ТЕМА 5. Компьютерная информация: обнаружение и анализ

Практическое занятие 5.3.

Учебные вопросы:

1. Криминалистический анализ СКТ (электронных носителей информации) средствами операционной системы.
2. Криминалистический анализ системных файлов, файлов реестра, хронологии событий операционной системы.

1. Криминалистический анализ СКТ (электронных носителей информации) средствами операционной системы

Краткие теоретические сведения:

Криминалистическое исследование компьютерной (электронной, машинной) информации и техники является одним из самых молодых направлений в криминалистике. Данное направление начало складываться в первой половине 90-х гг. XX в. В настоящее время указанные исследования проводятся практически по всем категориям уголовных дел. Наиболее часто исследования компьютерной информации и техники проводятся при расследовании следующих видов преступлений: в сфере информационной безопасности; терроризм и экстремизм, экономические и налоговые преступления, распространение порнографической продукции, преступных нарушений авторских и смежных прав, изготовление поддельной печатной продукции (например, бланков документов, денежных знаков, ценных бумаг). Экспертизы компьютерной информации стали повседневным явлением при рассмотрении гражданских, уголовных и административных дел.

Перед лицом производящем исследование ставится вопрос о получении информации об исследуемом объекте, установленном на него программном обеспечении, его структуры, файловой системе и т.д. В ходе исследования используется как встроенный функционал средств компьютерной техники, так и стороннее программное обеспечение. Таковыми служат стандартные средства операционных систем (Microsoft, Linux, Mac OS), пакет программ «Microsoft Office», криминалистический программный комплекс «EnCase», программный комплекс «Belkasoft» и др.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Перезагрузите компьютер. Войдите в систему BIOS.
2. В разделах «System Information, Device Configuration, Boot Option Properties» ознакомьтесь с информацией о рабочей станции, подключённых устройствах, а также порядка загрузки устройств. Обратить внимание на раздел «Boot Option Properties», где может содержаться информация об установленных операционных системах семейства Windows, Linux и т.д.

3. Перезагрузите компьютер.

4. При помощи встроенного функционала операционной системы ознакомится с базовой информацией об ОС (стандартной подпрограммы «Сведения о системе» (Win+R → msinfo32 → Enter), командная строка (Win+R → cmd → Enter → cd C:\Windows\System32 → systeminfo)).

5. При помощи встроенного функционала операционной системы ознакомится с учетными записями, зарегистрированными в ОС (кликнуть правой кнопкой мыши на ярлык «Мой компьютер» → Управление → Локальные пользователи и группы → Пользователи, либо Win+R → cmd → Enter → net user → Enter).

6. При помощи встроенного функционала операционной системы ознакомится с подключенными носителями информации (Win+R → diskmgmt.msc → Enter, либо Win+R → msinfo32 → Enter → Компоненты → Запоминающие устройства, USB).

7. Продемонстрируйте результаты преподавателю.

Используя полученные знания об основных функциональных возможностях BIOS, подготовьте файл-отчет, в котором выполните следующие действия[1]:

8.1. С помощью базовой системы ввода-вывода BIOS заполните таблицу:

Элемент системы	**Значение**
Конфигурация системы	
Подключенные устройства	
Порядок загрузки устройств	

8.2. При помощи встроенного функционала ОС заполните таблицу базовой информации об операционной системе:

Наименование операционной системы	
Версия	
Дата установки	
Системный каталог	

8.3. При помощи встроенного функционала ОС заполните таблицу структуры накопителей рабочей станции:

Описание	**Тип файловой системы**	**Объем всего**	**Распределенный объем**	**Свободный объем**

.

9. Продемонстрируйте файл-отчет преподавателю.

10. Подготовьте ответы на контрольные вопросы (см. ниже).

[1] Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (*например: «0341 Иванов 2.3»).* Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Какая информация о рабочей станции содержится в базовой системе ввода-вывода BIOS?
2. При исследовании системы BIOS на какие свойства необходимо акцентировать свое внимание?
3. Какие семейства операционных систем вы знаете?
4. Какие комбинации клавиш ОС семейства Microsoft Windows вы знаете для открытия окна «Выполнить», параметров Windows?
5. Каким образом запустить командную строку ОС семейства Microsoft Windows?
6. Каким образом можно узнать базовую информацию об операционной системе семейства Microsoft Windows?
7. Каким образом можно узнать информацию о зарегистрированных пользователях в ОС семейства Microsoft Windows?
8. Каким образом можно узнать информацию о подключенных накопителях информации в ОС семейства Microsoft Windows?

2. Криминалистический анализ системных файлов, файлов реестра, хронологии событий операционной системы

Краткие теоретические сведения:

2.1 *анализ системных файлов*

К системным файлам относятся файлы Thumbs, Pagefile, Hyberfil и папки System Volume Information и Recycle.bin

Скрытые системные папки и файлы необходимы для оптимизации работы операционной системы Windows 10 и др. Изменение, перемещение или удаление некоторых системных файлов и папок выводит систему из строя, поэтому по умолчанию они скрыты от пользователя.

С отсутствием или проблемами доступа к этим файлам могут быть связаны и ошибки в меню Пуска Windows 10 и неполадки в работе спящего режима (гибернации). Давайте рассмотрим подробнее основные системные файлы и папки Windows 10 и для чего они используются.

Восстановление системы — System Volume Information.

В System Volume Information сохраняются файлы, позволяющие восстановить состояние системы в случае серьезных сбоев. Точки восстановления создаются автоматически или вручную. В Windows 10 восстановление системы отключено по-умолчанию. Эта чрезвычайно полезная функция должна быть включена пользователем для создания бэкапа установленных приложений, реестра Windows, системных файлов и настроек.

Владельцы слабых ПК и любители видеоигр часто отключают восстановление Windows, пытаясь повысить производительность системы. В случае отказа от резервного копирования или удаления точек восстановления из System Volume Information, Windows невозможно восстановить.

Для устранения любого серьезного сбоя придется переустанавливать систему или через загрузку в безопасном режиме вручную заменять поврежденные файлы.

Корзина — файл Recycle.bin.

Файл Recycle.bin выполняет функции, связанные с удалением файлов.

Сейчас многие версии операционных систем используют временное хранилище для удаления файлов. Пользователь может задать размер Корзины или уничтожать файлы в обход папки Recycler. Некоторые файлы подлежат восстановлению даже после их удаления через Recycle.bin.

Кеширование эскизов изображений — Thumbs.db.

Скрытый файл Thumbs.db создается в папках с сохраненными изображениями. Единственной его функцией является создание уменьшенных копий (эскизов) просмотренных графических файлов. Пользователь может в любой момент удалить Thumbs.db.

Подобное действие не навредит системе, так как файл будет создан заново. Функцию можно отключить, но на слабых ПК подобное решение приведет к снижению производительности. Не рекомендуется передавать файл Thumbs посторонним лицам, так как они получат доступ к конфиденциальной информации, сохраненной в эскизах.

Виртуальный файл подкачки — Pagefile.sys.

Файл подкачки Pagefile.sys необходим для освобождения оперативной памяти, путем перемещения неактивных фрагментов из ОЗУ на накопитель. Как и Thumbs.db, файл подкачки сохраняет информацию о пользователе. Некоторые программы отключают Pagefile.sys на время своей работы. Пользователь дополнительно может очистить временные swap-файлы, но удалить сам файл подкачки невозможно.

Гибернация или спящий режим — Hiberfil.sys.

Для перевода ПК в спящий режим используется файл Hiberfil.sys, сохраняющий дополнительную информацию о текущем сеансе. После возобновления работы система возвращается в прежнее состояние. Гибернация позволяет регулировать расход заряда батареи во время автономной работы ноутбуков и планшетных компьютеров.

При необходимости можно самостоятельно задать размер файлов Pagefile и Hiberfil, в зависимости от объёма установленной оперативной памяти.

Вирусы часто подменяют файлы в системных папках, нарушая тем самым работу ОС. Продуманный менеджмент перечисленных папок и файлов позволяет избавиться от вредоносного программного обеспечения, дополнительно скрыв конфиденциальную информацию, которая извлекается злоумышленниками путем изучения разделов системного диска.

2.2. Криминалистический анализ реестра ОС Windows

Совершение правонарушений с использованием современных информационных технологий в наше время стало достаточно распространенным явлением. Компьютер - одно из самых распространенных средств совершения опасных и латентных преступлений. Как известно,

механизм совершения преступлений, использующих компьютерные технологии, предполагает внесение изменений в информационную среду компьютерных систем. Данные изменения и являются следами совершения преступлений. Однако в силу своей специфичности следы в информационной среде могут быть исследованы только специалистом, экспертом в области компьютерных информационных технологий.

Изучение следов в компьютерных устройствах связано с получением служебной информации, которая указывает на обстоятельства совершения преступлений. К такого рода информации относятся данные, хранящиеся в системном реестре Windows. Как показывает экспертная практика, системный реестр часто используется для решения таких задач, как определение факта использования зарегистрированным пользователем какой-либо программы, устройства внешней памяти и его содержимого, средств сетевой связи, времени инициализации и длительности этих событий. Без исследования реестра исследование информационной среды компьютера нельзя считать полным и объективным, поскольку значительная часть других областей следообразования имеет достаточно простую структуру и могут подвергаться корректировке со стороны злоумышленника.

Для уничтожения следов в реестре требуется знание программирования, поскольку известные программные средства не могут воздействовать на большинство следов, возникающих в нем в результате активности пользователя. Поэтому системный реестр является той областью, которую необходимо исследовать с целью получения объективной информации о событиях в системе.

Краткое описание структуры реестра

Физически Windows организует реестр в виде кустов или ульев («hive» - англ.), хранящихся в двоичных файлах. Кроме того, для каждого улья ОС создает дополнительные файлы, которые содержат резервные копии улья.

Физически ульи существуют только в двух корневых ключах: HKLM и HKU. Остальные являются ссылками на подключи этих двух корневых ключей.

Список загруженных ульев находится в разделереестраHKLM\SYSTEM\CurrentControlSet\ Control\hivelist. Можно заметить, что в этом ключе записаны значения с названиями двух видов: \REGISTRY\MACHINE* и \REGISTRY\ USER*. Первая группа относится к ульям HKLM, а вторая - к ульям HKU. Значения обеих групп имеют строковый тип и содержат путь до файла улья вида \Device\HarddiskVolumeN*, где \Device\HarddiskVolumeN обозначает логический раздел диска.

Ульи HKLM содержатся в файлах вида %SystemRoot%\System32\config*. Расположение файлов улья HKLM можно наглядно увидеть в табл. 1.

Название	Файл
\REGISTRY\MACHINE\HARDWARE	
\REGISTRY\MACHINE\SAM	%SystemRoot%\System32\config\sam
\REGISTRY\MACHINE\SECURITY	%SystemRoot%\System32\config\security

\REGISTRY\MACHINE\SOFTWARE	%SystemRoot%\System32\config\software
\REGISTRY\MACHINE\SYSTEM	%SystemRoot%\System32\config\system

HARDWARE содержит карту и описание аппаратных ресурсов. Этот улей единственный, не записанный в файле. Дело в том, что данный раздел формируется динамически при запуске операционной системы и не сохраняется после выключения. Сама конфигурация оборудования (профили) хранится в другом месте, а именно в одном из ключей HKLM\ SYSTEM\CurrentControlNNN\Enum.

SAM и SECURITY содержат базу данных локальной безопасности, в первом ключе хранятся локальные пользователи и группы, во втором - прочие установки безопасности.

SOFTWARE содержит настройки прикладных приложений (и некоторые системные). Чаще всего данные хранятся в ключах с путем следующего вида: HKLM\SOFTWARE\ VendorName\ ProgramName\Version.

В SYSTEM хранятся системные настройки, в ключах вида HKLM\SYSTEM\ControlSetNNN хранятся настройки различных конфигураций. Чаще всего в системах присутствуют 2 конфигурации (текущая и последняя успешная), однако всего может быть до четырех конфигураций. HKLM\SYSTEM\CurrentControlSet является ссылкой на один из профилей, а содержимое ключа HKLM\SYSTEM\Select указывает на то, какой из профилей является текущим.

Ульи HKU хранятся в файлах ntuser.dat и UsrClass.dat, расположенных в разных местах. Стоит заметить, что расположение файлов различное в разных версиях Windows. В табл. 2 находится информация для системы Windows.

Название	Файл
\REGISTRY\USER\.DEFAULT	%SystemRoot%\System32\config\default
\REGISTRY\USER\S-1-5-19	%SystemRoot%\ServiceProfiles\LocalService\ntuser.dat
\REGISTRY\USER\S-1-5-20	%SystemRoot%\ServiceProfiles\NetworkService\ntuser.dat
\REGISTRY\USER\SID	%UserProfile%\ntuser.dat
\REGISTRY\USER\SID_Classes	%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat

.DEFAULT содержит настройки пользователя, которые Windows применяет еще до входа какого-либо пользователя в систему.

S-1-5-19 (20) являются SID для учетных записей LocalService и NetworkService, нужны для запуска служб с правами данных учетных записей.

SID содержит различные пользовательские настройки, а SID_Classes регистрацию классов и ассоциацию файлов.

Логическая структура реестра похожа на структуру файловой системы. Реестр состоит из «ключей» (аналоги каталогов в файловых системах), при этом ключи могут быть вложены друг в друга. В ключах находятся «значения» (аналоги файлов), каждое из которых обладает следующими параметрами: именем (до 512 символов ANSI или до 256 символов UNICODE, за исключением символов (\), (?), (*)), типом (например, числовой тип

«REG_DWORD»; типы данных будут описаны позже) и содержащимися в значении данными.

В «корне» реестра находятся несколько корневых ключей, некоторые из которых являются ссылками на другие места в реестре.

Корневые ключи реестра:

- HKEY_CLASSES_ROOT (HKCR) содержит информацию о всех расширениях файлов, зарегистрированных в системе, и о классах объектов COM. Является объединением ключей HKLM\Software\Classes и HKCU\Software\Classes, причем более высокий приоритет имеет значение, записанное в последнем ключе (то есть если в обоих ключах есть одинаковые значения, то в HKCR записывается значение из HKCU\Software\Classes);

- HKEY_CURRENT_USER (HKCU) содержит параметры принтеров, ПО, раскладок клавиатуры и других настроек для пользователя, вошедшего в систему. Является ссылкой на HKU\SID вошедшего пользователя;

- HKEY_LOCAL_MACHINE (HKLM) содержит настройки компьютера, общие для всех пользователей: настройки аппаратного и программного обеспечения, настройки безопасности, настройки системы;

- HKEY_USERS (HKU) содержит настройки пользователей. В данном ключе содержится минимум 5 подключей: настройки до входа под какой-то учетной записью (.DEFAULT), учетная запись LocalSystem (S-1-5-18), LocalService (S-1-5-19), NetworkService (S-1-5-20) и Administrator;

- HKEY_CURRENT_CONFIG (HKCC) является ссылкой на ключ HKLM\SYSTEM\CurrentControlSet\HardwareProfiles\Current. Содержит конфигурационные данные текущего профиля оборудования. Каждое значение в реестре имеет свой тип данных. Наиболее часто используемые типы данных описаны ниже:

- REG_BINARY - двоичные данные, чаще всего отображаемые в шестнадцатеричном виде (пример: «0x40 75 13»);

- REG_DWORD - 32-х разрядное целое число. Этот тип может использоваться в качестве логических флагов (пример: «0X152DADBF»);

- REG_SZ - строковый параметр (пример: «C:\ProgramData»);

- REG_MULTI_SZ - мультистроковый параметр;

- REG_EXPAND_SZ - расширяемый строковый параметр. Может включать переменные окружения вроде %WINDIR%.

Формат хранения данных реестра в файлах реестра.

Пространство улья логически делится на блоки, имеющие размер, кратный 4096 байт, и сигнатуру hbin. При увеличении размера улья к нему добавляется нужное число блоков. Первый блок улья называется базовым блоком, в нем хранится базовая информация об улье: номер версии улья, дата последнего обновления улья, контрольная сумма и полное имя улья.

Внутри блока находятся ячейки, или соты (cell). Ячейка состоит из четырехбайтного заголовка и имеет длину, кратную 8 байтам. Ячейки могут быть различных типов: ячейка раздела (NK), значения (VK), списка значений, списка подразделов и ячейка дескриптора защиты (SK).

Для криминалистического исследования, зачастую очень важно получить сведения о записях, которые были удалены при деинсталляции компонент программной среды или методом редактирования реестра с помощью редакторов реестра.

Удаление и восстановление записей в реестре

Удаление записей.

Большинство информации, хранимой в ячейках, сохраняется при их удалении, однако некоторые ключевые данные уничтожаются, причем правила удаления для различных типов ячеек отличаются.

При удалении ключа указатели на листы подключей и дескриптор безопасности затирается (перезаписывается значением QxFFFFFFFF) и количество подключей устанавливается равным нулю. Сами ячейки подключей не перезаписываются и не повреждаются.

При удалении подключа его индекс удаляется из списка подключей родителя, и список перезаписывается в соответствующую ячейку. Размер ячейки со списком подключей при этом не меняет свой размер. Пусть у нас есть 4 подключа A, B, C, D, и мы удаляем последовательно ключи B, D, A.

Значение удаляется аналогично: из ячейки, содержащей список значений, удаляется соответствующий индекс, и в ячейку помещается получившийся список.

Что самое важное, в большинстве случаев ячейка значений и связанная с ней ячейка данных не изменяются при удалении, за исключением Windows 2000, где первые 4 байта этих ячеек заменяются на 0xFFFFFFFF; это делает невозможным чтение названия и сигнатуры. Подобное поведение замечено лишь в Windows 2000, что можно списать на ошибку в этой ОС.

Ячейка дескриптора защиты удаляется, только если все ссылающиеся на нее ячейки удалены или перенаправлены на другие дескрипторы защиты.

В результате операций с ячейками возникает ситуация, схожая с фрагментацией диска: пустые приемники находятся вперемешку с непустыми. Если встречается два пустых приемника подряд, то Диспетчер объединяет их в один как можно большего размера. Если пустые преемники находятся в конце, то Диспетчер уплотняет улей.

Алгоритм чтения удаленной информации следует составлять с учетом особенностей удаления информации в реестре.

Восстановление записи ключа

Создаем временную запись ключа, содержащую смещение.

Добавляем в улей запись из п. 1.

Пытаемся считать параметры ключа. Ячейка ключа не содержит контрольной суммы, так что невозможно точно сказать, повреждена ячейка или нет.

Рекурсивно считываем родительскую запись ключа. Необходимо выйти из рекурсии, если:

• достигнут ключ, который не является удаленным (дальше по иерархии передвигаться смысла нет, так как по общей логике программы до запуска отображения удаленных данных запускается считывание активных данных);

• запись-предок не является ключом. Рекурсивно считываем подключи и значения.

Если выполнение было завершено с ошибкой, то удаляем из улья добавленную в п. 2 запись, иначе добавляем в ключ-предок запись о том, что текущий ключ является подключом.

Восстановление записи значения

На данном этапе исследований восстановление пути, в котором находится удаленная запись значения, не представляется возможным, так как ссылка на нее удаляется из списка значений, а сама ячейка значения не содержит указателя на родительскую ячейку.

Впрочем, удаленные данные остаются в иерархии, если было удалено не само значение, а ключ, содержащий его.

Так как при удалении с ячейкой значений ничего не происходит, можно считать параметры значения и при отсутствии ошибок чтения добавить в результирующее множество данных.

Исследование данных реестра

Использование временных меток ключей

Все ключи реестра содержат временную метку (timestamp, last write value), похожую на дату 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.

При попытке сокрытия следов инцидента злоумышленники могут изменять данные в записях, отвечающих за хранение времени последнего изменения. В этом случае значение временной метки позволяет не только установить истинное время какого-либо события, но и установить факты намеренного редактирования реестра с целью сокрытия следов (изменение данных в значении, отвечающем за хранение времени последнего обновления).

В большинстве случаев временные метки являются единственным указателем на дату и время какого-либо события, например, подключения USB-носителя. Кроме этого, временные метки ключей позволяют построить временную линию событий путем анализа временных меток в различных разделах реестра.

Информация о системе

В значениях ключа «SOFTWARE\Microsoft\ Windows NT\CurrentVersion» хранятся различные параметры операционной системы: версия, издание, номер сборки, информация о сервис-паке и так далее. Кроме того, в этом разделе хранится регистрационная информация, что может быть полезно при анализе случаев нелицензионного использования ПО.

Получение информации о подключаемых USB-устройствах

Анализ подключаемых устройств может дать исследователю информацию о носителях, когда-либо подключенных к системе. Подобная информация может быть полезна, например, в случае расследования утечки данных: эксперту необходимо знать, с какими USBустройствами проводилась работа, а также идентификаторы этих устройств для сопоставления с уже имеющимися данными.

Когда съемное USB-устройство (например, флэш-накопитель) подключается к ПК, информация о нем будет сохранена в разделе HKLM > System > ControlSet00x > ENUM > USBSTOR.

В этой ветке реестра создаются ключи, каждый из которых представляет свой класс устройств. Имя ключа задается в следующем формате:

Type&Ven_{vendor}&Prod_{product}&Rev_ {rev} .

В этих ключах создаются подключи, представляющие экземпляр устройства. В качестве имени подключа используется серийный номер устройства.

Стоит обратить внимание, что у экземпляра устройства может не быть серийного номера (тогда устройство не пройдет сертификацию Microsoft). В этом случае в имени ключа, отвечающего за экземпляр устройства, вторым символом будет «&».

Особенности получения временных меток

После получения базовой информации об устройстве необходимо определить дату и время первого и последнего подключения устройства. Реестр не хранит информацию о первом подключении (она хранится в файле C:\Windows\inf\setupapi.dev.log).

Информацию о последнем подключении устройства нельзя брать из временной метки соответствующей устройству записи ключа, так как временные метки всех ключей из раздела «SYSTEM\ControlSet00x\ENUM\USBSTOR» периодически обновляются текущей датой (это происходит из-за существования нескольких конфигураций - текущей, последней удачной - и их синхронизации).

Для получения времени последнего подключения USB-устройства следует взять временную метку одного из подключей ключа SYSTEM\ControlSet00x \Control\DeviceClasses\ {53f56307-b6bf-11d0-94f2-00a0c91efb8b}\.

Поиск подключа проводится по названию, которое должно содержать серийный номер USB-устройства, для которого необходимо определить дату последнего подключения.

Установлено, что система хранит полный список USB-устройств, когда-либо подключавшихся к системе.

Получение информации о подключавшихся сетевым картах

Результат анализа списка сетевых карт может использоваться экспертом как доказательство использования внешней сетевой карты (или устройства, исполняющего роль внешней сетевой карты) или доказательство использования виртуальных машин.

При подключении новой сетевой карты система сохраняет данные в раздел SOFTWARE\ Microsoft\Windows NT\CurrentVersion\Network Cards.

Внутри этого раздела находятся подключи, каждый из которых хранит информацию по отдельной сетевой карте. Эти ключи не обновляются, соответственно, можно воспользоваться их временной меткой для выяснения даты установки сетевой карты.

Дополнительная информация может быть найдена в следующем ключе улья SYSTEM: SYSTEM\ControlSet00x\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\{00nn}, где {00nn} - имя соответствующего ключа из прошлого раздела.

Установлено, что система хранит полный список сетевых карт, когда-либо используемых системой.

Информация о сетевом окружении

Анализ информации, хранящейся по сетевому окружению, может дать исследователю представление о сетевой активности, которая была произведена на анализируемой системе.

Это установленные сетевые карты, сети, к которым подключалась машина, и, что самое важное, список беспроводных сетей. Известно много случаев использования анонимных беспроводных сетей для совершения противоправных действий.

Информация о сетевых интерфейсах хранится в следующем разделе реестра: SYSTEM\ControlSet00x\Services\Tcpip\Parameters\Interfaces.

Данный раздел содержит ключи, в качестве имени ключа используется GUID. В ключе содержится множество значений, описывающих параметры сетевого интерфейса: параметры DHCP, IP адрес, шлюз по умолчанию и так далее.

По GUID можно получить имя сети из раздела SYSTEM\ControlSet00x\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\{GUID}.

Беспроводные сети

Для любой беспроводной сети, к которой было произведено подключение, создается запись в разделе SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless.

Этот ключ лишь содержит список идентификаторов беспроводных сетей; подробная информация может быть получена путем связывания этих идентификаторов с сигнатурами из раздела SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\ Unmanaged.

После этого необходимо связать сигнатуру и профилем, находящиеся в записи значения ProfileGuid. Для этого необходимо выбрать данные из записи ключа SOFTWARE\ Microsoft\Windows NT\CurrentVersion\ NetworkList\Profiles\{ProfileGuid}.

Итоговые данные содержат следующую важную информацию:

• дата создания;

• дата последнего подключения;

• имя профиля;

• MAC шлюза по умолчанию (default gateway).

ОС хранит полный список беспроводных сетей, сигнатур и профилей (если пользователь не удаляет данные вручную).

Интранет-сети

Анализ интранет-сетей во многом похож на анализ беспроводных сетей. Для анализа интранет-сетей необходимо обратиться к разделу SOFTWARE\Microsoft\Windows NT\ CurrentVersion\NetworkList\Nla\Cache\ Intranet.

После получения подключей из данного раздела необходимо связать их с записями сетевых профилей, связывание производится через GUID.

Информация о пользовательской активности

Microsoft сохраняет списки пользовательской активности именно в реестре.

Такие списки пользовательской активности получили название «Списки недавно используемых элементов» (Most Recently Used lists - в дальнейшем MRU списки). MRU списки играют в расследовании инцидентов важную роль, и могут предоставить эксперту косвенное доказательство действий возможного злоумышленника или дать направление дальнейшего анализа.

В реестре Windows большинство пользовательских действий сохраняются в ульях NTUDSER.dat, для каждого пользователя создается свой улей.

Информация о запуске GUI-приложений через проводник Windows хранится в разделе NTUSER.dat\Software\Microsoft\Windows\ CurrentVersion\Explorer\UserAssist\{GUID}\ Count.

Для ОС Windows 7/8/10 значение {GUID} может быть одним из двух:

• в разделе {CEBFF5CD-ACE2-4F4F-9178- 9926F41749EA}\Count содержится информация по исполняемым приложениям;

• в разделе {F4E57C4B-2036-45F0-A9AB443BCFE33D9F}\Count содержится информация по открываемым ярлыкам.

Для каждого запускаемого приложения / открываемого ярлыка создается запись значения, имя которого кодируется алгоритмом ROT-13, а данные представляют собой двоичные данные размера 72 байта.

Информация о недавно открытых документах хранится в разделе реестра HKCU\Software\ Microsoft\Windows\CurrentVersion\Explorer\ RecentDoc.

Данный раздел реестра содержит подключи с именем, эквивалентным расширению открытого файла (например, .doc, .gif; также есть специальный ключ с именем Folder, в котором хранится информация о каталогах). Внутри каждого ключа хранится до десяти (это значение по умолчанию, оно может быть изменено) значений с именем, равным числу от 0 до 9.

Кроме этого, до 150 записей значений (которые описывают последние открытые документы без группировки по расширению, далее «общий список») хранятся внутри коревого ключа HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\RecentDoc.

Данные ячейки значения представляют собой строки, закодированные в двоичном формате. Сначала идет имя открытого файла в кодировке Unicode, затем имя открытого файла в кодировке UTF-8, затем опять имя файла в кодировке Unicode с небольшими изменениями в имени файла (добавляется .lnk в конце). К сожалению, каталог, в котором хранится файл, не сохраняется.

Особенности восстановления временной метки

Известно, что ячейки значения не хранят в себе временную метку, значит для каждого расширения можно узнать лишь время открытия последнего файла с данным расширением. Это ограничение можно обойти, воспользовавшись «общим списком».

Расставим «контрольные точки», взяв первые объекты из «общего списка» с еще не встречавшимся расширением. Сопоставим этим объектам временные метки, взятые из записи ключа с именем, равным расширению объекта.

Для всех объектов, располагающихся между контрольными точками, можно вычислить диапазон дат, когда этот объект мог быть открыт.

Приложение операционной системы «Выполнить» сохраняет до 26 выполненных команд в ключе HKCU\Software\Microsoft\ Windows\CurrentVersion\Explorer\RunMRU.

В данном ключе хранится до 26 значений с названиями от 'a' до 'z' и одно значение с названием MRUList. Все значения 'a' ... 'z' имеют строковый тип (REG_SZ) и в качестве значения содержат последнюю выполненную команду.

MRUList является строкой-перестановкой букв английского алфавита и задает порядок, в котором будет отображен список последних выполненных команд (и, соответственно, порядок их выполнения пользователем).

Многие прикладные программы сохраняют свои собственные списки последних открытых файлов. Не существует единого формата или единого хранилища MRU списков, поэтому анализ MRU списков конкретного приложения необходимо осуществлять вручную.

Большинство приложений хранит отдельные MRU списки для разных пользователей, следовательно, для первичного поиска можно использовать следующий шаблон: NTUSER. dat\Software\{vendor}\{application}\{version}.

Пакет Microsoft Office

Исследования показали, что Microsoft Office 2013 хранит до 50-и последних открытых файлов в значениях ключа HKCU\ Software\Microsoft\Office\{version}\{product}\ File MRU.

Из-за особенностей структуры хранения получение данных из удаленных структур невозможно.

Acrobat Reader

Приложение Acrobat Reader хранит список последних открытых файлов в подключах раздела NTU SER.dat\Software\Adobe\Acrobat Reader\{version} \AVGeneral\cRecentFiles. Значения внутри этих подключей описывают последний открытый документ.

В некоторых случаях исследователю может понадобится информация об удаленных компьютерах, к которым подключалась исследуемая система через протокол Remote Desktop Protocol. Приложение Remote Desktop Connection (mstsc.exe) хранит полный список серверов, к которым производилось подключение, в разделе NTU SER.dat\Software\ Microsoft\Terminal Server Client\Servers.

Однако эта информация не является списком последних используемых объектов как таковым; для получения этой информации (10 последних подключений) нужно воспользоваться разделом NTUSER.dat\Software\ Microsoft\Terminal Server Client\Default.

Исследование показало, что удаленных ключей в данном разделе нет, соответственно приложение хранит полный список серверов, к которым когда-либо подключалось приложение.

К сожалению, этой информации недостаточно для того, чтобы определить время первого или последнего подключения, а также длительность или количество подключений. Запущенные приложения сохраняются в кэше многоязычного пользовательского интерфейса (Multilingual User Interface Cache) - технологии Microsoft, которая позволяет приложениям использовать различные языки интерфейса в одной системе. Необходимая информация хранится в значениях ключа [8] USRCLASS.dat\Local Settings\ Software\Microsoft\Windows\Shell\MuiCache.

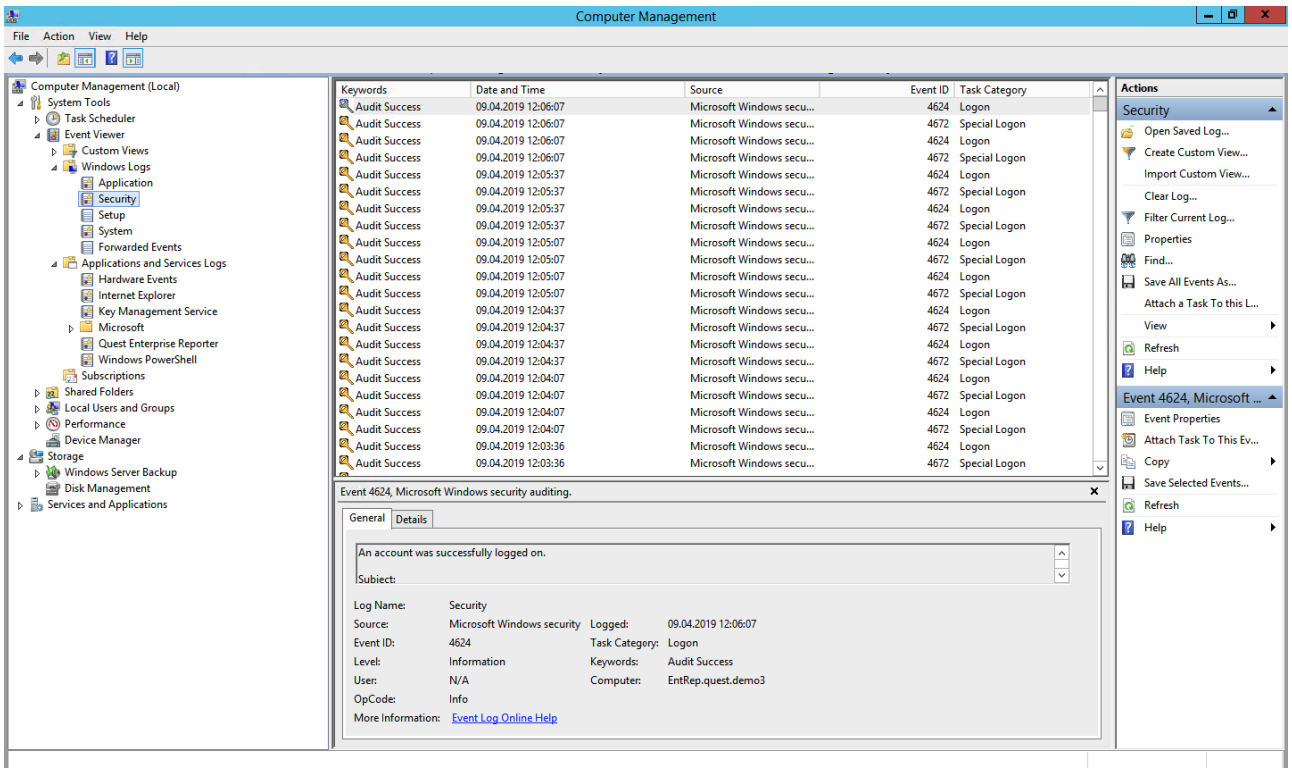
2.3. Криминалистический анализ хронологии событий ОС Windows

Пользовательская рабочая станция — самое уязвимое место инфраструктуры по части информационной безопасности. Пользователям может прийти на рабочую почту письмо вроде бы из безопасного источника, но со ссылкой на заражённый сайт. Возможно, кто-то скачает полезную для работы утилиту из неизвестно какого места. Да можно придумать не один десяток кейсов, как через пользователей вредоносное ПО может внедриться на внутрикорпоративные ресурсы. Поэтому рабочие станции требуют повышенного внимания, и в статье мы расскажем, откуда и какие события брать для отслеживания атак.

Для выявления атаки на самой ранней стадии в ОС Windows есть три полезных событийных источника: журнал событий безопасности, журнал системного мониторинга и журналы Power Shell.

Журнал событий безопасности (Security Log)

Это главное место хранения системных логов безопасности. Сюда складываются события входа/выхода пользователей, доступа к объектам, изменения политик и других активностей, связанных с безопасностью. Разумеется, если настроена соответствующая политика.



Перебор пользователей и групп (события 4798 и 4799). Вредоносное ПО в самом начале атаки часто перебирает локальные учетные записи пользователей и локальные группы на рабочей станции, чтобы найти учетные данные для своих тёмных делишек. Эти события помогут обнаружить вредоносный код раньше, чем он двинется дальше и, используя собранные данные, распространится на другие системы.

Создание локальной учётной записи и изменения в локальных группах (события 4720, 4722–4726, 4738, 4740, 4767, 4780, 4781, 4794, 5376 и 5377). Атака может также начинаться, например, с добавления нового пользователя в группу локальных администраторов.

Попытки входа с локальной учётной записью (событие 4624). Добропорядочные пользователи заходят с доменной учётной записью и выявление входа под локальной учётной записью может означать начало атаки. Событие 4624 включает также входы под доменной учетной записью, поэтому при обработке событий нужно зафильтровать события, в которых домен отличается от имени рабочей станции.

Попытка входа с заданной учётной записью (событие 4648). Такое бывает, когда процесс выполняется в режиме “Запуск от имени” (run as). В нормальном режиме работы систем такого не должно быть, поэтому такие события должны находиться под контролем.

Блокировка/разблокировка рабочей станции (события 4800-4803). К категории подозрительных событий можно отнести любые действия, которые происходили на заблокированной рабочей станции.

Изменения конфигурации файрволла (события 4944-4958). Очевидно, что при установке нового ПО настройки конфигурации файрволла могут меняться, что вызовет ложные срабатывания. Контролировать такие изменения

в большинстве случаев нет необходимости, но знать о них точно лишним не будет.

Подключение устройств Plug'n'play (событие 6416 и только для WIndows 10). За этим важно следить, если пользователи обычно не подключают новые устройства к рабочей станции, а тут вдруг раз — и подключили.

Windows включает в себя 9 категорий аудита и 50 субкатегорий для тонкой настройки. Минимальный набор субкатегорий, который стоит включить в настройках:

Logon/Logoff

- Logon;
- Logoff;
- Account Lockout;
- Other Logon/Logoff Events.

Account Management

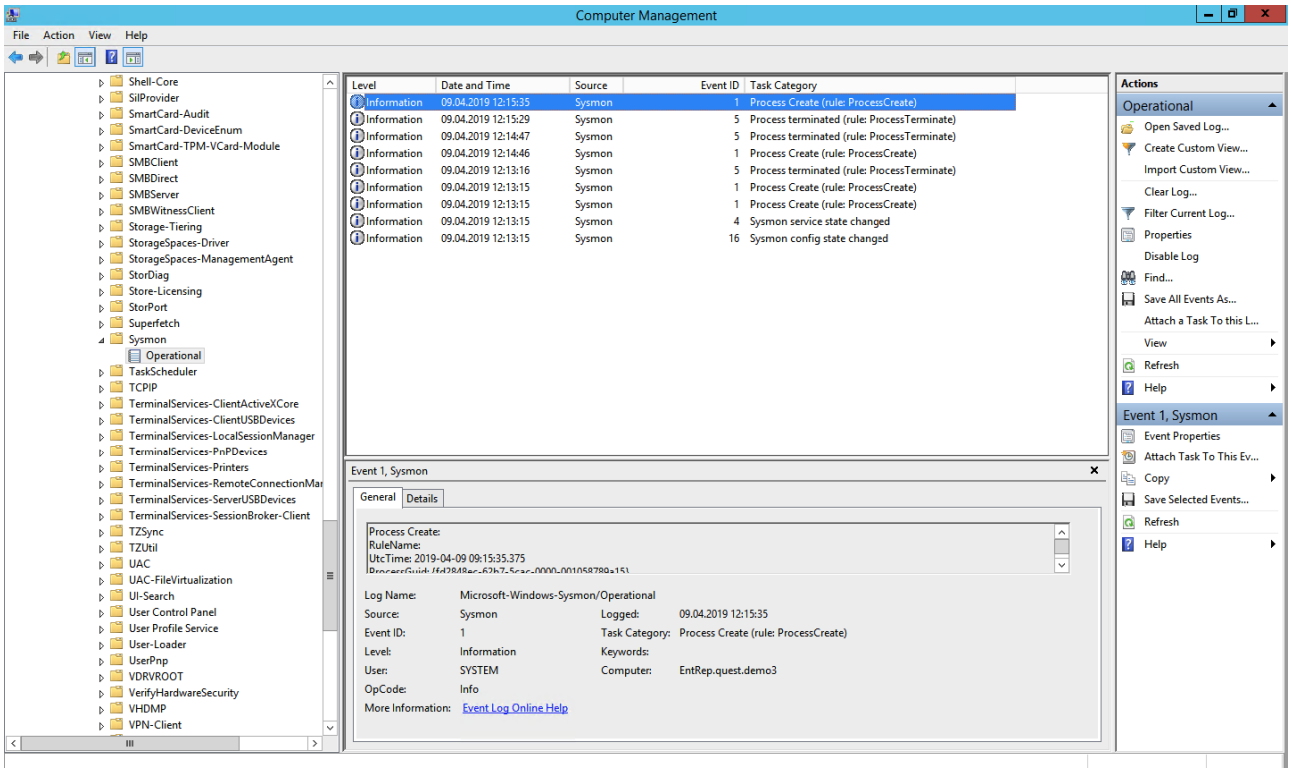
- User Account Management;
- Security Group Management.

Policy Change

- Audit Policy Change;
- Authentication Policy Change;
- Authorization Policy Change.

Системный монитор (Sysmon)

Sysmon — встроенная в Windows утилита, которая умеет записывать события в системный журнал. Обычно требуется его устанавливать отдельно.



Эти же события можно в принципе найти в журнале безопасности (включив нужную политику аудита), но Sysmon даёт больше подробностей. Какие события можно забирать из Sysmon?

Создание процесса (ID события 1). Системный журнал событий безопасности тоже может сказать, когда запустился какой-нибудь *.exe и даже покажет его имя и путь запуска. Но в отличие от Sysmon не сможет показать хэш приложения. Злонамеренное ПО может называться даже безобидным notepad.exe, но именно хэш выведет его на чистую воду.

Сетевые подключения (ID события 3). Очевидно, что сетевых подключений много, и за всеми не уследить. Но важно учитывать, что Sysmon в отличие от того же Security Log умеет привязать сетевое подключение к полям ProcessID и ProcessGUID, показывает порт и IP-адреса источника и приёмника.

Изменения в системном реестре (ID события 12-14). Самый простой способ добавить себя в автозапуск — прописаться в реестре. Security Log это умеет, но Sysmon показывает, кто внёс изменения, когда, откуда, process ID и предыдущее значение ключа.

Создание файла (ID события 11). Sysmon, в отличие от Security Log, покажет не только расположение файла, но и его имя. Понятно, что за всем не уследишь, но можно же проводить аудит определённых директорий.

А теперь то, чего в политиках Security Log нет, но есть в Sysmon:

Изменение времени создания файла (ID события 2). Некоторое вредоносное ПО может подменять дату создания файла для его скрытия из отчётов с недавно созданными файлами.

Загрузка драйверов и динамических библиотек (ID событий 6-7). Отслеживание загрузки в память DLL и драйверов устройств, проверка цифровой подписи и её валидности.

Создание потока в выполняющемся процессе (ID события 8). Один из видов атаки, за которым тоже нужно следить.

События RawAccessRead (ID события 9). Операции чтения с диска при помощи “\\.\”. В абсолютном большинстве случаев такая активность должна считаться ненормальной.

Создание именованного файлового потока (ID события 15). Событие регистрируется, когда создается именованный файловый поток, который генерирует события с хэшем содержимого файла.

Создание named pipe и подключения (ID события 17-18). Отслеживание вредоносного кода, который коммуницирует с другими компонентами через named pipe.

Активность по WMI (ID события 19). Регистрация событий, которые генерируются при обращении к системе по протоколу WMI.

Для защиты самого Sysmon нужно отслеживать события с ID 4 (остановка и запуск Sysmon) и ID 16 (изменение конфигурации Sysmon).

Журналы Power Shell

Power Shell — мощный инструмент управления Windows-инфраструктурой, поэтому велики шансы, что атакующий выберет именно его.

Для получения данных о событиях Power Shell можно использовать два источника: Windows PowerShell log и Microsoft-WindowsPowerShell / Operational log

Windows PowerShell log

Загружен поставщик данных (ID события 600). Поставщики PowerShell — это программы, которые служат источником данных для PowerShell для просмотра и управления ими. Например, встроенными поставщиками могут быть переменные среды Windows или системный реестр. За появлением новых поставщиков нужно следить, чтобы вовремя выявить злонамеренную активность. Например, если видите, что среди поставщиков появился WSMan, значит был начат удаленный сеанс PowerShell.

Журналирование модулей (ID события 4103). В событиях хранится информация о каждой выполненной команде и параметрах, с которыми она вызывалась.

Журналирование блокировки скриптов (ID события 4104). Журналирование блокировки скриптов показывает каждый выполненный блок кода PowerShell. Даже если злоумышленник попытается скрыть команду, этот тип события покажет фактически выполненную команду PowerShell. Ещё в этом типе события могут фиксироваться некоторые выполняемые низкоуровневые вызовы API, эти события обычно записывается как Verbose, но если подозрительная команда или сценарий используются в блоке кода, он будет зарегистрирован как с критичностью Warning.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Запустите системный реестр ОС Windows (Win+R → regedit → Enter), ознакомьтесь с интерфейсом указанного приложения
2. По пути «\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR», ознакомьтесь с историей подключенных устройств через USB. Изготовьте фотоснимок экрана.
3. По пути «\HKEY_CURRENT_USER\Software», ознакомьтесь с установленными приложениями на рабочей станции. Изготовьте фотоснимок экрана.
4. Закройте системный реестр ОС Windows.
5. Запустите стандартное приложение «Просмотр событий» (Пуск → Панель управления → Администрирование → Просмотр событий), ознакомьтесь с интерфейсом указанного приложения.
6. Перейдите в раздел «Журналы Windows/Безопасность», где проанализируйте события, произошедшие за сегодняшнюю дату. Изготовьте фотоснимок экрана.
7. Подготовьте файл-отчет о продлеанной работе, в котором разместите полученные в ходе выполнения задания 2-6 фотоснимки экрана
8. **Предъявите работу преподавателю.**

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что относится к системным файлам ОС Windows? В каком из

системных файлов находятся кэшированные эскизы изображений?

2. В чем отличие терминов «системные файлы» от «файловая система»?

3. Что такое реестр операционной системы Windows?

4. Какая информация важна для проведения криминалистического исследования реестра ОС?

5. Что такое протоколирование и аудит событий безопасности? Какие цели преследуются при использовании данных средств?

6. Опишите основные элементы интерфейса журнала событий ОС Windows?

7. Какие виды журналов представлены в категории «Журналы Windows»? Каково их предназначение?

8. Что такое код события? Каким образом расшифровывается его значение?