NCFI M3E WIN F-2017

Project: Live Digital Forensic

Anonymous ID: **193**

v1.0 from 2017-12-08

(* as part of the MISEB study at the NTNU)

Contents

1 Details for the project

Develop a software tool that automate the Live Digital Forensic process of a Windows 10 computer. The target group is non technical police officers that often are first on the crime scene. You can deside what you want to implement in your tool, but we advice you to keep it simple and do not use more than the estimated 80 hours.

The features you plan to implement must be presented to the rest of the class.

The Lesson about scripting should help you getting started with your project, but every possible implementation is not described in the syllabus. This means that you might need to use help functionality, resources online, discussion forum, etc.

2 Development documentation

Be aware that a development documentation is growing and growing and becomes often a little bit confusing for the reader in the end!

The workload should be documented in the developer documentation.

2.1 Order of Volatility

I first have done a little brainstorming about volatile data and put them into categories that reflect my personal view of order of volatility.

Save extreme transient volatile data first:

- dns cache (can not be taken from ram)
- arp cache (can not be taken from ram [Windows] or is away before ram is captured [Linux/macOS])

Save volatile data that directly influences life digital forensics workflow second:

- date, time and timezone
- clipboard (save it and do not use it!) (also in ram)
- shell history (also in ram)
- check for open programms incl. multiple desktops!
- information about loggedin user and his groups (Administrators)
- system information (imageinfo from volatility sometimes fails)
- network configuration (ip, netmask, route, dns, dns suffix, ...)
- processes (also in ram)
- network connections (also in ram)
- currently opened filehandles (also in ram)

- serving shares
- connected shares
- serialnumbers of physical storage <-> logical volumes (drive letters)
- detect active encryption
- export Bitlocker keys if present
- save and/or save ram
- image open containers

Save volatile data that influences the first survey/interrogation of the suspect third only if wanted by the investigator:

- saved WLAN credentials
- saved browser creds
- saved mail creds
- password hints for users
- NTLM/SHA512 hashes (pass-the-hash, cracking, ...)
- LDAP/OpenDirectory/ActiveDirectory

Save volatile data that directly influences search at the crime scene fourth:

- serialnumbers of connected usb devices (and search for them)
- network mapping (and try to get all nodes under your control)
- macaddress of a wlan nas (and search for them)

Skip volatile data in the second step that could be extracted from a memory dump if a memory dump could be performed.

I have captured the memory of an old AMD PC with 2GB Ram and Windows XP, a newer Intel PC with 16GB and Windows 7 and a new Intel PC with 32 GB and Windows 10 and checked what works and what not:

- clipboard seems to work
- cmdline, cmdscan and consoles seem to work
- imageinfo has sometimes more or less problems, better have a plan b!
- dumpregistry produced a lot of „Physical layer returned None for index 2000, filling with NULL.“ and all tools we have used in the course ware not robust enough to handle such corrupt files. That influences network configuration, password hints, serial numbers of usb devices, ... If I have enough time I plan to implement copy the registry hives via RawCopy[1] as a plan b.
- pslist, pstree, psscan, psxview, ... seem to work
- netscan seems to work (connections for XP too)

[1] https://github.com/jschicht/RawCopy

- handles seems to work

Skip data that could be extracted postmortem from the system:

- last opened files/folders/servers
- logfiles
- registry hives (connected usb/bluetooth devices, network config, password hints)
- shadow copies
- autostart
- services

A litte bit more about time in the second step:

- After starting the script time and date of start will be logged into the logfile.
- Start (time and date) of each command will also logged into the logfile before the execution of the command.
- End (time and date) of each command too.
- The script asks the user for the current real time on his watch (hopefully off-air clock) to be able to reconstruct possible time lag.

Because I have too little time for all I will focus on the first and second step as good as possible.

2.2 Output of Script

Because I have too little time for a nice PDF- or HTML-report I will just deliver the logfile and the redirected output of the single tools.

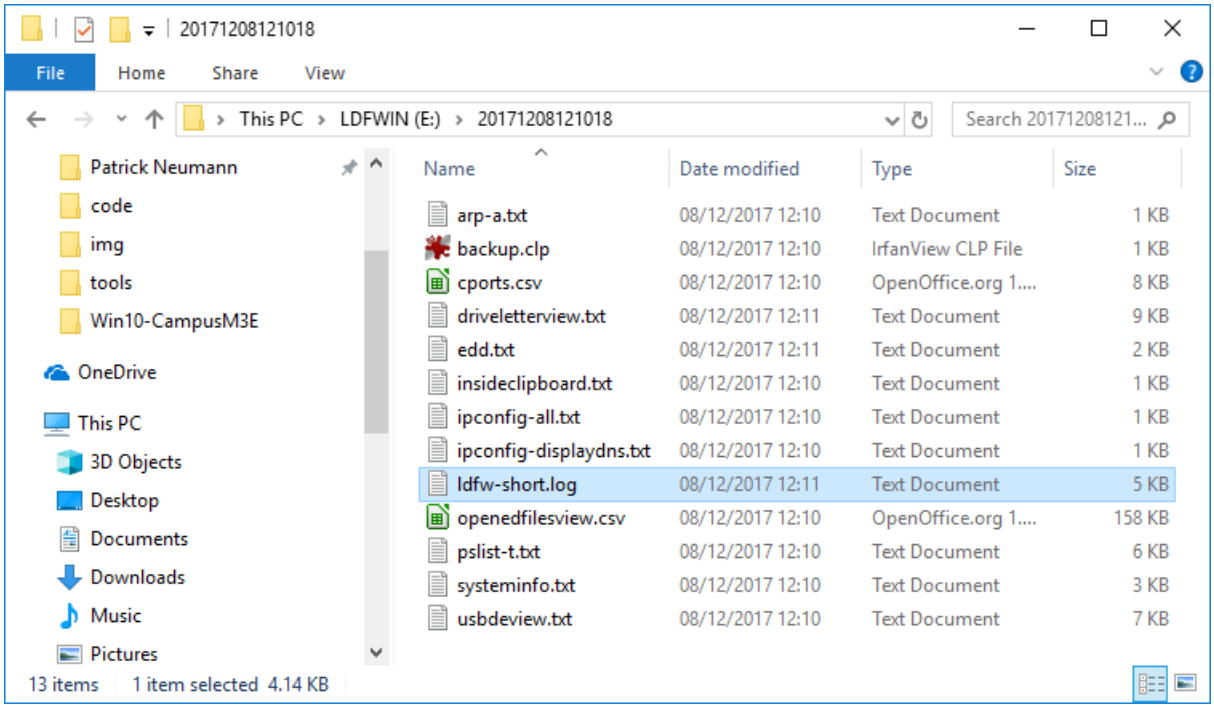


Figure 1: The output directory

For more details see the Example section!

2.3 Locard Principle

Because of lack of time I was not able to implement nice to have features.

I just made a decision of capture memory or execute some commands (insideclipboard, pslist, cports and openedfilesview).

I have chosen tools other developers have chosen in their similar project too. So I skipped investigation what each tool modifies to the system while running. If I had more time my tool of choise to check that would be process monitor[2] from „SysInternals“.

2.4 Features

I have tried to check the permissions by executing a command that needs admin privileges and if the return code is not 0 I executed a litle vbs script to switch to admin privileges by uac. After 4 hours an uac dialog pops up but in the script I have no admin privileges after clicking [Yes]. One more time wasted time.

I will cover that by explizit instrutions to the user.

The script will do the following:

[2]https://docs.microsoft.com/de-de/sysinternals/downloads/procmon

- empty PATH
- check if admin
- change drive and directory to script
- generate target dirname by date and time
- start logging
- ipconfig /displaydns
- apr -a
- detect bitness
- ask for case information
- systeminfo
- capture ram if answered with y
- do insideclipboard, pslist, cports and openedfilesview (if admin) otherwise
- ipconfig /all
- usbdeview
- driveletterview
- edd (only possible as admin, ALERT in red color if active encryption is detected)
- write end date and time to logfile
- close window if user hit enter

2.5 Best Programming Practice

I will chose the „Command Prompt“ over the „PowerShell“ because:

- it is available on Windows versions from XP to 10 (incl. Fall Creator Update)
- there are no big differences of the „Command Prompt“ in all Windows versions
- the „PowerShell“ is not available in Windows XP by default
- there are big changes in „PowerShell“ since their release
- there is no need of „Set-ExecutionPolicyl“ in the „Command Prompt“

100% static binaries on windows never worked and will never work.
On GNU/Linux it is much easier: just build static busybox and dropbear (ssh) for arm, x86 and x64 and you will only miss something in rare special situations.

If I will not trust the system I have to copy alle executables and dlls from another system with the same operating system, version, build and architecture to the same folder as my script. Because I have too little time and that part is really time consuming and does not work by 100% I will skip this one! I will also skip to generate a hash.db. Same time problem.

I will have to trust the Windows binaries on the system or use non standard Windows tools (that bring often a lot of but not all resources with them).

I will calculate the hash falues off all non standard Windows tools and add the sha256sums file beside the tools folder. I have given up to implement verifying the binaries by hash as posted one the page „Commands on the scene“ in PingPong after about 4 hours. The code snippets doesn't work.

But the script is designed to be run on the hackers mashine and not on the mashine of the hacked one where the hacker has manipulated a lot and installed a rootkit.

I will use the ability of comments to add as much as possible of information for the reader of the source code to the script.

To assess this part: read the source!

2.6 Correctness of artifacts

I have not selected to interpret content.

EDD detects also TrueCrypt[3], Ciphershed[4] and VeraCrypt[5] containers if they are open. Other software I was not able to verify.

If no container is open, edd detects none.

2.7 Forensically soundness

I have chosen the older version of winpmem because the newer one stores the image in aff4 format that is not very common up to now. A patch for volatility exists but is not part of volatility now.

I have also decided to not calculate a hash over the maybe big dump on the suspects machine because of too much load for what I can perform just some seconds later on my own machine.

If there were more time one additional feature could have been implemeted: imaging the decrypted virtual volume with ewfacquire. The result would be an EWF image. But I have skiped that!

2.8 Used non standard Windows tools

Had a look at other solutions (what tools do they use and how they do it).

I focus only on what I have planed to implement (see Order of Volatility)!

[3] https://truecrypt.ch/downloads/
[4] https://www.ciphershed.org/
[5] https://veracrypt.codeplex.com/wikipage?title=Downloads

Here is the list of the non standard Windows tools I have chosen (incl. SHA256 hash-sums):

```
SHA256(.\tools\cports_v236_x64.exe)= 1ca540a1a6c4014a2005665fcf3d72e1f705045b9648ceacaa656606856c0248
SHA256(.\tools\cports_v236_x86.exe)= 1f576522af90c5eabfb2d822587d97fc0aabc0f25c916649ec6e91cf9a591830
SHA256(.\tools\DriveLetterView_v146_x64.exe)= a36885e04b3ad2609f36d9095c64d69516ec1981e1b181b0429fa47499270b0c
SHA256(.\tools\DriveLetterView_v146_x86.exe)= 5747fd12096ef5220ae4c0c7bb08b25307f5ed0f93fba8aef76b334e2a219be6
SHA256(.\tools\EDD_v211.exe)= 3d5f467e3f875cda356ef9af1f1d38af6ba5782baa30b23d4347946b7e3f8ea5
SHA256(.\tools\InsideClipboard_v115.exe)= b74d220e672cbc2d23235ef5cf9047077288b0f6074a0d61440810cac6a16340
SHA256(.\tools\OpenedFilesView_v170_x64.exe)= cd878e1ba5a5318cbe00a9d1171af063639ea9d65f67467aec578468ac6d5358
SHA256(.\tools\OpenedFilesView_v170_x86.exe)= d6a0a6dc55bcc3b64cfb409d22892b70fe474742601f73d4a21bfe471bfefba9
SHA256(.\tools\pslist_v14_x64.exe)= e6901e8423da3e54bab25f7c90f60d3979bfa5bb61bcc46059662736253b8c72
SHA256(.\tools\pslist_v14_x86.exe)= 9927831e111ac61fd7645bf7efa1787db1a3e85b6f64a274ca04b213dc27fd08
SHA256(.\tools\USBDeview_v272_x64.exe)= b47352cfcdf0d58386c291687928fb6ffecce47e27f4ff950a247dd0061d9f92
SHA256(.\tools\USBDeview_v272_x86.exe)= b694f844f9cb2d4d2368c5a4e225b61b758e815c007faf14fc00f9b3e8ea9b8f
SHA256(.\tools\winpmem_1.6.2.exe)= 447502ac949e8d326603fe2d6555deca1057fb5b3bc5a73b3485a4e910bc348e
```

2.8.1 DEFT Linux

First there was DEFT-Extra. Some time later it was replaced by DART[6].

Both have a graphical user interface what will not be an option for this project.

I have downloaded DART v2, extracted it and doubleclicked dart.exe.

The disclaimer should inspire me:

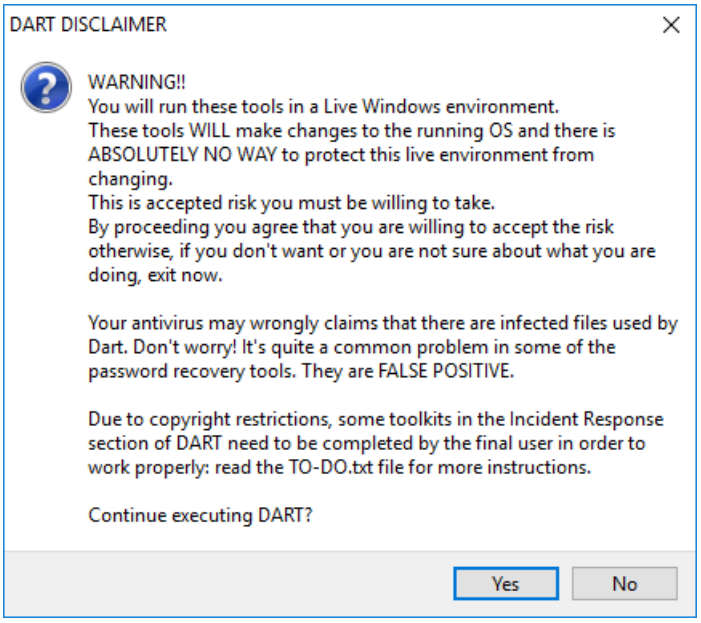


Figure 2: DART DISCLAIMER

Interesting tools are:

- RamCapturer
- USBDevView
- InsideClipboard

[6] http://www.deftlinux.net/2014/04/16/deft-8-1-and-dart-2-2014/

- CProcess
- DiskSmartView
- OpenedFilesView
- CurrPorts

I miss something usefull for detecting active encryption and some other parts I will try to implement.

The hashes for verification of all tools are stored in a central xml file.

DART is writing a logfile. Hashvalues of input and output files are also integrated.

2.8.2 C.A.IN.E.

First there was WinTaylor, NirLauncher (incl. Sysinternals and many other tools), WinUFO and now[7] there are just the tools without a gui?

I have downloaded caine9.iso, mounted it in Windows 10 and opened it with file explorer.

In the root of the iso image I doubleclicked NirLauncher.exe. Only NirSoft tools are integrated in this configuration.

Interesting tools are:

- AdapterWatch or NetworkInterfacesView
- CurrPorts
- CurrProcess
- DiskSmartView or DriveLetterView
- InsideClipboard
- OpenedFilesView
- USBDeview

There are no interesting tools (for me at this moment) in the subfolder winforensictools.

On the webpage of NirLauncher[8] you can read that it is easy to add more tools by yourself.

In the past the developers of C.A.IN.E. done that too. They have per example also included the SysInternalsSuite[9].

Interesting tools are:

- handle

[7] http://www.caine-live.net/page2/page2.html
[8] http://launcher.nirsoft.net/
[9] https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

- pslist
- TCPView

I still missing some tools for my problems (eg. active encryption).

2.8.3 FiRST

The first time I heared about FiRST was more then three years before its first release.

They use windows tools on the local machine.

They use a SysInternals tool.

They use winpmem for capture memory.

The use VeraStatus for detecting open VeraCrypt containers. But if you dig a little bit deeper in the source code there was done a lot of more work by the FiRST developers to detect encryption. Such a development would go beyound the scope of this 80 hours short project.

They do the extrem volatile stuff as I have planed to do it.

winpmem will also be my first choise for memory imaging from the command prompt.

Why only VeraCrypt? That is like looking at the problem with only a half open eye.

I will try to support a wider range of encryption software and will give Encrypted Disk Detector[10] from „Magnet Forensics“ a try. This tool will detect TrueCrypt, PGP, Bitlocker, SafeBoot, BestCrypt, Checkpoint, Sophos or Symantec encrypted volumes. Still not perfect but better anyway!

The logs of DART and FiRST are really good but the reports are really poor.

2.9 License for use

I can only define the license for my script.

For licenses of used non standard Windows tools check the webpages of the other developers!

2.9.1 OpenSource License

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

[10] https://www.magnetforensics.com/free-tool-encrypted-disk-detector/

2.9.2 Warrenty

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

2.9.3 Link

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

3 Burned time

Project implementation plan (presentation): 8 hours

Creating LaTeX template with named sections: 4 hours

Have a little bit deeper look at other Projects: 8 hours

Project implementation plan revision: 8 hours

Scripting: 20 hours

Failed implementing hash verify: 4 hours

Failed implementing UAC into the script: 4 hours

Testing and generating anonym example output: 4 hours

Merging all into/editing this LaTeX document: 20 hours

4 User manual

4.1 Preparations

1. Get an usb-stick of a size that a memory capture could be saved on it (eg: 128GB).

2. Format the usb-stick with a exFAT or NTFS. Give it a name that is individual and that you will remember a long time (eg: LDFWSHORT).

3. Copy the batch script ldfw-short.bat, tools (directory incl. alls files) and tools_sha256sums.txt to the root directory of the usb-stick.

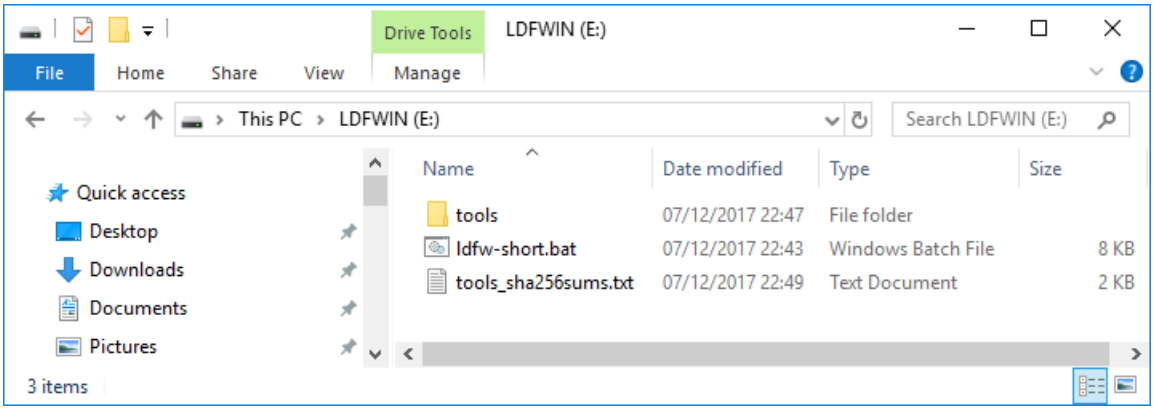


Figure 3: USB-Stick with ldfw-short.bat

4. Eject the usb-stick.

5. Ready!

4.2 Usage

1. Plug the usb-stick into the suspects computer that is running any kind of version of Microsoft Windows.

2. Do a rightklick on the Windows logo in the left lower corner and klick on file explorer.

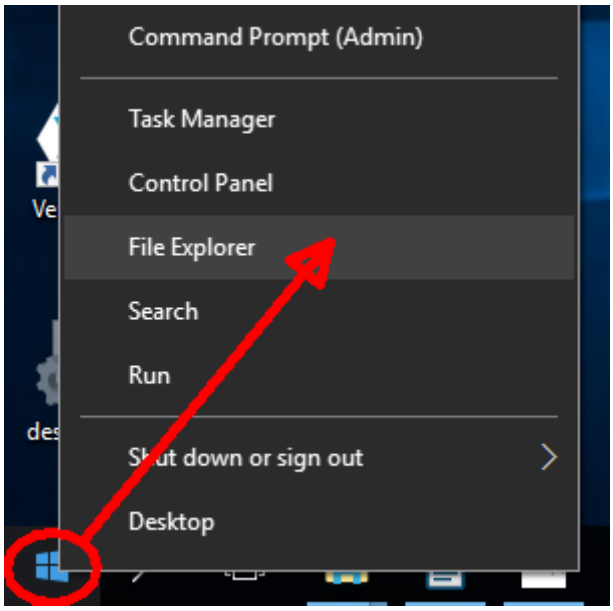


Figure 4: Rightclick Windows Logo -> file explorer

X. Do not doubleclick any icons that looks like the computer! It's easy to place such icons with a link to shutdown!

X. Do not press Windows-key + E! Keybindings could easily be manipulated to execute a different action, per example: shutdown!

3. Click on your usb-stick in the left panel of the file explorer.

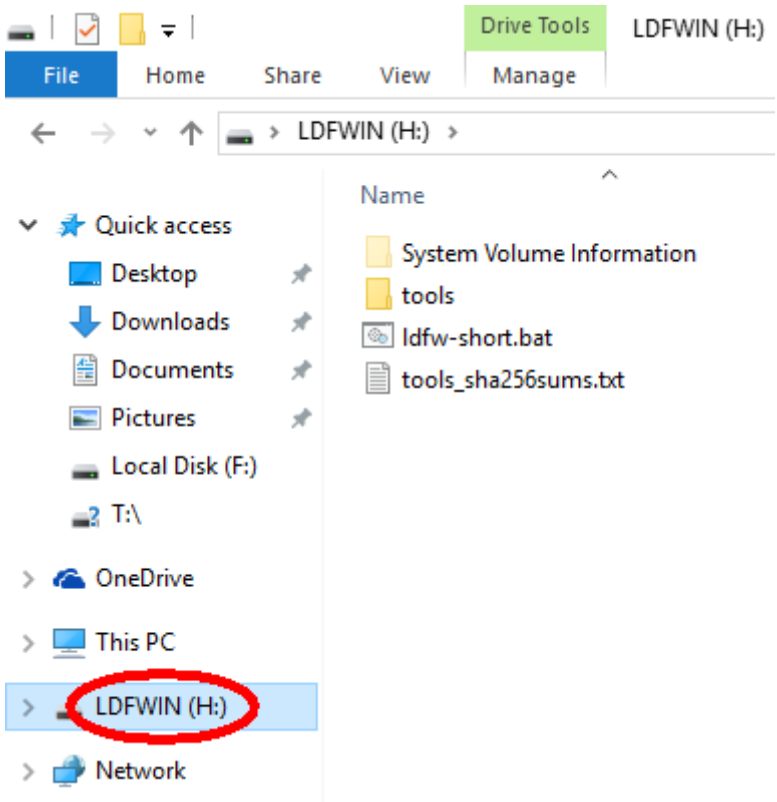


Figure 5: Click in the left panel

!. We advice you to start the script as an administrator! If it is not possible to elevate you rights it will be okay to gather less data as a normal user but the script will not be able to alert you if encryption is active!

4. Do a rightclick on ldfw-short.bat and klick on Run as administrator.

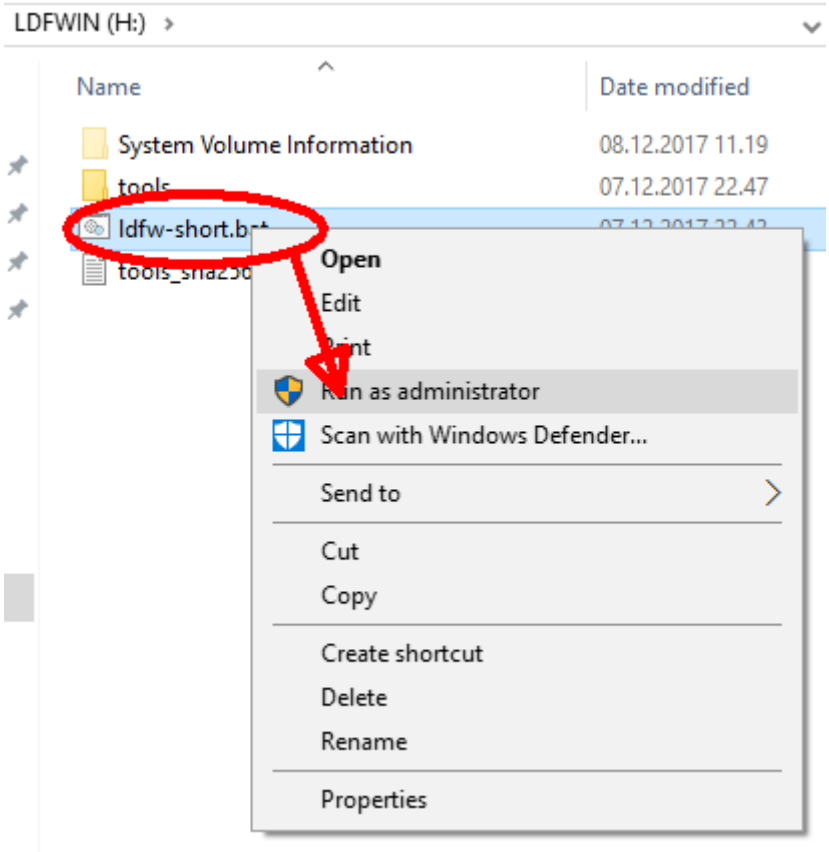


Figure 6: Run as admin

5. Enter the case information (case number, description, evidence number, examiner name, notes and the current real time) if asked for.

6a. If you answer the question Do you want to capture the memory now? with a single lower case y then memory will be captured and insideclipboard, pslist, cports and openedfilesview will be skipped.

6b. Every other input will skip capturing the memory and doing insideclipboard, pslist, cports and openedfilesview instead.

7a. If you have started the script with admin rights and there will no read text active encryption was not detected. But as you can not be sure by 100% it would be always a good idea to have someone else a look at the system!?

7b. If you see the red alert active encryption was detected. Do not power off the machine but call for an expert!

```
execution of edd startet on 08.12.2017 at 12.07.14,32
output was written to 20171208120111\edd.txt
execution of edd finished on 08.12.2017 at 12.07.19,21
ALERT !!! Do not shutdown this system !!! ALERT
ENCRYPTION !!! Call for an expert !!! ENCRYPTION
############################################################
```

Figure 7: ALERT!

8. If the window is no more needed you can just press enter to close it.

9. Eject the USB-Stick.

10. The first next action is to make a forensic image of the USB-Stick!

The expert will find the hint about the decrypted virtual volume in the file edd.txt in the output folder. Before shutting down the system he will make an forensic image of that volume. Most meta data information will then be present in the filesystem information. Maybe undeleting or carving will be possible too.

5 Examples

Example of the script report output; technical output report, user friendly report.

Example as admin without capturing the memory:

5.1 ldfw-short.log

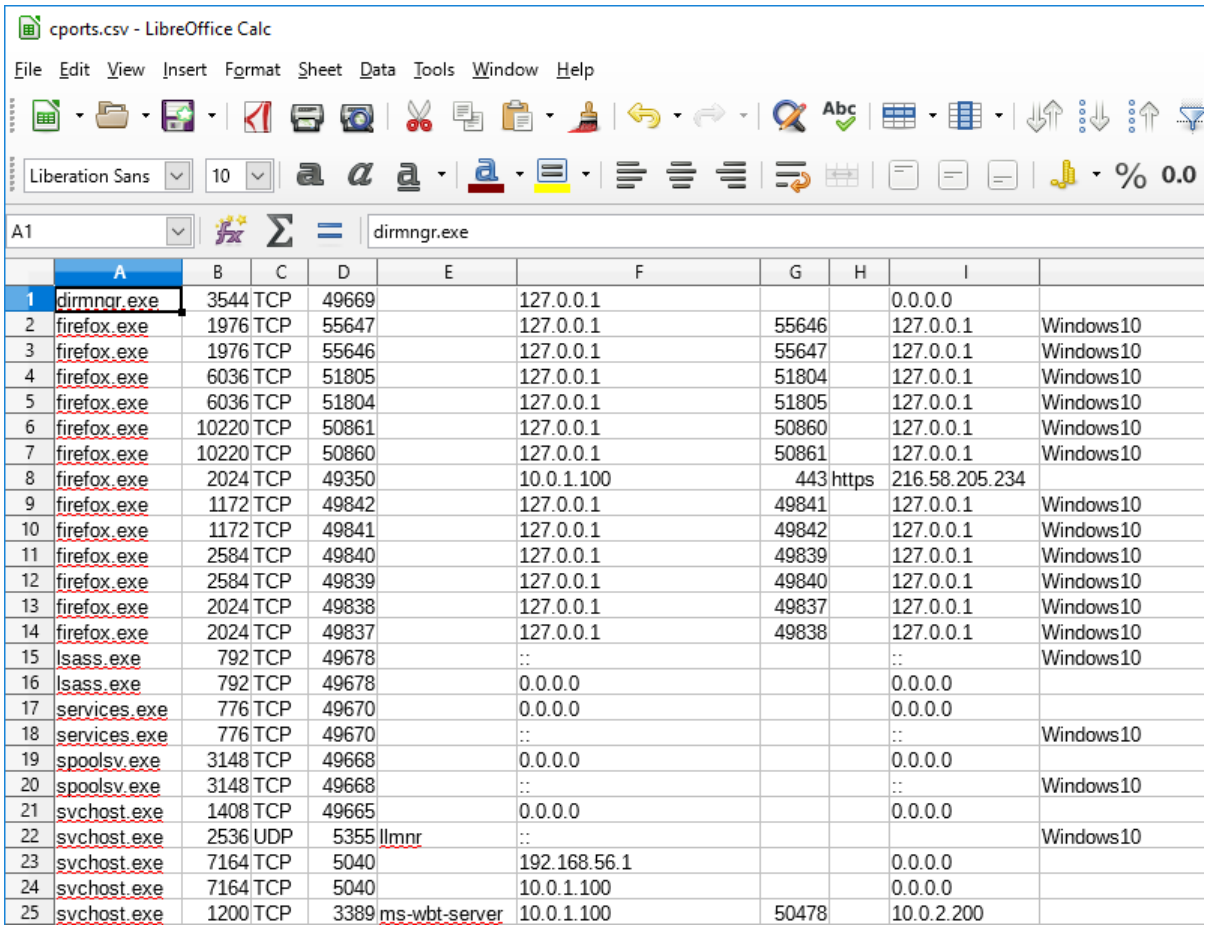
```
########################################################################
# ldfw-short.bat (Live Digital Forensics for Windows [short version])
#   startet on 08.12.2017 at 12.10.18,82
########################################################################
execution of ipconfig-displaydns startet on 08.12.2017 at 12.10.18,88
output was written to 20171208121018\ipconfig-displaydns.txt
execution of ipconfig-displaydns finished on 08.12.2017 at 12.10.18,98
------------------------------------------------------------------------
execution of arp-a startet on 08.12.2017 at 12.10.19,01
output was written to 20171208121018\arp-a.txt
execution of arp-a finished on 08.12.2017 at 12.10.19,07
------------------------------------------------------------------------
Operation System arch is 64 bit.
########################################################################
# Informations about the case
#-----------------------------------------------------------------------
# Case number:     1
# Description:     ldfw-short test
# Evidence number: 1
# Examiner name:   No. 193
# Notes:           as admin without ram
# Notes:           08.12.2017 at 12:10:30
########################################################################
execution of systeminfo startet on 08.12.2017 at 12.10.40,71
output was written to 20171208121018\systeminfo.txt
execution of systeminfo finished on 08.12.2017 at 12.10.44,73
------------------------------------------------------------------------
Capture memory was NOT or could NOT be chosen...
... skipping winpmem!
------------------------------------------------------------------------
execution of insideclipboard-1 startet on 08.12.2017 at 12.10.50,41
output was written to 20171208121018\insideclipboard.txt
execution of insideclipboard-1 finished on 08.12.2017 at 12.10.51,74
------------------------------------------------------------------------
execution of insideclipboard-2 startet on 08.12.2017 at 12.10.51,80
output was written to 20171208121018\backup.clp
execution of insideclipboard-2 finished on 08.12.2017 at 12.10.51,93
------------------------------------------------------------------------
execution of pslist-t startet on 08.12.2017 at 12.10.51,96
output was written to 20171208121018\pslist-t.txt
```

```
execution of pslist-t finished on 08.12.2017 at 12.10.52,74
------------------------------------------------------------------------
execution of cports startet on 08.12.2017 at 12.10.52,77
output was written to 20171208121018\cports.csv
execution of cports finished on 08.12.2017 at 12.10.54,20
------------------------------------------------------------------------
execution of openedfilesview startet on 08.12.2017 at 12.10.54,29
output was written to 20171208121018\openedfilesview.csv
execution of openedfilesview finished on 08.12.2017 at 12.10.57,60
------------------------------------------------------------------------
execution of ipconfig-all startet on 08.12.2017 at 12.10.57,63
output was written to 20171208121018\ipconfig-all.txt
execution of ipconfig-all finished on 08.12.2017 at 12.10.57,73
------------------------------------------------------------------------
execution of usbdeview startet on 08.12.2017 at 12.10.57,80
output was written to 20171208121018\usbdeview.txt
execution of usbdeview finished on 08.12.2017 at 12.10.57,91
------------------------------------------------------------------------
execution of driveletterview startet on 08.12.2017 at 12.10.57,94
output was written to 20171208121018\driveletterview.txt
execution of driveletterview finished on 08.12.2017 at 12.10.58,11
------------------------------------------------------------------------
execution of edd startet on 08.12.2017 at 12.10.58,12
output was written to 20171208121018\edd.txt
execution of edd finished on 08.12.2017 at 12.10.59,79
ALERT !!! Do not shutdown this system !!! ALERT
ENCRYPTION !!! Call for an expert !!! ENCRYPTION
########################################################################
# ldfw-short.bat (Live Digital Forensics for Windows [short version])
#   finished on 08.12.2017 at 12.10.59,98
########################################################################
```

5.2 arp

```
Interface: 10.0.1.100 --- 0xd
  Internet Address      Physical Address      Type
  10.0.1.1              00-06-4f-90-0d-ef     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x11
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
```

5.3 cports



	A	B	C	D	E	F	G	H	I	
1	dirmngr.exe	3544	TCP	49669		127.0.0.1			0.0.0.0	
2	firefox.exe	1976	TCP	55647		127.0.0.1	55646		127.0.0.1	Windows10
3	firefox.exe	1976	TCP	55646		127.0.0.1	55647		127.0.0.1	Windows10
4	firefox.exe	6036	TCP	51805		127.0.0.1	51804		127.0.0.1	Windows10
5	firefox.exe	6036	TCP	51804		127.0.0.1	51805		127.0.0.1	Windows10
6	firefox.exe	10220	TCP	50861		127.0.0.1	50860		127.0.0.1	Windows10
7	firefox.exe	10220	TCP	50860		127.0.0.1	50861		127.0.0.1	Windows10
8	firefox.exe	2024	TCP	49350		10.0.1.100	443	https	216.58.205.234	
9	firefox.exe	1172	TCP	49842		127.0.0.1	49841		127.0.0.1	Windows10
10	firefox.exe	1172	TCP	49841		127.0.0.1	49842		127.0.0.1	Windows10
11	firefox.exe	2584	TCP	49840		127.0.0.1	49839		127.0.0.1	Windows10
12	firefox.exe	2584	TCP	49839		127.0.0.1	49840		127.0.0.1	Windows10
13	firefox.exe	2024	TCP	49838		127.0.0.1	49837		127.0.0.1	Windows10
14	firefox.exe	2024	TCP	49837		127.0.0.1	49838		127.0.0.1	Windows10
15	lsass.exe	792	TCP	49678		::			::	Windows10
16	lsass.exe	792	TCP	49678		0.0.0.0			0.0.0.0	
17	services.exe	776	TCP	49670		0.0.0.0			0.0.0.0	
18	services.exe	776	TCP	49670		::			::	Windows10
19	spoolsv.exe	3148	TCP	49668		0.0.0.0			0.0.0.0	
20	spoolsv.exe	3148	TCP	49668		::			::	Windows10
21	svchost.exe	1408	TCP	49665		0.0.0.0			0.0.0.0	
22	svchost.exe	2536	UDP	5355	llmnr	::				Windows10
23	svchost.exe	7164	TCP	5040		192.168.56.1			0.0.0.0	
24	svchost.exe	7164	TCP	5040		10.0.1.100			0.0.0.0	
25	svchost.exe	1200	TCP	3389	ms-wbt-server	10.0.1.100	50478		10.0.2.200	

Figure 8: cports.csv in libreoffice

5.4 driveletterview

```
================================================
Drive Letter      : C:\
Drive Type        : Local Hardware
Drive Name        : VBOX HARDDISK
Drive Description : Disk drive
Connected         : Yes
Instance ID       : SCSI\Disk&Ven_VBOX&Prod_HARDDISK\4&2617aeae&0&000000
Device Path       : \Device\HarddiskVolume2
Physical Drive Name: \\?\PhysicalDrive0
Bus Type          : SATA
Last Update Time  :
File System       : NTFS
Volume Name       :
Volume Serial Number: EA39BDA6
Free Space        : 37.32 GB
Total Size        : 58.10 GB
% Free Space      : 64.2%
Cluster Size      : 4096
Product String    : VBOX HARDDISK
Product Revision  : 1.0
Vendor String     :
Serial Number     : VB206f4411-1eb127c2
================================================
```

```
[...]

================================================
Drive Letter      : H:\
Drive Type        : Local Hardware
Drive Name        : Philips USB Flash Drive USB Device
Drive Description : Disk drive
Connected         : Yes
Instance ID       : USBSTOR\Disk&Ven_Philips&Prod_USB_Flash_Drive&Rev_PMAP\0708533EB31C2846&0
Device Path       : \Device\HarddiskVolume4
Physical Drive Name: \\?\PhysicalDrive1
Bus Type          : USB
Last Update Time  :
File System       : FAT32
Volume Name       : LDFWIN
Volume Serial Number: 9CF6F1D7
Free Space        : 1.72 GB
Total Size        : 3.72 GB
% Free Space      : 46.2%
Cluster Size      : 4096
Product String    : USB Flash Drive
Product Revision  : PMAP
Vendor String     : Philips
Serial Number     : 027804865030
================================================
```

If you detect later multiple Windows installations on different devices it will be easier to reassemble them in your forensic software with this knowledge!

5.5 edd

```
Encrypted Disk Detector v2.1.1
Copyright (c) 2009-2017 Magnet Forensics Inc.
http://www.magnetforensics.com

* Checking physical drives on system... *

PhysicalDrive0, Partition 1 --- OEM ID: NTFS

PhysicalDrive0, Partition 2 --- OEM ID: NTFS

PhysicalDrive0, Partition 3 --- OEM ID: \\\\\\\\
PhysicalDrive0, Partition 3 might be an encrypted volume,
or contains a damaged boot sector.

PhysicalDrive1, Partition 1 ---       OEM ID: MSDOS5.0
PhysicalDrive1, Partition 1 --- Volume label: NO NAME

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: is located on PhysicalDrive0, Partition #2.
Drive D: is a CD-ROM/DVD device (#0).
Drive E: is located on PhysicalDrive0, Partition #3.
Drive F: appears to be a virtual disk
  - possibly a TrueCrypt or PGP encrypted volume
Drive G: appears to be a virtual disk
  - possibly a TrueCrypt or PGP encrypted volume
Drive H: is located on PhysicalDrive1, Partition #1.

* Completed checking logical volumes on system. *

* Now checking for running processes... *
```

```
* Completed checking running processes. *

*** Encrypted volumes and/or processes were detected by EDD. ***
```

Do you see which device is the decrypted virtual volume?

5.6 insideclipboard

```
================================================
Format ID         : 13
Format Name       : CF_UNICODETEXT
Handle Type       : Memory
Size              : 12
Index             : 1
================================================

================================================
Format ID         : 16
Format Name       : CF_LOCALE
Handle Type       : Memory
Size              : 4
Index             : 2
================================================

================================================
Format ID         : 1
Format Name       : CF_TEXT
Handle Type       : Memory
Size              : 6
Index             : 3
================================================

================================================
Format ID         : 7
Format Name       : CF_OEMTEXT
Handle Type       : Memory
Size              : 6
Index             : 4
================================================
```

In addition to that information the binary content of the clipboard is saved as backup.clp. You can reimport that file to insideclipboard and work with it.

5.7 ipconfig

Network configuration:

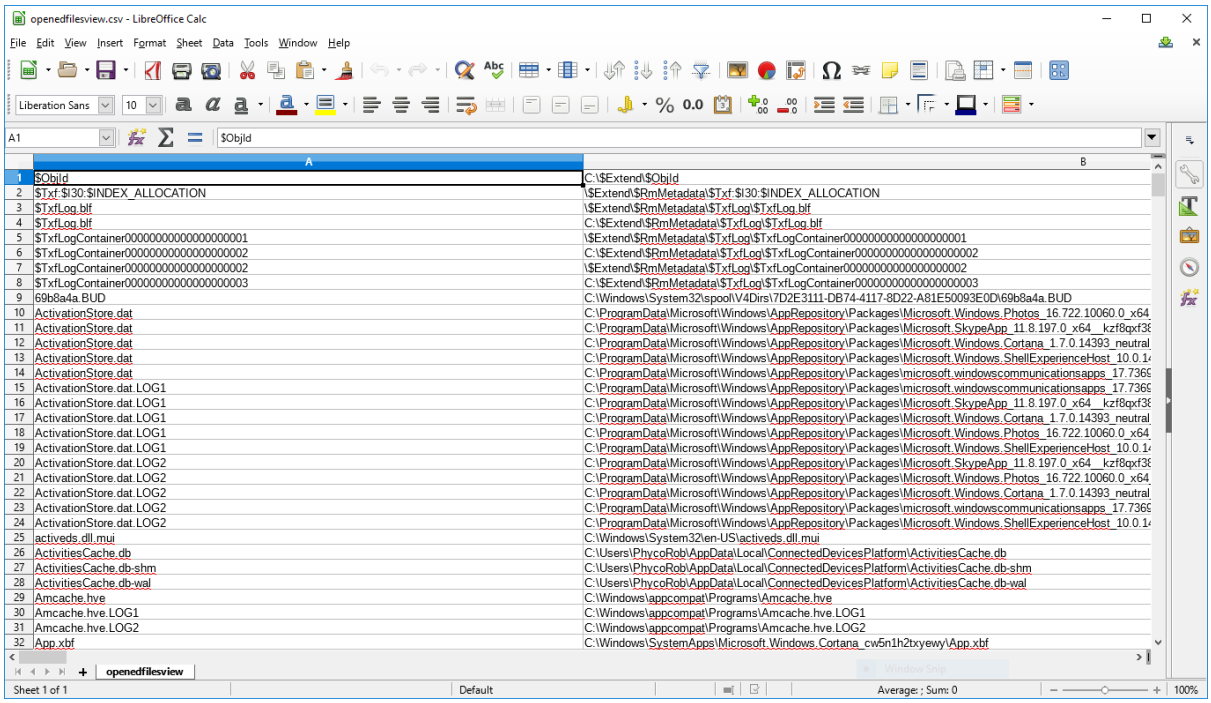
```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : Windows10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : local.domain

Ethernet adapter VirtualBox Host-Only Network:
```

```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-11
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::71e6:c0ad:e802:f2fb%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 352976935
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-DF-80-54-00-1F-C6-9B-96-82
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : local.domain
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-LM
   Physical Address. . . . . . . . . : 00-1F-C6-9B-96-82
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6841:a8cd:bb04:fdf1%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 04 December 2017 09:45:35
   Lease Expires . . . . . . . . . . : 08 December 2017 20:45:39
   Default Gateway . . . . . . . . . : 10.0.1.1
   DHCP Server . . . . . . . . . . . : 10.0.1.1
   DHCPv6 IAID . . . . . . . . . . . : 184557510
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-DF-80-54-00-1F-C6-9B-96-82
   DNS Servers . . . . . . . . . . . : 10.0.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter WLAN:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
   Physical Address. . . . . . . . . : A4-34-D9-2C-A3-1C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter LAN-Verbindung* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : A4-34-D9-2C-A3-1D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:78cf:1831:162b:f5ff:fe9b(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1831:162b:f5ff:fe9b%10(Preferred)
   Default Gateway . . . . . . . . . : ::
   DHCPv6 IAID . . . . . . . . . . . : 268435456
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-DF-80-54-00-1F-C6-9B-96-82
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

DNS cache:

```
Windows IP Configuration

    safebrowsing.googleapis.com
    ----------------------------------------
    Record Name . . . . . : safebrowsing.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 52
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 216.58.205.234


    stats.ciphershed.org
    ----------------------------------------
    Record Name . . . . . : stats.ciphershed.org
    Record Type . . . . . : 5
    Time To Live  . . . . : 958
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : ciphershed.org


    Record Name . . . . . : ciphershed.org
    Record Type . . . . . : 1
    Time To Live  . . . . : 958
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 31.171.246.15


    230.21.217.172.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 230.21.217.172.in-addr.arpa
    Record Type . . . . . : 12
    Time To Live  . . . . : 7700
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : fra16s13-in-f230.1e100.net


    cs9.wpc.v0cdn.net
    ----------------------------------------
    Record Name . . . . . : cs9.wpc.v0cdn.net
    Record Type . . . . . : 28
    Time To Live  . . . . : 269
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2606:2800:133:206e:1315:22a5:2006:24fd


        [...]
```

5.8 openedfilesview



	A	B
1	$ObjId	C:\$Extend\$ObjId
2	$Txf:$I30:$INDEX_ALLOCATION	\$Extend\$RmMetadata\$Txf:$I30:$INDEX_ALLOCATION
3	$TxfLog.blf	\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf
4	$TxfLog.blf	C:\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf
5	$TxfLogContainer00000000000000000001	\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
6	$TxfLogContainer00000000000000000002	C:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002
7	$TxfLogContainer00000000000000000002	\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002
8	$TxfLogContainer00000000000000000003	C:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000003
9	69b8a4a.BUD	C:\Windows\System32\spool\V4Dirs\7D2E3111-DB74-4117-8D22-A81E50093E0D\69b8a4a.BUD
10	ActivationStore.dat	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Photos_16.722.10060.0_x64
11	ActivationStore.dat	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_11.8.197.0_x64__kzf8qxf3
12	ActivationStore.dat	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.7.0.14393_neutral
13	ActivationStore.dat	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.1
14	ActivationStore.dat	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\microsoft.windowscommunicationsapps_17.736
15	ActivationStore.dat.LOG1	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\microsoft.windowscommunicationsapps_17.736
16	ActivationStore.dat.LOG1	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_11.8.197.0_x64__kzf8qxf3
17	ActivationStore.dat.LOG1	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.7.0.14393_neutral
18	ActivationStore.dat.LOG1	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Photos_16.722.10060.0_x64
19	ActivationStore.dat.LOG1	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.1
20	ActivationStore.dat.LOG2	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_11.8.197.0_x64__kzf8qxf3
21	ActivationStore.dat.LOG2	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Photos_16.722.10060.0_x64
22	ActivationStore.dat.LOG2	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.7.0.14393_neutral
23	ActivationStore.dat.LOG2	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\microsoft.windowscommunicationsapps_17.736
24	ActivationStore.dat.LOG2	C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.1
25	activeds.dll.mui	C:\Windows\System32\en-US\activeds.dll.mui
26	ActivitiesCache.db	C:\Users\PhycoRob\AppData\Local\ConnectedDevicesPlatform\ActivitiesCache.db
27	ActivitiesCache.db-shm	C:\Users\PhycoRob\AppData\Local\ConnectedDevicesPlatform\ActivitiesCache.db-shm
28	ActivitiesCache.db-wal	C:\Users\PhycoRob\AppData\Local\ConnectedDevicesPlatform\ActivitiesCache.db-wal
29	Amcache.hve	C:\Windows\appcompat\Programs\Amcache.hve
30	Amcache.hve.LOG1	C:\Windows\appcompat\Programs\Amcache.hve.LOG1
31	Amcache.hve.LOG2	C:\Windows\appcompat\Programs\Amcache.hve.LOG2
32	App.xbf	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\App.xbf

Figure 9: openedfilesview.csv in libreoffice

5.9 pslist

```
Process information for DESKTOP-QLJBPOF:

Name                                 Pid Pri Thd  Hnd      VM      WS    Priv
Idle                                   0   0   1    0      64       4       0
  System                               4   8 125  897    3480      20     128
    smss                             284  11   2   51 2147490076     276     368
    Memory Compression              1864   8  28    0   65408   34976     164
csrss                                368  13   9  312 2147535920    1532    1200
wininit                              444  13   1   89 2147529216     656     924
  services                           536   9   5  266 2147514204    4536    2856
    svchost                          336   8  28  585 2147609080   10692    8008
    VBoxService                      608   8  10  186   73320    2752    2372
    svchost                          632   8  22  732 2147579304   12192    7292
      TiWorker                       200   8   6  147 2147543468   10840    3732
      RuntimeBroker                  232   8  14  488 2147660200   22464   10304
      WmiPrvSE                      1604   8   9  157 2147523156    7920    2248
      dllhost                       2124   8   2  124 2147552464    8888    1584
      dllhost                       2432   8   5  232 2147589920   14060    2612
      smartscreen                   2700   8   9  170 2181130296   13744    8168
      Microsoft.Photos              2880   8  19  593   666480   34316   21452
      ShellExperienceHost           3172   8  34  986 2147796316   47092   21836
      SearchUI                      3316   8  30  844 2181652776   55936   34860
      ApplicationFrameHost          3512   8   5  377 2147632636   16600   10560
      SkypeHost                     3588   8  46 1074   287116    1848   27924
      InstallAgent                  4820   8   1  126 2147553944     924    1452
      InstallAgentUserBroker        4848   8   2  118 2147544720    1732    1716
      WmiPrvSE                      5280   8  11  285 2147541044   13932    5108
      SettingSyncHost               5384   6   4  471 2147628844     948    6896
      HxMail                        5392   8  47  970 2147889552   59172   21748
      HxTsr                         5944   8   8  322 2147598244   21608    4848
    svchost                          672   8  11  748 2147540340    6728    4656
```

```
    svchost                      852   8  60 2056 2147744048   33944   27504
      taskhostw                 2240   8  14  348 2147611116    6860    5800
      sihost                    3020   8  10  532 2147625228   14696    5824
    svchost                      864   8  22  484 2147608084   10980   14068
    atiesrxx                     896   8   4  115    26448     540     884
      atieclxx                  1036   8   8  172   100884    2476    2108
    svchost                      952   8  15  556 2151846564   36296   38532
      WUDFHost                  4040   8   8  266 2147534424    8104    1928
    svchost                     1000   8  14  531 2147564516   10200   11920
    svchost                     1108   8  17  498 2147581472    4252    5376
    svchost                     1176   8   9  223 2147535896    5076    2356
      audiodg                   2036   8   6  140 2147530660   10596    5988
    RtkAudioService64           1284   8   2  126    66812    1288    1640
    svchost                     1360   8  13  302 2147548664    2204    3068
    svchost                     1452   8   7  270 2147546636    2492    3960
    spoolsv                     1552   8   8  381 2147550280    2096    5088
    AERTSr64                    1724   8   2   44    15120     440     528
    svchost                     1732   8  13  367 2147603212   12044    5252
    SynTPEnhService             1792   8   3  198    23520     760     948
      SynTPEnh                  3004  10   5  311   108872    2136    3360
    MsMpEng                     1948   8  27  914 2147977364   82312  118272
    svchost                     1956   8   8  223 2147579036   11804    6068
    svchost                     2052   8   4  102 2147524052    6588    1732
    svchost                     2720   8   7  175 2147528600    1140    1700
    TrustedInstaller            2780   8   7  104 2147516940    6508    1736
    NisSrv                      2816   8   4  171 2147541168    2144    4028
    svchost                     3048   8   9  601 2147653624   16980    7540
    SearchIndexer               3272   8  14  592 2147737264    8904   25744
  lsass                          544   9   7  826 2147534536    5700    3936
csrss                            456  13  10  405 2147553216    2244    1328
winlogon                         512  13   5  197 2147542920    2960    1980
  dwm                            780  13  12  476 2147689408   53836   37840
explorer                        2288   8  88 2590 2148044844   93712   88356
  cmd                             92   8   1   39 2147505376    3700    1852
    pslist_v14_x64              3184  13   2  170    89280    7236    2368
    conhost                     5444   8   3  109 2147578564   12280    5048
  RAVBg64                       2612   8   3  132   106244    2532    3892
  cmd                           3084   8   1   36 2147503192    2408    1564
    conhost                     2548   8   5  168 2147586080   13940    5492
  MSASCuiL                      3860   8   3  218 2147590028    3832    3348
  VBoxTray                      3900   8  10  216   104860    2156    2220
  OneDrive                      4152   8  13  463   159700    6688    6132
  cmd                           5612   8   1   40 2147505864    3148    1788
    conhost                     2264   8   3  108 2147578580   11524    5052
SynTPHelper                     2620  10   1   48    48948     852     880
MpCmdRun                        2696   8   5  142 2147520820    4228    2136
soffice                         4232   8   1  140    83304    1212    1560
  soffice.bin                   4252   8  14  425   444136   21728   39216
    splwow64                    6108   8   4  175 2147573816    1960    3896
```

5.10 systeminfo

```
Host Name:                 DESKTOP-QLJBPOF
OS Name:                   Microsoft Windows 10 Education
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00328-00201-34110-AA207
Original Install Date:     06.09.2016, 00.29.35
System Boot Time:          08.12.2017, 10.48.22
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
```

```
                           [01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~2592 Mhz
BIOS Version:              innotek GmbH VirtualBox, 01.12.2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             no;Norwegian (Bokmal)
Input Locale:              no;Norwegian (Bokmal)
Time Zone:                 (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Total Physical Memory:     2048 MB
Available Physical Memory: 1096 MB
Virtual Memory: Max Size:  2688 MB
Virtual Memory: Available: 1534 MB
Virtual Memory: In Use:    1154 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-QLJBPOF
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB3176936
                           [02]: KB3199986
                           [03]: KB3201860
                           [04]: KB3197954
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Desktop Adapter
                                 Connection Name: Ethernet 2
                                 Status:          Media disconnected
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

By the way the timezone is there!

5.11 usbdeview

```
================================================
Device Name       : 0000.0012.0002.003.000.000.000.000.000
Description       : USB Video Device
Device Type       : Video
Connected         : No
Safe To Unplug    : Yes
Disabled          : No
USB Hub           : No
Drive Letter      :
Serial Number     :
Created Date      : 29.10.2016 17.41.56
Last Plug/Unplug Date: 06.09.2016 00.21.43
VendorID          : 090c
ProductID         : 37bc
Firmware Revision : 0.02
USB Class         : 0e
USB SubClass      : 03
USB Protocol      : 00
Hub / Port        :
Computer Name     : DESKTOP-QLJBPOF
Vendor Name       :
Product Name      :
ParentId Prefix   :
Service Name      : usbvideo
Service Description: @usbvideo.inf,%USBVideo.SvcDesc%;USB Video Device (WDM)
Driver Filename   : usbvideo.sys
Device Class      :
Device Mfg        : Microsoft
Friendly Name     : HP Webcam-101
Power             :
USB Version       :
Driver Description: USB Video Device
Driver Version    : 10.0.14393.82
Driver InfSection : USBVideo
Driver InfPath    : usbvideo.inf
Instance ID       : USB\VID_090C&PID_37BC&MI_00\6&321285bd&0&0000
Capabilities      : Removable, SilentInstall, SurpriseRemovalOK
```

```
================================================

[...]

================================================
Device Name       : USB Flash Drive
Description       : Philips USB Flash Drive USB Device
Device Type       : Mass Storage
Connected         : Yes
Safe To Unplug    : Yes
Disabled          : No
USB Hub           : No
Drive Letter      : H:
Serial Number     : 0708533EB31C2846
Created Date      : 08.12.2017 11.23.49
Last Plug/Unplug Date: 08.12.2017 11.23.49
VendorID          : 13fe
ProductID         : 4100
Firmware Revision : 1.00
USB Class         : 08
USB SubClass      : 06
USB Protocol      : 50
Hub / Port        :
Computer Name     : DESKTOP-QLJBPOF
Vendor Name       :
Product Name      :
ParentId Prefix   :
Service Name      : USBSTOR
Service Description: @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver
Driver Filename   : USBSTOR.SYS
Device Class      :
Device Mfg        : Compatible USB storage device
Friendly Name     :
Power             : 200 mA
USB Version       : 2.00
Driver Description: USB Mass Storage Device
Driver Version    : 10.0.14393.0
Driver InfSection : USBSTOR_BULK.NT
Driver InfPath    : usbstor.inf
Instance ID       : USB\VID_13FE&PID_4100\0708533EB31C2846
Capabilities      : Removable, UniqueID, SurpriseRemovalOK
================================================
```

You have to search for all external devices that are not allready in your box!

6 The source code

```
@echo off
:: FILE:          ldfw-short.bat
:: DESCRIPTION:   Life Digital Forensics for Windows (short version)
:: USAGE:         Just execute with admin rights
:: OPTIONS:       None
:: EXIT STATES:   Microsoft Windows defaults
:: REQUIREMENTS:  Windows and the tools folder
:: AUTHOR:        Anonymous ID 193
:: VERSION:       1.0
:: CREATED:       08.12.2017
:: COPYRIGHT (C): 2017 - Mr. "193"
:: LICENSE:       GPL3 (http://www.gnu.org/licenses/)
:: WARRANTY:      WITHOUT ANY WARRANTY
:: TODO:          The batch journey ends here!
:: HISTORY:       1.0 - Mr. "193" - Initial (for the peer reviewer eyes only) release

rem Empty evil PATH variable
set PATH=

rem Determine as what this script was startet
C:\Windows\System32\net.exe FILE 1>NUL 2>NUL
if '%errorlevel%' == '0' (
```

```
  set mode=admin
) else (
  set mode=user
)

rem Change to the device and then directory of the script
%~d0
cd "%~p0"

rem Create a target directory
set DAY=%DATE:~0,2%
set MONTH=%DATE:~3,2%
set YEAR=%DATE:~6%
set HOUR=%TIME:~0,2%
set HOUR=%HOUR: =0%
set MIN=%TIME:~3,2%
set SEC=%TIME:~6,2%
set TARGET=%YEAR%%MONTH%%DAY%%HOUR%%MIN%%SEC%
mkdir %TARGET%

rem Log start date and time
call :tee "########################################################################"
call :tee "# %~nx0 (Live Digital Forensics for Windows [short version])"
call :tee "#   startet on %DATE% at %TIME%"
call :tee "########################################################################"

rem Do not give away valuable time. Safe caches immediately!
call :exec_redir ipconfig-displaydns, "C:\Windows\System32\ipconfig.exe /displaydns"
call :tee "------------------------------------------------------------------------"

call :exec_redir arp-a, "C:\Windows\System32\ARP.EXE -a"
call :tee "------------------------------------------------------------------------"

rem Detect bitness
set Bitness=64
if %PROCESSOR_ARCHITECTURE% == x86 (
  if not defined ProgrammW6432 set Bitness=32
)
call :tee "Operation System arch is %Bitness% bit."

rem Read case data from keyboard and write to stdout and file
echo Please enter case info...
set /p caseNumber=Case number:
set /p description=Description:
set /p evidenceNumber=Evidence number:
set /p examinerName=Examiner name:
set /p notes=Notes:
set /p currentTime=Current time:

call :tee "########################################################################"
call :tee "# Informations about the case"
call :tee "#-----------------------------------------------------------------------"
call :tee "# Case number:     %caseNumber%"
call :tee "# Description:     %description%"
call :tee "# Evidence number: %evidenceNumber%"
call :tee "# Examiner name:   %examinerName%"
call :tee "# Notes:           %notes%"
call :tee "# Current Time:    %currentTime%"
call :tee "########################################################################"

rem Gather information that is difficult to get out of a ram capture
call :exec_redir systeminfo, "C:\Windows\System32\systeminfo.exe"
call :tee "------------------------------------------------------------------------"

rem Skip winpmem if we are only a simple user
if %mode% == user goto COMMANDS

rem Capture ram or do the commands (not and!)
echo Do you want to capture the memory now? [y/n]
set /p memory=
if %memory% NEQ y goto COMMANDS

:: needs admin rights!
call :tee "Capture memory was chosen..."
call :tee "... skipping insideclipboard, pslist, cports and openedfilesview!"
call :tee "------------------------------------------------------------------------"
call :exec_direct winpmem, "tools\winpmem_1.6.2.exe %TARGET%\memory_dump.raw", memory_dump.raw
call :tee "------------------------------------------------------------------------"
goto CONTINUE

:COMMANDS
call :tee "Capture memory was NOT or could NOT be chosen..."
call :tee "... skipping winpmem!"
call :tee "------------------------------------------------------------------------"
call :exec_direct insideclipboard-1, "tools\InsideClipboard_v115.exe /stext %TARGET%\insideclipboard.txt", insideclipboard.txt
call :tee "------------------------------------------------------------------------"
```

```
call :exec_direct insideclipboard-2, "tools\InsideClipboard_v115.exe /saveclp %TARGET%\backup.clp", backup.clp
call :tee "------------------------------------------------------------------------"

if %Bitness% == 64 (
  call :exec_redir pslist-t, "tools\pslist_v14_x64.exe -t -accepteula"
) else (
  call :exec_redir pslist-t, "tools\pslist_v14_x86.exe -t -accepteula"
)
call :tee "------------------------------------------------------------------------"

if %Bitness% == 64 (
  call :exec_direct cports, "tools\cports_v236_x64.exe /scomma %TARGET%\cports.csv", cports.csv
) else (
  call :exec_direct cports, "tools\cports_v236_x86.exe /scomma %TARGET%\cports.csv", cports.csv
)
call :tee "------------------------------------------------------------------------"

rem Skip openedfilesview if we are only a simple user
if %mode% == user goto CONTINUE

if %Bitness% == 64 (
  :: needs admin rights!
  call :exec_direct openedfilesview, "tools\OpenedFilesView_v170_x64.exe /scomma %TARGET%\openedfilesview.csv", openedfilesview.csv
) else (
  :: needs admin rights!
  call :exec_direct openedfilesview, "tools\OpenedFilesView_v170_x86.exe /scomma %TARGET%\openedfilesview.csv", openedfilesview.csv
)
  call :tee "------------------------------------------------------------------------"
:CONTINUE

rem Do the rest
call :exec_redir ipconfig-all, "C:\Windows\System32\ipconfig.exe /all"
call :tee "------------------------------------------------------------------------"

if %Bitness% == 64 (
  call :exec_direct usbdeview, "tools\USBDeview_v272_x64.exe /stext %TARGET%\usbdeview.txt", usbdeview.txt
) else (
  call :exec_direct usbdeview, "tools\USBDeview_v272_x86.exe /stext %TARGET%\usbdeview.txt", usbdeview.txt
)
call :tee "------------------------------------------------------------------------"

if %Bitness% == 64 (
  call :exec_direct driveletterview, "tools\DriveLetterView_v146_x64.exe /stext %TARGET%\driveletterview.txt", driveletterview.txt
) else (
  call :exec_direct driveletterview, "tools\DriveLetterView_v146_x86.exe /stext %TARGET%\driveletterview.txt", driveletterview.txt
)
call :tee "------------------------------------------------------------------------"

rem Detect encryption
if %mode% == admin (
  :: needs admin rights!
  call :exec_redir edd, "tools\EDD_v211.exe /batch /accepteula"
)

C:\Windows\System32\findstr.exe /C:"*** Encrypted volumes and/or processes were detected by EDD. ***" "%TARGET%\edd.txt" 1>NUL 2>NUL
if '%errorlevel%' == '0' (
  echo esc[91mALERT !!! Do not shutdown this system !!! ALERTecs[Om
  echo esc[91mENCRYPTION !!! Call for an expert !!! ENCRYPTIONesc[Om
  echo ALERT !!! Do not shutdown this system !!! ALERT >> "%TARGET%\ldfw-short.log"
  echo ENCRYPTION !!! Call for an expert !!! ENCRYPTION >> "%TARGET%\ldfw-short.log"
)

rem Log end date and time
call :tee "########################################################################"
call :tee "# %~nx0 (Live Digital Forensics for Windows [short version])"
call :tee "#   finished on %DATE% at %TIME%"
call :tee "########################################################################"

rem Keep window open unless return
set /p close=Press enter to close window

exit /b %ERRORLEVEL%

::
:: functions:
::

:tee
:: text with spaces surrounded by "" to write to stdout and file
echo %~1
echo %~1 >> "%TARGET%\ldfw-short.log"
exit /b 0

:: :execute
:exec_redir
:: %1 = filename compatible version of command incl. params
:: %~2 = command incl. spaces and params sourrounded by ""
```

```
call :tee "execution of %1 startet on %DATE% at %TIME%"
%~2 > "%TARGET%\%1.txt"
call :tee "output was written to %TARGET%\%1.txt"
call :tee "execution of %1 finished on %DATE% at %TIME%"
exit /b 0

:exec_direct
:: %1 = filename compatible version of command incl. params
:: %~2 = command incl. spaces and params sourrounded by ""
:: %3 = result file name
call :tee "execution of %1 startet on %DATE% at %TIME%"
%~2
call :tee "output was written to %TARGET%\%3"
call :tee "execution of %1 finished on %DATE% at %TIME%"
exit /b 0
```