# Статья Создание локального Runtime чекера антивирусами.

xss.is/threads/33978

Статья не новая(год ей), но как автор перепубликую ее тут.

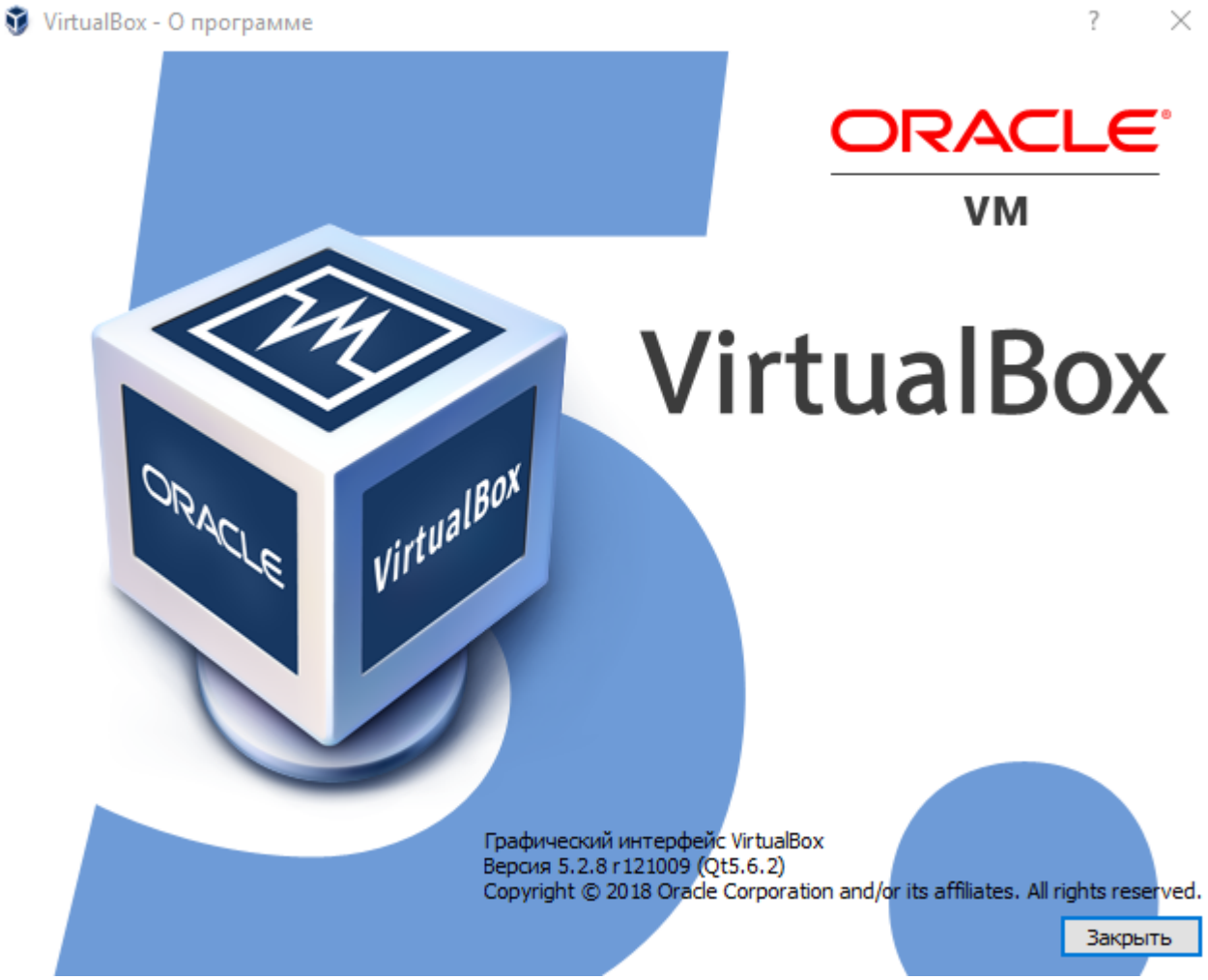
Создание локального Runtime чекера антивирусами.

Все привет, наконец то я нашел время и как обещал выкладываю стать о том как сделать чекера на динамические детекты антивирусов (Runtime Detect Checker) на локальной машине.

Я сделал этот проект два годна назад, т.к. мне было жалко платить подобным сервисам, да и редко надо. Писал я для себя на питоне со своими нюансами, в нашем же случаи для статьи я сделал проще на bat-никах. И самое интересно мне друзья дали еще чужие исходники на php, где написан сервис на подобии как у меня на Python'е с тем же принципом, что в статье.
И так все по порядку.

**0. Методика**
Вся суть методики: скоростное и эффективное создание одноразовых виртуальных машин с антивирусами на основе шаблонов, независимой заливкой файла и его запуском. Определение детектов происходит на основе скриншотов.

**1. Ставим виртуальную машину.**
Мы будем использовать виртуальную машину Virtual Box версии 5.28.8 x64 (обращаю ваше внимание, что API может отличаться в зависимости от релизов) на в операционной системе Windows(можно и на Linux, но локалка у меня виндовская).
1.png



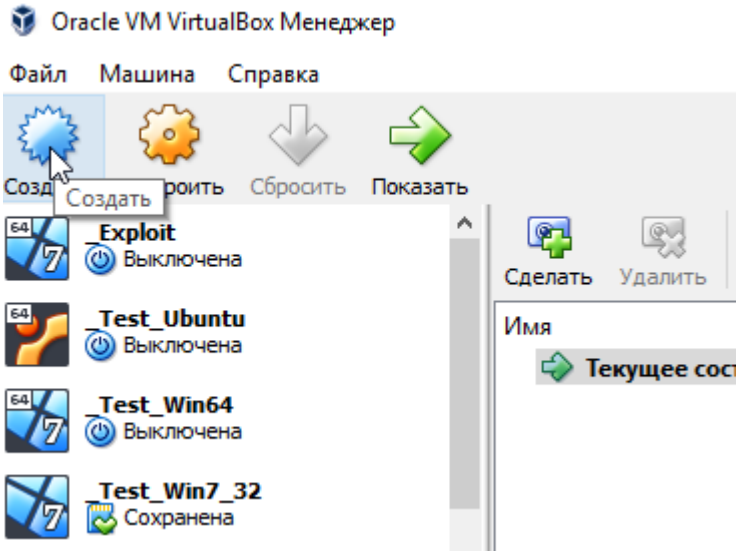

Выбираем x64 версия для Windows, скачиваем VirtualBox тут
http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html

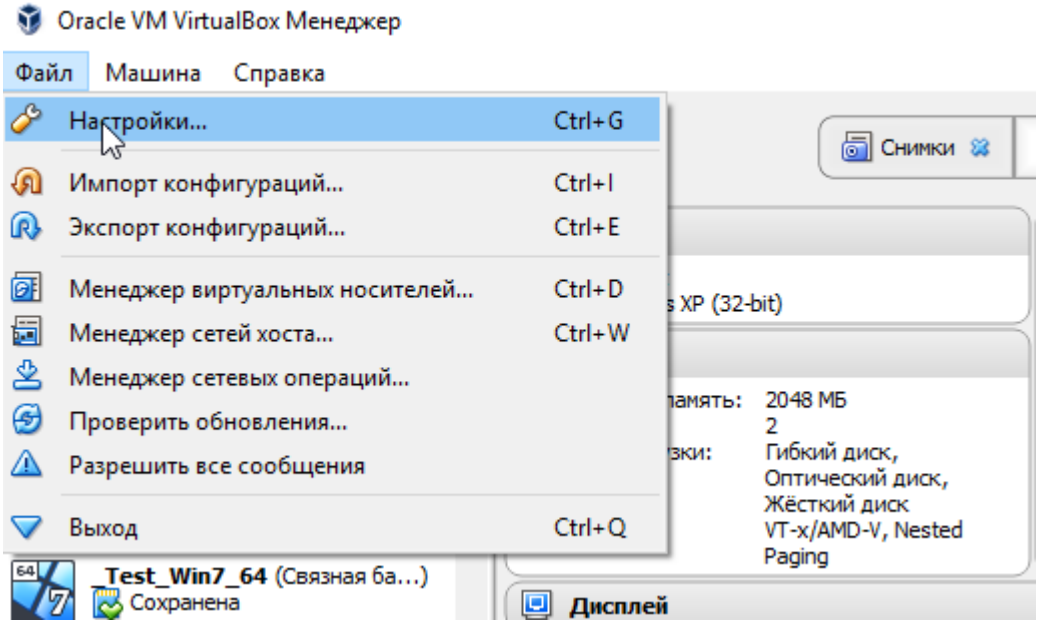
**2. Создаем шаблон ОС**

Я делал виртуальную машину на Win7x64 и на Win10x64 потому что многие антивирусы ниже семерки уже не поддерживаются, да и с Win7 недавно натолкнулся на проблемы. Если машина позволяет рекомендую Windows 10 x64. Хотел бы обратить внимание на то что процессор должен поддерживать аппаратную виртуализцию VT-x/AMD-V (https://ru.wikipedia.org/wiki/Аппаратная_виртуализация) и Hyper-threading (https://ru.wikipedia.org/wiki/Hyper-threading),
проверьте чтобы было включено в Bios'e. У меня Intel i7 на 3800Гц 8 ядер.
Если у вас нету хардварной виртуализции, то думаю статья эта вам не поможет, т.к. ВМ и сам компьютер будут ужасно тормазить и смысла ставить ВМ нету.
Так же стоит заранее позаботиться о свободном месте на жестком диске HDD(идеально конечно SSD), я рекомендую не менее 300Гб и желательно на отдельном жестком диске от основной операционной системы (иначе есть шанс ВМ

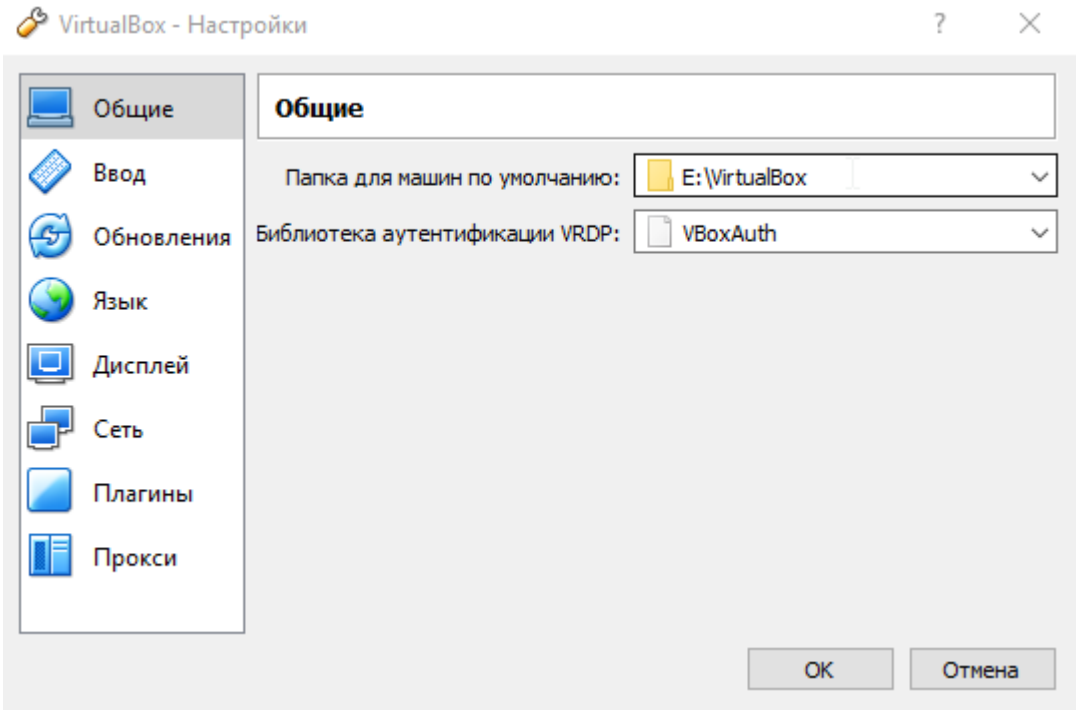
будут "давить" на жесткий диск, что будет отдавать на основную ОС). Про оперативную память - должно хватить 8Гб, но желательно иметь 16Гб.
Настраиваем месторасположения всем ВМ
2.png

3.png



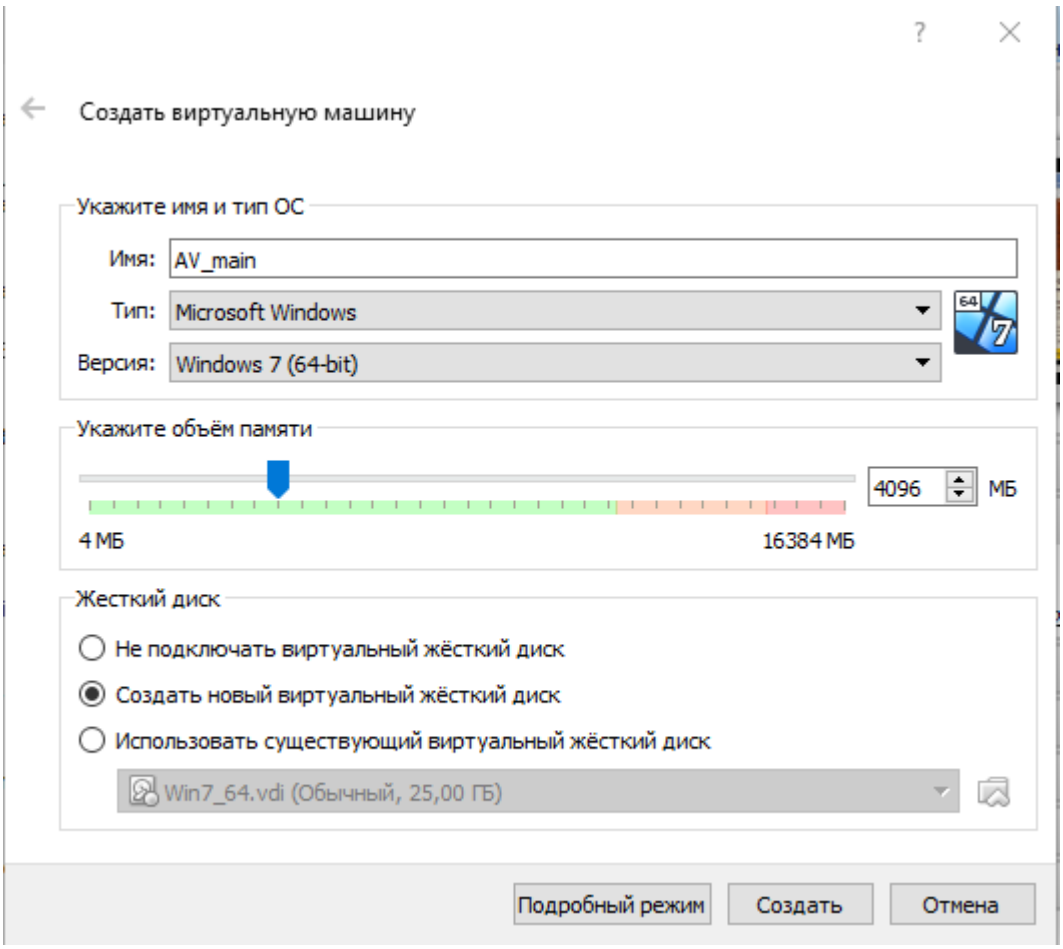




Для создания ВМ(виртуальной машины) надо запустить VirtualBox и нажать на иконку
4.png

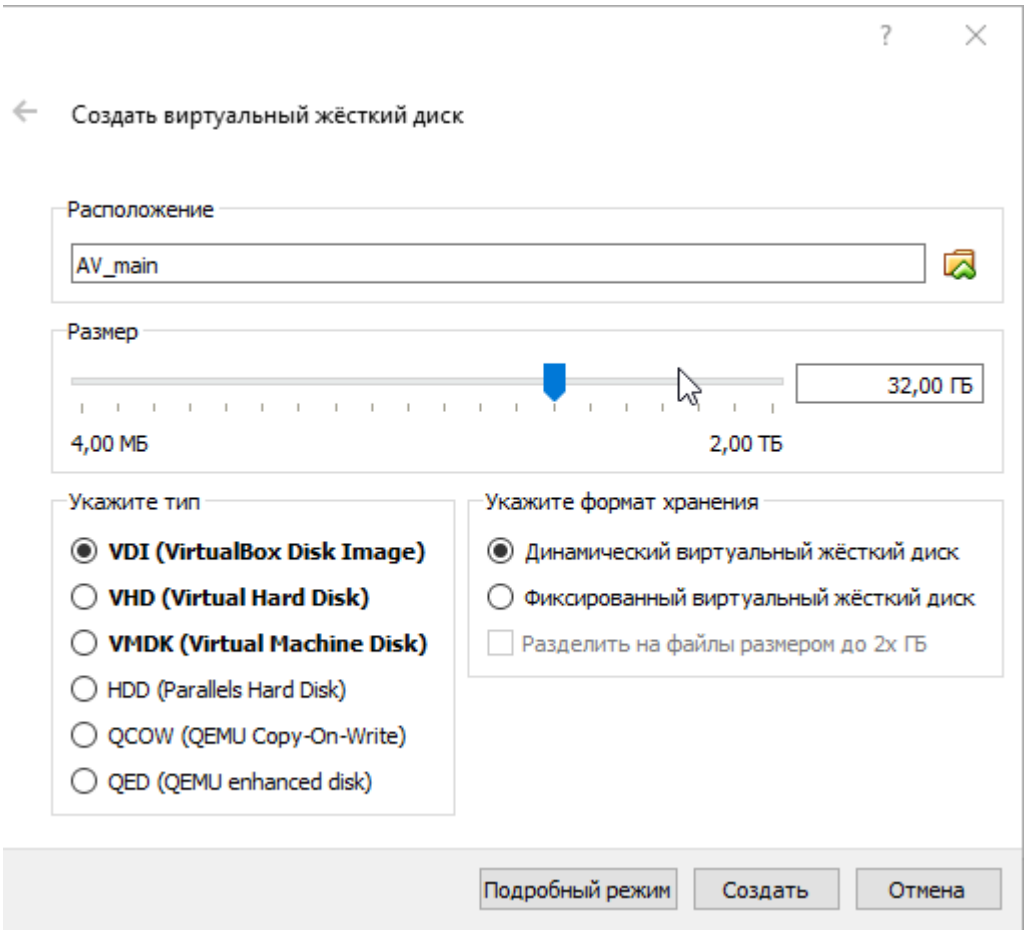



Выставляем название основного шаблона AV_main на нем мы настроим ОС и потом клонируем на шаблоны для антивирусов.

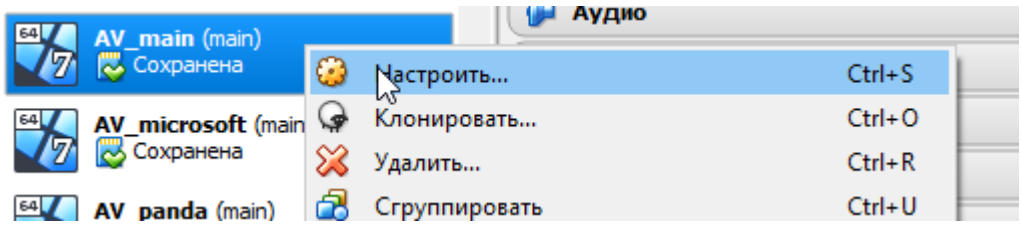
5.png



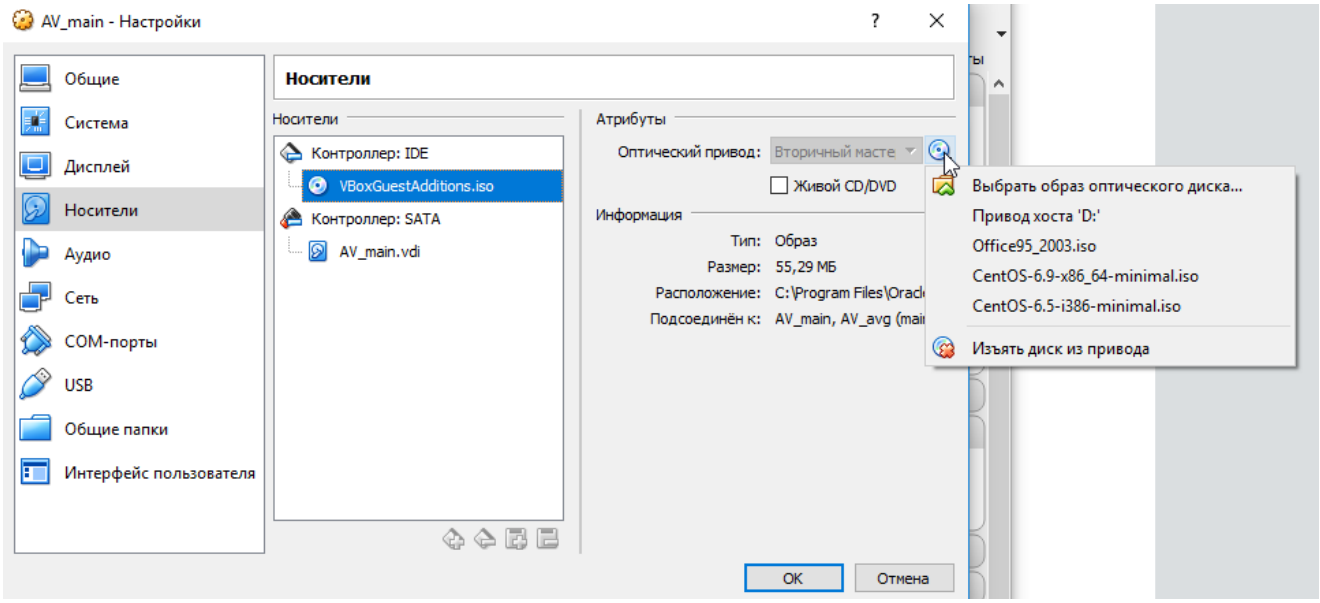
Ничего не трогаем, жмем Создать. После создания ВМ, находим ее в списке, выбираем и правой клавишей мышки на ней переходим в Настройки ВМ.
6.png



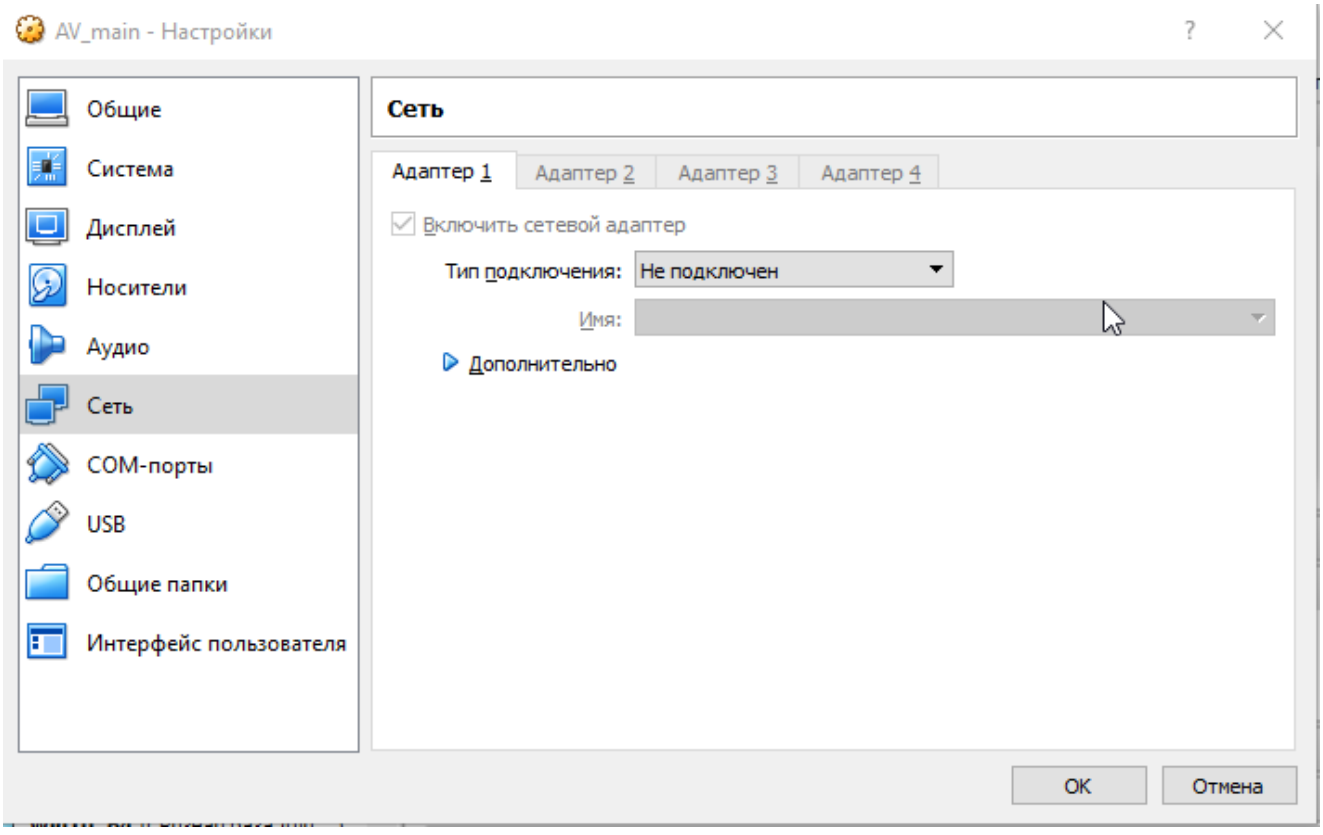

7.png



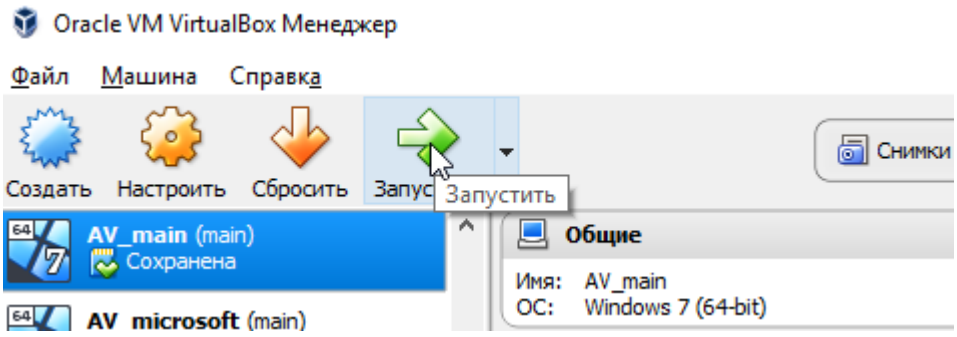

В настройках выбираем носители и в IDE контроллере выбираем Оптический привод, находим iso образ с установщиком Windows (в нашем случае это будет Win7x64)
8.png




В настройках выбираем сеть и оставляем Не подключен, чтобы ОС не смогла обновиться и не смогла отсылать данные. Жмем ОК, настройка самой ВМ готова.
9.png




Запускаем ВМ
10.png




**3. Настраиваем шаблон ОС**

Должно появиться окно ВМ с установкой Windows, ставим как обычно, НО:

**ВАЖНО!!! Имя юзера Admin пароль 12345**

После установки, необходимо ввести лицензию/кряк/кейген - на ваше усмотрение, но чтобы приложение которое лицензирует не висело в памяти, а то АВ его прихлопнут.

Для ускорения работы ВМ отключаем всякий трешь.

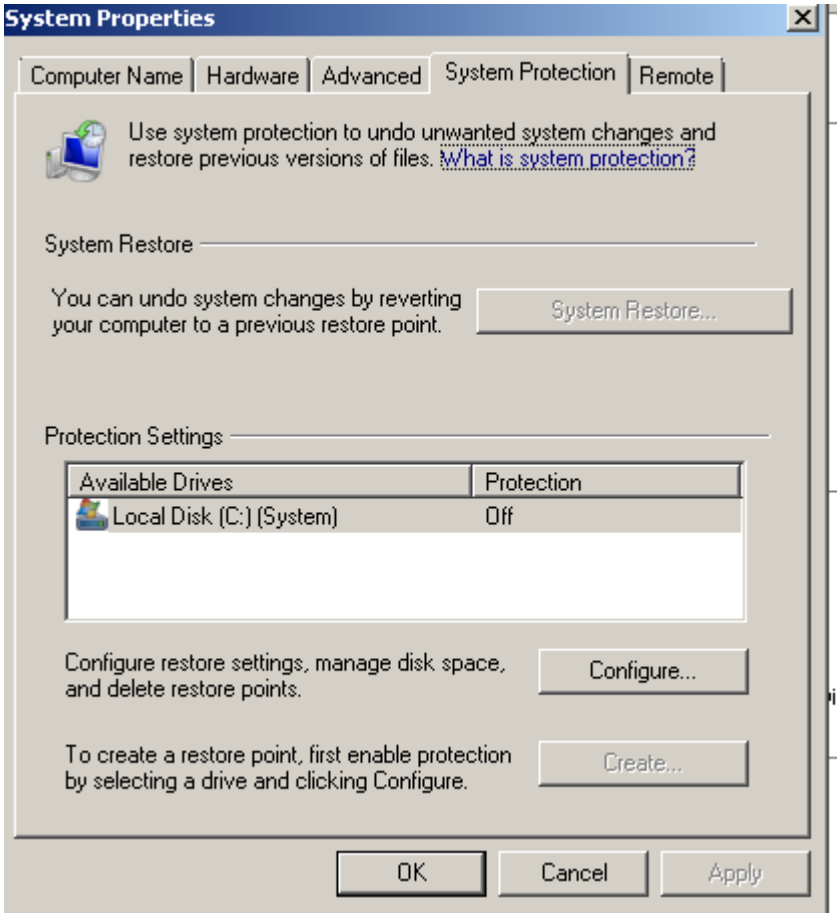
Отключаем службы: обновления, индексации файлов, кэширования и т.д.

11.png

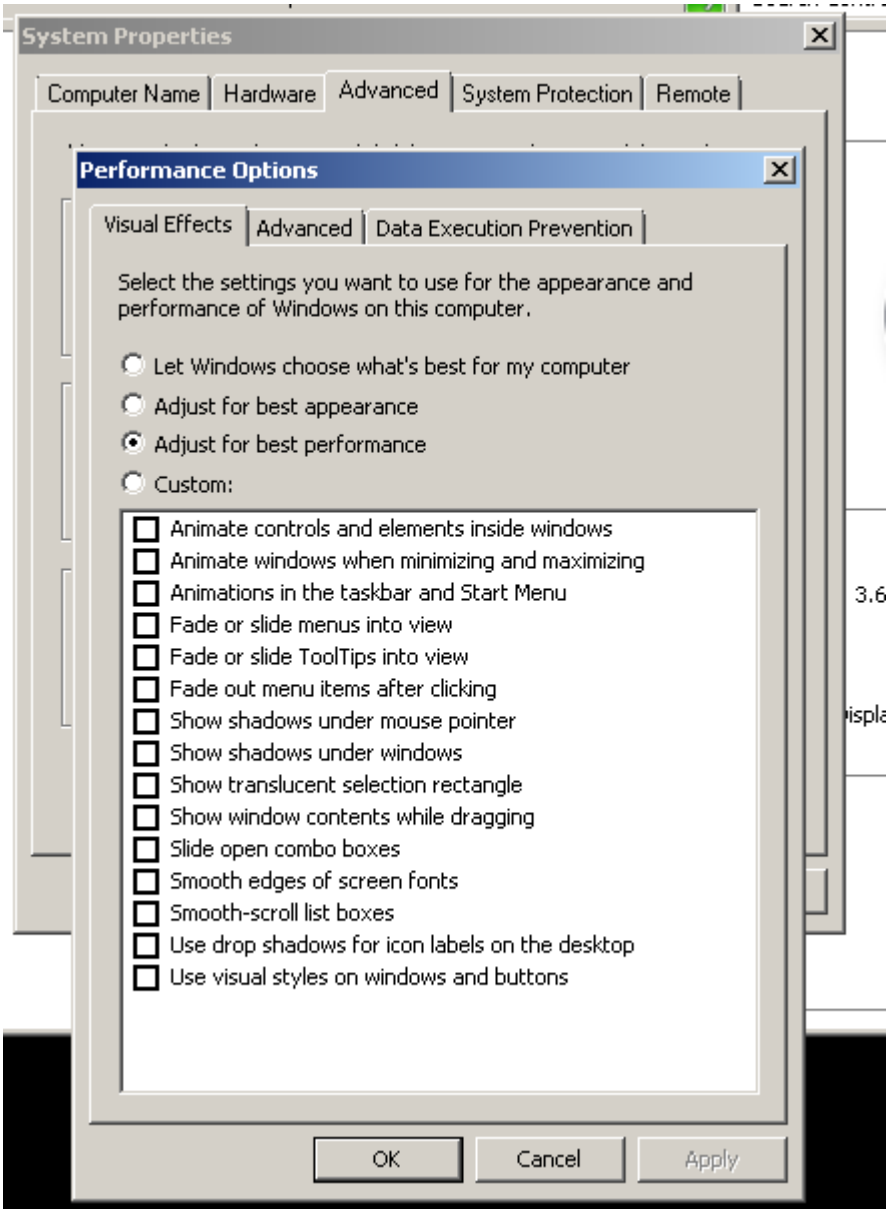
| | | | |
|---|---|---|---|
| Security Center | The WSCS... | Automatic (D... | Local Service |
| Software Protection | Enables th... | Disabled | Network S... |
| Windows Defender | Protection ... | Disabled | Local System |
| Windows Font Cache Service | Optimizes ... | Disabled | Local Service |
| Windows Search | Provides c... | Disabled | Local System |
| Windows Update | Enables th... | Disabled | Local System |
| BranchCache | This servic... | Disabled | Network S... |
| Google Update Service (gupdate) | Keeps your... | Disabled | Local System |
| Google Update Service (gupdatem) | Keeps your... | Disabled | Local System |
| Internet Connection Sharing (ICS) | Provides n... | Disabled | Local System |
| Media Center Extender Service | Allows Med... | Disabled | Local Service |
| Microsoft .NET Framework NGEN v2.0.50727_X64 | Microsoft .... | Disabled | Local System |
| Microsoft .NET Framework NGEN v2.0.50727_X86 | Microsoft .... | Disabled | Local System |
| Net.Tcp Port Sharing Service | Provides a... | Disabled | Local Service |
| Routing and Remote Access | Offers rout... | Disabled | Local System |
| Superfetch | Maintains a... | Disabled | Local System |

В альтернативных настройка, отключаем бэкапы

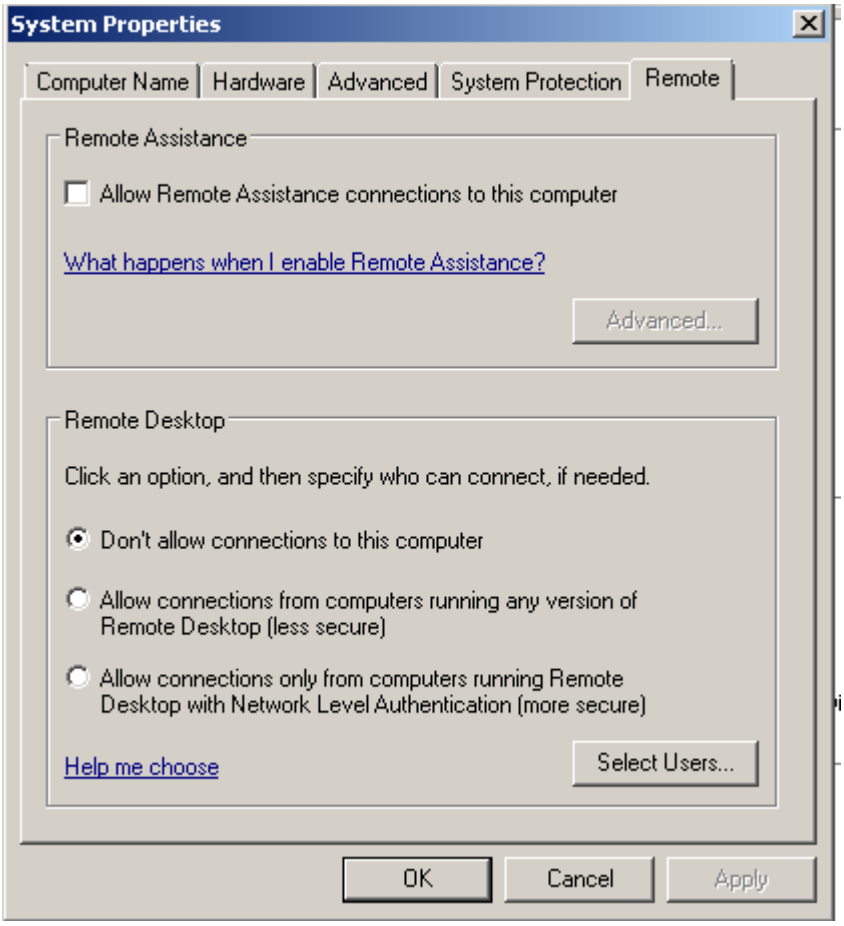
12.png



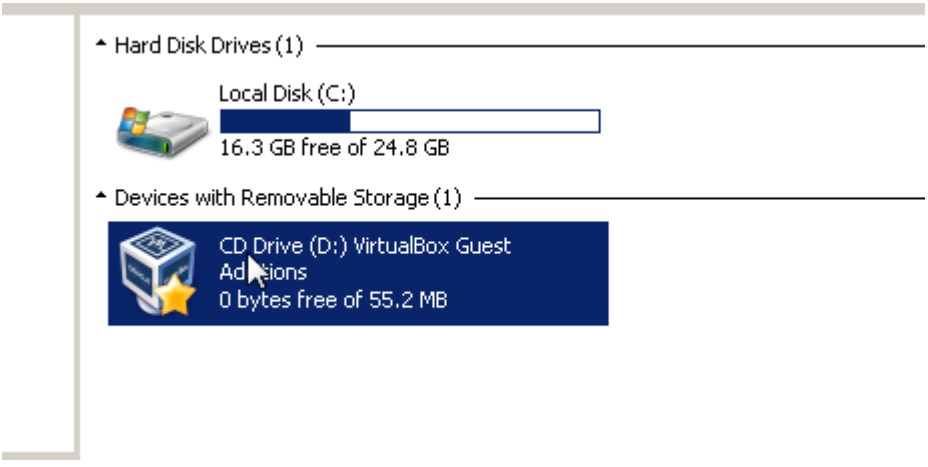

Ставим ускорение графики GUI
13.png



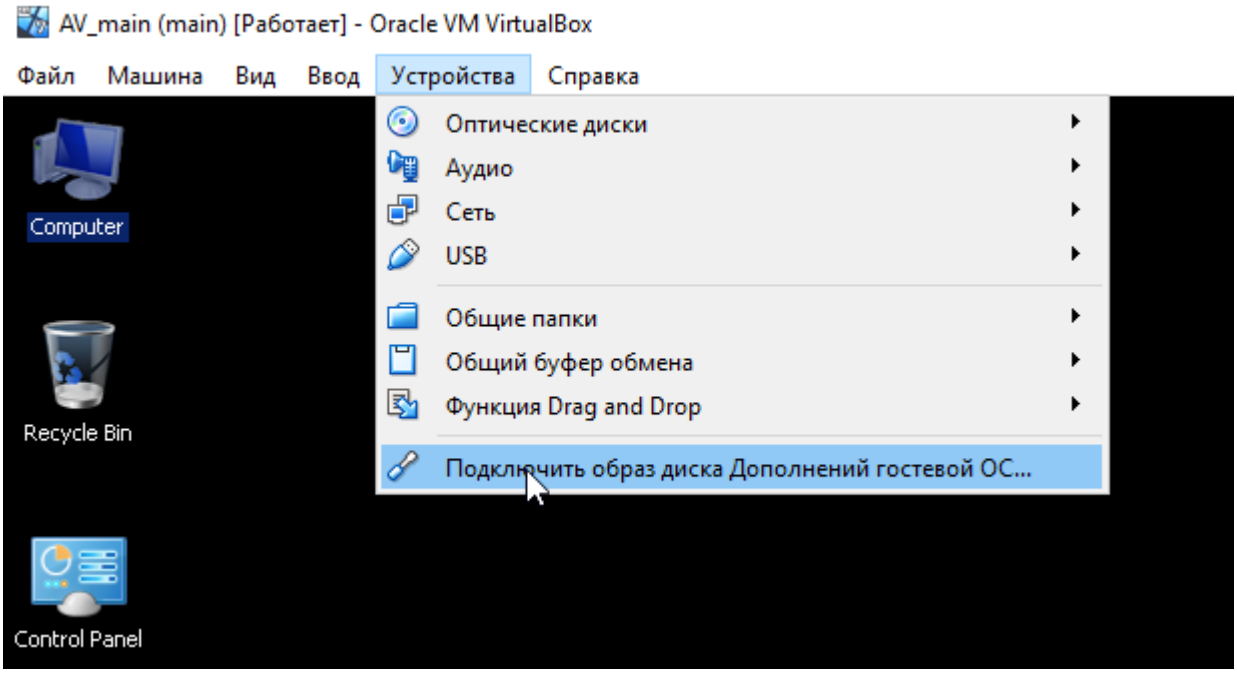

Убиваем удаленного помощника
14.png




Монтируем iso образ с VirtualBox Addons, устанавливаем драйвера и приложение VirtualBox Agent, если установка не началась то запустите вручную 17.png

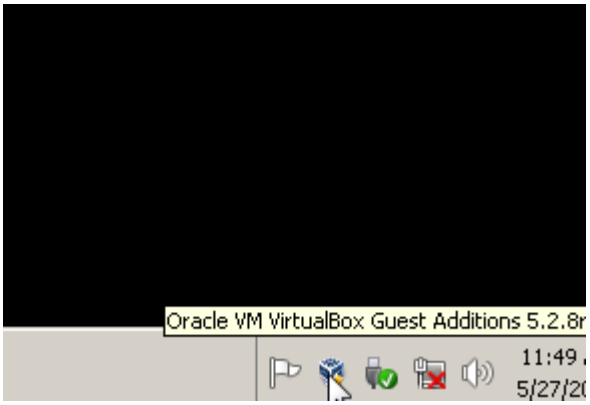



15.png



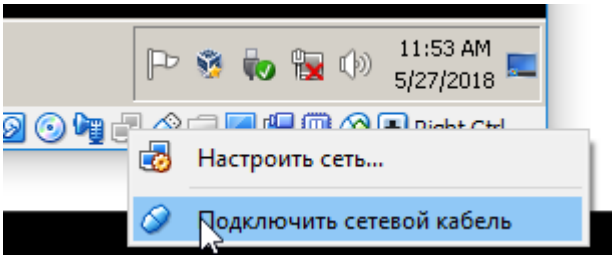

После установки и перезагрузки у вас появится значок приложения, значит вы все правильно сделали
16.png

Я еще установил Chrome для того чтобы потом на образах ВМ было легче антивирусы качать, только не забудте отключить службу обновления Хрома. Для скачивания я настроил
18.png



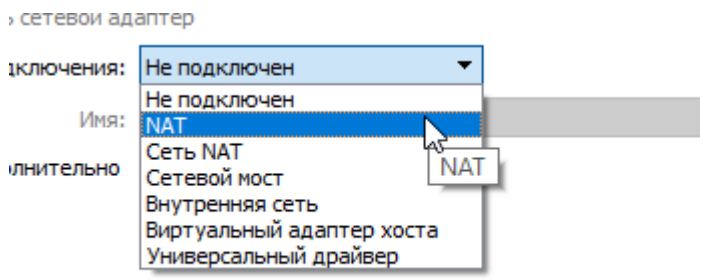

и подключил сеть
19.png

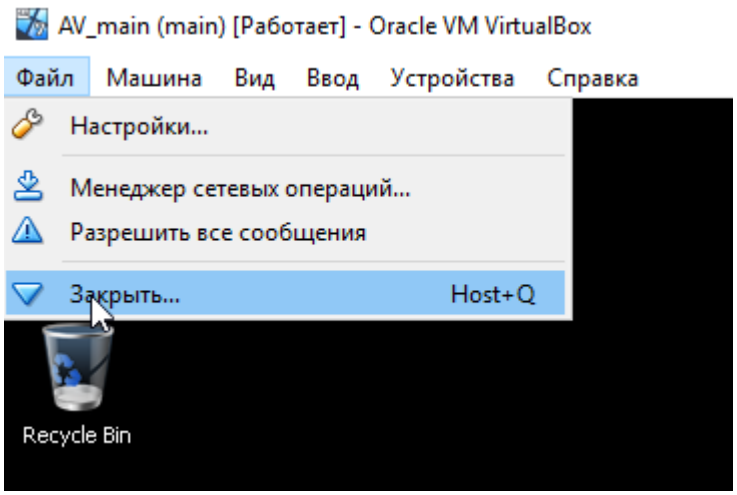
После всех установок надо отключить сеть, чтобы данные не утекали. Ну вот в принципе и готов шаблон ВМ с ОС, отключаем ВМ в Сохраненном состоянии, это даст нам существенное ускорение при запуске.
20.png

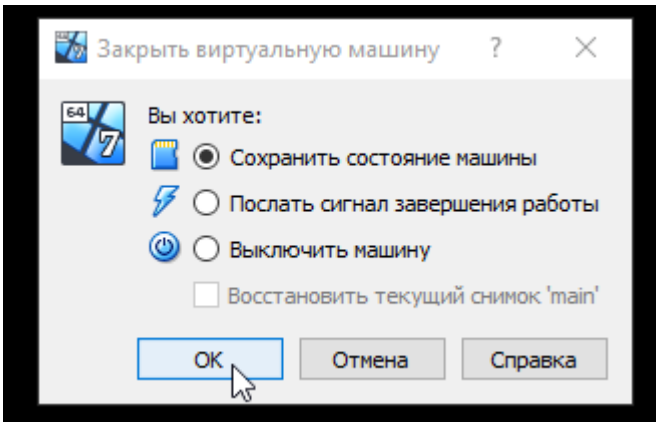


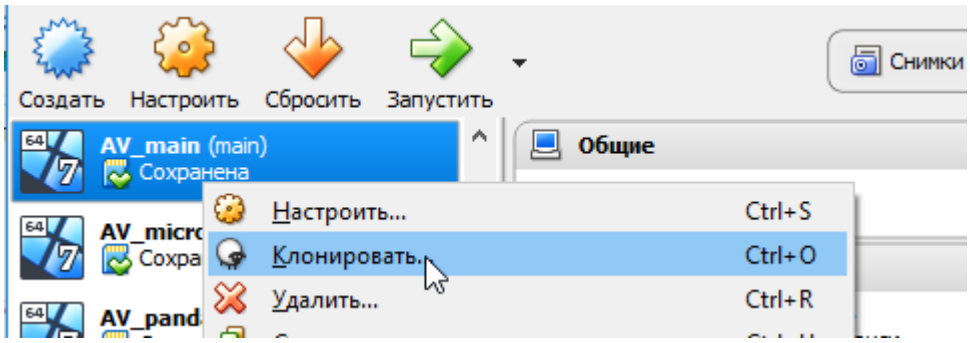

21.png

**4. Клонирование шаблона**
Выбираем наш шаблон и правым кликом мыши жмем Клонировать.
22.png

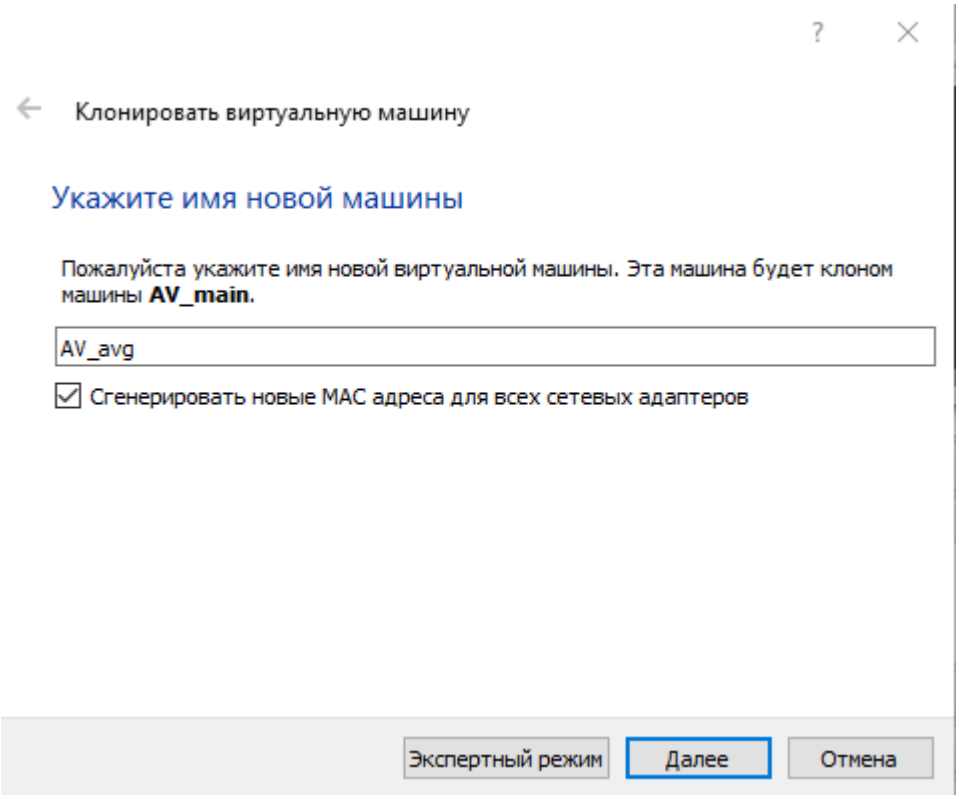

сетевой адаптер
ключения:
Не подключен
Имя:
лнительно
Не подключен
NAT
Сеть NAT
Сетевой мост
Внутренняя сеть
Виртуальный адаптер хоста
Универсальный драйвер
NAT


AV_main (main) [Работает] - Oracle VM VirtualBox
Файл
Машина
Вид
Ввод
Устройства
Справка
Настройки...
Менеджер сетевых операций...
Разрешить все сообщения
Закрыть...
Host+Q
Recycle Bin

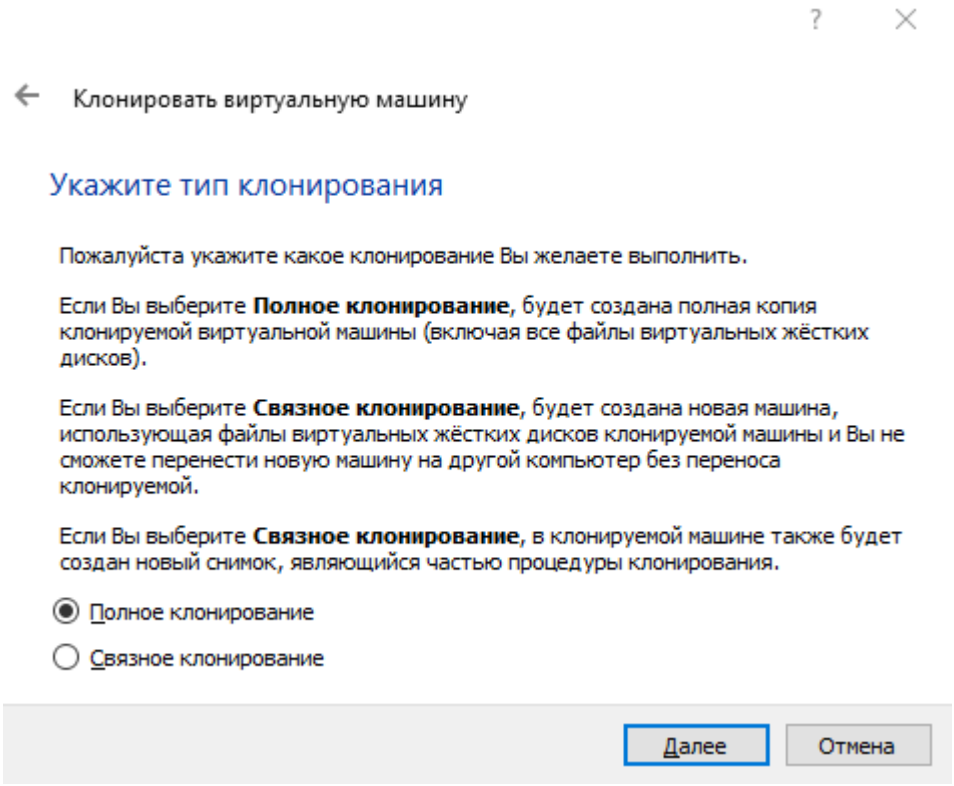

Закрыть виртуальную машину
Вы хотите:
Сохранить состояние машины
Послать сигнал завершения работы
Выключить машину
Восстановить текущий снимок 'main'
OK
Отмена
Справка


Создать
Настроить
Сбросить
Запустить
Снимки
AV_main (main)
Сохранена
Общие
Настроить...
Ctrl+S
Клонировать...
Ctrl+O
Удалить...
Ctrl+R

Подписываем новую ВМ (AV_avg, AV_avira, AV_kis и т.д.)- это будет шаблон ВМ с антивирусом, в нашем случае я выбрал AVG.
23.png




24.png

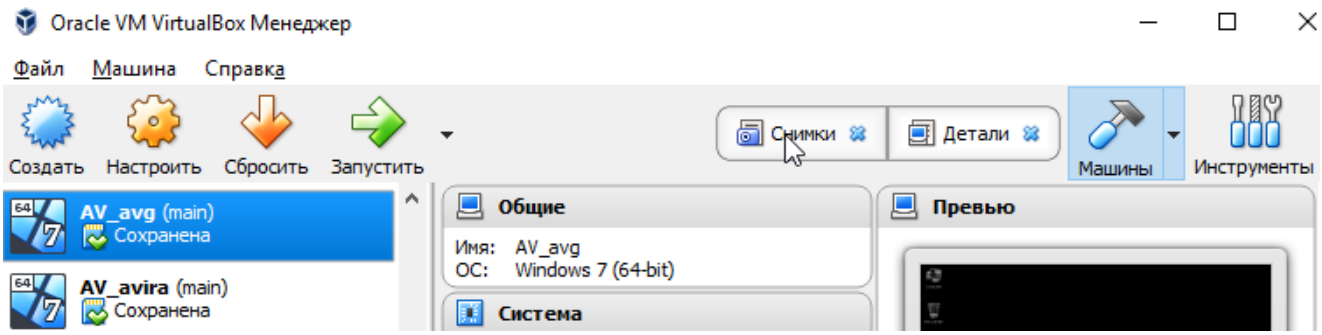



И так создаем все шаблоны ВМ для каждого антивируса который нам надо.

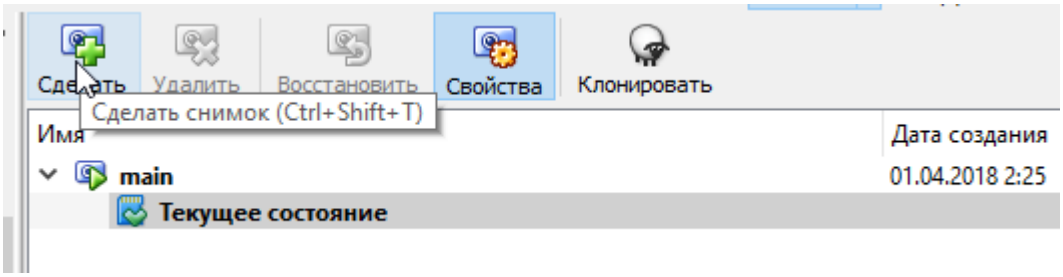
**5. Установка АВ на шаблоны**
После создания запускаем по очереди все виртуальные машины и на каждую ставим антивирус.
**ВАЖНО!!!: Незабываем включить сеть и после установки отключить, а ТАКЖЕ выключить ВМ с АВ в Сохраненном состоянии.**

**6. Создание срезов**
После подготовки шаблонов ВМ с АВ надо создать срезы (snapshot) - это фиксирование состояния ВМ для создания Связанной копии. Что это дает, это дает
нам быстрое создание копии ВМ из шаблона с нужным нам АВ, быстрый старт АВ, проверку exe и быстрое удаление ВМ без нагрузки на HDD/SDD
Срезы надо делать после обновления АВ в шаблонах.
**ВАЖНО!!! Перед созданием среза, убедитесь что остальные срезу удалены, иначе будут ошибки. На каждом шаблоне ВМ с АВ должен быть один срез с названием - "main"**

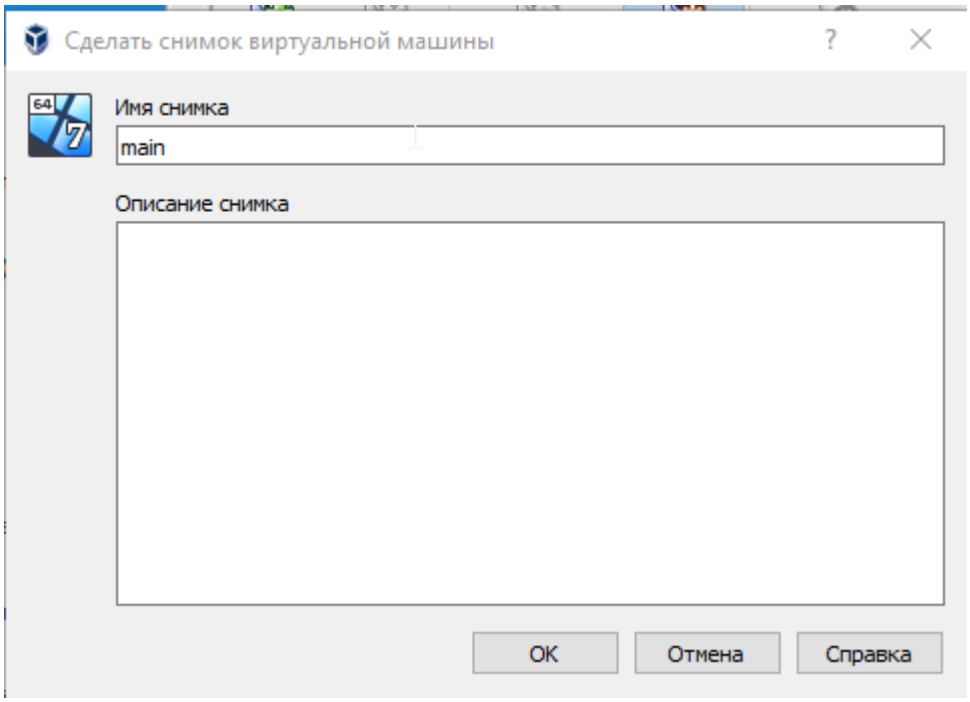
Срезы можно создать руками или автоматом.
**руками:** выберете шаблон ВМ с АВ и создайте срез
25.png




26.png




27.png




**автоматом:** для этого я создал bat файт _create_snapshot.bat(перед созданием ВСЕ АВ должны быть выключены) и для удаления всех срезов _del_snapshot.bat(перед удалением ВСЕ АВ должны быть выключены)
Т.е. еще раз повторюсь, срезы надо пересоздавать когда вы обновите антивирусы на шаблонах ВМ с АВ, должен быть только один срез с названием "main", перед пересозданием все ВМ должны быть выключены.

**7. Первый запуск**
Все шаблоны с АВ созданы, настроены, обновлены антивирусы, инет на них отключен, они выключены в Сохраненном состоянии, срезы сделаны.

Переходим к самой важной части - тестированию
Я подготовил bat файлик _start.bat как пример тестирования, тестировать мы будем hello.exe (мессажебокс)

Code:

```
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" clonevm AV_avg --snapshot main --name
AV_avg_tmp  --register --options link
TIMEOUT 5
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm AV_avg_tmp
TIMEOUT 40
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV_avg_tmp copyto
"C:\dynamic_check\hello.exe" --target-directory "C:\Users\Admin\AppData\Local\Temp" --
username "Admin" --password "12345" --verbose
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV_avg_tmp start --exe
"C:\Users\Admin\AppData\Local\Temp\hello.exe" --username "Admin" --password "12345" --verbose
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng
"src_avg_1.png"
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng
"src_avg_2.png"
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng
"src_avg_3.png"
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng
"src_avg_4.png"
TIMEOUT 1
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp poweroff
TIMEOUT 5
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" unregistervm AV_avg_tmp --delete
```

Теперь поясню каждую строку
**clonevm AV_avg --snapshot main --name AV_avg_tmp --register --options link**
делаем связанное клонирование шаблон ВМ с АВ с именем AV_avg используя срез "main" название новой одноразовой ВМ AV_avg_tmp

**startvm AV_avg_tmp**
старт одноразовой ВМ AV_avg_tmp

**guestcontrol AV_avg_tmp copyto "C:\dynamic_check\hello.exe" --target-directory "C:\Users\Admin\AppData\Local\Temp" --username "Admin" --password "12345" --verbose**
копируем наш тестовый файл "C:\dynamic_check\hello.exe" указанием полного пути в гостевую одноразовую ВМ AV_avg_tmp в папку "C:\Users\Admin\AppData\Local\Temp" использую учетную запись Admin

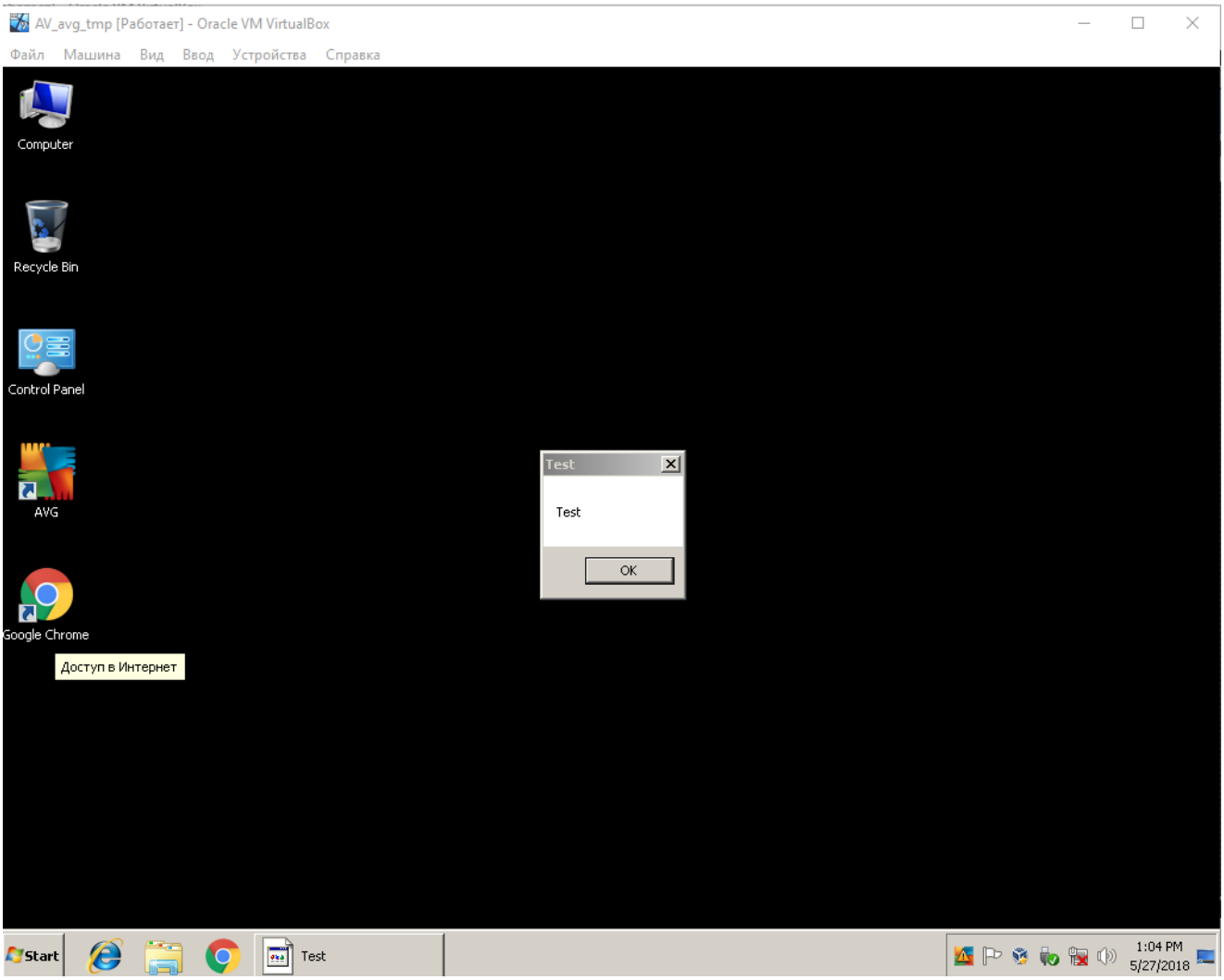
**guestcontrol AV_avg_tmp start --exe "C:\Users\Admin\AppData\Local\Temp\hello.exe" --username "Admin" --password "12345" --verbose**
запускаем наш "hello.exe" на одноразовой гостевой ВМ AV_avg_tmp использую учетную запись Admin

**controlvm AV_avg_tmp screenshotpng "src1.png"**
создания скриншотов гостевой одноразовой ВМ AV_avg_tmp

**controlvm AV_avg_tmp poweroff**
отключаем принудательно питание гостевой одноразовой ВМ AV_avg_tmp

**unregistervm AV_avg_tmp --delete**
удаляем гостевую одноразовую ВМ AV_avg_tmp из списка с удалением файла ВМ

Если все сделали правильно у вас в консоли будет такой лог и появятся скриншоты, а на экране одноразовой ВМ AV_avg_tmp будет такое окно
30.png




Далее вы можете анализировать скриншоты. Таймауты стоят относительные, вы сами можете с ними играться.

Консольный лог
Code:

```
C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" clonevm AV_avg --
snapshot main --name AV_avg_tmp  --register --options link
Machine has been successfully cloned as "AV_avg_tmp"

C:\dynamic_check>TIMEOUT 5

Время ожидания 5 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe"  startvm AV_avg_tmp
Waiting for VM "AV_avg_tmp" to power on...
VM "AV_avg_tmp" has been successfully started.

C:\dynamic_check>TIMEOUT 40

Время ожидания 40 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV_avg_tmp
copyto "C:\dynamic_check\hello.exe" --target-directory "C:\Users\Admin\AppData\Local\Temp" --
username "Admin" --password "12345" --verbose
Creating guest session as user 'Admin'...
Waiting for guest session to start...
Successfully started guest session (ID 1)
Copying from host to guest ...
Directory "C:\Users\Admin\AppData\Local" already exists
Source: C:\dynamic_check\hello.exe
Copying "C:\dynamic_check\hello.exe" to "C:\Users\Admin\AppData\Local\Temp" ...
Closing guest session ...

C:\dynamic_check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe"  guestcontrol AV_avg_tmp
start --exe "C:\Users\Admin\AppData\Local\Temp\hello.exe" --username "Admin" --password
"12345" --verbose
Creating guest session as user 'Admin'...
Waiting for guest session to start...
Successfully started guest session (ID 1)
Starting guest process ...
[4076 - Session 1]
Process successfully started!
Guest session detached

C:\dynamic_check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp
screenshotpng "src1.png"

C:\dynamic_check>TIMEOUT 3
```

```
Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp
screenshotpng "src2.png"

C:\dynamic_check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp
screenshotpng "src3.png"

C:\dynamic_check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp
screenshotpng "src4.png"

C:\dynamic_check>TIMEOUT 1

Время ожидания 1 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp
poweroff

C:\dynamic_check>TIMEOUT 5

Время ожидания 5 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" unregistervm AV_avg_tmp
--delete
```

Так же вкалдываю сонсольны хелп
Code:

```
Usage:

VBoxManage guestcontrol     <uuid|vmname> [--verbose|-v] [--quiet|-q]
                            [--username <name>] [--domain <domain>]
                            [--passwordfile <file> | --password <password>]

                            run [common-options]
                            [--exe <path to executable>] [--timeout <msec>]
                            [-E|--putenv <NAME>[=<VALUE>]] [--unquoted-args]
                            [--ignore-operhaned-processes] [--profile]
                            [--no-wait-stdout|--wait-stdout]
                            [--no-wait-stderr|--wait-stderr]
                            [--dos2unix] [--unix2dos]
                            -- <program/arg0> [argument1] ... [argumentN]]

                            start [common-options]
                            [--exe <path to executable>] [--timeout <msec>]
                            [-E|--putenv <NAME>[=<VALUE>]] [--unquoted-args]
                            [--ignore-operhaned-processes] [--profile]
                            -- <program/arg0> [argument1] ... [argumentN]]

                            copyfrom [common-options]
                            [--dryrun] [--follow] [-R|--recursive]
                            <guest-src0> [guest-src1 [...]] <host-dst>

                            copyfrom [common-options]
                            [--dryrun] [--follow] [-R|--recursive]
                            [--target-directory <host-dst-dir>]
                            <guest-src0> [guest-src1 [...]]

                            copyto [common-options]
                            [--dryrun] [--follow] [-R|--recursive]
                            <host-src0> [host-src1 [...]] <guest-dst>

                            copyto [common-options]
                            [--dryrun] [--follow] [-R|--recursive]
                            [--target-directory <guest-dst>]
                            <host-src0> [host-src1 [...]]

                            mkdir|createdir[ectory] [common-options]
                            [--parents] [--mode <mode>]
                            <guest directory> [...]

                            rmdir|removedir[ectory] [common-options]
                            [-R|--recursive]
                            <guest directory> [...]

                            removefile|rm [common-options] [-f|--force]
                            <guest file> [...]

                            mv|move|ren[ame] [common-options]
```

```
                            <source> [source1 [...]] <dest>

                            mktemp|createtemp[orary] [common-options]
                            [--secure] [--mode <mode>] [--tmpdir <directory>]
                            <template>

                            stat [common-options]
                            <file> [...]

VBoxManage guestcontrol     <uuid|vmname> [--verbose|-v] [--quiet|-q]

                            list <all|sessions|processes|files> [common-opts]

                            closeprocess [common-options]
                            <   --session-id <ID>
                              | --session-name <name or pattern>
                            <PID1> [PID1 [...]]

                            closesession [common-options]
                            <  --all | --session-id <ID>
                              | --session-name <name or pattern> >

                            updatega|updateguestadditions|updateadditions
                            [--source <guest additions .ISO>]
                            [--wait-start] [common-options]
                            [-- [<argument1>] ... [<argumentN>]]

                            watch [common-options]
```

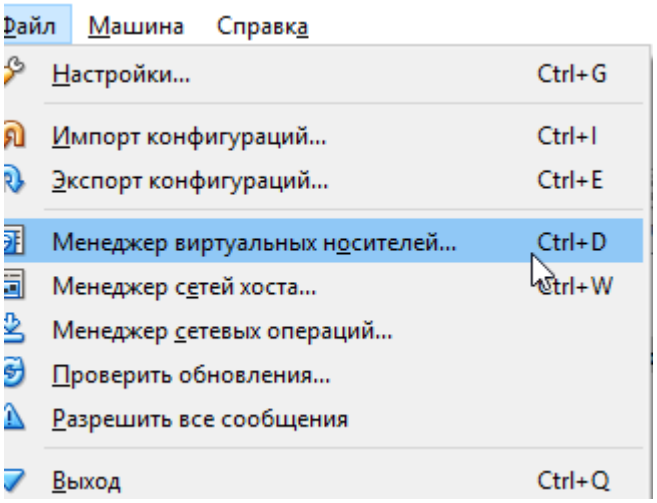
**8. Ошибки и литература**

Если по какой то причине вы не смогли удалить срез - значит он еще привязан к ВМ, удалите ВМ который был клонирован связанно, в нашем случае все ВМ с названием *_tmp - их не должно быть.

**ВАЖНО!!! Бывает по какойто причине ВМ *_tmp завершиласть некоректно, тогда надо удалить все ВМ *_tmp и удалить их файлы в папке где они храняться с названием *_tmp.**
**Иногда когда все удалено и ВМ выключены, пересоздать срез или ВМ *_tmp не возможно надо руками удалить носитель. Будте окуратнее**

28.png

29.png





Если вы что то сделали не так смотрите ошибки и перечитывайте статью. Полное описание всех команд вы найдете на официальном сайте https://www.virtualbox.org/manual/ и https://www.virtualbox.org/manual/ch08.html.

### 9. Пояснения

Азм постарался сделать как можно проще статью и примеры, чтобы было понятна сама методика Runtime проверки антивирусами, создания шаблонов и использования быстрого запуска.
Я не делал контроля запуска ВМ и ОС, так же не делал работу с сетью и запуск с использованием окружения - мне было лениво.

### 10. Подарок

Мне друзья для этой стать скинули исходники полноценного сервиса последовательной проверки на php, сервис использую примерно такую же методику, что я описал в статье. Если вы серьезный программист и вам понравилась статья, то можете поиграться с этим сервсим и реализовать свой.
Я правда считаю что пример в стать делать в виде массового сервиса не целесообразно, будет слишком огромное потребление ресурсов, для создания полноценного сервиса надо измениить подход и возможно использовать другие виртуальные машины к пример qemu, но суть методики останется та же.

**11. Файлы**
Ссылка:
https://mega.nz/#!IVgn0SDT!TLpiWj11SLanT57u6YOVI4bzupg63THIkrgZCM2IyIw
Пароль: exploit.in

**12. Дополнения**
Хотелось бы немного сказать про антидетект виртуальной машины, а то мне тут целую истерику устроили, что такой проект и методику может любой сделать, и что я слишком много внимания уделил простым вещам, надо было про антидект лучше написать - смешно. По антидетекту все в инте есть, а вот подобных статей НЕТУ!
По антидетекту
- есть замечательный опенсорс проект который чекает вм и показывает детекты https://github.com/a0rtega/pafish , там же есть бинарнник.
- есть замечательный проект с патчером vbox для антиэмуляции, он и мышку эмулирует и имена устройств меняет, реестр правит, куча всего для того чтобы софт не мог детектить вашу виртуалку https://github.com/hfirefox/VBoxHardenedLoader
- есть отличное сообщество http://www.kernelmode.info/forum/viewtopic.php?f=11&t=3478 где ребята обсуждают и дорабатывают патчер

В принципе больше по этой теме обсуждать нечего, все есть в наличии и в исходниках, но для их использования надо иметь скилл или делать еще одну статью.

Я много чего еще в этой статье не указал, потому что невозможно все охватить за раз, поэтому в задницу ваши претензии без внипетов и примеров.

**PS: народ пожалейте мою психику, не задавайте в ЛС мне вопросы**