

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

**«АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОИСКА СЛЕДОВ
СТЕГАНОГРАФИЧЕСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»**

Воронеж 2021

Содержание

1. Общие положения
2. Технология работы с системой
3. Развертывание системы
4. Получение трасологических данных
5. Учет трасологических данных и поиск следов присутствия

1. Общие положения

Автоматизированная система поиска следов стеганографического программного обеспечения предназначена для повышения эффективности проведения компьютерно-технических экспертиз стеганоаналитической направленности за счет автоматизации и компьютеризации процессов сбора, учета, хранения и поиска следов присутствия стеганографического программного обеспечения на компьютерах или носителях.

В качестве оборудования используется ПК с операционной системой не ниже Windows 10 или Linux с поддержкой контейнеризации.

Для автоматизации развёртывания и оптимизации управления приложениями используется микросервисная архитектура. В состав стека – технологий которой входят docker-образы PHP + Nginx и СУБД MS SQL Server.

Для сбора информации об инсталляционной активности используются портативные приложения для Windows: «Монитор файлов», «Монитор реестра» и для Linux: «Сканер логов».

В системе предполагается использование двух ролей: admin и user, где admin имеет полные права на уровне web-приложения, а user имеет доступ к просмотру учтенного ПО и поиску следов присутствия.

2. Технология работы с системой

Функциональная структура системы представлена тремя блоками:

- блок мониторинга инсталляционной активности (БМИА);
- блок учета и хранения (БУХ);
- блок поиска (БП).

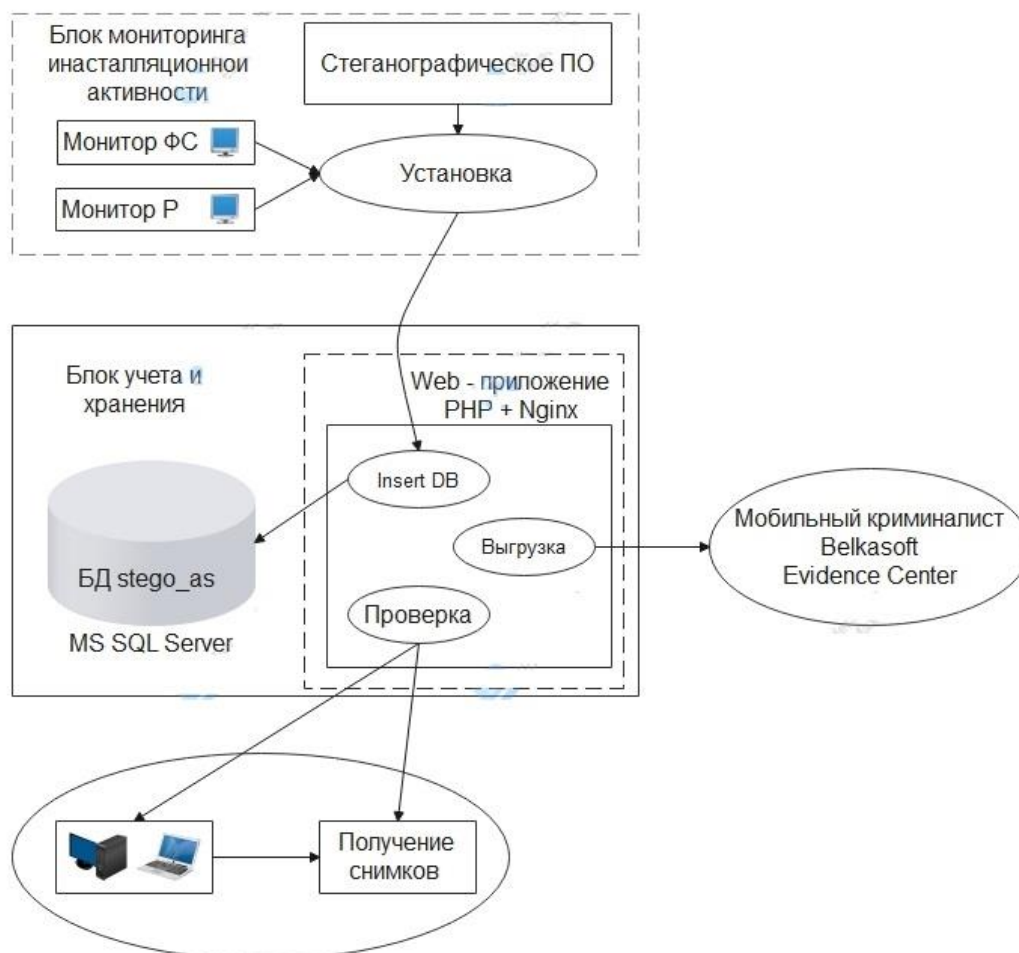


Рис. 2.1. Структурная схема АИС

Объекты в виде инсталляционных пакетов стеганографического ПО поступают на вход блока мониторинга инсталляционной активности (БМИА), который предназначен для получения трасологических данных в виде изменений файловой системы, реестра Windows.

На UNIX-подобных операционных системах, в целях поиска следов присутствия стеганографического программного обеспечения (в том числе удаленного) производится анализ .log файлов программ, предназначенных для установки, обновления и удаления программных пакетов (например, advanced packaging tool, dpkg) присутствующих на всех версиях операционных систем, на наличие записей об установке интересующих программ.

После учета и накопления трасологической и таксономической информации, поступающей из БМИА в БУХ становится возможна работа с БП, который предназначен для подтверждения факта использования

стеганографического программного обеспечения на исследуемых компьютерных системах или носителях и реализован в виде веб-приложения. Поиск следов стеганографических программ по хеш-суммам файлов для Windows и Linux аналогичны, технология представлена на (рис. 2.1).

3. Развертывание системы

Для того чтобы развернуть автоматизированную систему на Windows необходимо скачать и установить из репозитория <https://docs.docker.com/desktop/windows/install/> Docker Desktop для Windows. Для правильной работы Docker должна быть включена виртуализация и установлен пакет WSL. После установки открыть приложение Docker и в открывшемся окне нажимать кнопку Start. Открыть настройки и перейти во вкладку General. С пункта Expose daemon on tcp://localhost:2375 without TLS снять галочку.

Для того чтобы развернуть автоматизированную систему на Linux нужно обновить существующий список пакетов (все команды выполнять в terminal):

```
$ sudo apt update
```

Затем установить несколько необходимых пакетов, которые позволяют apt использовать пакеты через HTTPS:

```
$ sudo apt install apt-transport-https ca-certificates curl software-properties-common
```

Добавить ключ GPG для официального репозитория Docker в систему:

```
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add –
```

Добавить репозиторий Docker в источники APT:

```
$ sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"
```

Потом необходимо обновить базу данных пакетов и добавить в нее пакеты Docker из недавно добавленного репозитория:

```
$ sudo apt update
```

Убедится, что установка будет выполняться из репозитория Docker (рис. 3.1), а не из репозитория Ubuntu по умолчанию:

```
$ apt-cache policy docker-ce
```

Если все правильно, то должны получить следующий вывод, хотя номер версии Docker может отличаться:

```
docker-ce:
  Installed: (none)
  Candidate: 5:19.03.9~3-0~ubuntu-focal
  Version table:
    5:19.03.9~3-0~ubuntu-focal 500
    500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
```

Рис. 3.1. Установка из репозитория Docker

Установить Docker:

```
$ sudo apt install docker-ce
```

Проверить запуск Docker (рис. 3.2):

```
$ sudo systemctl status docker
```

```
Output
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-05-19 17:00:41 UTC; 17s ago
     TriggeredBy: ● docker.socket
        Docs: https://docs.docker.com
    Main PID: 24321 (dockerd)
       Tasks: 8
      Memory: 46.4M
    CGroup: /system.slice/docker.service
            └─24321 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
```

Рис. 3.2. Вывод о запуске Docker

Для обслуживания и мониторинга контейнеров с микросервисами желательно установить средство контейнеризации. Если обслуживание не планируется Portainer можно не устанавливать и следующие пункты пропустить.

Создать хранилище данных для контейнера:

```
$ sudo docker volume create portainer_data
```

Скачать образ Portainer:

```
$ sudo docker pull portainer/portainer:latest
```

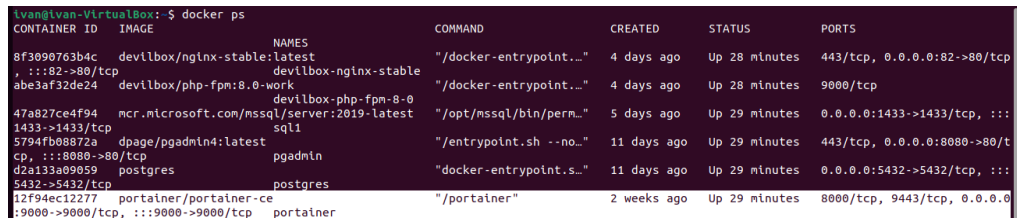
Запустить образ Portainer:

```
$ sudo docker run -d -p 9000:9000 --name=portainer --restart=always -v
/var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data
portainer/portainer
```

Эта команда настраивает автоматический запуск Portainer после перезагрузки, а также постоянное хранилище, чтобы настройки не потерялись при удалении и повторном разворачивании контейнера.

Получить список запущенных контейнеров (рис. 3.3).

\$ sudo docker ps



CONTAINER ID	IMAGE	NAMES	COMMAND	CREATED	STATUS	PORTS
8f3090763b4c	devilbox/nginx-stable:latest	devilbox-nginx-stable	"/docker-entrypoint..."	4 days ago	Up 28 minutes	443/tcp, 0.0.0.0:82->80/tcp
abe3af32de24	devilbox/php-fpm:8.0-work	devilbox-php-fpm-8-0	"/docker-entrypoint..."	4 days ago	Up 28 minutes	9000/tcp
47a827ce4f94	mcr.microsoft.com/mssql/server:2019-latest	mssql	"/opt/mssql/bin/pern..."	5 days ago	Up 29 minutes	0.0.0.0:1433->1433/tcp, ::1433->1433/tcp
5794fb08872a	dpape/pgadmin4:latest	pgadmin	"/entrypoint.sh --no..."	11 days ago	Up 29 minutes	443/tcp, 0.0.0.0:8080->8080/tcp, ::8080->8080/tcp
d2a133a09059	postgres	postgres	"docker-entrypoint.s..."	11 days ago	Up 29 minutes	0.0.0.0:5432->5432/tcp, ::5432->5432/tcp
12f94ec12277	portainer/portainer-ce	portainer	"/portainer"	2 weeks ago	Up 29 minutes	8000/tcp, 9443/tcp, 0.0.0.0:9000->9000/tcp, ::9000->9000/tcp

Рис. 3.3. Список запущенных контейнеров

Получить доступ к программе можно через веб-интерфейс на порту 9000. Открыть его в браузере.

localhost:9000

Ввести имя пользователя и пароль (рис. 3.4):

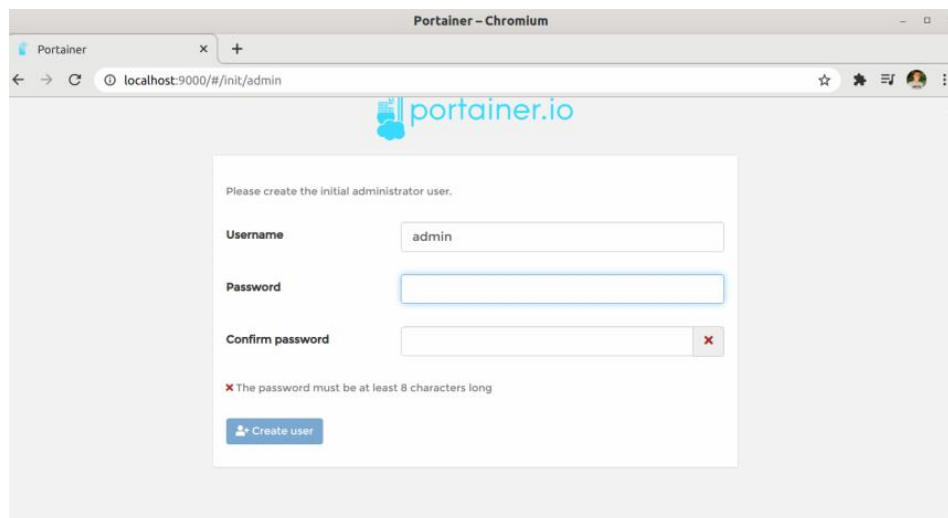


Рис. 3.4. Страница регистрации

Выбрать метод подключения к Docker (рис. 3.5). Для этого выбрать Local:

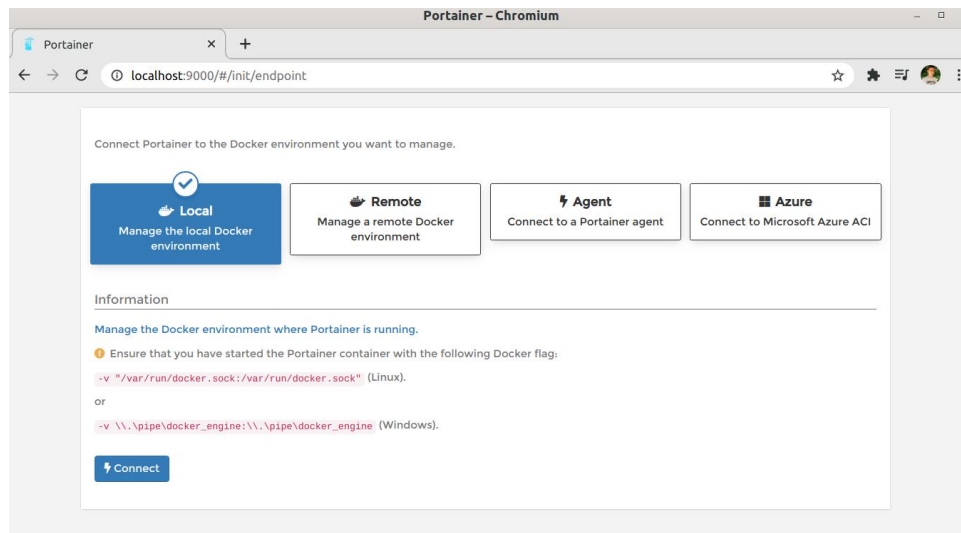


Рис. 3.5. Страница с методами подключения

Осуществить переход в панель управления контейнерами по нажатию Connect (рис. 3.6):

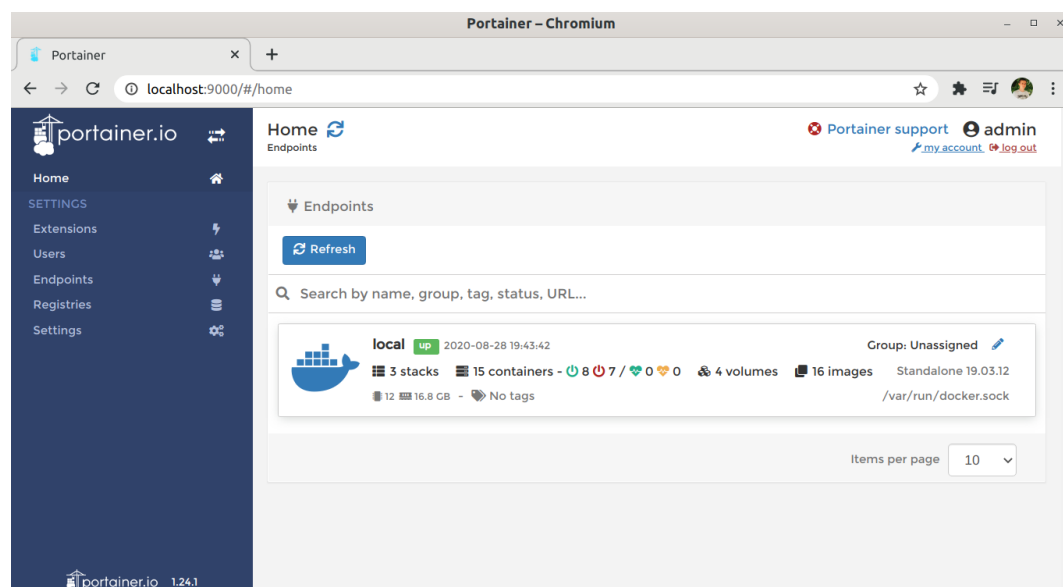


Рис. 3.6. Панель управления

Установить stack состоящий из веб-сервера Nginx, PHP_FPM и СУБД MSSQL SERVER из репозитория <https://github.com/ArturKram/stego>. Скачать каталог config и файл docker-compose.yml. Создать папку docker в папке «Документы» и поместить сюда скаченные файлы. Вызвать командную строку или терминал. Перейти в папку, где располагаются скаченные файлы (рис. 3.7) с помощью команды:

cd C:\docker\ для Windows

cd documents/docker/ для Linux.


```
ivan@ivan-VirtualBox:~$ cd Документы/docker/
ivan@ivan-VirtualBox:~/Документы/docker$
```

Рис. 3.7. Переход в папку docker

Запустить файл docker-compose.yml (рис. 3.8):

docker-compose up

```
ivan@ivan-VirtualBox: ~/Документы/docker
ivan@ivan-VirtualBox:~/Документы/docker$ docker-compose up
WARNING: The Docker Engine you're using is running in swarm mode.

Compose does not use swarm mode to deploy services to multiple nodes in a swarm. All containers will be scheduled on the current node.
To deploy your application across the swarm, use 'docker stack deploy'.

Creating sql_server ... done
Creating php-nginx ... done
Creating php-app ... done
Attaching to php-app, php-nginx, sql_server
php-nginx | /docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
php-nginx | /docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
php-nginx | /docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
php-nginx | 10-listen-on-ipv6-by-default.sh: info: /etc/nginx/conf.d/default.conf is not a file or does not exist
php-nginx | /docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
php-nginx | /docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
php-nginx | /docker-entrypoint.sh: Configuration complete; ready for start up
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: using the "epoll" event method
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: nginx/1.21.4
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: built by gcc 10.3.1 20210424 (Alpine 10.3.1_glt20210424)
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: OS: Linux 5.13.0-21-generic
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: start worker processes
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: start worker process 22
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: start worker process 23
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: start worker process 24
php-nginx | 2021/11/29 13:36:57 [notice] 1#1: start worker process 25
php-app | [29-Nov-2021 13:36:57] NOTICE: fpm is running, pid 1
php-app | [29-Nov-2021 13:36:57] NOTICE: ready to handle connections
sql_server | SQL Server 2019 will run as non-root by default.
sql_server | This container is running as user root.
sql_server | Your master database file is owned by UNKNOWN.
sql_server | To learn more visit https://go.microsoft.com/fwlink/?linkid=2099216.
sql_server | 2021-11-29 13:37:00.14 Server Setup step is FORCE copying system data file 'C:\templatedata\model_replicatedmaster.ldf' to
'/var/opt/mssql/data/model_replicatedmaster.ldf'.
```

Рис. 3.8. Запуск файла docker-compose

Проверить созданные контейнеры через Portainer (рис. 3.9).

<input type="checkbox"/>	Name	State	Quick actions	Stack	Image	Created	IP Address	Published Ports	C
<input type="checkbox"/>	php-app	running		docker	docker_app	2021-11-29 16:36:56	172.21.0.2	-	
<input type="checkbox"/>	php-nginx	running		docker	nginx:alpine	2021-11-29 16:36:56	172.21.0.4	8000:80	
<input type="checkbox"/>	sql_server	running		docker	mcr.microsoft.com/mssql/server:2019-latest	2021-11-29 16:36:56	172.21.0.3	1434:1433	

Рис. 3.9. Список созданных контейнеров

Скачать с указанного выше репозитория каталог www и поместить находящиеся в нем файлы в каталог Документы/docker/www (рис. 3.10).

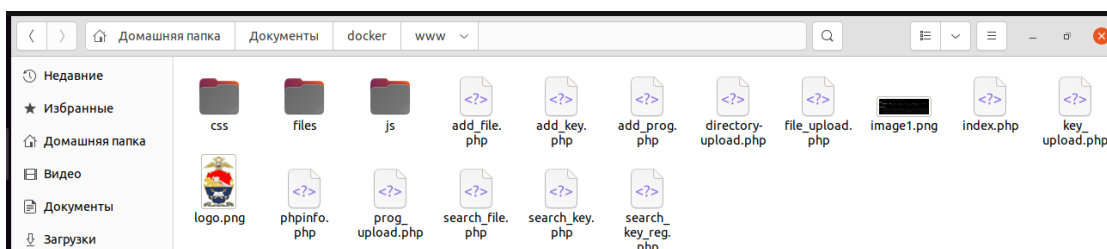


Рис. 3.10. Папка с файлами из репозитория

Запустить сайт введя в адресной строке `https:// «ваш Ip-address»:8000` (рис. 3.11):



Рис. 3.11. Проверка работоспособности сайта

4. Получение трасологических данных

Для получения свввеедений об инсталляционной активности стеганографических программ необходимо использовать прикладное программное обеспечение для Window: «Монитор файлов» и «Монитор реестра», а для Linux: «Сканер логов».

Для того чтобы отследить все файлы при инсталляции приложения необходимо запустить «Мониторинг файловой системы», выбрать раздел, на который будет осуществляться установка стеганографического ПО и нажать

кнопку «Включить мониторинг». Предполагаемые интерфейсы приведены на (рис. 4.1).

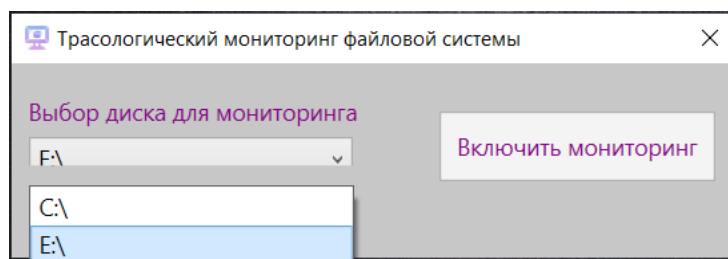


Рис. 4.1. Мониторинг файловой системы

Затем необходимо начать установку стеганографической программы на выбранный раздел, результат будет отображен в логе монитора файловой системы (рис. 4.2).

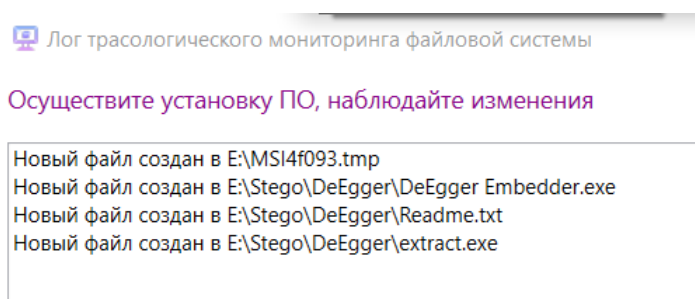


Рис. 4.2. Лог монитора файловой системы

Для получения снимков реестра необходимо использовать приложение «Мониторинг реестра» (рис. 4.3).

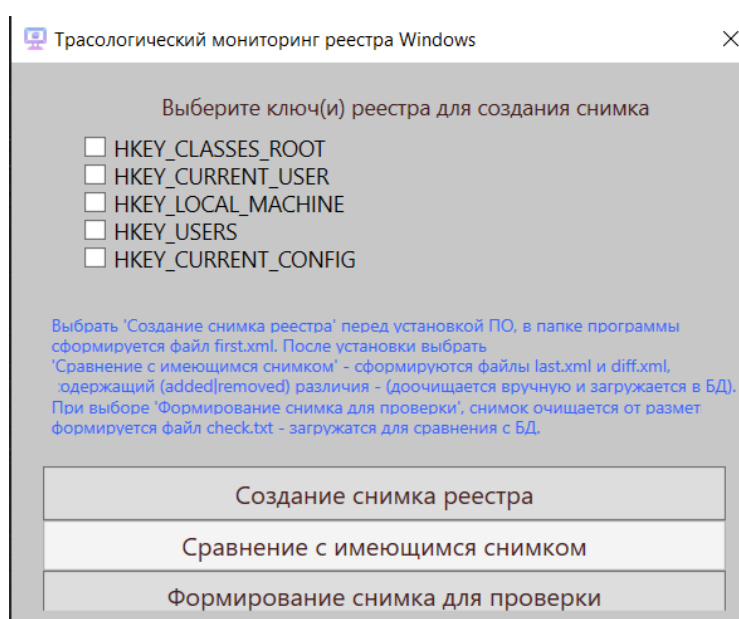


Рис. 4.3. Мониторинг реестра

Пользователь выбирает ключи реестра, снимки которых необходимо получить. Для создания первоначального снимка реестра необходимо выбрать необходимый ключ(и) реестра и нажать на кнопку «Создание снимка реестра». После этого, в папке с программой сформируется файл «first.xml» (рис. 4.4) – исходный снимок реестра.

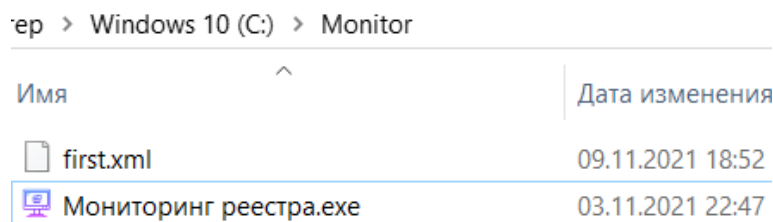


Рис. 4.4. Снимок до инсталляции ПО

После получения исходного снимка начать инсталляцию стеганографического ПО. После завершения установки выбрать раздел «Сравнение с имеющимся снимком» в результате выполнения, которого сформируются файлы last.xml (текущий снимок) и diff.xml (различия ключей реестра до и после установки).

Следующим шагом будет «Формирование списка для проверки» в результате чего снимок очищается от разметки и формируется файл check.txt, содержимое которого будет загружен в БД для сравнения.

Для работы с log-файлами в UNIX-подобных операционных системах, применяется скрипт, написанный на языке Python, определяющий записи, создаваемые при установке стеганографического программного обеспечения.

Лог файлы history.log и dpkg.log расположенные в директории /var/log/, обрабатываются скриптом, сканер логов, который определяет строки где содержится информация об установке либо удалении стеганографического программного обеспечения, которые и являются информацией, вносимой в БД.

Консольное приложение «Сканера логов» для Windows 10, представленное в виде python скрипта в удобную директорию на компьютере (рис. 4.6):

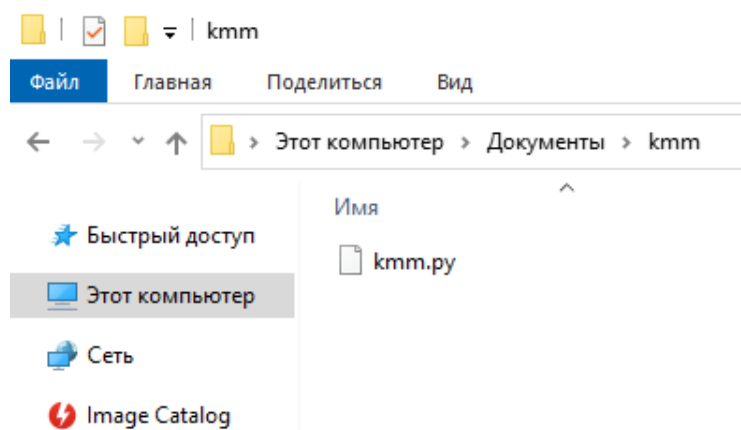


Рис. 4.6. Директория со скриптом

Подключите либо внесите на жесткий диск, лог-файлы с проверяемого компьютера (рис. 4.7):

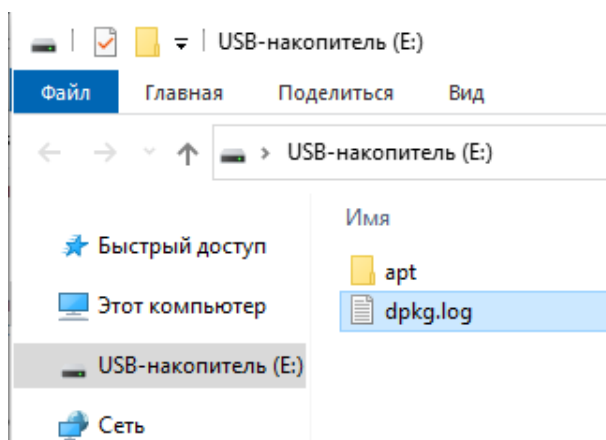


Рис. 4.7. Директория с log-файлами

Запустите среду Python и выполните скрипт (рис. 4.8):

```
python C:\*ПУТЬ К ФАЙЛУ СКРИПТА*\kmm.py
```

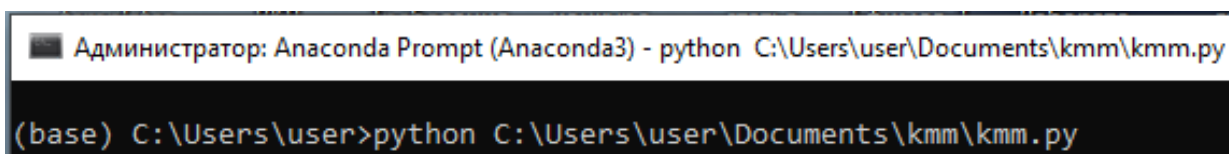


Рис. 4.8. Выполнение команды (на примере Anaconda Prompt)

Далее необходимо действовать согласно командам, которые предлагает скрипт программы:

Произвести выбор проверяемого log-файла (рис. 4.9):

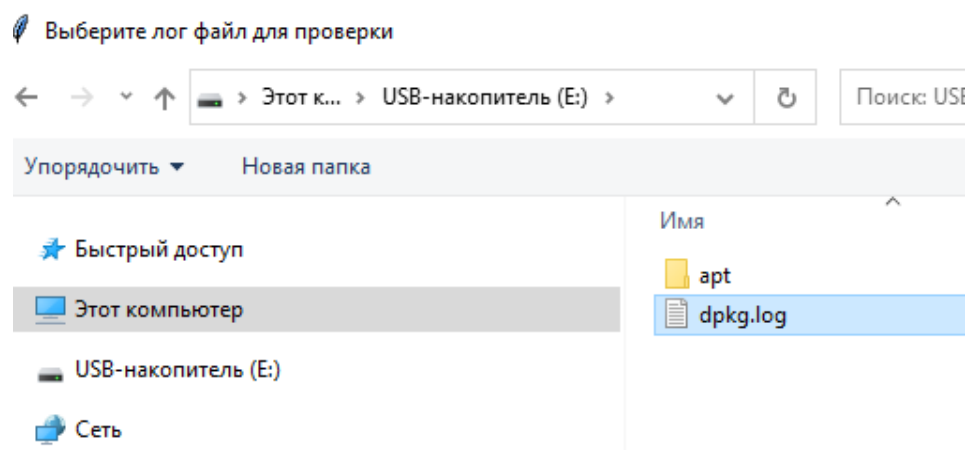
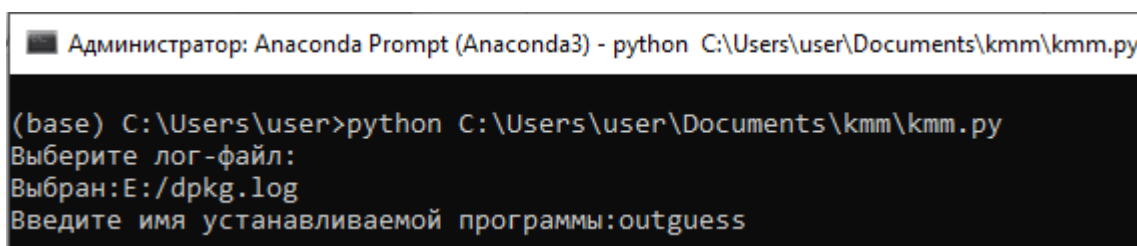


Рис. 4.9. Выбор log-файла для проверки

После чего выполняется возврат к консоли. Проверить, что выбран именно тот файл, произвести ввод названия программы, отслеживаемой при установке, т.е. имя программы, которое применяли при установке ее на Unix-подобную систему, что позволит отследить точные имена устанавливаемых

библиотек, а также зависимостей, которые могут быть вторичными признаками присутствия стеганографического ПО (рис. 4.10):



```
Администратор: Anaconda Prompt (Anaconda3) - python C:\Users\user\Documents\kmm\kmm.py  
  
(base) C:\Users\user>python C:\Users\user\Documents\kmm\kmm.py  
Выберите лог-файл:  
Выбран: E:/dpkg.log  
Введите имя устанавливаемой программы: outguess
```

Рис. 4.10. Ввод имени устанавливаемой программы

Далее согласно командам, осуществляется переход к сохранению результата (рис. 4.11).

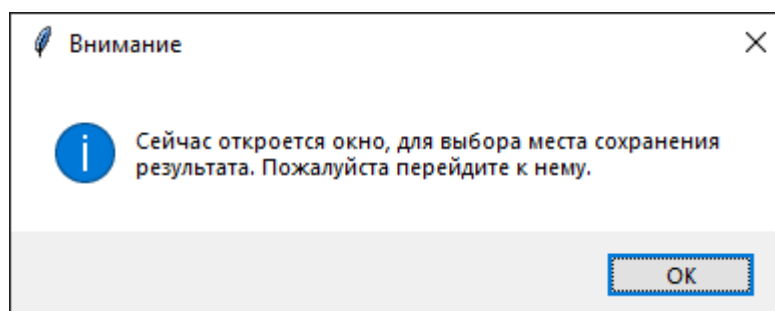


Рис. 4.11. Сообщение о необходимости перехода к сохранению файла

Затем необходимо выбрать путь для сохранения файла и указать имя (рис. 4.12).

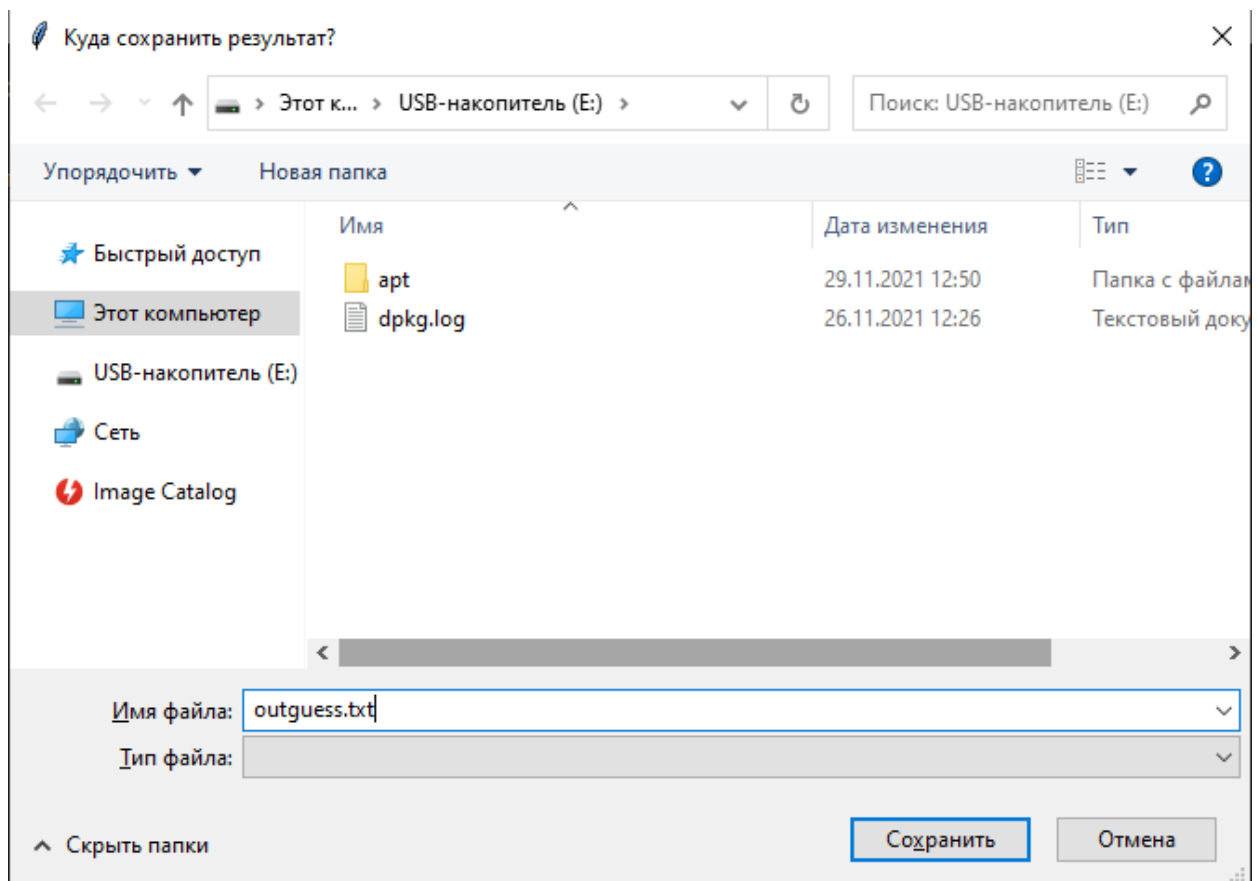


Рис. 4.12. Сообщение о необходимости перехода к сохранению файла

В результате сохранения в консоли будет выведено сообщение об успешном сохранении файла, а именно путь и кодировка итогового файла (рис. 4.13).

```

Администратор: Anaconda Prompt (Anaconda3)

(base) C:\Users\user>python C:\Users\user\Documents\kmm\kmm.py
Выберите лог-файл:
Выбран:E:/dpkg.log
Введите имя устанавливаемой программы:outguess
Файл проверен, результат сохранен в: <_io.TextIOWrapper name='E:/outguess.txt' mode='w+' encoding='cp1251'>

```

Рис. 4.13. Вывод результата в консоли

По итогам будет получен файл со всеми следами, которые оставляет стеганографическое ПО при установке в систему (рис. 4.14).

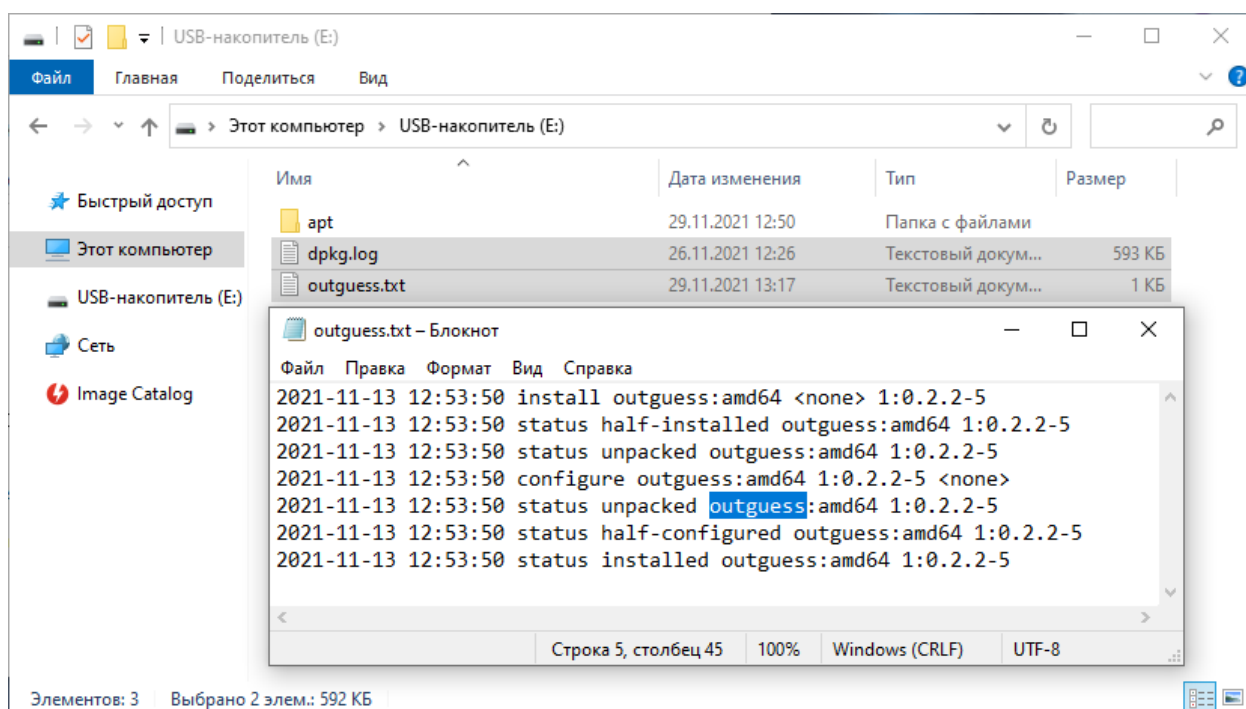


Рис. 4.14. Полученный результат при сканировании log-файлов

При использовании Unix – подобных систем необходимо поместить файл скрипта в удобную директорию на компьютере (рис. 4.15).

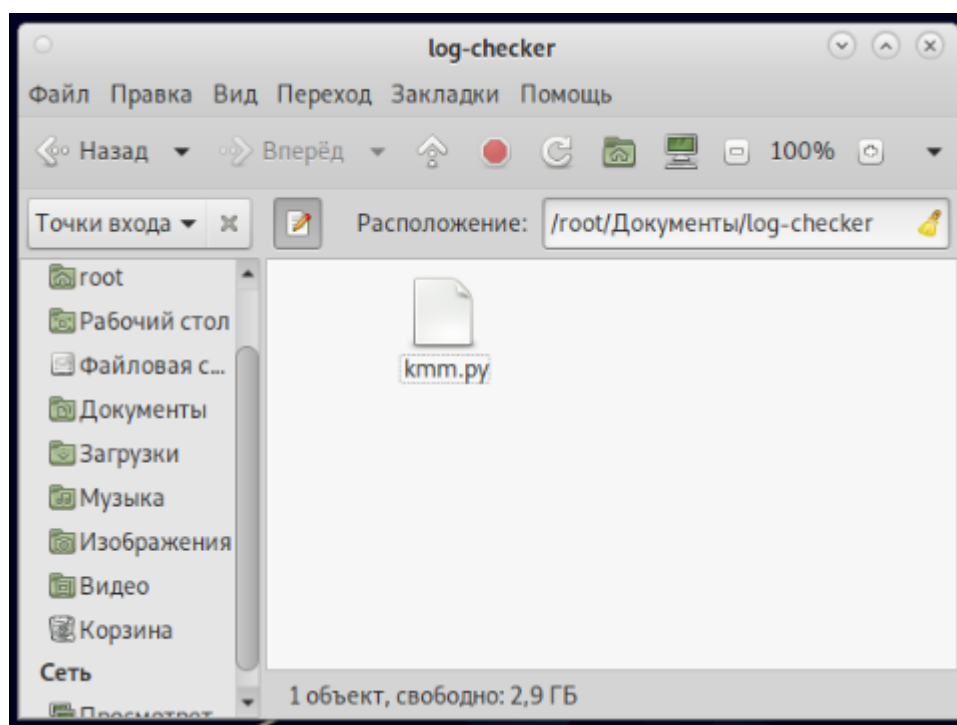


Рис. 4.15. Директория со скриптом

Подключите либо внесите на жесткий диск, лог-файлы с проверяемого компьютера (рис. 4.16):

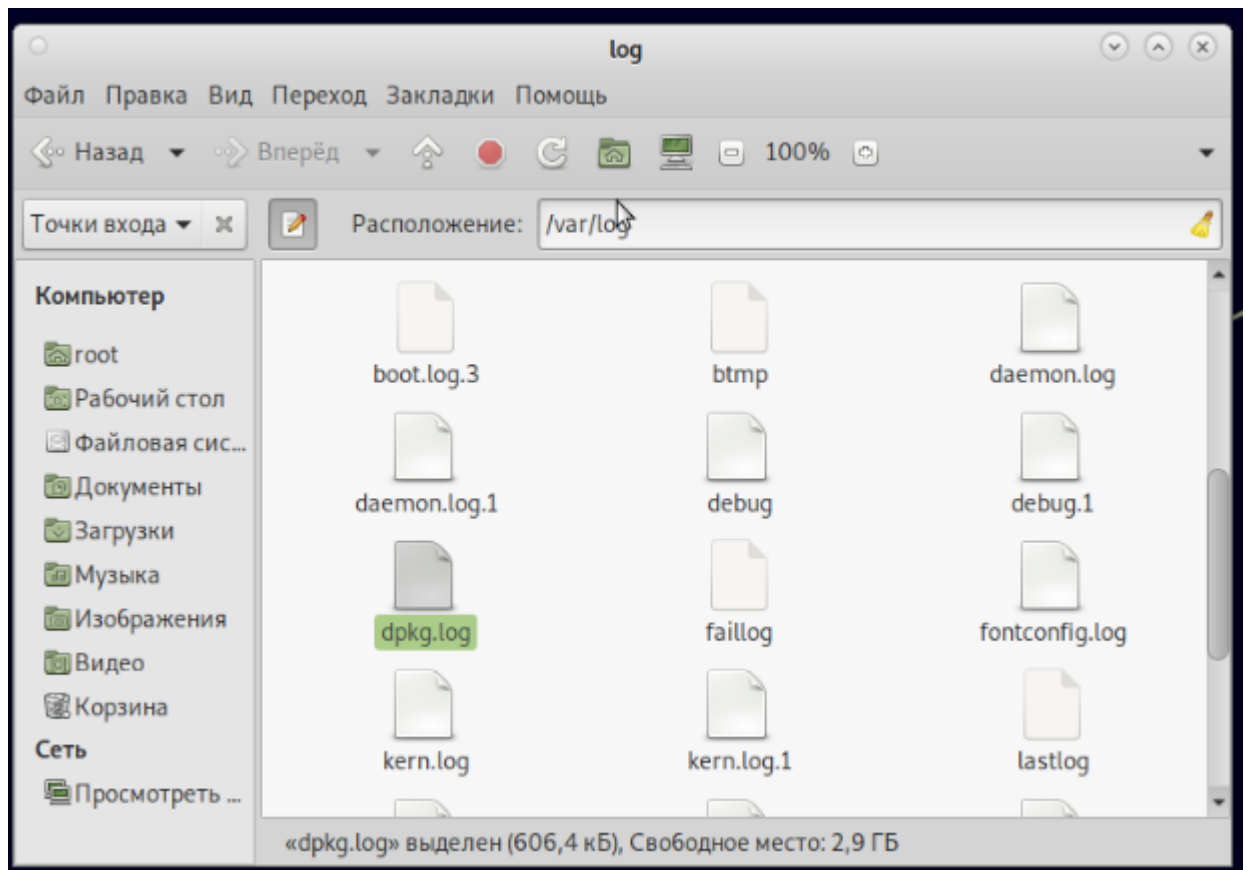


Рис. 4.16. Директория с log-файлами

Запустите среду Python и выполните скрипт (рис. 4.17):
`python kmm.py`

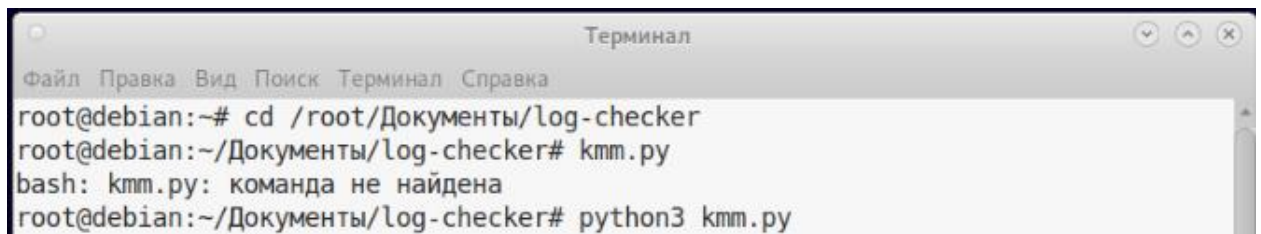


Рис. 4.17. Выполнение команды (на примере Терминала)

Далее необходимо действовать согласно командам, которые предлагает скрипт программы:

1) Произвести выбор проверяемого log-файла (рис. 4.18):

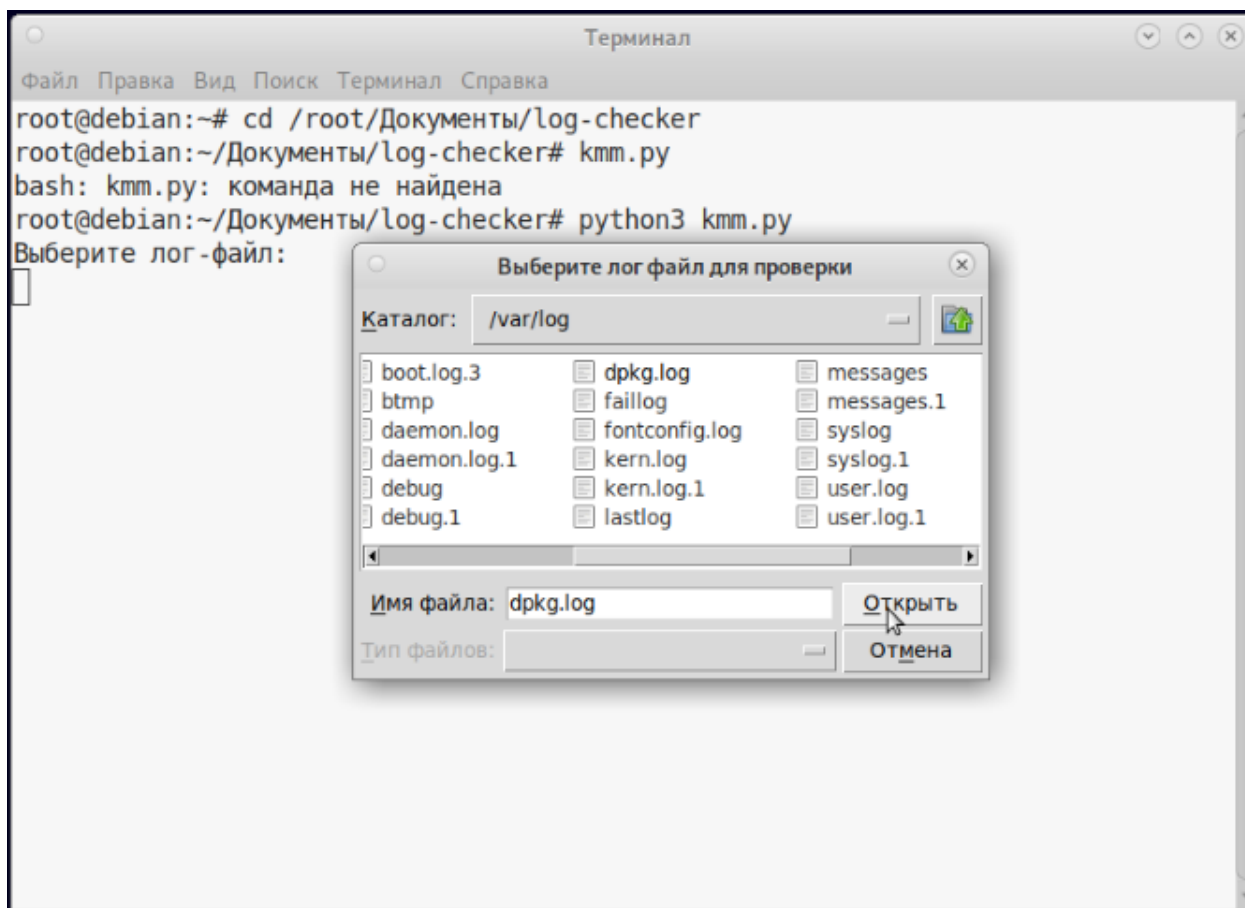


Рис. 4.18. Выбор log-файла для проверки

После чего выполняется возврат к консоли. Проверить, что выбран именно тот файл, произвести ввод названия программы, отслеживаемой при установке, т.е. имя программы, которое применяли при установке ее на Unix-подобную систему, что позволит отследить точные имена устанавливаемых библиотек, а также зависимостей, которые могут быть вторичными признаками присутствия стеганографического ПО (рис. 4.19):

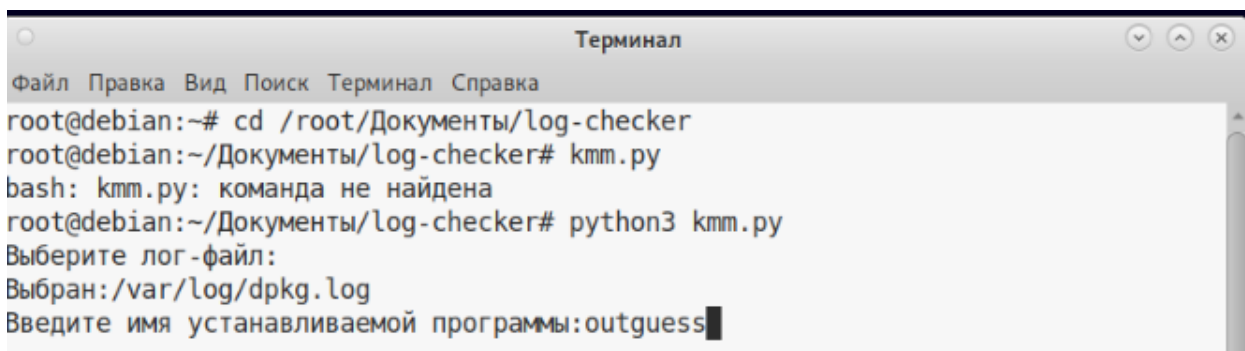


Рис. 4.19. Ввод имени устанавливаемой программы

Далее согласно командам, осуществляется переход к сохранению результата (рис. 4.20).

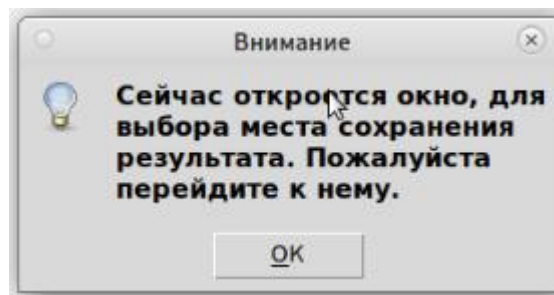


Рис. 4.20. Сообщение о необходимости перехода к сохранению файла

Затем необходимо выбрать путь для сохранения файла и указать имя (рис. 4.21).

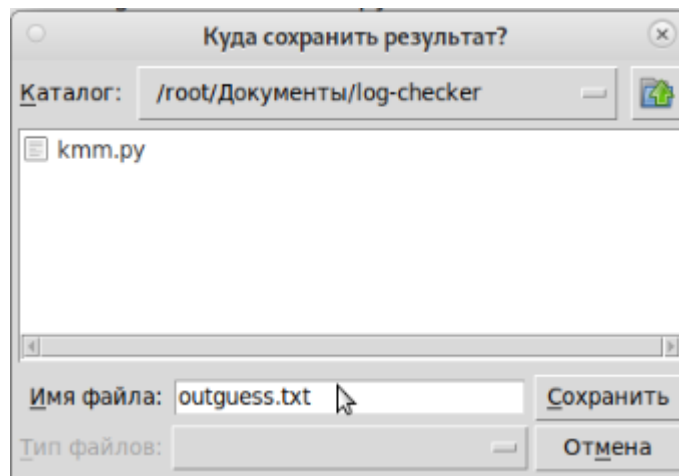


Рис. 4.21. Сообщение о необходимости перехода к сохранению файла

В результате сохранения в консоли будет выведено сообщение об успешном сохранении файла, а именно путь и кодировка итогового файла (рис. 4.22).

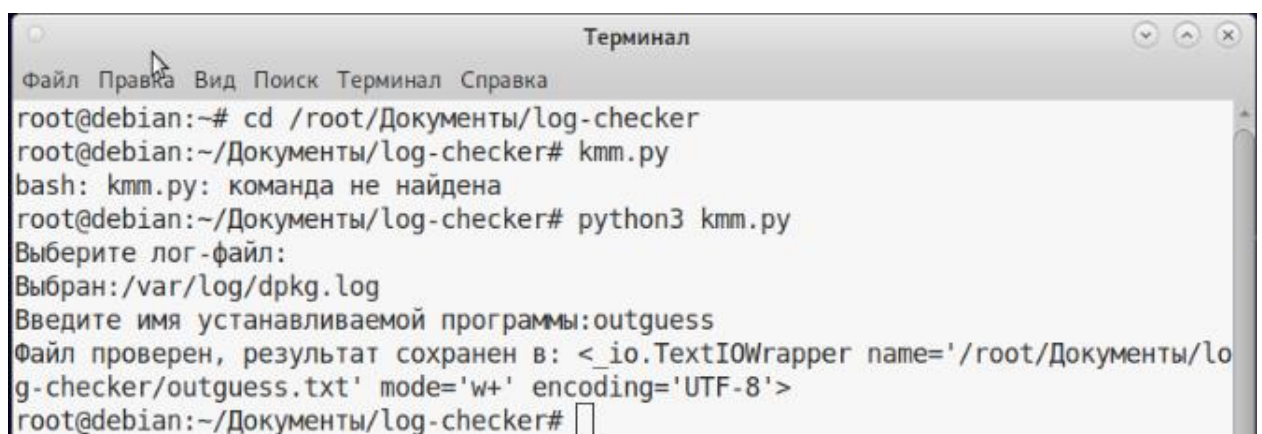


Рис. 4.22. Вывод результата в консоли

По итогам будет получен файл со всеми следами, которые оставляет стеганографическое ПО при установке в систему (рис. 4.23).

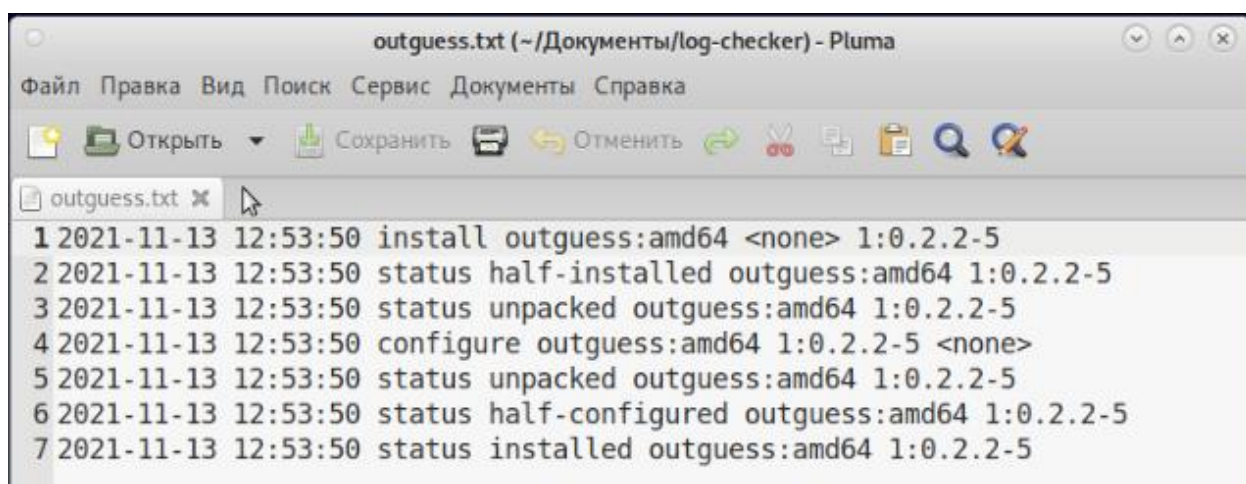


Рис. 4.23. Полученный результат при сканировании log-файлов

Полученные в результате сканирования данные, а именно имена основных программ пакетов, а также наиболее характерные зависимые библиотеки, которые устанавливаются к стеганографическому приложению дополнительно, администратору необходимо добавить в базу данных.

5. Учет трасологических данных

Web – приложение необходимо для взаимодействия с пользователем, передачи информации в базу данных и выгрузки архивов, содержащих информацию об инсталляционной активности стеганографических программ для дальнейшего импорта в приложения по поиску следов присутствия («Мобильный криминалист», «Evidence Center», etc.).

Для начала работы с системой необходимо авторизоваться (рис. 5.1). Для разграничения прав пользователей, используются две роли: администратор и пользователь.

ПОИСК СЛЕДОВ ПРИСУТСТВИЯ СТЕГАНОГРАФИЧЕСКОГО ПО

Главная Поиск следов Наша команда Контакты

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ
Кафедра автоматизированных информационных систем ОВД

АВТОРИЗАЦИЯ:

Логин:

Пароль:

ВХОД

Наша команда

 Солодуха Роман Александрович Руководитель проекта	 Кромских Артур Геннадьевич Капитан
 Романова Виктория Романовна Тестировщик	 Сумбулов Иван Сергеевич Разработчик
 Ефимов Алексей Олегович Проектировщик	 Скачкова Ульяна Олеговна Дизайнер

Рис. 5.1. Окно авторизации

После ввода пользователем своих учетных данных и нажатии на кнопку «Вход», происходит переход на главную страницу (рис. 5.2), которая состоит из следующих модулей:

1. Работа со стеганопрграммами, который позволяет:
 - Добавить стеганопрограмму;
 - Редактировать стегнопрограмму;
2. Стеганографические программы:
 - Список учтенных стеганографических программ;
 - Выгрузка в Excel;
3. Идентификация стеганопрограмм, с помощью которого можно:
 - Добавить файл;
 - Добавить папку с файлами;
 - Добавить ключи реестра;
4. Поиск следов присутствия:
 - Добавление поискового дела;
 - Поисковое дело (добавление объектов поиска);
 - Поиск объектов (в рамках конкретного дела).



Рис. 5.2. Главная страница

Модуль «Работа со стеганопрограммами» (рис. 5.3) позволяет добавлять таксономическую информацию о стеганографическом ПО в базу и вносить изменения при необходимости.

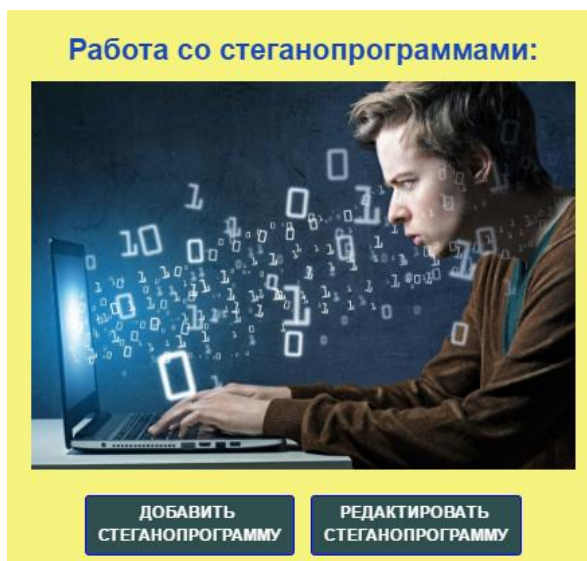


Рис. 5.3. Работа со стеганопрограммами

При нажатии на кнопку «Добавить стеганопрограмму», будет открыта следующая страница, на которой необходимо указать данные добавляемой стеганопрограммы, а именно: «Название стеганопрограммы», «Вид стеганографии», «Типы контейнеров», «Алгоритм стегановложения», «Год создания программы», «Автор», «Алгоритмы шифрования», «Система», «Требуется установка». Типовой алгоритм добавления данных в базу представлен ниже (рис. 5.4).

ДОБАВИТЬ СТЕГАНОПРОГРАММУ:

Название стеганопрограммы	<input type="text" value="Secret_iso"/>
Вид стеганографии	<input type="text" value="DIGITAL"/>
Типы контейнеров	<input type="text" value="JPEG"/>
Алгоритм стегановложения	<input type="text" value="LSB"/>
Год создания программы	<input type="text" value="2015"/>
Автор	<input type="text" value="Lexa Robot"/>
Алгоритмы шифрования	<input type="text" value="BlowFish"/>
Система	<input type="text" value="Linux"/>
<input checked="" type="checkbox"/> Требуется установка	

ДОБАВИТЬ СТЕГАНОПРОГРАММУ

Рис. 5.4. Добавление таксономической информации о стеганопрограмме

Отправляемые в базу данные, обрабатываются php-скриптом, после чего на экране появляется сообщение об успешном добавлении (рис. 5.5):

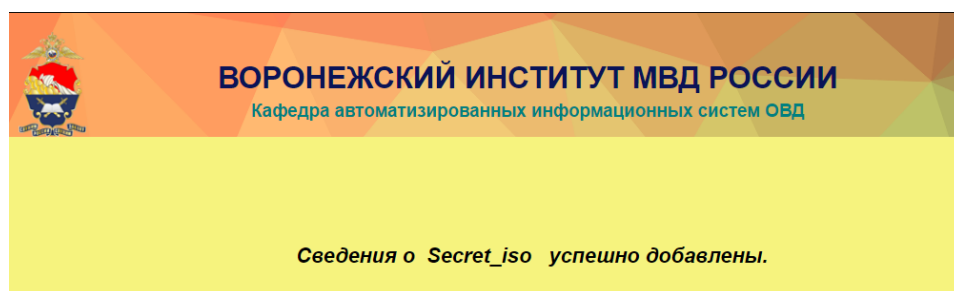


Рис. 5.5. Сообщение о добавлении

Модуль «Стеганографические программы» (рис. 5.6) предоставляет возможность просмотра списка учтенных стеганографических программ, а также реализует выгрузку данных с вычисленными хеш-значениями (MD5, SHA1, SHA256) в формате excel для импорта в системы цифровой криминалистики.



Рис. 5.6. Стеганографические программы

При нажатии на кнопку «Список учтенных стеганографических программ», на экран выводится список программ, информация о которых уже внесена в базу данных (рис. 5.7).

СПИСОК УЧТЕННЫХ СТЕГАНОГРАФИЧЕСКИХ ПРОГРАММ:

Номер	Программа	Портабельность	Расширения	Алгоритм	Автор	Год	Шифрование
1	Xio Steganography	с установкой	BMP	RC2, DES, RC4, Triple DES, Triple DES 112		2005	
2	winhip21	портабельная	BMP	Blowfish, Rijndael		2010	
3	WBStego 4	портабельная	JPG, PNG	Blowfish, Twofish,		1999	
4	Secret_iso	с установкой	JPEG	LSB		2015	BlowFish
5	Ultima Steganography	портабельная	PNG, BMP	RC2, DES, RC4		2013	

Рис. 5.7. Список учтенных программ

Для выгрузки данных из базы в файл формата excel необходимо нажать на кнопку «Выгрузка в EXCEL» и выбрать с какими хеш-значениями это сделать (рис. 5.8).

ВЫГРУЗКА В EXCEL:

☒ md5
 ☒ sha1
 ☐ sha256

Выгрузить в excel

Рис. 5.8. Выгрузка в EXCEL

По завершению выгрузки на экран будет выведено сообщение (рис. 5.9).

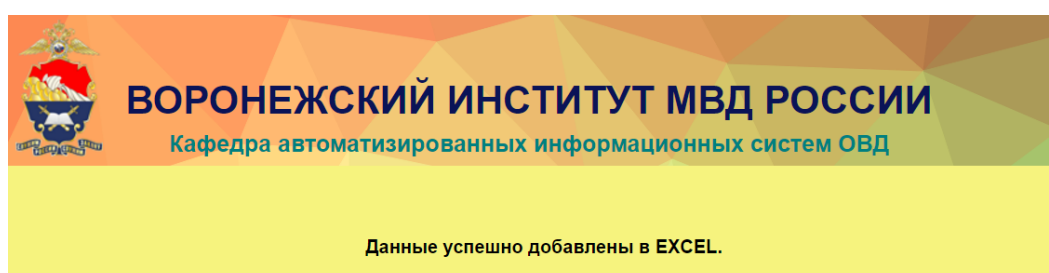


Рис. 5.9. Результат выгрузки

Модуль «Идентификация стеганопрограмм» включает в себя функциональные возможности по добавлению папок с файлами программы, файлов и ключей реестра и лог-файлов (рис. 5.10).



Рис. 5.10. Идентификация стеганопрограмм

При нажатии на кнопку «Добавить файл» открывается страница (рис. 5.11), на которой необходимо выбрать из предложенного списка название стеганопрограммы, затем выбрать файлы относящиеся к этому ПО и нажать кнопку «Добавить хэш», после чего будут вычислены хеш-значения файлов (MD5, SHA1, SHA256).

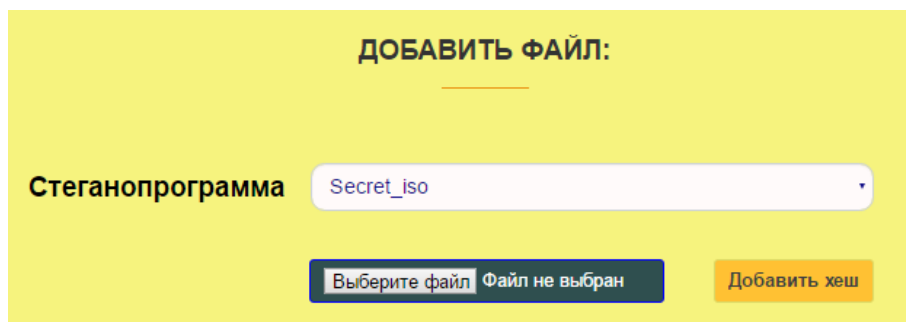


Рис. 5.11. Добавление файла для хеширования

Аналогичным образом происходит добавление папок с файлами и снимков ключей реестра, полученных с помощью программы «Монитор реестра».

Модуль «Поиск следов присутствия» (рис. 5.12) реализует поиск следов присутствия стеганографического ПО в файловых системах и массивах файлов в соответствии с разработанным алгоритмом.



Рис. 5.12. Поиск следов присутствия

Первый шаг: создание поискового дела (рис. 5.13), где необходимо ввести имя проверки и нажать кнопку «Добавить проверку».

The image shows a form with a yellow background. At the top, the text 'СОЗДАНИЕ ПОИСКОВОГО ДЕЛА' is centered. Below it is a horizontal line. Underneath the line is a text input field containing the text 'control_check_1'. To the right of the input field is a dark blue button with white text that says 'Добавить проверку'.

Рис. 5.13. Создание поискового дела

Второй шаг: добавление объектов поиска (рис. 5.14), где необходимо выбрать из предложенного списка название проверки, после чего выбрать папку для добавления файлов в базу и нажать кнопку «Добавить файлы».

The image shows a form with a yellow background. At the top, the text 'ПОИСКОВОЕ ДЕЛО (выбор объектов поиска):' is centered. Below it is a horizontal line. Underneath the line is the text 'ДОБАВЛЕНИЕ ФАЙЛОВ'. Below this text is a dropdown menu showing 'control_check_2'. Below the dropdown menu is a dark blue button with white text that says 'Выберите файл'. To the right of this button is a dark blue box with white text that says 'Число файлов: 10'. At the bottom of the form is a dark blue button with white text that says 'Добавить файлы'.

Рис. 5.14. Добавление файлов

При успешном добавлении на экран будет выведено сообщение (рис. 5.15).

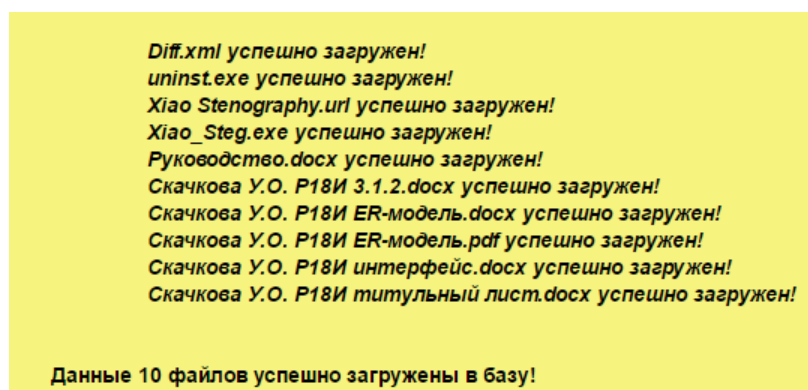


Рис. 5.15. Результат добавления

Третий шаг: добавление снимков реестра (рис. 5.16), для чего необходимо выбрать существующую проверку из списка и выбрать загружаемый файл, после чего нажать кнопку «Добавить».

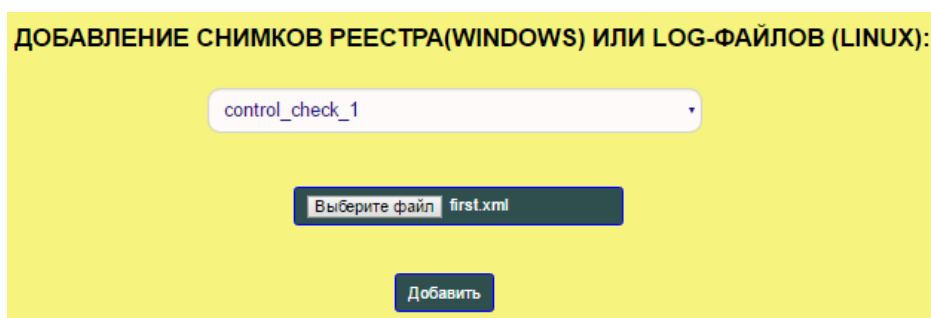


Рис. 5.16. Добавление снимка реестра

В случае успешного добавления на экран будет выведено сообщение (рис. 5.17).

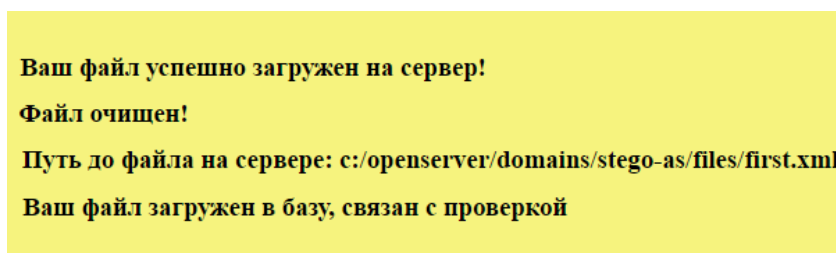


Рис. 5.17. Результат добавления снимка реестра

При работе с UNIX-подобными операционными системами, осуществляется загрузка log-файлов системы в приложение, в которых с помощью полнотекстового поиска производится поиск следов учтенного стеганографического программного обеспечения, аналогично поиску по снимку реестра.

Четвертый шаг: поиск следов присутствия, в рамках которого осуществляется выбор существующей проверки, включающей соответствующие файлы и снимки реестра и их дальнейшее сравнение с информацией, учтенной в базе данных (рис. 5.18).

ПОИСК ОБЪЕКТОВ
(в рамках конкретного дела):

ВЫБЕРИТЕ ПРОВЕРКУ

control_check_2

Поиск по базе

Рис. 5.17. Поиск следов

При успешном поиске объектов в базе данных результат отобразится в виде таблицы (рис. 5.18).

Проверка		Стеганопрограмма	Ключ в реестре	
control_check_2		OpenStego 0.7.1	OpenStego	
Нажали кнопку поиск.				
Проверка	Данные проверки	Данные базы	Программа	Хэш-сумма
control_check_2	uninst.exe application/x-msdownload 64356	uninst.exe application/x-msdownload 64356	Xio Steganography	003680196ca7c14a5b4c960be56d7fa1
control_check_2	Xiao Stenography.url application/octet-stream 49	Xiao Stenography.url application/octet-stream 49	Xio Steganography	57edf24fc58715ca4931eb19d8f1df52
control_check_2	Xiao_Steg.exe application/x-msdownload 348160	Xiao_Steg.exe application/x-msdownload 348160	Xio Steganography	e72aefbb78d42ad3792b782d45bd8011
По проверке control_check_2 обнаружены объекты в количестве 4.				

Рис. 5.18. Результат поиска объектов