Digital Forensics

Assignment 3 – Memory Image

10 points

Kush Patel

Note:
Sometimes, it can be hard to find where a certificate/private key is stored. Here are the steps to delete a key completely from the computer. We will use PowerShell, which is an enhanced command console.

1. PowerShell Get Certificate Thumbprint with Password PFX File

Get-PfxCertificate -FilePath Key.pfx

2. List any certificates with a thumbprint within powershell

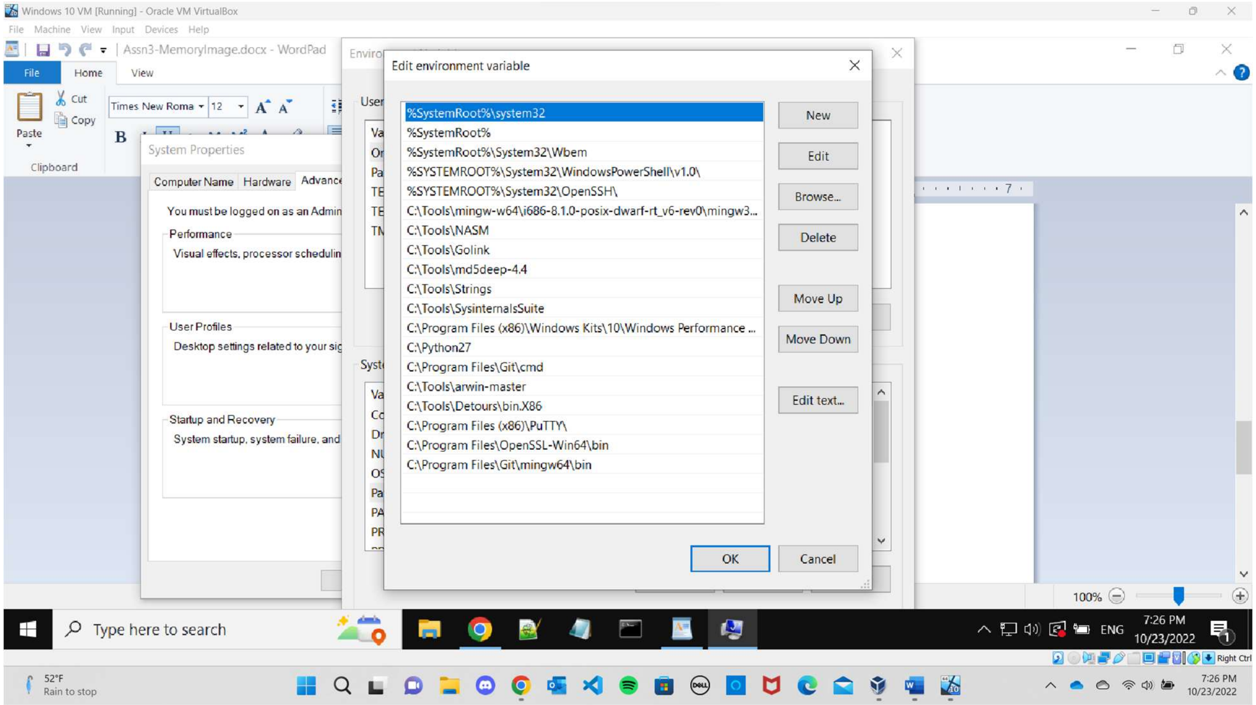
dir cert: -Recurse | Where-Object { $_.Thumbprint –like "*371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6*" }

3. Delete by thumbprint

Get-ChildItem Cert:\CurrentUser\My\371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6 | Remove-Item

QUESTIONS

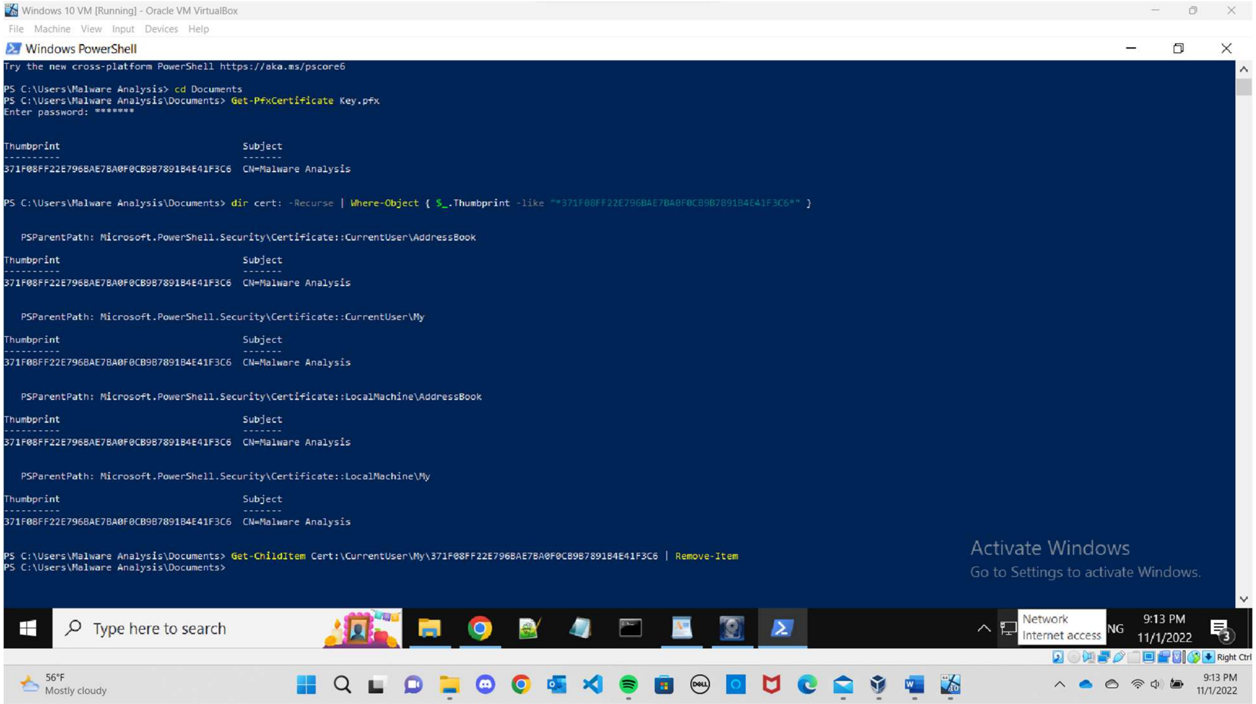
1. Please refer to [1] and add *C:\Program Files\Git\mingw64\bin*, where *openssl.exe* is stored, to the environment variable *path* in *System variables*. Please include a screenshot of the changed environment variable *path* below. (1 point)



Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Assn3-MemoryImage.docx - WordPad
File
Home
View
Cut
Copy
Paste
Clipboard
Times New Roma
12
System Properties
Computer Name
Hardware
Advanc
You must be logged on as an Admin
Performance
Visual effects, processor schedulin
User Profiles
Desktop settings related to your sig
Startup and Recovery
System startup, system failure, and
Enviro
Edit environment variable
New
Edit
Browse...
Delete
Move Up
Move Down
Edit text...
OK
Cancel
100%
Type here to search
ENG
7:26 PM
10/23/2022
52°F
Rain to stop
Right Ctrl

```
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Tools\mingw-w64\i686-8.1.0-posix-dwarf-rt_v6-rev0\mingw3...
C:\Tools\NASM
C:\Tools\Golink
C:\Tools\md5deep-4.4
C:\Tools\Strings
C:\Tools\SysinternalsSuite
C:\Program Files (x86)\Windows Kits\10\Windows Performance ...
C:\Python27
C:\Program Files\Git\cmd
C:\Tools\arwin-master
C:\Tools\Detours\bin.X86
C:\Program Files (x86)\PuTTY\
C:\Program Files\OpenSSL-Win64\bin
C:\Program Files\Git\mingw64\bin
```

2. It is recommended that students use the EFS key provided by the instructor. Open an EFS encrypted file in the Windows VM. Then delete the EFS key using the approach above. After the EFS key is deleted from the Certificate Store/computer,



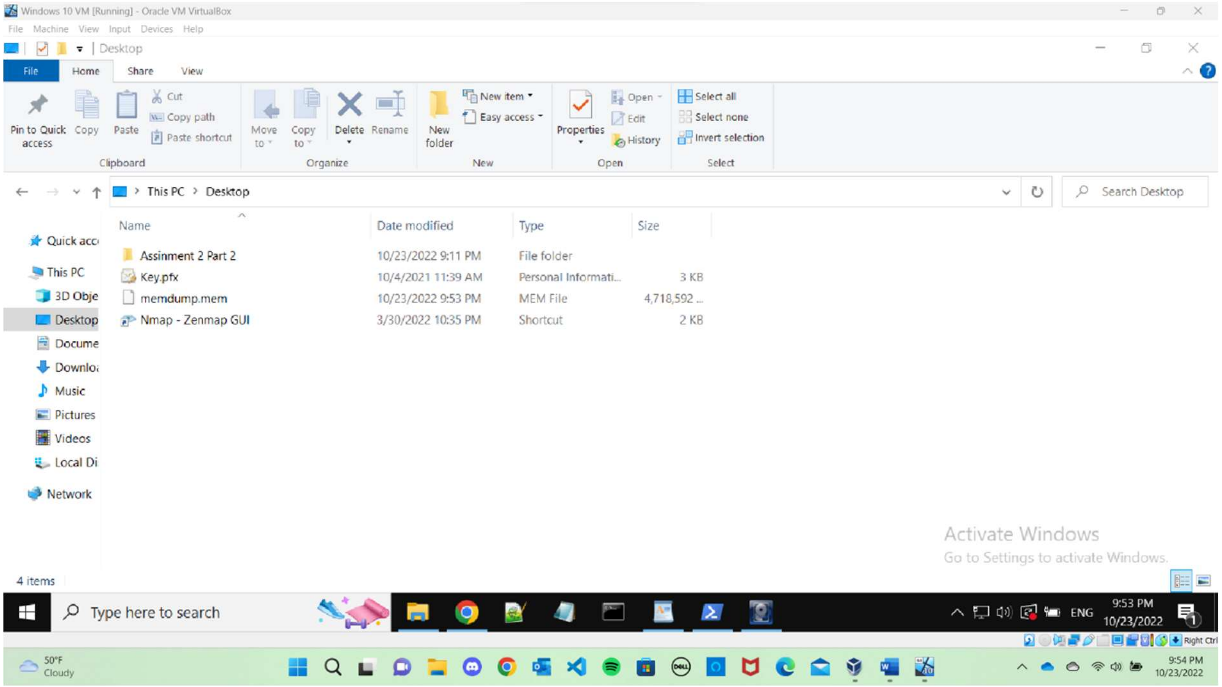
```
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Malware Analysis> cd Documents
PS C:\Users\Malware Analysis\Documents> Get-PfxCertificate Key.pfx
Enter password: *******


Thumbprint                                Subject
----------                                -------
371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6  CN=Malware Analysis


PS C:\Users\Malware Analysis\Documents> dir cert: -Recurse | Where-Object { $_.Thumbprint -like "*371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6*" }


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\AddressBook

Thumbprint                                Subject
----------                                -------
371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6  CN=Malware Analysis


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6  CN=Malware Analysis


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\AddressBook

Thumbprint                                Subject
----------                                -------
371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6  CN=Malware Analysis


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6  CN=Malware Analysis


PS C:\Users\Malware Analysis\Documents> Get-ChildItem Cert:\CurrentUser\My\371F08FF22E796BAE7BA0F0CB9B7891B4E41F3C6 | Remove-Item
PS C:\Users\Malware Analysis\Documents>
```

Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell
Activate Windows
Go to Settings to activate Windows.
Type here to search
Network
Internet access
9:13 PM
11/1/2022
56°F
Mostly cloudy

- Can the EFS encrypted file still be decrypted? (1 point)
  Yes, I was able to decrypt it.

- Why? (1 point)
  This is because the Key is no longer on the computer so the files are able to be decrypted without the key.

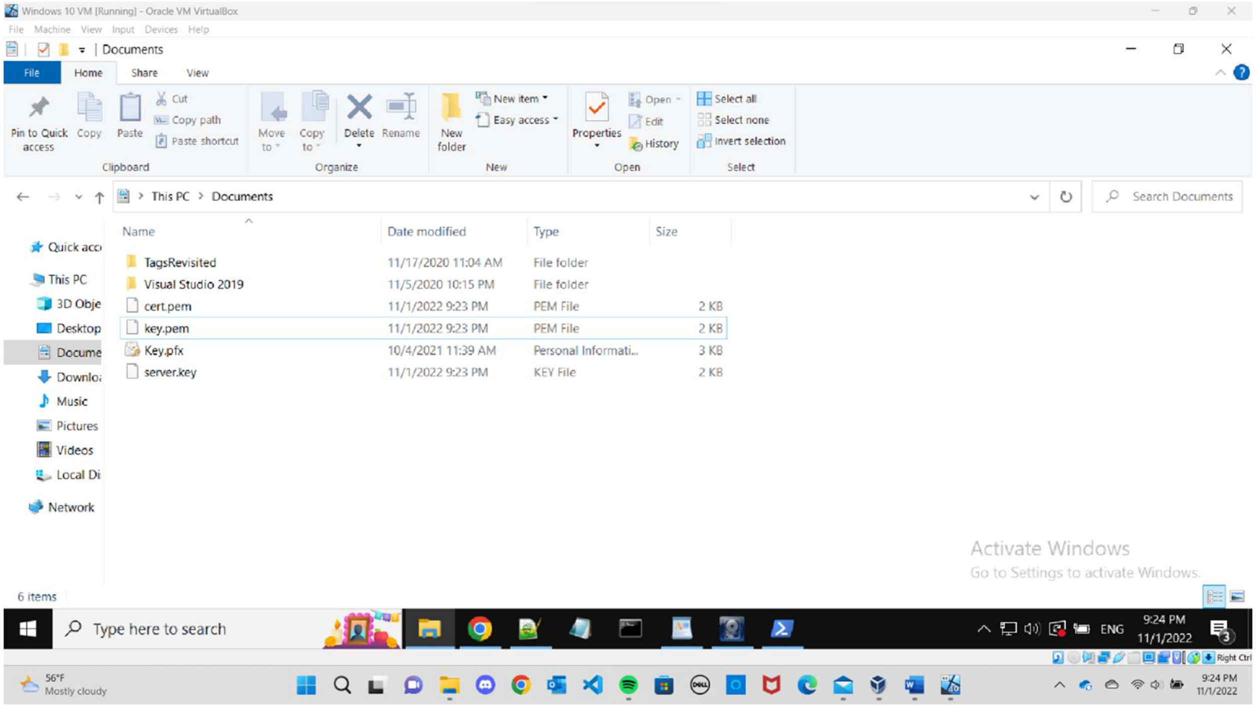
3. Use FTK Imager →File → Capture Memory … to dump the entire memory of the Windows VM. Include a screenshot of the memory dump file in File Explorer below. (1 point)



Name	Date modified	Type	Size
Assinment 2 Part 2	10/23/2022 9:11 PM	File folder	
Key.pfx	10/4/2021 11:39 AM	Personal Informati...	3 KB
memdump.mem	10/23/2022 9:53 PM	MEM File	4,718,592 ...
Nmap - Zenmap GUI	3/30/2022 10:35 PM	Shortcut	2 KB

4. Run the following command to export the private key from a .pfx file. Include a screenshot of *privkey.pem* below, which can be given another name of your choice, in File Explorer. (2 points)

Its called key.pem. Followed the instructions from the link in the question.



Name	Date modified	Type	Size
TagsRevisited	11/17/2020 11:04 AM	File folder	
Visual Studio 2019	11/5/2020 10:15 PM	File folder	
cert.pem	11/1/2022 9:23 PM	PEM File	2 KB
key.pem	11/1/2022 9:23 PM	PEM File	2 KB
Key.pfx	10/4/2021 11:39 AM	Personal Informati...	3 KB
server.key	11/1/2022 9:23 PM	KEY File	2 KB

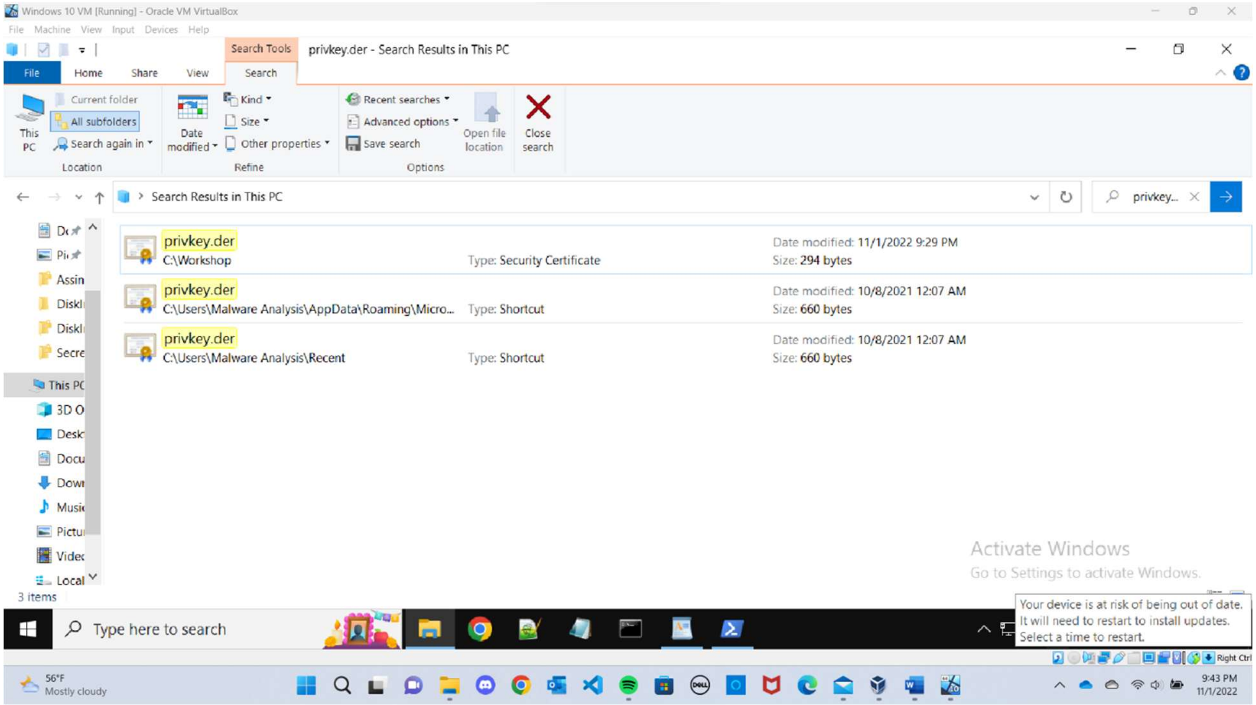
5. Edit privkey.pem with Notepad++ (or any text editor) and keep only the part from "-----BEGIN PRIVATE KEY-----" to "-----END PRIVATE KEY-----". Copy and paste the context of the revised privkey.pem below. (1 point)

-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDmATcNBHspjT0
Q
PceCLC0bJQeeEn7dpHBbr8uDZkw1TgyVNhy9uRZbJVI3LJDFbbpAfm9noqLtthrm
V0cddmKmv8PhRQhEzZ9y7uFijEAO5ZcGVepbWNTb3aVP+BUrEz6SmeI16OEr9W6k
BRiDHa7T3xxLijrA0umbsYk/BFaBaiboRz6GVDZ/UvVb0WjTH/RACl53zDsypAXO
FLSKYqbmheASyzX1aJSu09C0kvdfM9uLdkm0Wf6njSMfb495AE/2qoLukfFrpVWV
6sAZ6XJuf8HFdtrAivg5YkgRt9Hwb5kwyCN+K3LKxgGDPt8uoGDR+Yt5Qn1ru3Vm
LSpXYb8VAgMBAAECggEBAJ+qokO4I6Oht40pxfDYp+tbFmGmZ0mH2LPdYoLyJd8v
Mk72xJb0AM//JYbFui5D0PLqkn24CjDIpP3YArcyMqOdJeag3G+e6pyHthCKWgG9
Ycz1IX6OOR30TMkp59ACSQLOLpnL81xnwYm9O9nxZicQj/zklYq8H42EfkkvwrmM
3Tl3JpbrHzE7Cvd0u+Sjy9Na/gkhCRh/PeUCqWf5ZqapxZbgaEefkETX//AiP9Q5

```
yZL+gt5sCqJnQlk6UeFGf/Cgw+Y6ckrp76To0O1dilEjQj44y9ZQEBJ8MWo28wQL
jchR3bbT4xDPpcxMlhEyzFoASsYvGaKzaQhoRbkwlnUCgYEA7JuXmITj9W61aRAq
8W+T71+aQKETMEVGw+OtLj6GVFPVqz5CxBPwzqzx55yuXwB3tYFg8ZmEAnCtFyVo
qp1RS7zBvT7bO0CjJ537fZ4NLMm/+c4OP3/zn9UA1dr5FFIJ/68hRBbY721X/vWa
InDKLC3DBhVLv6mDuH/YFsBkNSsCgYEA+NsUpxR56kLNHhUamCFV/G4Dm+wN6d
Ci
99RJhOWys6knja6xBSw2SvLIoqMTVr1iFBW7E6Q/XgDbTfvylecH+mDVNEYQo6XF
dJ8zMf7non2ghtNfhi8qOujCgEX9/3/lNxRvFLLVSmkF35lFt8NLsbJlHpO4h72b
5OuAdyx4PL8CgYB+brYXHgvh/oKZ3bXUxda7Ns7qcigaxyoFSwgjie2l6hZnJyHu
POmUxv2M0kCrK0jMiJIRCANuel9D2w2O/fmPCxJL2ea0RtnoNZdJjMdlg3k+N0mN
zQWWBvAnVpd6sEv/gMm55KuPZVJ8PylZ9gNSkDGCcqbDiAWG9Wm23p+teQKBgHS
k
S1Pc9x/kW7wj7CkuRt1gu3RT+lmDnz9GU4dlGpO3T4DLRtHD3VbX4U7J3QClF9mO
LfeQ3tqy0BgHZbb5aPXkeUpdJONvidOV4ysl7XBuLdXEMVv1s3eVLcVuCRW+3rMo
csBi6jJMc6JQdysg8NPDaD4iwzVsnCt6buZtA5aFAoGANjM3+0NWmKUBr12ue+gs
1Vh5ciQzpe8F0niyMTQAWXRH3ZnRfyJ1exXuZNvHHM2ArElogxTcKng7/dFWWXAF
ld/BHYZrLxvLNV3s09fl8OPETtSxA3PqCoh6aOcKi+QSVGz1/qnYGiuIr/Q09uFT
bjWgJPRuzRGQBYIsn0n+otE=
-----END PRIVATE KEY-----
```

6. Convert openssl private key to the binary .der format, which contains the binary private key. The private key is saved in *privkey.der*, which can be given another name, in the example below. Include a screenshot of privkey.der in File Explorer below. (1 point)

openssl rsa -in c:\Workshop\privkey.pem *-pubout -outform DER -out* c:\Workshop\privkey.der



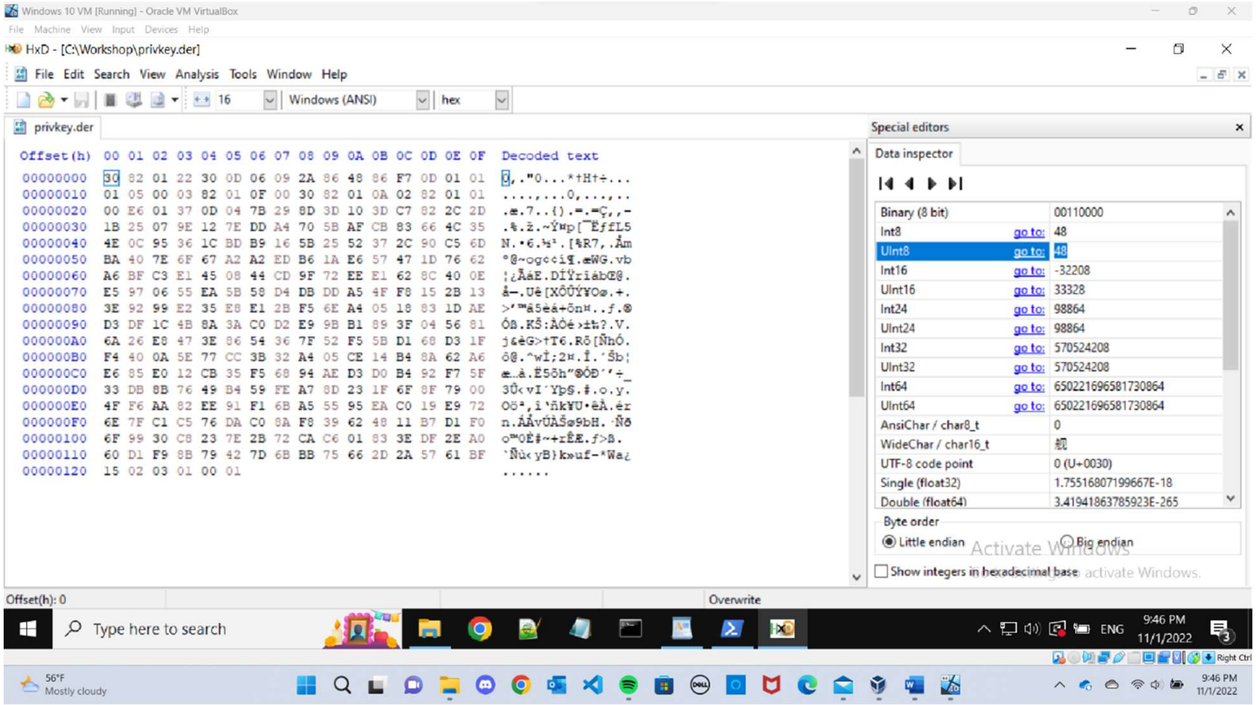
Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Search Tools
privkey.der - Search Results in This PC
File Home Share View Search
This PC
Current folder
All subfolders
Search again in
Location
Date modified
Kind
Size
Other properties
Refine
Recent searches
Advanced options
Save search
Options
Open file location
Close search
Search Results in This PC
privkey...
3 items
Type here to search
Activate Windows
Go to Settings to activate Windows.
Your device is at risk of being out of date. It will need to restart to install updates. Select a time to restart.
56°F
Mostly cloudy
9:43 PM
11/1/2022

privkey.der
C:\Workshop Type: Security Certificate Date modified: 11/1/2022 9:29 PM Size: 294 bytes

privkey.der
C:\Users\Malware Analysis\AppData\Roaming\Micro... Type: Shortcut Date modified: 10/8/2021 12:07 AM Size: 660 bytes

privkey.der
C:\Users\Malware Analysis\Recent Type: Shortcut Date modified: 10/8/2021 12:07 AM Size: 660 bytes

7. Use the hex editor HxD installed in the Windows VM to search the memory dump for the private key (stored in privkey.der) in the memory. Include a screenshot of found private key in HxD below. (2 points)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HxD - [C:\Workshop\privkey.der]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
privkey.der
Special editors
Data inspector
Offset(h): 0
Overwrite
Type here to search
ENG
9:46 PM
11/1/2022
Right Ctrl
56°F
Mostly cloudy
9:46 PM
11/1/2022

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01  0‚."0...*†H†÷...
00000010  01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01  ....‚...0‚...‚..
00000020  00 E6 01 37 0D 04 7B 29 8D 3D 10 3D C7 82 2C 2D  .æ.7..{).=.=Ç‚,-
00000030  1B 25 07 9E 12 7E DD A4 70 5B AF CB 83 66 4C 35  .%.ž.~Ý¤p[¯ËƒfL5
00000040  4E 0C 95 36 1C BD B9 16 5B 25 52 37 2C 90 C5 6D  N.•6.½¹.[%R7,.Åm
00000050  BA 40 7E 6F 67 A2 A2 ED B6 1A E6 57 47 1D 76 62  º@~og¢¢í¶.æWG.vb
00000060  A6 BF C3 E1 45 08 44 CD 9F 72 EE E1 62 8C 40 0E  ¦¿ÃáE.DÍŸrîábŒ@.
00000070  E5 97 06 55 EA 5B 58 D4 DB DD A5 4F F8 15 2B 13  å—.Uê[XÔÛÝ¥Oø.+.
00000080  3E 92 99 E2 35 E8 E1 2B F5 6E A4 05 18 83 1D AE  >’™â5èá+õn¤..ƒ.®
00000090  D3 DF 1C 4B 8A 3A C0 D2 E9 9B B1 89 3F 04 56 81  Óß.KŠ:ÀÒé›±‰?.V.
000000A0  6A 26 E8 47 3E 86 54 36 7F 52 F5 5B D1 68 D3 1F  j&èG>†T6.Rõ[ÑhÓ.
000000B0  F4 40 0A 5E 77 CC 3B 32 A4 05 CE 14 B4 8A 62 A6  ô@.^wÌ;2¤.Î.´Šb¦
000000C0  E6 85 E0 12 CB 35 F5 68 94 AE D3 D0 B4 92 F7 5F  æ…à.Ë5õh”®ÓÐ´’÷_
000000D0  33 DB 8B 76 49 B4 59 FE A7 8D 23 1F 6F 8F 79 00  3Û‹vI´Yþ§.#.o.y.
000000E0  4F F6 AA 82 EE 91 F1 6B A5 55 95 EA C0 19 E9 72  Oöª‚î‘ñk¥U•êÀ.ér
000000F0  6E 7F C1 C5 76 DA C0 8A F8 39 62 48 11 B7 D1 F0  n.ÁÅvÚÀŠø9bH.·Ñð
00000100  6F 99 30 C8 23 7E 2B 72 CA C6 01 83 3E DF 2E A0  o™0È#~+rÊÆ.ƒ>ß. 
00000110  60 D1 F9 8B 79 42 7D 6B BB 75 66 2D 2A 57 61 BF  `Ñù‹yB}k»uf-*Wa¿
00000120  15 02 03 01 00 01                                ......
```

Binary (8 bit)		00110000
Int8	go to:	48
UInt8	go to:	48
Int16	go to:	-32208
UInt16	go to:	33328
Int24	go to:	98864
UInt24	go to:	98864
Int32	go to:	570524208
UInt32	go to:	570524208
Int64	go to:	650221696581730864
UInt64	go to:	650221696581730864
AnsiChar / char8_t		0
WideChar / char16_t		舰
UTF-8 code point		0 (U+0030)
Single (float32)		1.75516807199667E-18
Double (float64)		3.41941863785923E-265

Byte order

● Little endian ○ Big endian

□ Show integers in hexadecimal base

References

[1] Add to the PATH on Windows 10, March 17, 2018
[2] about_Environment_Variables, 08/18/2021