
VMCloak Documentation

Release 4.x

Jurriaan Bremer

May 03, 2017

Contents

1	Requirements	3
2	Setup VMCloak	5
3	VirtualBox	7
3.1	Creating vboxnet0	7
4	Keyboard Layout possibilities	9
5	Configuration	11
5.1	Mounting the ISO Image	11
5.2	Serial Key	11
5.3	VM Name	11
5.4	Guest hostonly IP address	12
5.5	Guest hostonly Gateway	12
5.6	Guest hostonly network mask	12
5.7	Guest hostonly MAC address	12
5.8	Host host-ip	12
5.9	RAM Size	13
5.10	Resolution	13
5.11	Harddrive Size	13
5.12	Hardware Virtualization	13
5.13	Keyboard Layout	13
5.14	Cuckoo Directory	14
5.15	Tags	14
5.16	No Register Cuckoo	14
5.17	DNS Server	14
5.18	Visible VM Generation	14
6	Networking	15
6.1	Full-internet access	15
7	Hardware Configuration	17
7.1	Creating a Hardware Profile	17
8	VMCloak's License	19
9	Credits	31

9.1 nLite	31
10 Indices and tables	33

VMCloak is a utility for automatically creating Virtual Machines with Windows as guest Operating System. It has been tailored to generate Virtual Machines directly usable from within [Cuckoo Sandbox](#), but it can also be used for other purposes as *Cuckoo*'s components can be omitted through the configuration.

Please refer to the following blogposts for up-to-date installation methods and further information:

- [VMCloak 0.3 usage](#)
- [VMCloak 0.4.1 release](#)

Contents:

CHAPTER 1

Requirements

In order to run VMCloak you'll at the very least require the following software:

- Python 2.6 or 2.7
- mkisofs *or* genisoimage
- VirtualBox
- wget
- **root** access to *mount the Windows Installer ISO image*

To create a *Hardware Profile* **root** is required as well, as well as the following tools:

- dmidecode
- lshw

CHAPTER 2

Setup VMCloak

Given VMCloak is available as a [Python Package](#) it features a `setup.py` for easy installation. Besides of course installing VMCloak through `pip` using `pip install -U vmcloak` it is also possible to fetch the [Git repository](#) and install the package globally through `sudo python setup.py install` (or in a `virtualenv` through `python setup.py install`).

Fetching the repository through Git allows one access to the latest development version of VMCloak with features that may not have been pushed to the Python Package yet. A full example of installing VMCloak manually can be as follows:

```
$ git clone git://github.com/jbremer/vmcloak
$ cd vmcloak
$ sudo python setup.py install
```

For development purposes you'll want to install it in development mode, preferably inside of a `virtualenv`:

```
(venv)$ git clone git://github.com/jbremer/vmcloak
(venv)$ cd vmcloak
(venv)$ python setup.py develop
```


As of this moment VMCloak only supports VirtualBox (i.e., no VMWare, KVM, etc.)

VMCloak requires the hostonly interface `vboxnet0` in order to communicate with the Virtual Machine. If `vboxnet0` is not yet running (VMCloak will inform you about this), then *you have to create `vboxnet0`*.

To check whether `vboxnet0` exists run the following command. If it returns nothing then *you have to create it*.

```
VBoxManage list hostonlyifs
```

Creating `vboxnet0`

Executing the following two commands on the command line will create and start the `vboxnet0` network: (again, only required when **`vboxnet0` is not already present**)

```
VBoxManage hostonlyif create  
VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
```

This is equivalent to executing the `vmcloak-vboxnet0` script.

Keyboard Layout possibilities

For Windows XP:

Albanian
Belarusian
Belgian Dutch
Belgian French
Brazilian (ABNT)
Bulgarian
Bulgarian Latin
Canadian English (Multilingual)
Canadian French
Canadian French (Multilingual)
Croatian
Czech
Czech (QWERTY)
Danish
Dutch
Estonian
Finnish
French
German
German (IBM)
Greek
Greek Latin
Greek (220)
Greek (220) Latin
Greek (319)
Greek (319) Latin
Hungarian
Hungarian 101-key
Icelandic
Irish
Italian
Italian (142)
Latin American

```
Latvian
Latvian (QWERTY)
Lithuanian
Norwegian
Polish (Programmers)
Polish (214)
Portuguese
Romanian
Russian
Russian (Typewriter)
Serbian Cyrillic
Serbian Latin
Slovak
Slovak (QWERTY)
Slovenian
Spanish
Spanish variation
Swedish
Swiss French
Swiss German
Turkish F
Turkish Q
Ukrainian
United Kingdom
US
US-Dvorak
US-Dvorak for left hand
US-Dvorak for right hand
US-International
```

Since VMCloak 0.3 it no longer uses configuration files for simply creating VMs. However, a couple of things remain necessary to be performed before invoking VMCloak.

Mounting the ISO Image

In order to mount a Windows Installer ISO image a directory should be created with **root**, and then the image should be mounted on that directory, with root as well. The following bash snippet depicts how to setup an ISO mount on a Ubuntu/Debian system.

```
mkdir /mnt/winxp
mount -o loop,ro winxp.iso /mnt/winxp
```

In order to mount an image under BSD the following commands might be required.

```
mkdir /mnt/winxp
vnconfig /dev/vnd0d winxp.iso
mount -t cd9660 /dev/vnd0d /mnt/winxp
```

Serial Key

`--serial-key` specifies the **serial key** to be used to install Windows in the Virtual Machine. Although it is possible to randomize the serial key after the installation has been finished, a valid serial key is required during installation, and often times there is no *one serial key to rule them all*, thus make sure to have a valid serial key at hand.

VM Name

The Virtual Machine name represents the unique identifier for this VM. This value is the extra argument on the command line, e.g., `cuckoo1` in `vmcloak -s conf.ini cuckoo1`.

Semi-required configuration entries

A few configuration entries are not required, but should in most cases be provided.

- *Guest hostonly IP address*
- *Guest hostonly Gateway*
- *Guest hostonly network mask*
- *Guest hostonly MAC address*
- *Host host-ip*

Guest hostonly IP address

The IP address to assign to the Guest is set by `--hostonly-ip`. It defaults to `192.168.56.101`, which is perfectly fine when one only intends to create one VM. However, if one wants to create multiple VMs, then the static IP addresses should be unique. Normally one would start counting at `192.168.56.101` to `192.168.56.102`, `192.168.56.103`, etc.

Guest hostonly Gateway

The Gateway IP for the Guest to use. Set by `--hostonly-gateway`

Guest hostonly network mask

The Network mask for the Guest to use. Set by `--hostonly-mask`

Guest hostonly MAC address

The MAC address for the guest to use. Set by `--hostonly-macaddr`

Host host-ip

The IP address of the `vboxnet` interface for communication between guest and host. The communication is relevant for the installation process to finish. Set by `--host-ip`

Suggested configuration entries

Following are various configuration entries that are not necessary, but allow one to do some custom modifications on the guest VM, which can be quite useful if one needs to make a special VM for a custom analysis.

- *RAM Size*
- *Resolution*
- *Harddrive Size*

- *Hardware Virtualization*
- *Keyboard Layout*

RAM Size

With `--ramsize` one can specify the required RAM size of the VM in megabytes. By default this value will be set to **1024** (which results to 1 GB of RAM).

Resolution

`--resolution` sets the resolution of the VM. By default the resolution will be set to **1024x768**, a not too uncommon resolution if your PC was bought in the year 2006.

Harddrive Size

`--hdsiz` allows one to specify the harddrive size of the VM in megabytes. As the created harddrive is enlarged in size on-demand, rather than allocating all of the specified space at once, it doesn't really matter whether one puts 32 GB or 256 GB. By default this value is set to 256 GB, but this does mean that if at some point a VM really needs the 256 GB that the harddrive shouldn't run out of space.

Hardware Virtualization

If one hasn't enabled **VT-x** in the BIOS then it is not possible to use hardware virtualization. If one gets such error, then provide `--no-hwvirt`. To explicitly enable hardware virtualization provide `--hwvirt`. In the config file disable it with `hwvirt = false`.

Keyboard Layout

By default the `--keyboard-layout` defaults to **US**. See *Keyboard Layout possibilities* for a list of all available keyboard layouts.

Cuckoo Sandbox configuration entries

These configuration entries are related to direct interaction with Cuckoo Sandbox as VMCloak has the ability to automatically add the created VM to Cuckoo Sandbox.

- *Cuckoo Directory*
- *Tags*
- *No Register Cuckoo*

Cuckoo Directory

In order to add a created VM automatically to Cuckoo Sandbox one must run a recent version of Cuckoo Sandbox (**1.2-dev** or higher) which ships the `./utils/machine.py` utility script. The `--cuckoo` argument accepts a path to the root of your Cuckoo Sandbox setup to interact with Cuckoo Sandbox.

Tags

Optionally `--tags` adds tags for the created VM when registering it with Cuckoo Sandbox. For example, if you install the *dotnet40* (.NET v4.0) and *adobe/pdf* (Adobe PDF Reader) dependencies in your VM, then you might want to represent this in its Cuckoo Sandbox tags as `dotnet, adobe` or something like this. For more information on tags, see the [official Cuckoo Sandbox documentation](#).

No Register Cuckoo

If the `--cuckoo` argument is not provided, or it is provided but the created VM should not be registered with Cuckoo Sandbox, then the `--no-register-cuckoo` argument allows one to do that.

DNS Server

By default the generated Virtual Machine will use Google's 8.8.8.8 DNS Server. This can be changed through `--dns-server`.

Debugging configuration entries

As is there's not much debugging one can do. This limits one to *visual* debugging as described as per *Visible VM Generation*.

Visible VM Generation

The `--vm-visible` argument, if specified, runs the Virtual Machine in **GUI** mode instead of **headless** mode (terms as per VirtualBox.) This allows one to monitor the installation as it goes.

Often times the installation will hang at the serial key dialog. This is the case when the `conf-serial-key` provided is incorrect. At this point VMCloak is unable to detect it when this happens.

Deprecated since version 0.3: Since Cuckoo Sandbox 2.0-RC1 better options exist to handle per-analysis network routing. Please refer to Cuckoo's official documentation to learn more about this.

By default, and at the moment this is necessary for VMCloak to work, every generated Virtual Machine will have a hostonly network adapter. This adapter is used to talk to Cuckoo. However, as it is host-only, this does not allow the Virtual Machine to reach the internet.

In case you'd like the Virtual Machine to be able to have full access to the internet then that's also possible of course. However, do take into account that this indirectly allows **malware to abuse your internet connection**.

There are multiple approaches to getting networking inside the Virtual Machines working - following is the easiest approach. (Other approaches include, but are not limited to, a bridged network adapter, a NAT network, etc.)

Full-internet access

In order to setup full internet access for Virtual Machines the following two steps will be taken. **Note that these steps can also be taken after generating the Virtual Machines hence magically giving them internet access.**

- Setup hostonly network interface
- Run a bash script around iptables(8)

To start off *setup a hostonly interface for VirtualBox*. Then run the following bash script as **root**. For your convenience it can be found on your system by running `vmcloak-iptables` (the name of this script is subject to change in the future, though.)

```
#!/bin/sh
# Copyright (C) 2014-2015 Jurriaan Bremer.
# This file is part of VMCloak - http://www.vmcloak.org/.
# See the file 'docs/LICENSE.txt' for copying permission.

# Credits to Mark Schloesser, https://github.com/rep/cuckoo-contrib

if [ "$1" = "-h" ]; then
```

```

echo "Usage: $0 [ip_range/cidr] [interfaces..]"
echo "  $0 192.168.57.0/24 eth0 eth1"
echo
echo "Defaults to:"
echo "  $0 192.168.56.0/24 eth0 wlan0"
exit
fi

# Fetch the IP range and CIDR.
if [ "$#" -ne 0 ]; then
    VBOXNET="$1"
    shift
else
    VBOXNET="192.168.56.0/24"
fi

# Fetch the interfaces.
if [ "$#" -ne 0 ]; then
    INTERFACES="$*"
else
    INTERFACES="eth0 wlan0"
fi

iptables -F
iptables -t nat -F

for i in $INTERFACES; do
    iptables -t nat -A POSTROUTING -o $i -s "$VBOXNET" -j MASQUERADE
done

# Default drop.
iptables -P FORWARD DROP

# Existing connections.
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

# Accept connections from vboxnet to the whole internet.
iptables -A FORWARD -s "$VBOXNET" -j ACCEPT

# Internal traffic.
iptables -A FORWARD -s $VBOXNET -d $VBOXNET -j ACCEPT

# Log stuff that reaches this point, could be noisy though.
iptables -A FORWARD -j LOG

# Actually enable forwarding of packets. This is Debian/Ubuntu specific.
echo 1 > /proc/sys/net/ipv4/ip_forward

```

That being said setting up full internet access for your Virtual Machines boils down to running the following commands:

```

VBoxManage hostonlyif create
VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1
sudo vmcloak-iptables

```

Hardware Configuration

Through hardware profiles VMCloak is able to cloak the names, versions, etc of the various hardware components that the Virtual Machine software is emulating.

Creating a Hardware Profile

Creating a new hardware profile of a machine requires one to run `vmcloak-gethwconf <profile>` on said machine. The `profile` represents the name of this profile - the profile will be called after it and put in the `hwconf/` directory.

As an example, to create a hardware profile of a lenovo thinkpad, one may do:

```
vmcloak-gethwconf lenovo_x220
```

VMCloak's License

VMCloak **is** copyrighted by Jurriaan Bremer **and is** licensed under the following GNU General Public License version 3.

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>
Everyone **is** permitted to copy **and** distribute verbatim copies of this license document, but changing it **is not** allowed.

Preamble

The GNU General Public License **is** a free, copyleft license **for** software **and** other kinds of works.

The licenses **for** most software **and** other practical works are designed to take away your freedom to share **and** change the works. By contrast, the GNU General Public License **is** intended to guarantee your freedom to share **and** change all versions of a program--to make sure it remains free software **for** all its users. We, the Free Software Foundation, use the GNU General Public License **for** most of our software; it applies also to **any** other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, **not** price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (**and** charge **for** them **if** you wish), that you receive source code **or** can get it **if** you want it, that you can change the software **or** use pieces of it **in** new free programs, **and** that you know you can do these things.

To protect your rights, we need to prevent others **from denying** you these rights **or** asking you to surrender the rights. Therefore, you have certain responsibilities **if** you distribute copies of the software, **or if** you modify it: responsibilities to respect the freedom of others.

For example, **if** you distribute copies of such a program, whether gratis **or for** a fee, you must **pass** on to the recipients the same freedoms that you received. You must make sure that they, too, receive **or** can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights **with** two steps: (1) **assert** copyright on the software, **and** (2) offer you this License giving you legal permission to copy, distribute **and/or** modify it.

For the developers' **and authors'** protection, the GPL clearly explains that there **is** no warranty **for** this free software. For both users' **and authors'** sake, the GPL requires that **modified versions be marked as** changed, so that their problems will **not** be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install **or** run modified versions of the software inside them, although the manufacturer can do so. This **is** fundamentally incompatible **with** the aim of protecting users' **freedom to change the software**. The **systematic** pattern of such abuse occurs **in** the area of products **for** individuals to use, which **is** precisely where it **is** most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice **for** those products. If such problems arise substantially **in** other domains, we stand ready to extend this provision to those domains **in** future versions of the GPL, **as** needed to protect the freedom of users.

Finally, every program **is** threatened constantly by software patents. States should **not** allow patents to restrict development **and** use of software on general-purpose computers, but **in** those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms **and** conditions **for** copying, distribution **and** modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such **as** semiconductor masks.

"The Program" refers to **any** copyrightable work licensed under this License. Each licensee **is** addressed **as** "you". "Licensees" **and** "recipients" may be individuals **or** organizations.

To "modify" a work means to copy **from or** adapt **all or** part of the work **in** a fashion requiring copyright permission, other than the making of an exact copy. The resulting work **is** called a "modified version" of the earlier work **or** a work "based on" the earlier work.

A "covered work" means either the unmodified Program **or** a work based on the Program.

To "propagate" a work means to do anything **with** it that, without permission, would make you directly **or** secondarily liable **for** infringement under applicable copyright law, **except** executing it on a computer **or** modifying a private copy. Propagation includes copying, distribution (**with or** without modification), making available to the public, **and in** some countries other activities **as** well.

To "convey" a work means **any** kind of propagation that enables other parties to make **or** receive copies. Mere interaction **with** a user through a computer network, **with** no transfer of a copy, **is not** conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient **and** prominently visible feature that (1) displays an appropriate copyright notice, **and** (2) tells the user that there **is** no warranty **for** the work (**except** to the extent that warranties are provided), that licensees may convey the work under this License, **and** how to view a copy of this License. If the interface presents a **list** of user commands **or** options, such **as** a menu, a prominent item **in** the **list** meets this criterion.

1. Source Code.

The "source code" **for** a work means the preferred form of the work **for** making modifications to it. "Object code" means **any** non-source form of a work.

A "Standard Interface" means an interface that either **is** an official standard defined by a recognized standards body, **or, in** the case of interfaces specified **for** a particular programming language, one that **is** widely used among developers working **in** that language.

The "System Libraries" of an executable work include anything, other than the work **as** a whole, that (a) **is** included **in** the normal form of packaging a Major Component, but which **is not** part of that Major Component, **and** (b) serves only to enable use of the work **with** that Major Component, **or** to implement a Standard Interface **for** which an implementation **is** available to the public **in** source code form. A "Major Component", **in** this context, means a major essential component (kernel, window system, **and** so on) of the specific operating system (**if any**) on which the executable work runs, **or** a compiler used to produce the work, **or** an **object** code interpreter used to run it.

The "Corresponding Source" **for** a work **in** object code form means **all** the source code needed to generate, install, **and** (**for** an executable work) run the **object** code **and** to modify the work, including scripts to control those activities. However, it does **not** include the work's System Libraries, **or** general-purpose tools **or** generally available free programs which are used unmodified **in** performing those activities but which are **not** part of the work. For example, Corresponding Source includes interface definition files associated **with** source files **for** the work, **and** the source code **for** shared libraries **and** dynamically linked subprograms that the work **is** specifically designed to require, such **as** by intimate data communication **or** control flow between those subprograms **and** other parts of the work.

The Corresponding Source need **not** include anything that users can regenerate automatically **from other** parts of the Corresponding

Source.

The Corresponding Source **for** a work **in** source code form **is** that same work.

2. Basic Permissions.

All rights granted under this License are granted **for** the term of copyright on the Program, **and** are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output **from running** a covered work **is** covered by this License only **if** the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use **or** other equivalent, **as** provided by copyright law.

You may make, run **and** propagate covered works that you do **not** convey, without conditions so long **as** your license otherwise remains **in** force. You may convey covered works to others **for** the sole purpose of having them make modifications exclusively **for** you, **or** provide you **with** facilities **for** running those works, provided that you comply **with** the terms of this License **in** conveying **all** material **for** which you do **not** control copyright. Those thus making **or** running the covered works **for** you must do so exclusively on your behalf, under your direction **and** control, on terms that prohibit them **from making** any copies of your copyrighted material outside their relationship **with** you.

Conveying under **any** other circumstances **is** permitted solely under the conditions stated below. Sublicensing **is not** allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under **any** applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, **or** similar laws prohibiting **or** restricting circumvention of such measures.

When you convey a covered work, you waive **any** legal power to forbid circumvention of technological measures to the extent such circumvention **is** effected by exercising rights under this License **with** respect to the covered work, **and** you disclaim **any** intention to limit operation **or** modification of the work **as** a means of enforcing, against the work's users, your **or** third parties' **legal rights to forbid circumvention of** technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's **source code as you** receive it, **in any** medium, provided that you conspicuously **and** appropriately publish on each copy an appropriate copyright notice; keep intact **all** notices stating that this License **and any** non-permissive terms added **in accord with** section 7 apply to the code; keep intact **all** notices of the absence of **any** warranty; **and** give **all** recipients a copy of this License along **with** the Program.

You may charge **any** price **or** no price **for** each copy that you convey, **and** you may offer support **or** warranty protection **for** a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, **or** the modifications to produce it **from the** Program, **in** the form of source code under the terms of section 4, provided that you also meet **all** of these conditions:

- a) The work must carry prominent notices stating that you modified it, **and** giving a relevant date.
- b) The work must carry prominent notices stating that it **is** released under this License **and any** conditions added under section 7. This requirement modifies the requirement **in** section 4 to "**keep intact all notices**".
- c) You must license the entire work, **as** a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along **with any** applicable section 7 additional terms, to the whole of the work, **and all** its parts, regardless of how they are packaged. This License gives no permission to license the work **in any** other way, but it does **not** invalidate such permission **if** you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, **if** the Program has interactive interfaces that do **not** display Appropriate Legal Notices, your work need **not** make them do so.

A compilation of a covered work **with** other separate **and** independent works, which are **not** by their nature extensions of the covered work, **and** which are **not** combined **with** it such **as** to form a larger program, **in or** on a volume of a storage **or** distribution medium, **is** called an "aggregate" **if** the compilation **and** its resulting copyright are **not** used to limit the access **or** legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work **in** an aggregate does **not** cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work **in** object code form under the terms of sections 4 **and** 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, **in** one of these ways:

- a) Convey the **object** code **in, or** embodied **in**, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used **for** software interchange.
- b) Convey the **object** code **in, or** embodied **in**, a physical product (including a physical distribution medium), accompanied by a written offer, valid **for** at least three years **and** valid **for as long as** you offer spare parts **or** customer support **for** that product model, to give anyone who possesses the **object** code either (1) a copy of the Corresponding Source **for all** the software **in** the product that **is** covered by this License, on a durable physical medium customarily used **for** software interchange, **for** a price no

more than your reasonable cost of physically performing this conveying of source, **or** (2) access to copy the Corresponding Source **from a** network server at no charge.

c) Convey individual copies of the **object** code **with** a copy of the written offer to provide the Corresponding Source. This alternative **is** allowed only occasionally **and** noncommercially, **and** only **if** you received the **object** code **with** such an offer, **in** accord **with** subsection 6b.

d) Convey the **object** code by offering access **from a** designated place (gratis **or for** a charge), **and** offer equivalent access to the Corresponding Source **in** the same way through the same place at no further charge. You need **not** require recipients to copy the Corresponding Source along **with** the **object** code. If the place to copy the **object** code **is** a network server, the Corresponding Source may be on a different server (operated by you **or** a third party) that supports equivalent copying facilities, provided you maintain clear directions **next** to the **object** code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it **is** available **for as long as** needed to satisfy these requirements.

e) Convey the **object** code using peer-to-peer transmission, provided you inform other peers where the **object** code **and** Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the **object** code, whose source code **is** excluded **from the** Corresponding Source **as** a System Library, need **not** be included **in** conveying the **object** code work.

A "User Product" **is** either (1) a "consumer product", which means any tangible personal **property** which **is** normally used **for** personal, family, **or** household purposes, **or** (2) anything designed **or** sold **for** incorporation into a dwelling. In determining whether a product **is** a consumer product, doubtful cases shall be resolved **in** favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical **or** common use of that **class of** product, regardless of the status of the particular user **or** of the way **in** which the particular user actually uses, **or** expects **or is** expected to use, the product. A product **is** a consumer product regardless of whether the product has substantial commercial, industrial **or** non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" **for** a User Product means any methods, procedures, authorization keys, **or** other information required to install **and** execute modified versions of a covered work **in** that User Product **from a** modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified **object** code **is in** no case prevented **or** interfered **with** solely because modification has been made.

If you convey an **object** code work under this section **in, or with, or** specifically **for** use **in**, a User Product, **and** the conveying occurs **as** part of a transaction **in** which the right of possession **and** use of the User Product **is** transferred to the recipient **in** perpetuity **or for** a fixed term (regardless of how the transaction **is** characterized), the

Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does **not** apply **if** neither you nor **any** third party retains the ability to install modified **object** code on the User Product (**for** example, the work has been installed **in** ROM).

The requirement to provide Installation Information does **not** include a requirement to **continue** to provide support service, warranty, **or** updates **for** a work that has been modified **or** installed by the recipient, **or for** the User Product **in** which it has been modified **or** installed. Access to a network may be denied when the modification itself materially **and** adversely affects the operation of the network **or** violates the rules **and** protocols **for** communication across the network.

Corresponding Source conveyed, **and** Installation Information provided, **in** accord **with** this section must be **in** a **format** that **is** publicly documented (**and with** an implementation available to the public **in** source code form), **and** must require no special password **or** key **for** unpacking, reading **or** copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions **from one or** more of its conditions. Additional permissions that are applicable to the entire Program shall be treated **as** though they were included **in** this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove **any** additional permissions **from that** copy, **or from any** part of it. (Additional permissions may be written to require their own removal **in** certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, **for** which you have **or** can give appropriate copyright permission.

Notwithstanding **any** other provision of this License, **for** material you add to a covered work, you may (**if** authorized by the copyright holders of that material) supplement the terms of this License **with** terms:

- a) Disclaiming warranty **or** limiting liability differently **from the** terms of sections 15 **and** 16 of this License; **or**
- b) Requiring preservation of specified reasonable legal notices **or** author attributions **in** that material **or in** the Appropriate Legal Notices displayed by works containing it; **or**
- c) Prohibiting misrepresentation of the origin of that material, **or** requiring that modified versions of such material be marked **in** reasonable ways **as** different **from the** original version; **or**
- d) Limiting the use **for** publicity purposes of names of licensors **or** authors of the material; **or**
- e) Declining to grant rights under trademark law **for** use of some trade names, trademarks, **or** service marks; **or**

f) Requiring indemnification of licensors **and** authors of that material by anyone who conveys the material (**or** modified versions of it) **with** contractual assumptions of liability to the recipient, **for** any liability that these contractual assumptions directly impose on those licensors **and** authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, **or** any part of it, contains a notice stating that it **is** governed by this License along **with** a term that **is** a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing **or** conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does **not** survive such relicensing **or** conveying.

If you add terms to a covered work **in** accord **with** this section, you must place, **in** the relevant source files, a statement of the additional terms that apply to those files, **or** a notice indicating where to find the applicable terms.

Additional terms, permissive **or** non-permissive, may be stated **in** the form of a separately written license, **or** stated **as** exceptions; the above requirements apply either way.

8. Termination.

You may **not** propagate **or** modify a covered work **except as** expressly provided under this License. Any attempt otherwise to propagate **or** modify it **is** void, **and** will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, **if** you cease all violation of this License, then your license **from a** particular copyright holder **is** reinstated (a) provisionally, unless **and** until the copyright holder explicitly **and finally** terminates your license, **and** (b) permanently, **if** the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license **from a** particular copyright holder **is** reinstated permanently **if** the copyright holder notifies you of the violation by some reasonable means, this **is** the first time you have received notice of violation of this License (**for any work**) **from that** copyright holder, **and** you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does **not** terminate the licenses of parties who have received copies **or** rights **from you** under this License. If your rights have been terminated **and not** permanently reinstated, you do **not** qualify to receive new licenses **for** the same material under section 10.

9. Acceptance Not Required **for** Having Copies.

You are **not** required to accept this License **in** order to receive **or** run a copy of the Program. Ancillary propagation of a covered work

occurring solely **as** a consequence of using peer-to-peer transmission to receive a copy likewise does **not** require acceptance. However, nothing other than this License grants you permission to propagate **or** modify **any** covered work. These actions infringe copyright **if** you do **not** accept this License. Therefore, by modifying **or** propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license **from the** original licensors, to run, modify **and** propagate that work, subject to this License. You are **not** responsible **for** enforcing compliance by third parties **with** this License.

An "entity transaction" **is** a transaction transferring control of an organization, **or** substantially all assets of one, **or** subdividing an organization, **or** merging organizations. If propagation of a covered work results **from an** entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had **or could** give under the previous paragraph, plus a right to possession of the Corresponding Source of the work **from the** predecessor **in** interest, **if** the predecessor has it **or** can get it **with** reasonable efforts.

You may **not** impose **any** further restrictions on the exercise of the rights granted **or** affirmed under this License. For example, you may **not** impose a license fee, royalty, **or** other charge **for** exercise of rights granted under this License, **and** you may **not** initiate litigation (including a cross-claim **or** counterclaim **in** a lawsuit) alleging that **any** patent claim **is** infringed by making, using, selling, offering **for** sale, **or** importing the Program **or any** portion of it.

11. Patents.

A "contributor" **is** a copyright holder who authorizes use under this License of the Program **or** a work on which the Program **is** based. The work thus licensed **is** called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned **or** controlled by the contributor, whether already acquired **or** hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, **or** selling its contributor version, but do **not** include claims that would be infringed only **as** a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses **in** a manner consistent **with** the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer **for** sale, **import and** otherwise run, modify **and** propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" **is any** express agreement **or** commitment, however denominated, **not** to enforce a patent (such **as** an express permission to practice a patent **or** covenant **not** to sue **for** patent infringement). To "grant" such a patent license to a party means to make such an agreement **or** commitment **not** to enforce a

patent against the party.

If you convey a covered work, knowingly relying on a patent license, **and** the Corresponding Source of the work **is not** available **for** anyone to copy, free of charge **and** under the terms of this License, through a publicly available network server **or** other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, **or** (2) arrange to deprive yourself of the benefit of the patent license **for** this particular work, **or** (3) arrange, **in** a manner consistent **with** the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but **for** the patent license, your conveying the covered work **in** a country, **or** your recipient's use of the covered work **in** a country, would infringe one **or** more identifiable patents **in** that country that you have reason to believe are valid.

If, pursuant to **or in** connection **with** a single transaction **or** arrangement, you convey, **or** propagate by procuring conveyance of, a covered work, **and** grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify **or** convey a specific copy of the covered work, then the patent license you grant **is** automatically extended to **all** recipients of the covered work **and** works based on it.

A patent license **is** "discriminatory" **if** it does **not** include within the scope of its coverage, prohibits the exercise of, **or is** conditioned on the non-exercise of one **or** more of the rights that are specifically granted under this License. You may **not** convey a covered work **if** you are a party to an arrangement **with** a third party that **is in** the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, **and** under which the third party grants, to **any** of the parties who would receive the covered work **from you**, a discriminatory patent license (a) **in** connection **with** copies of the covered work conveyed by you (**or** copies made **from those** copies), **or** (b) primarily **for and in** connection **with** specific products **or** compilations that contain the covered work, unless you entered into that arrangement, **or** that patent license was granted, prior to 28 March 2007.

Nothing **in** this License shall be construed **as** excluding **or** limiting **any** implied license **or** other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement **or** otherwise) that contradict the conditions of this License, they do **not** excuse you **from the** conditions of this License. If you cannot convey a covered work so **as** to satisfy simultaneously your obligations under this License **and** any other pertinent obligations, then **as** a consequence you may **not** convey it at **all**. For example, **if** you agree to terms that obligate you to collect a royalty **for** further conveying **from those** to whom you convey the Program, the only way you could satisfy both those terms **and** this License would be to refrain entirely **from conveying** the Program.

13. Use **with** the GNU Affero General Public License.

Notwithstanding **any** other provision of this License, you have

permission to link **or** combine **any** covered work **with** a work licensed under version 3 of the GNU Affero General Public License into a single combined work, **and** to convey the resulting work. The terms of this License will **continue** to apply to the part which **is** the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination **as** such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised **and/or** new versions of the GNU General Public License **from time** to time. Such new versions will be similar **in** spirit to the present version, but may differ **in** detail to address new problems **or** concerns.

Each version **is** given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "**or any later version**" applies to it, you have the option of following the terms **and** conditions either of that numbered version **or** of **any** later version published by the Free Software Foundation. If the Program does **not** specify a version number of the GNU General Public License, you may choose **any** version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version **for** the Program.

Later license versions may give you additional **or** different permissions. However, no additional obligations are imposed on **any** author **or** copyright holder **as** a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "**AS IS**" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 **and** 16.

If the disclaimer of warranty **and** limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability **in** connection **with** the Program, unless a warranty **or** assumption of liability accompanies a copy of the Program **in return for** a fee.

END OF TERMS AND CONDITIONS

The development of the VMCloak project has been sponsored by the iTES Project, a research project between Avira and the German Federal Ministry of Education and Research.



nLite

Without the help of nLite this tool would probably not have been as complete as it is now. Inspiration on how to design the output ISO files has for a large part been derived from changes observed by nLite.

CHAPTER 10

Indices and tables

- `genindex`
- `modindex`
- `search`