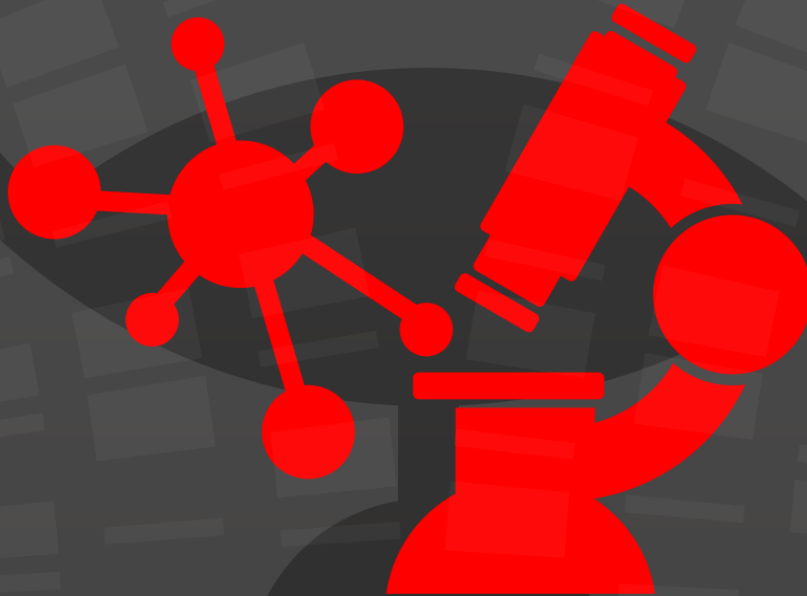




SECUPERTS
THE SECURITY EXPERTS



FORENSIC SYSTEM

Table of Contents

1 What is the SecuPerts-Forensic-System	4
1.1 What does it not do?.....	4
1.2 Which legal aspects have to be considered?.....	4
2 Startup process	4
2.1 Accessing the BIOS.....	4
2.2 Change boot order.....	5
2.3 Start from UEFI PCs.....	5
2.4 SecuPerts-Forensic-System does not boot.....	7
3 Forensic-System boot menu	7
3.1 Boot menu layout.....	8
3.2 Safe startup.....	8
4 Start screen	9
4.1 Upper assistant bar.....	10
4.2 Assistant categories.....	10
4.3 Startmenu programs.....	10
4.4 Updates.....	11
5 Forensic-System tools	11
5.1 Hard disk forensic.....	12
5.1.1 Recover files	12
5.1.2 Access volume shadow snapshots	12
5.1.3 Detect malicious software	14
5.1.4 Sort recovered files	16
5.2 Accessing caches storage anf history.....	16
5.2.1 Accessing firefox profiles	16
5.2.2 Windows-Jumplists	16
5.2.3 Recover Outlook-Mailboxes	17
5.2.4 Browser and chat history	17
5.3 Network forensic.....	18
5.3.1 OpenVAS	18
5.3.2 Wireshark	20
5.3.3 Zenmap	22
5.3.4 Accesspoint	23
5.4 Block device operations.....	24
5.4.1 Storage device image	24
5.4.2 Clone hard drive	25
5.4.3 Open image in VM	25

5.4.4 Delete drive	26
6 Useful menu and command prompt tools	26
6.1 SQLite Database-Browser.....	26
6.2 Skype-Logs.....	27
6.3 Connect network drives.....	27
6.4 Fred Forensic Registry Editor.....	27
7 Password tools	28
7.1 John the Ripper.....	28
7.2 Ophcrack.....	29
7.3 Ncrack.....	29
8 Linux-System	29
8.1 File system.....	30
8.2 Mount drives.....	30

1 What is the SecuPerts-Forensic-System

The SecuPerts-Forensic-System is a separated operating system which can either be run from DVD or an USB flash drive. This method does not alter your own operating system, which allows you to perform forensic actions undetected. You can also find the reason your windows might not start, whether it is caused by malicious software or hardware errors. Another feature of the SecuPerts-Forensic-System is the analysis of network traffic and infected network devices.

1.1 What does it not do?

It is not a "hacking-tool", but rather serves the purpose of analyzing systems and devices in your own network. The power of password crackers is knowingly held down and optimized for legal usage. You can for example use the SecuPerts-Forensic-System to detect weak passwords from co-workers (so stronger passwords can be chosen), but the possibility for deep "brute-force-attacks" is limited.

1.2 Which legal aspects have to be considered?

The SecuPerts-Forensic-System serves the purpose of analyzing systems and devices in your own network. If used in a company network there are labor- and IT-laws which have to be considered. The industrial council eventually needs to be informed. It can also be used to raise awareness for the problems of unencrypted storage mediums or quickly formatted hard disks.

The SecuPerts-Forensic-System has been developed to check the security and workload of the users own data network. With accepting the terms of use and disclaimer the user is obliged to use the software only within the law, especially within data safety regulations. This means to only use the SecuPerts-Forensic-System only with consent of all network users within a network.

2 Startup process

The SecuPerts-Forensic-System boots as an independent operating system and generally has to be started before the windows boot loader takes action. You received the SecuPerts-Forensic-System either as a DVD or as an USB-Stick. If you have bought a DVD, an USB-Stick can be created at another bootable computer. There is an EXE-file located inside the root folder of the DVD for this purpose. Ideally the manufacturer of your computer has already configured the BIOS or UEFI, so bootable devices can immediately be recognized.

If this is not the case, you may have to alter the boot order of your system. Depending on your device there are different methods. You usually have to press one of the following buttons while booting (will be displayed while booting): F2, F8, F9, F10, F11, F12, Alt, Esc or Tab. The desired device can be chosen in the next step.

2.1 Accessing the BIOS

Start the computer's BIOS immediately after booting your PC. The method for starting it differs depending on the model of the motherboard. The required key combination will usually appear during the startup process. Common keyboard shortcuts that need to be pressed directly after system startup are Delete, F2, F10 and Esc. Netbooks usually require an additional press of Ctrl and Alt. If none of these combinations work, you should do a Google search with the term 'BIOS access for your mainboard '.

2.2 Change boot order

The BIOS interface usually has a button named 'Boot', 'Boot Settings' or 'Boot Options'. You may have to go to advanced options first. After you found the correct option, you can select your DVD or USB drive as the first boot device.

2.3 Start from UEFI PCs

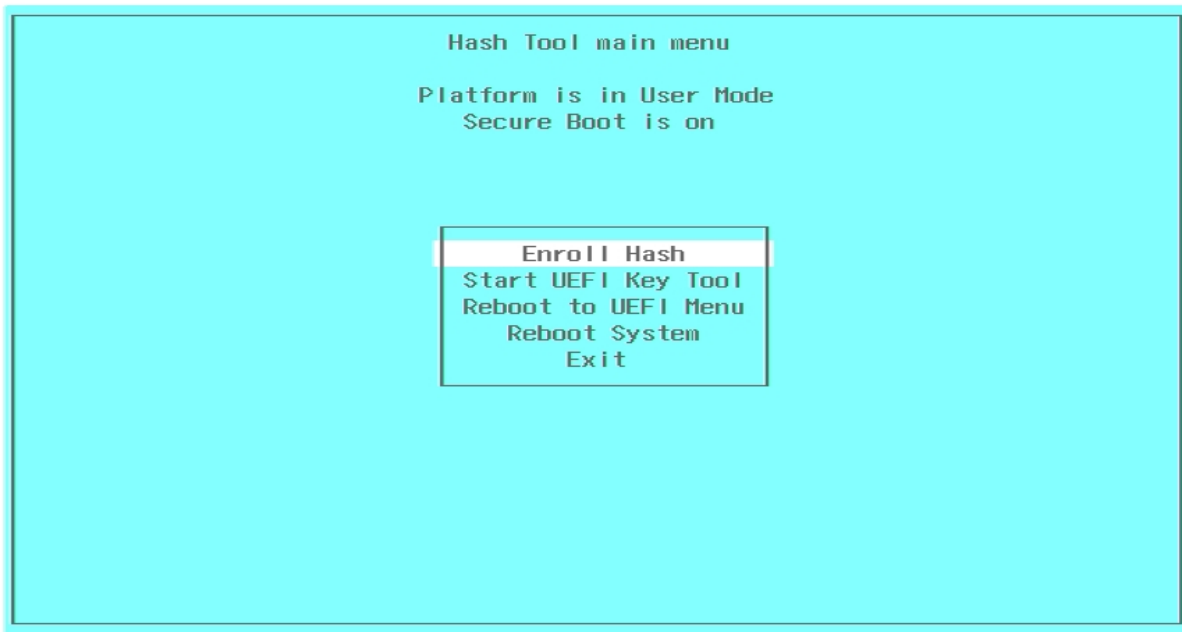
Newer versions of Windows (Windows 8 and above) usually use the BIOS successor UEFI ("Universal Extensible Firmware Interface") in combination with "Secure Boot". SecuPerts-Forensic-System also uses such a signed loader. If the setup does not start automatically you can start it manually from windows. Open the "Modern UI" in the PC settings. Then, click on "General" and "Restart Now". In the appearing menu select "Using a Device" as your setup media.

This starts the boot loader Gummiboot, in which you can select the boot of the forensic-system (the entry "UEFI Default Loader" starts windows). With an activated "Secure Boot" you will receive the following warning after the first start:



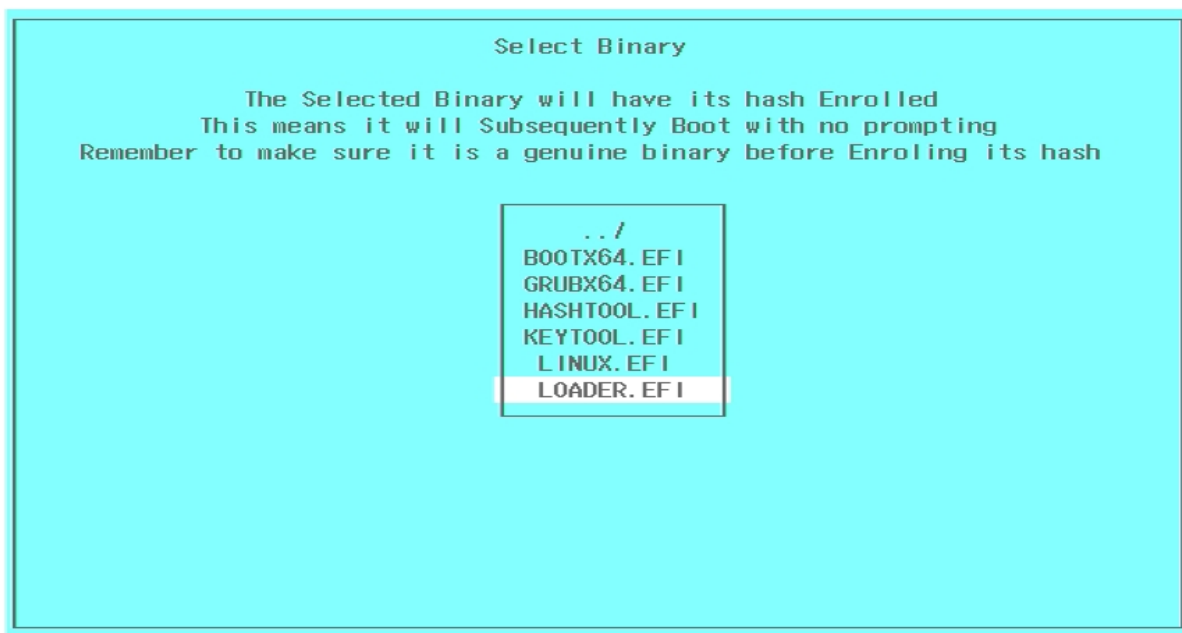
Confirm with "OK" to proceed to the hash tool

Confirm with "OK", which leads you to the hash tool. Select "Enroll Hash":



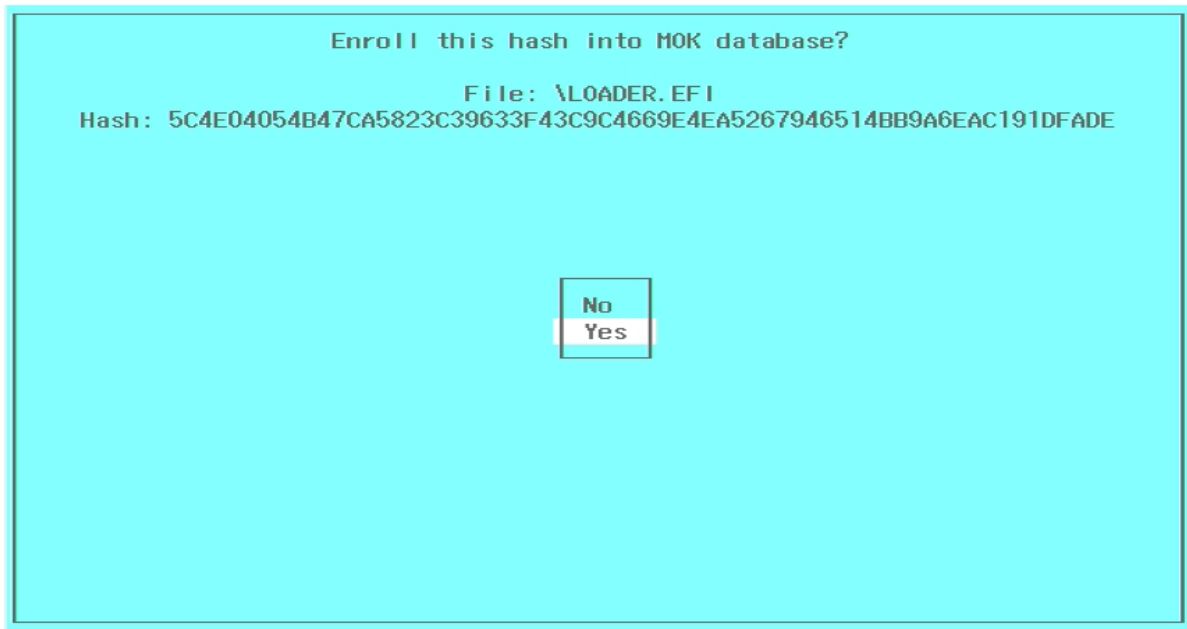
Select "Enroll Hash"

In the following "Select Binary" list select the file "LOADER.EFI":



First select LOADER.EFI, later LINUX.EFI

Now you will be asked, if the hash value should be added to the allowed list:



Answer all messages with YES

Answer all messages with YES and repeat this process with the "LINUX.EFI" file. Then leave the hash tool and select the start entry in the SecuPerts-Forensic-System boot menu.

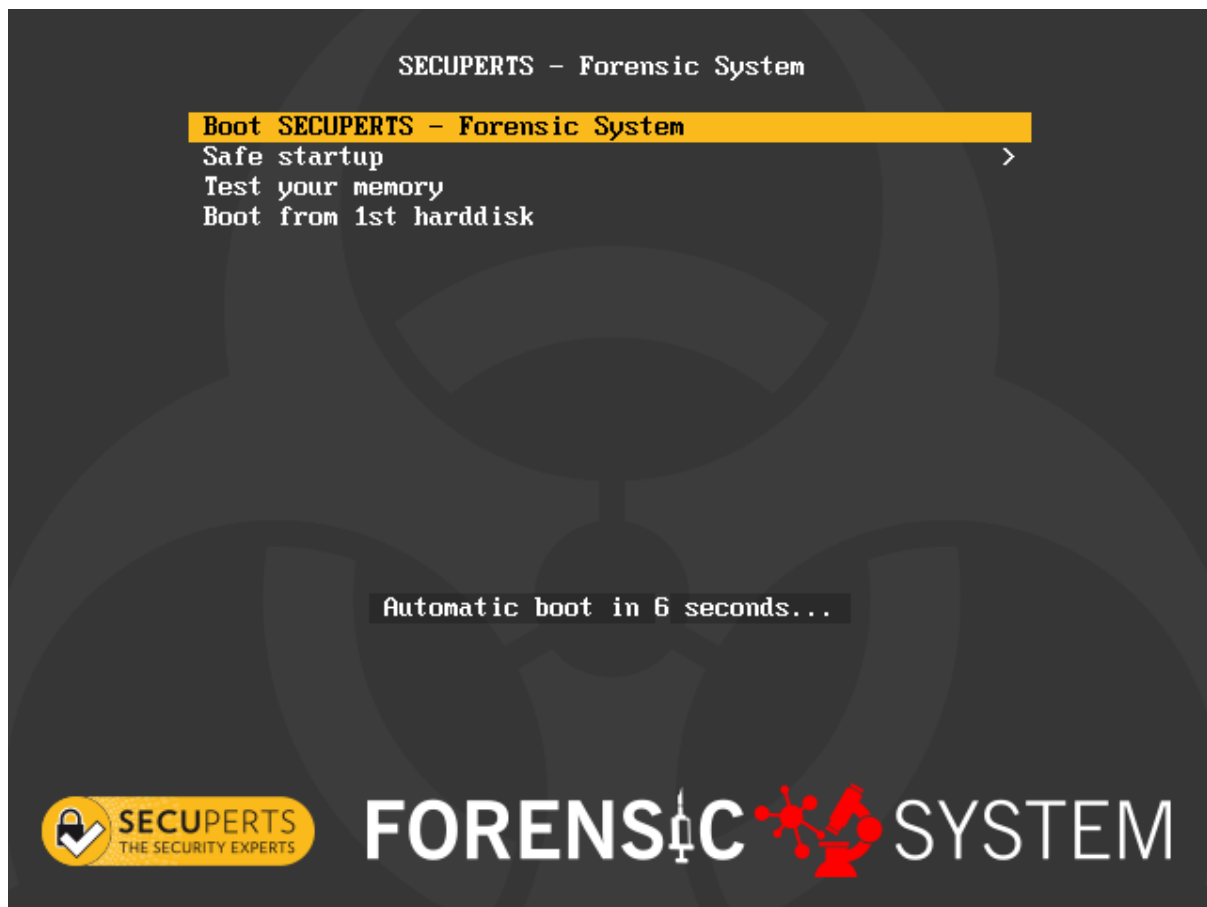
2.4 SecuPerts-Forensic-System does not boot

The SecuPerts-Forensic-System is based on the Linux system 'LessLinux'. It supports a variety of hardware configurations. In rare cases it may happen that just your system is not supported. You can try those fixes if you are affected:

- Restart your PC in 'Legacy only mode. Users with Windows 8 or higher should reactivate 'UEFI only' after they are done
- Try to use the available boot parameters, which can be reached through 'Safe Start' in the SecuPerts-Forensic-System boot menu
- If booting from USB-Stick fails, you can create start-cd/dvd with the "boot.iso" file, which allows you to bump the start from a connected stick

3 Forensic-System boot menu

The SecuPerts-Forensic-System usually starts directly from the boot menu screen, either after confirming with the enter-key or automatically after 30 seconds have passed. In some cases extra parameters have to be altered. These can be accessed through the menu point "Safe startup".



Boot menu on BIOS-Systems

3.1 Boot menu layout

- **Boot SecuPerts-Forensic-System:** Directly starts the Forensic-System
- **Safe startup:** Alter different parameters for the system start
- **Boot from 1st hard disk:** Leave the boot menu and boot your normal operating system

You also can use the Tab-key (BIOS) or the E-key (UEFI) to start editing mode in the boot-command-prompt, where boot parameters can be changed. To confirm your selection of parameters press the Enter-key. You only have to do this if you had contact with our support.

3.2 Safe startup

- **Go back:** Closes parameter selection and returns to the boot menu.
- **Start with default settings:** System start without any changes.
- **Start SecuPerts-Forensic-System (default settings):** The same as starting from the boot menu.
- **Start SecuPerts-Forensic-System (no copy to RAM):** If your system does not have enough RAM you can use this option.
- **Start with safe settings:** Boots the system under consideration of possible driver problems.
- **Safe ACPI settings + VESA graphics 1024x768:** Boots the system with a resolution of 1024x768. It also affects the energy management. Use this option if you have any problems with your graphic drivers.
- **Safe ACPI settings + VESA graphics auto:** Boots the system with the most compatible resolution using the VESA protocol. It also affects the energy management.

- **Safe ACPI settings + Xorg graphics auto:** Boots the system with the most compatible resolution using the Xorg protocol. It also affects the energy management.
- **VESA graphics 1024x768:** Boots the system with a fixed resolution of 1024x768.
- **VESA graphics auto:** Boots the system with the most compatible resolution using the VESA protocol.
- **Allow remote access (VNC or SSH):** Here you can remote maintain your computer. This should only be used in a known environment.
- **Unsafe remote VNC + local GUI:** Allows you to see what is currently done at your computer.
- **Unsafe remote VNC + no local GUI:** Disables visual representation as if your graphic card would not be working anymore.
- **Reverse VNC + local GUI:** Allows remote maintenance in an own window. The target computer has to be set up for this.
- **Reverse VNC + no local GUI:** Allows remote maintenance in an own window. The target computer has to be set up for this. Disables visual representation as if your graphic card would not be working anymore.

The VNC-Remote-Access-Modes allow you to use the Tab-key to get to the editing mode of the boot. command-prompt, where changes to resolution, password and target computer can be made.

4 Start screen

After the system has successfully been started, you have to accept the license agreement. Now you should see the category tiles of the assistant inside a desktop environment. Additionally a task bar can be accessed, if you move your cursor to the bottom of the screen. It contains a start menu, several program-icons and a button do toggle, if opened windows should be shown. The desktop can be used to deposit files or shortcuts just like in windows. The programs inside the start menu can often be used to double check analysis. There are also additional features which are not shown inside the assistant.



Assistant of the Forensic-System

4.1 Upper assistant bar

The bar located in the upper part of the assistant offers fast access for often used functions:

- **Open help:** Open the manual
- **Start browser:** Perform research on the internet
- **Network settings:** Connect to a WLAN network or select other options
- **USB-Installation:** Install the Forensic-System on an USB-Stick. You can also re install with different settings on a bigger device
- **Minimize assistant:** Hides the assistant to the task bar, so you have more space to do your work

4.2 Assistant categories

The assistant is divided into four categories:

- **hard disk forensic:** This category contains programs which work with hard disk, data and directory operations. This includes the recovery of deleted files, access to volume shadow copies, detecting malicious software and sorting recovered files based on their meta data.
- **Access to cache and history:** Here you gain access to the temporary storage of several programs like web browsers, email databases from outlook as well as data and program histories from windows.
- **Network forensic:** Listen to network traffic, check what computers use your network for and detect vulnerable devices with OpenVAS. Additionally you can open a WLAN-Accesspoint to analyze network traffic caused by smartphones.
- **Block device options:** Here you can find tools to work on a block level, which ignores data systems and type of saved files. This allows you to create perfect copies of your hard disk. You can also create images, even from single partitions or damaged storage mediums. Qemu can create virtual machines from bootable windows images. The feature "delete safely" makes sure that a hard disk you want to give away is free of sensible data.

4.3 Startmenu programs

The start menu inside the task bar offers more programs every day task, data recovery, data backup and some games to entertain you during longer operations. Some of those programs have the same or similar functionality as programs from the assistant. In such a case it is advised to use the assistant programs first because their functionality is usually better explained.



Startmenu and desktop of the SecuPerts-Forensic-System

- **Accessories:** Access network shares, Archive Manager, Calculator, DB Browser for SQLite, File Manager, FileZilla, Install additional software, Install to USB drive, KeePassX, Midnight Commander, Mount CIFS or WebDAV shares, Mousepad, Screenshot, Share drives, Start VNC server, Terminal Emulator, TrueCrypt, Virtual Keyboard, WiFi Accesspoint
- **Games:** Chess. Five or More, Mahjonggm, Mines, Nibbles, Quardapassel, Robots, Swell Foop
- **Internet:** Email client, Instantbird (Messenger), Web Browser, Wicd Network Manager
- **Office:** AbiWord (Notepad), Document Viewer (for PDFs), Gnumeric Spreadsheet
- **Other Tools:** Bulk Rename, DB Browser for SQLite, Disk Usage Analyser, File manager with root privileges, FRED Registry Editor, GHex, GParted partitioning tool, Grsync, Log Out, PartImage, Root shell, Show hardware information, Shutdown, SSHD (remote access), TeamViewer, Thunar File Manager, VSS access, Xfce Terminal
- **Rescue Tools:** Check SMART, Clone hard disk, Convert disk to VM image, Create rescue image, Disk shredder, Find lost partitions, QPhotoRec, Reset password, Reset windows shell, Resotore lost files, Xfburn
- **Sound & Video:** Audacious, Audio Mixer, Brasero, Ristretto Image Viewer, VLC Media Player, Xfburn

4.4 Updates

The SecuPerts-Forensic-System checks for possible Updates on startup and after around 10 minutes. If you do not have an internet connection during this time you can use the tool "Accessories > Search for system updates" to manually check for updates. Smaller updates for compatibility and stability will be installed into the RAM of the running system and usually take less than one minute to download. Safety and driver updates require the SecuPerts-Forensic-System to be installed on an USB-stick. After the update has finished, you need to restart the system. An assistant will guide you through this whole process.

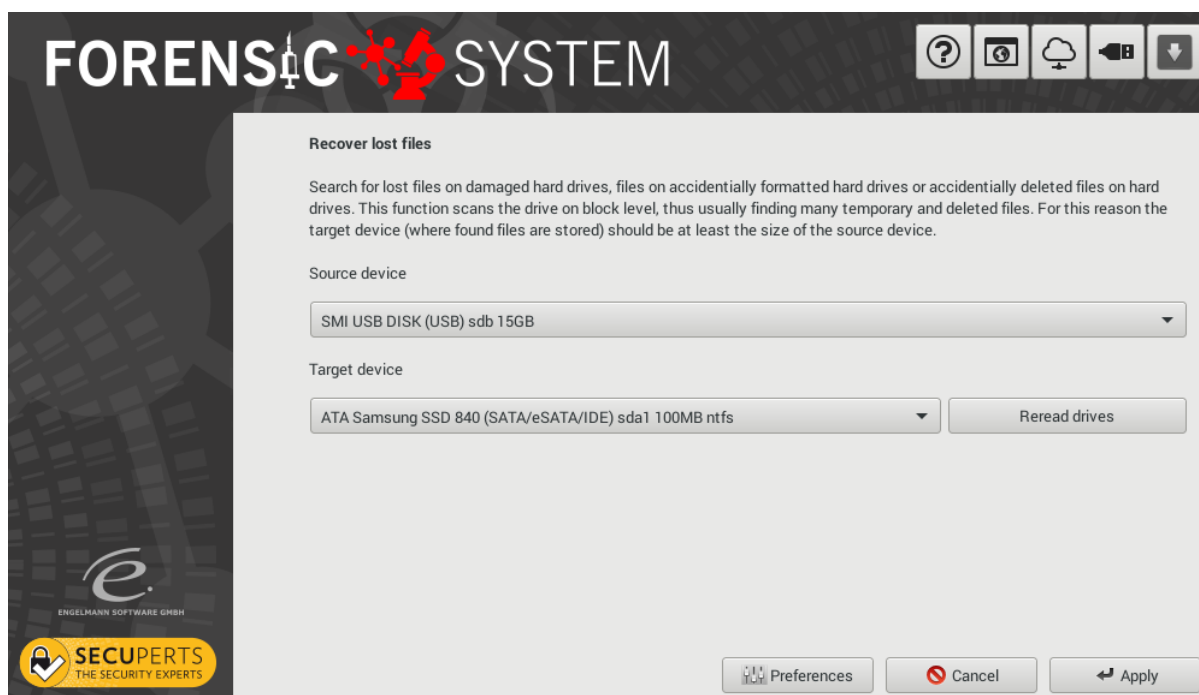
5 Forensic-System tools

5.1 Hard disk forensic

This category contains programs which work with hard disk, data and directory operations. This includes the recovery of deleted files, access to volume shadow copies, detecting malicious software and sorting recovered files based on their meta data.

5.1.1 Recover files

This function can help recover files, which were deleted accidentally or by formatting a hard disk/partition. The search can be performed on a partition or a complete hard disk. It usually ignores data systems to even find the most hidden files. If your hard disk has been used for a long time, found files could get as big as the selected source disk. In such cases the target disk should always be bigger than the source disk.



Files can also be recovered from damaged data systems

If you only want to scan a single partition, the target disk can be the same as the source disk, although this is not advised due to performance reasons. Searches on a whole disk require you to declare a different disk as the target disk. Damaged disks should be cloned to an undamaged one before further actions are performed. How long an analysis will take hardly depends on your disks transfer rate and the speed of your processor. Full disks usually achieve transfer speeds of around 10Mbyte/s, be aware that recovery of a terabyte disk could take more than one whole day.

The files will not be sorted automatically after the recovery has finished. They will strictly be named after their previous block address. The tool "Sort recovered files" allows you to sort the files through their meta data afterwards.

5.1.2 Access volume shadow snapshots

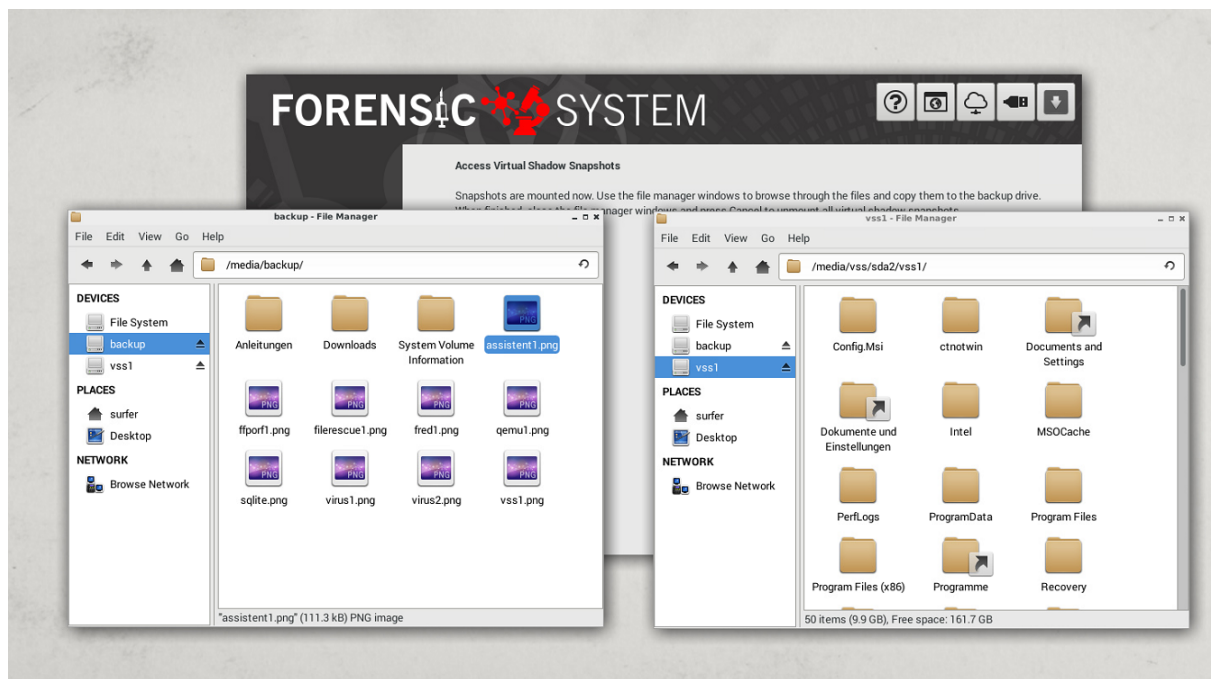
The NTFS file system allows creating so-called shadow snapshots. These are snapshots of the file system during the moment the snapshot is being created. Shadow snapshots are usually created if bigger changes to the system, like installing an update, are done. You can create them manually through the windows command prompt with "vssadmin". If you regularly update your system shadow

snapshots will be created around once a month and are saved for at least three months.



Before binding shadow snapshots, you have to choose a drive as a backup drive

After selecting "Access volume shadow snapshots" you initially have to declare a drive, which is mounted as writable, as a backup drive. All other NTFS drives will automatically mount shadow snapshots. If you want to compare current files and directories with a shadow snapshot, you have to mount the respective drive as read-only with the tool "Drives" inside the task bar. Now you can browse shadow snapshots like a mounted drive and recover files from them.



Drives with shadow snapshots will be mounted as read-only

After you are done searching a shadow snapshot click on "Cancel". This unmounts the shadow snapshot. Partitions, which have been mounted through the "Disks" tool have to be unmounted manually. File explorer windows, which are not needed anymore, can be closed or minimized.

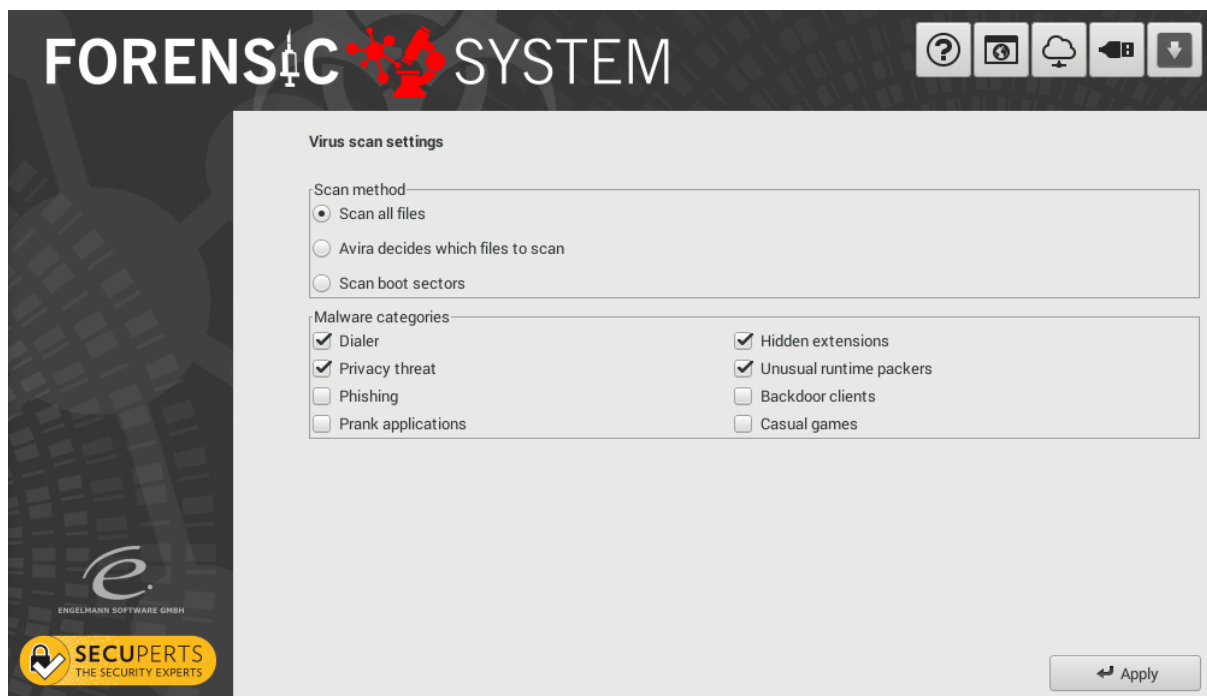
5.1.3 Detect malicious software

Malicious software can sometimes escape anti-virus-software under windows. This is a huge problem. Additionally, anti-virus-software cannot find remote control and spy software, if these are used to observe employees in some countries. If you are suspicious about a co-worker, who might have infested you with spy software, you can use these functions:



Choose drives which will be analyzed for malicious software

Select the drives you want to analyze and. Clicking on "Preferences" allows you to filter the search. "Joke programs" for example usually contain signatures from software, which is usually used by co-workers to drive windows users crazy.



Settings allow you to filter your search

Deleting the malicious software is not possible. This contradicts the essence of the Forensic-System, because it tries to perform analysis without affecting the system. You could use the Live-System of an

anti-virus-software manufacturer to remove those files.

5.1.4 Sort recovered files

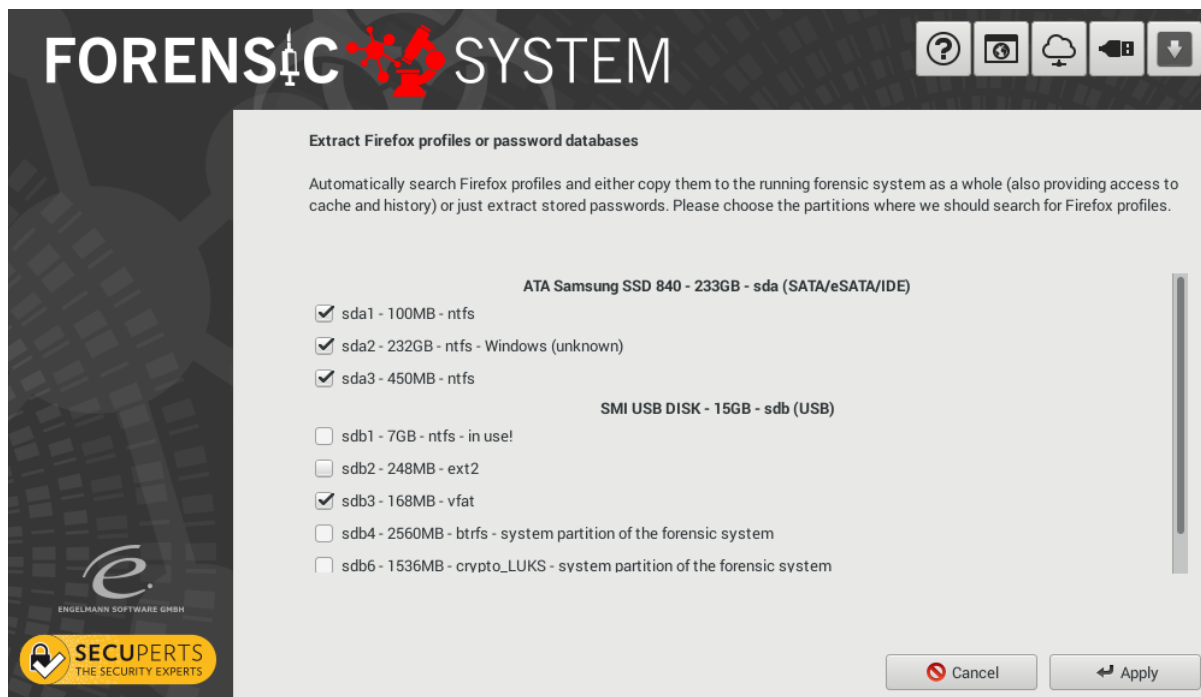
This function can be used as a data recovery, if file names have been lost or the analysis of cashed folders does not offer proper file names. The sort function uses meta data, which is usually located inside files themselves.

5.2 Accessing caches storage and history

Many programs create temporary files in data bases and folders on your drive. With this category you gain access to the temporary storage of many programs like web browsers, email databases from outlook as well as data and program histories from windows.

5.2.1 Accessing firefox profiles

Firefox saves its settings in JavaScript-files, SQLite-data bases and cache-folders. The easiest way to access a Firefox profile is to copy the complete profile or some data bases of the Firefox profile into the live-system. This tool automates this process. Selecting a profile after a successful search allows you to copy either only the password list or the complete profile containing search history, web history and bookmarks into the Forensic-System.



The Forensic-System automatically searches for Firefox profiles

Recovered passwords can be checked under "Settings > Security > Saved credentials". If you want to export long lists of passwords you have to install the Firefox add-on "Password Exporter".

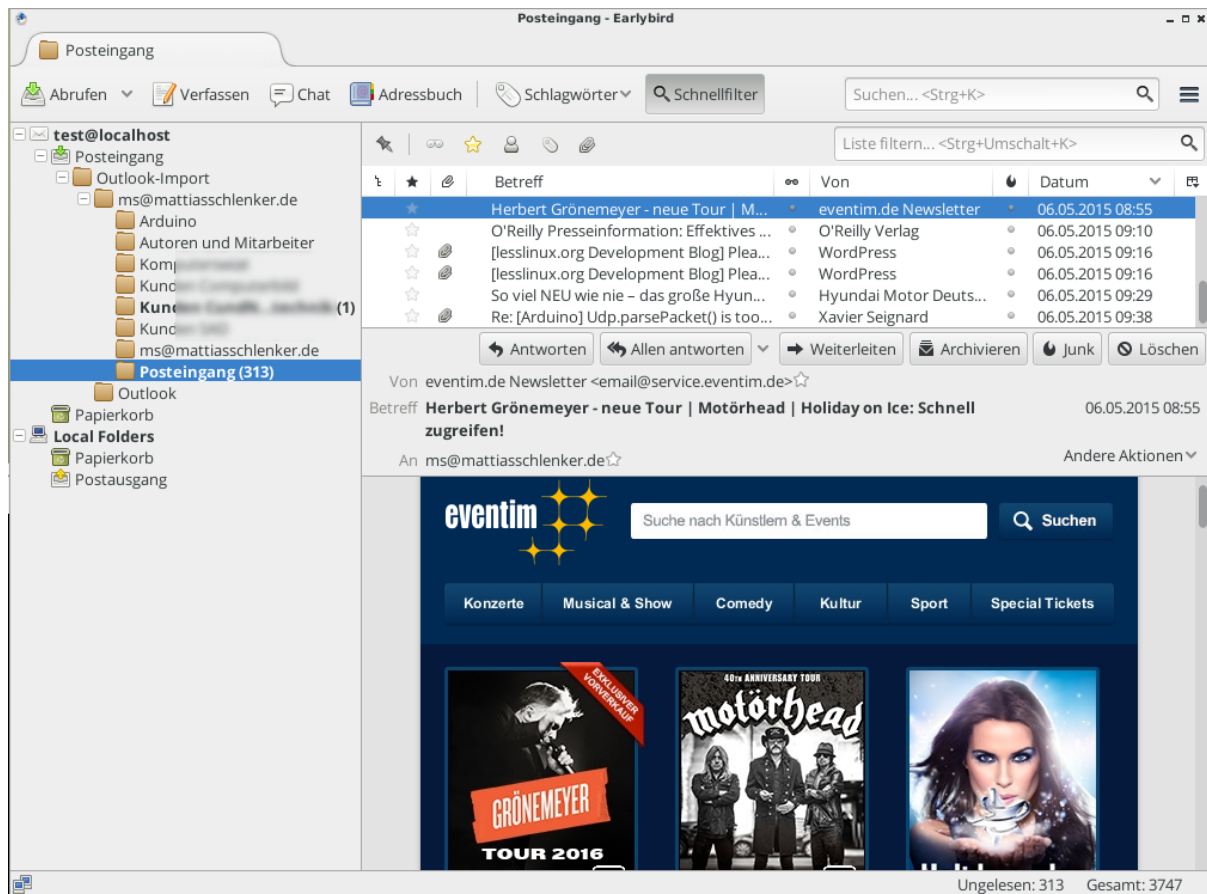
5.2.2 Windows-Jumplists

Since Windows Vista the operating system logs every file and program access in so-called jump lists. SecuPerts-Forensic-System can read these, which allows you to gain knowledge whether your computer has been used unauthorized.

The lists will be created as simple text based tables, which can be read outside the Forensic-System with software like Microsoft Excel. Please be aware that the time codes are based on the windows system time and can differ from the real time. You can use a small sample of data where you know the access time exactly as a clue to spot possible differences.

5.2.3 Recover Outlook-Mailboxes

Outlook saves its mailboxes in special database formats, which usually can only be opened by Outlook. Forensic scientist analyzed these formats and fortunately found a way to convert them into the often used Mbox-format, which for example can be used with Mozilla Thunderbird. This allows you to access the contents of an Outlook-Mailbox without the need to create an Outlook-Profile.



Outlook-Mailboxes can be converted and opened with Thunderbird

The conversion requires quite a lot of temporary storage. The Forensic-System will warn you if you don't have enough storage left. In this case you, should install the SecuPerts-Forensic-System on a bigger USB-Stick and retry the conversion. If only titles of the mails without content are found, you have to change the setting that only read e-mails will be downloaded completely. This setting is usually activated for users with mobile devices and saves bandwidth, but prevents the analysis of local files because they will only be stored on the server.

5.2.4 Browser and chat history

This tool can find and analyze database files created by web browsers and chat software. It currently supports Firefox, Chrome and Internet Explorer as well as the Skype chat history. The data will be

stored in formats which most spreadsheet software can read. Since the formats can change each version you should sometimes check for updates for the SecuPerts-Forensic-System.

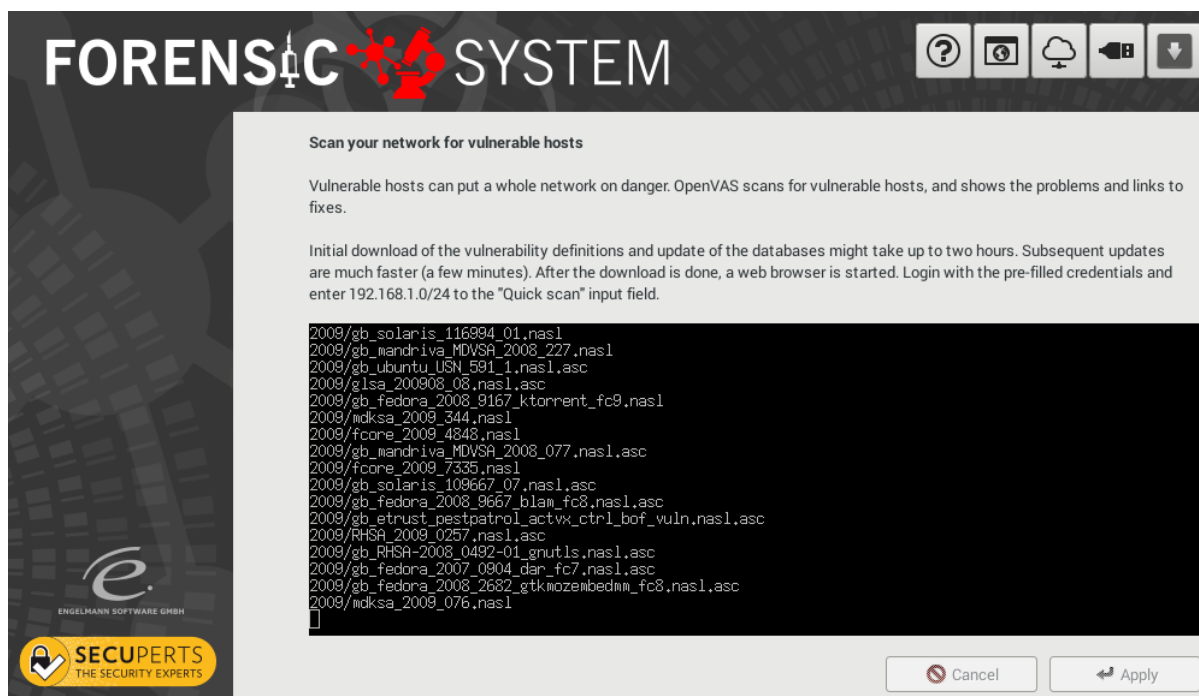
If the format has changed dramatically, you can check the profile folder of the respective application for huge files. These can be further investigated with the "file" command in the windows command prompt. If the file is a SQLite database you can analyze the data with "SQLite DB Browser", located under "Start menu > Accessories".

5.3 Network forensic

Do you exactly know what happens on your network? Your IP-Webcam could be part of a DDoS-Bot network or the TV might try to hack crack servers. Since bot networks like Mirai use Windows-PCs as a gateway to IoT-Devices it is important to know exactly what vulnerabilities your network might have.

5.3.1 OpenVAS

The "Open Vulnerability Assessment Scanner" detects vulnerable devices in your home network. OpenVAS firstly searches for devices in your network, performs a port scan and checks on the basis of databases, if any of them a vulnerable. The degree of the verification can be varied. OpenVAS is kind of hard to configure, but this is done by special scripts within the Forensic-System.

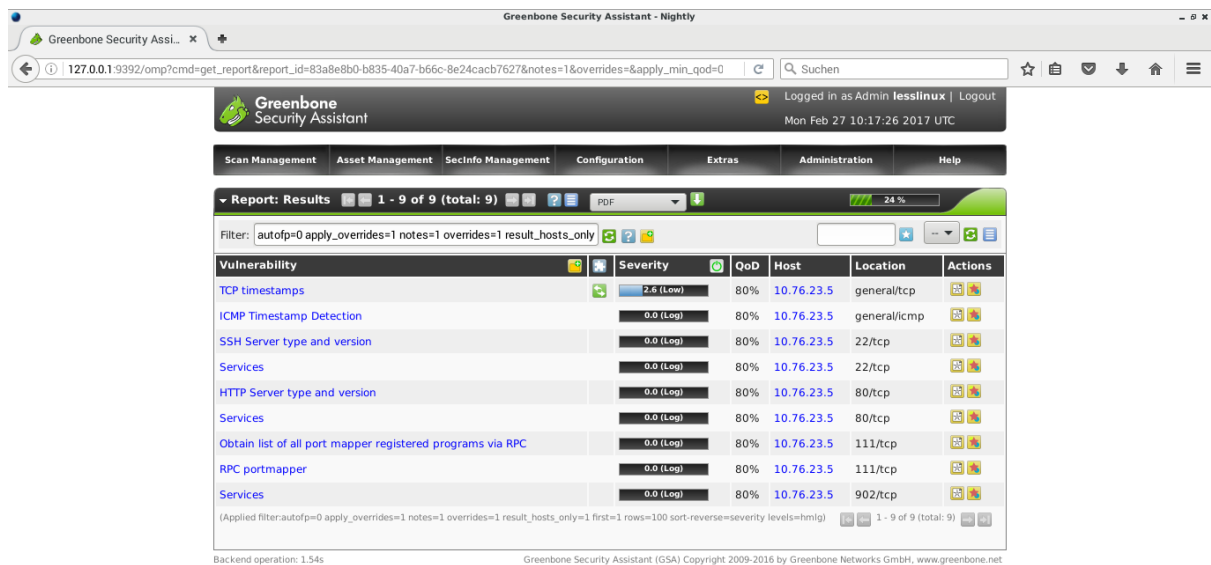


The first setup of OpenVAS can take several hours

OpenVAS has relatively high system requirements: The installation on an USB-stick is mandatory. After the first start around 1,5 gigabyte of vulnerability definitions are being downloaded and inserted into a database, so a USB-Stick with write speeds of 15MB/s or higher should be used. The first start requires patience: The initial setup of the vulnerability database can take several hours. Coming starts only update these databases and take anywhere from 10 to 30 minutes.

Firstly start a "Quick Scan" over a computer or the whole network

As soon as OpenVAS is done configuring, Firefox with an OpenVas web front end will start. Log in with the username "lesslinux" and password "lesslinux". The button "Quick Scan" on the right side allows you to scan either a single computer or a whole sub net. The first scan should be done with the complete sub net. If your router uses the ip adress "192.168.1.1" the sub net is usually "192.168.1.0/24". If you don't know the sub net, you can use the Linux terminal with the "ifconfig" command to get your current ip adress. Make sure your devices are connected to the network. This means smart tvs should be turned on and tablets/ smartphones should play for example a YouTube video.



Greenbone Security Assistant - Nightly

Greenbone Security Assistant

Logged in as Admin lesslinux | Logout
Mon Feb 27 10:17:26 2017 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Report: Results 1 - 9 of 9 (total: 9) PDF 24 %

Filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only

Vulnerability	Severity	QoD	Host	Location	Actions
TCP timestamps	2.6 (Low)	80%	10.76.23.5	general/tcp	
ICMP Timestamp Detection	0.0 (Log)	80%	10.76.23.5	general/icmp	
SSH Server type and version	0.0 (Log)	80%	10.76.23.5	22/tcp	
Services	0.0 (Log)	80%	10.76.23.5	22/tcp	
HTTP Server type and version	0.0 (Log)	80%	10.76.23.5	80/tcp	
Services	0.0 (Log)	80%	10.76.23.5	80/tcp	
Obtain list of all port mapper registered programs via RPC	0.0 (Log)	80%	10.76.23.5	111/tcp	
RPC portmapper	0.0 (Log)	80%	10.76.23.5	111/tcp	
Services	0.0 (Log)	80%	10.76.23.5	902/tcp	

(Applied filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort=reverse=severity levels=html)

Backend operation: 1.54s

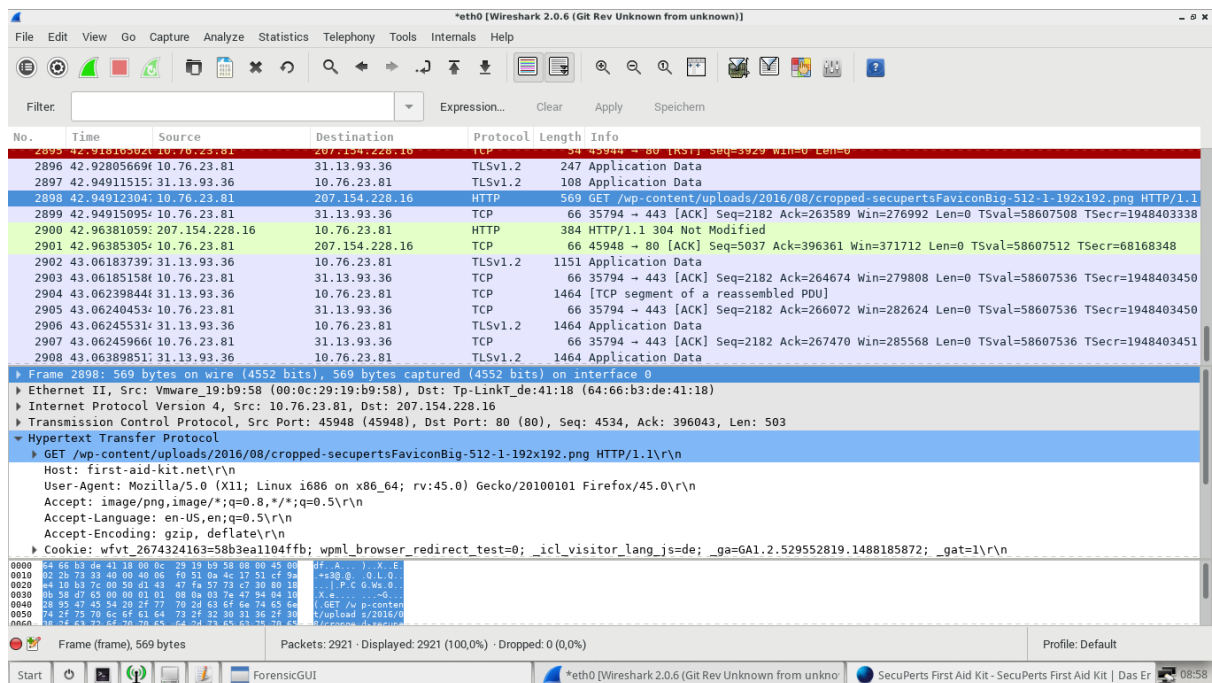
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

OpenVAS sorts found vulnerabilities by degree of severity

The logs can be accessed while a scan is running. Found vulnerabilities can sometime just be "False Positives", because OpenVAS standard settings do not allow real attacks. If you can handle some crashes of your network, you can turn them on with "Full and very deep ultimate". Vulnerable services are often patched already. If this is not the case, "real attacks" might lead to crashes.

5.3.2 Wireshark

Use Wireshark to monitor the network traffic from single devices or the whole network (e.g. to identify which data a smart tv sends/ receives). The monitoring of network traffic should be done through the ethernet card. Furthermore, the ethernet card and the switch need to interact while switching to the promiscuous mode and possible access points may not filter the WLAN traffic separately. If that does not work, read information about the fourth program in this section, which explains how to span a bridge between the ethernet and WLAN interface.



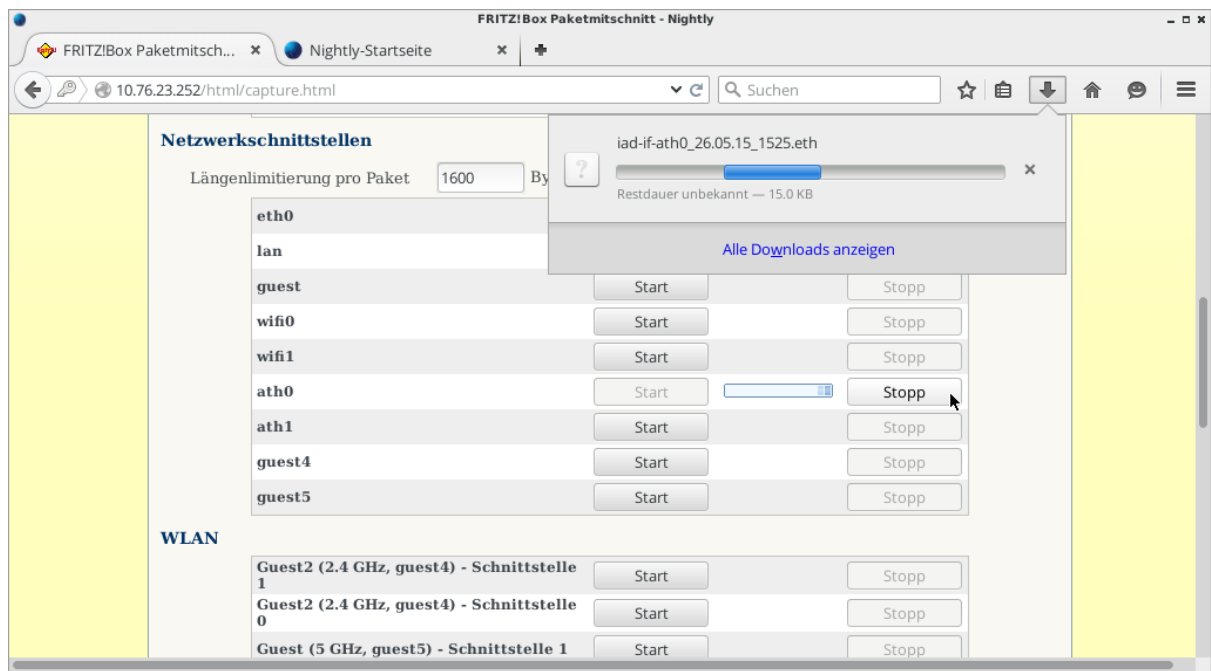
Use Wireshark to monitor and evaluate network traffic

Click on the green shark fin to start the live monitoring. During the monitoring you can display single network packets or sort by source, target or used protocol. After it has finished, you have the possibility to save the session in a separate file.

If you want to monitor for a longer period of time we do not advise to use Wireshark. In this case you should use tcpdump with

```
tcpdump -i eth0 -w /tmp/dump.pcap
```

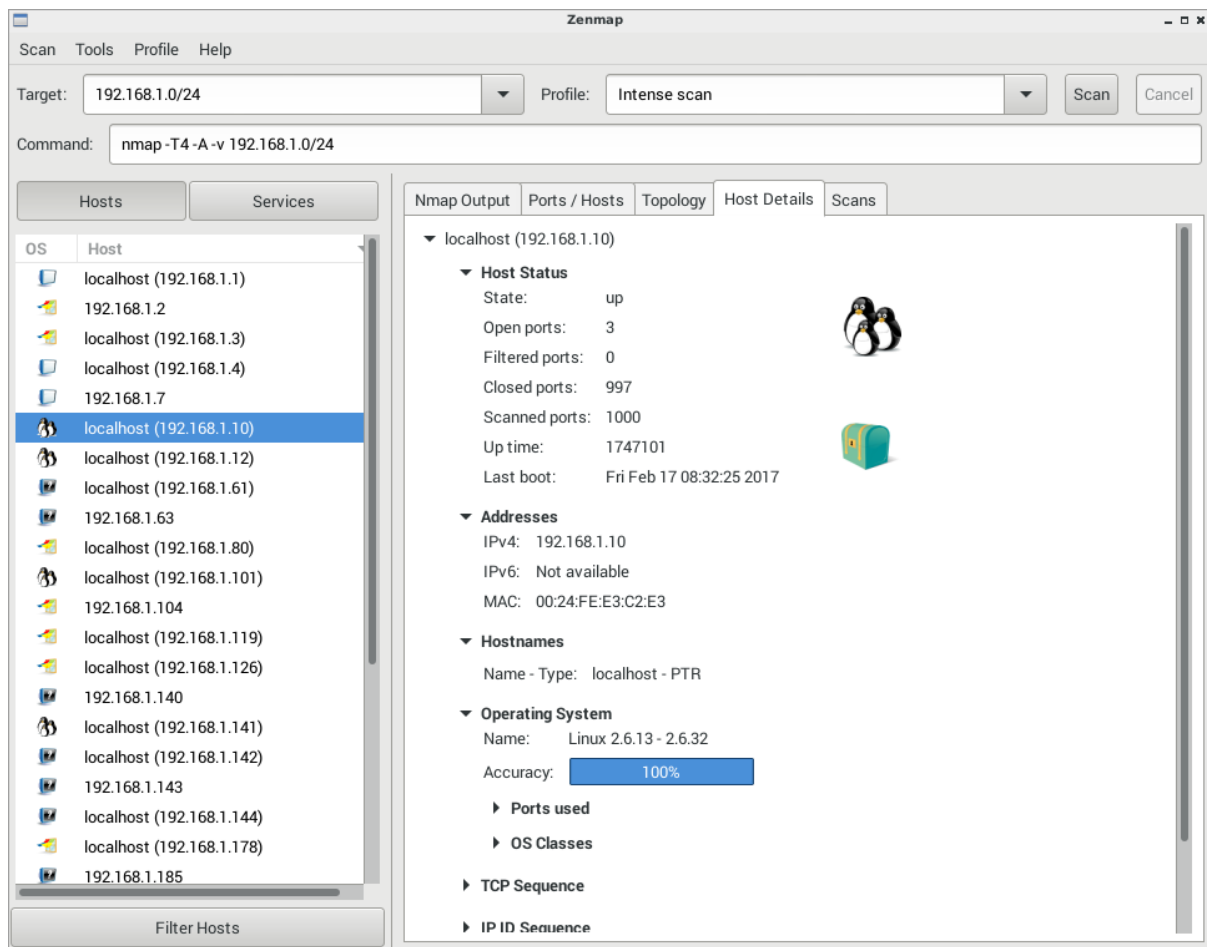
to create a binary file of the network traffic. Many DSL-Router like AVMs Fritzbox or OpenWRT based routers have tcpdump preinstalled. Sometimes they even have a web interface to limit the monitoring on a single host. These files can then be opened and analyzed with Wireshark.



Many DSL-Routers offer own tools for longer traffic monitoring

5.3.3 Zenmap

Zenmap is basically OpenVAS small brother and the GUI for the port scanner Nmap. The biggest advantage of Zenmap is that you do not need to download huge files first. The downside is that Zenmap only scans open ports and can't offer penetration tests. It is mainly used to give a good overview about connected devices and services inside a network.

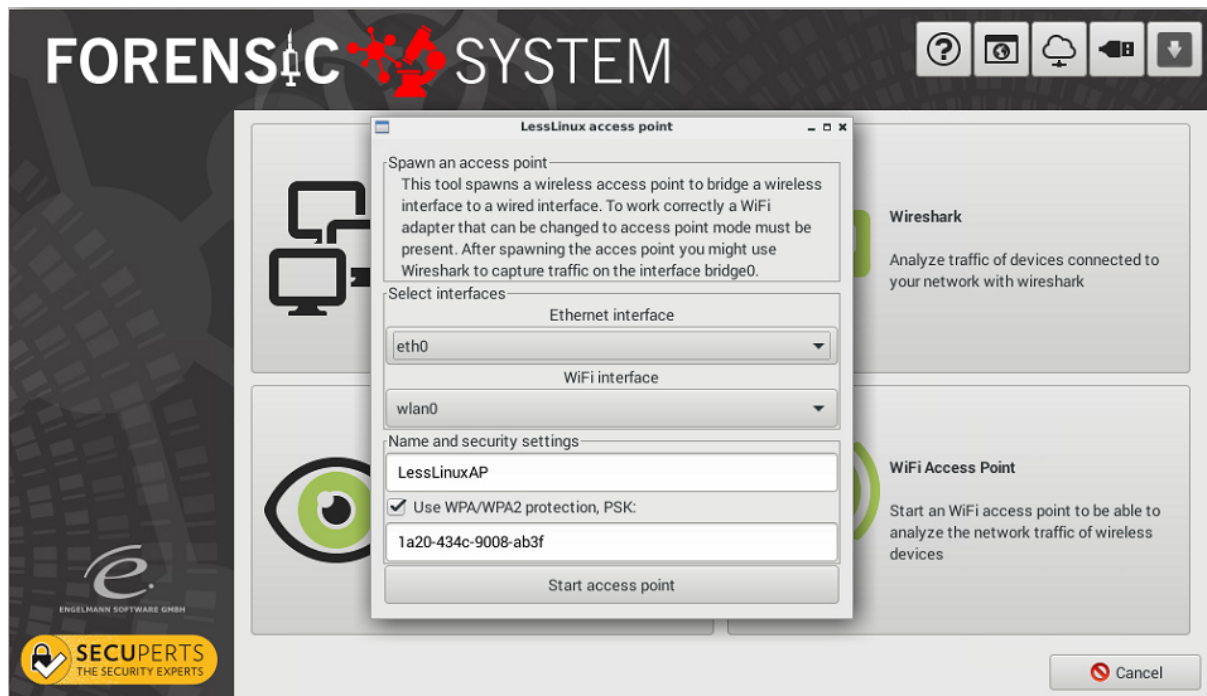


The port scanner Zenmap gives a quick overview about all services inside a network

Enter either the ip adress "192.168.1.1" or the sub net "192.168.1.0/24" into the "Target" field to start a scan. Other settings should not be activated for the first scan. Scanning the whole network usually takes 5 to 10 minutes, single hosts only 30 seconds. After the scan has finished you can click on "Computer" on the left side to display the found devices. Click on a device and then on "Computer properties" to get more details about this network device.

5.3.4 Accesspoint

If monitoring with Wireshark is not possible due to technical reasons, you can span an access point with "WLAN Accesspoint", which acts as a bridge between ethernet and WLAN. This allows monitoring the traffic of connected devices through the "bridge0" interface. Spanning an access point is only possible, if you have not been connected to a wireless network during this PC start. After you have an ethernet connection, you can turn the access point on.



The integrated access point allows monitoring network traffic of computers inside you WLAN

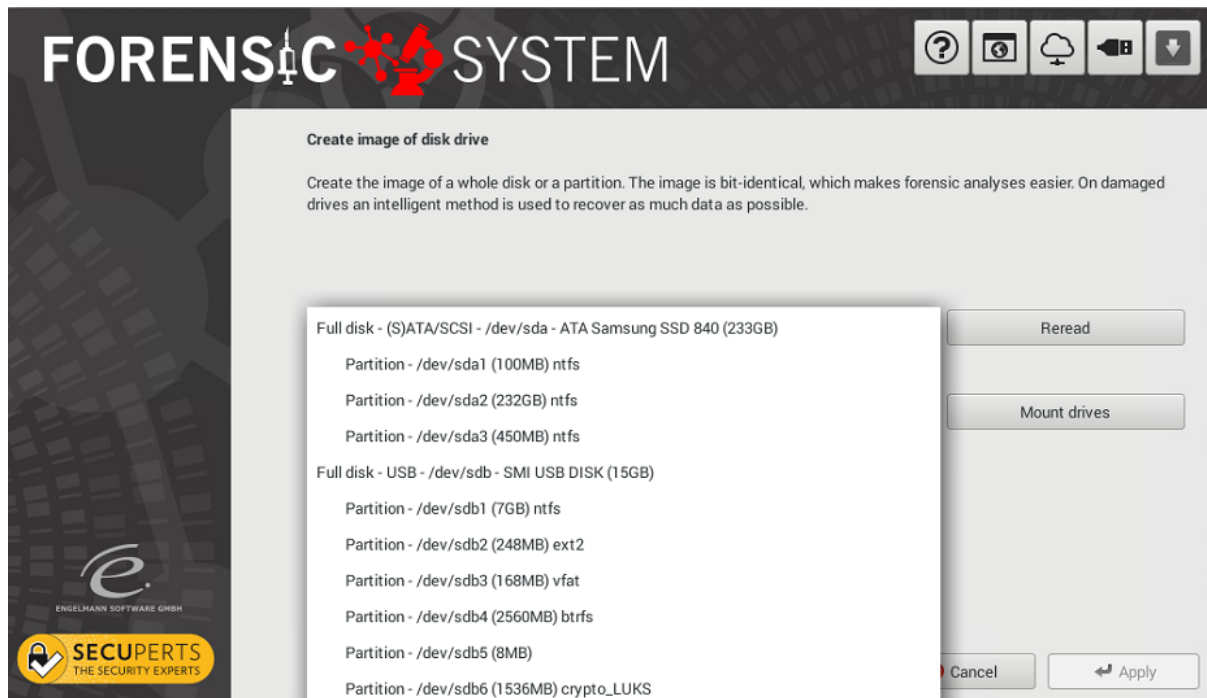
Try it again without encryption, if the connection does not work: Not every WLAN chip set allows access point encryption. If the access point is not visible, you could have one of those chip sets. In such a case you could try a different notebook or an USB-WLAN-stick.

5.4 Block device operations

In this category you can find tools which operate on "raw" block device, namely hard disk partitions and whole drives. The presented features ignore partitioning and data systems. This means they can also be used on damaged drive images or clones for further analysis.

5.4.1 Storage device image

This function creates a perfect image of a partition or whole hard disk. Even damaged drives can be copied by smartly detecting defect parts. Make sure to mount the target drive as writable. Additionally the target drive should have at least the same amount of storage left the source drive has. The source drive has to be mounted as read-only. This affects the speed of copying a little bit, but keeps the integrity of the result.



The Image-Function creates images of partitions or whole disks

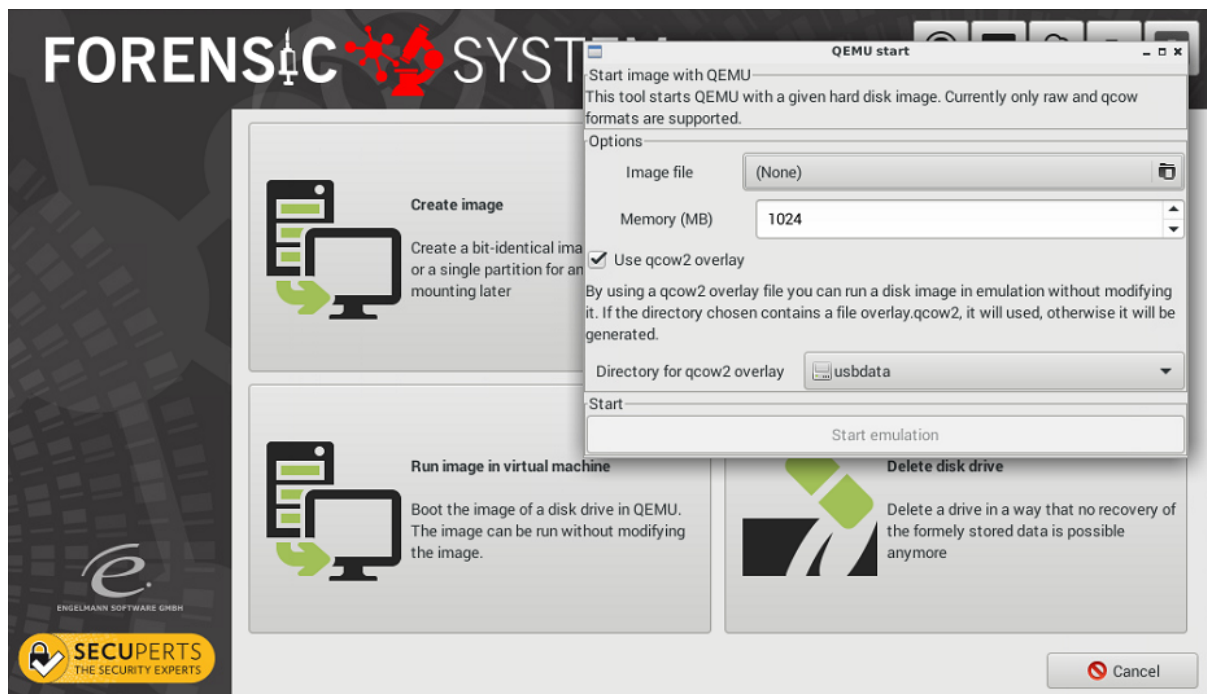
If you only want to save data with Qphotorec an image of the partition should be enough. If you want to create a bootable image you should create an image of a whole drive. This can for example later be used for a virtual machine.

5.4.2 Clone hard drive

This program clones a drive 1:1 to another drive. The target drive again should be the same size as the source drive. After cloning a smaller drive to a bigger one, the partitioning can be altered with the Gparted tool.

5.4.3 Open image in VM

Open the image file of a whole drive with the virtual machine Qemu. An overlay image can be activated to catch write attempts. This reserves the integrity of the underlying image. Be aware that the network is activated. If you want to start it without a network, you have to start Qemu through the command prompt.



Drive image with boot sector can be started directly with Qemu

The hardware of the virtual machine is usually significantly worse than your computers. This means that not all operating systems will work flawlessly. The most problematic ones are Windows XP and Server 2003. Windows versions since Windows Vista should work fine. Most Linux system will work as well, but the sometimes have graphics and network problems.

5.4.4 Delete drive

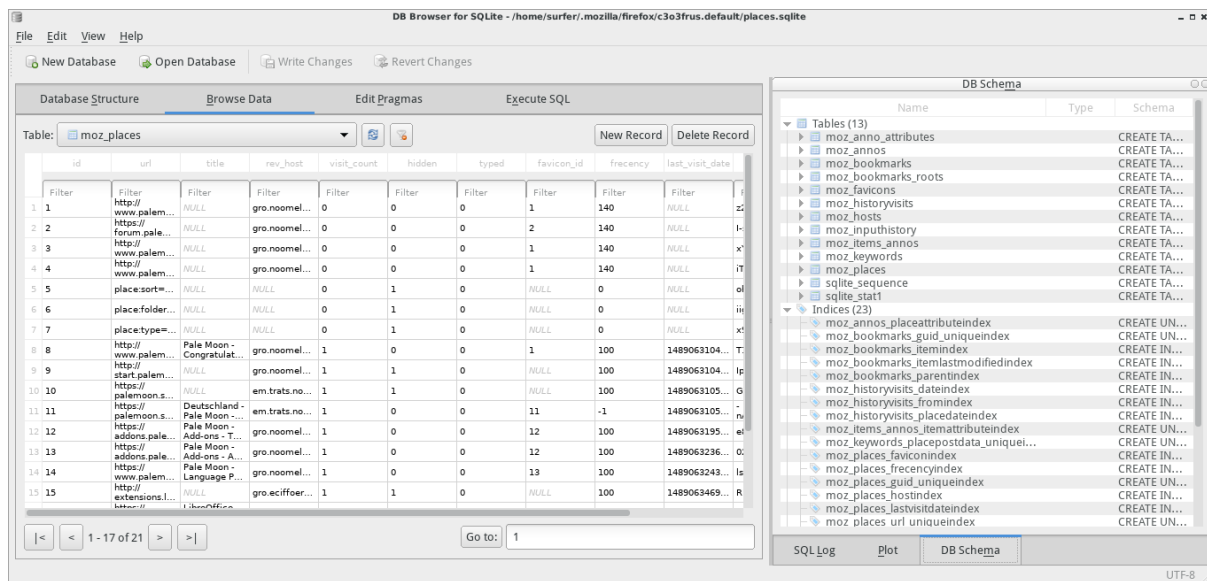
If you want to give away a hard disk or sell your PC the drive has to be completely wiped first. This holds especially for drives with much sensible data. Copy-on-Write-file-system like NTFS usually even save files if single files are overwritten first. SSDs will be overwritten once, before they are trimmed with nullbytes, which accelerates future writes.

6 Useful menu and command prompt tools

Not every useful tool can be within the assistant. A glimpse at the start menu shows some gems. More tools are hidden inside the command prompt.

6.1 SQLite Database-Browser

Passwords and histories are usually saved as SQL-Databases, often in version 3.X. Data bases with this format can be opened with the SQLite Database-Browser. You can access it through "Start menu > Accessories > DB Browser for SQLite". The files can either be opened with drag&drop or by using "Open file".



The SQLite-Browser presents the commonly used SQLite-Database format neatly arranged

6.2 Skype-Logs

Even Skype saves its chat logs in the SQLite3-Database format. It is easier to use a program specifically developed for these logs instead of looking for the files manually. For this reason, SecuPerts-Forensic-System includes the software "Skype Xtractor", which is accessed by the command prompt.

```
cd /usr/share/skype_xtractor
python skype.py -o /tmp/skype /path/to/main.db
```

The parameter "-C" additionally creates chatsyncs. The created HTML-files can then be found under "/tmp/skype".

6.3 Connect network drives

The software "Accessories > bind CIFS- and WebDAV-Shares" can bind CIFS-/SMB-Shares (Windows-Shares) or WebDAV-Drives (internet drives). This is helpful if you don't have enough space locally and want to save files on a NAS or in cloud storage. As the Share-Label use this format:

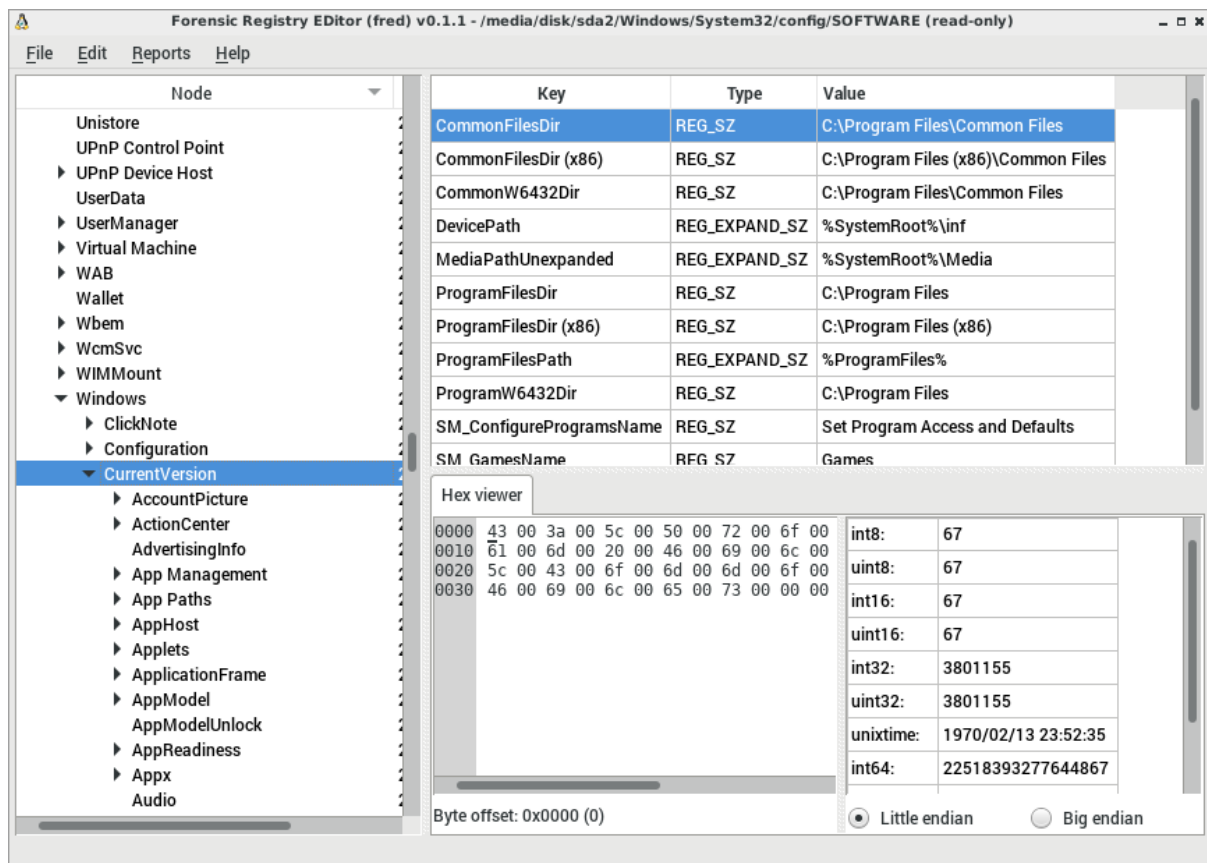
```
https://webdav.provider/path/
```

or

```
cifs://192.168.0.24/sharename
```

6.4 Fred Forensic Registry Editor

An advanced registry editor can be found under "Start menu > Other Tools > FRED Registry Editor". You can choose a registry database through "File > Open Hive". These can be found under "Windows/System32/config". The files "SOFTWARE" and "SYSTEM" are the same-named branches. "USERS" is located at the home directory of the user. Now you can click through the structure on the left side and their values on the right side, just like with the Windows registry editor. Editing them is not supported for security reasons. This option can be changed through "Edit > Enable write support".



Windows Registry can be analyzed with the forensic registry editor FRED

7 Password tools

Are your passwords not safe enough? The answer to this question is given by several password crackers from the SecuPerts-Forensic-System. They are usually used in company environments to increase its password security. They are based on lists from known passwords (<https://wiki.skullsecurity.org/Passwords>) and dictionaries. If these won't work they will try out every combination of letter/ numbers. Passwords are often used multiple times, which leads to huge problems, if they are being phished. After detecting such passwords, Administrators can disable them and force the user to choose a better one. The password crackers are able to use the graphics card as support to try out a lot more passwords in a given time frame. If used seriously in a company environment, a dedicated machine with a powerful graphics card might be a good idea.

Caution: These tools are obviously only meant to be used with your own systems. Attacking passwords and authentication systems of other is a criminal offense.

7.1 John the Ripper

This program uses word lists and brute force attacks. Its standard word list ("password.lst") leaked and phished passwords as well as often used english words. It can be extended with a dictionary in your language or other password list.

John works best when a password database contains the password-hashes in plain text. Open a rootshell and set the admin ("root") password as something simple like "test1" with the "passwd" command. Now you can start John:

```
cd /opt/john-1.8.0-jumbo-1/run
./john /etc/shadow
```

Cracking windows passwords is a bit more tricky. At first the SAM-File has to be found and read. The program "samdump2" can be used for this. The following command will extract the hashes to "/tmp/sam.txt":

```
samdump2 /media/disk/sda2/WINDOWS/system32/config/SAM /tmp/sam.txt
```

Afterwards John has to be used again. In this case, you have to set the hash type:

```
john -format=LM /tmp/sam.txt
```

More information about the usage of John can be found under <http://www.openwall.com/john/doc/EXAMPLES.shtml>. Among others John can also be used to crack passwords from encrypted containers like Truecrypt/Veracrypt or LUKS.

7.2 Ophcrack

Ophcrack works, unlike John, with so-called rainbow tables, which reduce the hash value calculation and replace searching through a database. The hash tables can, depending on covered password length, be several terabytes big. The hash tables should be located on a fast hard disk or even better an SSD. Go to <http://ophcrack.sourceforge.net/tables.php> to download rainbow tables for specific purposes.

Now use the command

```
ophcrack --help
```

to get information about to tell Ophcrack where your tables are saved.

7.3 Ncrack

Ncrack is used to crack passwords, which are used for network authentication, like FTP, SSH, HTTP, SMB, RDP, VNC or MySQL. It uses password lists, which are either passed separated by commas or with a specific file name. First, start the SSH-Service in a root-shell:

```
/etc/rc.d/0600-openssh.sh start
```

Now set an easy to guess password with "passwd". Using the word list from John the Ripper you can simulate an attack:

```
ncrack -v --user root -P /opt/john-1.8.0-jumbo-1/run/password.lst localhost:22
```

Detailed information about all the options can be displayed with "ncrack --help". If you want to perform a real brute force attack with Ncrack, you first have to create word lists (e.g. with Perl or Ruby scripts) and use these.

8 Linux-System

The SecuPerts-Forensic-System is a Linux based system and differs from windows in many aspects.

8.1 File system

The biggest difference is the organization of the file system. Windows uses drives with corresponding letters where folders and files are located. Linux uses a root directory, where hard disks, partitions and optical drives are displayed as device files and the `"/dev"` directory. The root directory has the following structure:

- `/bin`: Directories with basic shell-commands, comparable to DOS.
- `/boot`: Files which are needed for the boot.
- `/dev`: Hardware like hard disks will be displayed here.
- `/home/username`: Private files for normal users.
- `/media`: Removable media like CD/DVD/BD-Drives and USB sticks.
- `/mnt`: Directory for mounted file systems.
- `/opt`: Directory for manually installed software.
- `/root`: Directory for personal data from the administrator.
- `/srv`: Files for services like FTP and HTTP.
- `/tmp`: Temporary files.
- `/usr`: Static and read-only files.
- `/var`: Files which are created during usage of the system.

8.2 Mount drives

Existing drives will not be automatically mounted during startup and as to be done manually. The drives are marked as device files under `"/dev"`. As an example, the first hard disk is named `"sda"`, its first partition `"sda1"`. Clicking this file will not lead to the saved data. The device file has to be mounted to a folder first. The mount point can be located anywhere in the file system. Typically a sub folder in `"/media/disk"` like `"/media/disk/sda1"` will be used. The easiest way to mount a drive is the tool `"Disks"`, where you can decide through a checkbox whether a drive should be writable. Clicking `"bind partitionX (sdaX, ntfs)"` will mount the drive and open an explorer. The drive will stay mounted until you manually unmount it or the system is shut down.