



Design a site like this with WordPress.com

Get started



# DFIR on the Mountain

[Home](#) [Contact](#)

## 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 WebCacheVo1.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

The WebCacheVo1.dat file is an ESE (Extensible Storage Engine) database file and 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

#### 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](#)



#### Privacy & Cookies

We, WordPress.com, and our advertising partners store and/or access information on your device and also process personal data, like unique identifiers, browsing activity, and other standard information sent by your device including your IP address. This information is collected over time and used for personalised ads, ad measurement, audience insights, and product development specific to our ads program. If this sounds good to you, select "I Agree!" below. Otherwise, you can get more information, customize your consent preferences for over 51 different ad vendors, or decline consent by selecting "Learn More". Note that your preferences apply to all websites in the [WordPress.com network](#), and if you change your mind in the future you can update your preferences anytime by visiting the Privacy link displayed under each ad or by using the "Privacy" option in the Action Bar located at the bottom-right corner of the screen. One last thing, our partners may process some of your data based on legitimate interests instead of consent but you can object to that by choosing "Learn More" and then disabling the Legitimate Interests toggle under any listed Purpose or Partner.

[View Partners](#)

[Learn More](#)

[I Agree!](#)



Get started

```
C:\WINDOWS\system32>esentutl.exe /?

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

DESCRIPTION:  Database utilities for the Extensible Storage Engine for Microsoft(R) Windows(R).

MODES OF OPERATION:
  Defragmentation:  /d <database name> [options]
  Recovery:        /r <logfile base name> [options]
  Integrity:       /g <database name> [options]
  Checksum:        /k <file name> [options]
  Repair:          /p <database name> [options]
  File Dump:       /m[mode-modifier] <filename>
  Copy File:       /y <source file> [options]

<<<<<  Press a key for more help  >>>>>
D=Defragmentation, R=Recovery, G=inteGrity, K=checkKsum,
P=rePair, M=file duMp, Y=copY file
=>

COPY FILE:
  DESCRIPTION:  Copies a database or log file.
  SYNTAX:      /y <source file> [options]
  PARAMETERS:  <source file> - name of file to copy
  OPTIONS:     zero or more of the following switches, separated by a space:
                /d<file> - destination file (default: copy source file to
                        current directory)
                /i      - ignore IO read errors
                /o      - suppress logo
                /vss     - copies a snapshot of the file, does not replay
                        logs.
                /vssrec <basename> <logpath>
                        - copies a snapshot of a live database, replays
                        logs.
                /vsssystempath <systempath>
                        - location of system files (eg. checkpoint file)
                        (default: log file path)
```

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

“esentutl.exe /y WebCacheVo1.dat /d C:\Path\To\Save\WebCacheVo1.dat”

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

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

Initiating COPY FILE mode.
  Source File: c:\users\█████\appdata\local\Microsoft\Windows\WebCache\WebCache
  Destination File: c:\users\█████\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.



Design a site like this with WordPress.com

Get started

```
Initializing VSS subsystem...

Initiating COPY FILE mode...
Source File: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy39\Users\user\AppData
Destination File: c:\Users\user\Desktop\webcachevo1.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 WebCacheVo1.dat file in ESEDatabaseView or BrowsingHistoryView, I see browsing history leading up to my testing. Initially, I thought it was grabbing a copy of the file from a previous Volume Shadow Copy (VSC) 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 WebCacheVo1.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\WebCacheVo1.dat /vssrec Vo1 . /d
c:\exports\webcachevo1.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

So we know we can use esentutl.exe to copy ESE database files but what about other 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.

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



Design a site like this with WordPress.com

Get started

or using Powershell. Blue Teams can detect this type of activity by auditing process creation and looking for activity by esentutl.exe, particularly with the /vss switch.

## 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...

### Related

#### Start-ImageParsing.ps1

October 5, 2018  
In "DFIR"

#### More Automation: Get-ZimmermanTools.ps1

October 12, 2018  
In "DFIR"

#### Installing Volatility on Windows

October 29, 2018  
In "DFIR"

Tagged: DFIR, ESE Database, ESENTUTL.EXE



### Published by Mike Cary

*View all posts by Mike Cary*

#### Published

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>.

Comment

Reblog

Subscribe

Privacy



Design a site like this with WordPress.com

Get started

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

I executed it like this:

rawcopy64.exe

/FileNamePath:”C:\Users\IEUser\AppData\Local\Microsoft\Windows\WebCache\WebCac  
heVo1.dat” /OutputPath:C:\Windows\

Cheers!

★ Like

↩ Reply

Aky

January 16, 2019 at 10:47 am

By the way the file WebCacheVo1.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 webcachvo1.dat file but that didn’t work for me.

★ Like

↩ Reply

Alex

February 11, 2019 at 11:28 am

Nice post, having the WebCacheVo1.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



Comment



Reblog



Subscribe



Privacy





Design a site like this with WordPress.com

Get started

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

Are you running from an admin/elevated command prompt? I get that if I’m not running as admin.

★ Like

↩ Reply

## Leave a comment

### Follow Us

[Blog at WordPress.com.](#)