Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Windows Dead Analysis

DFIR-06-L1
PowerForensics

Lab Objective

Learn how to retrieve information from a raw image file taken from a compromised system.

Lab Mission

Investigate the raw image content using PowerForensics to determine where an attack originated.

Lab Duration

15–25 minutes

Requirements

- Knowledge of PowerShell scripting
- Basic knowledge of PowerForensics

Resources

- Environment & Tools
    - VirtualBox
        - Windows 10
            - OSFMount
- Extra Lab Files
    - ***Windows Dead Analysis OVA***

Textbook References

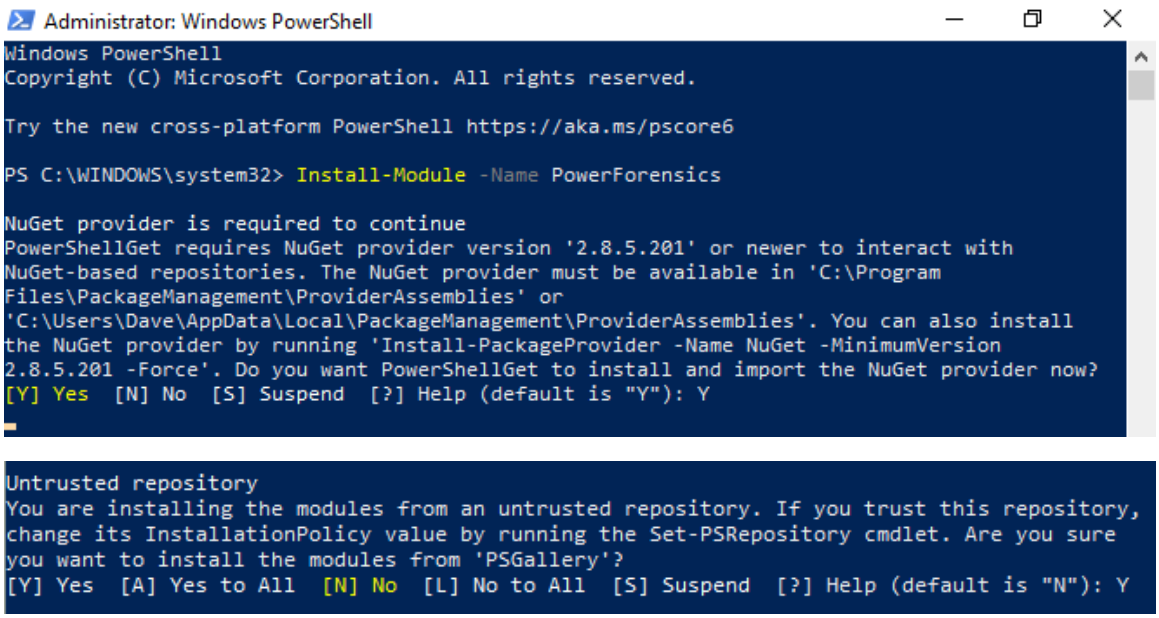
- Chapter 6: Windows Dead Analysis
    - Section 1: PowerForensics

Lab Task: Investigate to Find the Source of an Attack

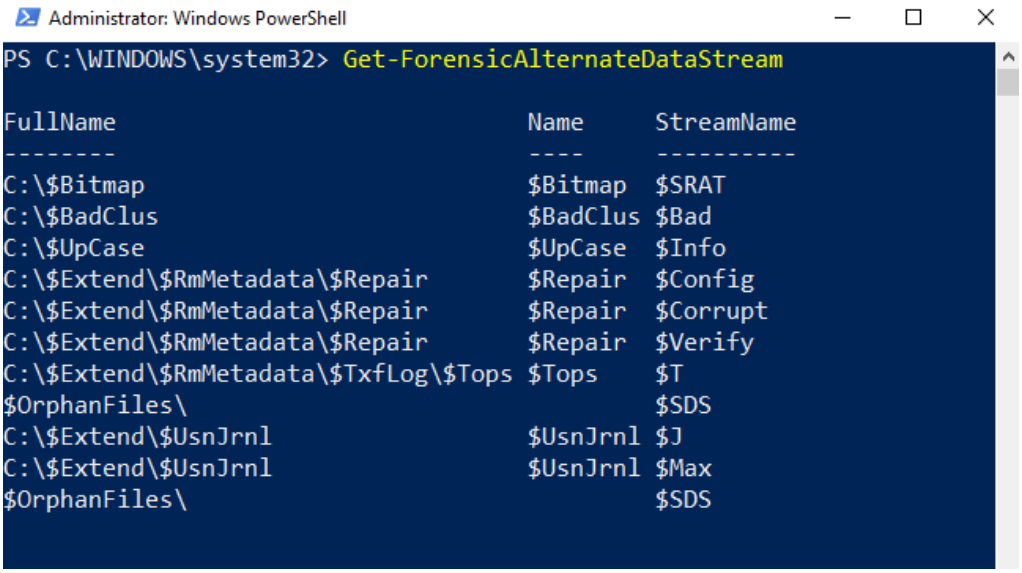
Investigate the raw image using PowerForensics to find the source of the attack.

Note: All lab files are in the ***Windows Dead Analysis OVA***.

1. Import the ***Windows Dead Analysis OVA*** into VirtualBox and start it.
2. Use the provided OVA to initiate the Windows station and start the machine.
3. Extract the ***PowerForensics.zip*** file to the desktop to install the PowerForensics module with PowerShell in administrative mode. Use the command ***Install-Module -Name PowerForensics*** to start the module's installation and Type **Y** when prompted to install NuGet.

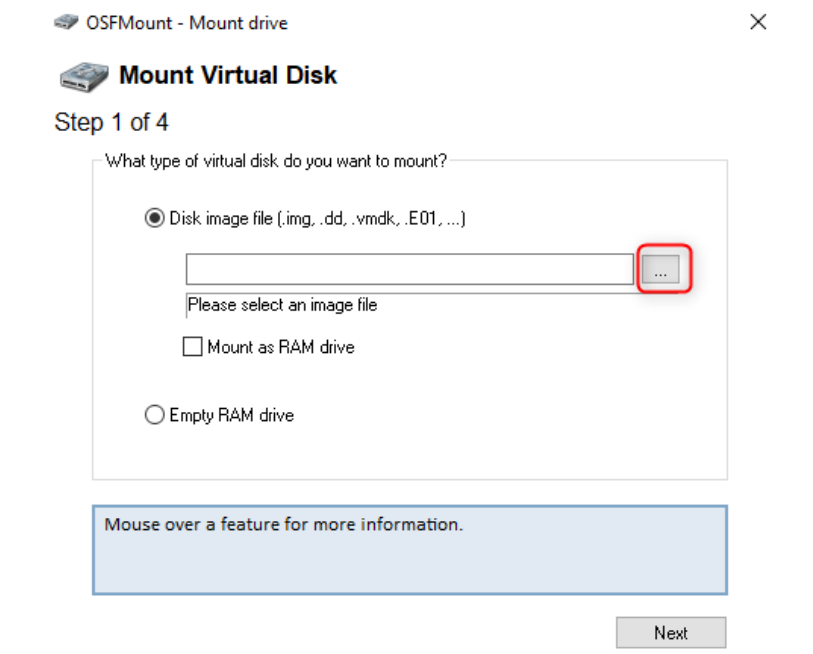


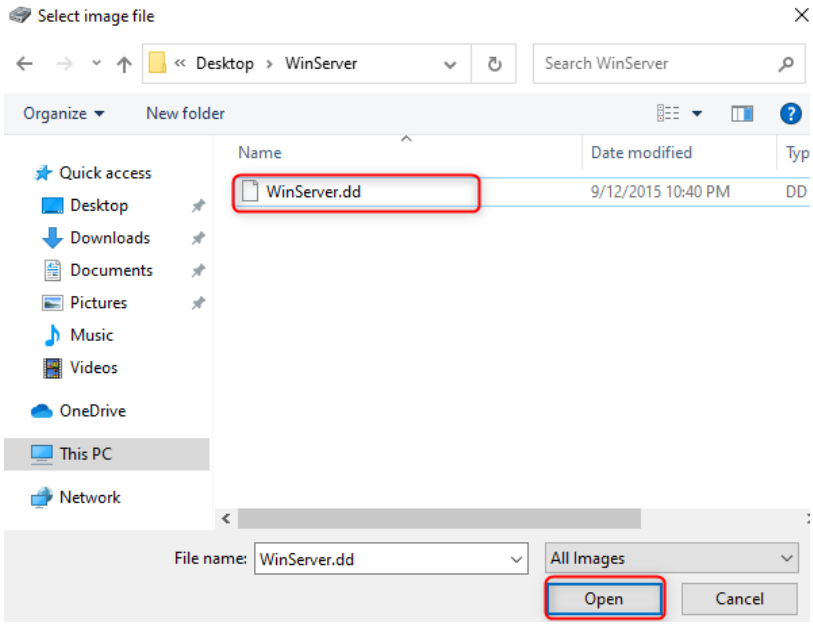
4 Use the command ***Get-ForensicAlternateDataStream*** to display alternate data stream objects with PowerForensics.



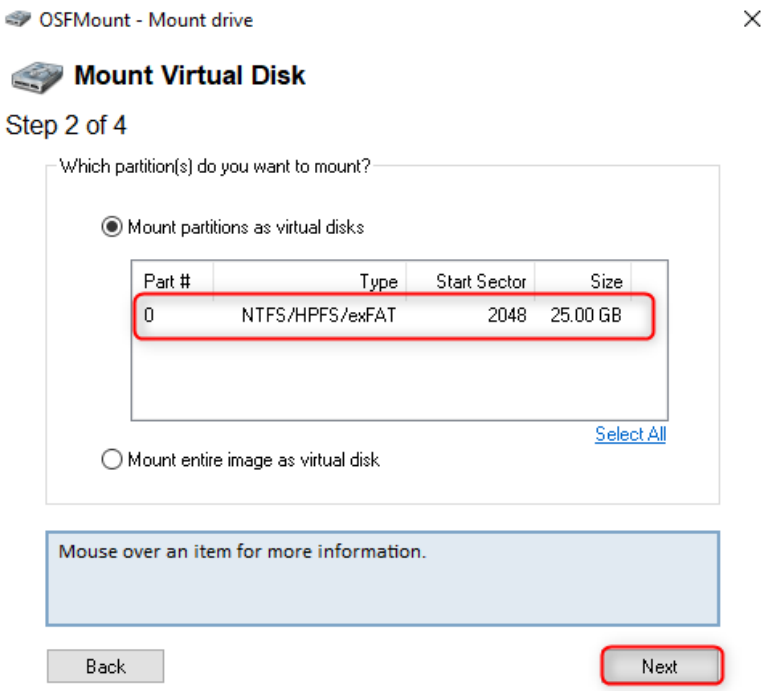
5 Extract ***WinServer.zip*** to the desktop and start the **OSFMount**.

6 Use **OSFMount** to view the ***WinServer.dd*** file by clicking **Mount new…** and selecting the ***WinServer.dd*** file. Then click **Next** to go to step 2 of 4.

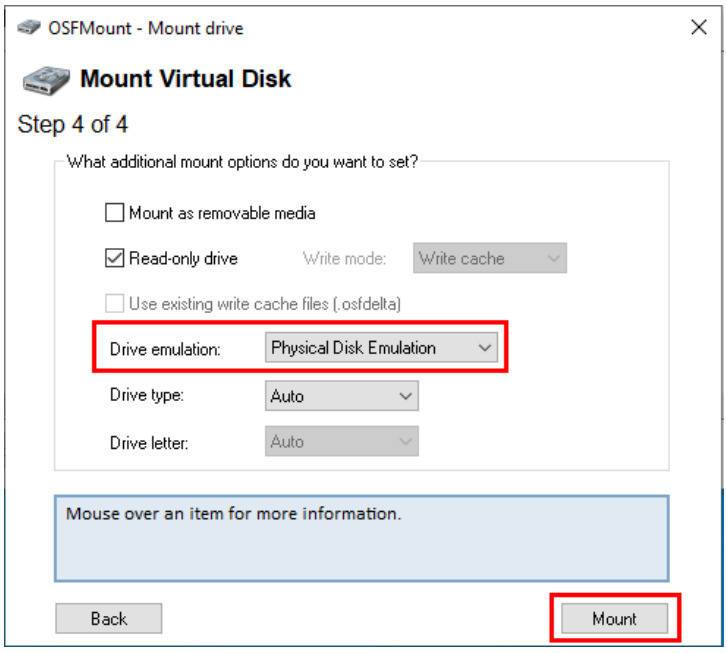

OSFMount - Mount drive
Mount Virtual Disk
Step 1 of 4
What type of virtual disk do you want to mount?
Disk image file (.img, .dd, .vmdk, .E01, ...)
...
Please select an image file
Mount as RAM drive
Empty RAM drive
Mouse over a feature for more information.
Next


Select image file
Desktop › WinServer
Search WinServer
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Typ
WinServer.dd
9/12/2015 10:40 PM
DD
File name: WinServer.dd
All Images
Open
Cancel

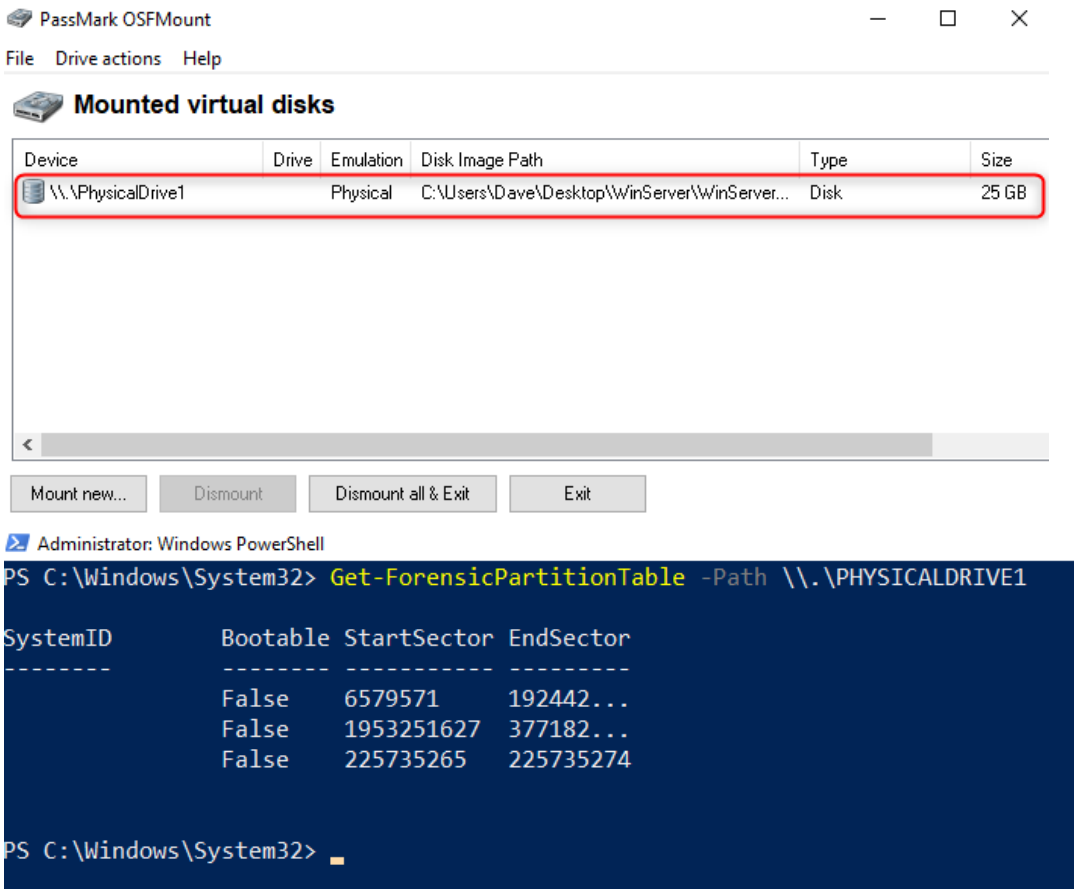
7 In step 2 of 4, be sure the ***Mount partitions as virtual disks*** option is selected and click **Next**.



8 In step 4 of 4, make sure ***Drive emulation*** is selected as ***Physical Disk Emulation***, then click **Mount**.

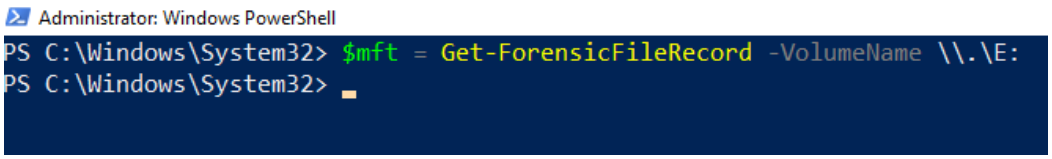


9 In PowerShell, run the command ***Get-ForensicPartitionTable -Path \\.\PHYSICALDRIVE1***

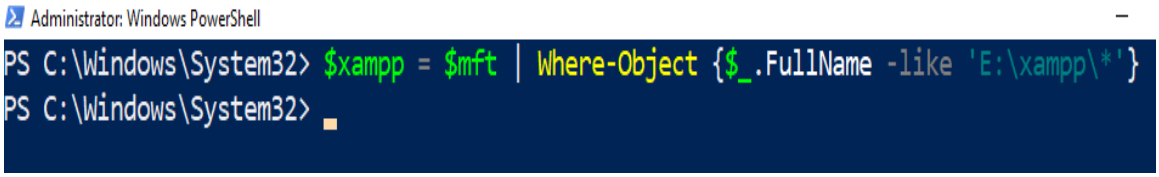


10 Use variable ***mft*** to save a list of the image's MFT file records. Use the command ***$mft = Get-ForensicFileRecord -VolumeName \\.\E:***

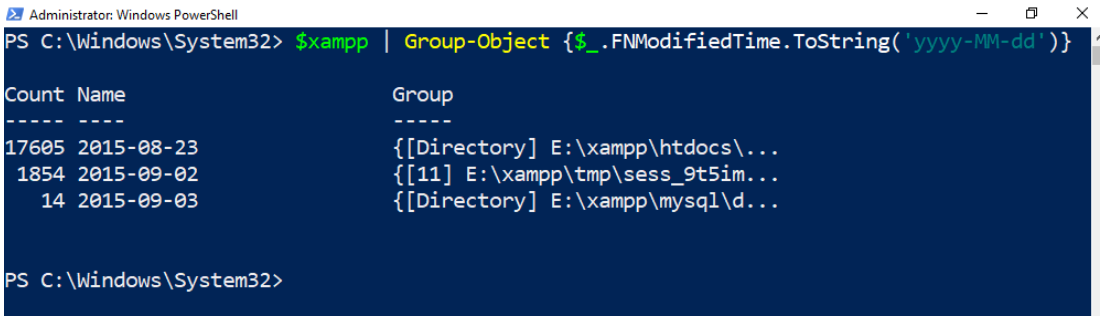
Note: Verify the variable with ***$mft[0]***



11 Save the MFT file records that belong to the ***xampp*** directory to a variable and print its count. Run ***$xampp = $mft | Where-Object {$_.Fullname -like 'E:\xampp*'}***



12 Group the files by their modification date and find the one with the most recent modifications. Use the ***powershell Group-Object*** function to run ***$xampp | Group-Object {$_.FNModifiedTime.ToString('yyyy-MM-dd')}***



13 Now filter the contents in the ***$xampp*** variable by the most recent modification, but this time, use the ***FNModifiedTime*** attribute and save it to a new variable. Run ***$xampp_filtered = $xampp | Where-Object {$_.FNModifiedTime.ToString('yyyy-MM-dd') -eq '2015-09-03'}***

Note: Verify the filter with ***$xampp_filtered[0]***

14 Utilize the ***Select-Object*** function to inspect the files using the two attributes found in the previous step, **FullName** and **FNModifiedTime**. The command is **$xampp_filtered | Select-Object Fullname, FNModifiedTime**

Note: The interesting files are appended with **.php**

15 Get the content of the suspicious files (***phpshell***) and find information on the source of the attack. Using the ***Get-ForensicContent*** with the ***-Path*** provided in the previous command. Ex.: ***Get-ForensicContent -Path E:\xampp\mysql\data\dvwa\db.opt***

16 One of the .php files should have revealed an IP address and port number.

Hints

Investigate to Find the Source of an Attack

- When importing the OVA, ensure the USB controller is unchecked.
- Install PowerForensics using PowerShell and the ***Install-Module*** command.
- Accept all the requests during the PowerForensics installation.
- Test the installation by typing **Get-Foren** and pressing the ***Tab*** key to auto-complete. If properly installed, PowerShell should auto-complete to ***Get-ForensicAlternateDataStream***
- After mounting, use ***Get-ForensicPartitiontable*** with a path to verify that data can be read from the image (DFIR Chapter 6).
- Initiate a variable from PowerShell with the ***$*** symbol ***($variable = data***).
- Filter data using object search methods, such as ***Where-Object***
  $filtered = $original | Where-Object {$_.FullName [comparison method] '[search term]'}
- Use the PowerShell ***Group-Object*** function to group objects within the array. For example, group by a date format using:
  $variable | Group-Object {$_.FNModifiedTime.ToString('yyyy-MM-dd')}
- Use ***Select-object*** to display specific files from an object:
  $variable | Select-Object [attribute1], [attribute2]