Артефакты Windows

Матвеева Веста
ведущий специалист по компьютерной криминалистике

Основные источники доказательств

1. Реестр. Общие настройки

\Windows\System32\config (все версии ОС):

SYSTEM	HKEY_LOCAL_MACHINE\SYSTEM	аппаратные и системные настройки ОС
SOFTWARE	HKEY_LOCAL_MACHINE\SOFTWARE	настройки ПО в ОС
SAM	HKEY_LOCAL_MACHINE\SAM	настройки учетных записей в ОС
SECURITY	HKEY_LOCAL_MACHINE\SECURITY	Хранит информацию о подсистеме безопасности локального компьютера

Основные источники доказательств

2. Реестр. Настройки учетных записей

Путь до файла	Имя файла реестра	Раздел реестра	Пояснения
\Users\<имя учетной записи>\ (в Windows Vista и выше) \Documents and Settings \<имя учетной записи>\ (до Windows XP)	NTUSER.DAT	HKEY_CURRENT_USER	программные настройки учетной записи
\Users\<имя учетной записи>\ AppData\Local\Microsoft\Windows\ (в Windows Vista и выше)	UsrClass.dat	HKEY_CURRENT_USER \SOFTWARE\Classes	параметры по умолчанию, которые относятся ко всем пользователям локального компьютера.

ВАЖНО!

Временные метки разделов реестра Regedit не извлекает. Временные метки имеются только у разделов реестра, но не у отдельных ключей. При изменении значения какого либо ключа меняется значение временной метки раздела, в которой хранится этот ключ.

Раздела HKLM\SYSTEM\CurrentControlSet в неактивной ОС Вы не найдете, т.к. этот раздел динамический и формируется во время загрузки ОС на основании значения ключа HKLM\SYSTEM\Select\Current. Кроме того, привычного «HKEY_LOCAL_MACHINE\SYSTEM» и т.п. Вы также не найдете, вместо этого пути будет «$$$PROTO.HIV».

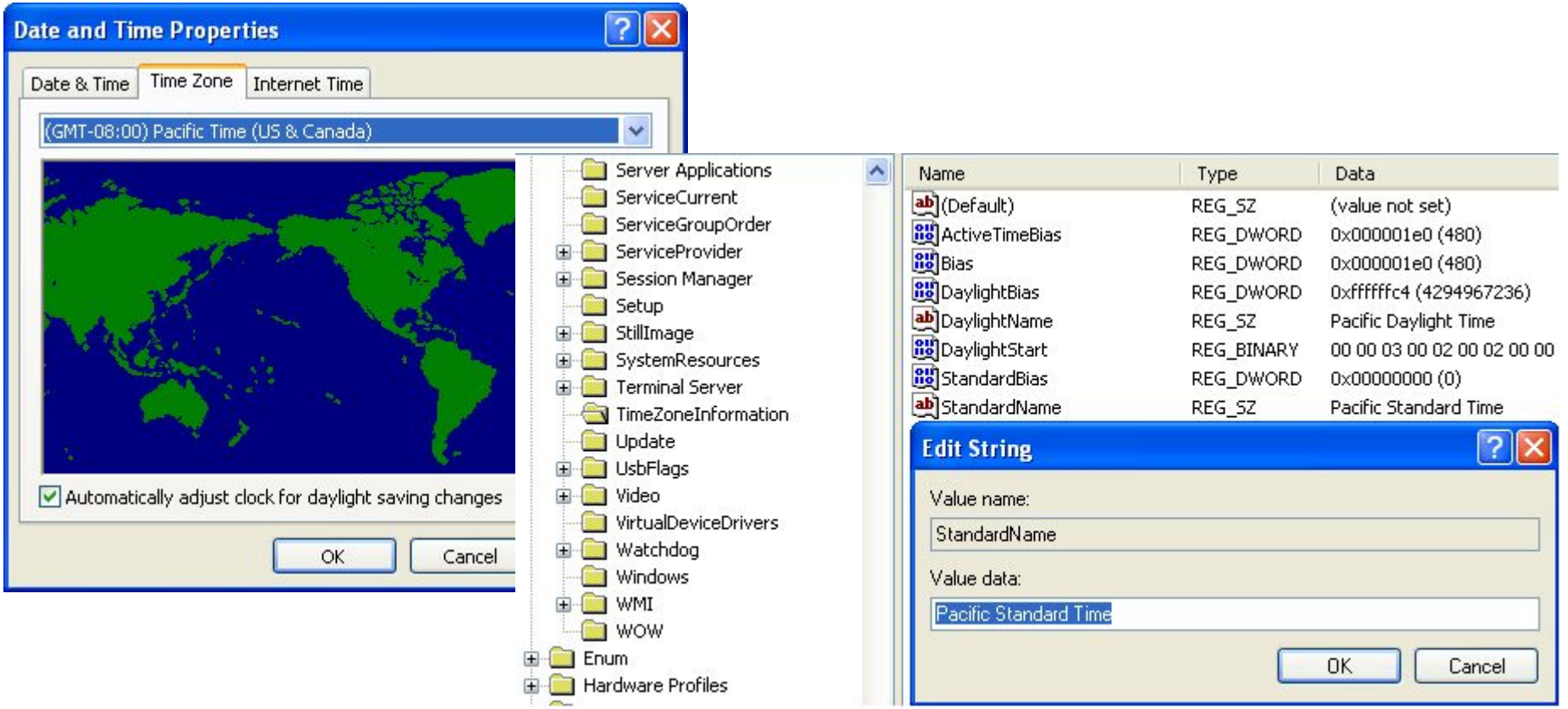
Раздел HKEY_LOCAL_MACHINE\SYSTEM

Полный путь к ключу	Название ключа
Имя компьютера	
\ControlSet00X\Control\ComputerName\ComputerName	ComputerName
Время последнего выключения компьютера (в формате Win64 DateTIme)	
\ControlSet00X\Control\Windows	ShutdownTime
Пути к ресурсам, к которым разрешен доступ по сети	
\ControlSet00X\Services\LanmanServer\Shares	-
Сетевые адаптеры, и их параметры	
\ControlSet00X\Services\Tcpip\Parameters\Interfaces	-
Разрешение входящих подключений по протоколу RDP	
\ControlSet00X\Control\Terminal Server	fDenyTSConnections
Часовой пояс	
\ControlSet001\Control\TimeZoneInformation	StandardName

Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM

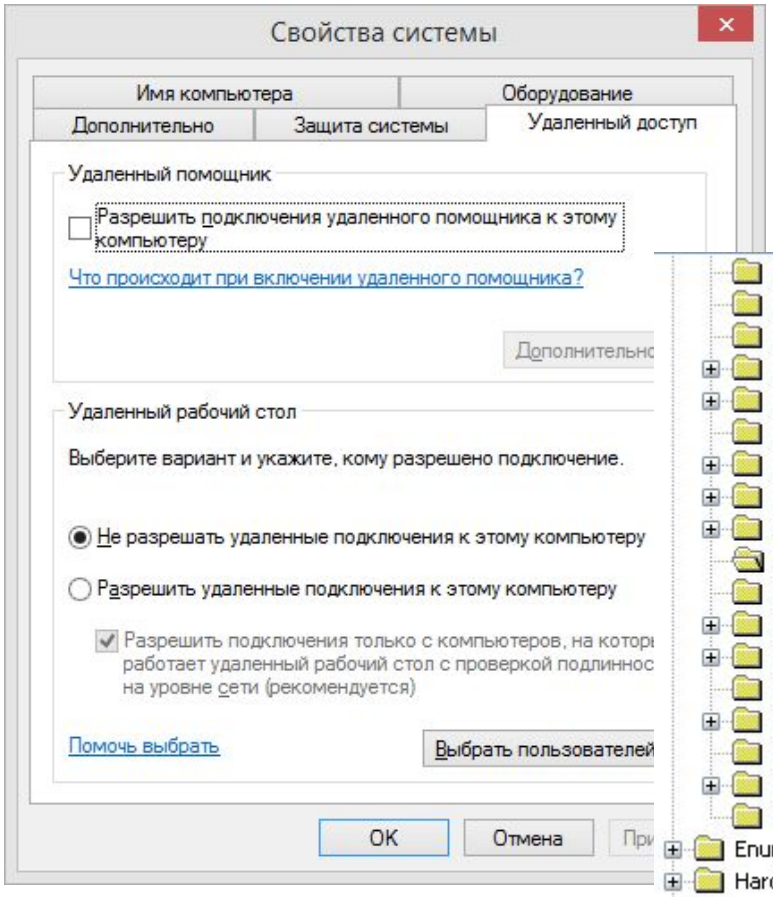
Настройки времени (текущий часовой пояс)

\ControlSet00X\Control\TimeZoneInformation

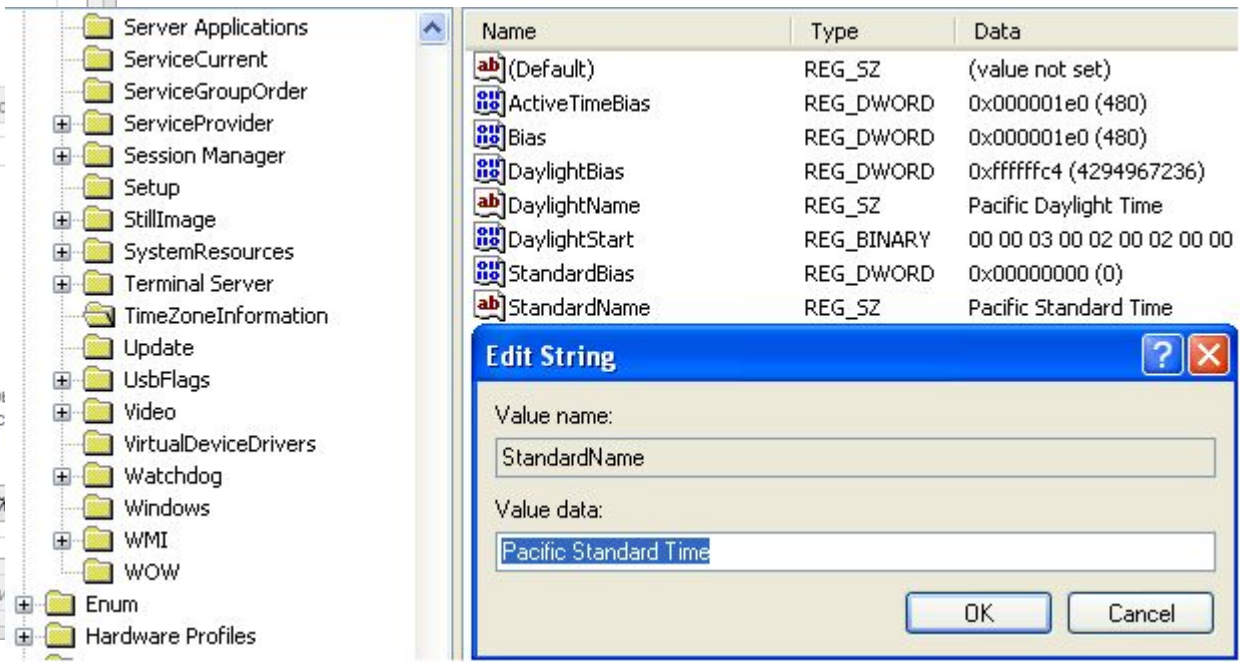


Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM

Запрет на входящие подключения по протоколу RDP



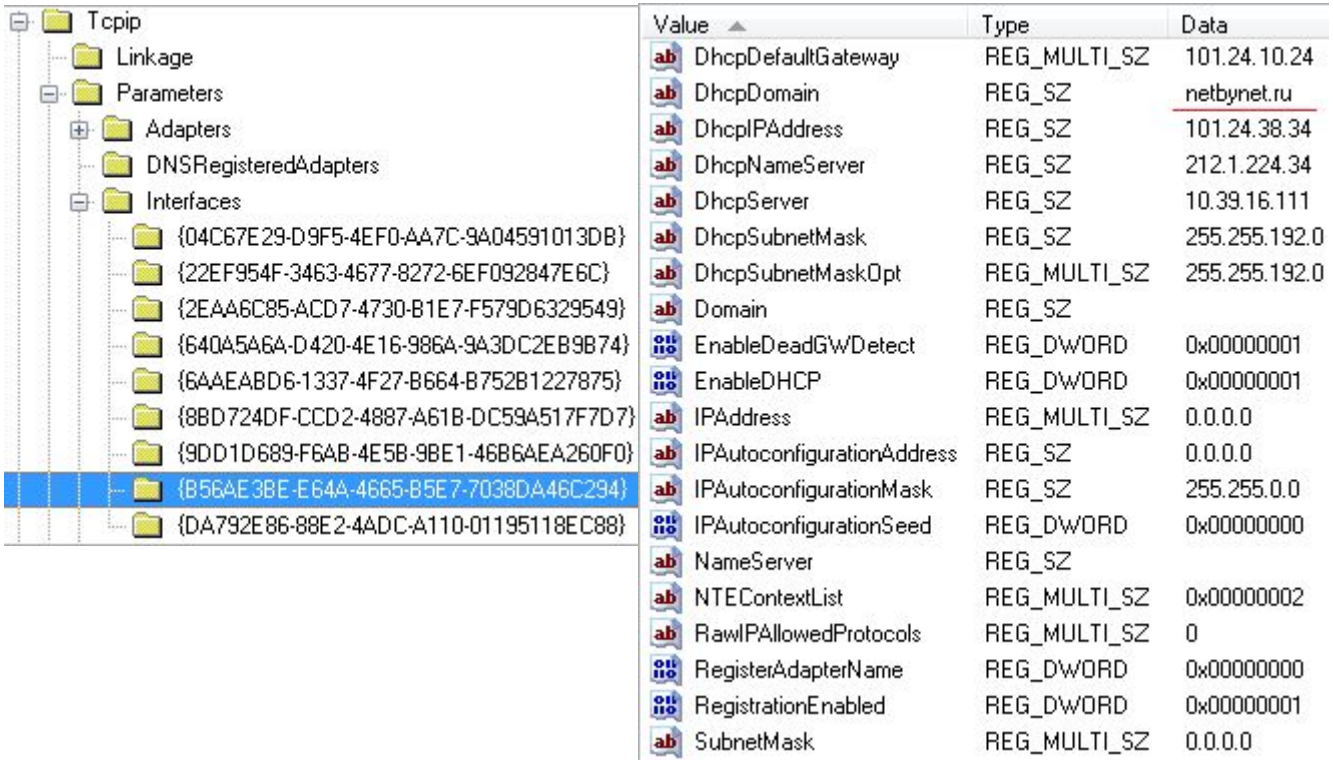
\ControlSetooX\Control\Terminal Server



Раздел реестра HKEY_LOCAL_MACHINE\SYSTEM

Сетевые настройки

\ControlSetooX\Services\Tcpip\Parameters\Interfaces



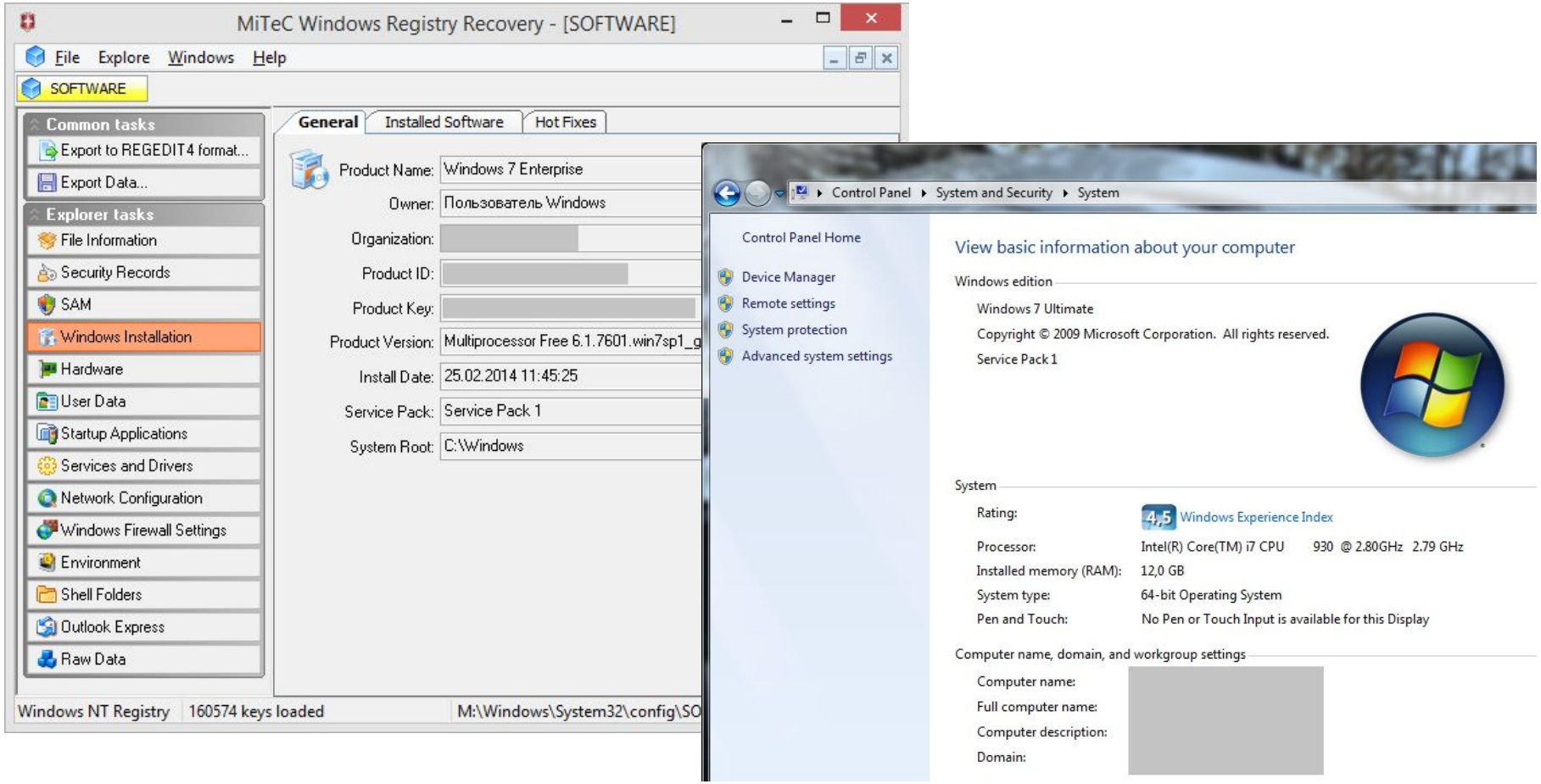
Раздел HKEY_LOCAL_MACHINE\SOFTWARE

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

Основные источники доказательств

Сведения о установленной ОС

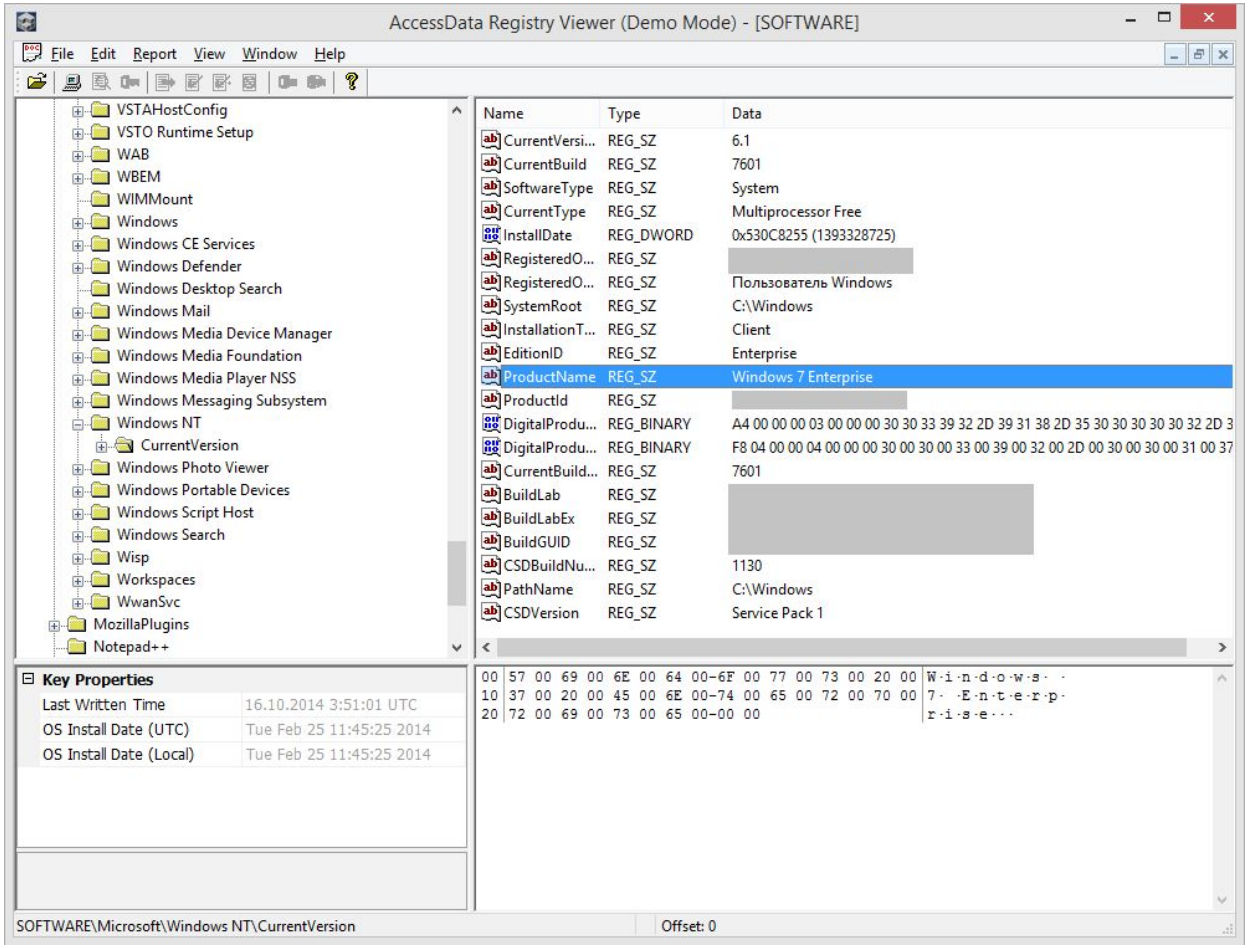
\Microsoft\Windows NT\CurrentVersion



Основные источники доказательств

Сведения о установленной ОС

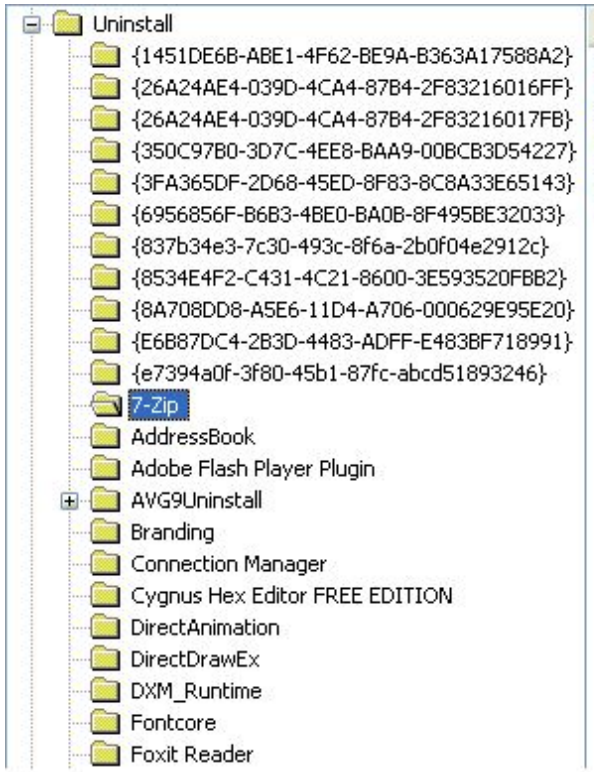
\Microsoft\Windows NT\CurrentVersion



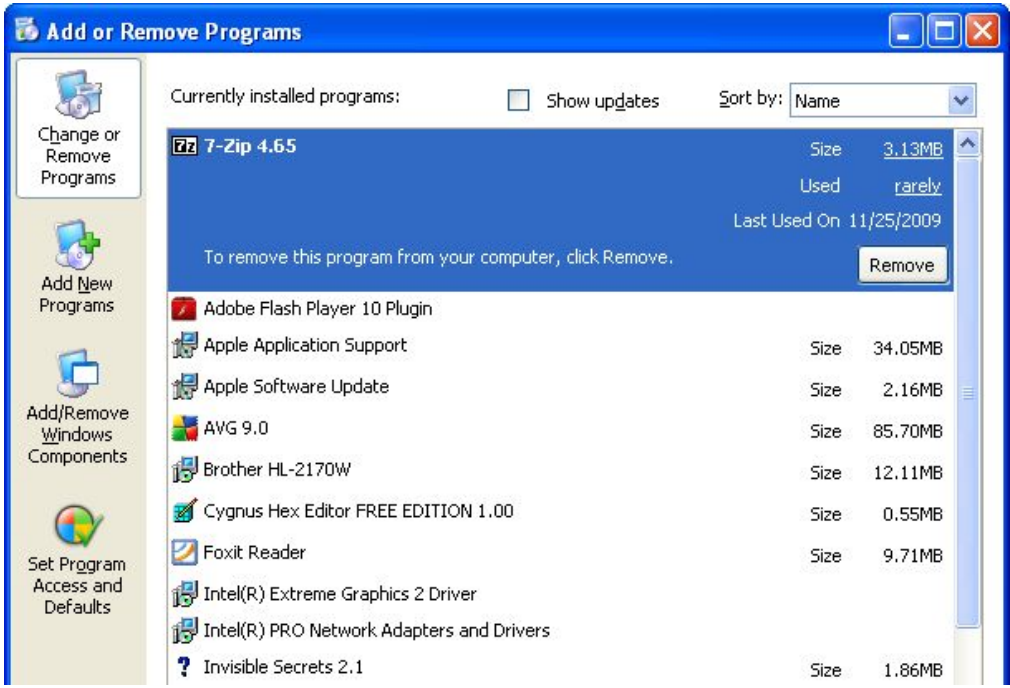
Раздел реестра HKEY_LOCAL_MACHINE\SOFTWARE

Сведения о ПО, установленном в ОС

\Microsoft\Windows NT\CurrentVersion\Uninstall

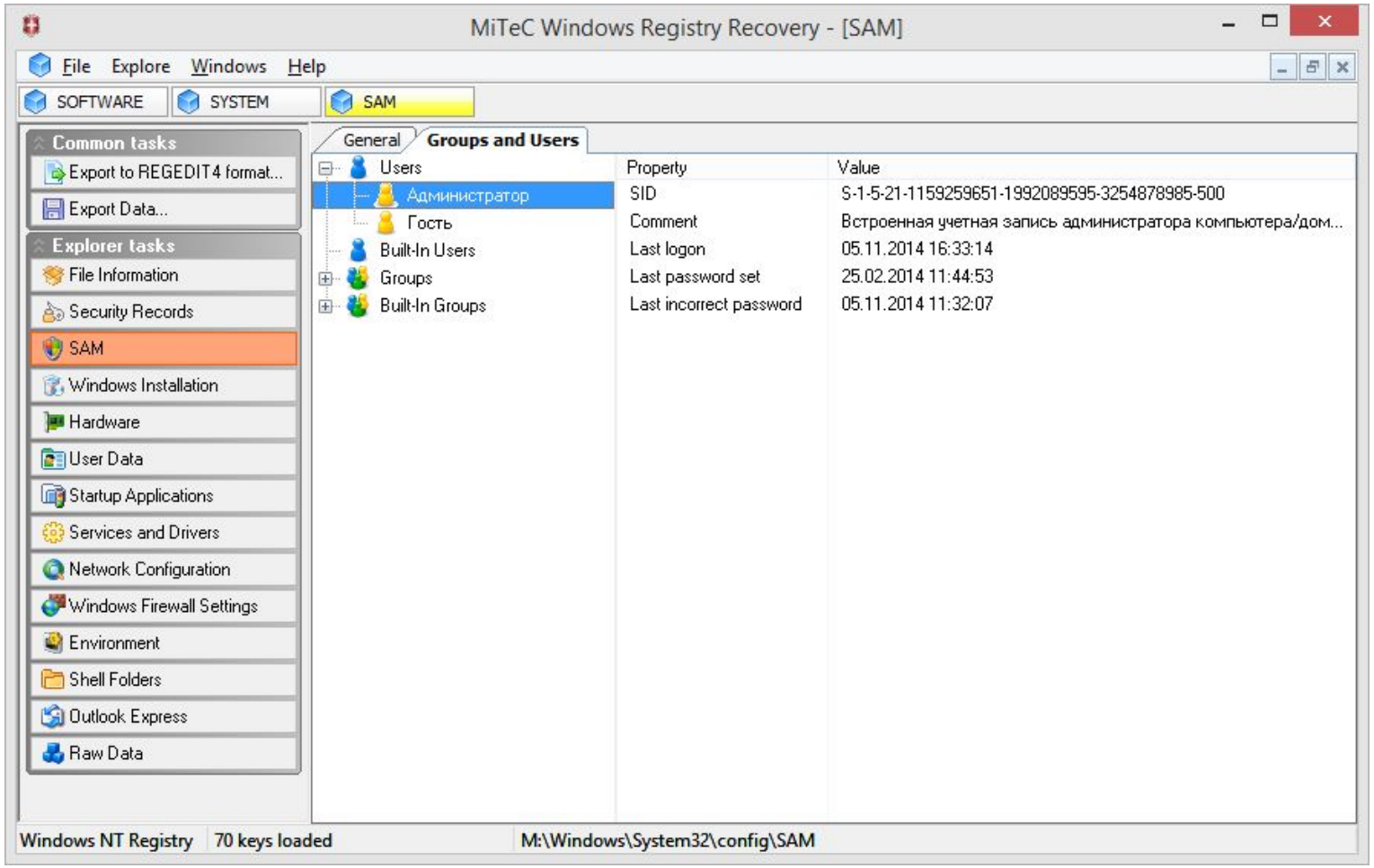


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	7-Zip 4.65
NoModify	REG_DWORD	0x00000001 (1)
NoRepair	REG_DWORD	0x00000001 (1)
UninstallString	REG_SZ	"C:\Program Files\7-Zip\Uninstall.exe"



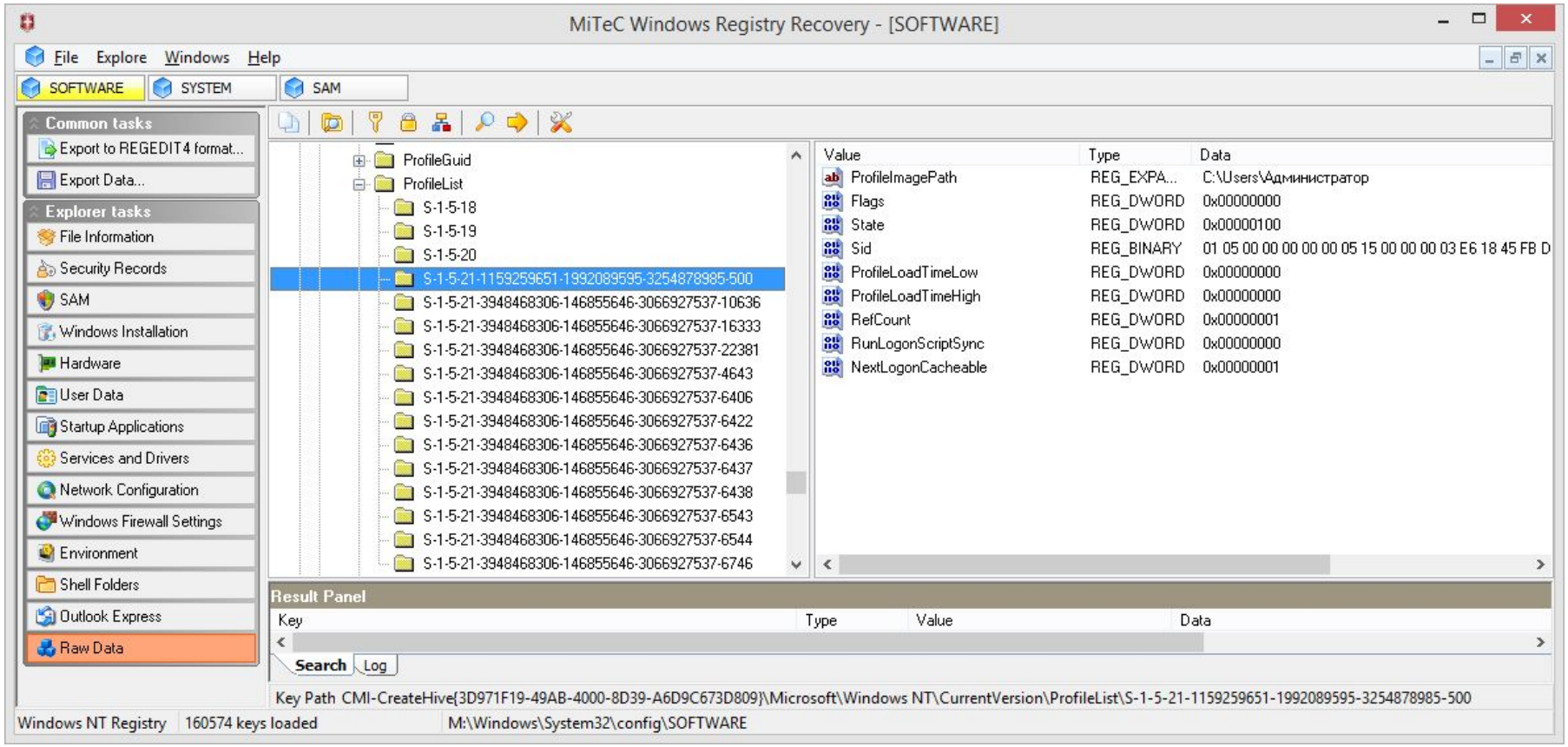
Раздел реестра HKEY_LOCAL_MACHINE\SAM

Сведения о об учетных записях в ОС



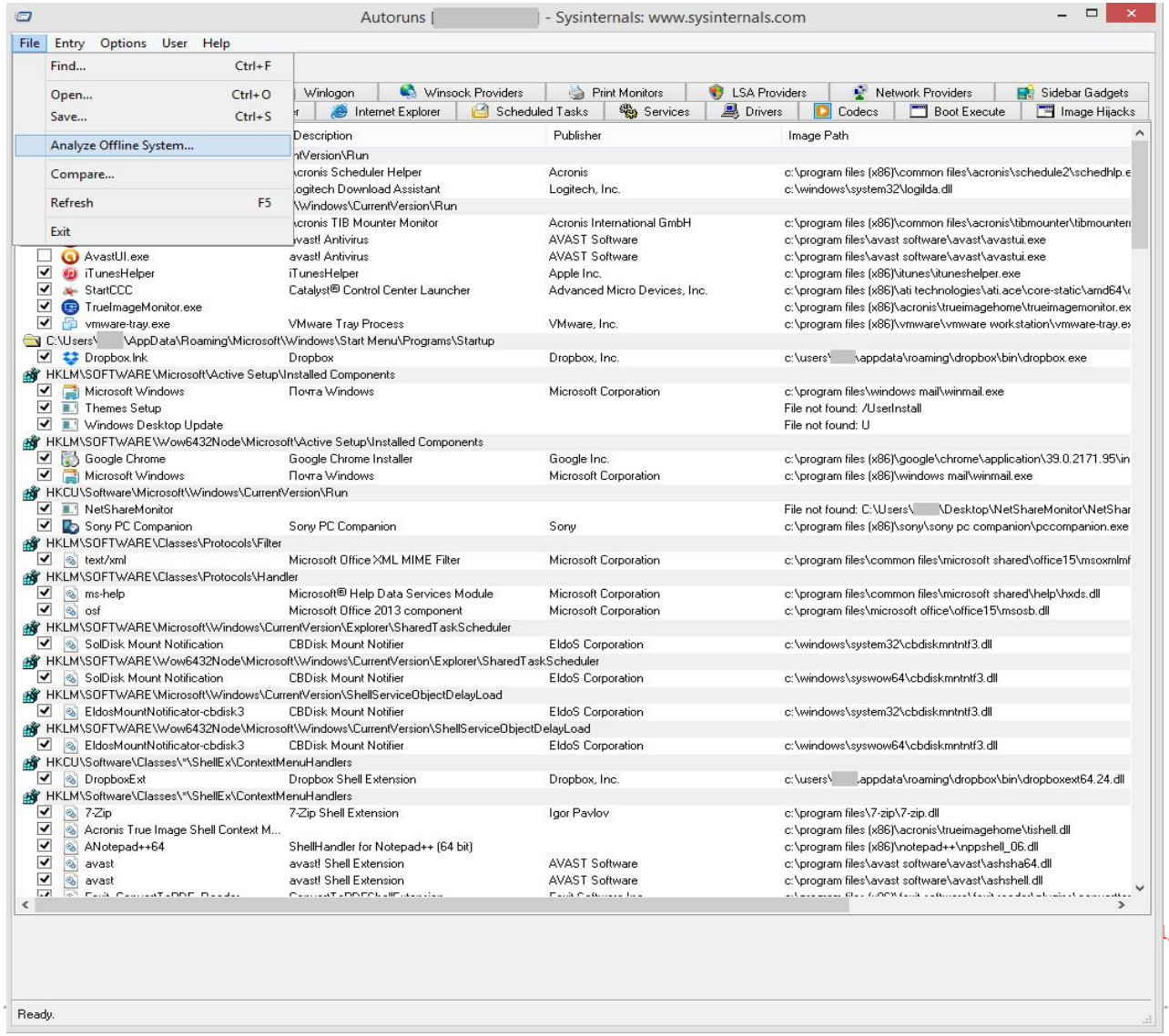
Раздел реестра HKEY_LOCAL_MACHINE\SAM

Сведения о об учетных записях в ОС



Основные источники доказательств

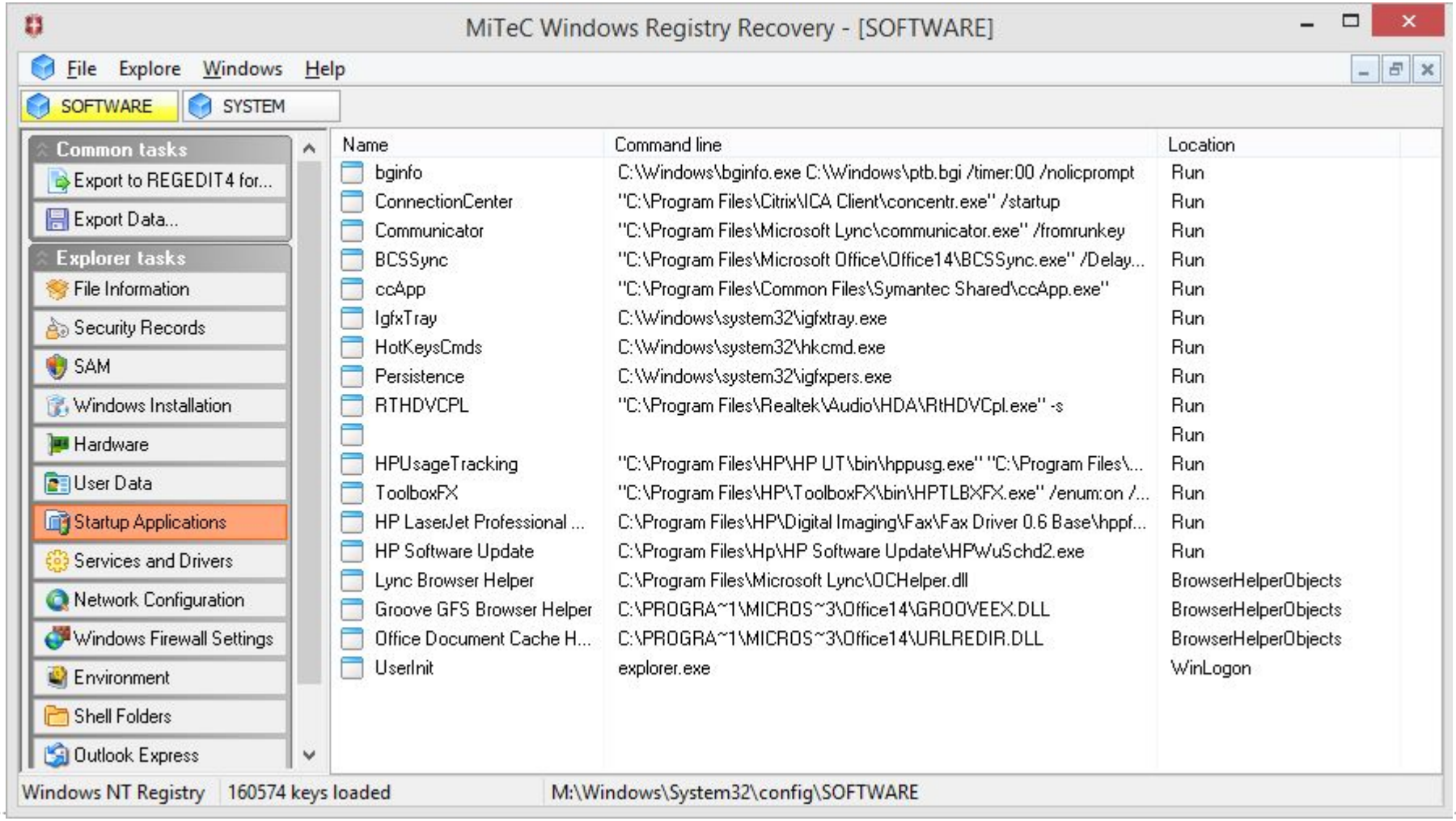
3. Автозагрузка



GROUP IB

Основные источники доказательств

3. Автозагрузка

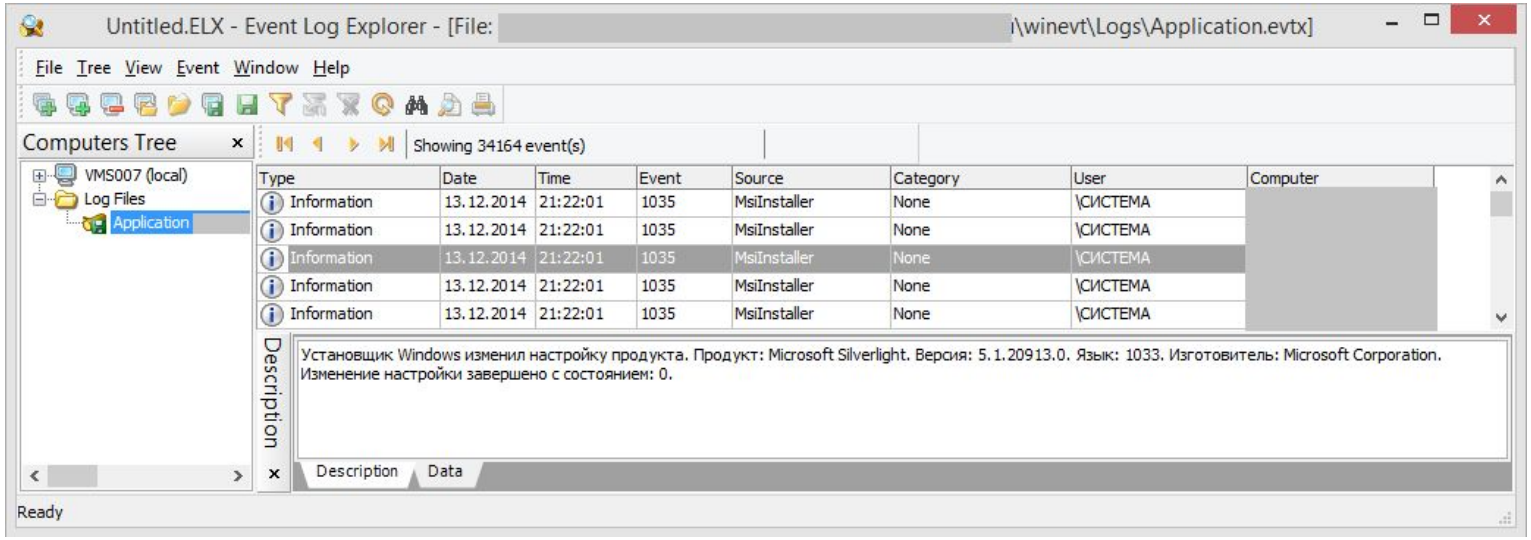


Основные источники доказательств

4. Журналы ОС

\Windows\System32\config (до Windows XP) .evt
\Windows\System32\winevt\Logs (Windows Vista и выше) .evtx

SysEvent.evt (System.evtx)	Регистрация системных событий ОС
AppEvt.evt (Application.evtx)	Регистрация программных событий ОС
SecEvent.evt (Security.evtx)	Регистрация событий аутентификации в ОС



Основные источники доказательств

5. Сетевая активность. История (ОС Microsoft Windows)

Internet Explorer
Каталог «\Documents and Settings\[имя пользователя]\Local Settings\» в Windows XP (файлы: index.dat)
Каталог «\Users\[имя пользователя]\AppData\Local\Microsoft\Windows\History» в Windows Vista, 7, 8, 8.1

Mozilla Firefox
Каталог «\Documents and Settings\[имя пользователя]\Application Data\Mozilla\Firefox\Profiles\» в Windows XP (файл: places.sqlite)
Каталог «\Users\[имя пользователя]\AppData\Mozilla\Firefox\Profiles\» в Windows Vista, 7, 8, 8.1 (файл: places.sqlite)

Google Chrome
Каталог «\Documents and Settings\[имя пользователя]\Local Settings\Application Data\Google\ Chrome\» в Windows XP (файлы: History, Archived History)
Каталог «\Users\[имя пользователя]\AppData\Local\Google\Chrome\User Data\Default» в Windows Vista, 7, 8, 8.1 (файлы: History, Archived History)

Opera
Каталог «\Documents and Settings\[имя пользователя]\Application Data\Opera\Opera\» в Windows XP (файл: global_history.dat)
Каталог «\Users\[имя пользователя]\AppData\Roaming\Opera\Opera\ » в Windows Vista, 7, 8, 8.1 (файл: global_history.dat)

Основные источники доказательств

5. Сведения о запуске программ или доступе к ним

NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\User Assist\{GUID}\Count	Программы, запущенные пользователем вручную
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ OpenSaveMRU	Программы, открытые или сохраненные через проводник
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU	Программы, открытые или сохраненные через проводник, действия с которыми производились недавно
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Запуск через Пусть -> Выполнить (Start -> Run)
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache	Доступ к исполняемым файлам (проверка совместимости)
HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache (XP, 2000, 2003) HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache (Vista, 7, 2008).	Запуск программ через проводник
\Windows\Prefetch	Кеширование запускаемых программ для ускорения работы ОС

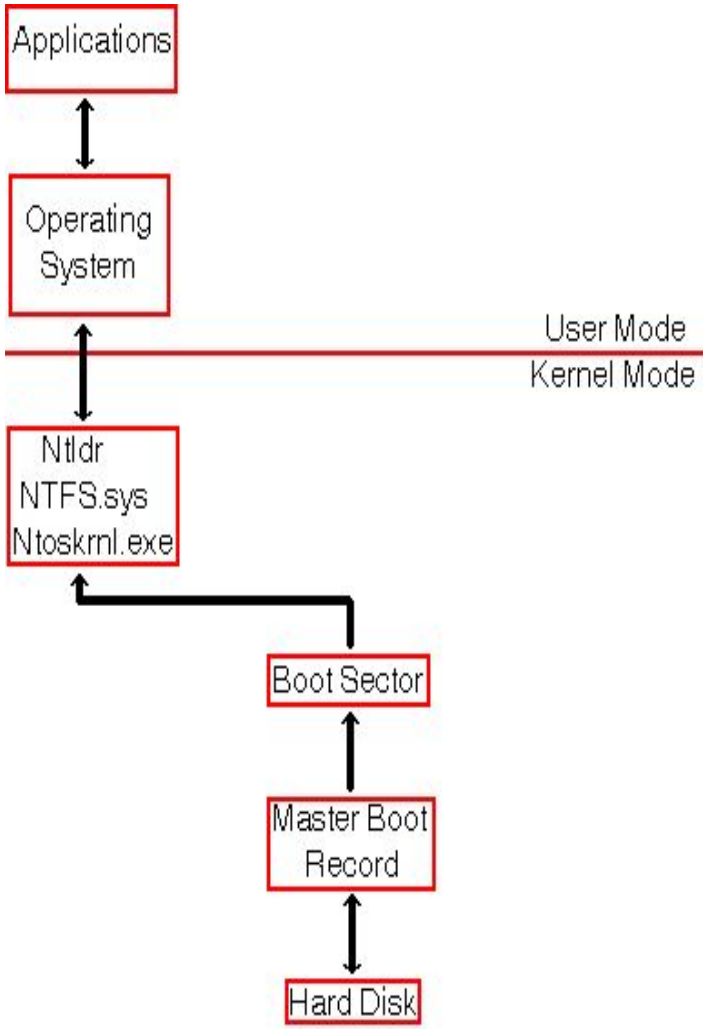
Криминалистика НЖМД

GROUP IB

Практика

- → Устанавливаем SIFT Workstation
- → Изучаем структуру НЖМД
- → Делаем таймлайн

Архитектура



Архитектура

Изучение строения НЖМД

MBR (Master Boot Record)

Смещение 0x1be – начало описания первого раздела (16 байт)

Смещение 0x1c2 – тип файловой системы (1 байт)

Смещение 0x1c6 – первый сектор раздела (4 байта)

Смещение 0x1ca – размер раздела в кластерах (4 байта)

Volume boot record

Смещение 0x28 – размер раздела в кластерах (8 байт)

Смещение 0x48 – уникальный серийный номер тома (8 байт)

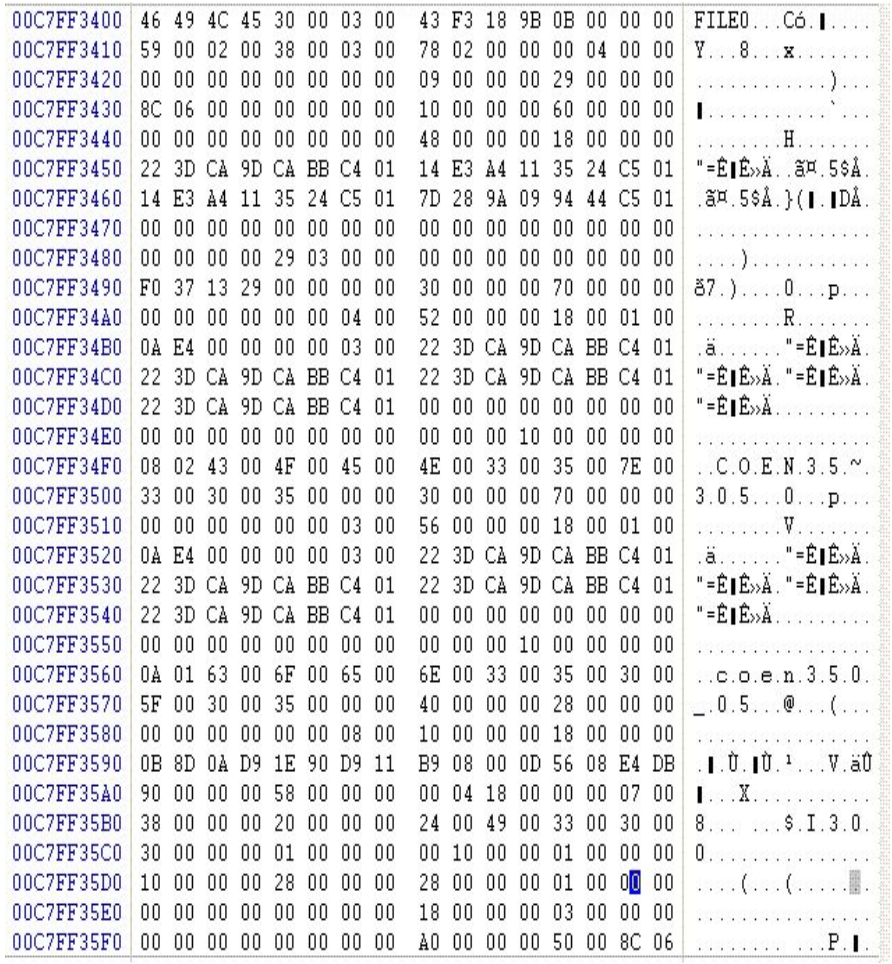
Смещение 0x0B – размер раздела в кластерах (8 байт)

Смещение 0x0D – уникальный серийный номер тома (8 байт)

1 сектор – 512 байт

1 кластер – 4096 байт

Файловые записи



```
00C7FF3400  46 49 4C 45 30 00 03 00  43 F3 18 9B 0B 00 00 00  FILE0...Có.▌....
00C7FF3410  59 00 02 00 38 00 03 00  78 02 00 00 00 04 00 00  Y...8...x.......
00C7FF3420  00 00 00 00 00 00 00 00  09 00 00 00 29 00 00 00  ............)...
00C7FF3430  8C 06 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ▌...........`...
00C7FF3440  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......
00C7FF3450  22 3D CA 9D CA BB C4 01  14 E3 A4 11 35 24 C5 01  "=Ê▌É»Ä..ã¤.5$Å.
00C7FF3460  14 E3 A4 11 35 24 C5 01  7D 28 9A 09 94 44 C5 01  .ã¤.5$Å.}(▌.▌DÅ.
00C7FF3470  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FF3480  00 00 00 00 29 03 00 00  00 00 00 00 00 00 00 00  ....)...........
00C7FF3490  F0 37 13 29 00 00 00 00  30 00 00 00 70 00 00 00  ð7.)....0...p...
00C7FF34A0  00 00 00 00 00 00 04 00  52 00 00 00 18 00 01 00  ........R.......
00C7FF34B0  0A E4 00 00 00 00 03 00  22 3D CA 9D CA BB C4 01  .ä......"=Ê▌É»Ä.
00C7FF34C0  22 3D CA 9D CA BB C4 01  22 3D CA 9D CA BB C4 01  "=Ê▌É»Ä."=Ê▌É»Ä.
00C7FF34D0  22 3D CA 9D CA BB C4 01  00 00 00 00 00 00 00 00  "=Ê▌É»Ä.........
00C7FF34E0  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00  ................
00C7FF34F0  08 02 43 00 4F 00 45 00  4E 00 33 00 35 00 7E 00  ..C.O.E.N.3.5.~.
00C7FF3500  33 00 30 00 35 00 00 00  30 00 00 00 70 00 00 00  3.0.5...0...p...
00C7FF3510  00 00 00 00 00 00 03 00  56 00 00 00 18 00 01 00  ........V.......
00C7FF3520  0A E4 00 00 00 00 03 00  22 3D CA 9D CA BB C4 01  .ä......"=Ê▌É»Ä.
00C7FF3530  22 3D CA 9D CA BB C4 01  22 3D CA 9D CA BB C4 01  "=Ê▌É»Ä."=Ê▌É»Ä.
00C7FF3540  22 3D CA 9D CA BB C4 01  00 00 00 00 00 00 00 00  "=Ê▌É»Ä.........
00C7FF3550  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00  ................
00C7FF3560  0A 01 63 00 6F 00 65 00  6E 00 33 00 35 00 30 00  ..c.o.e.n.3.5.0.
00C7FF3570  5F 00 30 00 35 00 00 00  40 00 00 00 28 00 00 00  _.0.5...@...(...
00C7FF3580  00 00 00 00 00 00 08 00  10 00 00 00 18 00 00 00  ................
00C7FF3590  0B 8D 0A D9 1E 90 D9 11  B9 08 00 0D 56 08 E4 DB  .▌.Ù.▌Ù.¹...V.äÛ
00C7FF35A0  90 00 00 00 58 00 00 00  00 04 18 00 00 00 07 00  ▌...X...........
00C7FF35B0  38 00 00 00 20 00 00 00  24 00 49 00 33 00 30 00  8... ...$.I.3.0.
00C7FF35C0  30 00 00 00 01 00 00 00  00 10 00 00 01 00 00 00  0...............
00C7FF35D0  10 00 00 00 28 00 00 00  28 00 00 00 01 00 00 00  ....(...(.....▒.
00C7FF35E0  00 00 00 00 00 00 00 00  18 00 00 00 03 00 00 00  ................
00C7FF35F0  00 00 00 00 00 00 00 00  A0 00 00 00 50 00 8C 06  ........ ...P.▌.
```

0x10 STANDARD_INFORMATION
0x30 $FILE_NAME0
0x60 $VOLUME_NAME
0x80 $DATA

Временные атрибуты

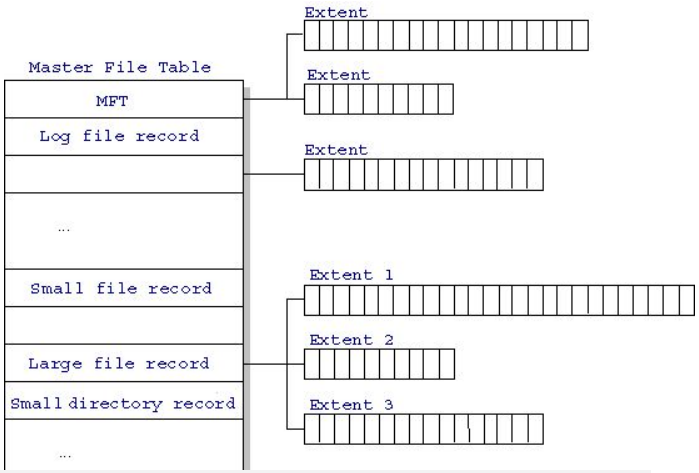
0x00	8		File Creation Time
0x08	8		File Alteration Time
0x10	8		MFT Change
0x18	8		File Read Time
0x20	4		DOS File Permissions
0x24	4		Maximum number of versions
0x28	4		Version number
0x2C	4		Class ID
0x30	4	2 K	Owner ID

Создание таймлайна

GROUP IB

NTFS

Временные метки
- Creation time
- Last accessed time
- Last written time
- Last Modification time



System File	File Name	MFT Record	Purpose of the File
Master file table	$Mft	0	Contains one base file record for each file and folder on an NTFS volume. If the allocation information for a file or folder is too large to fit within a single record, other file records are allocated as well.
Master file table 2	$MftMirr	1	A duplicate image of the first four records of the MFT. This file guarantees access to the MFT in case of a single-sector failure.
Log file	$LogFile	2	Contains a list of transaction steps used for NTFS recoverability. Log file size depends on the volume size and can be as large as 4 MB. It is used by Windows NT/2000 to restore consistency to NTFS after a system failure.
Volume	$Volume	3	Contains information about the volume, such as the volume label and the volume version.
Attribute definitions	$AttrDef	4	A table of attribute names, numbers, and descriptions.
Root file name index	$	5	The root folder.
Cluster bitmap	$Bitmap	6	A representation of the volume showing which clusters are in use.
Boot sector	$Boot	7	Includes the BPB used to mount the volume and additional bootstrap loader code used if the volume is bootable.
Bad cluster file	$BadClus	8	Contains bad clusters for the volume.
Security file	$Secure	9	Contains unique security descriptors for all files within a volume.
Upcase table	$Upcase	10	Converts lowercase characters to matching Unicode uppercase characters.
NTFS extension file	$Extend	11	Used for various optional extensions such as quotas, reparse point data, and object identifiers.
		12-15	Reserved for future use.

Создание таймлайна

- SIFT Workstation (http://davnads.blogspot.com/2012/12/4n6time-release-notice.html)
- Plaso (http://plaso.kiddaland.net/)
- 4n6time (http://davnads.blogspot.com/2012/12/4n6time-release-notice.html)

Timeline

Просмотр наличия ФС на образе

mmls <путь к файлу образа>

Запомнить смещение в секторах!

У нас 63. В байтах 512*63=32256

Монтирование образа в режиме чтения

sudo mount –t ntfs-3g -o ro,loop,nodev,noexec,show_sys_files,streams_interf

=windows,offset=32256 /cases/DBO/raw.dd /mnt/windows_mount

Извлечение MFT

icat -i raw -f ntfs -o 63 /cases/DBO/raw.dd 0 > /cases/DBO/raw.mft

Timeline

Конвертация MFT

cd /cases/DBO/

log2timeline -f mft -z Europe/Moscow -m C: raw.mft -w timeline.csv

log2timeline-sift –z EST5EDT –p 0 –i partition.dd

Создание timeline

log2timeline -p -r -f winxp -z Europe/Moscow /mnt/windows_mount -w timeline.csv

Обработка TimeLine

l2t_process -b timeline.csv MM-DD-YYYY..MM-DD-YYYY

Работа с ФС

fls –o 63 raw.dd

Просмотр атрибутов файлов

istat –o 63 raw.dd <node number>

Матвеева Веста

+7 (495) 984-33-64 доб.313

matveeva@group-ib.ru

+7 (495) 984-33-64 www.group-ib.ru info@group-ib.ru

facebook.com/group-ib twitter.com/group-ib