FPT University

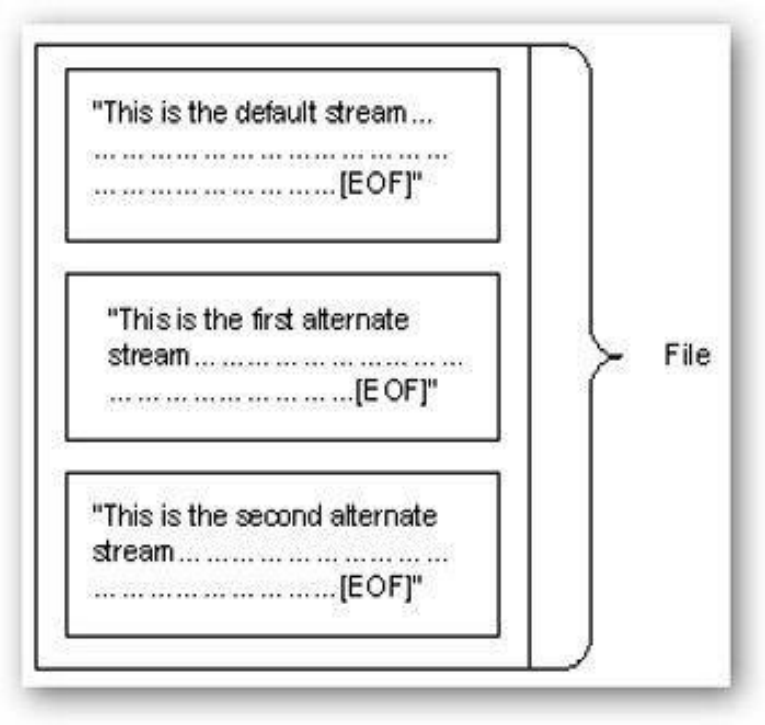
Lab 14: Using TSK for Network and Host

Because teaching teaches
teachers to teach

Alternate data streams (ADS)

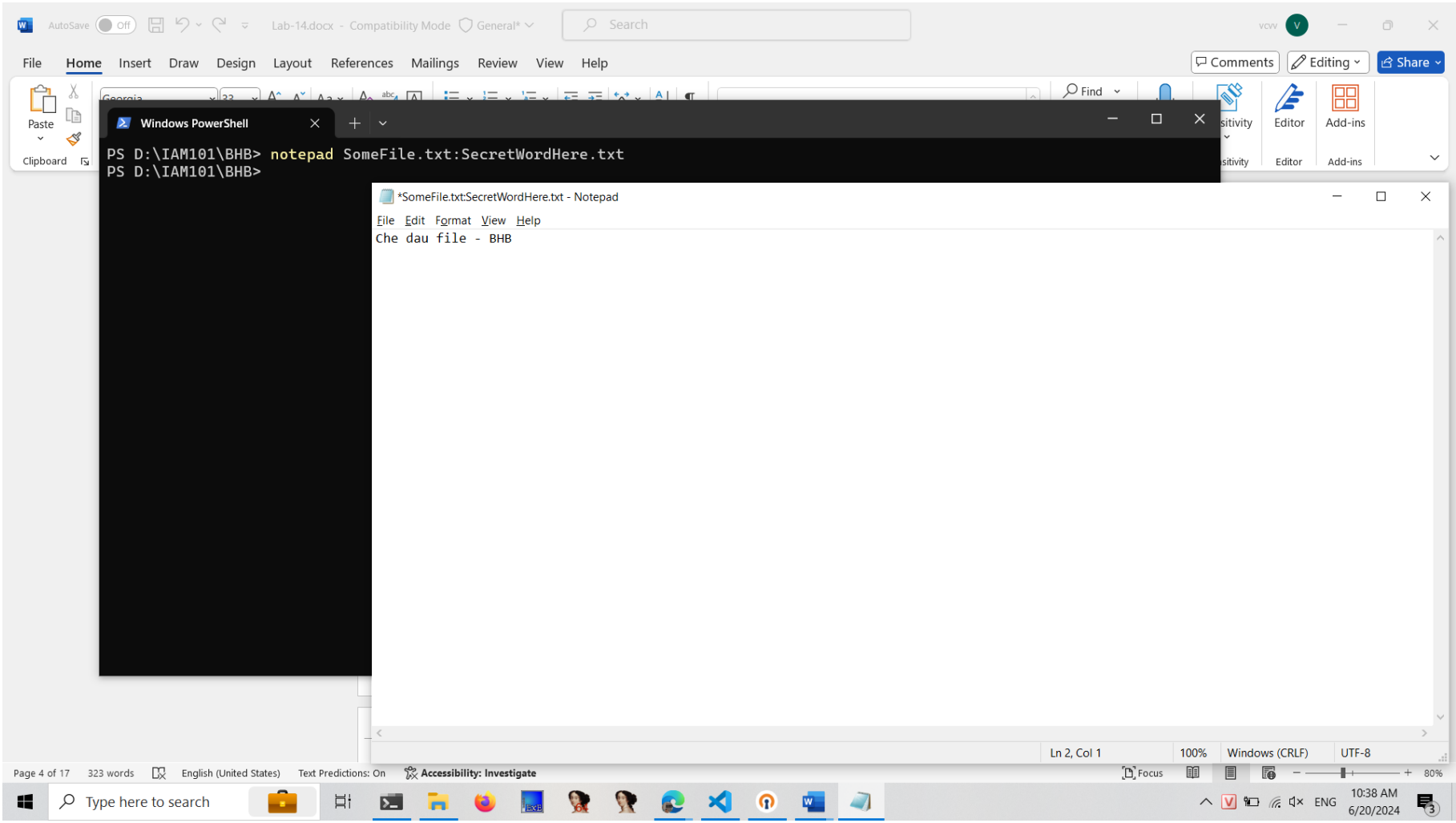
- Explorer and command-line directory listings (via cmd.exe) don't show data in ADS, so this allows malware to hide files from anyone who doesn't have special tools to view them.
- In this recipe, we'll discuss how those tools work and how you can leverage TSK to detect ADS on both live systems and mounted drives.

Alternate data streams (ADS)

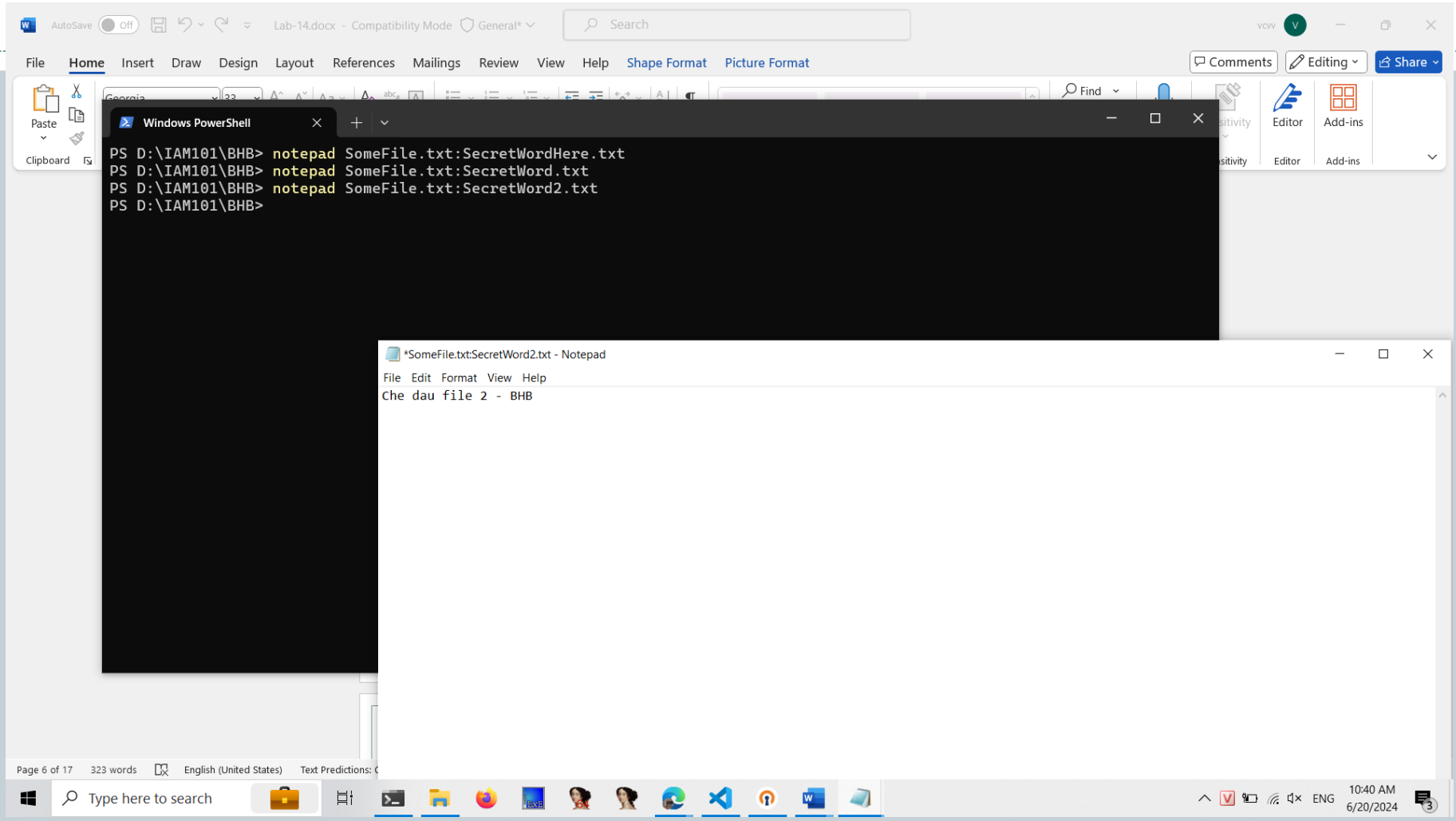


Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows.

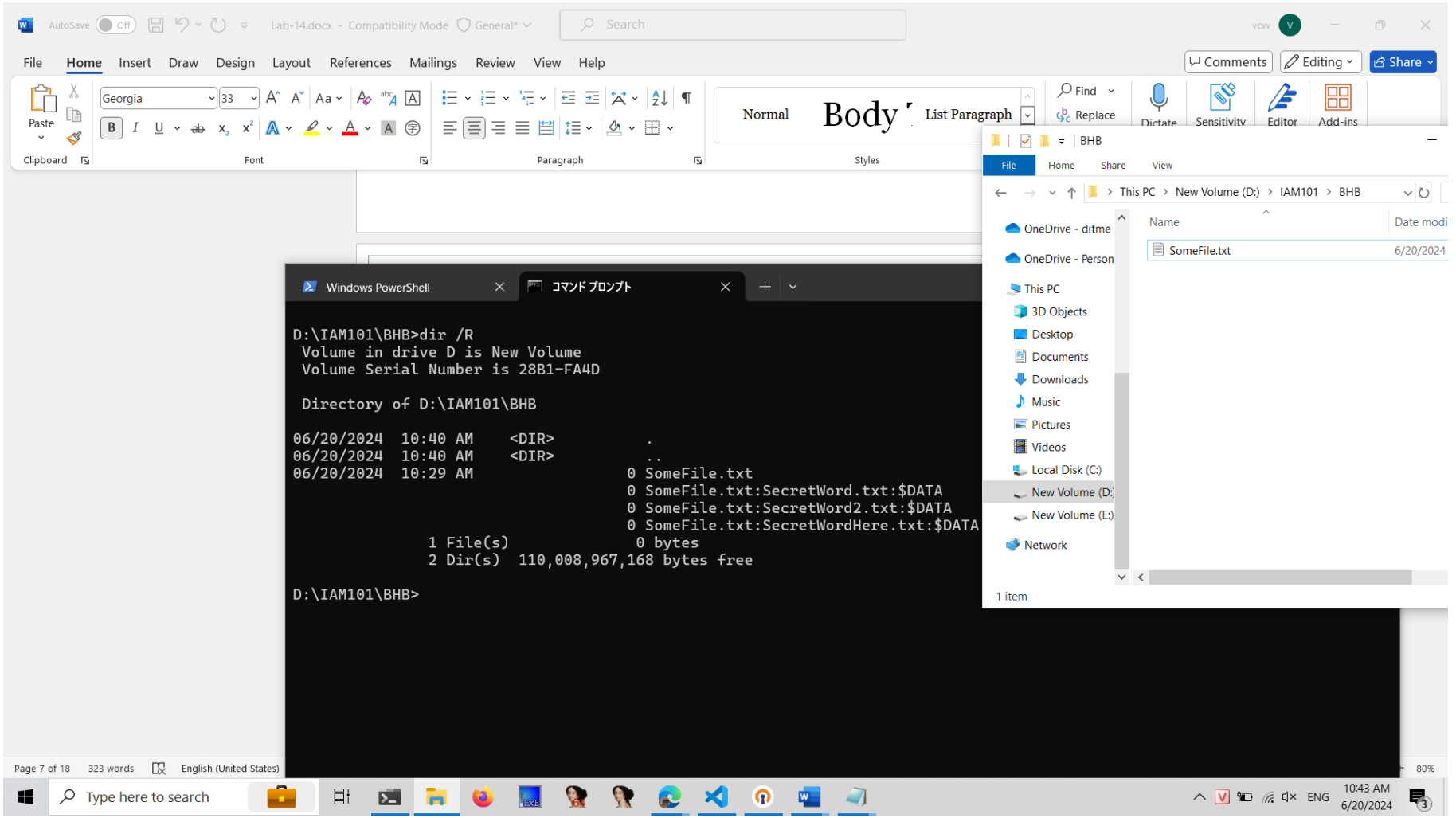
“Hide” data LEVEL 1



“Hide” data LEVEL 2



Detect “Hide” data



Why ADS is not good?

- Alternate Data Streams (ADS) have been given a bad reputation because their capability to hide data from us on our own computer, has been abused by malware writers in the past.

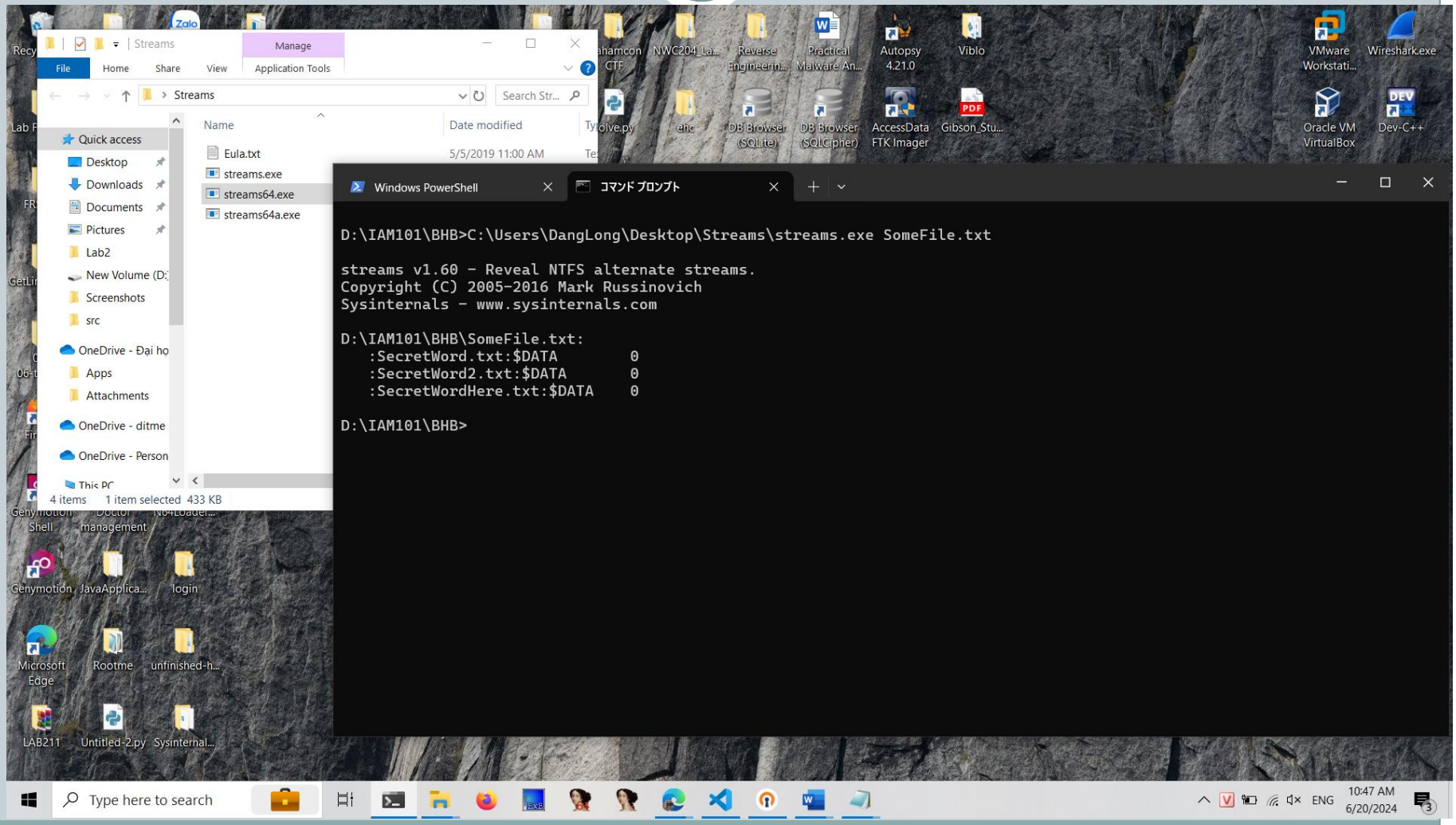
Using TSK or autospy

- To discovery ADS
- To detect hidden files

To discovery ADS

- lads.exe1 by Frank Heyne
- lns.exe2 by Arne Vidstrom
- sfind.exe3 by Foundstone
- streams.exe4 by Mark Russinovich

streams.exe


Streams
Manage
File
Home
Share
View
Application Tools
Search Str...
Quick access
Desktop
Downloads
Documents
Pictures
Lab2
New Volume (D:
Screenshots
src
OneDrive - Đại ho
Apps
Attachments
OneDrive - ditme
OneDrive - Person
Name
Date modified
Eula.txt
5/5/2019 11:00 AM
streams.exe
streams64.exe
streams64a.exe
4 items
1 item selected 433 KB
Windows PowerShell
コマンド プロンプト
D:\IAM101\BHB>C:\Users\DangLong\Desktop\Streams\streams.exe SomeFile.txt
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
D:\IAM101\BHB\SomeFile.txt:
:SecretWord.txt:$DATA 0
:SecretWord2.txt:$DATA 0
:SecretWordHere.txt:$DATA 0
D:\IAM101\BHB>
Type here to search
ENG
10:47 AM
6/20/2024

Analyzing the Master File Table (MFT) for ADS Info

- **mmls \\.\PhysicalDrive0**

```
C:\Users\DangLong>mmls \\.\PhysicalDrive0
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0000534527   0000532480   EFI system partition
005:  001       0000534528   0000567295   0000032768   Microsoft reserved partitio
006:  002       0000567296   0315140639   0314573344   Basic data partition
007:  -------   0315140640   0315142143   0000001504   Unallocated
008:  003       0315142144   0316276735   0001134592
009:  -------   0316276736   0316280831   0000004096   Unallocated
010:  004       0316280832   0664897535   0348616704   Basic data partition
011:  005       0664897536   0951617535   0286720000   Basic data partition
012:  -------   0951617536   0951619583   0000002048   Unallocated
013:  006       0951619584   0953667583   0002048000   Basic data partition
014:  007       0953667584   0999804927   0046137344   Basic data partition
015:  008       0999804928   1000214527   0000409600   Basic data partition
016:  -------   1000214528   1000215215   0000000688   Unallocated
```

Analyzing the Master File Table (MFT) for ADS Info

- **fls –o2048 -r -p \\.\PhysicalDrive0**

:SecretTwo.txt:$DATA 16
:SecretWord.txt:$DATA 18
:SecretWord2.txt:$DATA 0
:SecretWordHere.txt:$DATA 12

To detect Hidden Files

- Using tsk-xview.exe

```
C:\WINDOWS\system32>fls -o2048 -r -p \\.\PhysicalDrive0
r/r 3:  SYSTEM      (Volume Label Entry)
d/d * 5:        Tools
d/d 6:  EFI
d/d 20102:      EFI/Microsoft
d/d 20230:      EFI/Microsoft/Boot
d/d 20358:      EFI/Microsoft/Boot/bg-BG
r/r 20487:      EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r 20490:      EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 20496:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{b51167a0-f158-42ca-b6cc-82cf9993084e}
r/r * 20499:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r * 20505:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{1228734c-ecf3-476e-bd48-09b1faf524c1}
r/r * 20508:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 20514:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui.{6ab99604-1c83-43a9-8b17-9d9996a0929e}
r/r * 20517:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r * 20523:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{40928a0d-b9f3-4019-8bbd-207ee9db4f52}
r/r * 20526:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 20532:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui.{57d76562-a529-4dc0-bf87-235522e38fcc}
r/r * 20535:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r * 20541:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{89b6e265-0006-44a7-b8b3-f1520f83830b}
r/r * 20544:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 20550:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui.{cc4b06fc-101b-4d34-a39a-98554f17de6b}
r/r * 20553:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r * 20559:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{1d145e8b-2db3-47e1-9a7a-32ef80934954}
r/r * 20562:    EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 20568:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui.{ab1c1032-841d-4341-94b3-8a07bab6a08f}
r/r * 20571:    EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
```

To detect malware

- Eight timestamps:
  - 4 from the $STANDARD_INFORMATION Attribute (SIA)
  - 4 from the $FILE_
  - When malware uses SetFileTime to change the last access, last write, or creation time of a file, the change applies only to the timestamps in the SIA.NAME Attribute (FNA)

To detect malware

- Using tsk-xview.exe

```
raw_read: byte offset: 6160384 len: 65536
raw_read: found in image 0 relative offset: 6160384 len: 65536
raw_read: byte offset: 6225920 len: 65536
raw_read: found in image 0 relative offset: 6225920 len: 65536
raw_read: byte offset: 6291456 len: 65536
raw_read: found in image 0 relative offset: 6291456 len: 65536
raw_read: byte offset: 6356992 len: 65536
raw_read: found in image 0 relative offset: 6356992 len: 65536
raw_read: byte offset: 6422528 len: 65536
raw_read: found in image 0 relative offset: 6422528 len: 65536
raw_read: byte offset: 6488064 len: 65536
```

Q & A