Как подключиться к дедику через тор

Whonix — это дистрибутив, который базируется на Debian и при этом состоит из двух частей. Когда я говорю «из двух частей», я имею в виду, что для работы Whonix необходимы две виртуальные машины. Первая — это шлюз (Whonix Gateway), который работает только через Tor и Торифицирует абсолютно весь траффик, а вторая — полностью изолированная рабочая станция (Whonix Workstation), настроенная таким образом, что подключается только к шлюзу и берет интернет только оттуда.

Таким образом, абсолютно все приложения, запущенные на рабочей станции пускают свой траффик через Tor, потому что Workstation берет интернет с Gateway. При этом Workstation не знает свой реальный IP адрес, и если рабочую станцию взломают, злоумышленник так и не сможет узнать ваш реальный IP адрес.

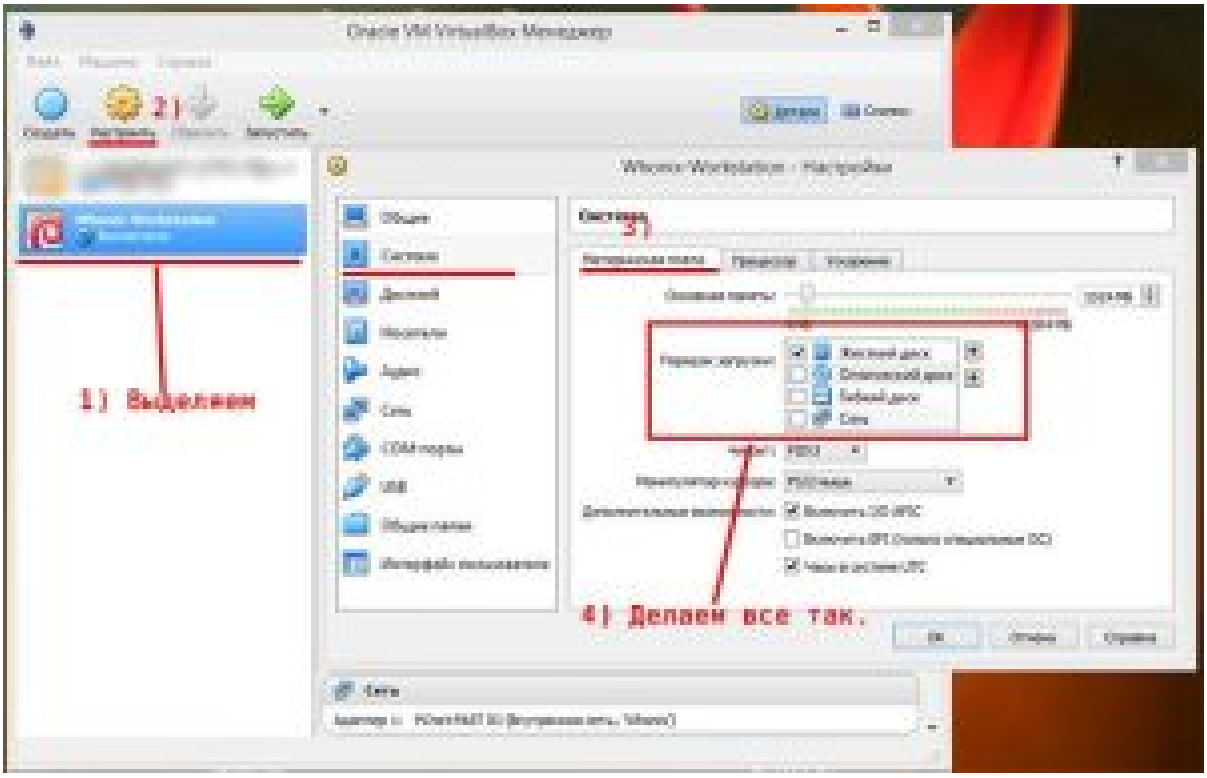
Из особенностей Whonix можно выделить также то, что каждое предустановленные в нем приложение работает на отдельном Socks-порту, что означает, что для каждого такого приложения создается отдельная цепочка из узлов Tor. Whonix отлично защищен от утечек DNS. У Whonix хорошая защита от идентификации пользователя при помощи так называемого Fingerprinting.

Как установить Whonix

Для начала нужно скачать VirtualBox. Теперь идем на сайт Whonix и скачиваем два образа «.ova» — Whonix Gateway и Whonix Workstation. С этой страницы скачиваем образы: Образы для VirtualBox. По ссылкам «Download Whonix-Gateway» и «Download Whonix-Workstation».

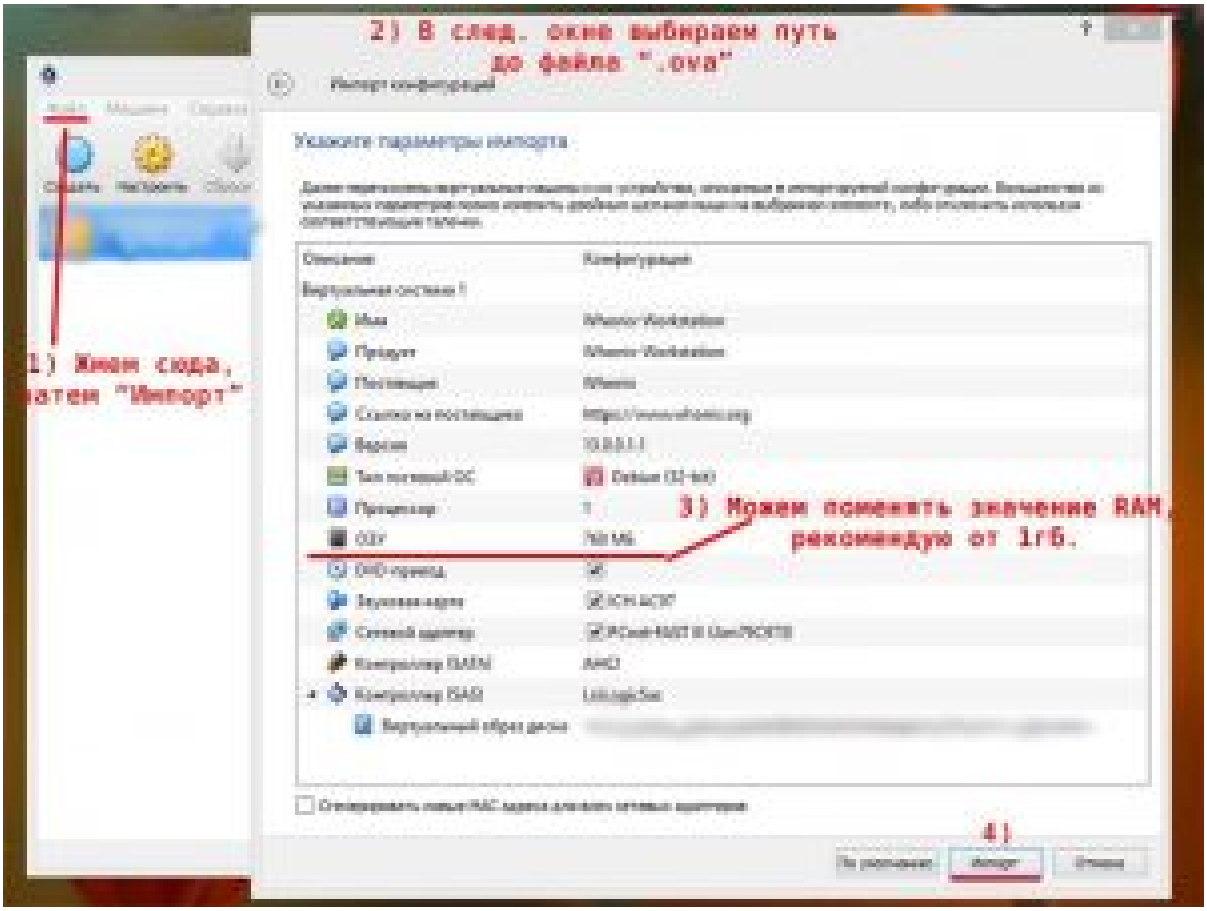
Открываем виртуалбокс, жмем File -> Import Appliance. Выбираем скаченный образ Whonix Gateway, жмем «Далее». Появится окошко

с настройками, все оставляем по-умолчанию, кроме графы RAM, эту графу по желанию можно изменить. Жмем «Import» и ждем.



Точно такую же операцию проделываем для Whonix Workstation. Лично я для Whonix Workstation выделяю обычно не меньше 1024mb RAM (если есть возможность, выделяйте побольше гига), а для первого запуска Whonix Gateway оставляю по-умолчанию (768mb).

Теперь у нас в нашем виртуалбоксе появились две виртуальные машины, но мы их пока не запускаем. Немного настроим. Жмем на виртуалку, потом «Настройки», переходим на вкладку «System». Тут мы должны поменять порядок загрузки и снять лишние галочки. Выбираем «Hard Disk» и стрелочками перемещаем его на первую строку, «Optical» – на вторую строку. Снимаем галочки с «Floppy» и «Optical», оставляем только на «Hard Disk». Теперь переходим во вкладку «Storage», там на Контроллере ставим галочку «Use Host I/O Cache». Точно такую же операцию проделываем и со второй виртуалкой.



Как запустить Whonix

Запускаем GW (Gateway) и WS (Workstation). Порядок запуска таков: сначала Gateway, затем Workstation.

Перед нами сразу появится окно, дважды жмем «Understood» (но сначала читаем!). На GW должно быть отмечено «Iam Ready to Enable Tor», ждем «Next» несколько раз, потом «Yes. Automatically install updates from the Whonix team», жмем «Next», выбираем «Whonix Stable Repository» (рекомендую выбирать именно это) и далее до конца. На WS все аналогично. Теперь на обеих виртуалках автоматически должен запуститься так называемый whonixcheck.

Когда whonixcheck прошел, он покажет «Warning», где будет ругаться на то, что система не обновлена.

На обеих виртуалках открываем эмулятор терминала Konsole с ярлыка на рабочей столе.

На обеих VM вводим

```
sudo apt-get update && sudo apt-get upgrade -y && sudo apt-get dist-upgrade -y
```

Спросит пароль.

Стандартный логин – user

Пароль от user – changeme

Пароль от root – changeme

Позже мы поменяем пароль. Вводим пароль -> сидим с открытым ртом и ждем пока закончится обновление, процесс не быстрый. Обновление может прерваться по неизвестным причинам, если это случилось, повторно вводите команду выше, процесс продолжится.

Если все прошло окей, то повторно запускаем whonixcheck – вводим в терминале whonixcheck или запускаем с ярлыка на рабочем столе WhonixCheck. Лично я предпочитаю делать whonixcheck в терминале. Смотрим, чтоб не было «Warning». Если есть «Warning» в том же месте что и в прошлый запуск, то возвращаемся на абзац выше и обновляем систему. Если нет

«Warning», то идем дальше.

Теперь на Workstation нам нужно скачать/обновить Tor Браузер. Запукаем Tor Browser Downloader с ярлыка на раб. столе или вводим update-torbrowser в терминале. Начнется процесс, вам будет предложено выбрать версию Tor Браузера для скачивания, 6.0.7 и остальные. Версия 6.0.7 – стабильная версия, все остальные версии – тестинг или девелоперс. Я ставлю 6.0.7, вы ставите что хотите (лучше стабильную). В случае если программа была запущена с ярлыка на раб. столе, отметьте нужную версию кружочком (радиобаттон), в случае запуска скрипта через терминал, введете нужную версию вручную, как только предложат это сделать (в моем случае я ввел «6.0.7») и жмете интер. После скачивания, вам будет предложено установить его, жмете кнопку ‘Yes’ или вводите «y» в терминале и жмете интер. Версия «6.0.7» актуальна на момент написания статьи.

Меняем стандартный пароль. Открываем терминал, вводим

sudo -i

Водим пароль, теперь мы работаем из под root. Меняем пароль, сначала для root

passwd root

Дважды вводим пароль. Теперь пароль от root поменялся. Теперь для user

passwd user

Дважды вводим пароль. Теперь пароль от user поменялся. Теперь вводим exit.

Желательно чтобы пароль от root и от user были разные. Данную операцию можно проделать на обеих виртуалках.

Обновляем локали. Вводим

sudo dpkg-reconfigure locales

Появится графическое окошко. Навигация вверх-вниз –

стрелочками на клаве. Листаем вниз и ищем <ru_RU.UTF-8 UTF-8>. Отмечаем по нажатию на пробел. Через нажатие на Tab переключаемся на <Ok>. Теперь нам предложат выбрать язык в системе по умолчанию, здесь на ваше усмотрение. Я оставлю английский (чего и вам рекомендую), поэтому выбираю <en_US.UTF-8>, а вы можете выбрать <ru_RU.UTF-8>.

Ставим некоторый софт/пакеты, которые могут вам понадобиться

```
sudo apt-get install htop git openvpn openssl nmap psi-plus etherape openssh-client
```

htop – консольный task manager

git – git

nmap – сканер портов

psi-plus – Jabber клиент. Вместо него может быть pidgin

etherape – для графического мониторинга сетевого траффика

openssh-client – чтоб подрубаться по ssh куда-нибудь

Еще ставим данную группу пакетов

```
sudo apt-get install build-essential pkg-config make automake autoconf
```

Работа с Whonix Gateway

Лично я запуская GW в консольном режиме, потому что во-первых GUI жрет не мало RAM, во-вторых GUI по большому счету не нужен GW – все операции можно провести через консоль, все ярлыки на раб. столе спокойно заменяются командами в консоли.

Итак, для того чтобы запускать GW в консольном режиме, нужно выделить виртуалке поменьше RAM. По-умолчанию, минимально значение RAM, которое должно быть выделено для GW, чтобы он запускался в GUI режиме – 480mb. Значит, если выделено меньше 480mb, то GW запустится в консольном режиме.

Идем в виртуалбокс, выбираем GW -> жмем настройки -> переходим на вкладку «System» -> перемещаем ползунок. Выбираем значение меньше 480.

Но что делать, если мы хотим выделить GW побольше RAM, скажем, 512 или оставить 768, но при этом запускать в консольном режиме? Редактируем файл /etc/rads.d/30_default.conf

sudo nano /etc/rads.d/30_default.conf

Ищем строчку «rads_minimum_ram». Эта строчка сообщает системе, какое минимальное количество RAM должно быть выделено, чтобы машина запускалась в GUI режиме. Как видите, по умолчанию стоит 480. Берем и меняем значение на любое другое, скажем, 1024 -> сохраняем -> выходим. Идем в настройки вирт. машины Gateway (выше) и выделяем сколько нужно RAM и в пределах 1024mb – будет запускаться в консольном режиме.

Ярлыки на Whonix Gateway

Грубо говоря, ярлыки условно можно разделить на пять групп:

1) Ярлыки, для управления Tor (Stop Tor, Reload Tor, Restart Tor)

2) Ярлыки, для управления Firewall (Global Firewall Settings, User Firewall Settings, Reload Firewall)

3) Ярлыки, для редактирования конфигурационных файлов Tor (Tor User Config, Tor Examples, Tor Data)

4) Ярлыки Whonix (WhonixCheck, WhonixSetup, Whonix Repository)

5) Остальные ярлыки – приложения (Konsole, Arm)

Stop Tor – остановить службу Tor. После выполнения пропадет интернет и приложения на Whonix Workstation работать не будут. Заменяется следующей командой в консоли

sudo service tor@default stop

Reload Tor – перезагружает службу Tor. При выполнении перечитывает конфигурационные файлы и перезагружает цепочку Tor для приложений на Whonix Workstation. Заменяется следующей командой в консоли

```
sudo service tor@default reload
```

Restart Tor – перезапускает службу Tor. Трудно сейчас будет объяснить чем отличается от Reload Tor. Сначала служба Tor останавливается, затем запускается по новой. Если вам нужно перезагрузить цепочку, то используйте Tor Reload. Заменяется следующей командой в консоли

```
sudo service tor@default restart
```

Global Firewall Settings – открывает глобальные настройки Firewall по адресу /etc/whonix_firewall.d/30_default.conf в текстовом редакторе kwrite. Если вы не знаете, зачем это нужно, то данный ярлык не используйте. Заменяется следующей командой в консоли

```
sudo nano /etc/whonix_firewall.d/30_default.conf
```

User Firewall Settings – открывает пользовательские настройки Firewall по адресу /etc/whonix_firewall.d/50_user.conf в текстовом редакторе kwrite. Если вы не знаете, зачем это нужно, то данный ярлык не используйте. Заменяется следующей командой в консоли

```
sudo nano /etc/whonix_firewall.d/50_user.conf
```

Reload Firewall – перезагружает Firewall, если вдруг вы внесли изменения в /etc/whonix_firewall.d/30_default.conf или /etc/whonix_firewall.d/50_user.conf. Заменяется следующей командой в консоли

```
sudo whonix_firewall
```

Tor User Config – открывает основной конфигурационный файл /etc/tor/torrc в текстовом редакторе kwrite. Если вы не знаете ничего про конфигурационный файл torrc, зачем он нужен, что

туда добавлять и как с ним работать, то неичего там не меняйте. /etc/whonix_firewall.d/30_default.conf или /etc/whonix_firewall.d/50_user.conf. Заменяется следующей командой в консоли

sudo nano /etc/tor/torrc

Tor Examples – открывает файл /etc/tor/torrc.examples, который является примерно конфигурационного файла /etc/tor/torrc в текстовом редакторе в режиме «только для чтения». Это пример, в этом файле не нужно ничего редактировать. Если интересно – можете почитать. Заменяется следующей командой в консоли

nano /etc/tor/torrc.examples

Tor Data – открывает папку /var/lib/tor/ в файловом менеджере Dolphin. Заменяется следующей командой в консоли

cd /var/lib/tor/

WhonixCheck – запускает проверку. Нельзя запускать от рута.Заменяется следующей командой в консоли

whonixcheck

WhonixSetup – запускает Хуниксовский Setup Wizard. Заменяется следующей командой в консоли

sudo whonixsetup

Arm – мощный инструмент для мониторинга Tor. С помощью него можно контролировать Tor различным образом. Заменяется следующей командой в консоли

arm

Как подключиться к дедику через tor

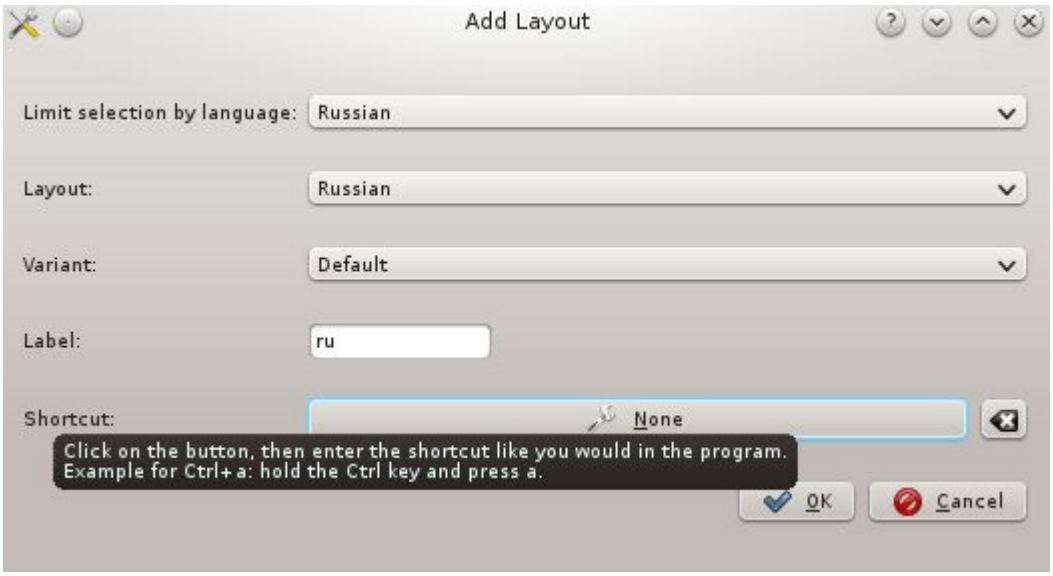
Для коннекта к дедикам, будем использовать Remmina

На рабочем столе дважды жмем Konsole (терминал)

Вводим в терминале

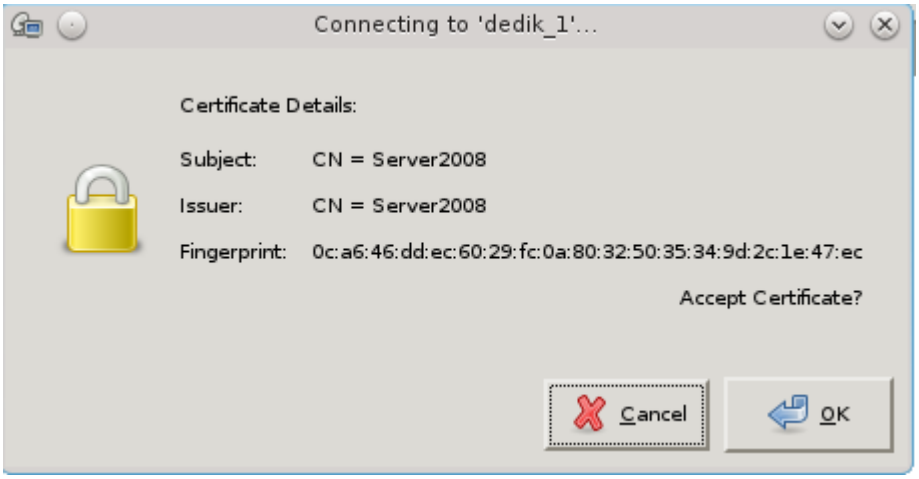
```
sudo apt-get install remmina
```

Добавим русскую раскладку. Remmina System Settings > Input Devices. Далее «Add» – выбираем русскую раскладку.



По умолчанию для смены расскладки используеться комбинация «ctr+alt+k», но можно ее изменить задав значение в пункте Shortcut.

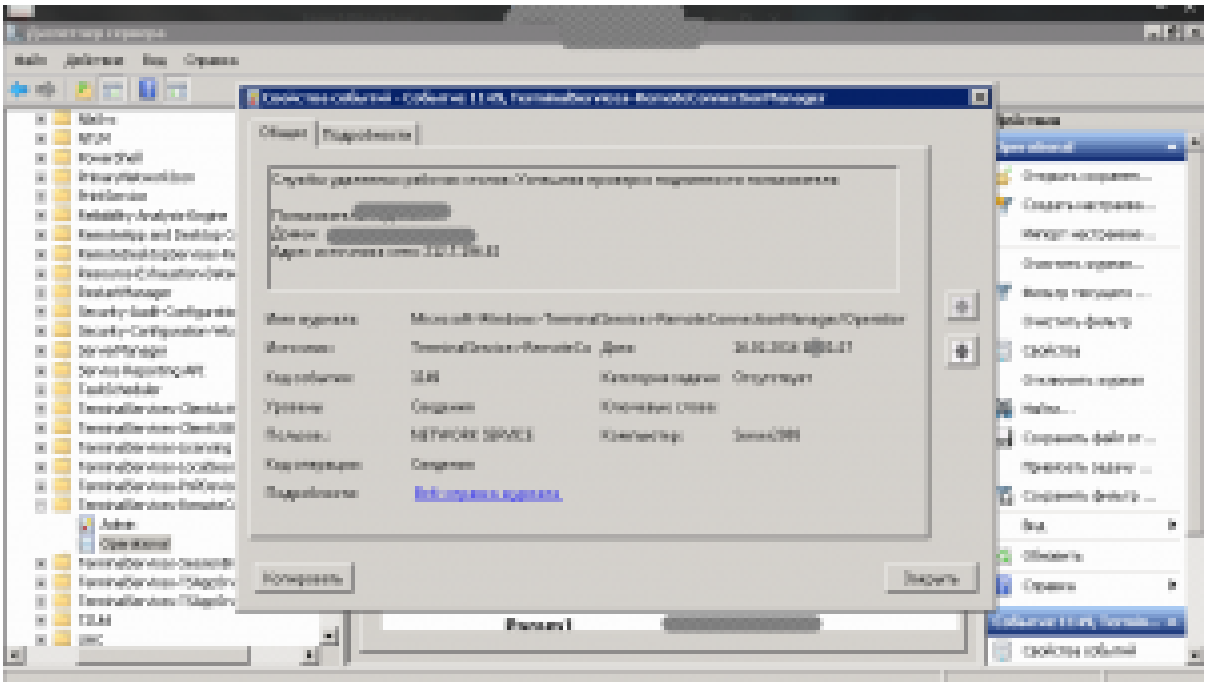
Запускаем Remmina и жмем «New». Заполняем поля. Далее «Save» или «Connect». Принимаем, сертификат.



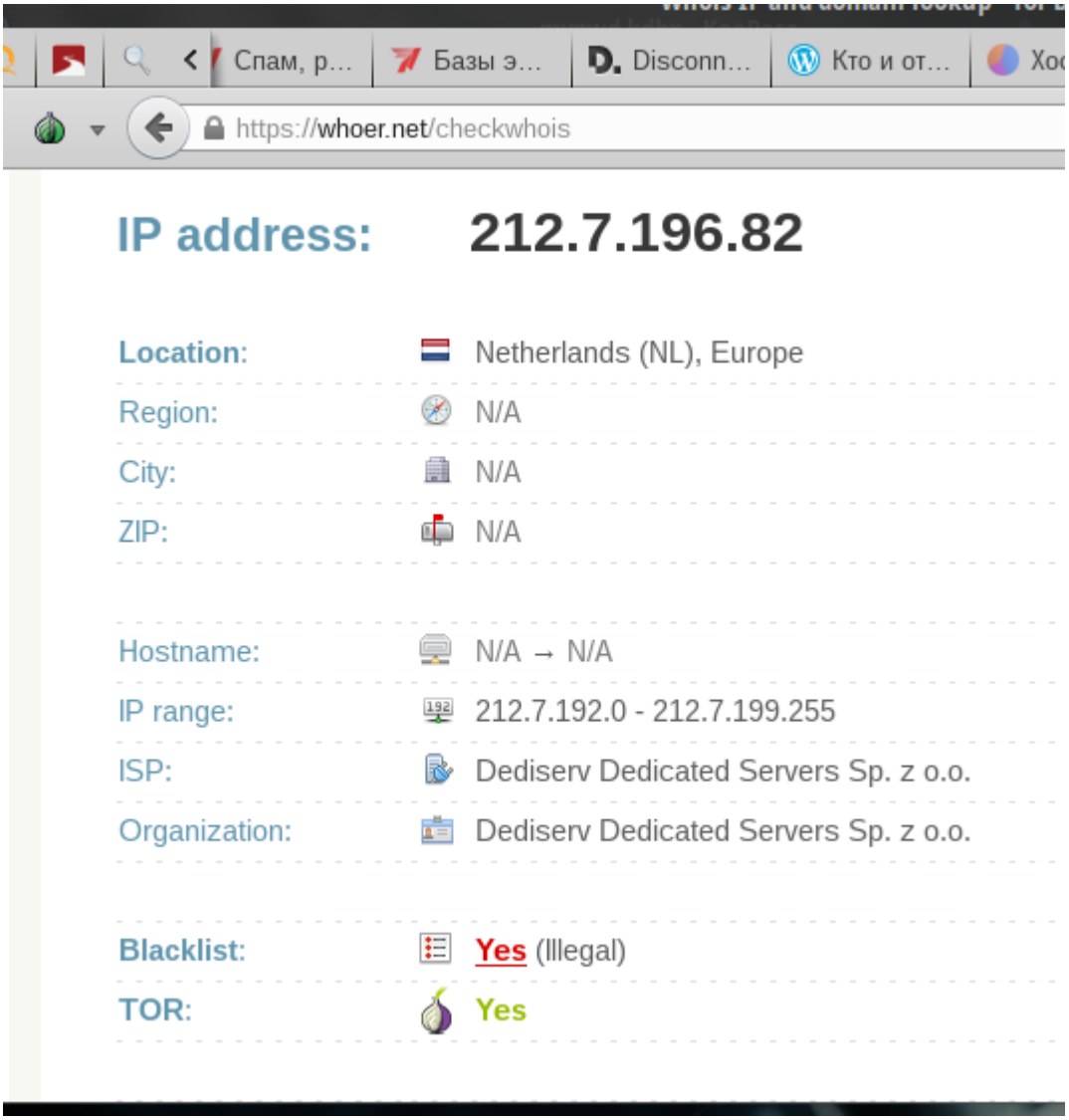
Проверим с какого IP мы сейчас подключились.

Идем на дедике в: Server Manager > Diagnostics > Event Viewer > Applications ans Services Logs > Microsoft > Windows > TerminalServices-LocalSessionManager > Operational

Открываем журнал на дедике > Server Manager > Diagnostics > Event Viewer > Applications ans Services Logs > Microsoft > Windows > TerminalServices-LocalSessionManager > Operational



И видим IP сети Tor.



Аналог Remmina – rdesktop. Устанавливаем

```
sudo apt-get install rdesktop
```

Использование rdesktop

```
rdesktop 255.255.255.255 -u логин -p пароль
```

Где 255.255.255.255 – ip дедика.