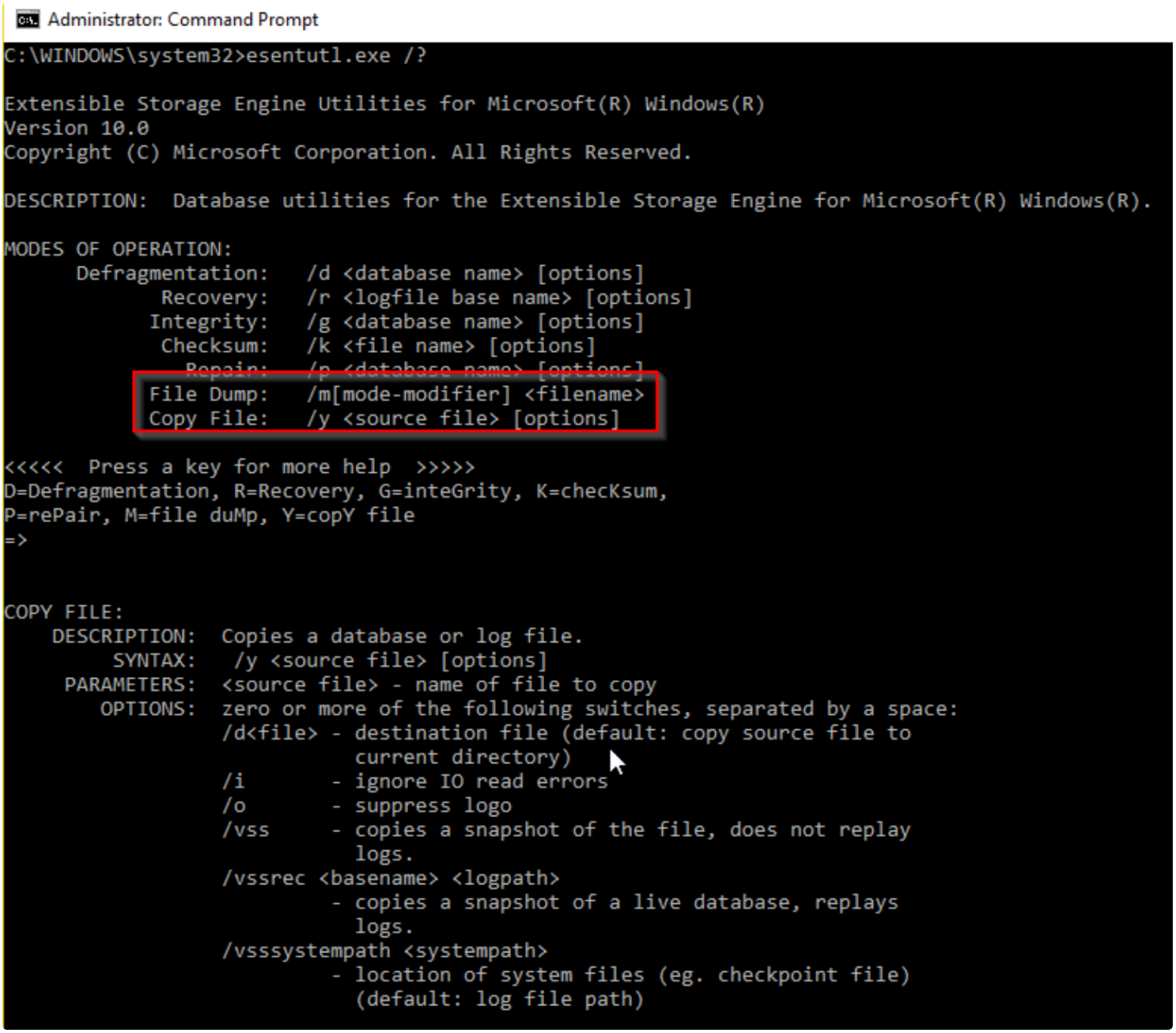
Locked File Access Using ESENTUTL.exe

Mike Cary Uncategorized December 6, 2018 3 Minutes

I'm currently working on a solution to collect files off a live system to be used during some IR processes. I won't go into any great detail but I'm limited to only using built-in Windows utilities. I need access to browser history data and while Chrome and Firefox allow copying of the history files, the WebCacheV01.dat file that IE and Edge history are stored in is a locked file and cannot be copied using native copy commands/cmdlets like Xcopy, Copy-Item, RoboCopy, etc.

ESE Database Files and ESENTUTL.EXE

there is a built-in tool for performing maintenance operations on such files: esentutl.exe. I started wondering if I could use this tool to export the database or at least dump the history. Running esentutl.exe from a command prompt, we see two interesting options: /m to dump a file and /y to copy a file.



Copying the file sounds great to me. Let's try

"esentutl.exe /y WebCacheV01.dat /d C:\Path\To\Save\WebCacheV01.dat"

```
Initiating COPY FILE mode...
     Source File: c:\users\[redacted]\appdata\local\Microsoft\Windows\WebCache\WebCache
Destination File: c:\users\[redacted]\Desktop\webcachev01.dat

                    Copy Progress (% complete)

         0    10   20   30   40   50   60   70   80   90  100
         |----|----|----|----|----|----|----|----|----|----|
         FAILURE: CreateFile:  (32), The process cannot access the file because it is being used by another process.



Operation terminated with error -1 (JET_wrnNyi, Function Not Yet Implemented) after 0.15 seconds.
```

Strike 1. That gives us the same "file is being used" error that I received with other copy commands. Ok so taking another look at the copy options, I see the /vss and /vssrec options. A couple of important distinctions here:

- I am running Windows 10, build 1803. The /vss and /vssrec options are only available on Win 10 and Server 2016 or later.
- The /vss and /vssrec options require you to be running as an admin

The /vss option "copies a snapshot of the file, does not replay the logs". We'll talk a little more about the transaction logs later but let's go with the /vss option for now.

```
C:\WINDOWS\system32>esentutl.exe /y /vss c:\users\[redacted]\appdata\local\Microsoft\Windows\WebCache\WebCacheV01.dat /d c:\users\[redacted]\Desktop\webcachev01.dat

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initializing VSS subsystem...

Initiating COPY FILE mode...
     Source File: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy39\Users\[redacted]\App
Destination File: c:\users\[redacted]\Desktop\webcachev01.dat

                    Copy Progress (% complete)

         0    10   20   30   40   50   60   70   80   90  100
         |----|----|----|----|----|----|----|----|----|----|
         ..................................................

       Total bytes read             = 0x9f80000 (167247872) (159 MB)
       Total bytes written          = 0x9f80000 (167247872) (159 MB)


Operation completed successfully in 10.578 seconds.
```

OK, that's much better. If I open up the WebCacheV01.dat file in ESEDatabaseView or BrowsingHistoryView, I see browsing history leading up to my testing. Initially, I

but that isn't the case. Esentutl.exe is able to use the Volume Shadow Copy service to make a backup of a locked file. This can be done even if VSCs are disabled on the system.

What about the /vssrec option? Data is not written directly to the database file. In simple terms, data is instead written to RAM and then to transaction logs before being flushed into the database file. Microsoft's documentation says: "The data can be written to the database file later; possibly immediately, potentially much later."

I did some testing with this and I'm not sure under what scenarios this doesn't happen right away. I opened up Edge and navigated to a new page, then immediately copied the WebCacheV01.dat file while Edge was still open and it contained this new entry.

Just keep in mind that when using the /vss option only, we have the potential to miss entries that have not been written to the database. Using the /vssrec option will replay these transaction logs. This is the syntax used:

esentutl.exe /y C:\Path\To\WebCacheV01.dat /vssrec V01 . /d c:\exports\webcachev01.dat

This can be a double-edged sword though because you also have the potential to lose deleted records that have yet to be purged from the database once the logs are flushed. If this is a concern you could go with both options and just save two copies of the file. This article from SANS provides more details on the ins and outs of ESE databases and transaction logs.

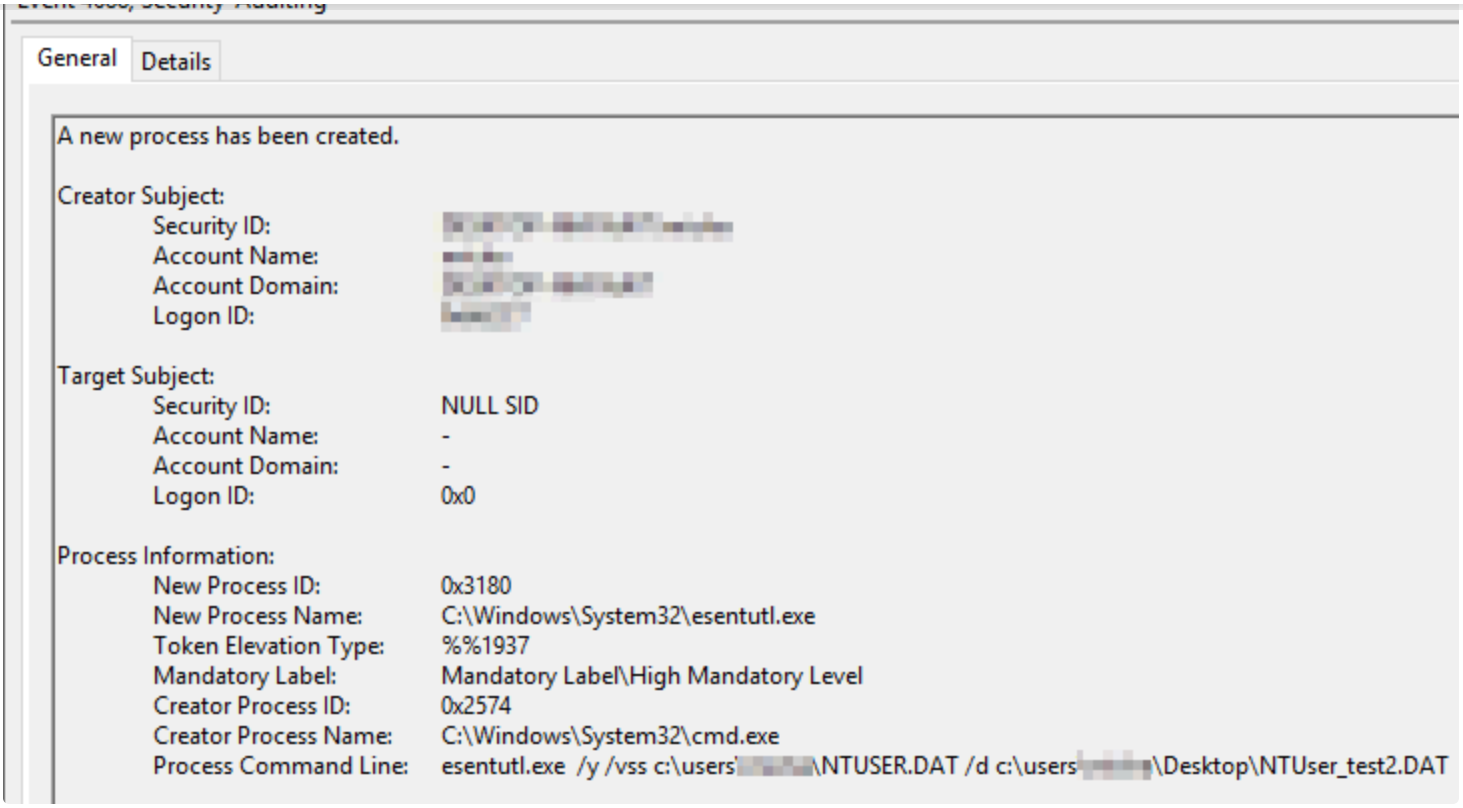
https://digital-forensics.sans.org/blog/2015/06/03/ese-databases-are-dirty

Additional Uses of Esentutl.exe

locked files? Well, it turns out you can. In this example, I grab a copy of the NTUSER.dat file for the currently logged in account.

```
C:\WINDOWS\system32>esentutl.exe /y /vss c:\users\[redacted]\NTUSER.DAT /d c:\users\[redacted]\Desktop\NTUser.DAT

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initializing VSS subsystem...

Initiating COPY FILE mode...
     Source File: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy42\Users\[redacted]\NTU
Destination File: c:\users\[redacted]\Desktop\NTUser.DAT

                     Copy Progress (% complete)

         0    10   20   30   40   50   60   70   80   90  100
         |----|----|----|----|----|----|----|----|----|----|
         ..................................................

        Total bytes read                = 0x940000 (9699328) (9 MB)
        Total bytes written             = 0x940000 (9699328) (9 MB)


Operation completed successfully in 11.812 seconds.
```

I really like this as an option for copying system files when doing investigations or even testing. I'm sure it has value to Red Teams as well as it allows you to grab other hives like the SAM and other ESE databases like NTDS.dit without introducing outside tools or using PowerShell. Blue Teams can detect this type of activity by auditing process



Final Thoughts

I'm still looking for a good way to get IE/Edge browser history on the versions of Windows that do not have the /vss switch so if you've got any ideas there, let me know.

Share this:

Twitter Facebook

Loading...

Tagged: DFIR, ESE Database, ESENTUTL.EXE

View all posts by Mike Cary

December 6, 2018

‹ Installing Volatility on Windows

RDP Event Log DFIR ›

6 thoughts on “Locked File Access Using ESENTUTL.exe”

Aky

January 16, 2019 at 10:38 am

Mike this is great work!

I was in your shoes a few months ago and I didn’t come upon this solution till reading your blog.

The way I got around this case was to use Raw Copy solution from https://github.com/jschicht/RawCopy.

You need to run it as admin and it shows history till the date when you extracted the file.

Basically, it does the same thing but with an external tool.

I executed it like this:
rawcopy64.exe

Cheers!

★ Like

↳ Reply

Aky

January 16, 2019 at 10:47 am

By the way the file WebCacheV01.dat is being locked by taskhost.exe on W7 and taskhostw.exe on W10

★ Like

↳ Reply

Mike Cary

January 16, 2019 at 4:21 pm

Hey Aky thanks for the comment! I've used RawCopy on some other projects and it works great. In my case I couldn't use any 3rd party tools to extract the file so I couldn't use it this time which is what led me to esentutl.exe. When I was researching things, I came across a post that said you could suspend or kill the taskhost.exe/taskhostw.exe process and it should allow you to copy the webcachv01.dat file but that didn't work for me.

★ Like

↳ Reply

February 11, 2019 at 11:28 am

Nice post, having the WebCacheV01.dat file locked is the main reason we built our free tool, Browser History Capturer:
https://www.foxtonforensics.com/browser-history-capturer/

Great to see there is also an option without using 3rd party tools.

★ Liked by 1 person

↳ Reply

curtmcgirt

January 22, 2020 at 6:58 pm

with the /vss switch

VSS Subsystem Init failed, 0x80042316
Operation terminated with error -2403 (JET_errOSSnapshotNotAllowed, OS Shadow copy not allowed (backup or recovery in progress)) after 0.188 seconds.

?

★ Like

↳ Reply

Mike Cary

January 22, 2020 at 8:45 pm

> running as admin.
>
> ★ Like
>
> ↳ Reply

Leave a comment

Follow Us

Recent Posts

RDP Event Log DFIR

Locked File Access Using ESENTUTL.exe

Installing Volatility on Windows

More Automation: Get-ZimmermanTools.ps1

Start-ImageParsing.ps1

Follow Us

Loading...