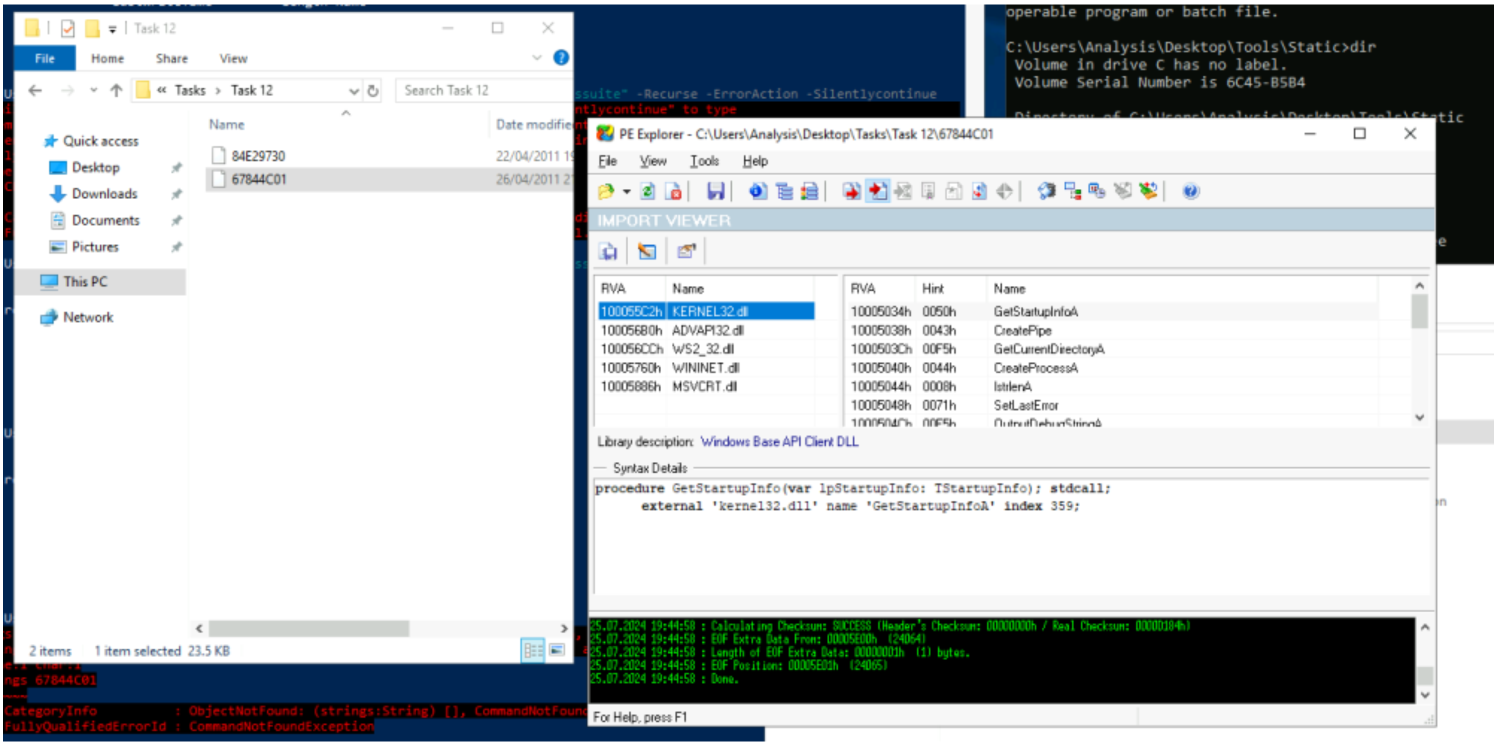
Getting Started
Tools
Plug-ins
PE File Basics

PE Explorer home page:
www.heaventools.com

For Help, press F1

```
C:\Users\Analysis\Desktop\Tools\Static\PE Tools>\PE Explorer.lnk
'\PE' is not recognized as an internal or external command,
operable program or batch file.
```

I searched for the specified file specified in this task, dragged and dropped it in the PE Explorer as seen below. I checked on the view → import in this application and was able to see the number of imports.



Tasks › Task 12

Name	Date modified
84E29730	22/04/2011 1
67844C01	26/04/2011 2

2 items 1 item selected 23.5 KB

```
operable program or batch file.

C:\Users\Analysis\Desktop\Tools\Static>dir
 Volume in drive C has no label.
 Volume Serial Number is 6C45-B5B4
```

PE Explorer - C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01

IMPORT VIEWER

RVA	Name
100055C2h	KERNEL32.dll
10005680h	ADVAPI32.dll
100056CCh	WS2_32.dll
10005760h	WININET.dll
10005886h	MSVCRT.dll

RVA	Hint	Name
10005034h	0050h	GetStartupInfoA
10005038h	0043h	CreatePipe
1000503Ch	00F5h	GetCurrentDirectoryA
10005040h	0044h	CreateProcessA
10005044h	0008h	lstrlenA
10005048h	0071h	SetLastError
1000504Ch	00F5h	OutputDebugStringA

Library description: Windows Base API Client DLL

Syntax Details

```
procedure GetStartupInfo(var lpStartupInfo: TStartupInfo); stdcall;
      external 'kernel32.dll' name 'GetStartupInfoA' index 359;
```

```
25.07.2024 19:44:58 : Calculating Checksum: SUCCESS (Header's Checksum: 00000000h / Real Checksum: 0000184h)
25.07.2024 19:44:58 : EOF Extra Data From: 00005E00h  (24064)
25.07.2024 19:44:58 : Length of EOF Extra Data: 00000001h  (1) bytes.
25.07.2024 19:44:58 : EOF Position: 00005E01h  (24065)
25.07.2024 19:44:58 : Done.
```

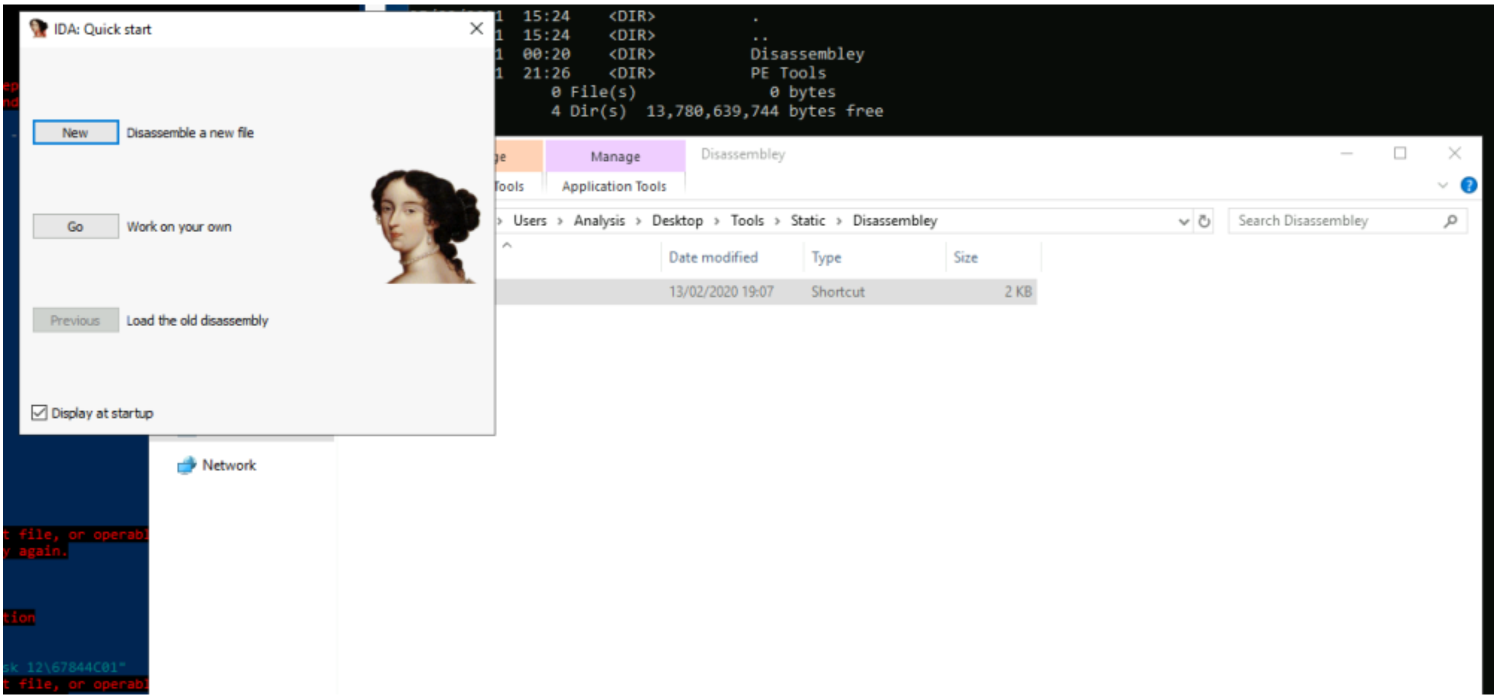
For Help, press F1

How many references are there to the library "**msi**" in the "**Imports**" tab of IDA Freeware for "**install.exe**"

9

✓ Correct

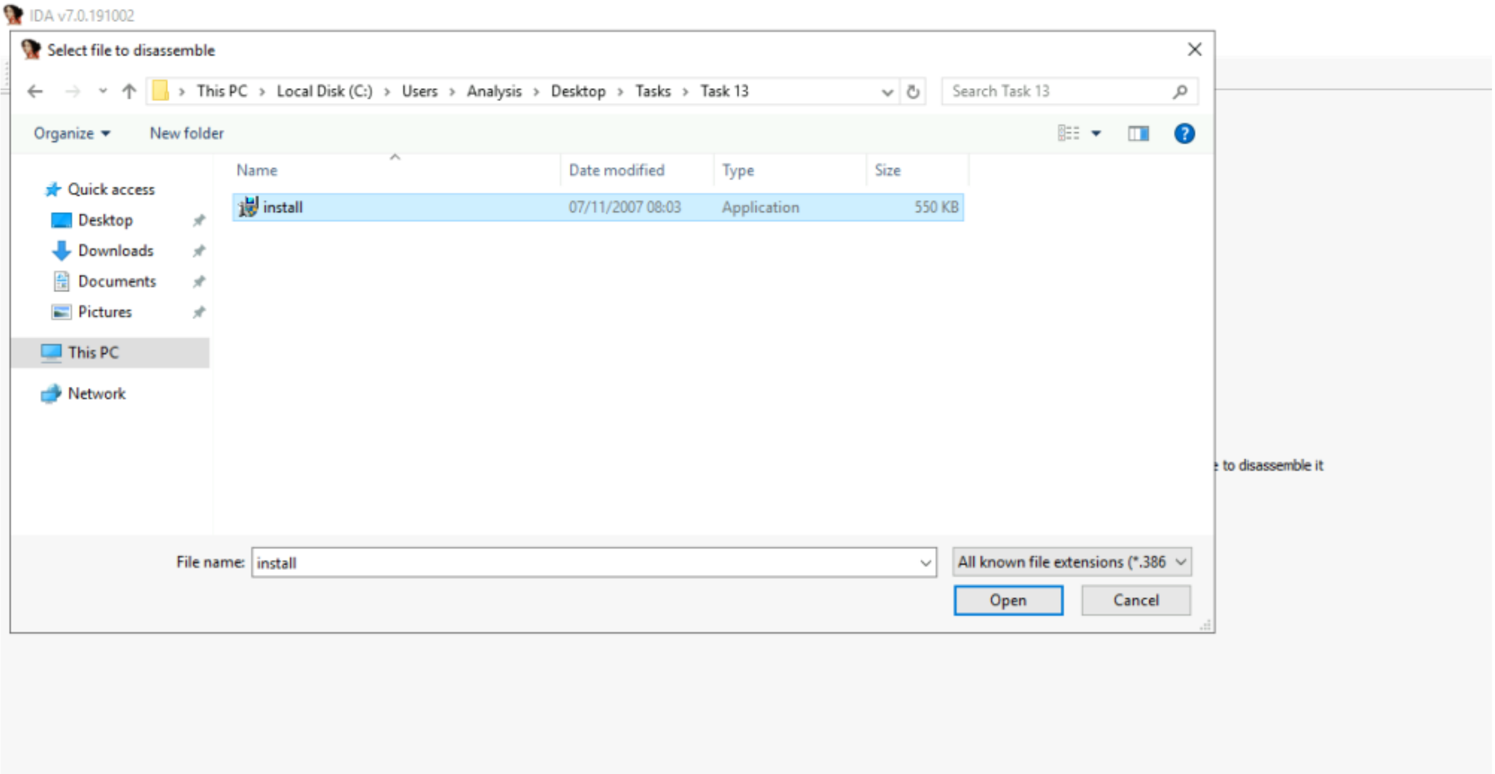
I first lauched the IDA Freeware as seen below.
- Use IDA Freeware.
- Open a new file, choose the install.exe.
- Click on the “import”.
- Move to the bottom, you will see the “Msi”s.



```
1  15:24    <DIR>          .
1  15:24    <DIR>          ..
1  00:20    <DIR>          Disassembley
1  21:26    <DIR>          PE Tools
      0 File(s)              0 bytes
      4 Dir(s)  13,780,639,744 bytes free
```

```
t file, or operabl
y again.

tion

sk 12\67844C01"
t file, or operabl
```

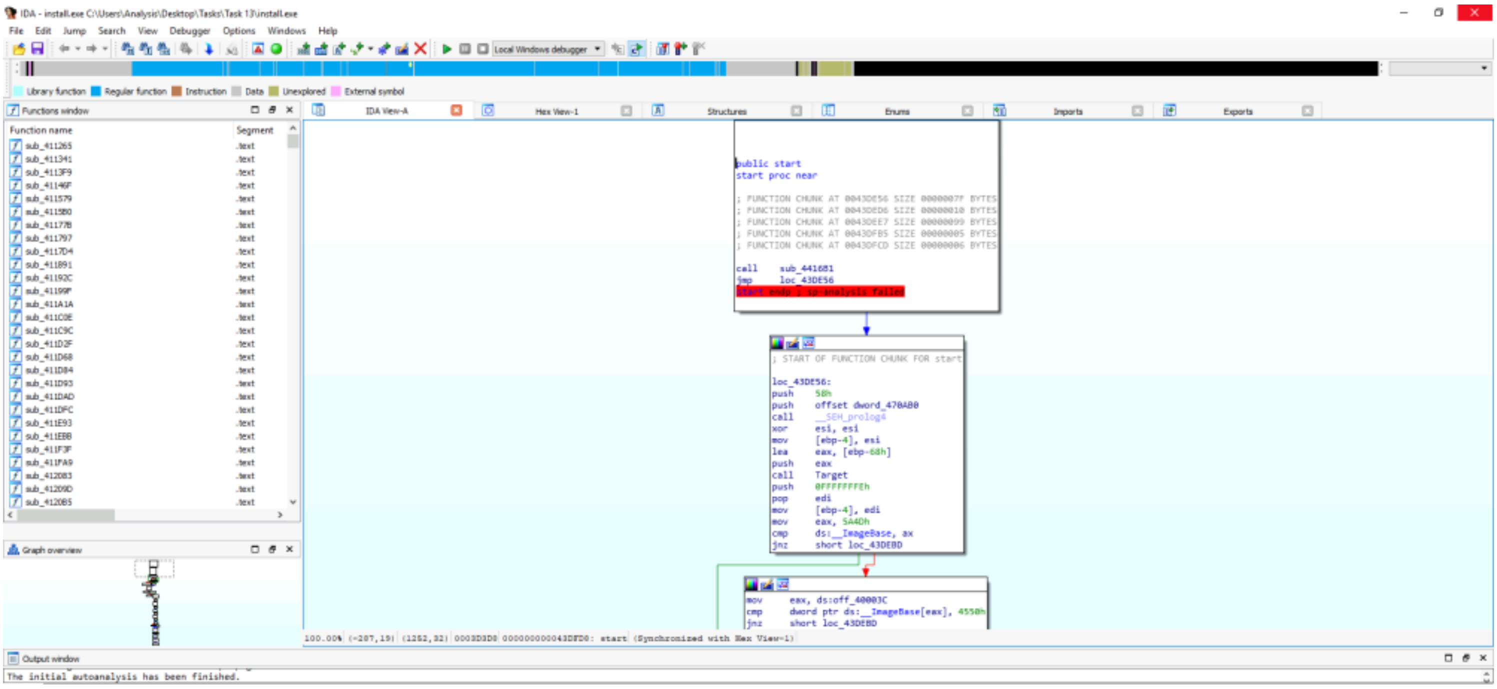
Date modified	Type	Size
13/02/2020 19:07	Shortcut	2 KB



Name	Date modified	Type	Size
install	07/11/2007 08:03	Application	550 KB

File name: install

All known file extensions (*.386


IDA - install.exe C:\Users\Analysis\Desktop\Tasks\Task 13\install.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output window

Function name	Segment
sub_411265	.text
sub_411341	.text
sub_4113F9	.text
sub_41146F	.text
sub_411579	.text
sub_4115B0	.text
sub_41177B	.text
sub_411797	.text
sub_4117D4	.text
sub_411891	.text
sub_41192C	.text
sub_41199F	.text
sub_411A1A	.text
sub_411C0E	.text
sub_411C9C	.text
sub_411D2F	.text
sub_411D68	.text
sub_411D84	.text
sub_411D93	.text
sub_411DAD	.text
sub_411DFC	.text
sub_411E93	.text
sub_411EBB	.text
sub_411F3F	.text
sub_411FA9	.text
sub_412083	.text
sub_41209D	.text
sub_4120B5	.text

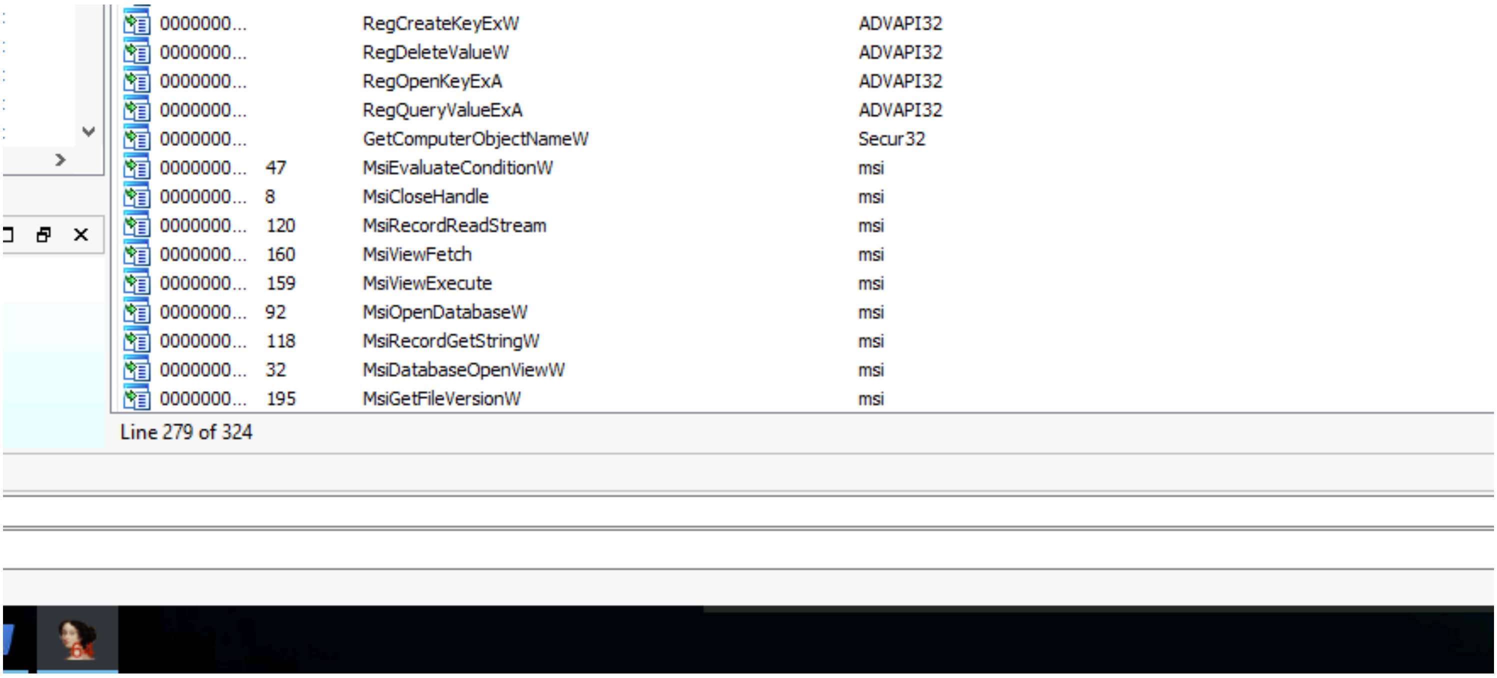
```
public start
start proc near

; FUNCTION CHUNK AT 0043DE56 SIZE 0000007F BYTES
; FUNCTION CHUNK AT 0043DED6 SIZE 00000010 BYTES
; FUNCTION CHUNK AT 0043DEE7 SIZE 00000099 BYTES
; FUNCTION CHUNK AT 0043DFB5 SIZE 00000005 BYTES
; FUNCTION CHUNK AT 0043DFCD SIZE 00000006 BYTES

call    sub_441681
jmp     loc_43DE56
start endp ; sp-analysis failed
```

```
; START OF FUNCTION CHUNK FOR start

loc_43DE56:
push    58h
push    offset dword_470AB0
call    __SEH_prolog4
xor     esi, esi
mov     [ebp-4], esi
lea     eax, [ebp-68h]
push    eax
call    Target
push    0FFFFFFFEh
pop     edi
mov     [ebp-4], edi
mov     eax, 5A4Dh
cmp     ds:__ImageBase, ax
jnz     short loc_43DEBD
```

```
mov     eax, ds:off_40003C
cmp     dword ptr ds:__ImageBase[eax], 4550h
jnz     short loc_43DEBD
```

```
100.00% (-287,19) (1252,32) 0003D3D0 000000000043DFD0: start (Synchronized with Hex View-1)
```

```
The initial autoanalysis has been finished.
```



0000000...		RegCreateKeyExW	ADVAPI32
0000000...		RegDeleteValueW	ADVAPI32
0000000...		RegOpenKeyExA	ADVAPI32
0000000...		RegQueryValueExA	ADVAPI32
0000000...		GetComputerObjectNameW	Secur32
0000000...	47	MsiEvaluateConditionW	msi
0000000...	8	MsiCloseHandle	msi
0000000...	120	MsiRecordReadStream	msi
0000000...	160	MsiViewFetch	msi
0000000...	159	MsiViewExecute	msi
0000000...	92	MsiOpenDatabaseW	msi
0000000...	118	MsiRecordGetStringW	msi
0000000...	32	MsiDatabaseOpenViewW	msi
0000000...	195	MsiGetFileVersionW	msi

Line 279 of 324

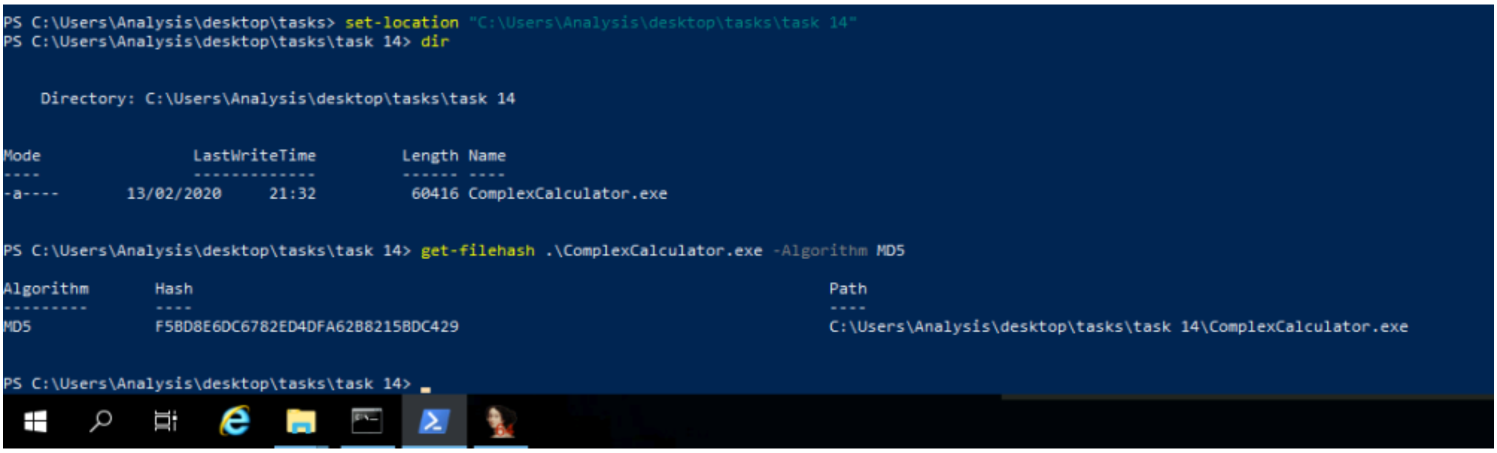
For this final section of this room, It was testing if I understood the basics of using various tools to analyse a file.

What is the MD5 Checksum of the file?

f5bd8e6dc6782ed4dfa62b8215bdc429

✓ Correct

Just as I did it in one of the previous tasks, I was able to retreive the filehash from the powershell terminal of the complexcalculator.exe as seen below



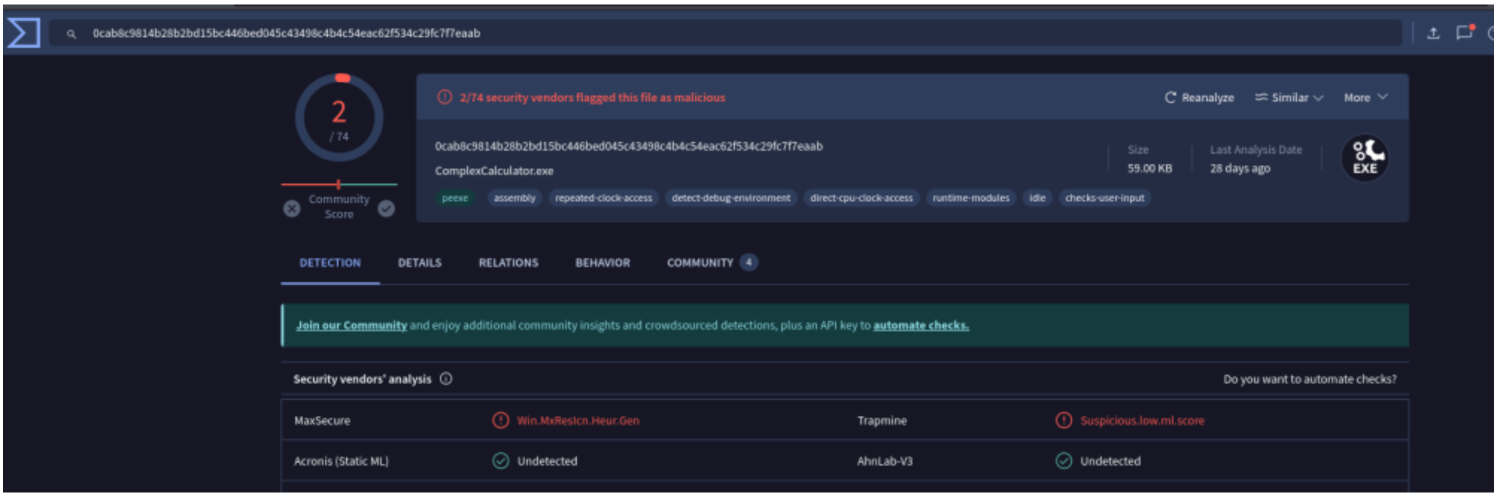
```
PS C:\Users\Analysis\desktop\tasks> set-location "C:\Users\Analysis\desktop\tasks\task 14"
PS C:\Users\Analysis\desktop\tasks\task 14> dir


    Directory: C:\Users\Analysis\desktop\tasks\task 14


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       13/02/2020     21:32          60416 ComplexCalculator.exe


PS C:\Users\Analysis\desktop\tasks\task 14> get-filehash .\ComplexCalculator.exe -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             F5BD8E6DC6782ED4DFA62B8215BDC429                                       C:\Users\Analysis\desktop\tasks\task 14\ComplexCalculator.exe


PS C:\Users\Analysis\desktop\tasks\task 14> _
```

Does Virustotal report this file as malicious? (Yay/Nay)

Yay

✓ Correct

I pasted this filehash on virus total, and it was flagged to be malicious by 2 vendors as it can be seen below.



0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

2 / 74

Community Score

2/74 security vendors flagged this file as malicious

0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

ComplexCalculator.exe

Size 59.00 KB

Last Analysis Date 28 days ago

peexe assembly repeated-clock-access detect-debug-environment direct-cpu-clock-access runtime-modules idle checks-user-input

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

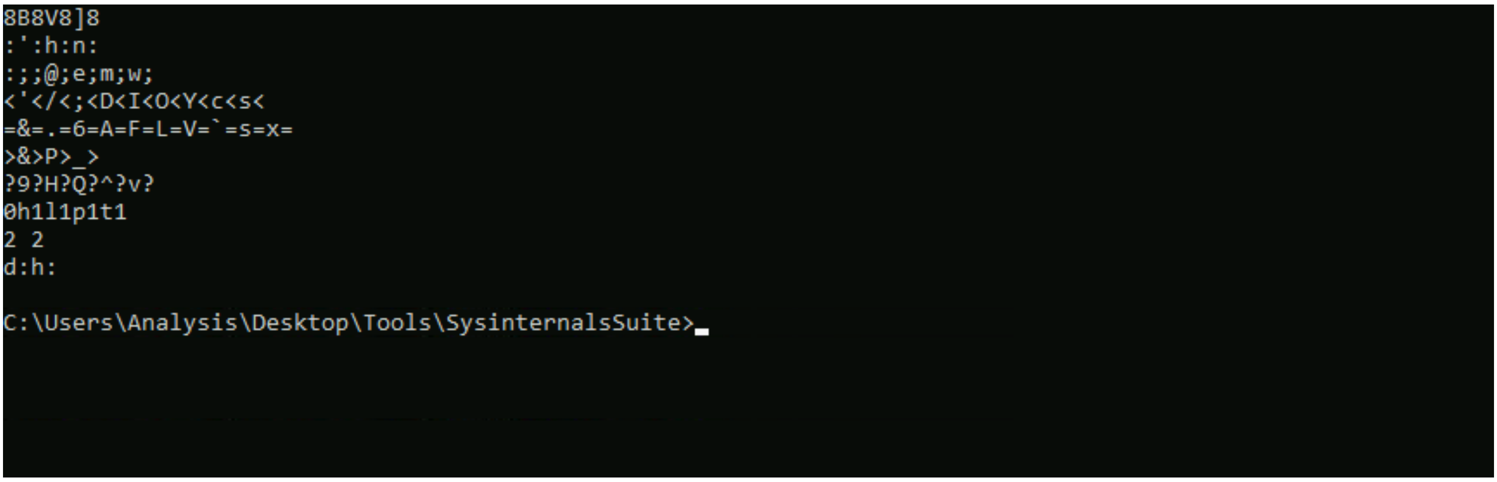
MaxSecure	Win.MxResIcn.Heur.Gen	Trapmine	Suspicious.low.ml.score
Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected

What is the last string outputted?

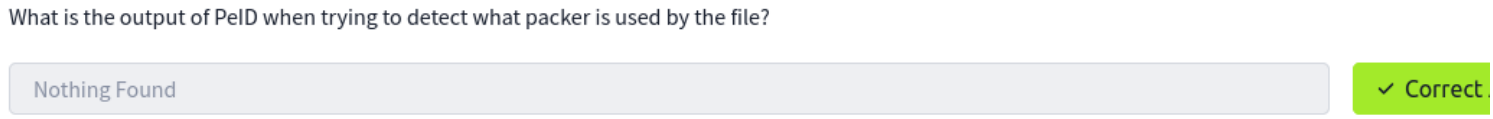
d:h:

✓ Correct

Using the strings cmd, I was able to retreive the last string outputted as shown below.



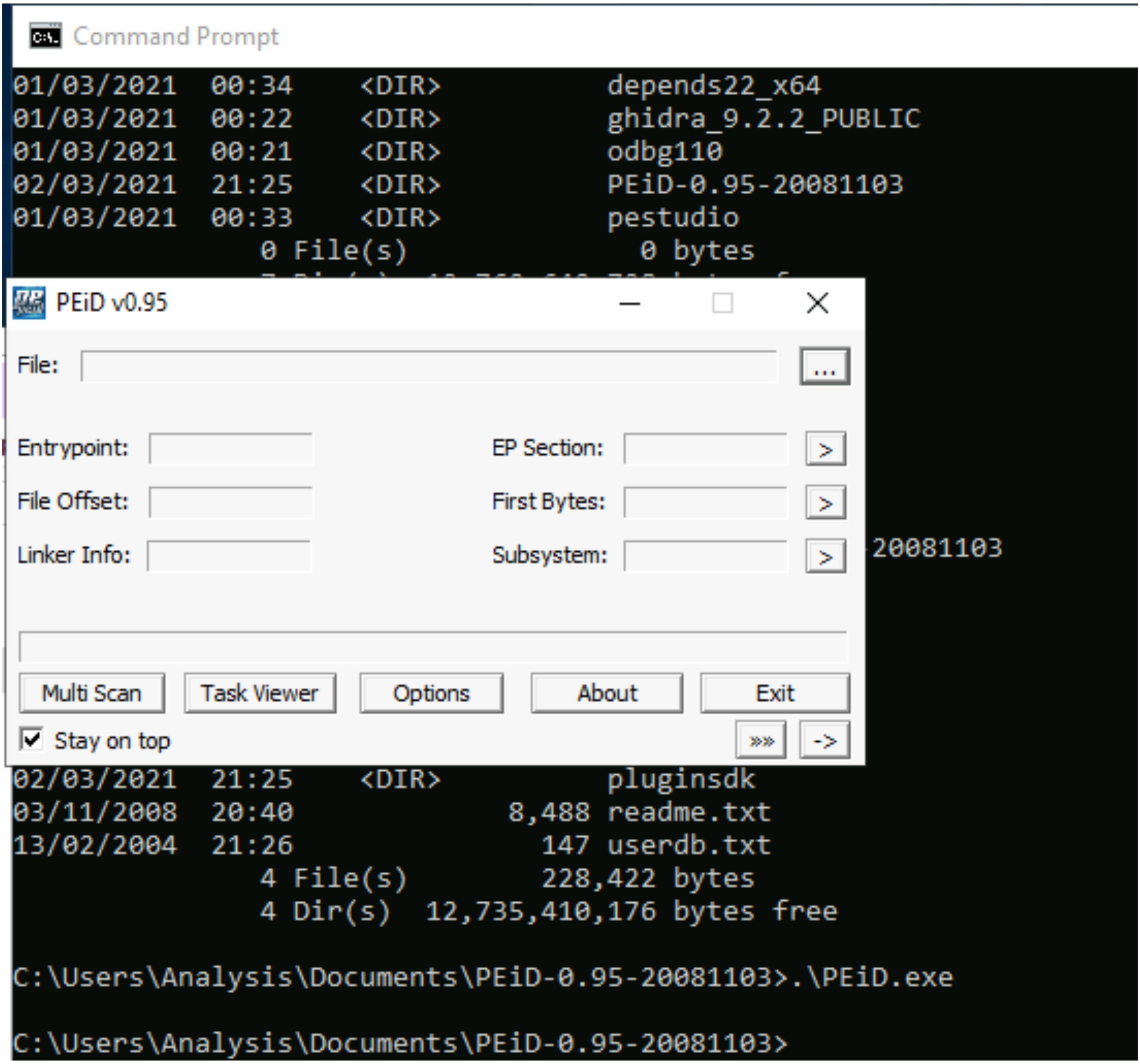
```
8B8V8]8
:':h:n:
:;;@;e;m;w;
<'</<;<D<I<O<Y<c<s<
=&=.=6=A=F=L=V=`=s=x=
>&>P>_>
?9?H?Q?^?v?
0h1l1p1t1
2 2
d:h:

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>_
```



What is the output of PeID when trying to detect what packer is used by the file?

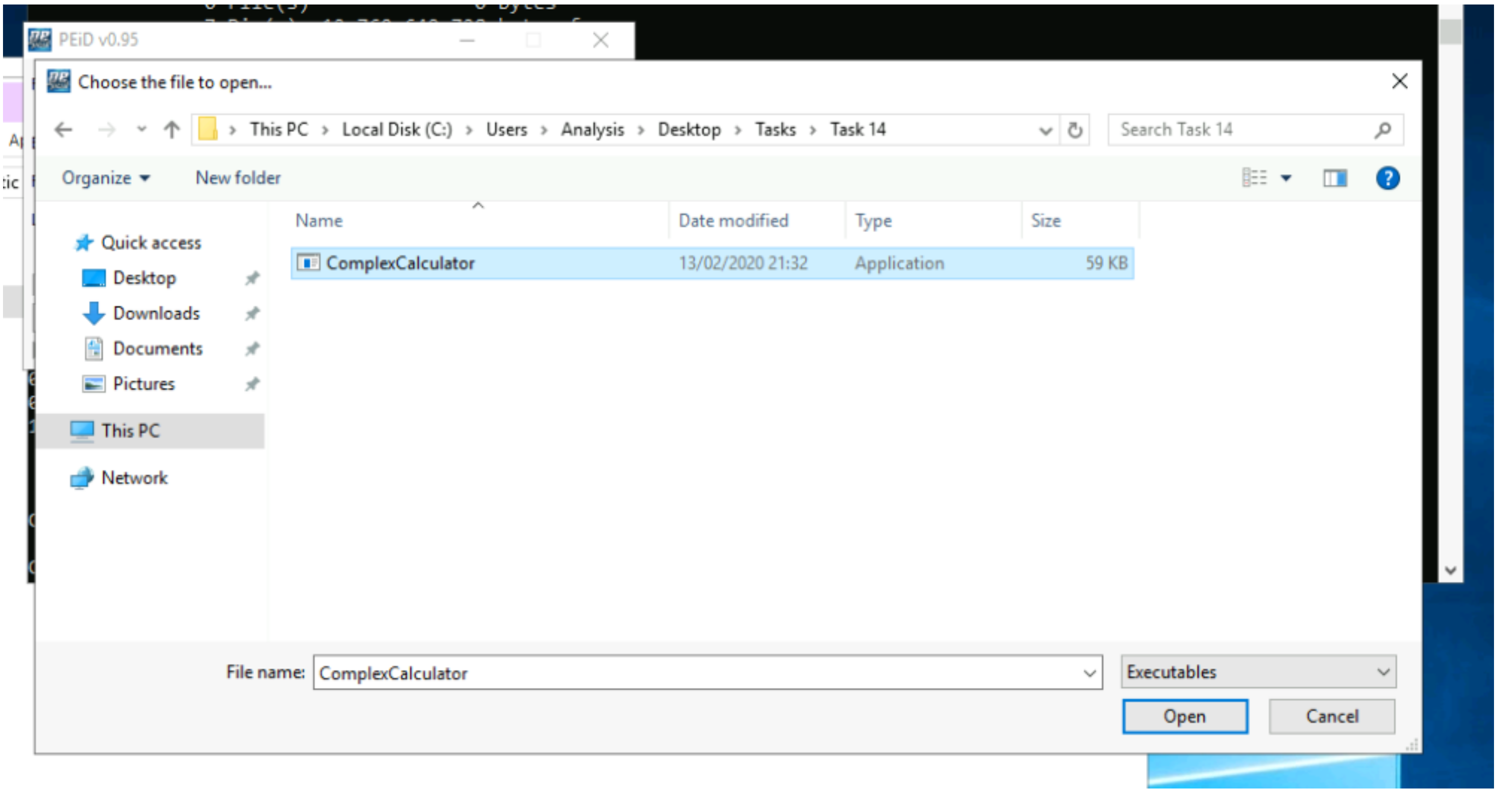
Nothing Found

I launched the PeID application as seen below.



```
01/03/2021  00:34    <DIR>          depends22_x64
01/03/2021  00:22    <DIR>          ghidra_9.2.2_PUBLIC
01/03/2021  00:21    <DIR>          odbg110
02/03/2021  21:25    <DIR>          PEiD-0.95-20081103
01/03/2021  00:33    <DIR>          pestudio
               0 File(s)              0 bytes

02/03/2021  21:25    <DIR>          pluginsdk
03/11/2008  20:40             8,488 readme.txt
13/02/2004  21:26               147 userdb.txt
               4 File(s)        228,422 bytes
               4 Dir(s)  12,735,410,176 bytes free

C:\Users\Analysis\Documents\PEiD-0.95-20081103>.\PEiD.exe

C:\Users\Analysis\Documents\PEiD-0.95-20081103>
```

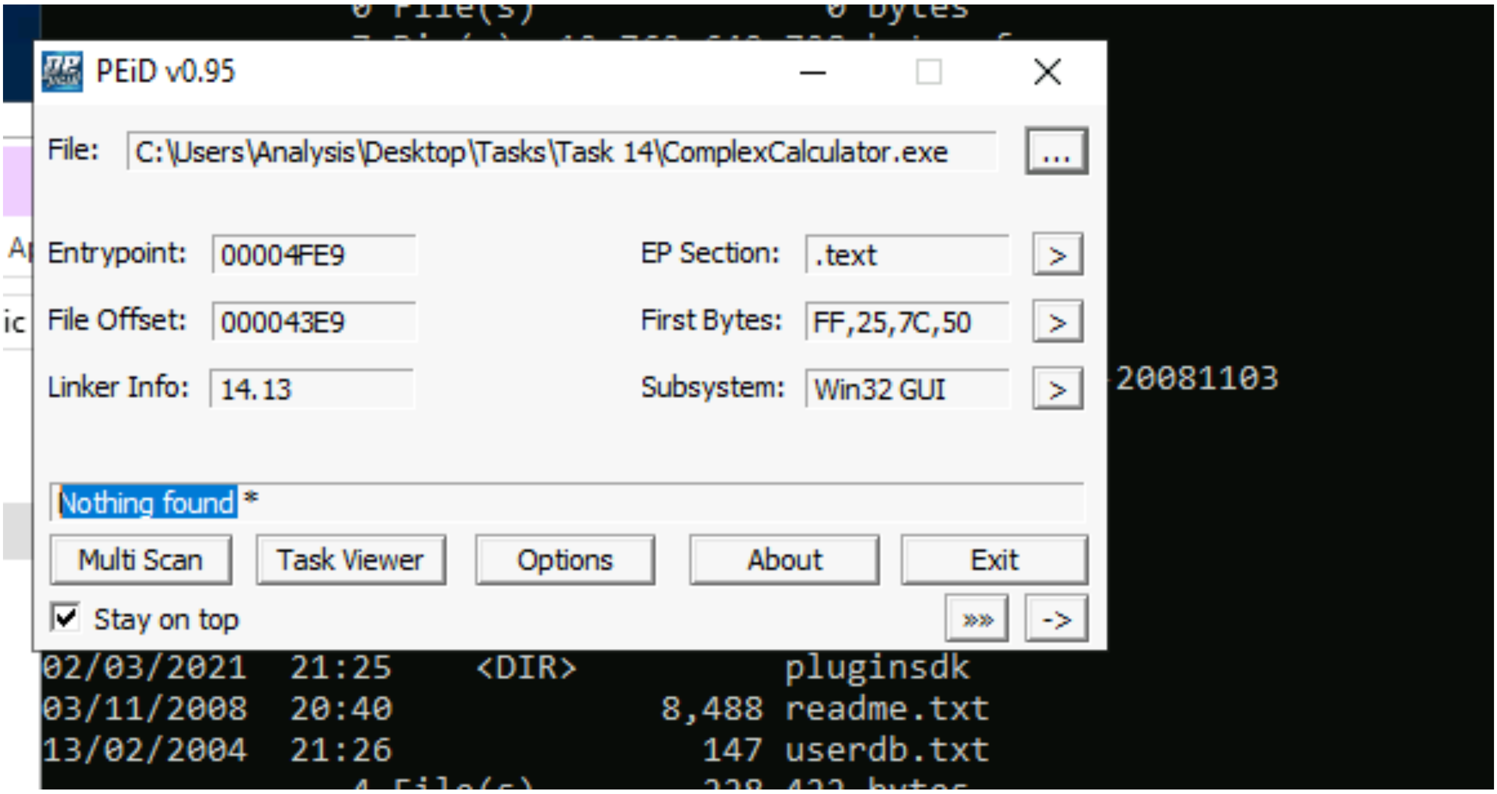
Selected the .exe file to be analysed as seen below.



Name	Date modified	Type	Size
ComplexCalculator	13/02/2020 21:32	Application	59 KB

File name: ComplexCalculator

No packer was found. as seen from the image below.



File: C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculator.exe

Entrypoint: 00004FE9

EP Section: .text

File Offset: 000043E9

First Bytes: FF,25,7C,50

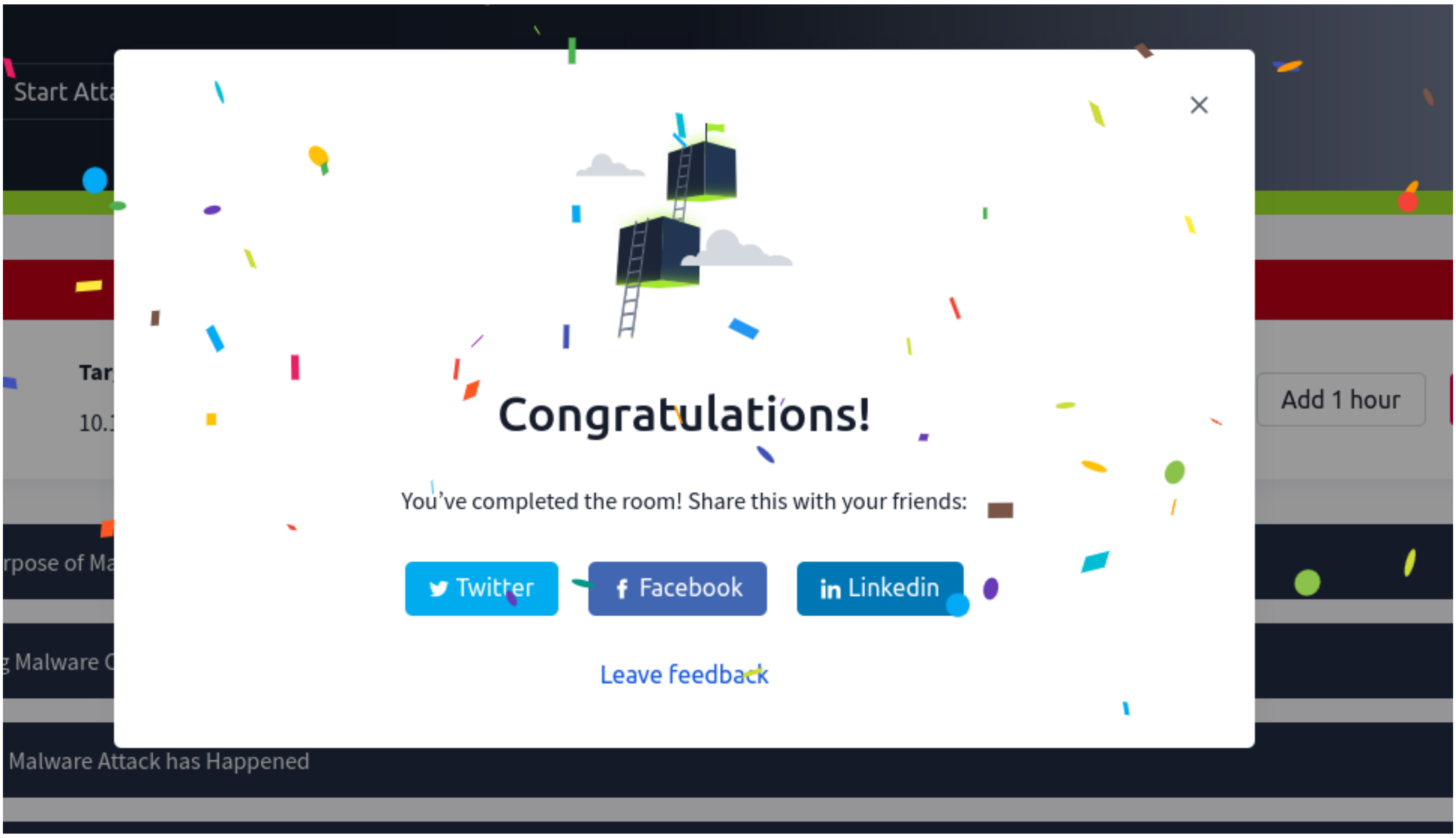
Linker Info: 14.13

Subsystem: Win32 GUI

Nothing found *

```
02/03/2021  21:25    <DIR>          pluginsdk
03/11/2008  20:40             8,488 readme.txt
13/02/2004  21:26               147 userdb.txt
```

This marked the end of this room.



Congratulations!

You've completed the room! Share this with your friends:

https://tryhackme.com/r/room/malmalintroductory

Conclusion

Understanding malware is crucial in the ongoing battle against cyber threats. By analyzing points of entry, identifying indicators of execution, assessing performance, and developing prevention strategies, we can enhance our defenses against these malicious entities. This introductory guide is just the beginning; future explorations will delve deeper into the sophisticated techniques and tools that empower us to stay ahead in the ever-evolving landscape of cybersecurity.