

Using PowerForensics to Perform Disk Analysis



Liam Cleary

Microsoft MVP and Microsoft Certified Trainer at SharePlicity

@helloitsliam | www.helloitsliam.com



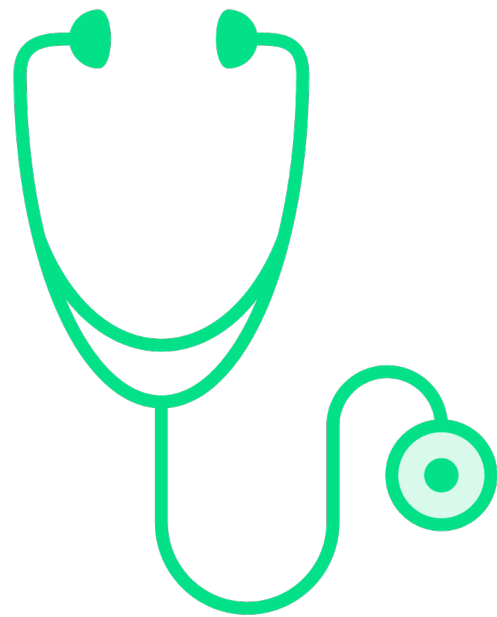
Overview

Goal: Utilize PowerForensics

- Understand disk forensics
- Review PowerForensics
- Install and import PowerForensics
- Performing hard disk forensics
- Creating a timeline using PowerForensics



Live Response and Forensics



Initial Triage

Retrieve System Information



Examination

Analyze disk storage for further evidence





Understand Disk Forensics



Disk Forensics

The process of analyzing contents of a computer's storage media, such as a hard drive or flash drive, to uncover evidence of criminal activity or other information of interest.



Purpose of Disk Forensics



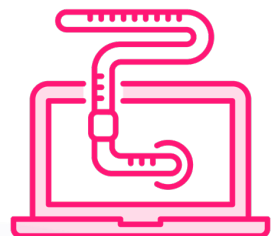
Criminal Investigations



Civil Litigation



Corporate Investigations



Cybersecurity Incident Response



Disk Forensic Steps



Imaging



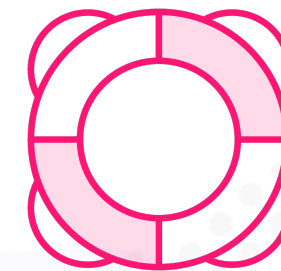
Analysis



Examination



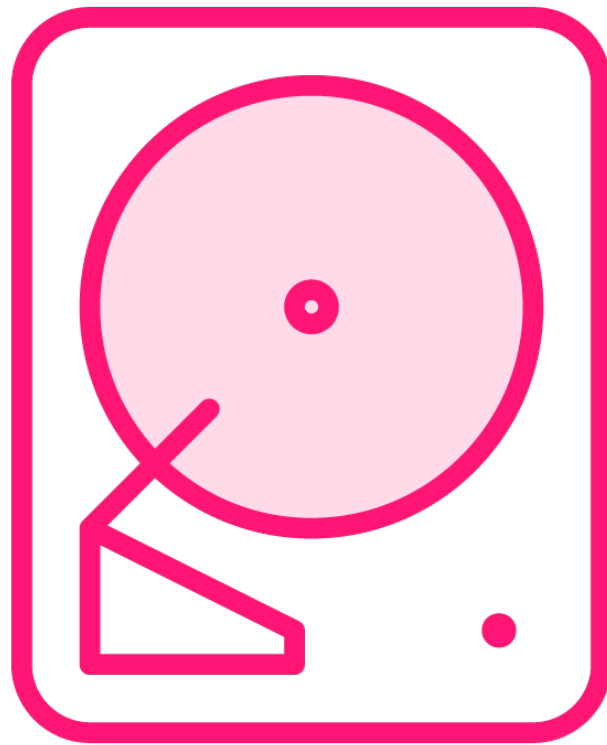
Reporting



Preservation



Disk Forensics



Data Clusters

Temporary Files

History Files

Unallocated Space

File Stack

Partition Information

Hidden Files





**1st rule of digital forensics is to always make a
clone of the original media**

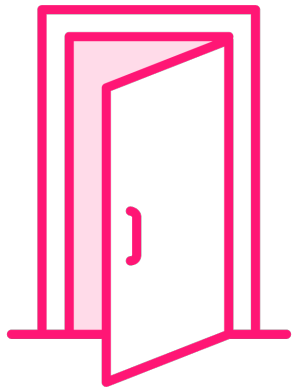




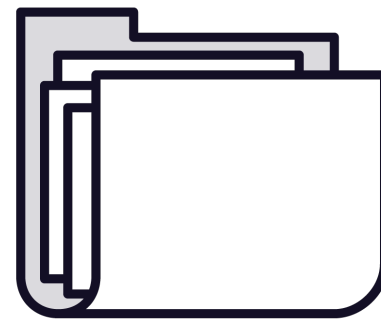
Review PowerForensics



PowerForensics



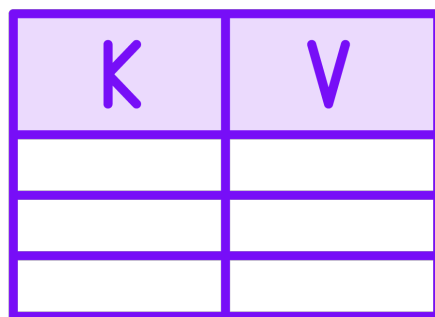
Free and Open-source



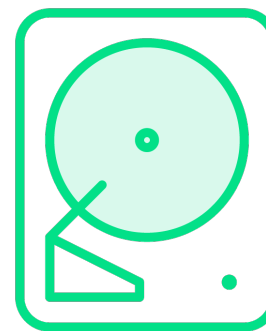
**Analyze Data from
Windows File Systems**



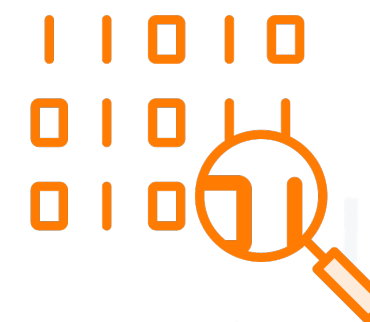
PowerShell Module



**Extract and Analyze File
Metadata**



Create Forensic Images



**Perform Forensic
Analysis**



PowerForensics Cmdlet Groups

1

File System

2

Windows Artifacts

3

**Application Compatibility
Cache**

4

Windows Registry

5

Forensic Timeline

6

Utilities



Install and Import PowerForensics



Installing PowerForensics



PowerShell Gallery



GitHub Download



Install PowerForensics

```
# Install PowerForensics
```

```
Install-Module PowerForensics
```

```
# Import PowerForensics
```

```
Import-Module PowerForensics
```

```
# Check the installation and import
```

```
Get-Command -Module PowerForensics
```



Installing PowerForensics from GitHub



Navigate to the GitHub repository

- <https://github.com/Invoke-IR/PowerForensics/releases>

Download the zip files

Extract the zip file into the "PSModulePath"

- C:\Program Files\WindowsPowerShell\Modules

Import the module

- Import-Module PowerForensics



Install PowerForensics

Import the PowerForensics Module

Test PowerForensics





Performing Hard Disk Forensics



Hard Disk Forensics Steps



Clone the hard disk



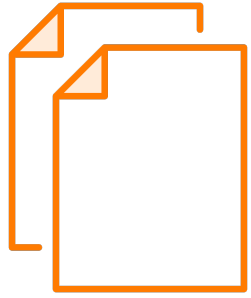
Mount the cloned hard disk



Execute forensic analysis



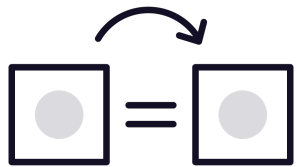
Example Disk Cloning Applications



Disk2vhd



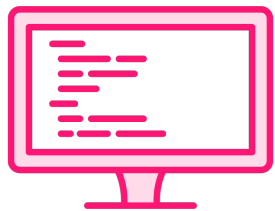
FTK Imager



OSFClone



EnCase



dd for Windows



KAPE



Example PowerForensics Commands

Retrieve deleted file records

```
Get-ForensicFileRecord -VolumeName F: | Where-Object { $_.Deleted }
```

Retrieve modified file records by date

```
Get-ForensicFileRecord -VolumeName F: | `
    Where-Object { $_.ModifiedTime -gt "01/25/2023 3:00:00 AM" }
```

Export the master file table (MFT)

```
$mft = Get-ForensicFileRecord -VolumeName F: -Index 0
$mft.CopyFile('.\Forensics\Evidence\Export.mft')
```

Retrieve Windows prefetch files

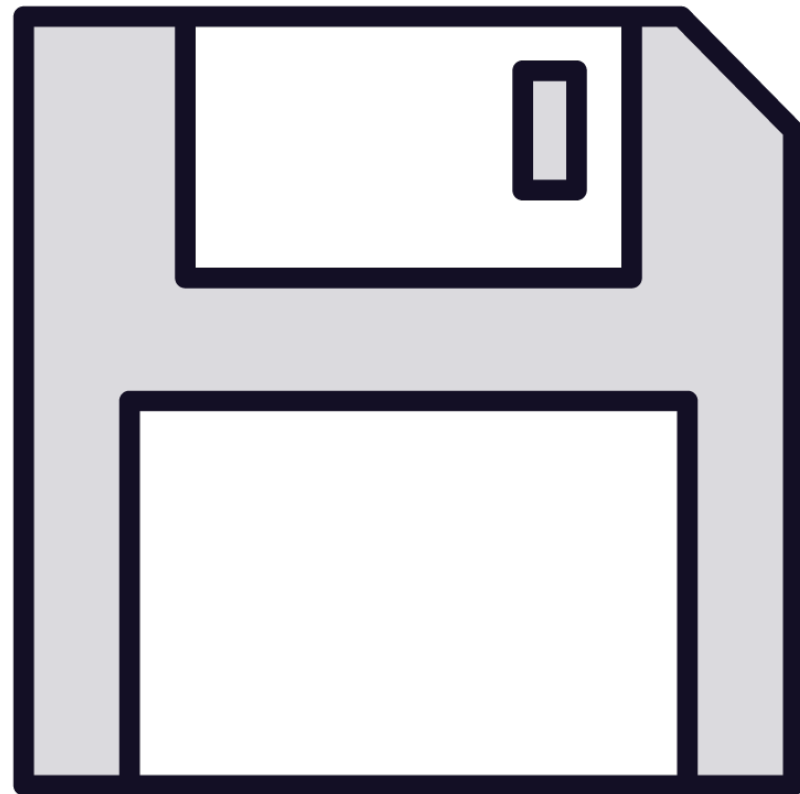
```
Get-ForensicPrefetch -VolumeName F:
```

Retrieve previously executed applications

```
Get-ForensicAmcache -VolumeName F:
```



Disk Forensic Timelines



Visual representation of the activity on a storage media over time

Created by analyzing the file system metadata and the file contents of a disk image

Identify and reconstruct events that occurred on a system

Provide information about the usage patterns of a system

Reveals identity of the users who performed actions



PowerForensics Timelines

Retrieve a forensic timeline

```
Get-ForensicTimeline -VolumeName F:
```

Retrieve a forensic timeline of activity for 'exe' files

```
Get-ForensicTimeline -VolumeName F: | Where-Object { $_.FileName -like '*.exe' }
```

Retrieve a forensic timeline grouped by source

```
Get-ForensicTimeline -VolumeName F: | `
    Group-Object -Property Source | `
    Format-Table Count, Name
```

Retrieve a forensic timeline using date range

```
Get-ForensicTimeline -VolumeName F: | `
    Where-Object {
        $_.Date -gt "01/01/2013 11:59:00 PM" -and
        $_.Date -lt "01/20/2013 11:59:00 PM" }
```



Perform Basic Disk Analysis using PowerForensics

- Export the master file table
- Filter the master file table
- Review deleted files
- Restore deleted files
- Perform general disk inspection
- Create a forensic timeline



Summary

Goal: Utilize PowerForensics

- Reviewed disk forensics
- Installed, imported, and executed some base PowerForensics commands
- Ran core PowerForensics commands to extract information such as deleted files
- Created a forensic timeline

