

# Snoop Project

Область применения:  
OSINT & CTF

Общее руководство



# Оглавление

|  |           |
|--|-----------|
| Описание инструмента Snoop.....                                | 3         |
| Рекомендуемые системные требования.....                        | 3         |
| Запуск Snoop на OS Windows.....                                | 3         |
| Запуск и использование Snoop на OS GNU/Linux.....              | 8         |
| Сборка Snoop из исходного кода.....                            | 8         |
| Самостоятельная сборка утилиты Snoop для OS GNU/Linux.....     | 8         |
| Самостоятельная сборка утилиты Snoop для OS Windows.....       | 9         |
| Самостоятельная сборка утилиты Snoop для OS Android.....       | 9         |
| Основные процессы поддержания жизненного цикла ПО.....         | 10        |
| Технические детали.....  | 10        |
| Принцип работы и разработки Snoop Project.....                 | 10        |
| Проверка подписи.....  | 12        |
| <b>База данных Snoop Project.....</b>                          | <b>12</b> |
| Справка по ключам Snoop.....                                   | 13        |
| Обновление утилиты Snoop.....                                  | 14        |
| Основные ошибки при поиске: ложноположительные результаты..... | 15        |
| Плагины Snoop Project.....                                     | 17        |
| Плагин GEO_IP/domain.....                                      | 18        |
| Плагин Reverse Vgeocoder.....                                  | 21        |
| Плагин Yandex_parser.....                                      | 23        |
| Получение Snoop Project Full version.....                      | 25        |

## Описание инструмента Snoor

Основная функция Snoop Project — отслеживать «username» в публичных данных, расширенная функциональность — различные OSINT плагины. Snoop Project внесён в реестр отечественного ПО РФ с заявленным кодом 26.30.11.16: *Программное Обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий:: №7012 приказ 07.10.2020 №515.*

Snoor Project разработан на материалах исследовательской работы в области скрапинга публичных данных. На данный момент Snoor отслеживает nickname по > **2200+** интернет ресурсам. Это самое перспективное [OSINT](#) ПО для поиска «username» с учётом СНГ локации (для сравнения: подобные инструменты БД::Sherlock ~**350** сайтов, Whatsmyname ~**300** сайтов, Namechk ~**100** сайтов).

Snoor Project имеет плагины, которые позволяют работать с различными данными: IPv4/v6/domain/url/GEO-координатами/Яндекс\_сервисами. Плагины в будущем будут пополняться и обновляться.

Пользователь инструмента Snoop Project вправе самостоятельно изучить местное законодательство своей страны/округа на предмет разрешения пользования подобными сканерами.

Snoor успешно протестирован на OS:

- Windows 7 (32/64bit); Windows 10 (32/64bit);
- GNU/Linux (deb);
- Android 7/10 (Termux).

## Рекомендуемые системные требования

**OS:** Windows7-10 (32-64bit); GNU/Linux (amd64); Android 7/10 (Termux).

**RAM** (Snoop for Linux/Android): 2 Гб; **RAM** (Snoop for Windows): 4 Гб.

**CPU:** Intel; AMD; ARM.

## Выход в Сеть Internet.

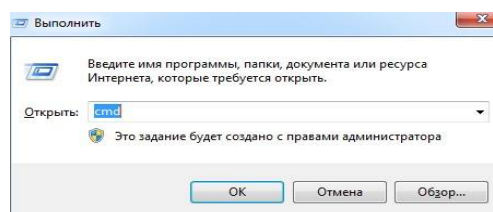
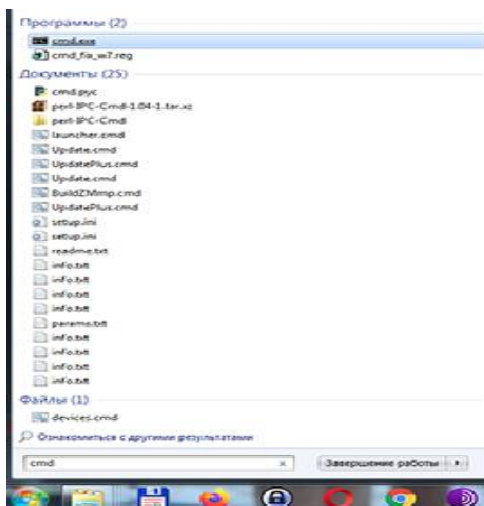
Для запуска Snoor build-версии на OS GNU/Linux требуется версия пакета: GLIBC (**libc-bin**) не ниже 2.29-10.

snoor.exe/snoor — автономное ПО и не требует инсталляции на жёсткий диск, кроме случая самостоятельной сборки утилиты из открытого исходного кода.

Пользователю доступны готовые сборки утилиты Snoop из открытого [исходного кода](#) (то есть пользователю не требуется устанавливать зависимости/библиотеки и Python).

## Запуск Snooper на OS Windows

- 1) **Распаковать** rar-архив (с выбранной версией *Snoor*, например *RU*) в любое место на диске.
- 2) Проверить подпись и контрольные суммы ПО *Snoor*.
- 3) Нажать «меню пуск», набрать на клавиатуре «cmd», запустить cmd.exe (*альтернатива cmd — powershell*).

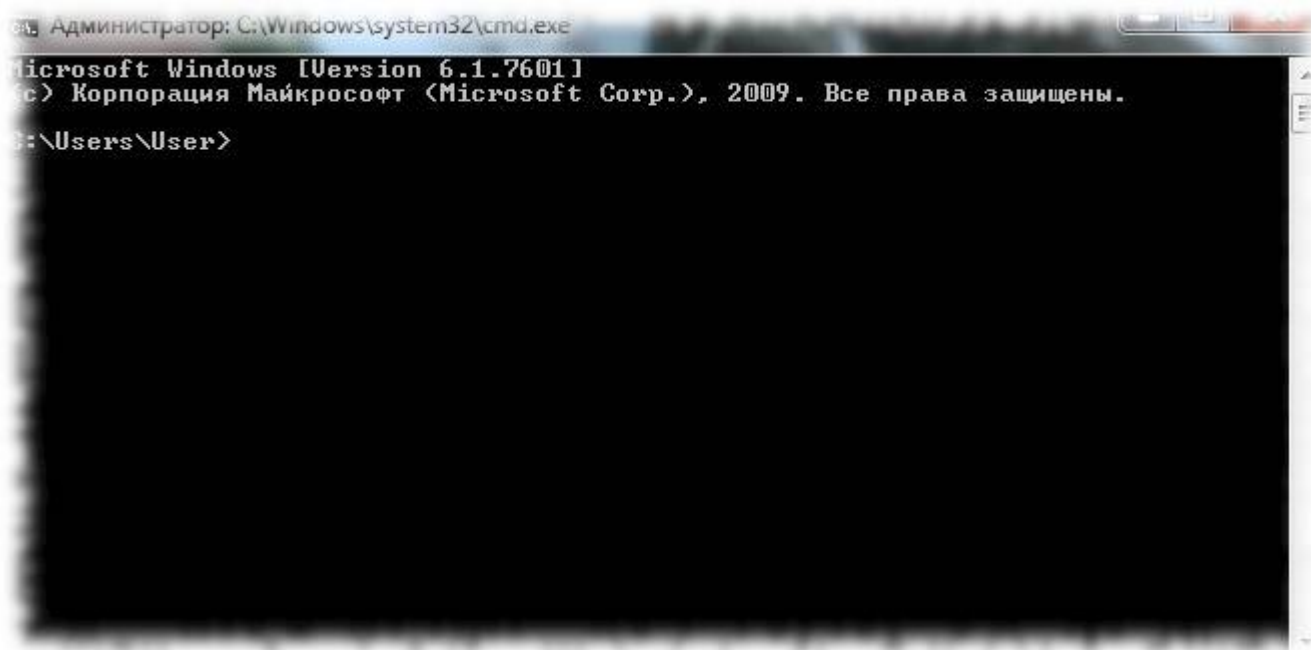


Альтернативный вариант:

1. Нажать комбинацию клавиш win+r
2. Набрать на клавиатуре «cmd», «enter».

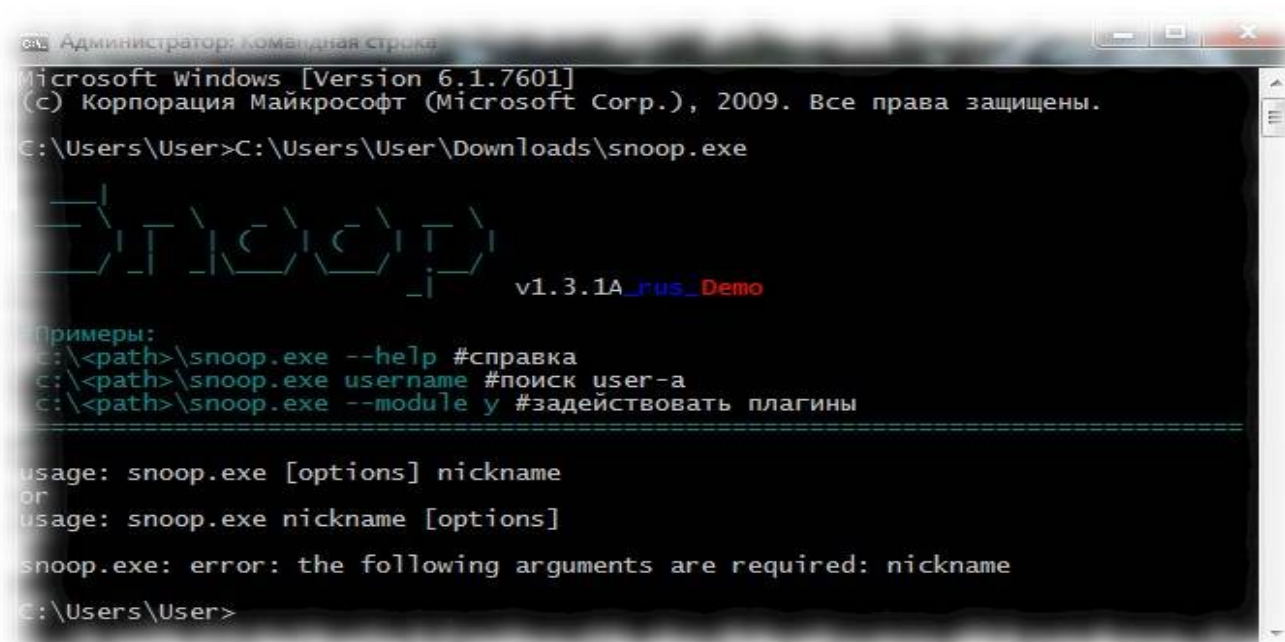


Откроется командная строка OS Windows.



4) Нажать ЛКМ на файле snoop.exe и не отпуская ЛКМ потянуть файл на окно командной строки (*операция перемещения файла*). После перемещения snoop.exe в окно командной строки в cmd будет указан полный путь к файлу snoop.exe. Нажать «enter».

Snoop запущен.



5) Чтобы попробовать выследить первого username, нажмите на клавиатуре клавишу стрелка вверх «↑», в командной строке автоматически пропишется полный путь к snoop.exe (*примечание — не нужно перетаскивать каждый раз файл в окно терминала, используйте стрелку «↑»*).

Допишите «-f admin -t 9» и нажмите «enter».



Snoop поддерживает поиск логинов в формате «username с пробелом», пример поиска такого логина:

```
snoop.exe «ivan ivanov»  
snoop.exe ivan_ivanov  
snoop.exe ivan-ivanov
```

Snoop поддерживает поиск логинов из E-mail\_адреса, пример:

```
snoop.exe bobbimonov@yandex.ru
```

'ctrl-c' — прервать поиск.

Snoop поддерживает возможность одновременного поиска нескольких людей, пример:

```
snoop.exe username1 username2 username3
```

или указать файл со списком людей с ключом «--userload»:

```
snoop.exe --userload C:\file.txt start
```

В файле (кодировка *utf-8*) «file.txt» могут быть записаны десятки nickname's, и Snoop будет пытаться искать аккаунты всех перечисленных людей из файла «file.txt».

**Snoop не разыскивает номера телефонов и их владельцев.**

Для удобства пользователя присутствует поддержка сокращения ключей, пример:

```
snoop.exe -c -t 9 -n -v -w -C username
```

эквивалентно команде:

```
snoop.exe --country --time 9 --no-func --verbose --web-base --cert-on username
```

Подробная справка по ключам Snoop доступна по команде (см. стр. 13 данного руководства) в зависимости от версии ПО Snoop:

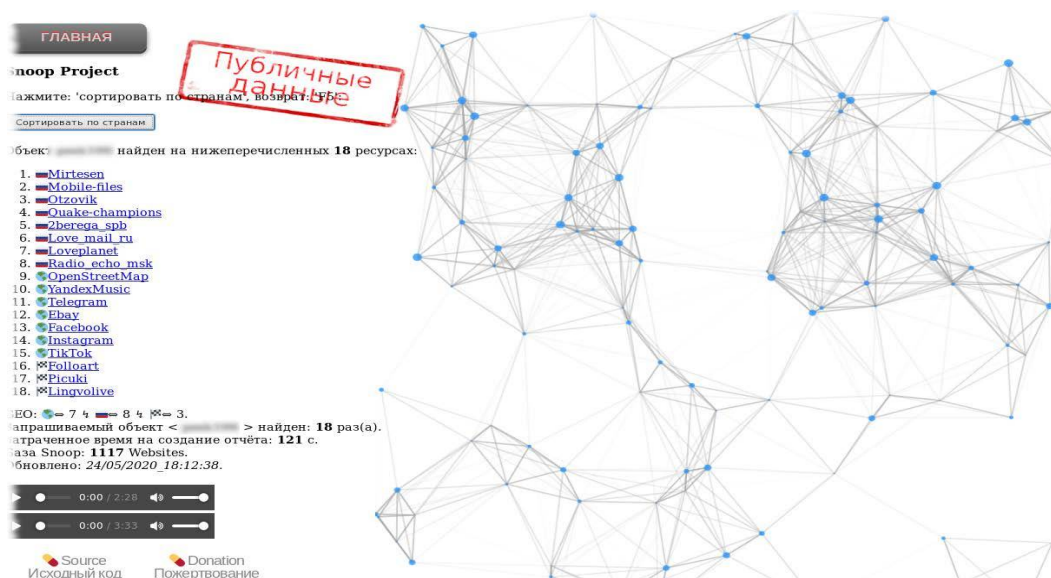
```
~$ snoop.exe --help # для запуска build-версии на OS Windows
```

```
~$ snoop --help # для запуска build-версии на OS GNU/Linux
```

```
~$ python3 snoop.py --help # для запуска source-версии на OS GNU/Linux/Termux
```

```
~$ python snoop.py --help # для запуска source-версии на OS Windows
```

**7)** По окончании работы Snoop запустится браузер с успешными результатами поиска.

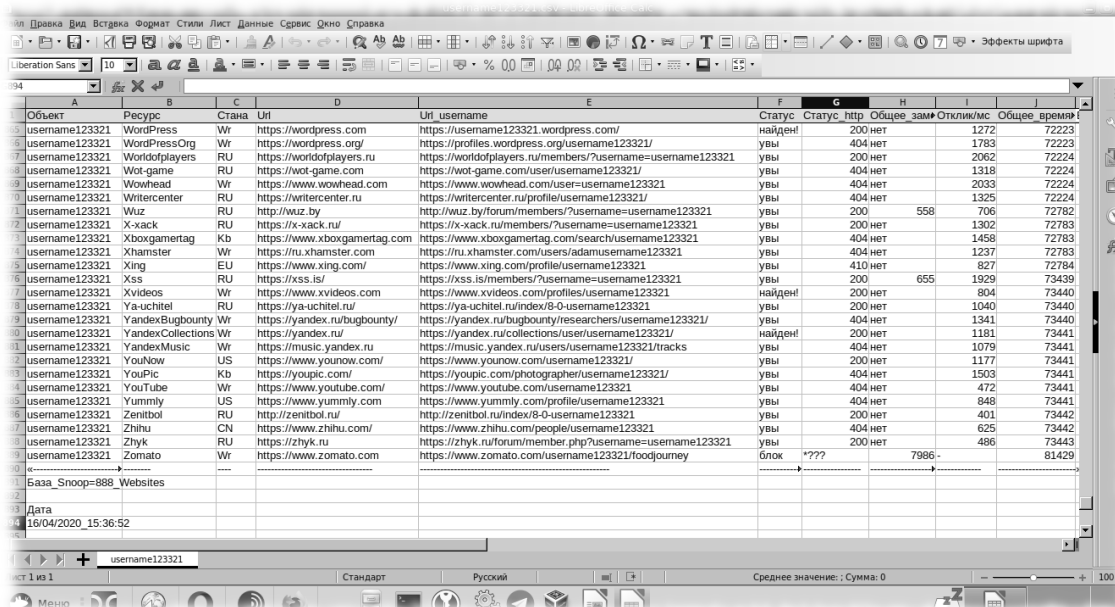


Пример отчета в HTML-формате



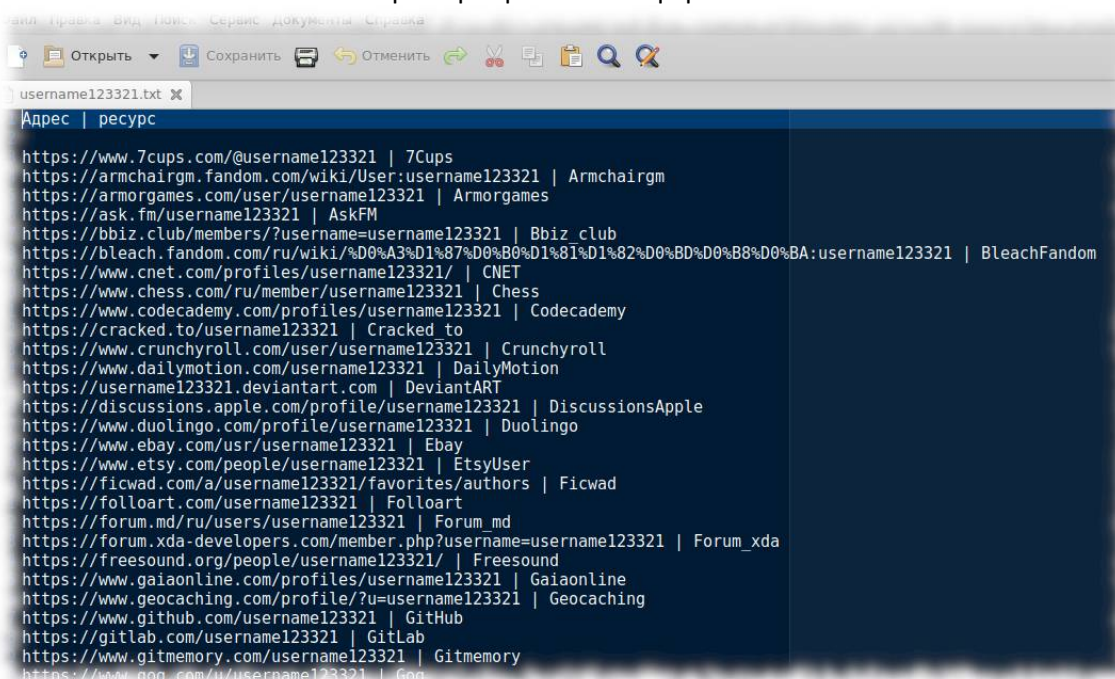
Клик по ссылке откроет персональную страницу «username» на найденном интернет ресурсе, где зарегистрирован разыскиваемый пользователь.

Для быстрого доступа к предыдущим результатам поиска найденных аккаунтов или отчётам в других форматах (*csv/txt*) нажмите кнопку «Главная» в Web-browser-е на странице результатов поиска Snoor. Все успешные результаты поиска сохраняются на HDD/SSD. Поддерживаемые форматы (*save report*): html; txt; csv. Внимание! CSV-отчёты открывать в \*office, разделитель полей - запятая.



| Объект         | Ресурс            | Стана | Uri                          | Uri username   | Статус  | Статус http | Общие зам | Отклики/мс | Общее время |
|----------------|-------------------|-------|------------------------------|--|---------|-------------|-----------|------------|-------------|
| username123321 | WordPress         | Wr    | https://wordpress.com        | https://username123321.wordpress.com/                      | найден! | 200 нет     |           | 1272       | 72223       |
| username123321 | WordPressOrg      | Wr    | https://wordpress.org        | https://profiles.wordpress.org/username123321/             | увы     | 404 нет     |           | 1783       | 72223       |
| username123321 | Worldofplayers    | RU    | https://worldofplayers.ru    | https://worldofplayers.ru/members/?username=username123321 | увы     | 200 нет     |           | 2062       | 72224       |
| username123321 | Wow-game          | RU    | https://wow-game.com         | https://wow-game.com/user/username123321/                  | увы     | 404 нет     |           | 1318       | 72224       |
| username123321 | Wowhead           | Wr    | https://www.wowhead.com      | https://www.wowhead.com/user/username123321                | увы     | 404 нет     |           | 2033       | 72224       |
| username123321 | Writercenter      | RU    | https://writercenter.ru      | https://writercenter.ru/profile/username123321             | увы     | 404 нет     |           | 1325       | 72224       |
| username123321 | Wuz               | RU    | http://wuz.by                | http://wuz.by/forum/members/?username=username123321       | увы     | 200         | 558       | 706        | 72782       |
| username123321 | X-xack            | RU    | https://x-xack.ru            | https://x-xack.ru/members/?username=username123321         | увы     | 200 нет     |           | 1302       | 72783       |
| username123321 | Xboxgamertag      | Kb    | https://www.xboxgamertag.com | https://www.xboxgamertag.com/search/username123321         | увы     | 404 нет     |           | 1458       | 72783       |
| username123321 | Xhamster          | WR    | https://ru.xhamster.com      | https://ru.xhamster.com/users/adamusername123321           | увы     | 404 нет     |           | 1237       | 72783       |
| username123321 | Xing              | EU    | https://www.xing.com         | https://www.xing.com/profile/username123321                | увы     | 410 нет     |           | 827        | 72784       |
| username123321 | Xss               | RU    | https://xss.is               | https://xss.is/members/?username=username123321            | увы     | 200         | 655       | 1929       | 73439       |
| username123321 | Xvideos           | Wr    | https://www.xvideos.com      | https://www.xvideos.com/profiles/username123321            | найден! | 200 нет     |           | 804        | 73440       |
| username123321 | Ya-uchitel        | RU    | https://ya-uchitel.ru        | https://ya-uchitel.ru/index/8-0-username123321             | увы     | 200 нет     |           | 1040       | 73440       |
| username123321 | YandexBugbounty   | WR    | https://yandex.ru/bugbounty/ | https://yandex.ru/bugbounty/researchers/username123321/    | увы     | 404 нет     |           | 1341       | 73440       |
| username123321 | YandexCollections | Wr    | https://yandex.ru            | https://yandex.ru/collections/user/username123321/         | найден! | 200 нет     |           | 1181       | 73441       |
| username123321 | YandexMusic       | Wr    | https://music.yandex.ru      | https://music.yandex.ru/users/username123321/tracks        | увы     | 404 нет     |           | 1079       | 73441       |
| username123321 | YouNow            | US    | https://www.younow.com       | https://www.younow.com/user/username123321/                | увы     | 200 нет     |           | 1177       | 73441       |
| username123321 | YouPic            | Kb    | https://yopic.com            | https://yopic.com/photographer/username123321/             | увы     | 404 нет     |           | 1503       | 73441       |
| username123321 | YouTube           | Wr    | https://www.youtube.com      | https://www.youtube.com/profile/username123321             | увы     | 404 нет     |           | 472        | 73441       |
| username123321 | Yummy             | US    | https://www.yummy.com        | https://www.yummy.com/profile/username123321               | увы     | 404 нет     |           | 848        | 73441       |
| username123321 | Zenitbol          | RU    | http://zenitbol.ru           | http://zenitbol.ru/index/8-0-username123321                | увы     | 200 нет     |           | 401        | 73442       |
| username123321 | Zhihu             | CN    | https://www.zhihu.com        | https://www.zhihu.com/people/username123321                | увы     | 404 нет     |           | 625        | 73442       |
| username123321 | Zhyk              | RU    | https://zhyk.ru              | https://zhyk.ru/forum/member.php?username=username123321   | увы     | 200 нет     |           | 486        | 73443       |
| username123321 | Zomato            | Wr    | https://www.zomato.com       | https://www.zomato.com/username123321/foodjourney          | блок    | ***?        |           | 7986       | 81429       |

Пример report-a в csv-формате



```
Адрес | ресурс
https://www.7cups.com/@username123321 | 7Cups
https://armchairgm.fandom.com/wiki/User:username123321 | Armchairgm
https://armorgames.com/user/username123321 | Armorgames
https://ask.fm/username123321 | AskFM
https://bbiz.club/members/?username=username123321 | Bbiz club
https://bleach.fandom.com/ru/wiki/%D0%A3%D1%87%D0%B8%D1%81%D1%82%D0%BD%D0%B8%D0%BA:username123321 | BleachFandom
https://www.cnet.com/profiles/username123321/ | CNET
https://www.chess.com/ru/member/username123321 | Chess
https://www.codecademy.com/profiles/username123321 | Codecademy
https://cracked.to/username123321 | Cracked to
https://www.crunchyroll.com/user/username123321 | Crunchyroll
https://www.dailymotion.com/username123321 | DailyMotion
https://username123321.deviantart.com | DeviantART
https://discussions.apple.com/profile/username123321 | DiscussionsApple
https://www.duolingo.com/profile/username123321 | Duolingo
https://www.ebay.com/usr/username123321 | Ebay
https://www.etsy.com/people/username123321 | EtsyUser
https://ficwad.com/a/username123321/favorites/authors | Ficwad
https://folloart.com/username123321 | Folloart
https://forum.md/ru/users/username123321 | Forum md
https://forum.xda-developers.com/member.php?username=username123321 | Forum_xda
https://freesound.org/people/username123321/ | Freesound
https://www.gaiaonline.com/profiles/username123321 | Gaiaonline
https://www.geocaching.com/profile/?u=username123321 | Geocaching
https://www.github.com/username123321 | GitHub
https://gitlab.com/username123321 | GitLab
https://www.gitmemory.com/username123321 | Gitmemory
https://www.gog.com/u/username123321 | Gog
```

Пример report-a в txt-формате

Результаты поиска сохраняются по разным путям в зависимости от используемой OS:

в OS GNU/Linux — это каталог «*/home/user/snoop/results/\**»;

в OS Windows — это каталог «*C:\Users\User\AppData\Local\snoop\results\\**»;

в OS Android/Termux — это каталог «*/data/data/com.termux/files/home/snoop/results/\**»;

В исходниках на любой OS — это каталог «*results/\**» в корне директории Snoor.

Уничтожить все результаты поиска — удалить каталог 'results', либо:

snoop.exe --autoclean y # команда на автоудаление всех отчётов Snoor в OS Windows.

# Запуск и использование Snoor на OS GNU/Linux.

Запуск Snoor с ключами на GNU/Linux аналогичен вышеописанному процессу использования Snoor в OS Windows.

```
~$ ldd --version && dpkg -I libc-bin
# Для работы Snoor требуется версия GLIBC (libc-bin) >= 2.29-10
```

```
# Если у пользователя GLIB ниже версии 2.29, то
~$ apt-get update && apt-get install libc-bin
```

```
# Дать права на выполнение (+x) файлу 'snoor'
~$ chmod +x snoor
```

Пользователь не должен запускать файл «snoor» из домашней директории **"home/user/snoor"**. Возникнет ошибка: «*NotADirectoryError: [Errno 20] Not a directory*», потому что при запуске ПО snoor создает/проверяет каталог с таким же именем «snoor» в домашней директории. Запуск файла snoor из любого другого каталога, например, **"home/user/Desktop/snoor"** и не используя root-права. Либо переименуйте snoor, например, в «great\_snoor», в таком случае можно запускать «great\_snoor» из домашней директории: **"home/user/great\_snoor"**.

## Сборка Snoor из исходного кода

### Самостоятельная сборка утилиты Snoor для OS GNU/Linux

**Примечание:** Требуемая версия python 3.7 и выше.

```
# Клонировать репозиторий
$ sudo apt-get update && apt-get install git
$ git clone https://github.com/snoopr/snoor
```

```
# Войти в рабочий каталог
$ cd ~/snoor
```

```
# Установить python3 и python3-pip, если они не установлены
$ sudo apt-get update && apt-get install python3 python3-pip
```

```
# Установить зависимости 'requirements'
$ pip install --upgrade pip
$ python3 -m pip install -r requirements.txt
```

```
# Если вместо флагов стран отображаются спецсимволы (на GNU/Linux), доставить
пакет шрифта, например, монохромный::
$ apt-get install ttf-ancient-fonts
# или цветной::
$ apt-get install fonts-noto-color-emoji
```



## Самостоятельная сборка утилиты Snoop для OS Windows

**Примечание:** Требуемая версия python 3.7 и выше

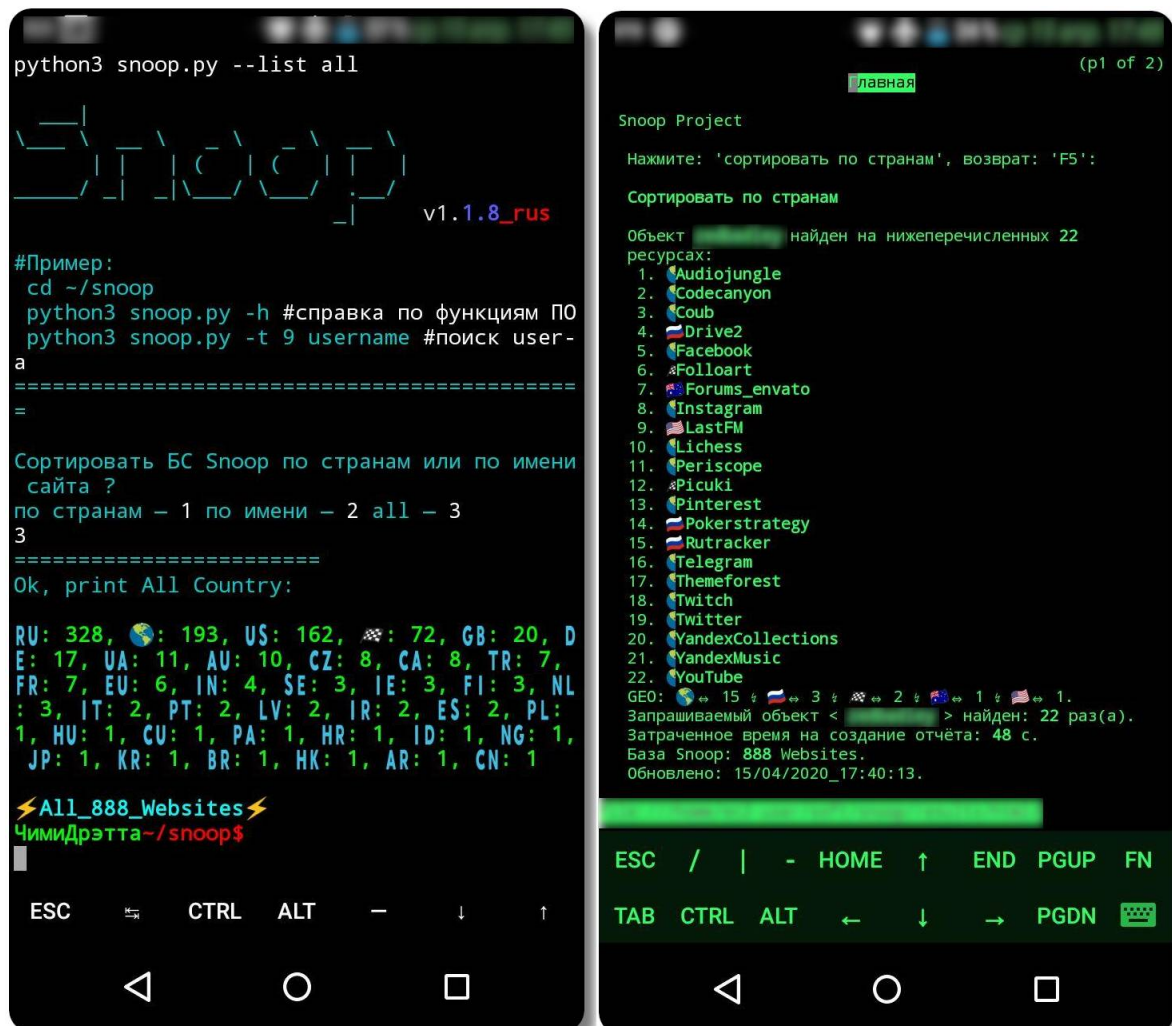
```
# Установить Git для своей версии ОС
# Клонировать репозиторий
$ git clone https://github.com/snooppr/snoop

# Войти в рабочий каталог
$ cd ~/snoop

# Установить python3 с официального сайта https://www.python.org/
# Установить зависимости 'requirements'
$ python -m pip install -r requirements.txt

# На OS Windows использовать cmd или powershell (на выбор — по удобству), но не WSL!
```

## Самостоятельная сборка утилиты Snoop для OS Android



## Инсталляция

### Установить Termux

```
# Примечание: установка Snoop на Termux продолжительная по времени
# Войти в домашнюю папку Termux (т.е. просто открыть Termux)
$ termux-setup-storage
```

```
$ pwd #/data/data/com.termux/files/home #дефолтный/домашний каталог
```

```
# Установить python3 и зависимости
```

```
# Примечание: установка продолжительная по времени
```

```
$ apt update && pkg upgrade && pkg install python libcrypt libxml2 libxslt git
```

```
$ pip install --upgrade pip
```

```
# Клонировать репозиторий Snoor и перейти в ветку Snoor/Termux
```

```
$ git clone https://github.com/snooppr/snoor -b snoor_termux
```

```
# (Если флешка FAT (ни ext4), в таком случае,
```

```
# клонировать репозиторий только в ДОМАШНЮЮ директорию Termux)
```

```
# Войти в рабочий каталог Snoor
```

```
$ cd ~/snoor
```

```
# Установить зависимости 'requirements'
```

```
$ python3 -m pip install -r requirements.txt
```

```
# Чтобы расширить вывод терминала в Termux (по умолчанию 2к строк отображе-  
ние в CLI), например, отображение всей БД опции '--list all [1/2]' добавить строку  
'terminal-transcript-rows=10000' в файл '~/.termux/termux.properties' (фича доступна в  
Termux v0.114+). Перезапустить Termux.
```

```
# Пользователь также может запустить snoor по команде 'snoor' из любого места в  
CLI, создав alias.
```

```
$ printf "alias snoor='cd && cd snoor && python snoor.py'" >> .bashrc
```

```
# Пользователь также может выполнить быструю проверку интересующего его сай-  
та по БД, не используя опцию "--list all", используя команду "snoorcheck"
```

```
$ alias snoorcheck='cd && cd snoor && printf 2 | python snoor.py --list all | grep -i'
```

```
>> .bashrc
```

## Основные процессы поддержания жизненного цикла ПО

### Технические детали

#### Принцип работы и разработки Snoor Project

При использовании основной функции ПО (*поиск username*), с ip адреса пользовате-  
ля поступают http-запросы (*от 10 до 30 запросов в секунду*) на сайты, социальные сети,  
форумы, блоги, интернет порталы, которые проиндексированы в базе данных  
Snoor (*> 2200+ сайтов*) и получение от них http-ответов. Иными словами, при поис-  
ке «username» пользователь сканирует интернет ресурсы, которые  
проиндексированы в базе данных Snoor. По окончании сканирования/поиска  
формируются и сохраняются отчеты в форматах: html; csv; txt о проделанной  
работе. Если пользователь при поиске «username» в результате сбоя/Internet  
Censorship обрабатывает менее 98% БД Snoor Project, то по окончании поиска  
получает об этом предупреждение в CLI и рекомендации об устранении про-  
блем. Сборка (*snoor Windows build-версия*) работает в два/три раза медленнее в  
сравнении со сборкой (*snoor GNU/Linux build-версии*) по причине того, что Snoor под-  
держивается на старых версиях OS: Windows 7\_32-bit и одноядерных ПК. Сбор-  
ка для GNU/Linux работает на современных OS и на платформе не ниже (*amd64*).

ПО Snoor базируется на открытом исходном коде, а значит каждый пользо-  
ватель в ходе эксплуатации ПО может проверить исходный код Snoor и внести  
свои замечания, исправления (*патчи*) и предложения. Специальная страница (*баг-  
трекер ПО Snoor*) для таких предложений расположена по адресу:

<https://github.com/snooppr/snoor/issues>. Чтобы внести предложения, замеча-  
ния или улучшения по работе ПО Snoor пользователь должен зарегистриро-

ваться на портале разработчиков Github и принять правила и политику конфиденциальности интернет ресурса — <https://github.com/>.

Конечное решение по дальнейшей разработке и принятию исправлений в Snoor решает только разработчик Snoor Project.

ПО Snoor в своей кодовой базе использует свободные библиотеки, которые с течением времени обновляются, поэтому в новых релизах (*обновлённые версии*) Snoor могут быть реализованы новые функции, улучшения, исправления или некоторые ошибки, связанные, например, с использованием свободных библиотек и допущенных в них ошибках.

База данных Snoor (*база websites/BDFull/BDdemo*) обновляется и корректируется с учётом изменений, происходящих на websites неподконтрольными разработчику Snoor Project. Например, изменения в api или ответе от интернет ресурса, который был ранее проиндексирован в базе данных Snoor, требует повторной индексации ресурса в БД Snoor, который изменил свой api/ответ. Приблизительно раз в две недели происходит самотестирование БД Snoor на такое поведение websites. И если требуется коррекция БД Snoor с учётом всех этих изменений, то исправление вносится самим разработчиком в ручном режиме, при этом конечному пользователю доступно это обновление без специального уведомления (*запуск ПО Snoor с ключом «-w», пример, snoor.exe -w username*). Информация об обновлении/выходе новых версий Snoor записывается в файл changelog.txt, расположенному по адресу:

<https://raw.githubusercontent.com/snoopr/snoop/master/changelog.txt>

В связи с вышеописанными процессами, обновлённые релизы (*сборки*) Snoor Project являются «плавающими», что является нормой при разработке подобного ПО, а лицензия для конечного пользователя действует с момента эксплуатации ПО (*обновлённого релиза*) до его изъятия. Snoor Project full version предоставляется пользователю по лицензии сроком на 365 дней (*годовая лицензия*).

Сведения о программном обеспечении не составляют государственную тайну и программное обеспечение не содержит сведений, составляющих государственную тайну, кроме того Snoor взаимодействует только с открытыми (*публичными*) источниками данных.

Программное обеспечение Snoor не имеет принудительного обновления и или управления из-за рубежа. До разработки Snoor Project развивал с командой разработчиков популярный OSINT-инструмент — «*Sherlock*». На момент создания Snoor (*февраль 2020г.*) ~1/3 базы данных Sherlock - это работа разработчика Snoor (*Хабр, Пикабу и десятки других добавленных RU-ресурсов в БД Sherlock*).

Соглашение, порядок, требования и условия, в том числе техническая поддержка ПО, между разработчиком и конечным пользователем регулируется лицензией Snoor Project (*COPYRIGHT*) и публичной офертой для ознакомления.

Техническая поддержка и модернизация программного обеспечения, в том числе согласно лицензии Snoor, осуществляется только самим разработчиком Snoor Project (*гражданином РФ*).



## Проверка подписи

Программное Обеспечение Snoor подписано уникальной цифровой подписью разработчика (*sig*), которую пользователю предлагается проверить. В противном случае, для пользователя существуют риски подвергнуться угрозам: подделки, клона, модификации и т.д. похожего вредоносного/программного обеспечения.

Никакое другое программное обеспечение не может иметь цифровую подпись, если оно не было подписано разработчиком Snoop Project.

Отпечаток ключа: 076DB9A00B583FFB606964322F1154A0203EAE9D

Публичный ключ для проверки цифровой подписи находится по адресу:

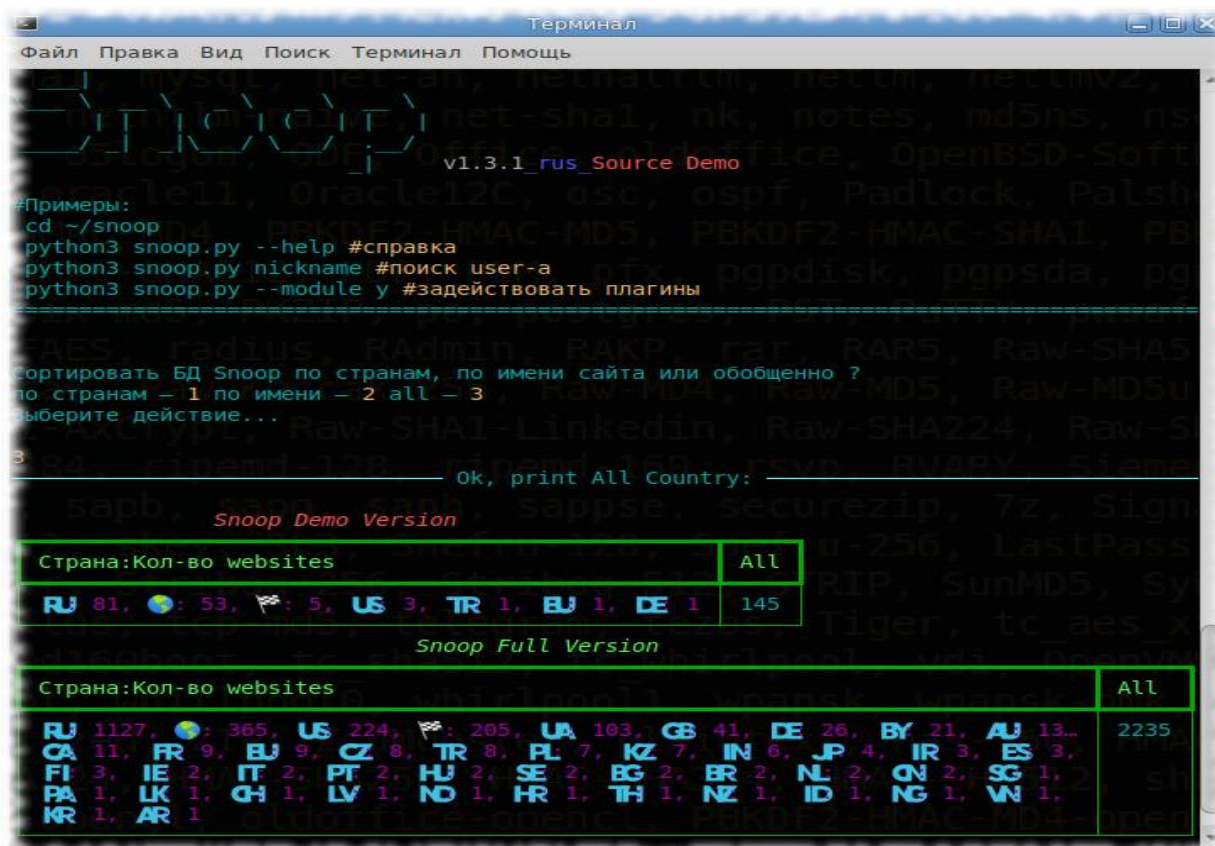
raw.githubusercontent.com/snooppr/snoop/master/PublicKey.asc

или в общедоступной базе ключей.

Существует множество способов для проверки подписи, например, с помощью gpg4usb: <https://gpg4usb.org>.

## База данных Snoop Project

БД Snoop - это самый главный компонент ПО (*поддержка свыше 2k сайтов*) и более **21000 строк кода**. Чтобы развить OSINT-инструмент до такого профессионального уровня/популярности (*Github-рейтинг Snoop Project*) приходилось изучать (*исследовательская работа*) и делать diff на уровне символов, а не строк в исходных кодах (*в т.ч. и обфусцированных*) более 1-й тысячи web-страниц (*см. исходный код Snoop Project*).



Справка о БД доступна по команде:

```
~$ snoop --list all --> [1/3]#запуск Snoop build-версии в OS GNU/Linux
```

```
~$ snoop.exe --list all --> [1/3] # запуск Snoop build-версии в OS Windows
```

```
~$ python3 snoop.py --list all --> [1/3] #запуск Snoop source-версии на OS GNU/Linux/Termux
```

```
~$ python snoop.py --list all --> [1/3] #запуск Snoop source-версии OS Windows
```

```
Файл Правка Вид Поиск Терминал Помощь
krb5, krb5asrep, krb5pa-sha1, krb5tgt, krb5-17, krb5-18, k...
leet, lotus5, lotus85, LUKS, MD2, mdc2, Mediaw...
v1.3.1.rus
happv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, myst...
База DemoRU содержит: 145
База DemoEN содержит: 93
Обновлено, всего — 180 сайта(ов) в blacklist.json
БД сайтов упорядочена по алфавиту.
База данных выровнена, информационные элементы базы данных отсортированы по ключам. Сгенерирован файл 'BDFlag'.
Проверка базы данных:
Общее количество/строк кода информационных элементов в базе данных:: 21079
Ключевые элементы базы данных:
Сайтов в базе BDFull:: 2236
Методов обнаружения:: Counter({'message': 1226, 'status_code': 650, 'redirection': 239, 'response_url': 121})
Используемых api:: 15
Модели Флагов стран:: Counter({'RU': 1129, 'US': 365, 'GB': 205, 'UA': 103, 'DE': 40, 'ES': 26, 'BY': 21, 'AU': 13, 'CA': 11, 'FR': 9, 'EU': 9, 'CZ': 8, 'TR': 8, 'PL': 7, 'KZ': 7, 'IN': 6, 'JP': 4, 'IR': 3, 'ES': 3, 'FI': 3, 'IE': 2, 'IT': 2, 'PT': 2, 'HU': 2, 'SE': 2, 'BG': 2, 'BR': 2, 'NL': 2, 'CN': 2, 'SG': 1, 'PA': 1, 'LK': 1, 'CH': 1, 'LV': 1, 'NO': 1, 'HR': 1, 'TH': 1, 'NZ': 1, 'ID': 1, 'NG': 1, 'VN': 1, 'KR': 1, 'AR': 1})
Буквенных кодов стран:: Counter({'RU': 1129, 'W': 365, 'U': 224, 'K': 205, 'U': 103, 'G': 40, 'D': 26, 'B': 21, 'A': 13, 'I': 11, 'F': 9, 'E': 9, 'C': 8, 'T': 8, 'P': 7, 'Z': 7, 'N': 6, 'J': 4, 'R': 3, 'S': 3, 'F': 3, 'IE': 2, 'IT': 2, 'PT': 2, 'HU': 2, 'SE': 2, 'BG': 2, 'BR': 2, 'NL': 2, 'CN': 2, 'SG': 1, 'PA': 1, 'LK': 1, 'CH': 1, 'LV': 1, 'NO': 1, 'HR': 1, 'TH': 1, 'NZ': 1, 'ID': 1, 'NG': 1, 'VN': 1, 'KR': 1, 'AR': 1})
```

**Благодаря покупке/пожертвованиям пользователей Snoop — база данных Snoop Project поддерживается в актуальном состоянии.** Регулярные обновления БД доступны пользователю при запуске snoop с ключом «-w». Один из [примеров](#) требуемой коррекции БД Snoop Project.

## Справка по ключам Snoop

\$ snoop [ключи] username #пример запуска Snoop на OS GNU/Linux Build-версии.

```
Файл Правка Вид Поиск Терминал Помощь
Snoop v1.3.2.rus.Demo
Примеры:
$ snoop --help #справка
$ snoop username #поиск user.a
$ snoop --module y #задействовать плагины

Использование: snoop [options] nickname
или
$ snoop nickname [options]

Справка
Optional arguments:
-h, --help show this help message and exit

Service arguments:
--version, -V About: вывод на печать версий:: OS: Snoop;
Python и Лицензия
--list all, -l y Вывести на печать детальную информацию о базе
данных Snoop
--donate y, -d y Пожертвовать на развитие Snoop Project-a,
получить/приобрести Snoop Full Version
--autoclean y, -a y Удалить все отчеты, очистить место
--update y, -U y Обновить Snoop/B demo Build version функция
отключена

Plugins arguments:
--module y, -m y OSINT поиск: задействовать различные плагины
Snoop:: IP/GEO/YANDEX (список плагинов будет
пополняться)

Search arguments:
nickname Минимум, раскрытого пользователя.
Поддерживается поиск одновременно нескольких имён.
Ник, содержащий в своем имени пробел, заключается в
кавычки.
--verbose, -v Во время поиска 'username' выводить на печать
подробную вербализацию
--base, -b <path> Указать для поиска 'username' другую БД
(Локально)/B demo version функция отключена
--web-base, -w Подключиться для поиска 'username' к
обновляемой web БД (Онлайн)/ B demo version функция
отключена
--site, -s chess Указать имя сайта из БД '--list all'. Поиск
'username' на одном указанном ресурсе, возможно
использовать опцию '-s' несколько раз
--exclude, -e RU Исключить из поиска выбранный регион,
допустимо использовать опцию '-e' несколько раз,
например, '-e ru -e ua' исключить из поиска Россию и
Украину
--one-level, -o UA Включить в поиск только выбранный регион,
допустимо использовать опцию '-o' несколько раз,
например, '-o us -o ua' поиск по США и Украине
--country, -c Сортировка 'вывода' на
печать/запись результатов' по странам, а не по
алфавиту
--time-out, -t 9 Установить выделение макс.времени на ожидание
ответа от сервера (секунды). Влияет на
продолжительность поиска. Влияет на 'Timeout
ошибки': 'Вкл. эту опцию необходимо при медленном
интернет соединении, чтобы избежать длительных
зависаний при неполадках в сети (по умолчанию значение
выставлено 5с)
--found-print, -f Выводить на печать только найденные аккаунты
--no-func, -n Монохронный терминал, не использовать цвета
в url. Отключить звук. Запретить открытие web
browser-a. Отключить вывод на печать флагов стран
Отключить индикацию и статус прогресса. Экономит
ресурсы системы и ускоряет поиск
--userload, -u Указать файл со списком user.ov. Пример,
'snoop -u ~/listusers.txt start'
--save-page, -S Сохранять найденные странички пользователей в
локальные файлы
--cert-on, -C Вкл проверку сертификатов на серверах. По
умолчанию проверка сертификатов на серверах отключена,
что даёт меньше ошибок и больше положительных
результатов при поиске nickname
--normal, -N Переключатель режимов: SNOOPninja >
нормальный режим > SNOOPninja. По умолчанию (GNU/Linux
Full Version) вкл. 'режим SNOOPninja': ускорение поиска
~25pct, экономия ОЗУ ~50pct, повторное 'гибкое'
соединение на своих ресурсах. Режим SNOOPninja
```

Справка доступна по команде:

~\$ snoop.exe --help #запуск Snoop build-версии в OS Windows

~\$ snoop --help #запуск Snoop build-версии в OS GNU/Linux

~\$ python3 snoop.py --help #запуск Snoop source-версии из исходного кода на OS GNU/Linux/Termux

~\$ python snoop.py --help #запуск Snoop source-версии из исходного кода на OS Windows



# Обновление утилиты Snoop

Обновления утилиты Snoop доступны для ПО собранного из исходного кода.

~\$ python3 snoop.py --update y #запуск Snoop source-версии из исходного кода на GNU/Linux/Termux

~\$ python snoop.py --update y #запуск Snoop source-версии из исходного кода на Windows

```
$python3 snoop.py --update y
v1.1.6_rus
#Пример:
cd ~/snoop
python3 snoop.py -h #справка по функциям ПО
python3 snoop.py -t 9 username #поиск user-a

Вы действительно хотите:
update Snoop?
нажмите 'y' y
Функция обновления Snoop требует установки <Git> на OS GNU/Linux
Нет локальных изменений для сохранения
Обновление 55a7ef7..531a0ef
Fast-forward
 README.md      | 29 +-
 bad_data.json  | 55 +++
 bad_site.md    | 68 +++
 changelog.txt  | 84 +++
 data.json      | 2638 +++++
-----
 example_data.json | 6 +-
 gray_list       | 69 +++
 images/V1.1.7.png | Bin 0 -> 73182 bytes
 sites.md        | 1451 +++++
 snoop.py        | 300 +++++
 10 files changed, 3138 insertions(+), 1562 deletions(-)
 create mode 100644 images/V1.1.7.png
Выход
```

Для скомпилированной версии утилиты Snoop Build (исполняемый файл) доступно только обновление базы данных Snoop Project:

~\$ snoop -w username # подключиться к базе (последней версии online) для поиска «username»

# или менее удобный вариант:

~\$ snoop --update y # «ctrl+s» скачать последнюю версию базу

~\$ snoop -b BDFull username # использовать свежую/скачанную базу для поиска «username».

Либо ожидание выхода обновлённого и стабильного релиза версии Snoop.

<https://github.com/snooppr/snoop/releases>

```
##Snoop Project
v1.2.9
* Переработан и обновлён информативный вывод, Snoop стал выглядеть еще более презентабельнее.
(Изменённый внешний вид (особенно/теперь) будет замечен у пользователей Snoop for Windows,
многие вещи будут автоматически подгоняться под размеры консоли для всех ОС).

* К прогрессу добавлены параметры: прядильщик и истёкшее время.

* По просьбе донатора обновлена опция '-f': 'вывод на печать только найденных аккаунтов'
(ранее опция '-f' выводила найденные аккаунты и оповещения капчи/egg, служебные и
пользовательские оповещения в этом режиме теперь подавляются).

* Обновлена опция '-v' - подробная вербализация
(вывод стал более читабельным).

* Все плагины Snoop обновлены до следующих версий
(исправлены некоторые ошибки, связанные со специфичными путями и спецсимволами,
убран 'Я Район' из плагина 'Yandex_parser' по причине закрытия сервиса. В плагине GEO_IP/domain
добавлен режим 'Offline_тихий поиск', в таблицы добавлена сортировка по значениям).

Изменения коснулись всех версий Snoop 6 из 10 программ (Snoop for Termux/Source;
Windows/Linux/Demo/Full/RU/Build) кроме EN версий. Дальнейшая поддержка EN версий
пока под вопросом (Последние версии Snoop/EN/Build v1.2.8).
```

<https://raw.githubusercontent.com/snooppr/snoop/master/changelog.txt>



# Основные ошибки при поиске: ложноположительные результаты

| Сторона   | Проблема   | Решение |
|-----------|--|---------|
| =====     | =====  | =====   |
| Клиент    | Блокировка соединения проактивной защитой (*Kaspersky)             | 1       |
|           | Недостаточная скорость интернет соединения EDGE / 3G               | 2       |
|           | Слишком низкое значение опции '-t'                                 | 2       |
|           | недопустимое username  | 3       |
|           | Ошибки: [GipsysTeam; RamblerDating; Mamochki; Virtualireland; Ddo] | 7       |
| =====     | =====  | =====   |
| Провайдер | Internet Censorship  | 4       |
| =====     | =====  | =====   |
| Сервер    | Сайт изменил свой ответ/API  | 5       |
|           | Блокировка сервером диапазона ip-адресов клиента                   | 4       |
|           | Срабатывание/защита ресурса captch-ей                              | 4       |
|           | Некоторые сайты временно недоступны, технические работы            | 6       |
| =====     | =====  | =====   |

## Решения:

1. Перенастроить свой Firewall (например, Kaspersky блочит Ресурсы для взрослых).

2. Проверить скорость своего интернет соединения:

```
$ python3 snoop.py -v username
```

Если какой-либо из параметров сети выделен красным цветом, Snoop может подвисать во время поиска.

При низкой скорости увеличить значение 'x' опции '--time-out x':

```
$ python3 snoop.py -t 15 username
```

3. Фактически это не ошибка. Исправить username

(например, на некоторых сайтах недопустимы символы кириллицы; "пробелы"; или 'вьетнамо-китайская\_кодировка' в именах пользователей, в целях экономии времени: — запросы фильтруются).

#### 4. Сменить свой ip-адрес

("Серый" ip и цензура - самое частое из-за чего пользователь получает ошибки пропуска/ложного срабатывания/и в некоторых случаях 'Увы'.

При использовании Snoop с IP адреса провайдера мобильного оператора скорость может упасть в разы, зависит от провайдера.

Например, самый действенный способ решить проблему — ИСПОЛЬЗОВАТЬ VPN, Tor не очень хорошо подходит для данной задачи.

Правило: одного сканирования с одного ip недостаточно для получения максимальной отдачи от Snoop).

#### 5. Открыть в Snoop репозитории на Github-е Issue/Pull request

(сообщить об этом разработчику).

6. Не обращать внимание, сайты иногда уходят на ремонтные работы и возвращаются в строй.

7. [Проблема](<https://wiki.debian.org/ContinuousIntegration/TriagingTips/openssl-1.1.1> "проблема простая и решаемая") с обновленной openssl в некоторых дистрибутивах GNU/Linux

Решение (п7):

```
$ sudo nano /etc/ssl/openssl.cnf
```

# Изменить в самом низу файла строки:

```
[MinProtocol = TLSv1.2]
```

на

```
[MinProtocol = TLSv1]
```

```
[CipherString = DEFAULT@SECLEVEL=2]
```

на

```
[CipherString = DEFAULT@SECLEVEL=1]
```

# Плагины Snoop Project

В дополнение к основной функциональности Snoop Project: поиск username в сети интернет для ПО Snoop разрабатываются плагины.

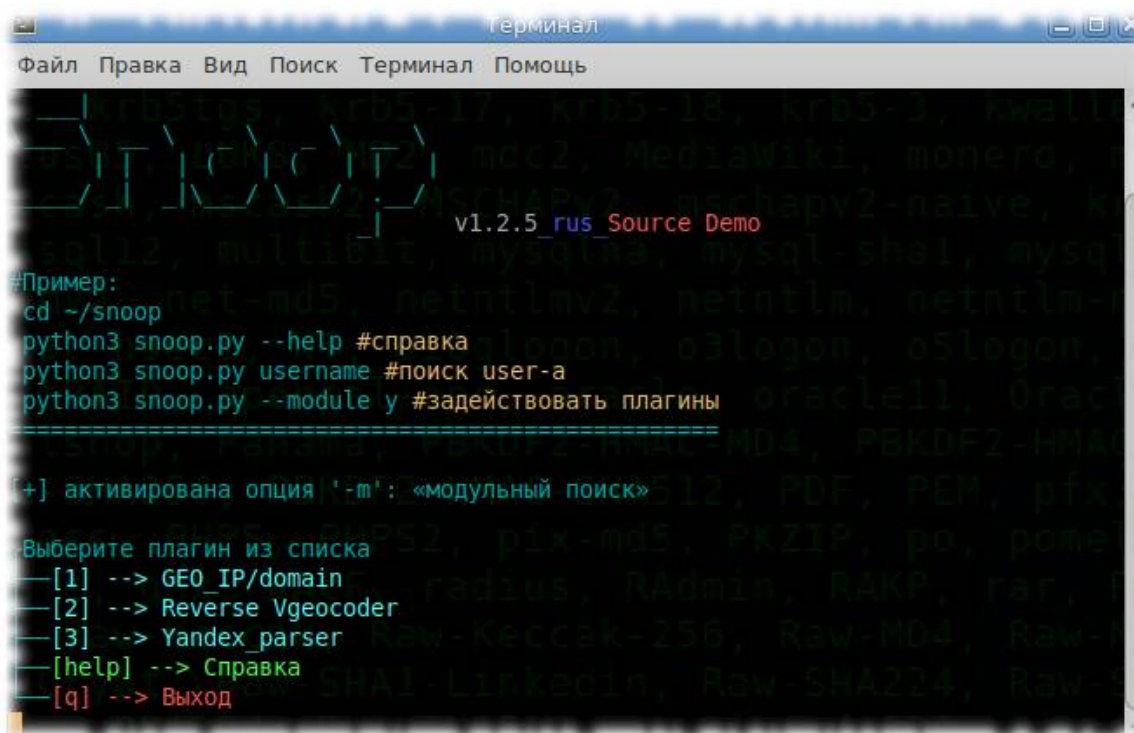
Для выбора плагина используйте команду на запуск:

~\$ snoop.exe --module y #запуск плагинов Snoop build-версии в OS Windows

~\$ snoop --module y #запуск плагинов Snoop build-версии в OS GNU/Linux

~\$ python3 snoop.py --module y #запуск плагинов Snoop source-версии на OS GNU/Linux/Termux

~\$ python snoop.py --module y #запуск плагинов Snoop source-версии на OS Windows



```
терминал
Файл  Правка  Вид  Поиск  Терминал  Помощь

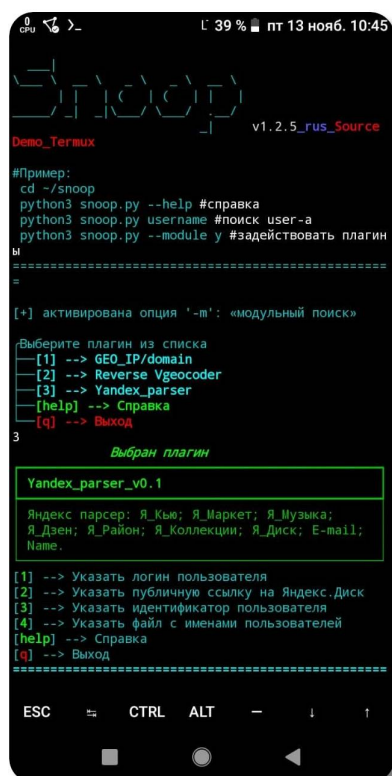
v1.2.5_rus_Source Demo

#Пример:
cd ~/snoop
python3 snoop.py --help #справка
python3 snoop.py username #поиск user-a
python3 snoop.py --module y #задействовать плагины

[+] активирована опция '-m': «модульный поиск»

Выберите плагин из списка
--[1] --> GEO_IP/domain
--[2] --> Reverse Vgeocoder
--[3] --> Yandex_parser
--[help] --> Справка
--[q] --> Выход
```

Пример запуска плагинов Snoop Project на OS GNU/Linux.



```
v1.2.5_rus_Source Demo_Termux

#Пример:
cd ~/snoop
python3 snoop.py --help #справка
python3 snoop.py username #поиск user-a
python3 snoop.py --module y #задействовать плагины

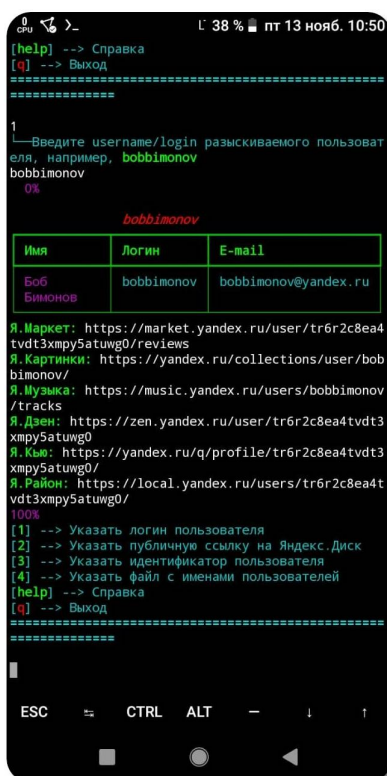
[+] активирована опция '-m': «модульный поиск»

Выберите плагин из списка
--[1] --> GEO_IP/domain
--[2] --> Reverse Vgeocoder
--[3] --> Yandex_parser
--[help] --> Справка
--[q] --> Выход

Выбран плагин
Yandex_parser_v0.1

Яндекс парсер: Я_Кью; Я_Маркет; Я_Музыка;
Я_Дзен; Я_Район; Я_Коллекции; Я_Диск; E-mail;
Name.

[1] --> Указать логин пользователя
[2] --> Указать публичную ссылку на Яндекс.Диск
[3] --> Указать идентификатор пользователя
[4] --> Указать файл с именами пользователей
[help] --> Справка
[q] --> Выход
```



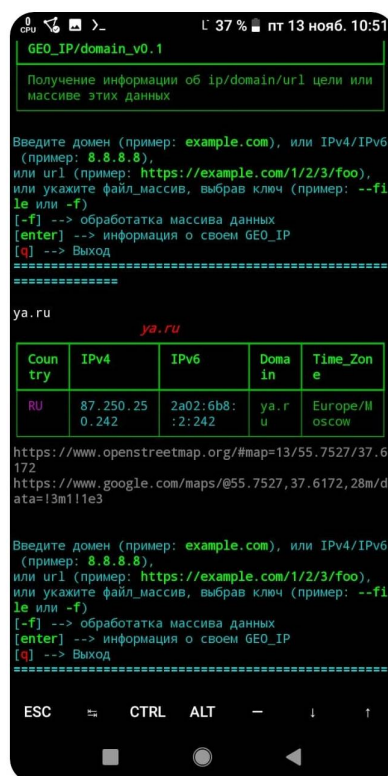
```
[help] --> Справка
[q] --> Выход

1
Введите username/login разыскиваемого пользоват
еля, например, bobbimonov
bobbimonov

bobbimonov

Имя    Логин    E-mail
Боб    bobbimonov    bobbimonov@yandex.ru

Я_Маркет: https://market.yandex.ru/user/tr6r2c8ea4
tvdt3xmpy5atuwg0/reviews
Я_Картинки: https://yandex.ru/collections/user/bob
bimonov/
Я_Музыка: https://music.yandex.ru/users/bobbimonov
/tracks
Я_Дзен: https://zen.yandex.ru/user/tr6r2c8ea4tvdt3
xmpy5atuwg0
Я_Кью: https://yandex.ru/q/profile/tr6r2c8ea4tvdt3
xmpy5atuwg0/
Я_Район: https://local.yandex.ru/users/tr6r2c8ea4t
vdt3xmpy5atuwg0/
100%
[1] --> Указать логин пользователя
[2] --> Указать публичную ссылку на Яндекс.Диск
[3] --> Указать идентификатор пользователя
[4] --> Указать файл с именами пользователей
[help] --> Справка
[q] --> Выход
```



```
GEO_IP/domain_v0.1

Получение информации об ip/domain/url цели или
массиве этих данных

Введите домен (пример: example.com), или IPv4/IPv6
(пример: 8.8.8.8),
или url (пример: https://example.com/1/2/3/foo),
или укажите файл_массив, выбрав ключ (пример: --fi
le или -f)
[-f] --> обработка массива данных
[enter] --> информация о своем GEO_IP
[q] --> Выход

ya.ru

ya.ru

Country  IPv4  IPv6  Doma  Time_Zon
in     e
RU       87.250.25  2a02:6b8:  ya.r  Europe/M
0.242   :2:242   u     oscow

https://www.openstreetmap.org/#map=13/55.7527/37.6
172
https://www.google.com/maps/@55.7527,37.6172,28m/d
ata=!3m1!1e3

Введите домен (пример: example.com), или IPv4/IPv6
(пример: 8.8.8.8),
или url (пример: https://example.com/1/2/3/foo),
или укажите файл_массив, выбрав ключ (пример: --fi
le или -f)
[-f] --> обработка массива данных
[enter] --> информация о своем GEO_IP
[q] --> Выход
```

Пример запуска плагинов Snoop Project на OS Android/Termux.



## Плагин GEO\_IP/domain

Данный плагин позволяет выбирать в качестве цели массивы данных: ip/domain/url.

1) Реализует онлайн одиночный поиск цели по IP/url/domain и предоставляет статистическую информацию: IPv4/v6; GEO-координаты/ссылку; локация.

*(Лёгкий ограниченный поиск).*

2) Реализует онлайн поиск цели по списку данных: и предоставляет статистическую и визуализированную информацию: IPv4/v6; GEO-координаты/ссылки; страны/города; отчеты в CLI/txt/csv форматах; предоставляет визуализированный отчет на картах OSM.

*(Умеренный не быстрый поиск: ограничения запросов:: 15к/час; не предоставляет информацию о провайдерах).*

3) Реализует офлайн поиск цели по списку данных, используя БД: и предоставляет статистическую и визуализированную информацию: IPv4/v6; GEO-координаты/ссылки; локации; провайдеры; отчеты в CLI/txt/csv форматах; предоставляет визуализированный отчет на картах OSM. Например, можно определить любых (*множество*) интернет-провайдеров по ip за несколько секунд.

*(Сильный и быстрый поиск).*

Результаты по [1 и 2] методу могут отличаться и быть неполными - зависит от персональных настроек DNS/IPv6 пользователя.

Список данных — текстовый файл (*в кодировке utf-8*), который пользователь указывает в качестве цели, и который содержит ip или domain или url (*или их комбинации*).

### Метод 'Online поиск'.

Модуль GEO\_IP/domain от Snoop Project использует публичный api и создает статистическую и визуализированную информацию по ip/url/domain цели (*массиву данных*).

*(Ограничения: запросы ~15к/час, невысокая скорость обработки данных, отсутствие информации о провайдерах).*

Преимущества использования 'Online поиска':

в качестве массива данных можно использовать не только ip-адреса, но и domain/url.

Пример файла массива данных (*массив.txt*):

1.1.1.1

2606:2800:220:1:248:1893:25c8:1946

google.com

https://example.org/fo/bar/7564

случайная строка

## Метод 'Offline поиск'.

Модуль GEO\_IP/domain от Snoor Project использует специальные базы данных и создает статистическую и визуализированную информацию только по ip цели (массиву данных).

(Базы данных доступны свободно для скачивания от компании Maxmind после регистрации аккаунта. Ограничения: скачанные базы можно использовать для личных целей или внутри организации. По лицензии Maxmind БД нельзя распространять разработчикам, поэтому БД не поставляются со Snoor Project, но доступны для бесплатного скачивания с оф.сайта Maxmind).

Скачать бесплатно базы: <https://dev.maxmind.com/geoip/geoip2/geolite2/>

Для использования поиска необходимо скачать две бесплатные базы: ~40Мб 'GeoLite2-City.mmdb' и 'GeoLite2-ASN.mmdb'.

Преимущества использования 'Offline поиска': скорость (обработка тысяч ip без задержек), стабильность (отсутствие зависимости от интернет соединения и персональных настроек DNS/IPv6 пользователя), масштабный охват/покрытие (предоставляется информация об интернет-провайдерах).

Пример файла списка данных (массив.txt):

8.8.8.8

93.184.216.34

2606:2800:220:1:248:1893:25c8:1946

случайная строка

Snoor довольно умен и способен определять в массиве данных: IPv4/v6/domain/url, вычищая ошибки и случайные строки.

По окончании обработки данных пользователю предоставляются: статистические отчеты в [txt/csv и визуализированные данные на карте OSM].

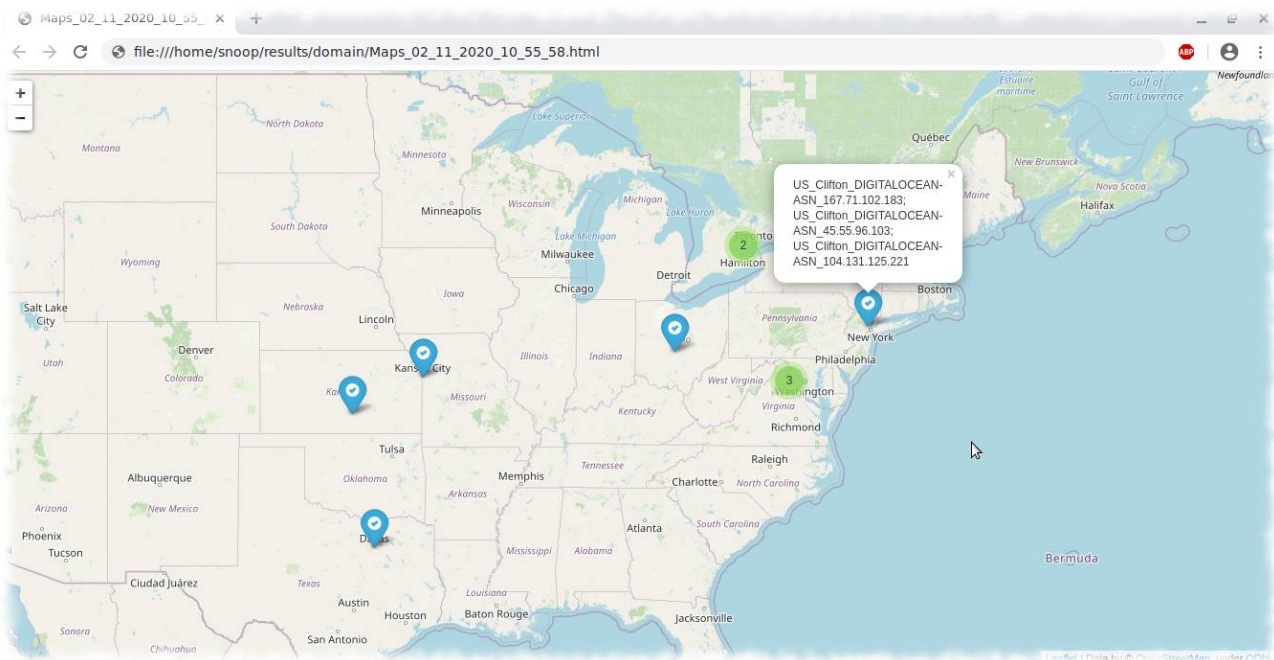
Примеры для чего можно использовать модуль GEO\_IP/domain от Snoor Project. Например, если у пользователя имеется список ip адресов от DDoS атаки, он может проанализировать откуда исходила max/min атака и от кого (провайдеры). Решая квесты-CTF, где используются GPS/IPv4/v6. В конечном итоге юзать плагин в образовательных целях или из естественного любопытства (проверить любые ip-адреса и их принадлежность к провайдеру и местности).

Пример отчетов при использовании плагина GEO\_IP/domain в Snoor Project.

```
Терминал
Файл Правка Вид Поиск Терминал Помощь
00:04 100% 52.220.198.205
Country Time_Zone Provider Latitude longitude
SG Singapore AMAZON-02 1.2929 103.8547
00:04 100%
Country statistics
US:181(46.9%), RU:85(22.0%), DE:47(12.2%), FR:14(3.6%), NL:10(2.6%), GB:9(2.3%), CA:9(2.3%), UA:6(1.6%), FI:3(0.8%), LU:2(0.5%), CN:2(0.5%), AU:2(0.5%), SE:2(0.5%), CZ:2(0.5%), EE:2(0.5%), LV:1(0.3%), IE:1(0.3%), NO:1(0.3%), PT:1(0.3%), BY:1(0.3%), BE:1(0.3%), LT:1(0.3%), CH:1(0.3%), None:1(0.3%), SG:1(0.3%)
city statistics
None:276(71.5%), Moscow:22(5.7%), Ashburn:15(3.9%), Frankfurt am Main:6(1.6%), Dallas:4(1.0%), Boardman:3(0.8%), San Jose:3(0.8%), Clifton:3(0.8%), Amsterdam:3(0.8%), Beauharnois:3(0.8%), Kansas City:3(0.8%), Helsinki:3(0.8%), Berlin:2(0.5%), St Petersburg:2(0.5%), London:2(0.5%), Washington:1(0.3%), Ansbach:1(0.3%), Dublin:1(0.3%), Krasnoyarsk:1(0.3%), Bratsk:1(0.3%), Grunwald:1(0.3%), Yelets:1(0.3%), Kyiv:1(0.3%), Fremont:1(0.3%), Podolsk:1(0.3%), Portland:1(0.3%), Montreal:1(0.3%), Calistoga:1(0.3%), Paris:1(0.3%), Stockholm:1(0.3%), Langenbach:1(0.3%), Los Angeles:1(0.3%), Remseck:1(0.3%), Santa Clara:1(0.3%), Sydney:1(0.3%), Kirov:1(0.3%), Columbus:1(0.3%), Magny-les-Hameaux:1(0.3%), Canterbury:1(0.3%), Oldenzaal:1(0.3%), Nuremberg:1(0.3%), Berkeley:1(0.3%), Mogilev:1(0.3%), Brussels:1(0.3%), Mannheim:1(0.3%), Prague:1(0.3%), Guelph:1(0.3%), San Francisco:1(0.3%), Volgograd:1(0.3%), Haarlem:1(0.3%), Singapore:1(0.3%)
ISP_statistics
CLOUDFLARENET:74(19.2%), Hetzner Online GmbH:36(9.3%), AMAZON-02:27(7.0%), AMAZON-AES:19(4.9%), OVH SAS:19(4.9%), FASTLY:14(3.6%), DIGITALOCEAN-ASN:9(2.3%), computeit Limited:8(2.1%), Domain names registrar REG.RU, Ltd:8(2.1%), TimeWeb Ltd:7(1.8%), 000 Network of data-centers Selectel:6(1.6%), HURRICANE:6(1.6%), Mos-guard Ltd:5(1.3%), Linode, LLC:5(1.3%), Beget LLC:4(1.0%), WEBRX:4(1.0%), RealHost Ltd:4(1.0%), GOOGLE:4(1.0%), Mail.Ru LLC:3(0.8%), JSC The First:3(0.8%), online S.a.s.:2(0.5%), AS-26496-GO-DADDY-COM-LLC:2(0.5%), HLL LLC:2(0.5%), AKAMAI-AS:2(0.5%), LIQUIDWEB:2(0.5%), Internet-Hosting Ltd:2(0.5%), Ihor Hosting LLC:2(0.5%), United Network LLC:2(0.5%), LeaseWeb Netherlands B.V.:2(0.5%), P.a.g.m. Ou:2(0.5%), 000 National Telecommunications:2(0.5%), Filanco LLC:2(0.5%), HVC-AS:2(0.5%), AIS-WEST:2(0.5%), MICROSOFT-CORP-MSN-AS-BLOCK:1(0.3%), root SA:1(0.3%), LLC Server v arendy:1(0.3%), Innova Co S.A.R.L.:1(0.3%), Castlake Company Ltd:1(0.3%), SprintHost.ru LLC:1(0.3%), Majordomo LLC:1(0.3%), LeaseWeb Deutschland GmbH:1(0.3%), IBS Expertise LLC:1(0.3%), Ningxia West Cloud Data Technology Co.Ltd.:1(0.3%), Transdata AS:1(0.3%), Rambler Internet Holding LLC:1(0.3%), NetConnex Broadband Ltd.:1(0.3%), PlusServer GmbH:1(0.3%), TURBINE:1(0.3%), VarTV Ltd.:1(0.3%), EDGECAST:1(0.3%), JOESDATACENTER:1(0.3%), EBAY:1(0.3%), Dataweb Global Group B.V.:1(0.3%), myLoc managed IT AG:1(0.3%), Docker LTD:1(0.3%), Novaya
```

Отчет в CLI (обработка случайно-сгенерированных ip-адресов).





Отчет в HTML-формате на карте OSM.

| Страна | IP  | Провайдер                              | Широта, Долгота | Файл с IP адресами |
|--------|-----|--|-----------------|--------------------|
| US     | 52  | AMAZON-AES                             | 37.751,-4       | ip                 |
| US     | 104 | CLOUDFLARENET                          | 37.751,-4       | ip                 |
| RU     | 91  | RealHost Ltd.                          | 55.7386,-8      | ip                 |
| US     | 104 | CLOUDFLARENET                          | 37.751,-4       | ip                 |
| UA     | 91  | First Ukrainian Internet Registrar LLC | 50.4522,-7      | ip                 |
| UA     | 188 | Ltd Hostpro Lab                        | 50.4522,-7      | ip                 |
| US     | 104 | CLOUDFLARENET                          | 37.751,-4       | ip                 |
| FR     | 164 | OVH SAS                                | 48.8582,-2      | ip                 |
| US     | 35  | GOOGLE                                 | 39.1028,-78     | ip                 |
| US     | 208 | LIQUIDWEB                              | 37.751,-4       | ip                 |
| SE     | 91  | ODERLAND Webshotell AB                 | 59.3247,-18     | ip                 |
| US     | 54  | AMAZON-02                              | 37.3388,-114    | ip                 |
| US     | 45  | Limode LLC                             | 32.7787,-17     | ip                 |
| RU     | 196 | SINGLEHOP-LLC                          | 37.751,-4       | ip                 |
| RU     | 37  | JSC The First                          | 55.7386,-8      | ip                 |
| UA     | 45  | Zomro B.V.                             | 50.4522,-7      | ip                 |
| US     | 104 | CLOUDFLARENET                          | 37.751,-4       | ip                 |
| NO     | 106 | New Work SE                            | 47.080,-19      | ip                 |
| RU     | 196 | Ddos-guard Ltd                         | 55.7522,-6      | ip                 |
| FI     | 95  | Hetzner Online GmbH                    | 60.1719,-7      | ip                 |
| RU     | 37  | Internet-Hosting Ltd                   | 55.7386,-8      | ip                 |
| RU     | 196 | Computbyte Limited                     | 55.7522,-6      | ip                 |
| CN     | 103 | CHINA UNICOM China169 Backbone         | 34.7725,-66     | ip                 |
| US     | 104 | CLOUDFLARENET                          | 37.751,-4       | ip                 |
| RU     | 188 | TimeWeb Ltd.                           | 55.7386,-8      | ip                 |
| SG     | 52  | AMAZON-02                              | 1.2929,1        | 7 ip               |

Отчет в csv-формате (\*office).

```

#IP13_11_2021_10_06_0110 %
994 DE || 188.96.166.151 || Vodafone GmbH || 53.5389,10.128
995 DE || 2.171.2.143 || Deutsche Telekom AG || 51.2993,9.491
996 US || 134.250.181.218 || WEST-NET-WEST || 37.6771,-113.062
997 JP || 60.115.95.187 || Softbank BB Corp. || 35.6772,139.7708
998 US || 54.188.65.224 || AMAZON-02 || 45.8491,-119.7143
999 RU || 188.19.224.49 || Rostelecom || 66.0833,76.6333
1000 RO || 136.255.78.48 || Vodafone Romania S.A. || 45.9968,24.997
1001 RU || 192.124.187.120 || IT_Energy_Service || 55.7522,37.6156
1002
1003
1004 Страны:
1005 US:423(42.3%), CN:96(9.6%), JP:51(5.1%), KR:31(3.1%), GB:30(3.0%), DE:28(2.8%), IT:21(2.1%), CA:21(2.1%), BR:19(1.9%), FR:18(1.8%), AU:
18(1.8%), RU:17(1.7%), MX:15(1.5%), TW:14(1.4%), SG:12(1.2%), ES:11(1.1%), NO:11(1.1%), NL:10(1.0%), KZ:9(0.9%), PL:9(0.9%), SE:8(0.8%), ID:
7(0.7%), CO:7(0.7%), IN:7(0.7%), DK:6(0.6%), AR:5(0.5%), HK:5(0.5%), IL:4(0.4%), BE:4(0.4%), CL:4(0.4%), EG:4(0.4%), CZ:4(0.4%), AT:4(0.4%),
PK:4(0.4%), ZA:3(0.3%), CH:3(0.3%), IR:3(0.3%), PH:3(0.3%), PT:3(0.3%), TR:3(0.3%), MY:2(0.2%), SA:2(0.2%), FI:2(0.2%), MA:2(0.2%), BA:
2(0.2%), HU:2(0.2%), RS:2(0.2%), IE:2(0.2%), UA:2(0.2%), RO:2(0.2%), BG:1(0.1%), MP:1(0.1%), BO:1(0.1%), None:1(0.1%), OM:1(0.1%), LV:
1(0.1%), NZ:1(0.1%), CI:1(0.1%), MG:1(0.1%), KE:1(0.1%), CR:1(0.1%), BN:1(0.1%), LR:1(0.1%), AM:1(0.1%), KW:1(0.1%), UY:1(0.1%), PA:1(0.1%),
AW:1(0.1%), BG:1(0.1%), PE:1(0.1%), EC:1(0.1%), GT:1(0.1%), TH:1(0.1%), VN:1(0.1%)
1006
1007 Провайдеры:
1008 ATT-INTERNET4:21(2.1%), CHINA UNICOM China169 Backbone:17(1.7%), COMCAST-7922:15(1.5%), Chinanet:15(1.5%), LEVEL3:14(1.4%), Korea Telecom:
11(1.1%), DNIC-ASBLK-00721-00726:10(1.0%), Telecom Italia:10(1.0%), Deutsche Telekom AG:9(0.9%), MICROSOFT-CORP-MSN-AS-BLOCK:9(0.9%), UUNET:
8(0.8%), China Education and Research Network Center:8(0.8%), NTT Communications Corporation:8(0.8%), AMAZON-02:6(0.6%), Orange Espagne SA:
6(0.6%), SPCS:6(0.6%), Tele Danmark:5(0.5%), SURFnet bv:5(0.5%), China Unicom IP network China169 Guangdong province:5(0.5%), SFR SA:5(0.5%),
Softbank BB Corp.:5(0.5%), Alibaba (US) Technology Co., Ltd.:5(0.5%), COGENT-174:5(0.5%), TIM S/A:5(0.5%), Data Communication Business Group:
5(0.5%), WINDSTREAM:5(0.5%), Liberty Global B.V.:4(0.4%), China Unicom Beijing Province Network:4(0.4%), Guangdong Mobile Communication
Co.Ltd.:4(0.4%), CELLCO:4(0.4%), Telia Company AB:4(0.4%), SK Broadband Co Ltd:4(0.4%), AMAZON-AES:4(0.4%), CENTURYLINK-US-LEGACY-QWEST:
4(0.4%), JSC Kazakhtelecom:4(0.4%), Daimler AG:4(0.4%), British Telecommunications PLC:4(0.4%), Uninet S.A. de C.V.:4(0.4%), LG POWERCOMM:
4(0.4%), KODI CORPORATION:3(0.3%), BELLSOUTH-NET-BLK:3(0.3%), Telefonica Germany:3(0.3%), ASN852:3(0.3%), ARTERIA Networks Corporation:
3(0.3%), TWC-11426-CAROLINAS:3(0.3%), CELLCO-PART:3(0.3%), Free SAS:3(0.3%), Telstra Corporation Ltd:3(0.3%), Globalconnect As:3(0.3%),

```

Отчет в txt-формате.



## Плагин Reverse Vgeocoder

Обратный геокодер для визуализации координат на карте OSM и статистическим анализом в csv/txt форматах.

Плагин реализует оффлайн поиск цели по заданным координатам и предоставляет статистическую и визуализированную информацию.

Предназначение — СТФ.

Плагин поддерживает два режима геокодирования:

Метод 'Простой': На карте OSM расставляются маркеры по координатам. Все маркеры подписаны геометками.

Для данного метода доступны сокращенные отчёты с геометками в html-формате и статистической информацией в txt-формате.

Метод 'Подробный': На карте OSM расставляются маркеры по координатам. Все маркеры подписаны геометками; странами; округами и городами.

Статистические отчёты *(с расширенной геоинформацией, а также расчётом количественной информацией процентного соотношения)* сохраняются с подробностями в [txt.html.csv] форматах.

Данный метод довольно точно расставляет маркеры с геометками, но подписывает их адресом к ближайшим населённым пунктам от 2000 человек. Например, если пользователь загрузит для обработки, координаты указывающие в 500 метрах от г. Выкса (*лес*), то маркер на карте OSM встанет точно (*в лесу*), а подписан он будет примерно так: ('Ш:55.3301 Д:42.2604::Страна:RU::ГородскойОкруг1: Nizhnij Novgorod::ГородскойОкруг2:Vyksa'). То есть метод работает на основе — '[Евклидово дерево](#)'.

Плагин Reverse Vgeocoder - работает в оффлайн режиме и укомплектован гео-БД *(БД предоставляются под свободной лицензией от gonames.org)*. То есть для работы плагина не требуется подключение к сети.

Это удобный плагин, если пользователю необходимо, например, не только обработать геокоординаты, но и найти хаотичные данные - или наоборот.

Для визуализации данных на карте OSM укажите *(при запросе)* текстовый файл с координатами в кодировке utf-8 *(с расширением .txt или без расширения)*.

Каждая точка координат *(широта, долгота)* с новой строки в файле *(желательно)*.

Споор довольно умён: распознаёт и выбирает геокоординаты через запятую, слэш, пробел'ы, или делает интеллектуальную выборку, вычищая случайные строки и символы.

Пример файла с геокоординатами *(как может быть записан файл с координатами, который необходимо указывать)*:

51.352, 108.625

55.466,64.776

52.40662,66.77631

53.028 -104.680

54.505 73.773

Москва 55.75, 37.62 Калининград54.71 20.51 Ростов-на-Дону 47.23/39.72

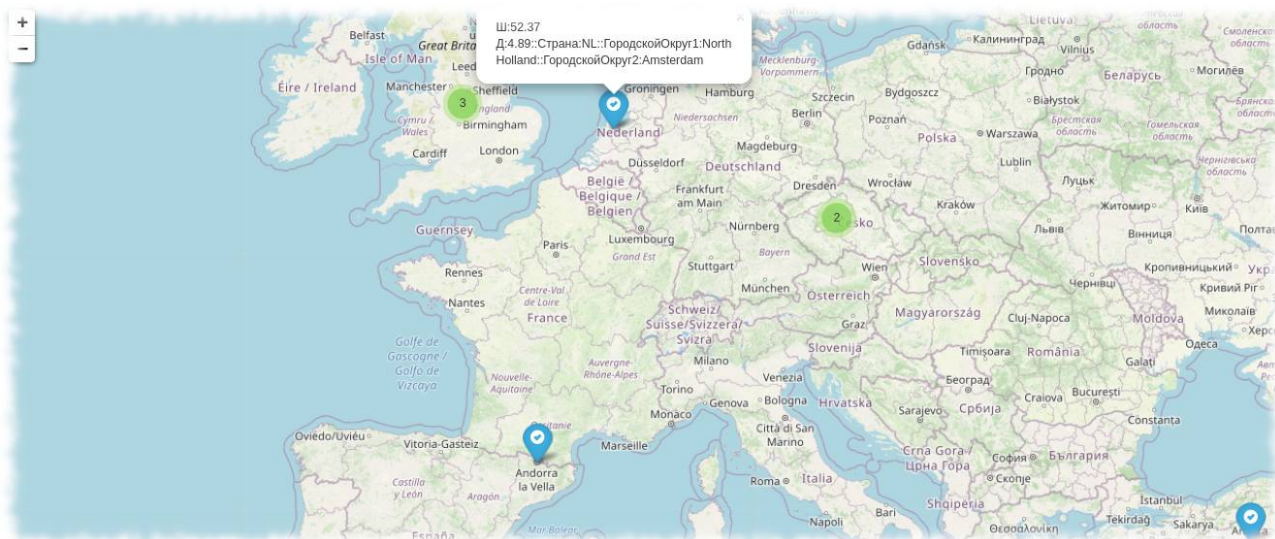
случайная\_строка1, которая\_будет обработана Казань 55.7734/49.1436

случайная строка2, которая не будет обработана

По окончании рендеринга откроется webbrowser с визуальным результатом.

Для статистической обработки информации (сортировка по странам/координатам/  
raw\_данным) пользователь должен изучить отчёт в csv-формате.

Все результаты сохраняются в '~/snoop/results/ReverseVgeocoder/  
\*[.txt.html.csv]'



Визуализация подписанных геокоординат, точек на карте OSM.

```
TR || Ankara || Ankara || 39.92,32.85
MG || Analamanga || Antananarivo || -18.91,47.54
WS || Tuamasaga || Apia || -13.83,-171.77
CZ || Praha || Mala Strana || 50.0744,14.3952
CZ || Central Bohemia || Trhovy Stepanov || 49.7112,15.0073
GB || England || Smethwick || 52.505,-1.9575
GB || England || Newark on Trent || 53.0869,-0.8226
GB || England || Stretford || 53.4379,-2.3163
JP || Iwate || Yamada || 38.2465,145.0558

Страны:
RU:8(32.0%), AE:1(4.0%), NG:1(4.0%), ET:1(4.0%), GH:1(4.0%), DZ:1(4.0%), JO:1(4.0%), NL:1(4.0%), AD:1(4.0%), TR:1(4.0%), MG:1(4.0%), WS:
1(4.0%), CZ:2(8.0%), GB:3(12.0%), JP:1(4.0%)

Гор.Округ1:
Moscow:3(12.0%), Rjazan:2(8.0%), Tula:1(4.0%), Chelyabinsk:1(4.0%), Abu Dhabi:1(4.0%), Abuja Federal Capital Territory:1(4.0%), Adis Abeba:
1(4.0%), Greater Accra:1(4.0%), Alger:1(4.0%), Amman:1(4.0%), North Holland:1(4.0%), Andorra la Vella:1(4.0%), Jaroslavl:1(4.0%), Ankara:
1(4.0%), Analamanga:1(4.0%), Tuamasaga:1(4.0%), Praha:1(4.0%), Central Bohemia:1(4.0%), England:3(12.0%), Iwate:1(4.0%)

Гор.Округ2:
'Sokol:1(4.0%), Polyany:1(4.0%), Zamoskvorech'ye:2(8.0%), Ryazan':1(4.0%), Mendeleyevskiy:1(4.0%), Magnitogorsk:1(4.0%), Abu Dhabi:1(4.0%),
Abuja:1(4.0%), Addis Ababa:1(4.0%), Accra:1(4.0%), Birkhadem:1(4.0%), Amman:1(4.0%), Amsterdam:1(4.0%), Andorra la Vella:1(4.0%), Jaroslavl:
1(4.0%), Ankara:1(4.0%), Antananarivo:1(4.0%), Apia:1(4.0%), Mala Strana:1(4.0%), Trhovy Stepanov:1(4.0%), Smethwick:1(4.0%), Newark on Trent:
1(4.0%), Stretford:1(4.0%), Yamada:1(4.0%)'

=====
Необработанные данные из файла 'координаты':
58.0637111111 38.8595555555
=====
```

Отчёт в txt-формате. Подобные отчёты создаются (раскрашенные в CLI) и csv-форматах.

В последних версиях Snoop выборка геокоординат стала еще более интеллектуальной и строка:

«58.0637111111 38.8595555555» будет успешно обработана.

## Плагин Yandex\_parser

Плагин позволяет получить информацию о пользователе/пользователях сервисов Яндекс: Я\_Отзывы; Я\_Кью; Я\_Маркет; Я\_Музыка; Я\_Дзен; Я\_Район; Я\_Коллекции; Я\_Диск; E-mail; Name.

И связать полученные данные между собой с высокой скоростью и масштабно. Предназначение — OSINT.

Плагин разработан на идее и материалах уязвимости, отчёт был отправлен Яндексу в рамках программы «Охота за ошибками».

Попал в зал славы Яндекса, получил финансовое вознаграждение, а транснациональная корпорация исправила ошибки по своему усмотрению.

```
=====
[1] --> Указать логин пользователя
[2] --> Указать публичную ссылку на Яндекс.Диск
[3] --> Указать идентификатор пользователя
[4] --> Указать файл с именами пользователей
[help] --> Справка
[q] --> Выход
=====
```

### Однопользовательский режим

\* **Логин** — левая часть до символа '@', например, bobbimonov@ya.ru, логин 'bobbimonov'.

\* **Публичная ссылка на Яндекс.Диск** — это ссылка для скачивания/просмотра материалов, которую пользователь выложил в публичный доступ, например 'https://yadi.sk/d/7C6Z9q\_Ds1wXkw' или 'https://disk.yandex.ru/d/7C6Z9q\_Ds1wXkw'.

\* **Идентификатор** — хэш, который указан в url на странице пользователя, например, в сервисе Я.Район: https://local.yandex.ru/users/tr6r2c8ea4tvdt3xmpy5atuwg0/ идентификатор — 'tr6r2c8ea4tvdt3xmpy5atuwg0'.

Плагин Yandex\_parser выдает меньше информации по идентификатор-у пользователя (в сравнении с другими методами), причина — fix уязвимости от Яндекса.

По окончании успешного поиска выводится отчёт в CLI, сохраняется в txt и открывается браузер с персональными страницами пользователя/пользователей в сервисах Яндекс-а.

### Многопользовательский режим

\* **Файл с именами пользователей** — файл (в кодировке UTF-8 с расширением .txt или без него), в котором записаны логины.

Каждый логин в файле должен быть записан с новой строки, например:

```
bobbimonov
username
username2
username3
случайная строка
```

При использовании многопользовательского режима по окончании поиска (быстро) открывается браузер с расширенным отчётом<sup>1</sup>, в котором перечислены:

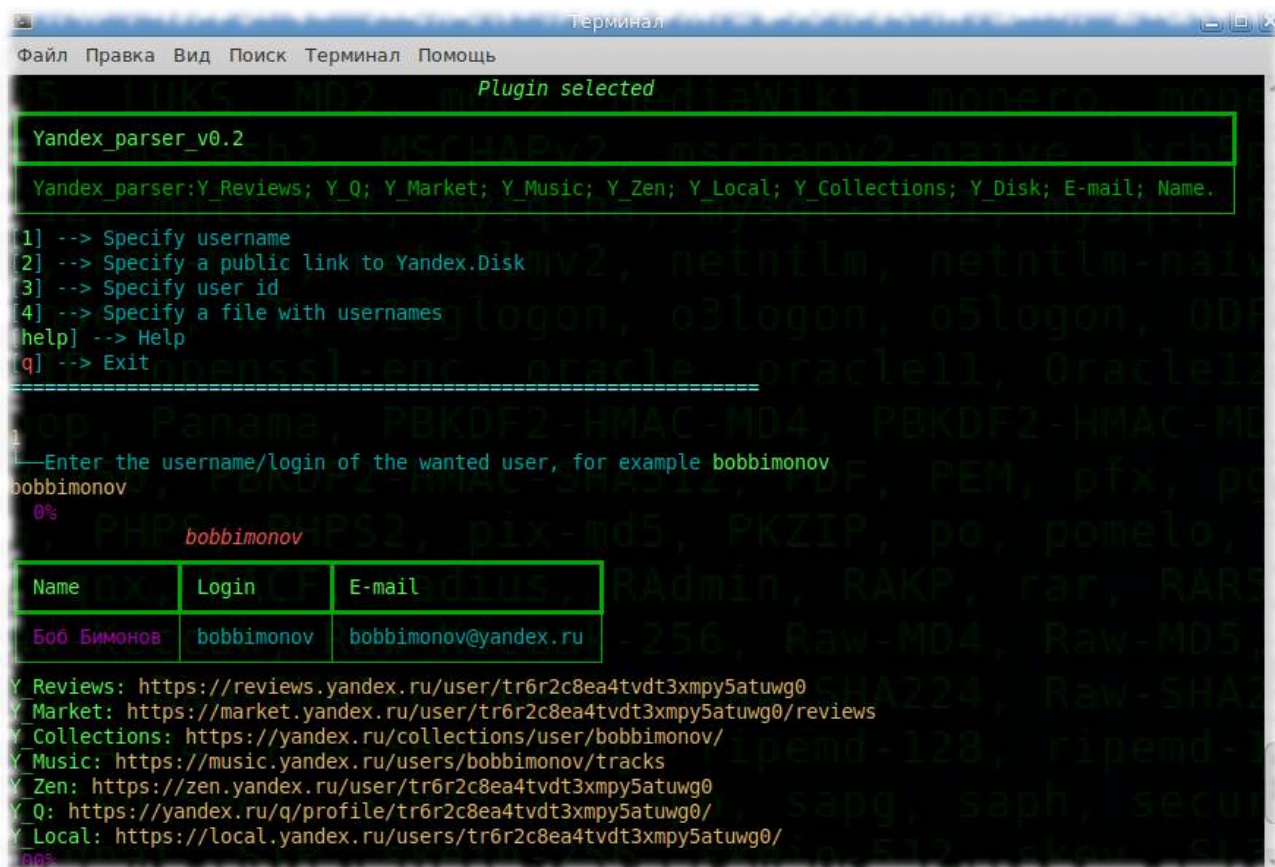


логины пользователей; их имена; e-mail's и их персональные ссылки на сервисы Яндекса.

Плагин генерирует, но не проверяет 'доступность' персональных страниц пользователей по причине: частая защита страниц Я.капчей.

Все результаты сохраняются в '~/snoop/results/Yandex\_parser/\*'

## Отчеты при использовании плагина Yandex\_parser в Snoop Project.



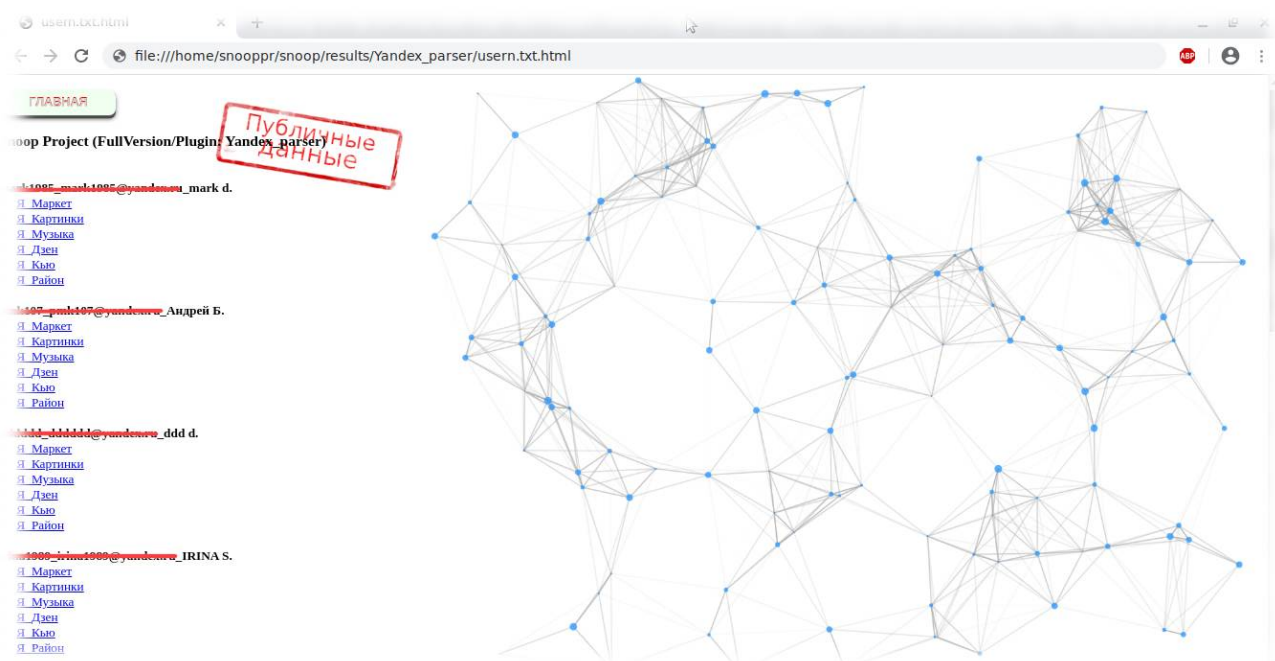
```
Plugin selected
Yandex_parser_v0.2
Yandex_parser:Y_Reviews; Y_Q; Y_Market; Y_Music; Y_Zen; Y_Local; Y_Collections; Y_Disk; E-mail; Name.
[1] --> Specify username
[2] --> Specify a public link to Yandex.Disk
[3] --> Specify user id
[4] --> Specify a file with usernames
[help] --> Help
[q] --> Exit

Enter the username/login of the wanted user, for example bobbimonov
bobbimonov
0%
bobbimonov

Name | Login | E-mail
-----|-----|-----
Бобб Бимонов | bobbimonov | bobbimonov@yandex.ru

Y_Reviews: https://reviews.yandex.ru/user/tr6r2c8ea4tvd3xmpy5atuwg0
Y_Market: https://market.yandex.ru/user/tr6r2c8ea4tvd3xmpy5atuwg0/reviews
Y_Collections: https://yandex.ru/collections/user/bobbimonov/
Y_Music: https://music.yandex.ru/users/bobbimonov/tracks
Y_Zen: https://zen.yandex.ru/user/tr6r2c8ea4tvd3xmpy5atuwg0
Y_Q: https://yandex.ru/q/profile/tr6r2c8ea4tvd3xmpy5atuwg0/
Y_Local: https://local.yandex.ru/users/tr6r2c8ea4tvd3xmpy5atuwg0/
```

Работа плагина в CLI в Snoop Project EN версии (один из примеров).



HTML отчёт по поиску одного десятка пользователей в Яндекс сервисах.

Сохраняется и персональный отчёт в формате «report.txt».



# Получение Snoop Project Full version

Для получения Snoop Full версий (годовая лицензия - 1400 р.) команды:

~\$ snoop.exe --donate у #запуск Snoop build-версии в OS Windows


~\$ snoop -- donate у #запуск Snoop build-версии в OS GNU/Linux

~\$ python3 snoop.py -- donate у #запуск Snoop source-версии из исходного кода на OS GNU/Linux/Termux

~\$ python snoop.py -- donate у #запуск Snoop source-версии из исходного кода на OS Windows

Студенты по направлению ИБ/Криминалистика и органы государственной власти могут получить Snoop Full версии на безвозмездной основе в опытную эксплуатацию (см. *оферту*).

Пример запроса Snoop Full version для федеральных органов исполнительной власти

  
МВД России

УПРАВЛЕНИЕ  
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
по МАГАДАНСКОЙ ОБЛАСТИ  
(УМВД России по Магаданской области)

пр. Карла Маркса, 45, Магадан, 685000  
Тел/факс (4132) 696996  
31 мая 2021 г. № 27/ 1053  
на № \_\_\_\_ от \_\_\_\_ 2021 г.

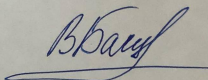
snoopproject@yandex.ru

О направлении запроса

В связи с возникшей служебной необходимостью прошу Вас предоставить Snoop.exe full version for Windows 7/10 (32-64 bit) RU для использования с целью идентификации лиц, причастных к незаконному обороту наркотиков.

Благодарю за сотрудничество.

Оперуполномоченный управления  
по контролю за оборотом наркотиков  
УМВД России по Магаданской области

 В.В. Бачурин

Исп. Бачурин В.В.  
тел.: (4132) 696-996

E-mail (только для госорганов): [snoopproject@yandex.ru](mailto:snoopproject@yandex.ru)

С последней версией документации Snoop Project пользователь может ознакомиться [здесь](#).