Криминалистический анализ реестра операционной системы Windows

РЕЕСТР ОС Windows

Реестр – это компонент операционной системы компьютера, который в иерархической базе данных хранит важнейшие установки и информацию о приложениях, системных операциях и пользовательской конфигурации.

- Регистрационная база данных (Registration Database) Windows, в первую очередь является базой данных параметров операционной системы, приложений и драйверов оборудования. Реестр содержит огромный объем информации, начиная с параметров учетных записей пользователя и заканчивая цветами рабочего стола.

- **До создания Реестра Microsoft использовала обычные текстовые файлы для управления системой. В MS-DOS конфигурация системы контролировалась двумя следующими файлами:**
- **Config.sys** содержал конфигурационную информацию, необходимую для функ ционирования MS-DOS. В основном, это были общие параметры оборудования, используемого различными приложениями, например работа верхней и нижней памяти.
- **Autoexec.bat** был пакетным файлом, служившим для выполнения процедур ав тозагрузки.

Реестр выполняет следующие основные функции:

- Отслеживает все системные устройства и их установки, включая такие ресурсы, как запросы на прерывания (**IRQ**) и номера каналов прямого доступа памяти (**DMA**).
- Работает как база данных, которая унифицирует функционирование приложений.
- Проверяет наличие необходимых драйверов для инсталируемого оборудования. При добавлении нового переферийного устройства *Диспетчер конфигурации (Configuration manager)* операционной системы помещает конфигурационные данные устройства в реестр.
- Предоставляет системные сервисы, которые необходимы для работы многих приложений.
- Обеспечивает запуск необходимого приложения при щелчке мышью.
- Сохраняет информацию относящуюся к системным правилам, профилям пользователей и средствам администрирования.

Приложения MS-DOS самостоятельно регулировали все свои параметры и совместное с другими приложениями использование таких устройств, как принтер и звуковая карта.

Параметры хранились в текстовых файлах, называемых файлами инициализации (.INI).

- **Program.ini** - содержал параметры Менеджера программ Windows (Windows Program Manager), обеспечивающего графический интерфейс пользователя (graphical user interface - GUI), для работы в Windows.
- **Control.ini** - содержал множество пользовательских настроек Windows, включая параметры рабочего стола, звука и принтера.
- **Win.ini** -этот файл содержал информацию о визуальном оформлении Windows и параметры установленных приложений.
- **System.ini** - содержал параметры конфигурации оборудования и определял, как Windows будет с ним взаимодействовать.

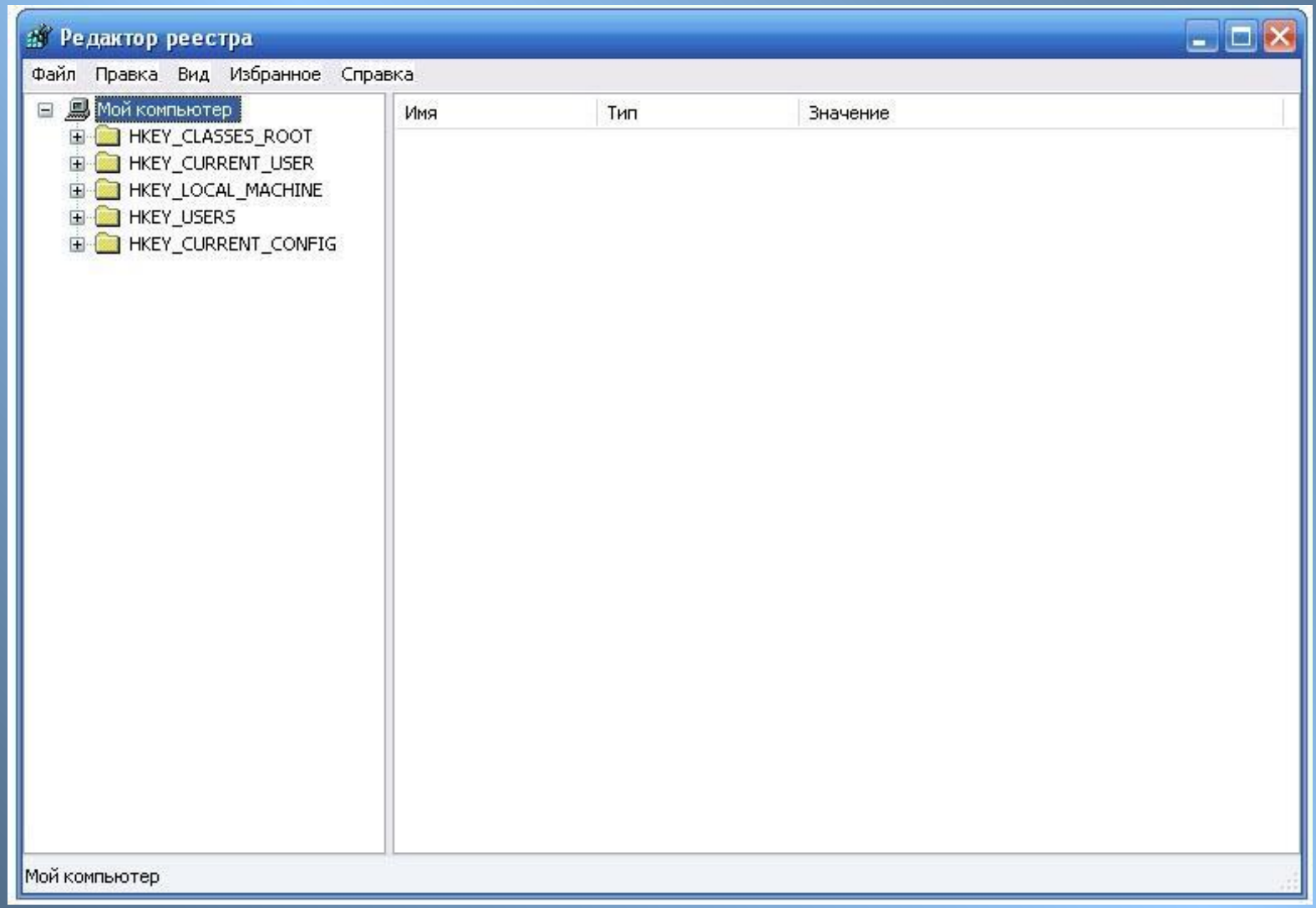
- С появлением Windows NT на свет появился новый Реестр. 64 кб ограничение было снято, и теперь Реестр мог занимать столько места, сколько ему было необходимо.
- Один файл был заменен несколькими, но при этом сохранилась единая иерархическая структура, объединяющая вместе все записи.
- С момента появления Windows NT Реестр практически не изменился.

РЕЕСТР ОС Windows

Реестр Windows 2000, XP, 7, 8 хранится в следующих файлах:

- DEFAULT,
- SAM, (находятся по адресу
- SECURITY, C:\WINDOWS
- SOFTWARE, \System32\Config)
- SYSTEM
- NTUSER.DAT (по адресу C:\Documents andSettings\[Профиль пользователя])

Ключи реестра



HKEY_CLASSES_ROOT

- В основном, HKEY_CLASSES_ROOT (HKCR) обеспечивает совместимость с 16-разрядными приложениями Windows. HKCR содержит информацию об ассоциациях файлов -т.е. какие приложения открывают определенные типы файлов. Более важным для многих людей является то, что HKCR содержит определения всех объектов среды Windows XP. Ключи, контролирующие эти определения, контролируют информацию о внешнем интерфейсе объекта, как, например, команды, доступные в контекстном меню данного объекта.
- 32-битные приложения обращаются к этим данным через их копию в подключе Software\Classess подкаталога HKEY_LOCAL_MACHINE. На самом деле - это не совсем копии, а просто информация, хранящаяся в одном кусте, но рассматриваемая как бы с двух разных точек. Если изменить параметр в одном месте, то он изменится и в другом.
    - **В HKCR преобладают два следующих типа ключей:**
- **Ключи расширений** файлов названы так же, как и представляемые ими расширения (.doc, .txt и так далее). Параметры этих ключей определяют, какие приложения открывают файлы с соответствующим расширением. Эти ключи могут содержать и подключи, контролирующие дополнительные функции, такие как список программ меню Открыть с помощью (Open With).
- **Ключи определения класса** содержат информацию об объектах, соответствующих Общей модели объектов (Component Object Model - COM) - модели, позволяющей программистам разрабатывать объекты, доступные всем COM - совместимым приложениям. Технологии Внедрения и связывания объектов (Object Linking and Embedding - OLE) и ActiveX основаны на COM.

HKEY_USERS

Содержит информацию, определяемую пользователем (например, пользовательские настройки *рабочего стола*): установки по умолчанию (HKEY_USERS\.DEFAULT) для рабочего стола, меню Пуск (Start), приложений и т. д.

Когда новый пользователь входит в систему, установки по умолчанию копируются в отдельный подраздел, название которого совпадает с именем пользователя. Все изменения, которые пользователь в дальнейшем произведёт с этими установками сохраняются в этом подразделе.

HKEY_CURRENT_USER

- Пользовательские настройки из HKEY_USERS вступают в силу в процессе входа пользователя в систему. При этом содержимое подраздела HKEY_USERS\name, где name - имя текущего пользователя, или подраздела HKEY_USERS\.DEFAULT копируется в раздел HKEY_CURRENT_USER.

  Раздел HKEY_CURRENT_USER содержит несколько подразделов:

- AppEvents - содержит пути звуковых файлов, используемых для озвучивания системных событий.
- Control Panel - содержит различные данные, которые могут быть изменены в панели управления.
- Display - содержит пользовательские установки экрана для текущего пользователя (этот подраздел доступен, только если разрешены *пользовательские профили (user profiles)*).
- InstallLocationsMRU - содержит пути, использованные в процессе последней инсталляции.
- keyboard layout - содержит информацию о раскладке клавиатуры. Текущая раскладка клавиатуры устанавливается с использованием пункта **Клавиатура (Keyboard)**панели управления.
- Network - содержит подразделы, описывающие постоянные и недавно установленные сетевые соединения, а также состояние сети.
- RemoteAccess - необязательный подраздел, доступный только в случае, если установлен сервис *удалённого доступа*.
- SOFTWARE - содержит пользовательские настройки приложений. Этот раздел ссылается на раздел HKEY_LOCAL_MACHINE, в которой также хранятся настройки приложений.

HKEY_LOCAL_MACHINE

Этот раздел определяет всю информацию, относящуюся к локальному компьютеру, такую как драйверы, установленное программное обеспечение, наименование портов и конфигураций программного обеспечения. Эта информация верна для всех пользователей, подключённых к системе.

Состоит из нескольких подразделов:

- Config - хранит конфигурацию компьютера. Содержимое данного подраздела обновляется в процессе установки и запуска Windows.

- Enum - Windows использует так называемую шинную нумерацию (bus enumeration) для учёта всех установленных компонента оборудования. Данные для этих компонентов хранятся в этом подразделе и используются для построения "дерева оборудования" на вкладке **Устройства (Drevices)** диалога **Система(System)**, вызываемого из панели управления.

HKEY_LOCAL_MACHINE

- Hardware - содержит установки для последовательных портов доступных на локальном компьютере. Подраздел Description содержит записи для устройств в системе.
- Network - когда Windows работает в сети, этот подраздел содержит регистрационную информацию пользователя (т. е. имя пользователя, сетевого провайдера, подтверждения регистрации и т.д.)
- Security - доступен для сетевых машин и содержит информацию о провайдере безопасности.
- Software - вся информация о программах, установленных на компьютере. Подраздел \Classes этого раздела используется для построения раздела HKEY_CLASSES_ROOT.
- System - содержит всю необходимую информацию для запуска Windows. Здесь содержится подраздел CurrentControlSet, в котором содержатся подразделы Control и Servicer. Подраздел Control содержит такую информацию, как имя компьютера, параметры файловой системы и т.д.

HKEY_CURRENT_CONFIG

- Этот ключ отвечает за устройство Plug&Play и содержит информацию о текущей конфигурации компьютера с переменным составом аппаратных средств. Установки этого раздела, соответствуют конфигурационным установкам, хранящимся в разделе HKEY_LOCAL_MACHINE\Config

- **Hardware** - соответствует подключу HKLM\Hardware. Данный параметр не имеет своего значения, так как информация об оборудовании не хранится на диске.

- **SAM**-соответствует подключу HKLM\SAM.
- **Security** - соответствует подключу HKLM\SECURITY.
- **Software** - соответствует подключу HKLM\Software.
- **System** - соответствует подключу HKLM\System.
- **Default** - соответствует подключу HKU\Default.

Таблица 1 Ключи Реестра и файлы хранения.	
Куст реестра	Файлы
HKEY_LOCAL_MACHI N E\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACH!NE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav

Работа с реестром

- при обычной работе

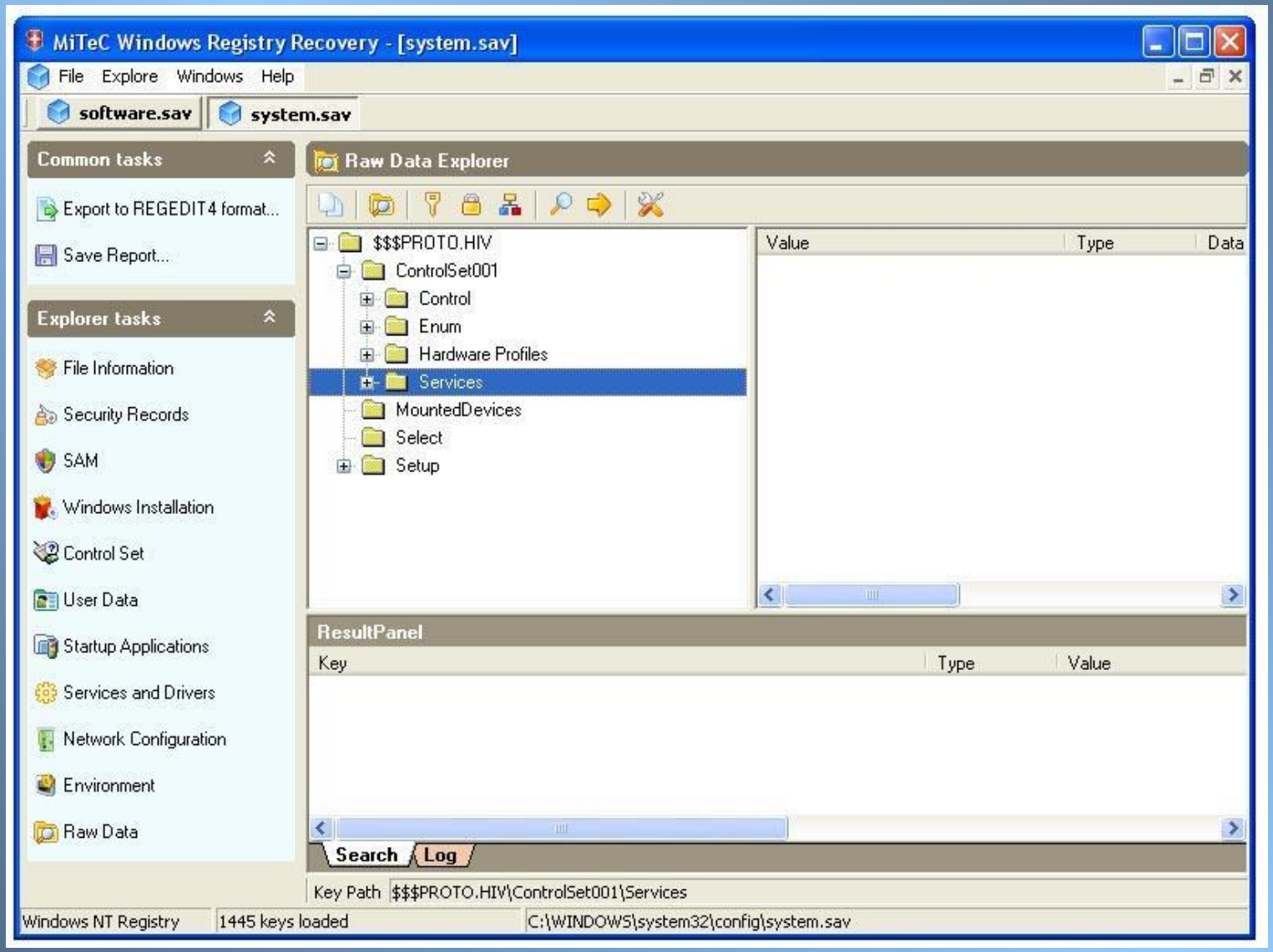
  программа **REGEDIT**

- при исследовании отдельного накопителя

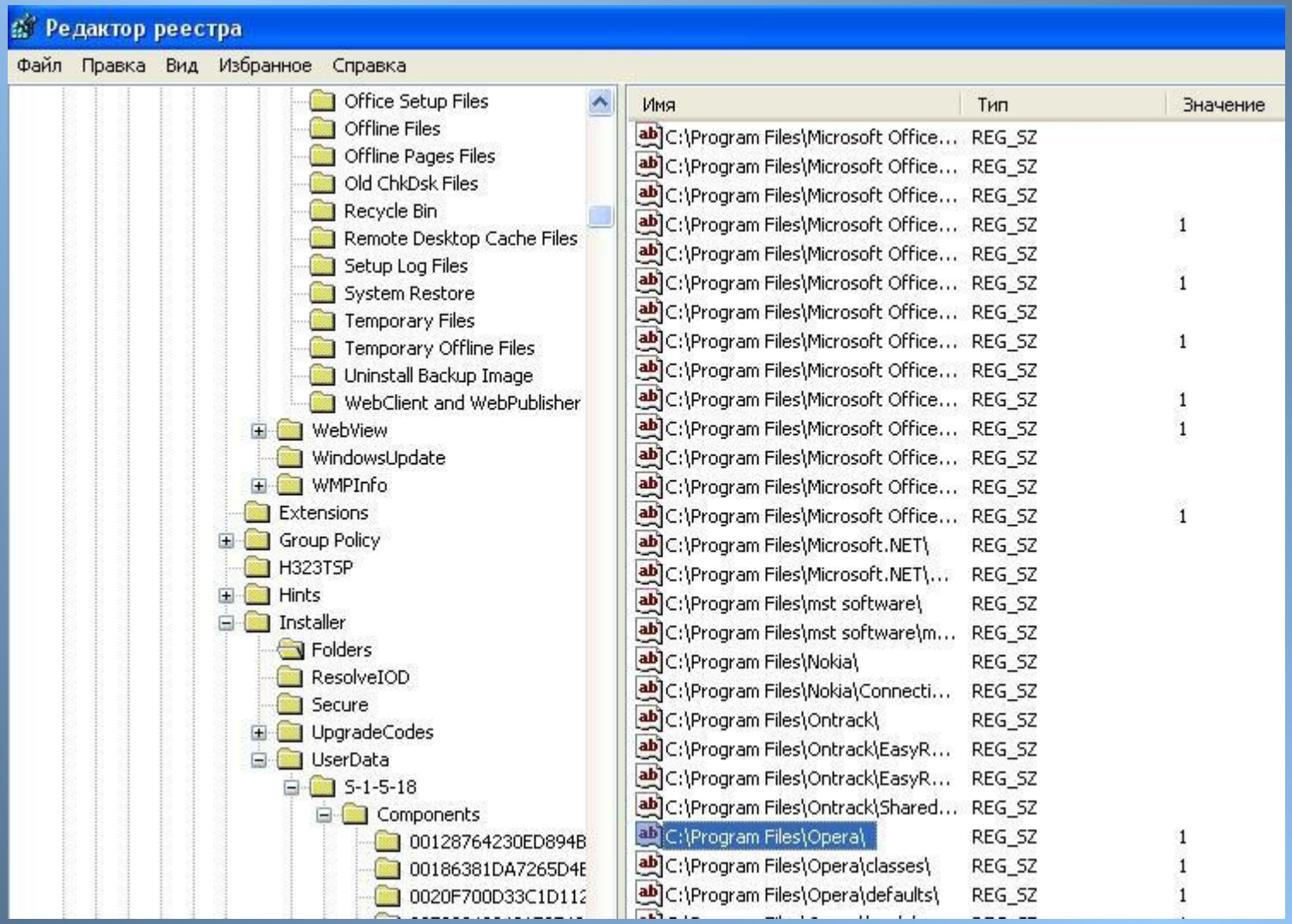
  программа **MiTEC Windows**

  Registry Recovery

MiTEC Windows Registry Recovery



- данные реестра



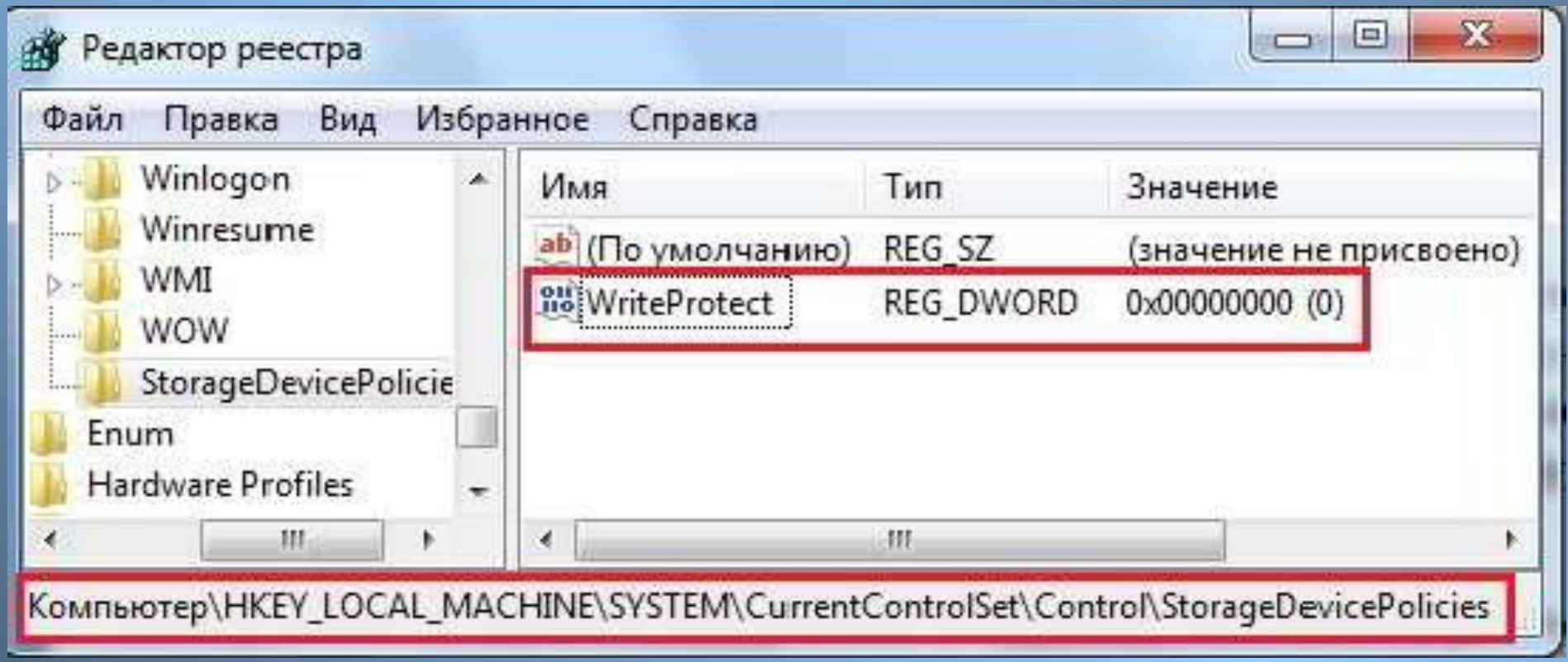
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders

Изменения в реестре

Монитор реестра (RegMon)

Криминалистически значимые области реестра

1. Блокировка/разблокировка записи через порты USB



Если раздела **StorageDevicePolicies** в резделе **Control** нет, то его необходимо создать.

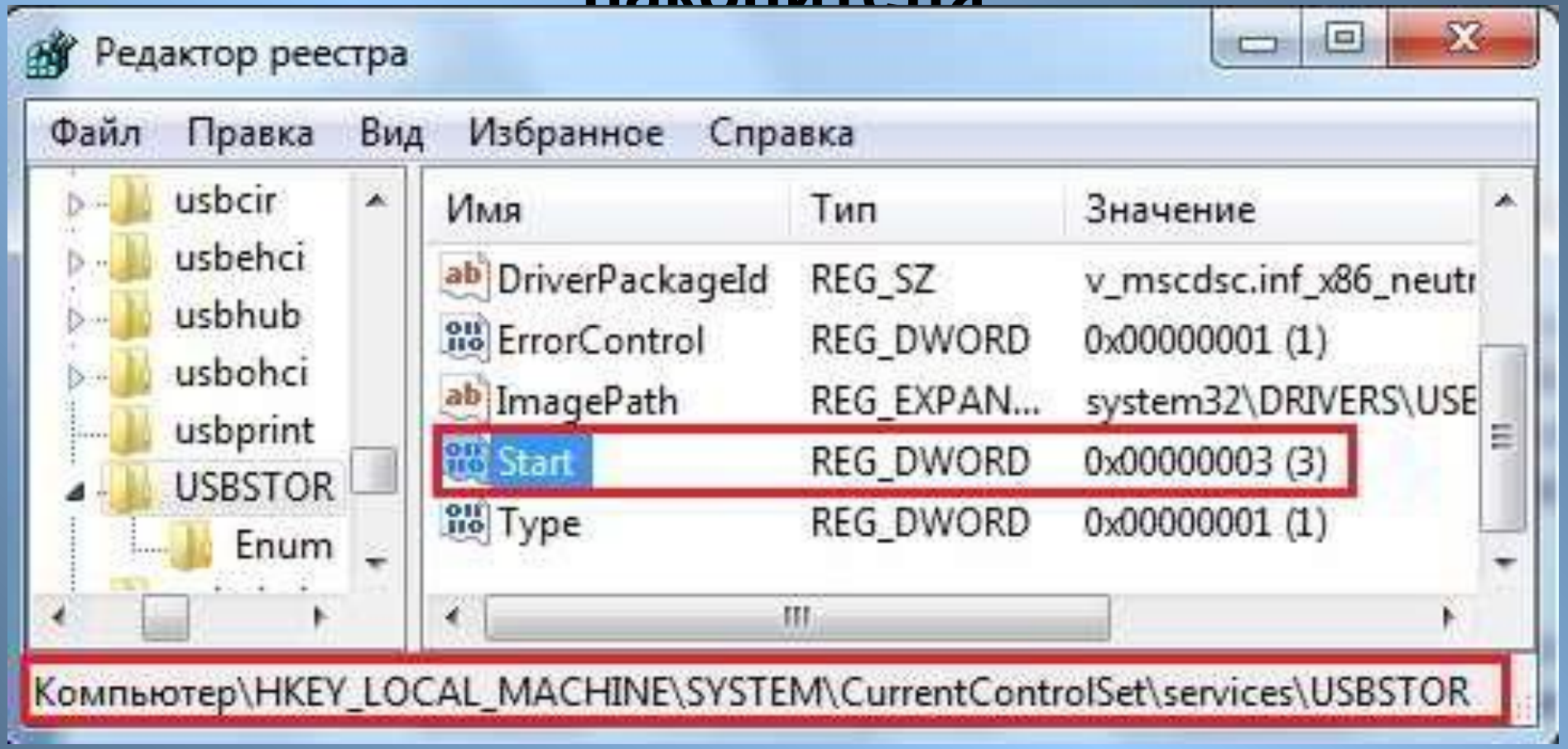
Далее создаём параметр **WriteProtect**, тип **dword**

При значении параметра **WriteProtect** :

1 - режим чтения (readonly)

0 - режим записи

2. Запрет на использование USB накопителя

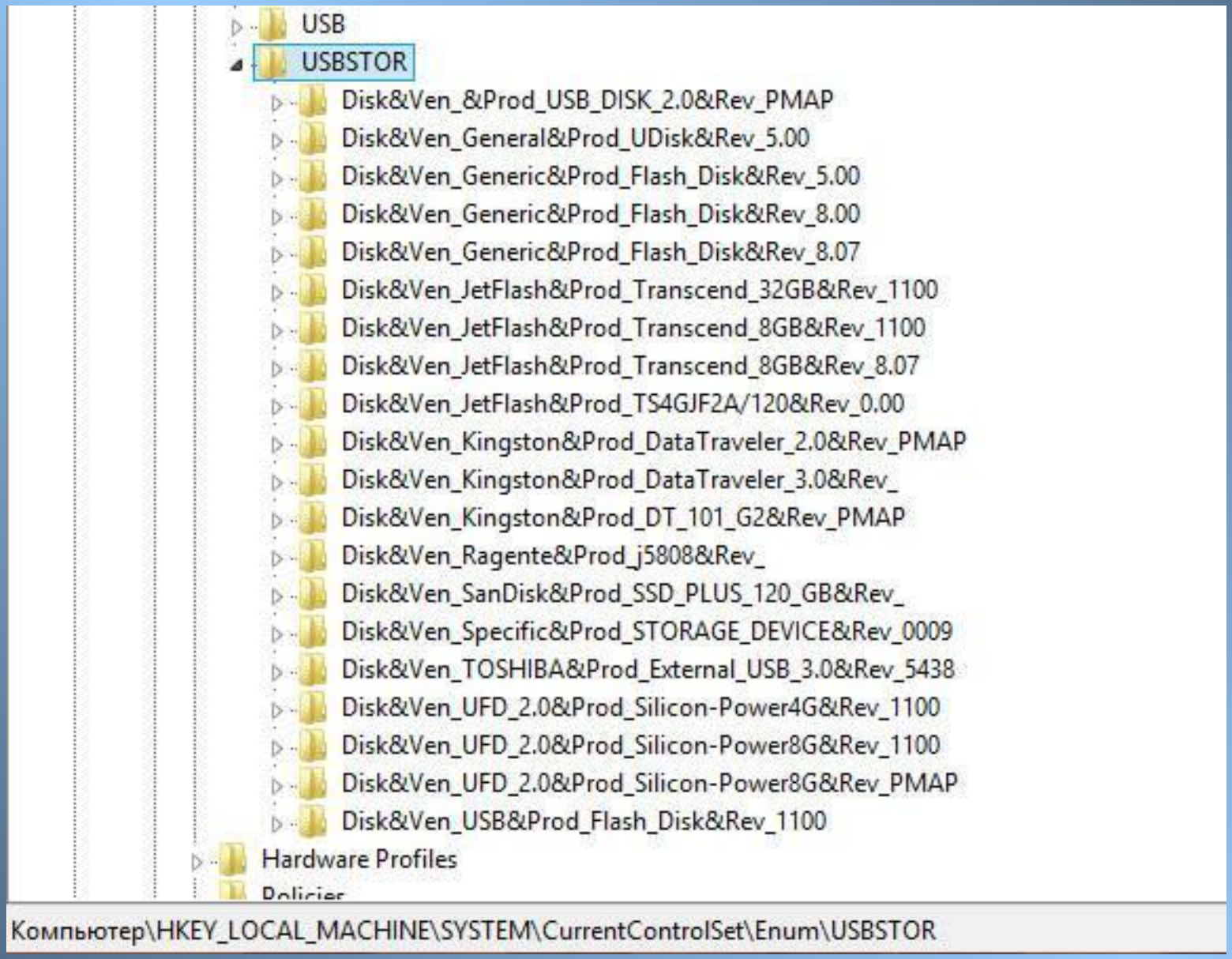


При значении параметра Start :

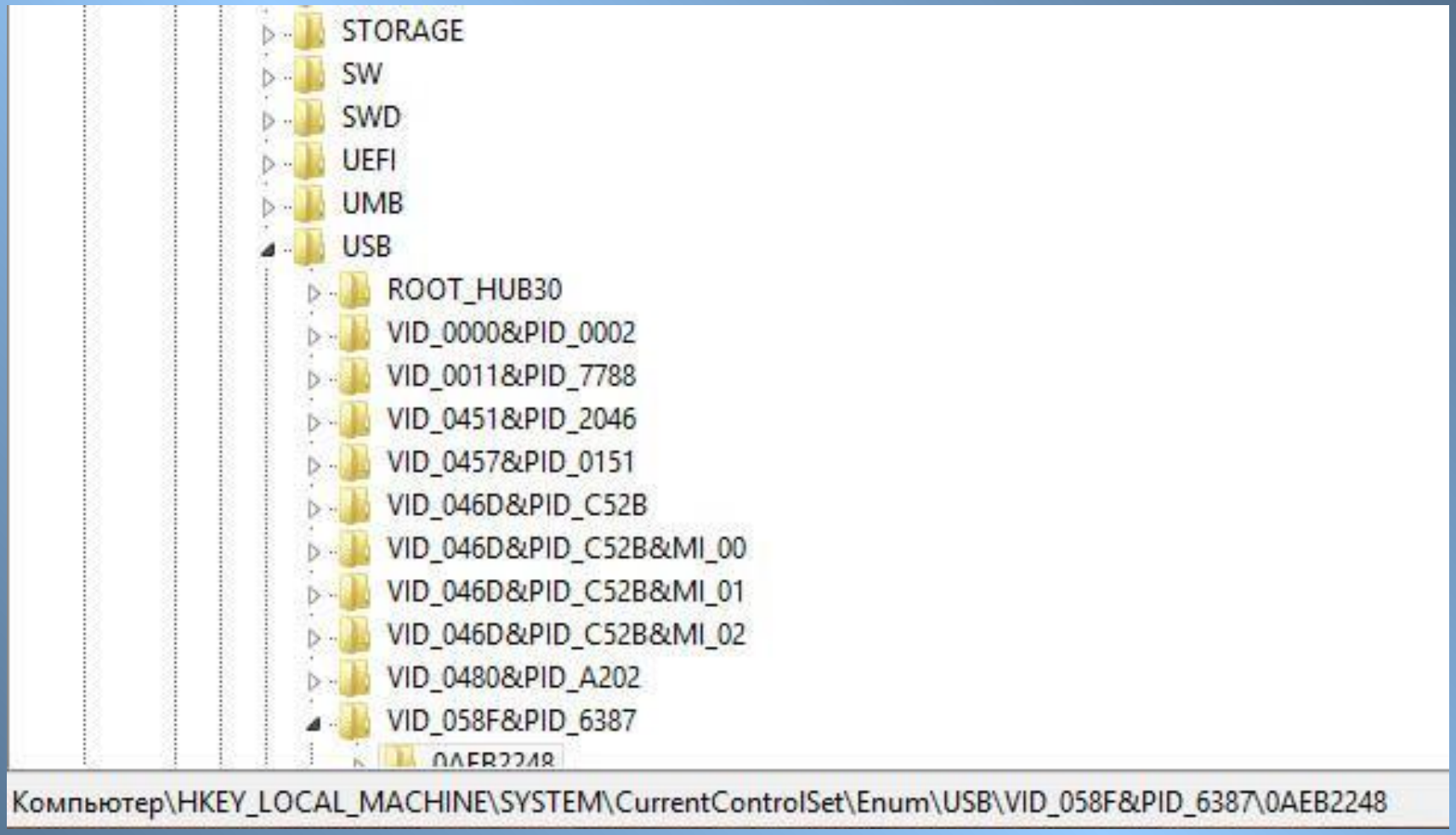
4 - блокировка USB накопителя

3 - стандартный режим (без блокировок)

3. Подключенные через USB накопители



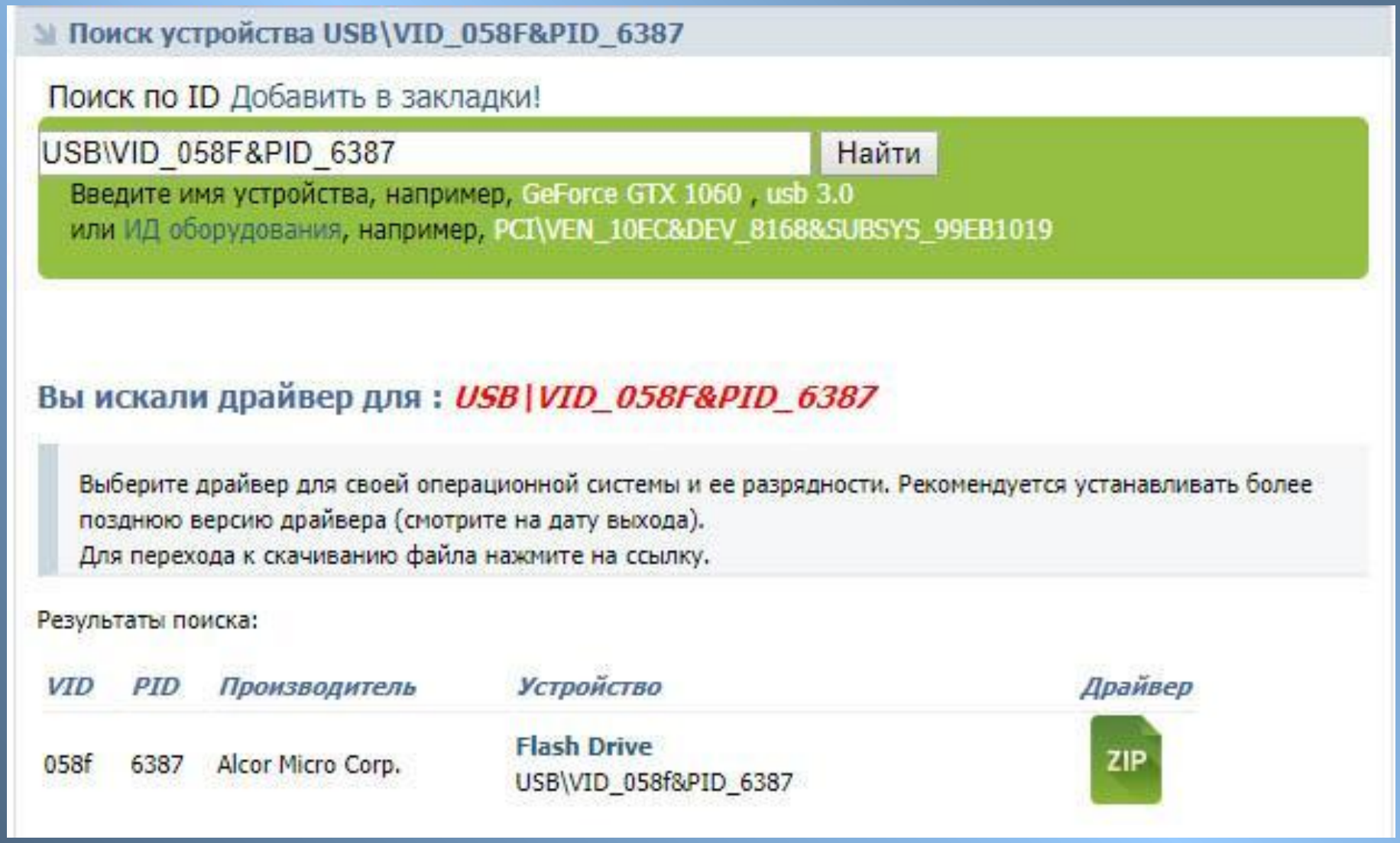
4. Устройства USB



Сведения об устройстве по VID и PID на сайтах:

- **flashboot.ru**
- **driverslab.ru**

driverslab.ru

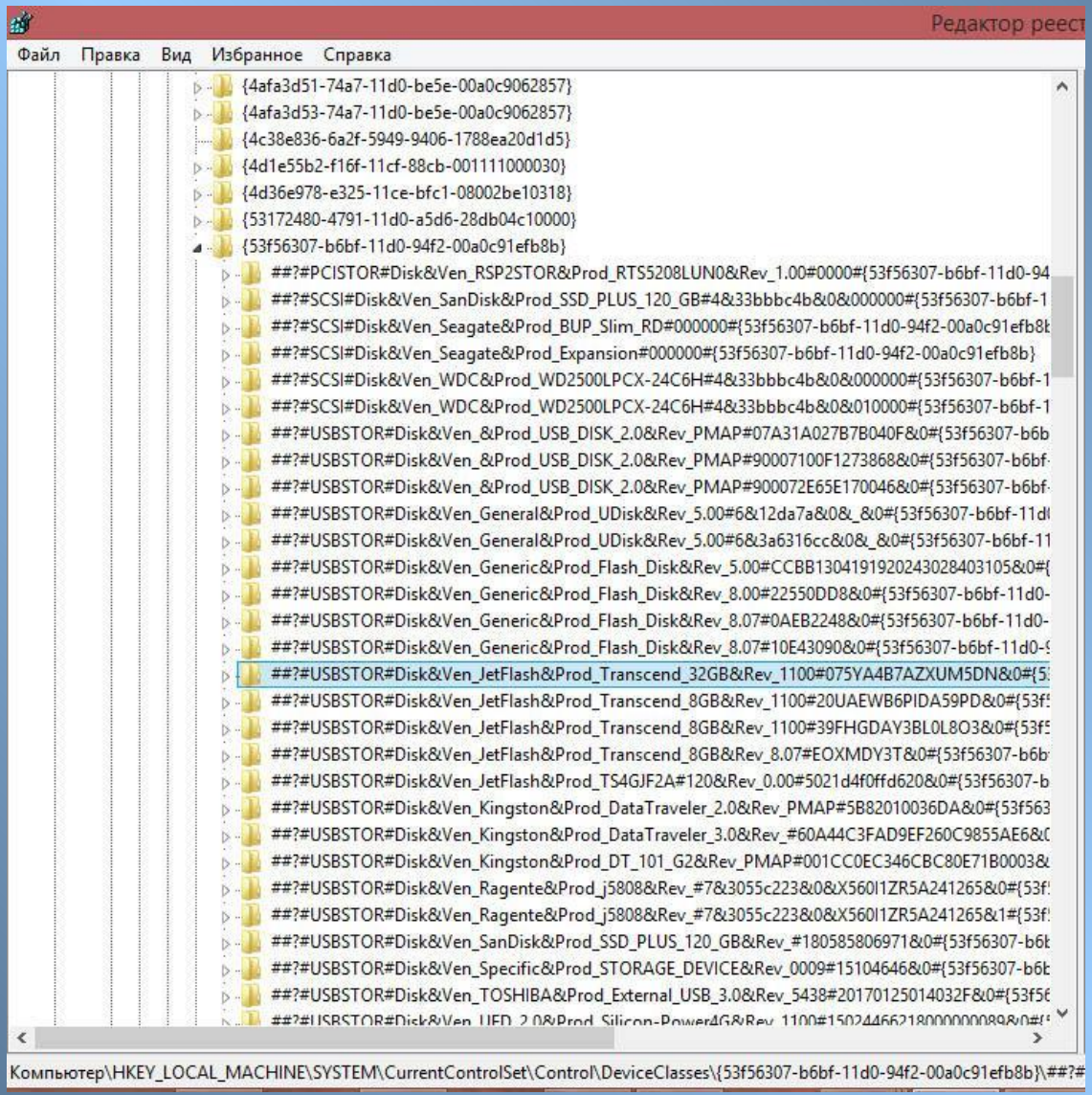


5. ВременнЫе метки

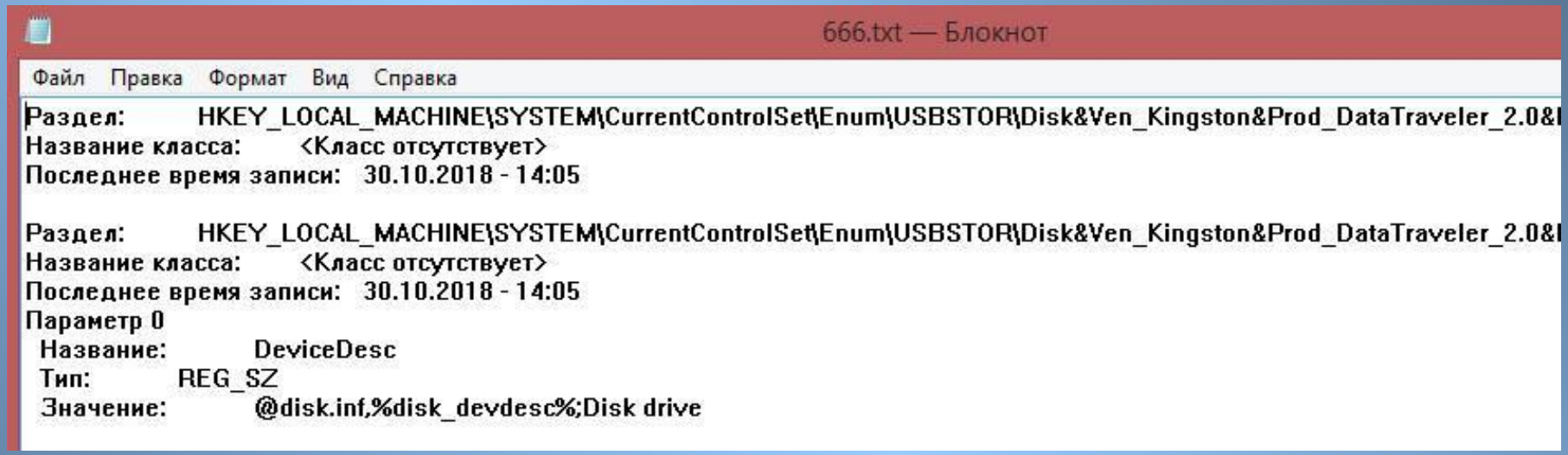
- Все ключи реестра содержат временную метку (timestamp, last write value), аналогично дате последнего изменения для файлов.

- Это значение хранится в структуре FILETIME и показывает дату и время того, когда ключ реестра был изменен. Это значение обновляется, когда ключ был создан, изменен или удален. Временная метка есть только у ключей реестра, значения реестра такого поля не содержат.

Обнаружение метки



Экспорт



Экспортируем ключ реестра в файл формата *.txt

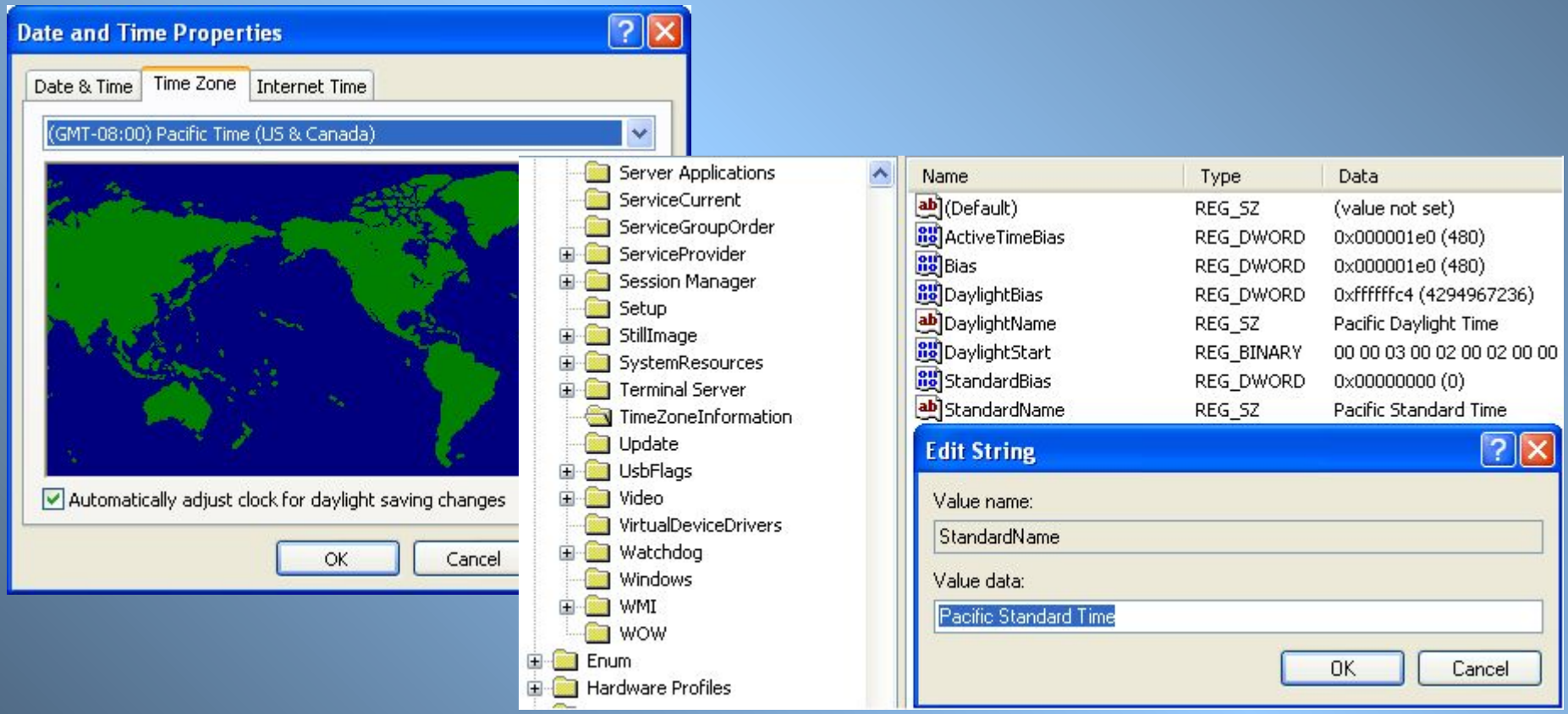
6. Иные сведения

Параметр	Путь к ключу	Название ключа
Имя компьютера	\ControlSet00X\Control\ComputerName\ComputerName	LENOVO-PC
Время последнего выключения компьютера	\ControlSet00X\Control\Windows	ShutdownTime
Сетевые шары	\ControlSet00X\Services\LanmanServer\Shares	
Сетевые адаптеры, и их параметры	\ControlSet00X\Services\Tcpip\Parameters\Interfaces	
Разрешение входящих подключений по протоколу RDP	\ControlSet00X\Control\Terminal Server	

Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM

Настройки времени (текущий часовой пояс)

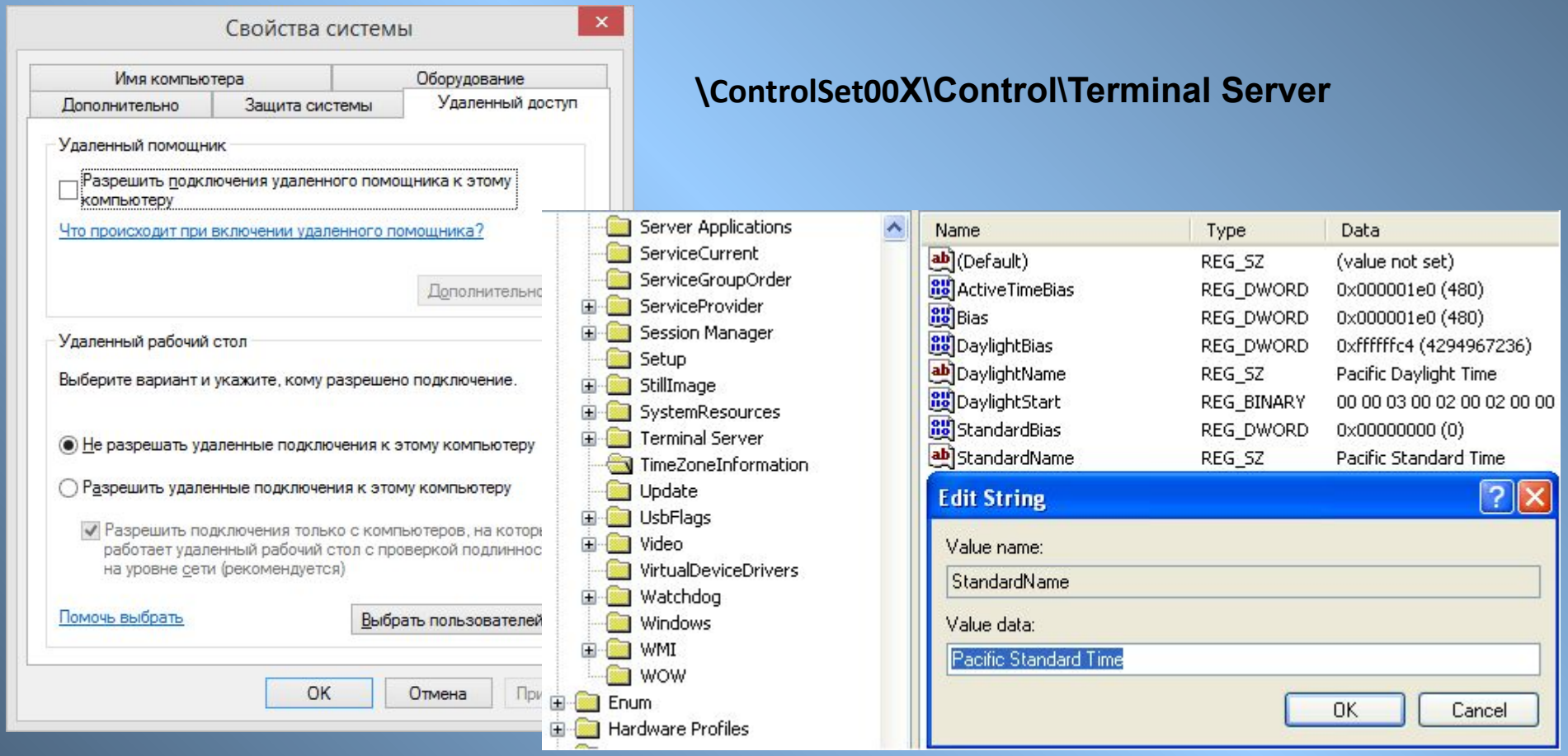
\ControlSet00X\Control\TimeZoneInformation



Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM

Запрет на входящие подключения по протоколу RDP

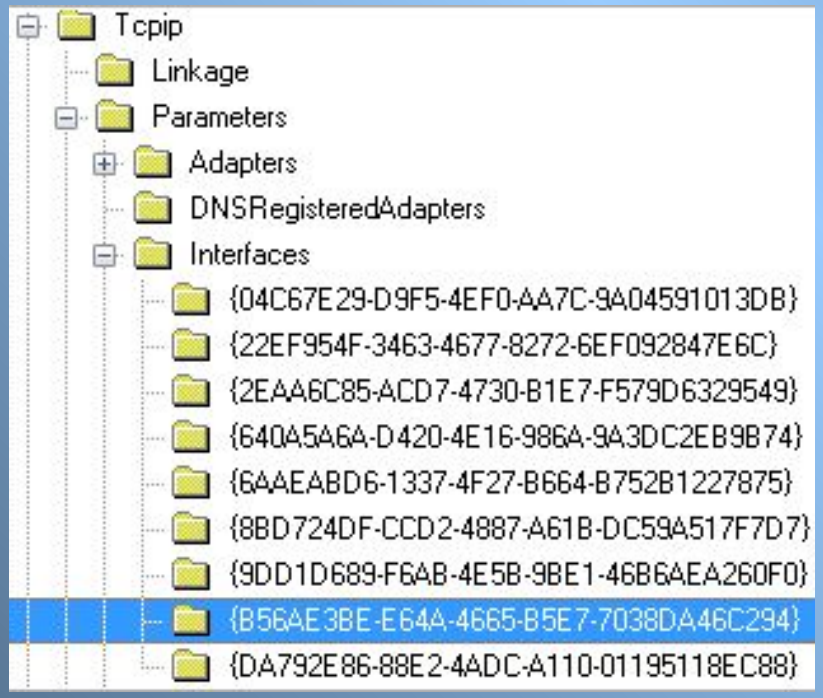
\ControlSet00X\Control\Terminal Server



Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM

Сетевые настройки

\ControlSet00X\Services\Tcpip\Parameters\Interfaces



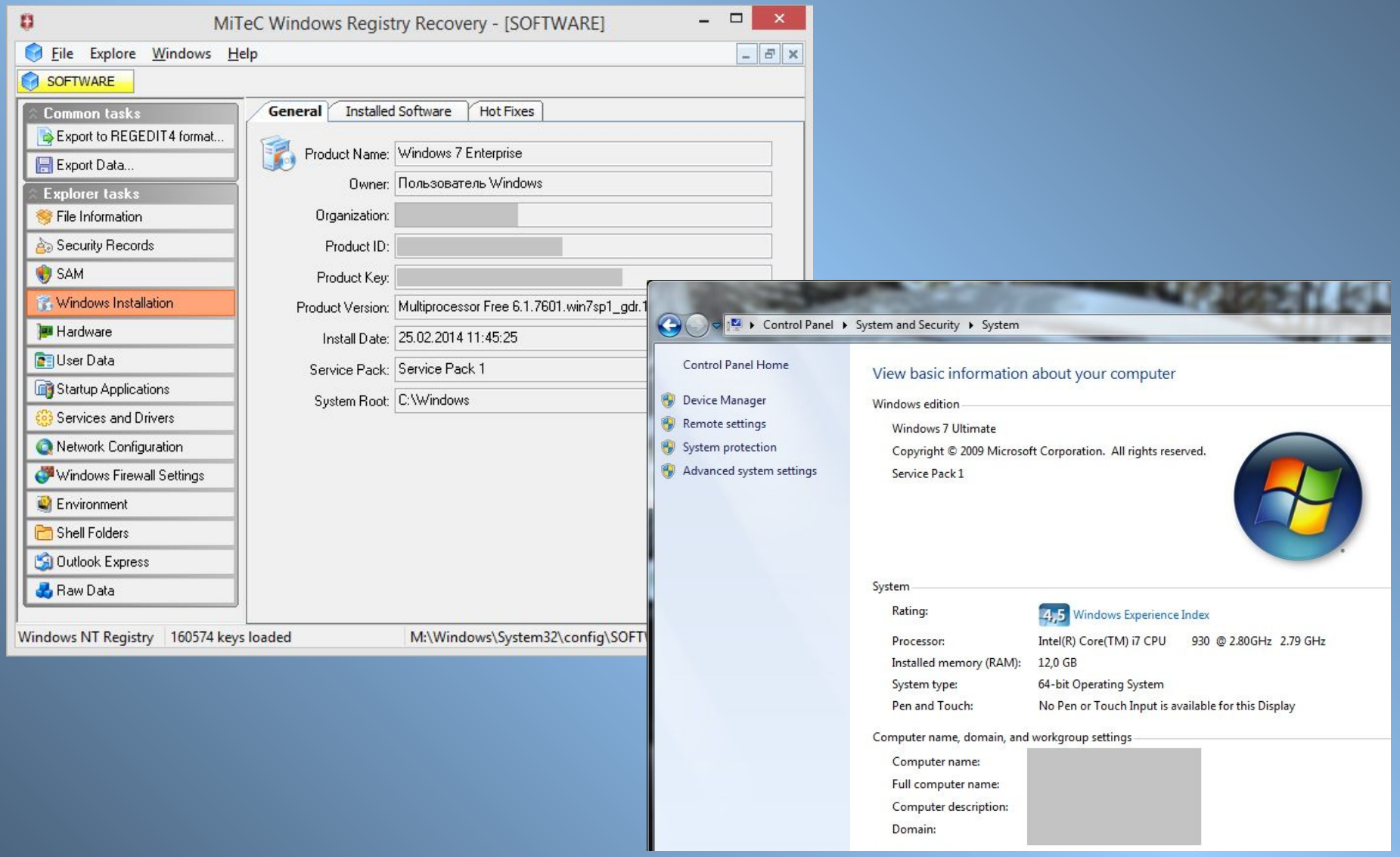
Value	Type	Data
DhcpDefaultGateway	REG_MULTI_SZ	101.24.10.24
DhcpDomain	REG_SZ	netbynet.ru
DhcpIPAddress	REG_SZ	101.24.38.34
DhcpNameServer	REG_SZ	212.1.224.34
DhcpServer	REG_SZ	10.39.16.111
DhcpSubnetMask	REG_SZ	255.255.192.0
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.192.0
Domain	REG_SZ	
EnableDeadGWDetect	REG_DWORD	0x00000001
EnableDHCP	REG_DWORD	0x00000001
IPAddress	REG_MULTI_SZ	0.0.0.0
IPAutoconfigurationAddress	REG_SZ	0.0.0.0
IPAutoconfigurationMask	REG_SZ	255.255.0.0
IPAutoconfigurationSeed	REG_DWORD	0x00000000
NameServer	REG_SZ	
NTEContextList	REG_MULTI_SZ	0x00000002
RawIPAllowedProtocols	REG_MULTI_SZ	0
RegisterAdapterName	REG_DWORD	0x00000000
RegistrationEnabled	REG_DWORD	0x00000001
SubnetMask	REG_MULTI_SZ	0.0.0.0

Раздел HKEY_LOCAL_MACHINE\SOFTWARE

Полный путь к ключу	Название ключа
Сведения об установленном ПО	
\Microsoft\Windows NT\CurrentVersion\Uninstall	-
Сведения об установленной ОС	
\Microsoft\Windows NT\CurrentVersion	

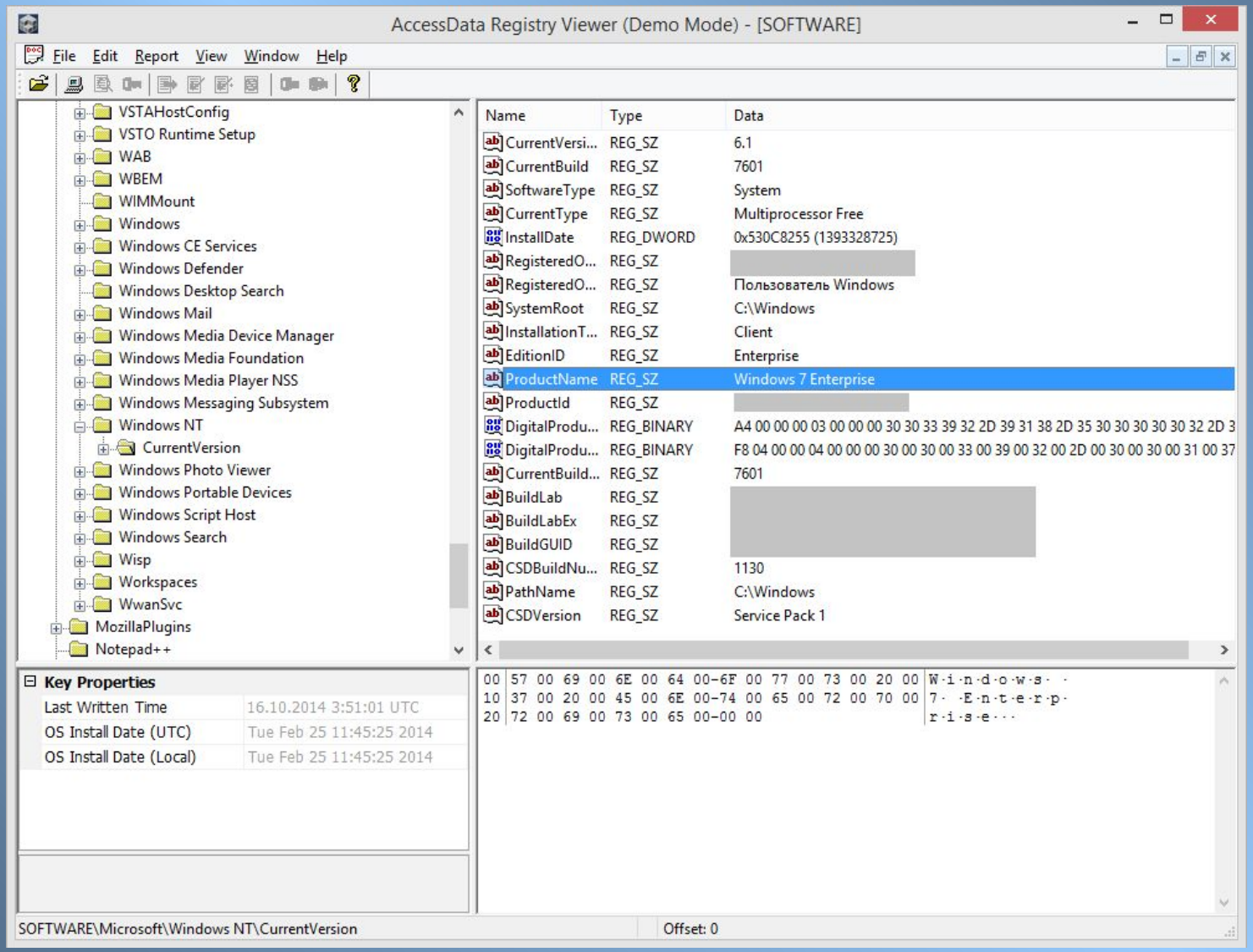
Сведения об установленной ОС

\Microsoft\Windows NT\CurrentVersion



Сведения об установленной ОС

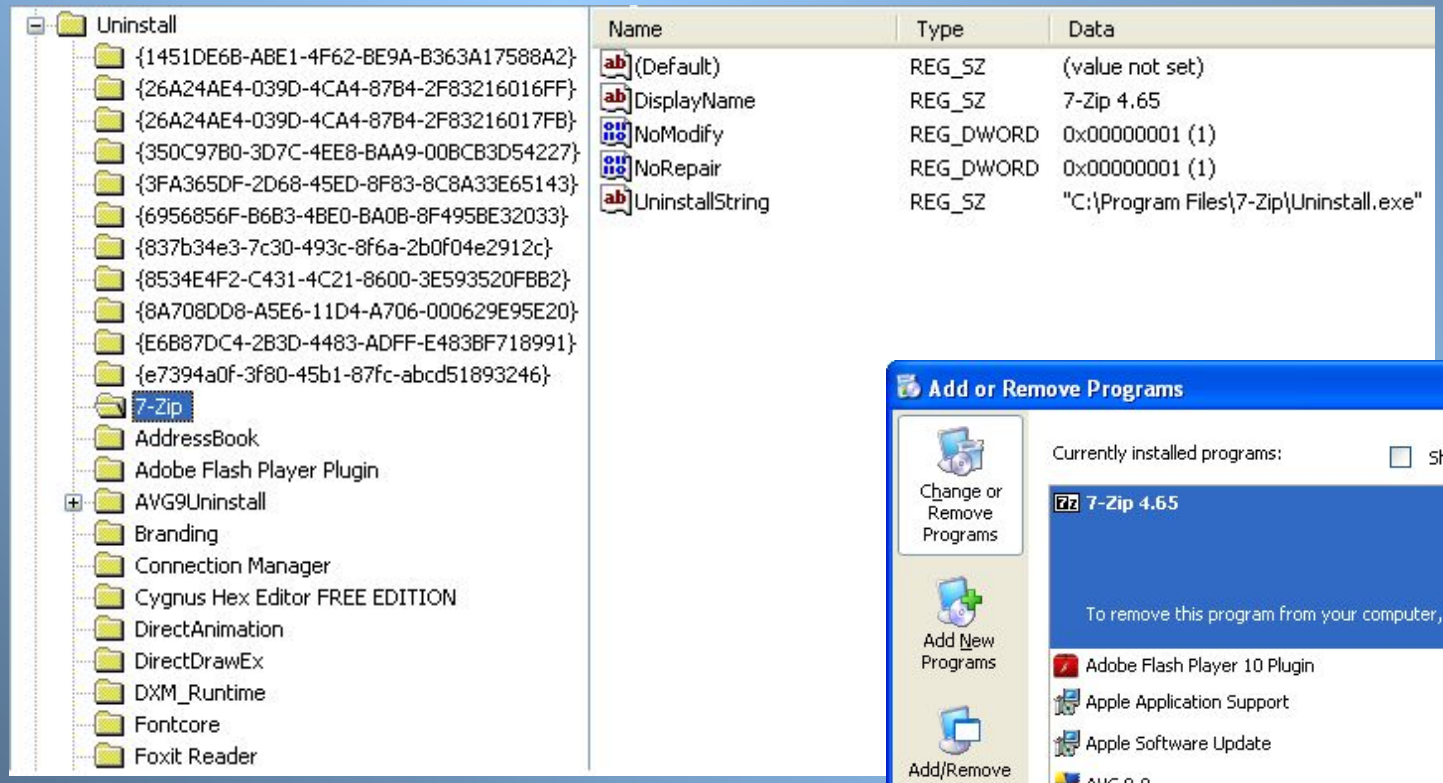
\Microsoft\Windows NT\CurrentVersion

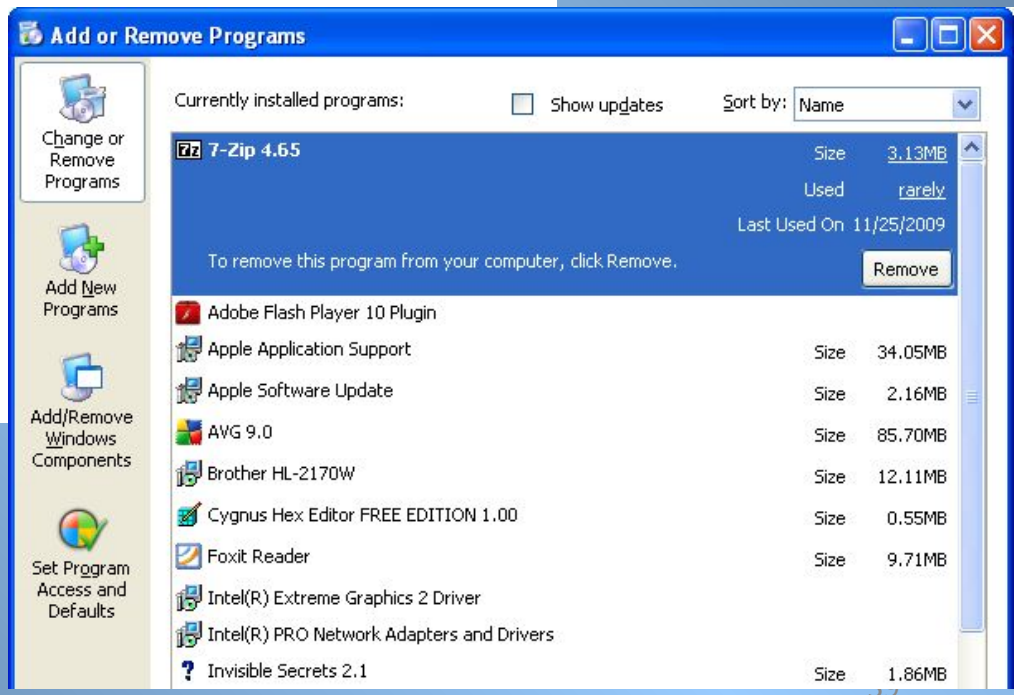


Сведения об установленном ПО

Раздел реестра HKEY_LOCAL_MACHINE\SOFTWARE

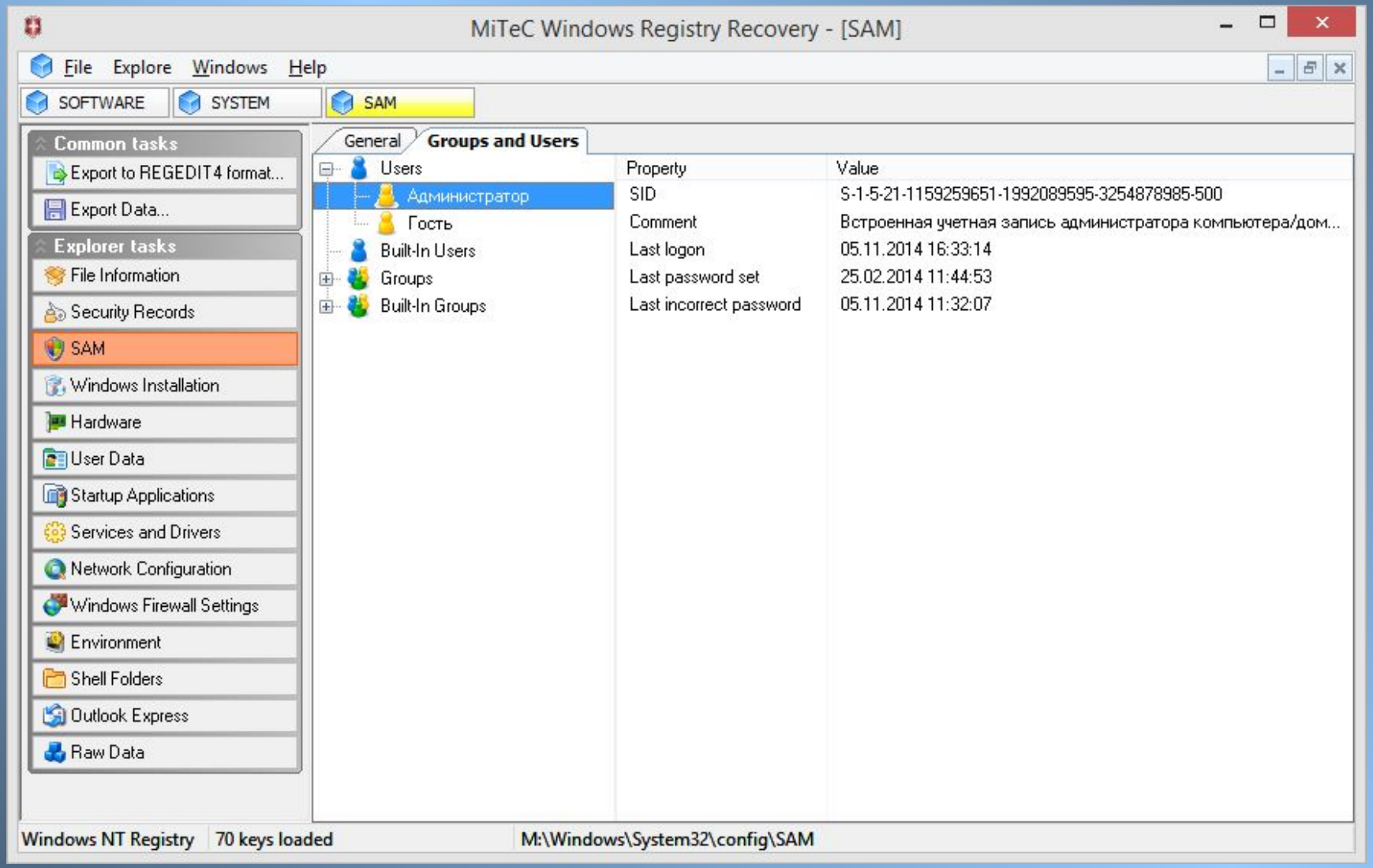
\Microsoft\Windows NT\CurrentVersion\Uninstall





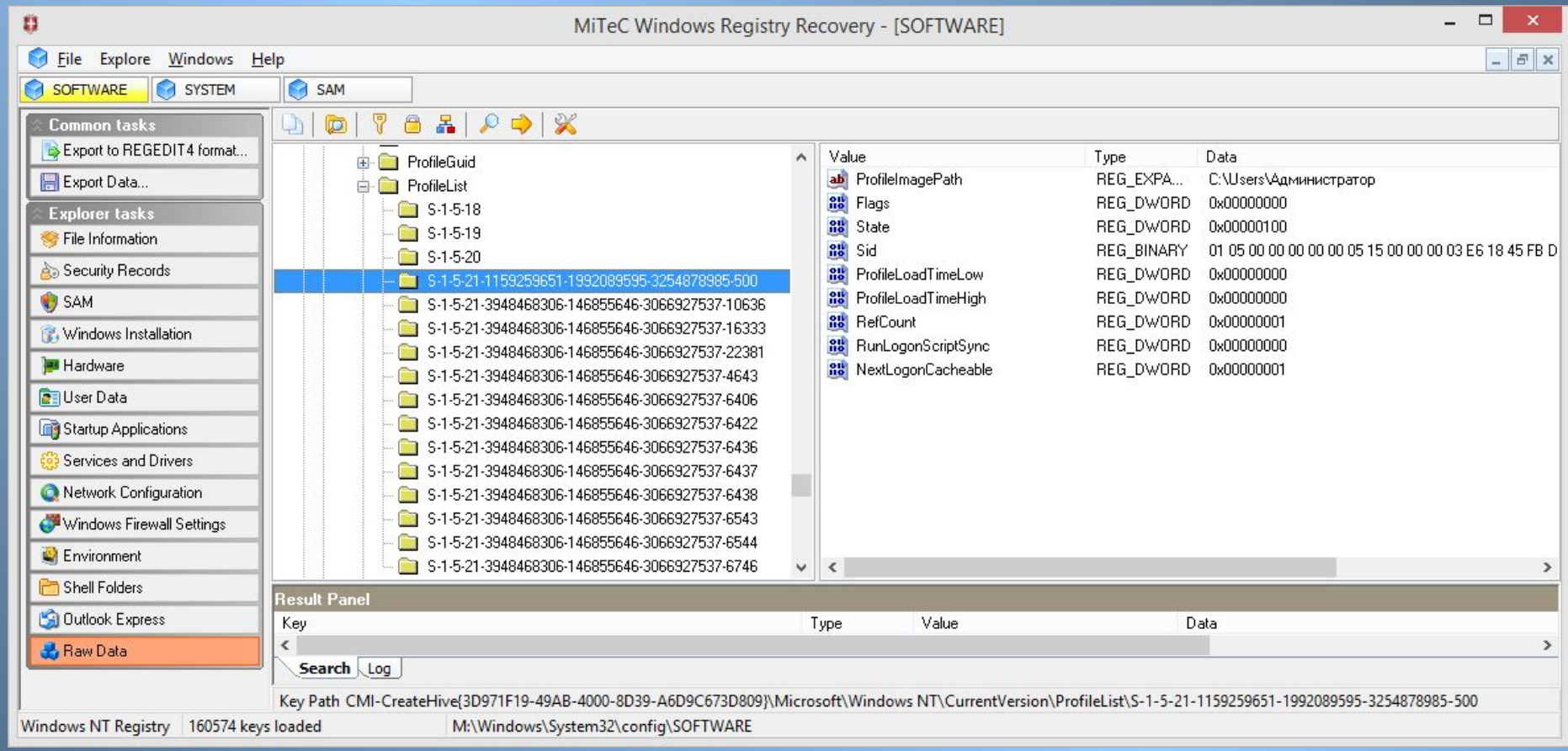
Сведения о об учетных записях в ОС

Раздел реестра HKEY_LOCAL_MACHINE\SAM



Сведения о об учетных записях в ОС

Раздел реестра HKEY_LOCAL_MACHINE\SAM



HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Содержит до 26 записей командной строки