Университет ИТМО
Факультет программной инженерии и компьютерной техники

Лабораторная работа №3
по дисциплине «Информационная безопасность»
Вариант 6

Выполнил:Ларочкин Г.И
Группа: P3400
Преподаватель: Маркина Т.А.

Санкт-Петербург
2021 г.

Оглавление

Цель

Изучить объекты реестра, ознакомиться с основными принципами управления доступом к объектам реестра. Изучить основные способы настройки доступа к реестру.

Постановка задачи

1. Какие конкретно ветки и ключи доступны
    a) Пользователю хотя бы на чтение
    b) только Администратору
    c) только System.

2. Опишите в отчете способ резервного копирования реестра

3. Укажите ключ, который отвечает за указанный параметр системы
    a. Задание классического вида панели управления
    b. Отображение пароля к сетевым ресурсам
    c. Автоматическое завершение всех приложений при выключении компьютера.

4. Настройте на аудит какую-либо ветку реестра и проследите появление событий (минимум 5 подразделов)

5. Приведите примеры аналогов Regedit. Приведите плюсы и минусы по сравнению с Regedit (минимум 3)

Программные и аппаратные средства

- Oracle VM VirtualBox 6.1
- Microsoft Windows 10 Pro
- 3GB RAM, 64GB Постоянной памяти
- Intel Core i5-6200U, Nvidia GeForce 940MX

Основная часть

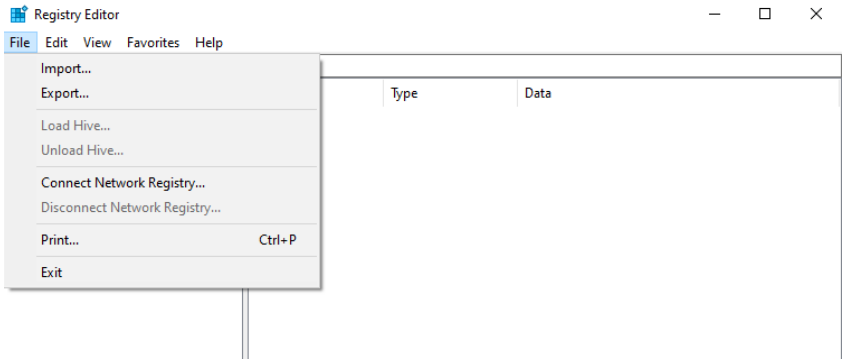
1. Права веток и ключей

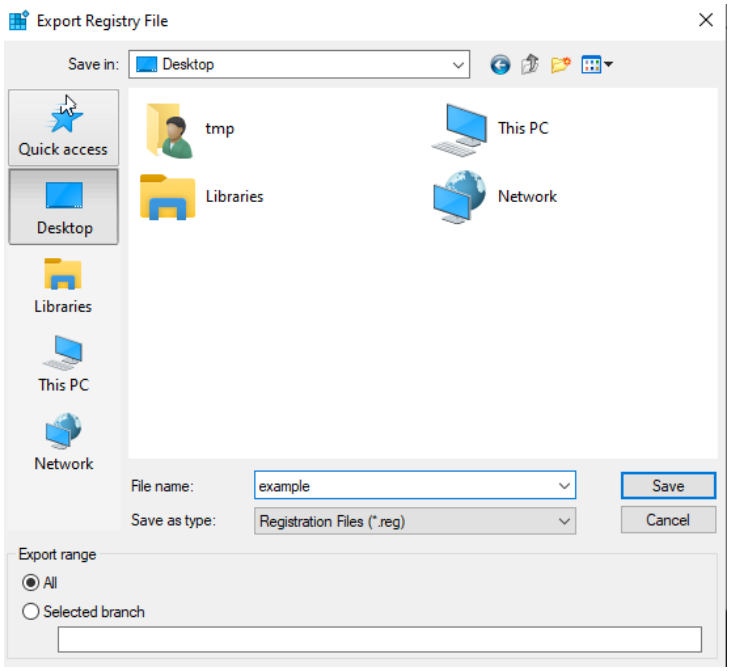
Для пользователя доступно на чтение:
HKEY_CLASSES_ROOT**
HKEY_CURRENT_USER**
HKEY_USERS**

Только для администратора не доступно ничего
Только для System
HKEY_LOCAL_MACHINE\SAM
HKEY_LOCAL_MACHINE\SECURITY

2. Резервное копирование реестра

1. Открываем regedit.msc
2. File -> Export
3. Выбираем путь и имя файла .reg
4. Ожидаем завершения (regedit может показать Not response в это время)

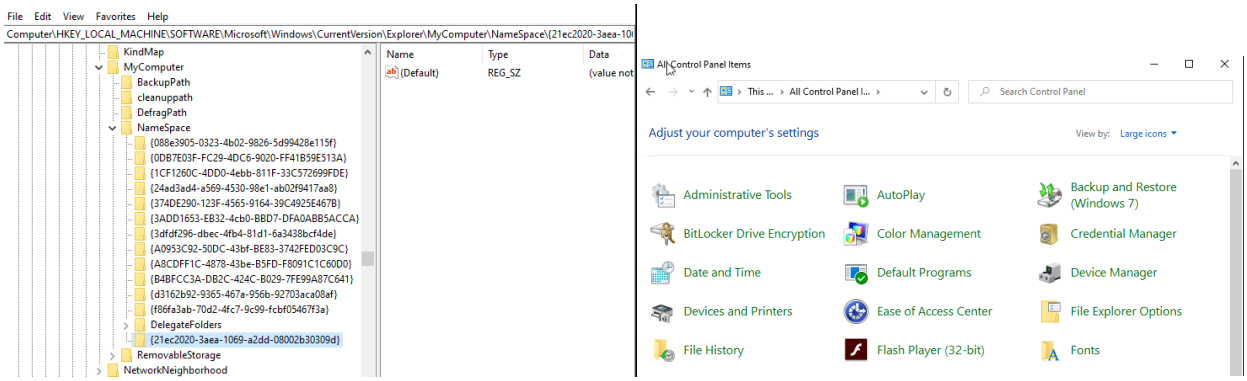




3. Ключи реестра с различным параметром системы

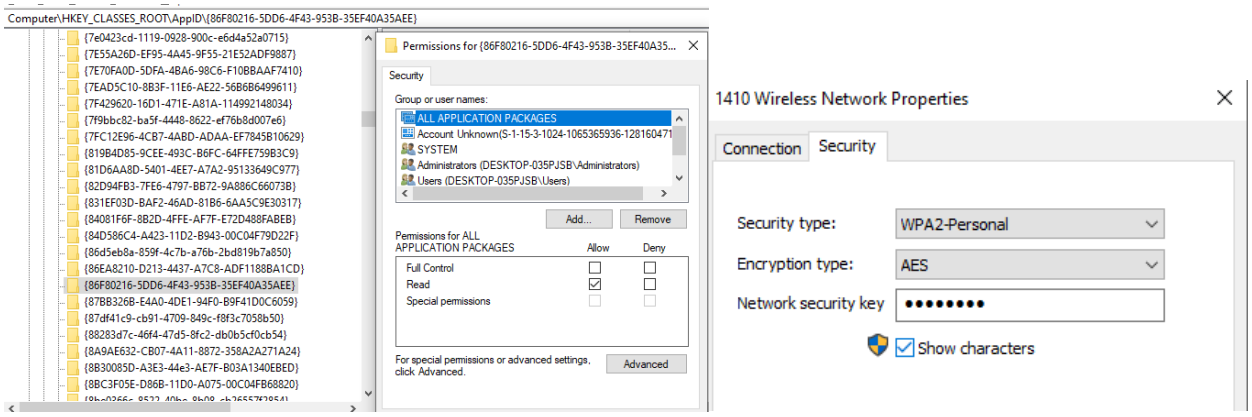
Классическая панель управления

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MyComputer\NameSpace
2. Добавляем ключ *{21ec2020-3aea-1069-a2dd-08002b30309d}* для добавления классической панели с большими иконками

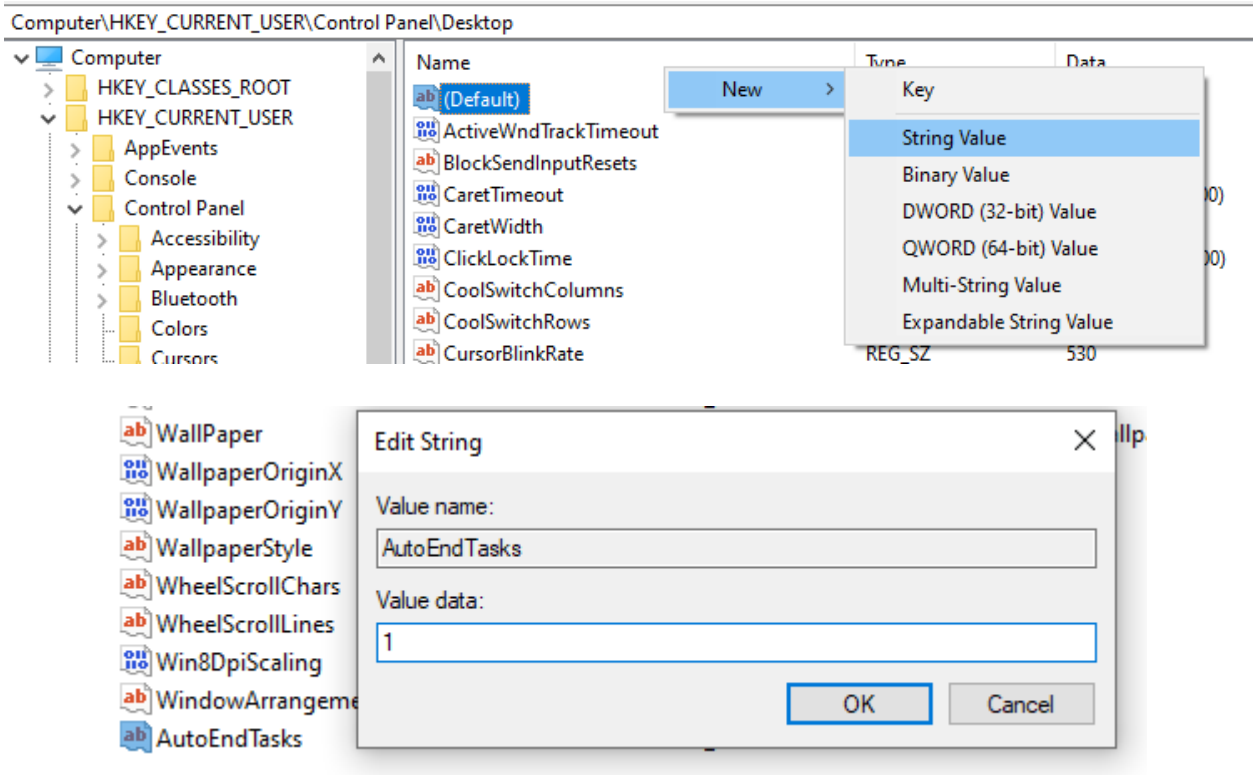


Отображение сетевого пароля

За это отвечает ключ HKEY_CLASSES_ROOT\AppID\{86f80216-5dd6-4f43-953b-35ef40a35aee}. Если его удалить, то не будет отображения сетевого пароля.

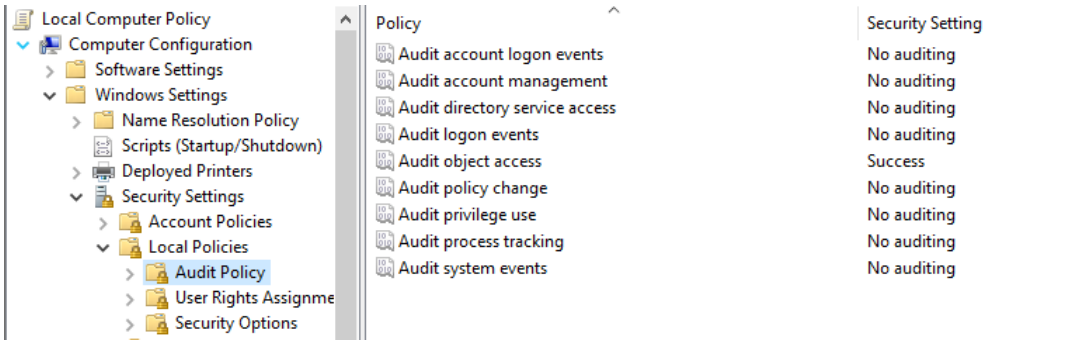


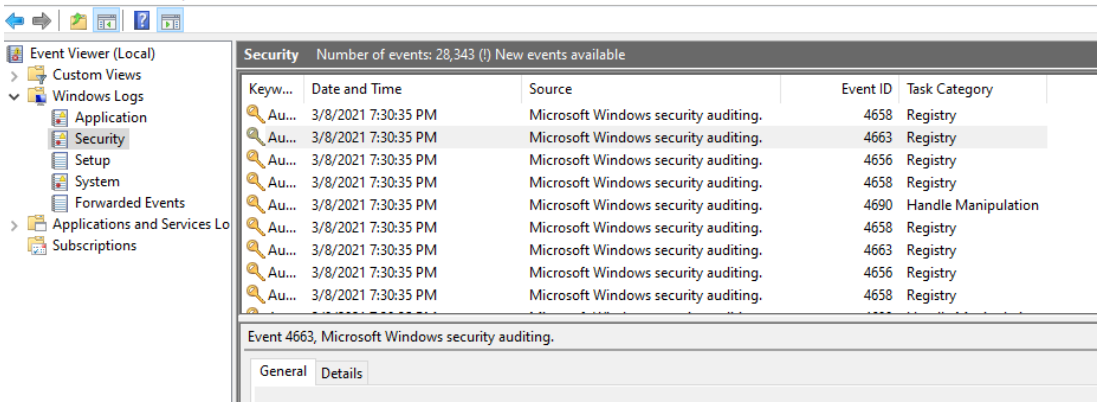
Автоматическое завершение задач
За это отвечает значение *AutoEndTasks* (0 или 1) у *HKEY_CURRENT_USER\Control Panel\Desktop*



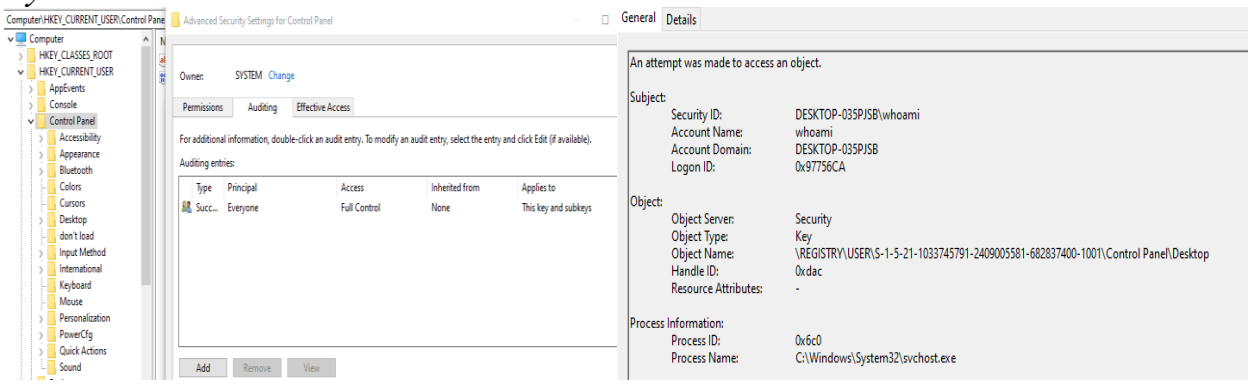
4. Настройка аудита реестра
    1. Win+R -> gpedit.msc
    2. Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy
    3. Меняем Audit object access на Success
    4. Для просмотра аудита используется Event Viewer: Windows Logs -> Security

5. Для аудита ветки: regedit.msc -> ПКМ по ветке -> Permissions -> Advanced -> Auditing -> Добавляем субъектов для аудита

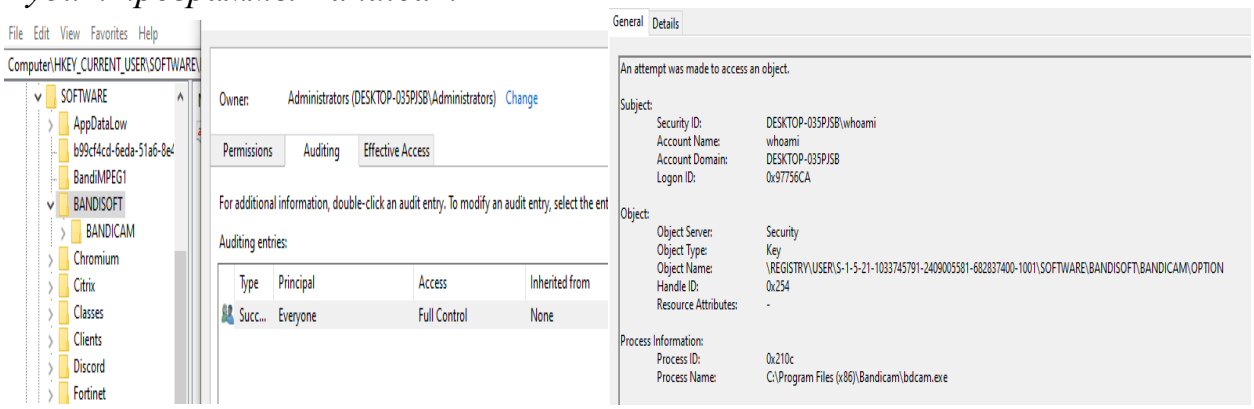




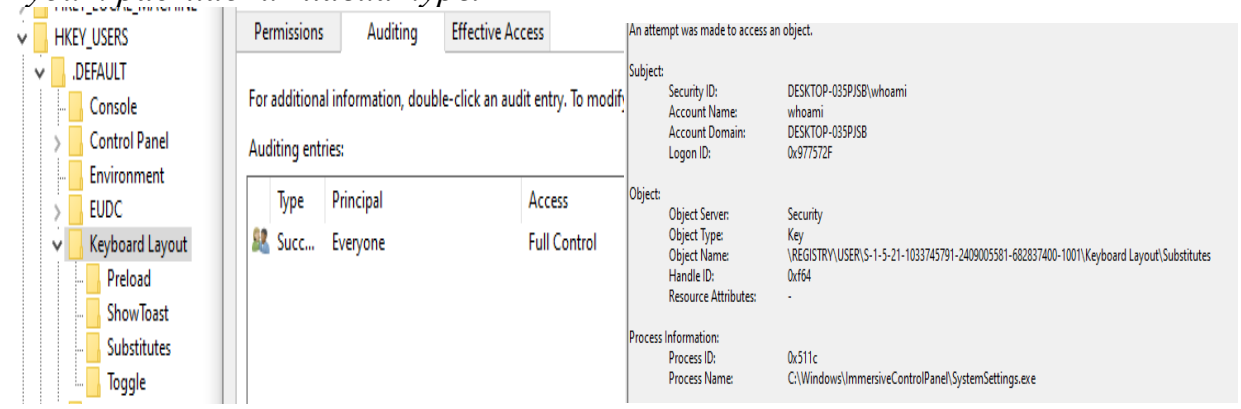
Аудит Control Panel



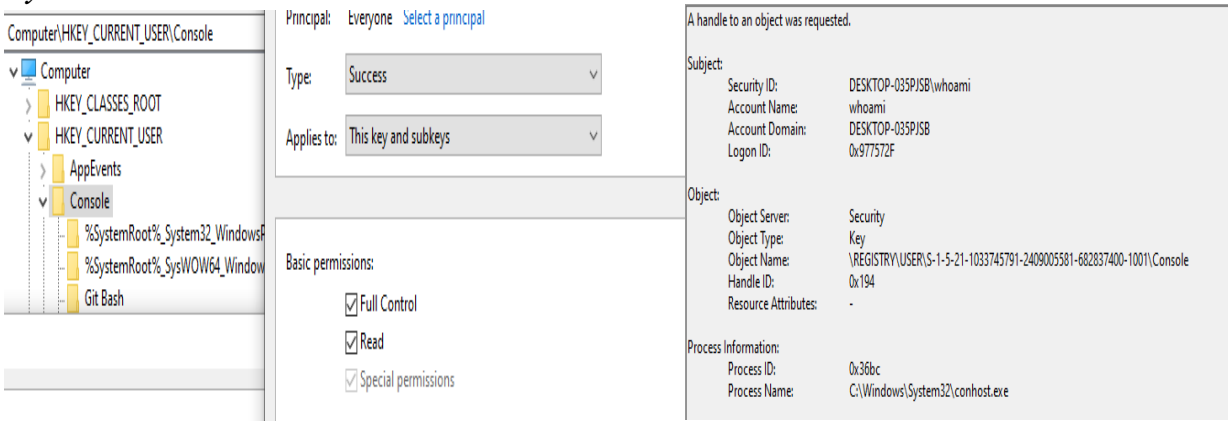
Аудит программы Bandicam



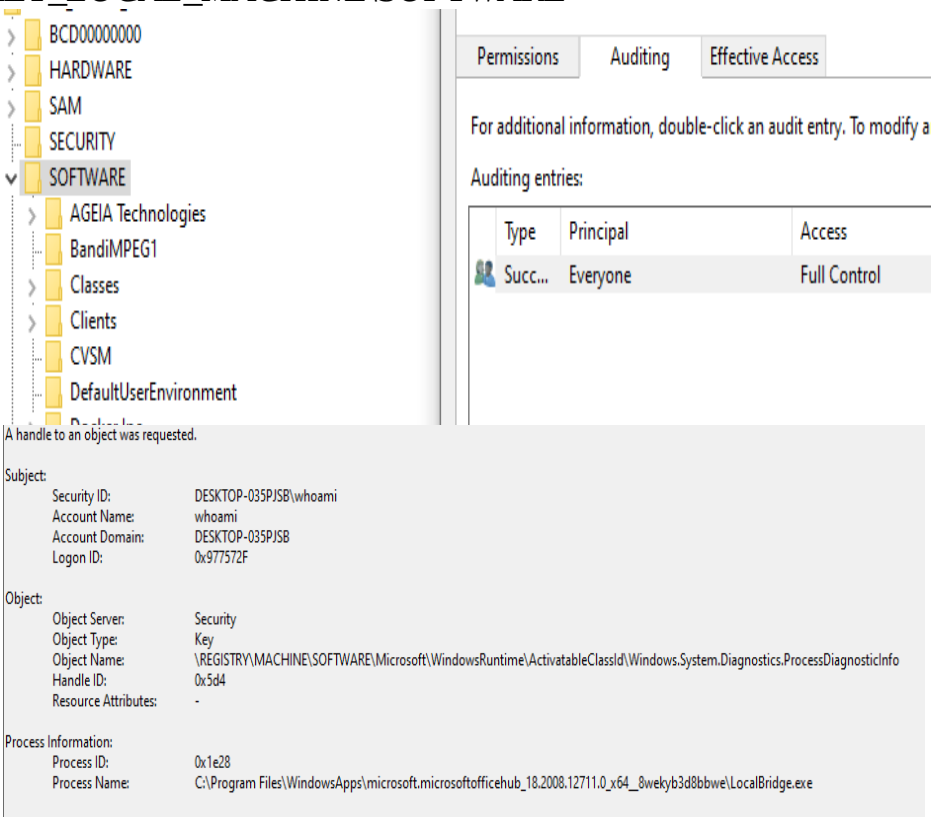
Аудит раскладки клавиатуры



Аудит консоли Git Bash

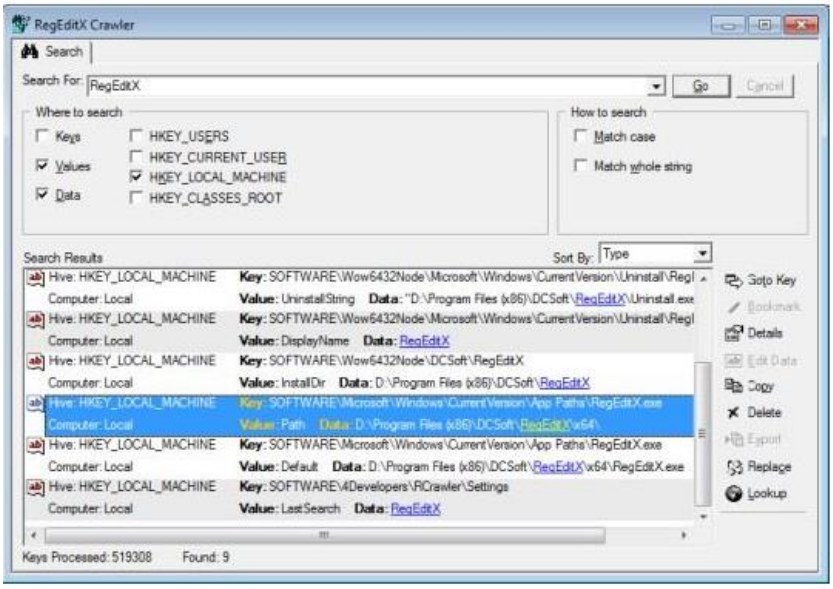


Аудит HKEY_LOCAL_MACHINE\SOFTWARE



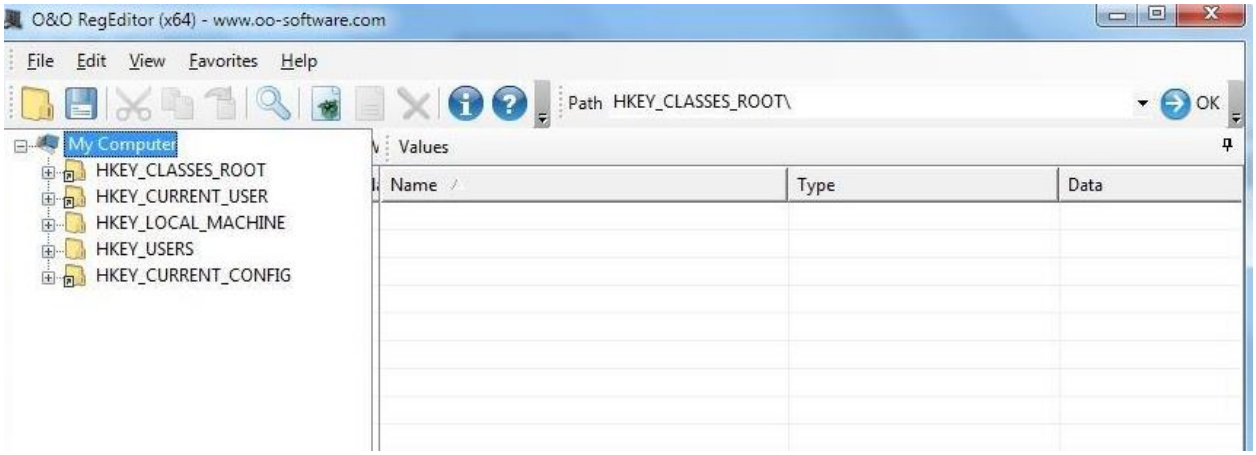
5. Аналоги Regedit

RegEditX (Платный)



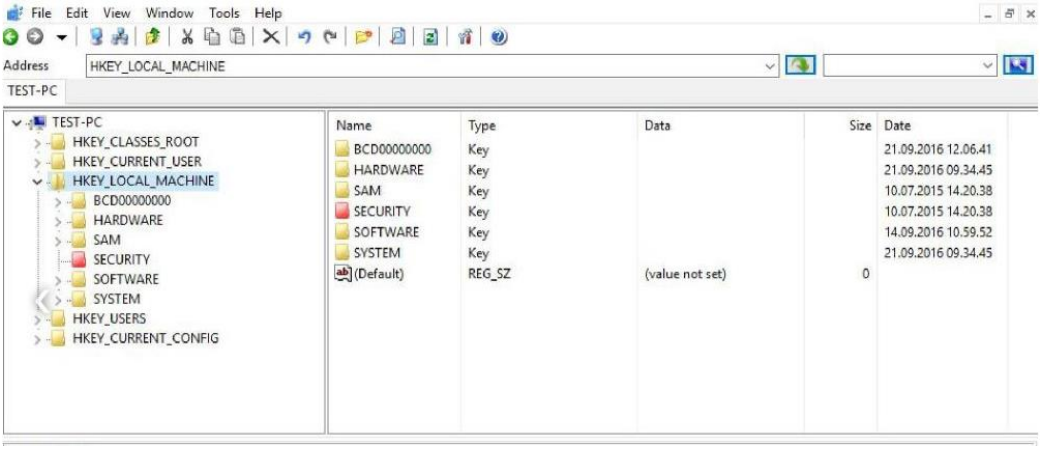
Данный аналог позволяет быстро в реестре. Поиск можно производить по ключам, по данным и по значениям. Для поиска может использоваться регулярное выражение. В поиске подсвечиваются искомые данные. Однако имеет довольно нагруженный.

O & O RegEditor (бесплатный)



Данный редактор имеет главное ключевое преимущество – он позволяет копировать/вставлять значения, а также отменять предыдущие действия. Однако этот редактор не поддерживает Windows Server 2012+

RegCool (бесплатный)



Данный редактор позволяет отменять, повторять действия. Поиск с заменой, сравнение реестров, копирование/вставка. Также позволяет производить оптимизацию реестра (дефрагментирование). Не поддерживает Windows Server.

Вывод

В ходе данной лабораторной работы я изучил работу с реестром windows. Изучил настройки доступа к реестру, а также настройки для аудита.