



# *Lab 14: Using TSK for Network and Host*

*Because teaching teaches  
teachers to teach*

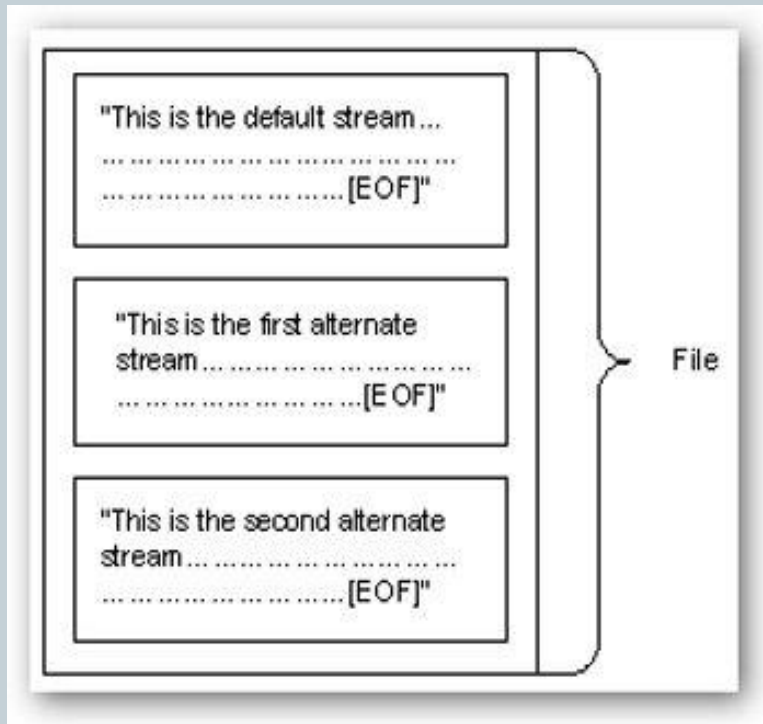
# *Alternate data streams (ADS)*

2

- 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)

3



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

4

Command Prompt

```
C:\Users\BHB>  
C:\Users\BHB>more < SomeFile.txt:SecretWordHere.txt  
banhabanfjfj  
  
C:\Users\BHB>notepad SomeFile.txt:SecretWord.txt
```

SomeFile.txt:SecretWord.txt - Notepad

File Edit Format View Help

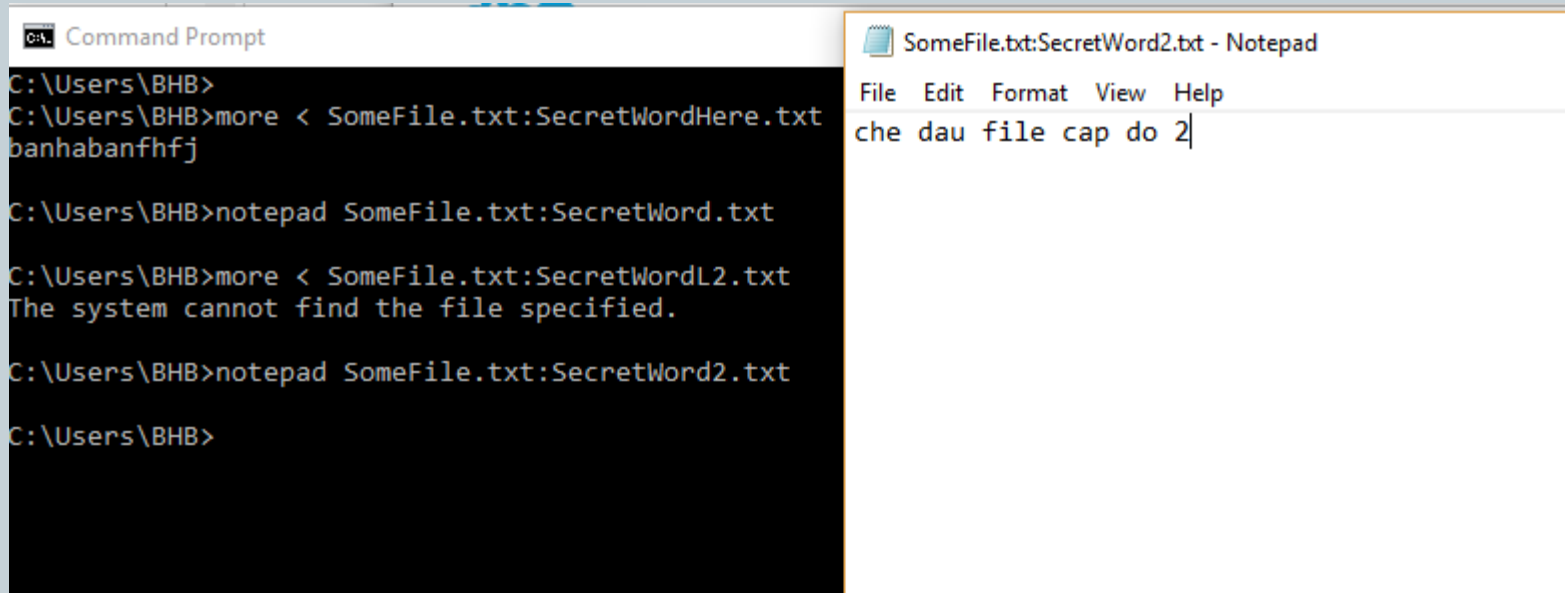
Che dau file - BHB

SomeFile.txt - Notepad

File Edit Format View Help

# “Hide” data LEVEL 2

5



The screenshot shows a Windows desktop with two windows. On the left is a 'Command Prompt' window with a black background and white text. It shows the user 'BHB' at the 'C:\Users\BHB' directory. The user has entered three commands: 1) 'more < SomeFile.txt:SecretWordHere.txt' which outputs 'banhabanfhfj'; 2) 'notepad SomeFile.txt:SecretWord.txt'; and 3) 'more < SomeFile.txt:SecretWordL2.txt' which results in an error message 'The system cannot find the file specified.'. On the right is a 'Notepad' window titled 'SomeFile.txt:SecretWord2.txt'. It has a standard menu bar (File, Edit, Format, View, Help) and contains the text 'che dau file cap do 2'.

```
C:\Users\BHB>
C:\Users\BHB>more < SomeFile.txt:SecretWordHere.txt
banhabanfhfj

C:\Users\BHB>notepad SomeFile.txt:SecretWord.txt

C:\Users\BHB>more < SomeFile.txt:SecretWordL2.txt
The system cannot find the file specified.

C:\Users\BHB>notepad SomeFile.txt:SecretWord2.txt

C:\Users\BHB>
```

SomeFile.txt:SecretWord2.txt - Notepad

File Edit Format View Help

che dau file cap do 2

# Detect “Hide” data

6

```
C:\Users\BHB>dir /R SomeFile.txt
Volume in drive C is OS
Volume Serial Number is 73C8-6A00

Directory of C:\Users\BHB

08/18/2017  09:57 AM                0 SomeFile.txt
                16 SomeFile.txt:SecretTwo.txt:$DATA
                18 SomeFile.txt:SecretWord.txt:$DATA
                0 SomeFile.txt:SecretWord2.txt:$DATA
                12 SomeFile.txt:SecretWordHere.txt:$DATA
                1 File(s)                0 bytes
                0 Dir(s) 221,155,078,144 bytes free
```

# *Why ADS is not good?*

7

- 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 autopsy*

8

- To discovery ADS
- To detect hidden files



# To discovery ADS

9

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

# streams.exe

10

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.15063]  
(c) 2017 Microsoft Corporation. All rights reserved.
```

```
C:\WINDOWS\system32>cd C:\Users\BHB
```

```
C:\Users\BHB>streams.exe SomeFile.txt
```

```
streams v1.60 - Reveal NTFS alternate streams.  
Copyright (C) 2005-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
C:\Users\BHB\SomeFile.txt:  
:SecretTwo.txt:$DATA 16  
:SecretWord.txt:$DATA 18  
:SecretWord2.txt:$DATA 0  
:SecretWordHere.txt:$DATA 12
```

# Analyzing the Master File Table (MFT) for ADS Info

11

- **mmls \\.\\PhysicalDrive0**

	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	0001026047	0001024000	EFI system partition
005:	001	0001026048	0001107967	0000081920	Basic data partition
006:	002	0001107968	0001370111	0000262144	Microsoft reserved partition
007:	003	0001370112	0002906111	0001536000	Basic data partition
008:	004	0002906112	1119629311	1116723200	Basic data partition
009:	005	1119629312	1120550911	0000921600	
010:	006	1120550912	2207825919	1087275008	Basic data partition
011:	007	2207825920	3259879423	1052053504	Basic data partition
012:	008	3259879424	3884044287	0624164864	Basic data partition
013:	-----	3884044288	3884046335	0000002048	Unallocated
014:	009	3884046336	3907022598	0022976263	Microsoft recovery partition
015:	-----	3907022599	3907024646	0000002048	Unallocated

# Analyzing the Master File Table (MFT) for ADS Info

12

- **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

13

- Using tsk-xview.exe

```
C:\tools>tsk-xview.exe -r -v

[INFO] High-level enumeration. Please wait.
[INFO] Found 95773 files and dirs
[INFO] Opened \\.\PhysicalDrive0
[INFO] Partition NTFS (0x07) at sector 56
[INFO] Low-level enumeration. Please wait.
[STREAM] C:/NUL:hidden
Inode: 12991-128-3
Size: 8
SIA Created:      Tue Sep 20 10:56:14 2011
SIA File Modified: Tue Sep 20 10:57:27 2011
SIA MFT Modified:  Tue Sep 20 10:57:27 2011
SIA Accessed:     Tue Sep 20 10:57:27 2011
FNI Created:      Tue Sep 20 10:56:14 2011
FNI File Modified: Tue Sep 20 10:56:14 2011
FNI MFT Modified:  Tue Sep 20 10:56:14 2011
FNI Accessed:     Tue Sep 20 10:56:14 2011
```

# To detect malware

14

- 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

15

- Using tsk-xview.exe

```
SIA Created:      Mon Apr 14 08:00:00 2008
SIA File Modified: Mon Feb 09 07:10:48 2009
SIA MFT Modified:  Fri Jun 25 15:18:16 2010
SIA Accessed:     Fri Jun 25 15:00:52 2010

FNA Created:      Fri Jun 25 15:18:16 2010
FNA File Modified: Fri Jun 25 15:18:16 2010
FNA MFT Modified:  Fri Jun 25 15:18:16 2010
FNA Accessed:     Fri Jun 25 15:18:16 2010
```

