Worcester Polytechnic Institute
Department of Computer Science

Module 1: Memory Acquisition with WinPMem

Objectives

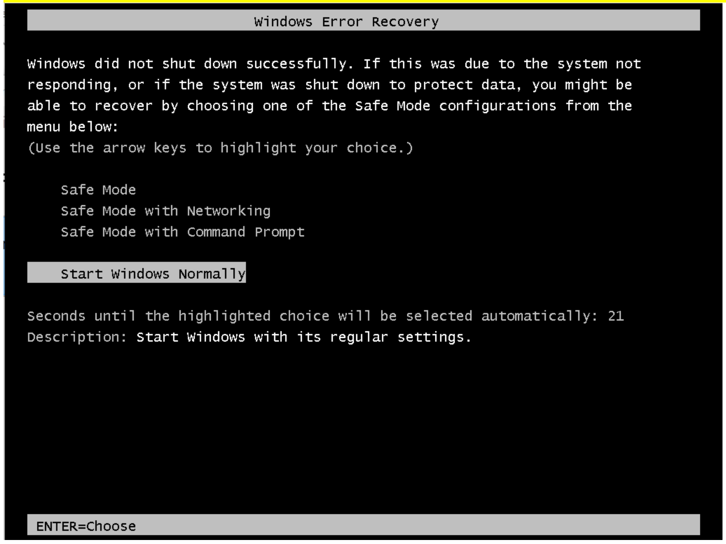
- Understand how to use WinPMem in the command line

Tasks

Task 0. Prepare a Windows 7 Virtual Machine

(While you could do this activity (Activity 10-1) on your host machine, the next module, Activity 10-2, will **require** using WinPMem on a Windows 7 machine to analyze malware so you will save time if you do this activity on a Windows 7 machine now.)

If you are using the prepared Windows 7 virtual machine you can skip to task 2

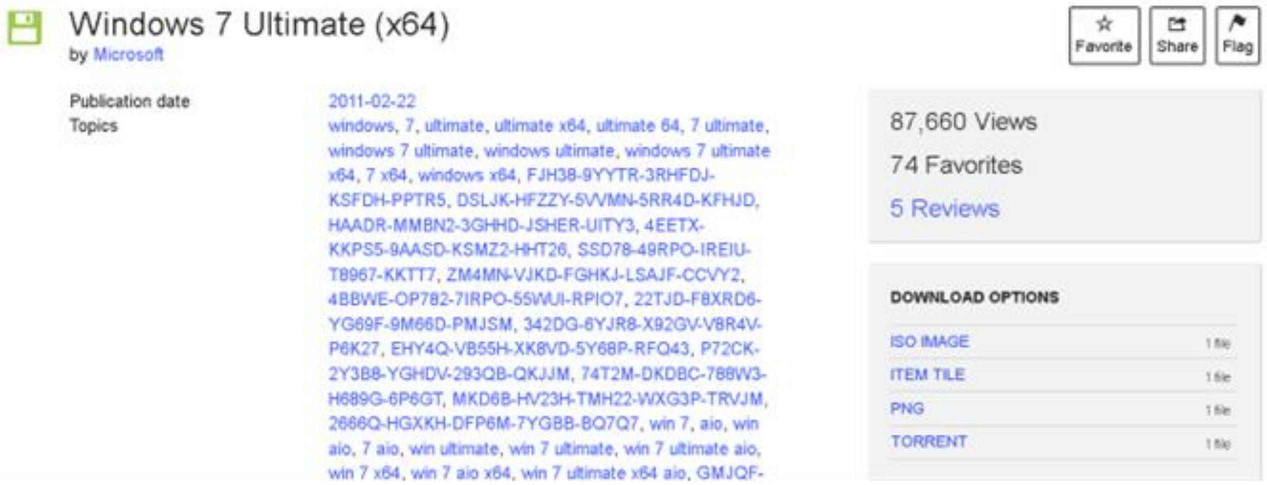


```
                          Windows Error Recovery

Windows did not shut down successfully. If this was due to the system not
responding, or if the system was shut down to protect data, you might be
able to recover by choosing one of the Safe Mode configurations from the
menu below:
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Start Windows Normally

Seconds until the highlighted choice will be selected automatically: 21
Description: Start Windows with its regular settings.

 ENTER=Choose
```

And If you see this screen on the prepared Windows 7 virtual machine, start windows normally by selecting it and hitting enter.

1. https://archive.org/details/windows7ultimatex64_201912

Click “Iso image” on the right to download the iso.



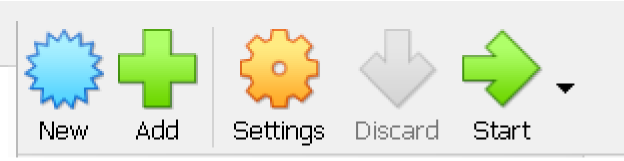
Windows 7 Ultimate (x64)
by Microsoft

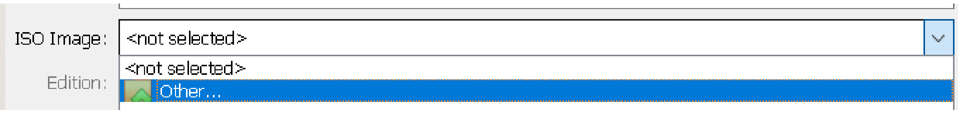
Publication date 2011-02-22
Topics windows, 7, ultimate, ultimate x64, ultimate 64, 7 ultimate, windows 7 ultimate, windows ultimate, windows 7 ultimate x64, 7 x64, windows x64, FJH38-9YYTR-3RHFDJ-KSFDH-PPTR5, DSLJK-HFZZY-5VVMN-5RR4D-KFHJD, HAADR-MMBN2-3GHHD-JSHER-UITY3, 4EETX-KKPS5-9AASD-KSMZ2-HHT26, SSD78-49RPO-IREIU-T8967-KKTT7, ZM4MN-VJKD-FGHKJ-LSAJF-CCVY2, 4BBWE-OP782-7IRPO-55WUI-RPIO7, 22TJD-F8XRD6-YG69F-9M66D-PMJSM, 342DG-6YJR8-X92GV-V8R4V-P6K27, EHY4Q-VB55H-XK8VD-5Y68P-RFQ43, P72CK-2Y3B8-YGHDV-293QB-QKJJM, 74T2M-DKDBC-788W3-H689G-6P6GT, MKD6B-HV23H-TMH22-WXG3P-TRVJM, 2666Q-HGXKH-DFP6M-7YGBB-BQ7Q7, win 7, aio, win aio, 7 aio, win ultimate, win 7 ultimate, win 7 ultimate aio, win 7 x64, win 7 aio x64, win 7 ultimate x64 aio, GMJQF-

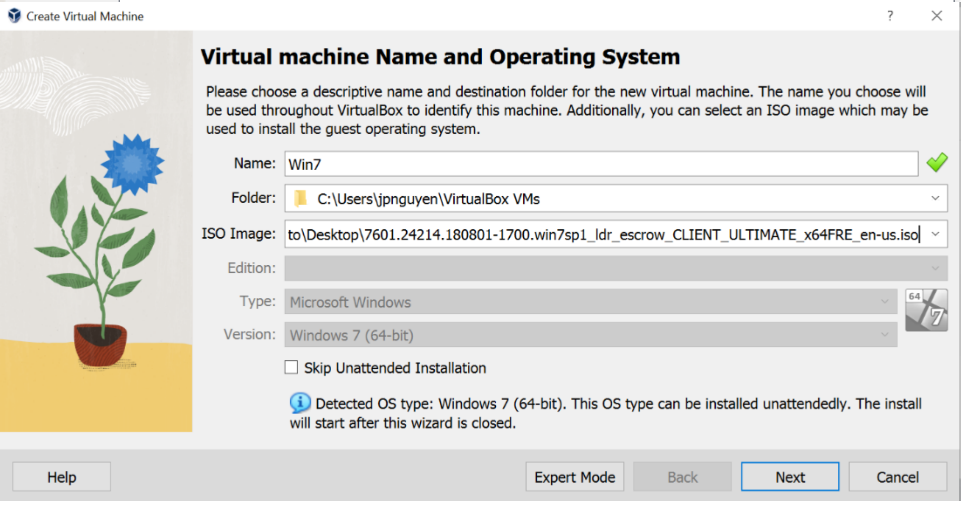
87,660 Views
74 Favorites
5 Reviews

DOWNLOAD OPTIONS
ISO IMAGE 1 file
ITEM TILE 1 file
PNG 1 file
TORRENT 1 file

2. In VirtualBox, click New to create a new virtual machine and use the ISO image we just downloaded. Then click Next.







Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Win7

Folder: C:\Users\jpnguyen\VirtualBox VMs

ISO Image: to\Desktop\7601.24214.180801-1700.win7sp1_ldr_escrow_CLIENT_ULTIMATE_x64FRE_en-us.iso

Edition:

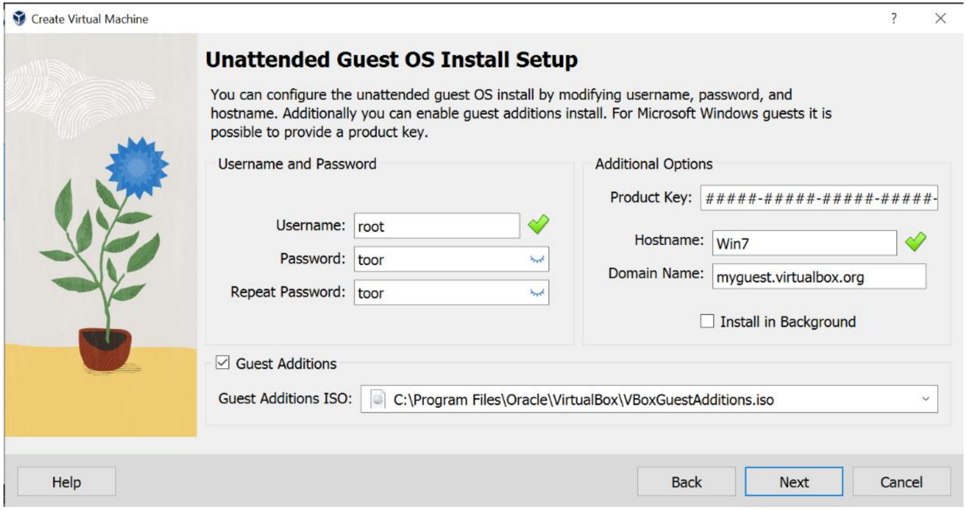
Type: Microsoft Windows

Version: Windows 7 (64-bit)

□ Skip Unattended Installation

Detected OS type: Windows 7 (64-bit). This OS type can be installed unattendedly. The install will start after this wizard is closed.

3. Choose any username and password. Then check the “Guest Additions” box



Unattended Guest OS Install Setup

You can configure the unattended guest OS install by modifying username, password, and hostname. Additionally you can enable guest additions install. For Microsoft Windows guests it is possible to provide a product key.

Username and Password

Username: root

Password: toor

Repeat Password: toor

Additional Options

Product Key: #####-#####-#####-#####-

Hostname: Win7

Domain Name: myguest.virtualbox.org

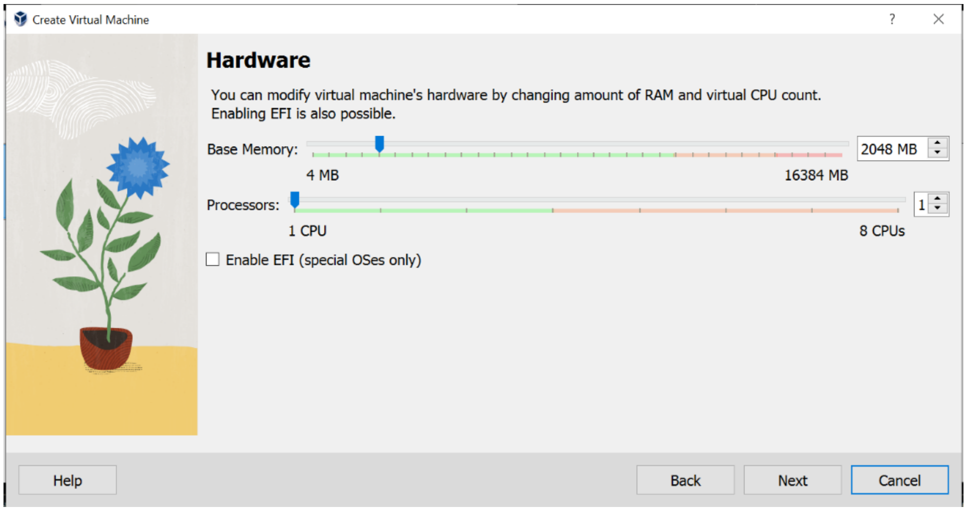
□ Install in Background

☑ Guest Additions

Guest Additions ISO: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso

4. Keep the default 2048 mb and click Next.

(Note: the prepared virtual machine also uses 2048mb)



Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB

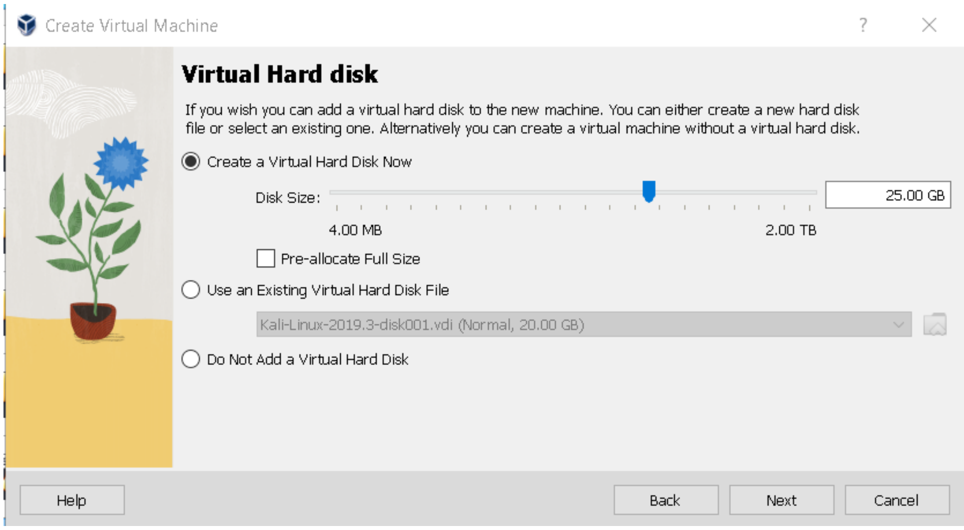
4 MB 16384 MB

Processors: 1

1 CPU 8 CPUs

□ Enable EFI (special OSes only)

5. For the virtual hard disk, the default is 32GB but to save space you can use 25GB instead.



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 25.00 GB

4.00 MB — 2.00 TB

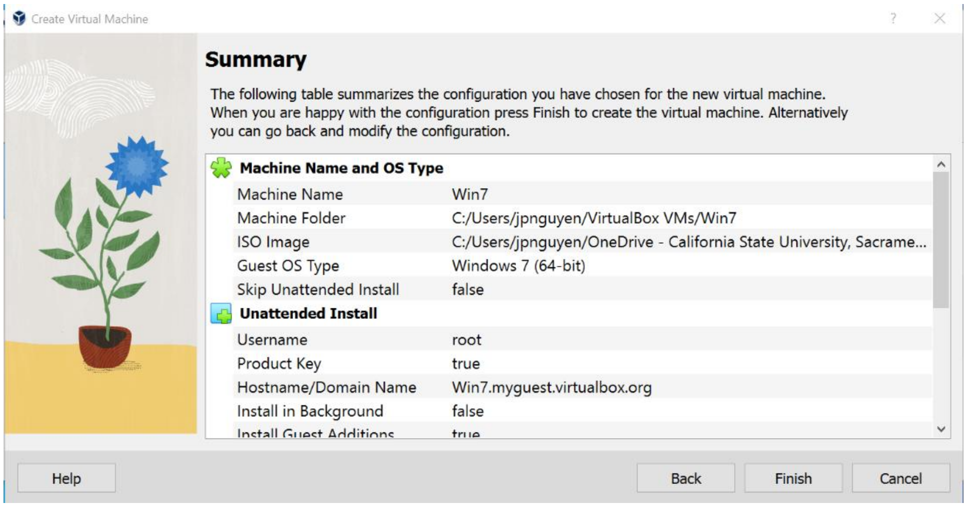
□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

Kali-Linux-2019.3-disk001.vdi (Normal, 20.00 GB)

○ Do Not Add a Virtual Hard Disk

6. Click Finish

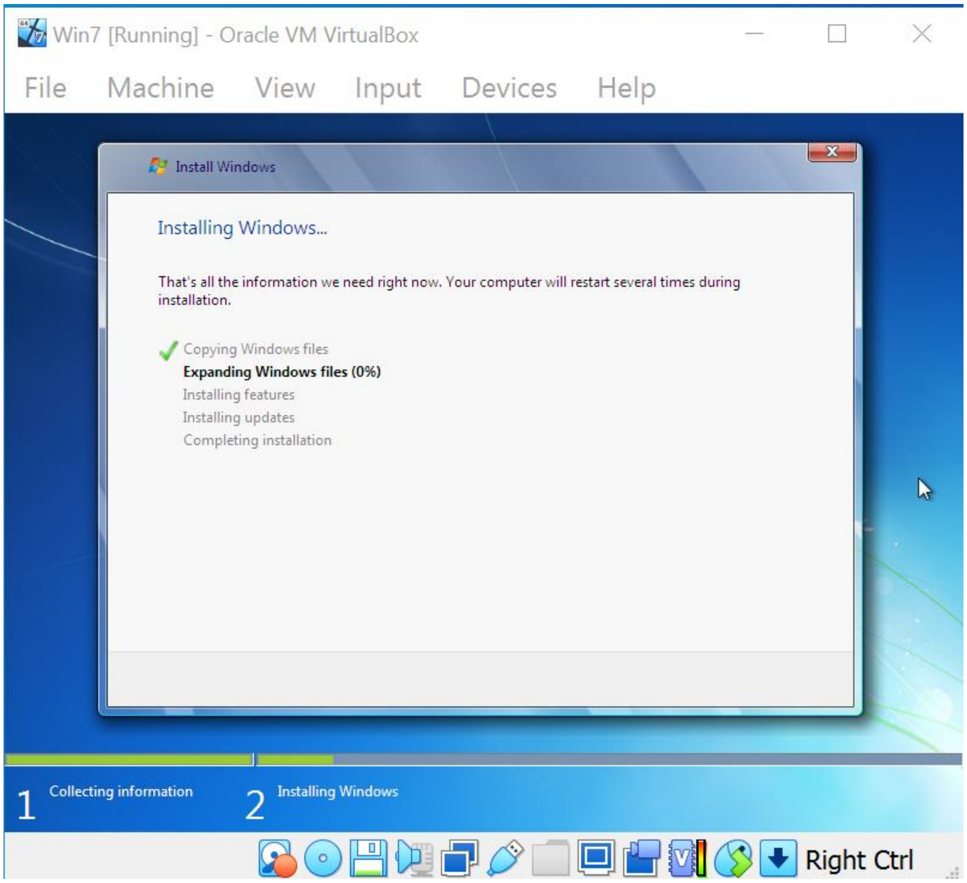


Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	Win7
Machine Folder	C:/Users/jpnguyen/VirtualBox VMs/Win7
ISO Image	C:/Users/jpnguyen/OneDrive - California State University, Sacrame...
Guest OS Type	Windows 7 (64-bit)
Skip Unattended Install	false
Unattended Install	
Username	root
Product Key	true
Hostname/Domain Name	Win7.myguest.virtualbox.org
Install in Background	false
Install Guest Additions	true

7. The virtual machine will automatically install Windows on start up.

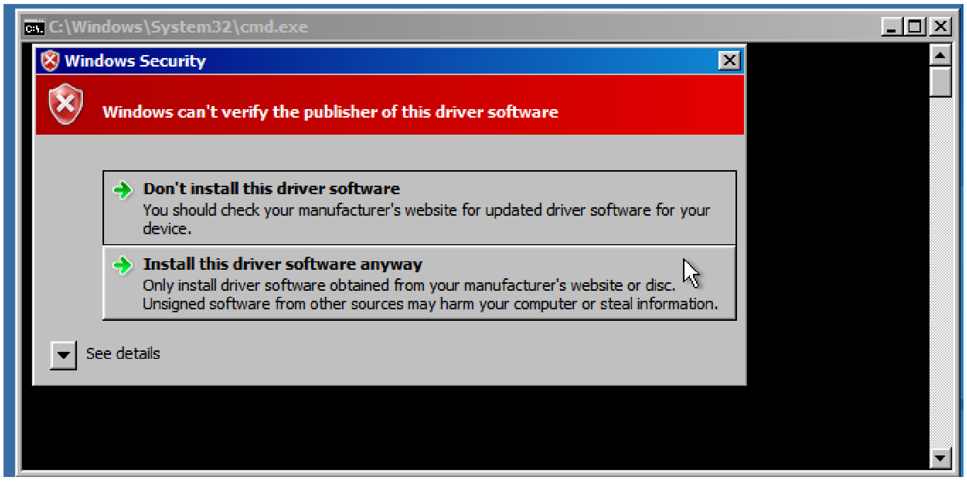


Installing Windows...

That's all the information we need right now. Your computer will restart several times during installation.

✓ Copying Windows files
Expanding Windows files (0%)
Installing features
Installing updates
Completing installation

8. If you receive this popup, click “Install this driver software anyway”

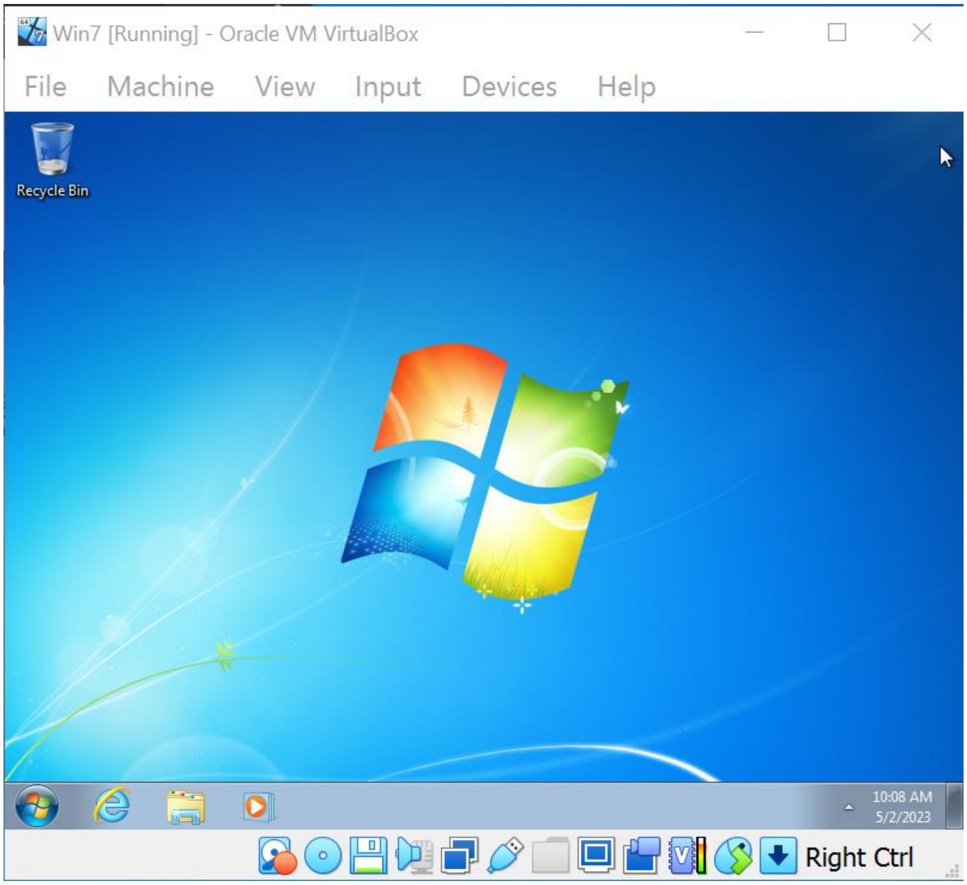


Windows can't verify the publisher of this driver software

Don't install this driver software
You should check your manufacturer's website for updated driver software for your device.

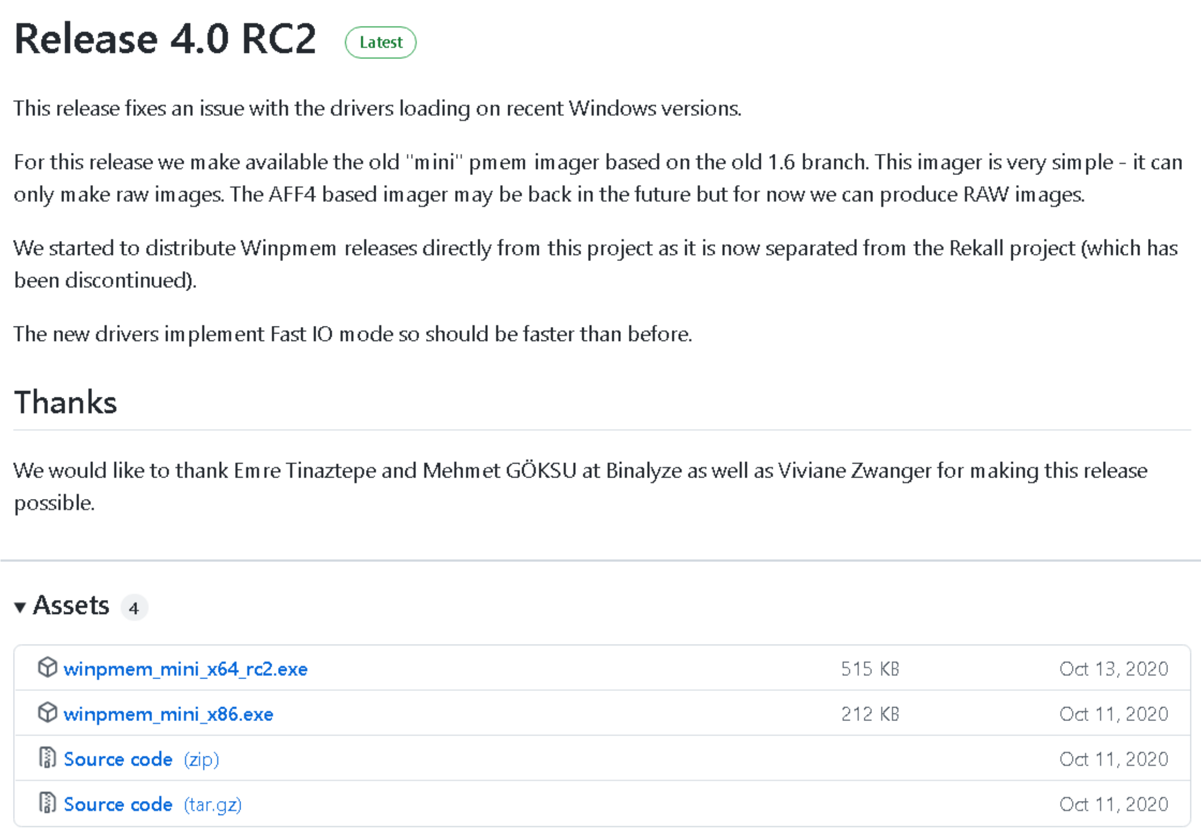
Install this driver software anyway
Only install driver software obtained from your manufacturer's website or disc. Unsigned software from other sources may harm your computer or steal information.

9. When it’s done, the virtual machine should be ready to use.



Task 1. Download WinPMem from Github

1. The github page can be found here:
https://github.com/Velocidex/WinPmem
The download page can be found here:
https://github.com/Velocidex/WinPmem/releases



Release 4.0 RC2

This release fixes an issue with the drivers loading on recent Windows versions.

For this release we make available the old "mini" pmem imager based on the old 1.6 branch. This imager is very simple - it can only make raw images. The AFF4 based imager may be back in the future but for now we can produce RAW images.

We started to distribute Winpmem releases directly from this project as it is now separated from the Rekall project (which has been discontinued).

The new drivers implement Fast IO mode so should be faster than before.

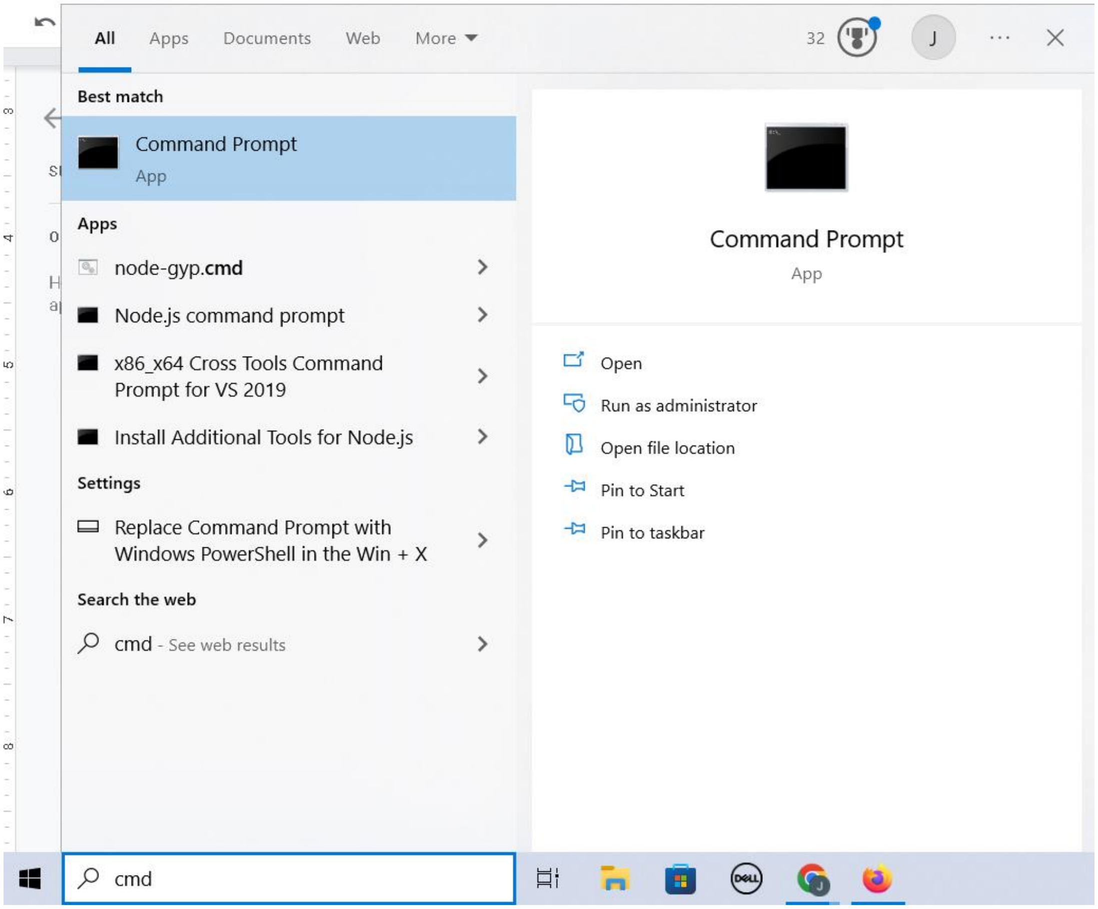
Thanks

We would like to thank Emre Tinaztepe and Mehmet GÖKSU at Binalyze as well as Viviane Zwanger for making this release possible.

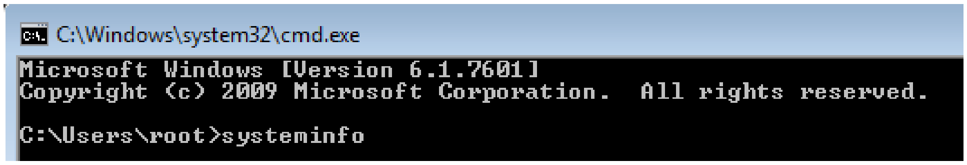
▾ Assets 4

winpmem_mini_x64_rc2.exe	515 KB	Oct 13, 2020
winpmem_mini_x86.exe	212 KB	Oct 11, 2020
Source code (zip)		Oct 11, 2020
Source code (tar.gz)		Oct 11, 2020

2. **(OPTIONAL, skip to step 5 if you know your PC's system type)** If you are not sure what system type your computer is, you can click the Windows icon on the task bar and type "cmd" or "command prompt"

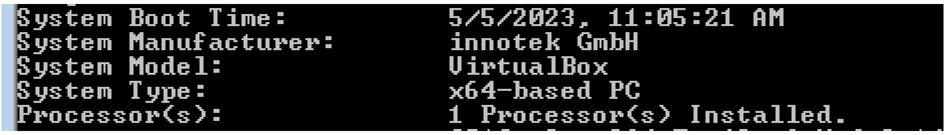


3. Now type in "systeminfo"



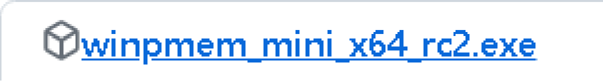
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\root>systeminfo
```

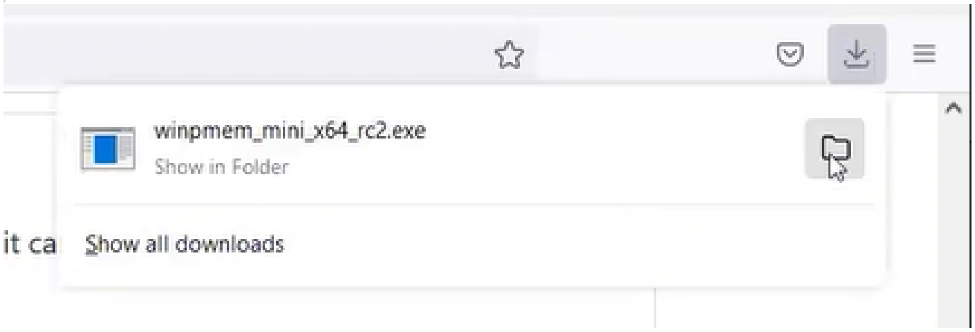
4. Scroll through the info until you find “System type” and it will show which version of windows you have.



```
System Boot Time:          5/5/2023, 11:05:21 AM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
```

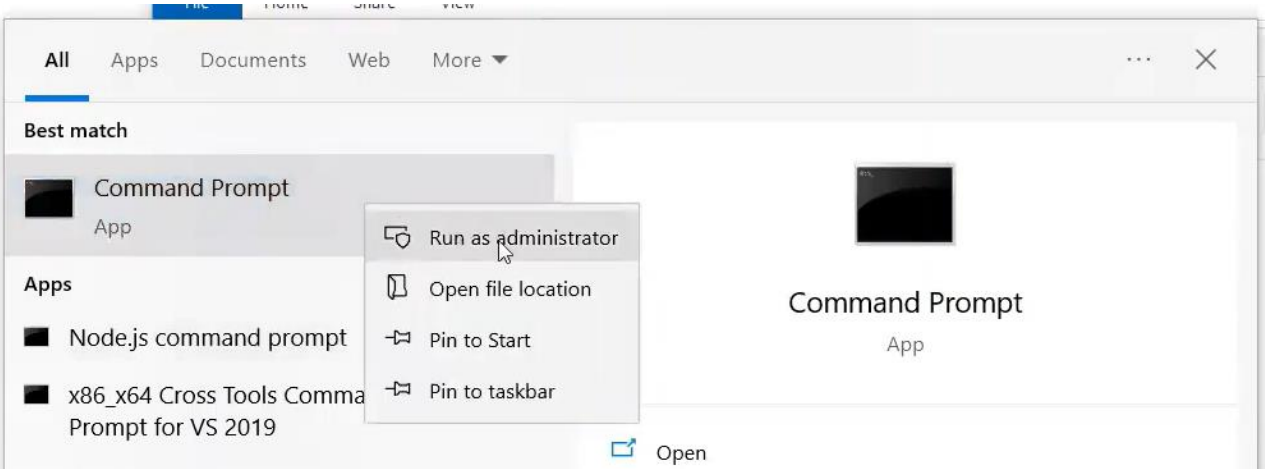
5. Download the correct version of WinPMem by clicking the appropriate version on the github downloads page



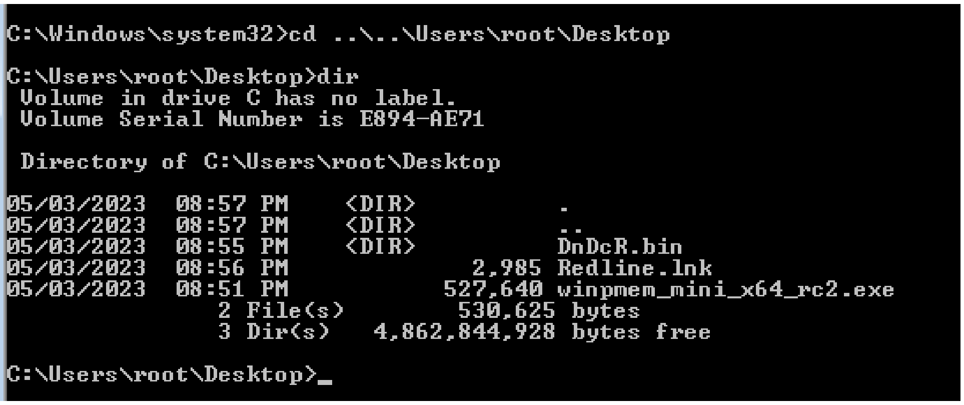


Task 2. Run WinPMem in the command line

6. Open the command prompt by right clicking it and clicking “Run as administrator”



7. Now navigate to the directory you have WinPMem in by using the cd command.
Your commands may look different since you might have a different username and path.



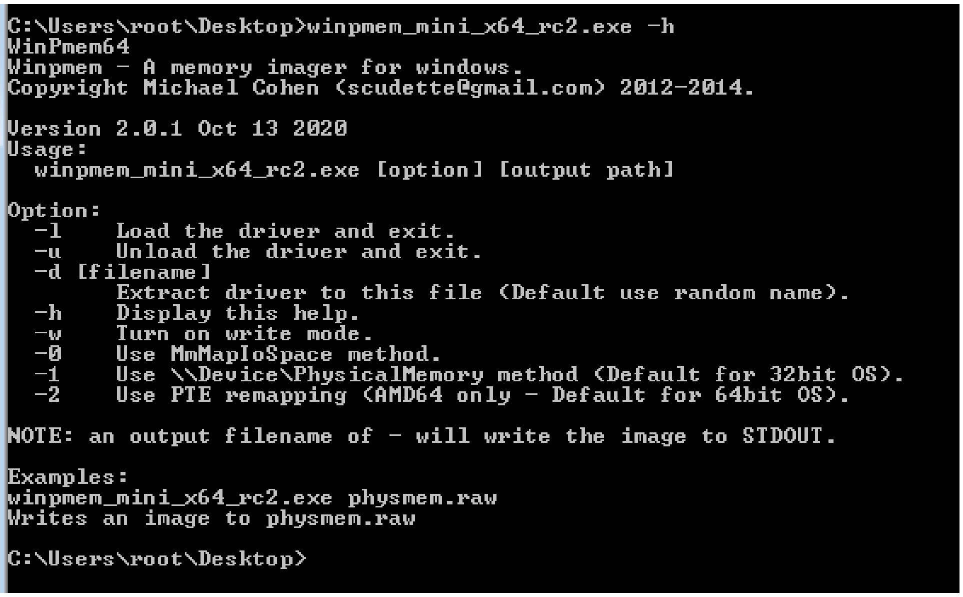
```
C:\Windows\system32>cd ..\..\Users\root\Desktop

C:\Users\root\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is E894-AE71

 Directory of C:\Users\root\Desktop

05/03/2023  08:57 PM    <DIR>          .
05/03/2023  08:57 PM    <DIR>          ..
05/03/2023  08:55 PM    <DIR>          DnDcR.bin
05/03/2023  08:56 PM             2,985 Redline.lnk
05/03/2023  08:51 PM           527,640 winpmem_mini_x64_rc2.exe
               2 File(s)        530,625 bytes
               3 Dir(s)   4,862,844,928 bytes free

C:\Users\root\Desktop>_
```

(If you are unsure of WinPMem's location, you can right click WinPMem and select Properties to see the location)

8. Type the name of the file you downloaded with the -h argument. In this screenshot, the x64 version was used, so this is the command that was typed:

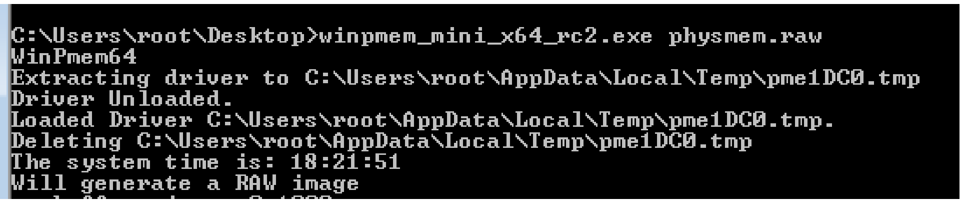
winpmem_mini_x64_rc2.exe -h

At the bottom of the information, you will see an example of how to write an image to physmem.raw.

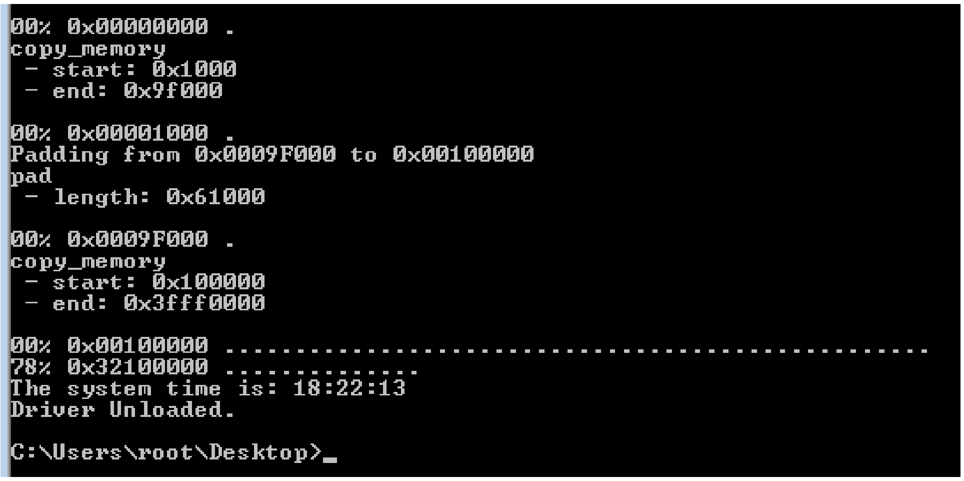


```
C:\Users\root\Desktop>winpmem_mini_x64_rc2.exe -h
WinPmem64
Winpmem - A memory imager for windows.
Copyright Michael Cohen (scudette@gmail.com) 2012-2014.

Version 2.0.1 Oct 13 2020
Usage:
  winpmem_mini_x64_rc2.exe [option] [output path]

Option:
  -l    Load the driver and exit.
  -u    Unload the driver and exit.
  -d [filename]
        Extract driver to this file (Default use random name).
  -h    Display this help.
  -w    Turn on write mode.
  -0    Use MmMapIoSpace method.
  -1    Use \\Device\PhysicalMemory method (Default for 32bit OS).
  -2    Use PTE remapping (AMD64 only - Default for 64bit OS).

NOTE: an output filename of - will write the image to STDOUT.

Examples:
winpmem_mini_x64_rc2.exe physmem.raw
Writes an image to physmem.raw

C:\Users\root\Desktop>
```

9. Using the information found by using the –h argument, write an image to a raw file. The following screenshot shows the command "winpmem_mini_x64_rc2.exe physmem.raw" being used to start winpmem. This step may take awhile to load.

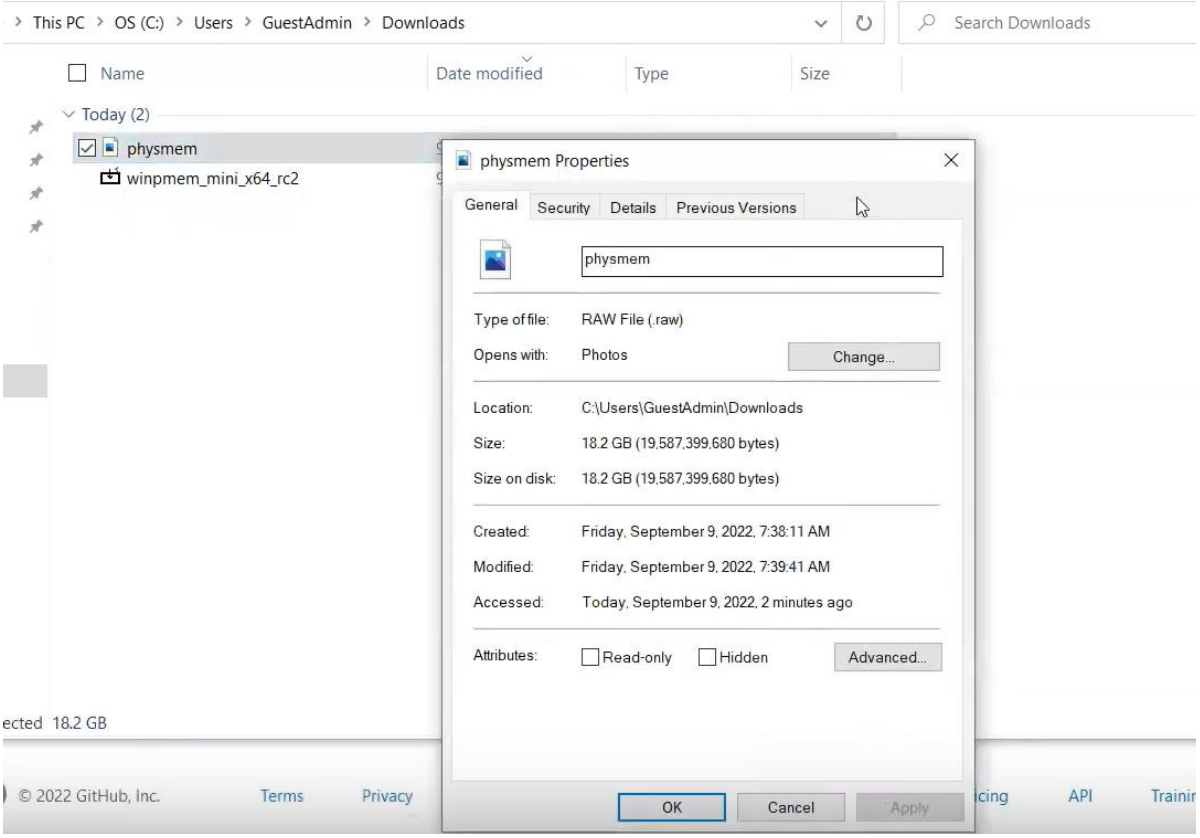


```
C:\Users\root\Desktop>winpmem_mini_x64_rc2.exe physmem.raw
WinPmem64
Extracting driver to C:\Users\root\AppData\Local\Temp\pme1DC0.tmp
Driver Unloaded.
Loaded Driver C:\Users\root\AppData\Local\Temp\pme1DC0.tmp.
Deleting C:\Users\root\AppData\Local\Temp\pme1DC0.tmp
The system time is: 18:21:51
Will generate a RAW image
```



```
00% 0x00000000 .
copy_memory
 - start: 0x1000
 - end: 0x9f000

00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
pad
 - length: 0x61000

00% 0x0009F000 .
copy_memory
 - start: 0x100000
 - end: 0x3fff0000

00% 0x00100000 ..................................................
78% 0x32100000 ..............
The system time is: 18:22:13
Driver Unloaded.

C:\Users\root\Desktop>_
```

10. Now we can see the .raw file in the same location that we had WinPMem in. Right click the file and click properties to see information on your memory dump, such as the size.



physmem

Type of file: RAW File (.raw)

Opens with: Photos

Location: C:\Users\GuestAdmin\Downloads

Size: 18.2 GB (19,587,399,680 bytes)

Size on disk: 18.2 GB (19,587,399,680 bytes)

Created: Friday, September 9, 2022, 7:38:11 AM

Modified: Friday, September 9, 2022, 7:39:41 AM

Accessed: Today, September 9, 2022, 2 minutes ago

Attributes: □ Read-only □ Hidden

Questions:

1. Provide a screenshot of step 10 to prove that you have used WinPMem. Compare the size of the memory dump to the size of the ram we used in Task 0, step 4.

2. What does the –h argument do?

3. Explore the github page of WinPMem (linked in Task 1) and read the information provided. How many different independent methods are there to create a memory dump?

4. How would you change the command "winpmem_mini_x64_rc2.exe physmem.raw" to make a raw file called "clean.raw"?

5. What argument would you use in the command line to turn on write mode for WinPMem?

Deliverable:

Explicitly answer all questions above one by one. Provide screenshots as necessary. You will be evaluated based on the correctness, completeness, clarity and quality of English writing.