Следы преступлений экстремисткой направленности в операционной системе Windows

А.Д. Попов

Registro de Windows

El registro es una enorme base de datos que almacena todos los registros sobre la configuración y los parámetros de los programas, servicios y todo el sistema operativo en su conjunto.

los desarrolladores han creado una utilidad especial para trabajar y administrar el registro, que se llama Editor del Registro. La utilidad en sí se encuentra en una carpeta a lo largo de la ruta: \ Windows \ System32.

Реестр Windows

Реестр - это огромная база данных, которая хранит в себе все записи о настройке и параметрах программ, служб и всей операционной системы в целом.

разработчики создали специальную утилиту для работы и управления реестром, которая называется Редактор реестра. Сама эта утилита находится в папке по пути: \Windows\System32 .

Ubicación física del registro

Después de instalar Windows en una unidad en el directorio %SystemRoot%\System32\Config\ se almacenan los siguientes archivos:

SYSTEM
SOFTWARE
SAM
SECURITY
DEFAULT
NTUSER

(Todos los archivos (nombres de archivo) sin extensiones. Una copia de estos archivos se almacena en el directorio % SystemDrive% \ Windows \ Repair\)

Физическое расположение реестра

После установки Windows на диске в каталоге %SystemRoot%\System32\Config\ хранятся следующие файлы:

SYSTEM
SOFTWARE
SAM
SECURITY
DEFAULT
NTUSER

(Все файлы (имена файлов) без расширений. Копия этих файлов хранится в каталоге %SystemDrive%\ Windows\Repair\)

Estructura del registro de Windows

1) HKEY_CLASSES_ROOT (HKCR) – contiene los datos sobre los formatos de todos tipos de archivos y asociaciones registrados en la red;

2) HKEY_CURRENT_USER (HKCU) – guarda la información de un usuario concreto, que integró en sistema en el momento real (las carpetas de usuario, color de pantalla y parametros de cobfiguración);

3) HKEY_LOCAL_MACHINE (HKLM) – contiene la información sobre la parte de aparato de una computadora (controladores de dispositivo, información de inicio de Windows, configuración de software y más.);

4) HKEY_USERS (HKU) –contiene información sobre todos los perfiles cargados activos de los usuarios de computadora personal que tienen acceso al sistema operativo;

5) HKEY_CURRENT_CONFIG (HKCC) – contiene información sobre el perfil de hardware utilizado por la computadora local al iniciar el sistema.

Структура реестра Windows

1) HKEY_CLASSES_ROOT (HKCR) – содержит сведения о расширениях всех зарегистрированных в системе типов файлов и ассоциациях;
2) HKEY_CURRENT_USER (HKCU) – хранит информацию о конкретном пользователе, вошедшем в систему в настоящий момент (папки пользователя, цвет экрана и параметры панели управления);
3) HKEY_LOCAL_MACHINE (HKLM) – содержит информацию об аппаратной части компьютера (драйвера устройств, сведения о загрузке Windows, настройки ПО и т.д.);
4) HKEY_USERS (HKU) – содержит информацию о всех активных загруженных профилях пользователей ПК, имеющих доступ к операционной системе;
5) HKEY_CURRENT_CONFIG (HKCC) – содержит информацию о профиле оборудования, используемом локальным компьютером при запуске системы.

Información sobre el sistema

Para determinar información sobre el sistema operativo, se puede usar los datos del registro :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Fecha de instalación InstallDate (fecha de instalación del sistema operativo se almacena en formato hexadecimal y decimal).
El parámetro InstallDate indica la cantidad de segundos que transcurrieron desde el 1 de enero de 1970 hasta que se instaló el sistema operativo.
Números de identificación del producto y rutas de instalación.

Si el sistema está en un estado activo, encendido, utilizan los datos obtenidos mediante el comando: "systeminfo".

Информация о системе

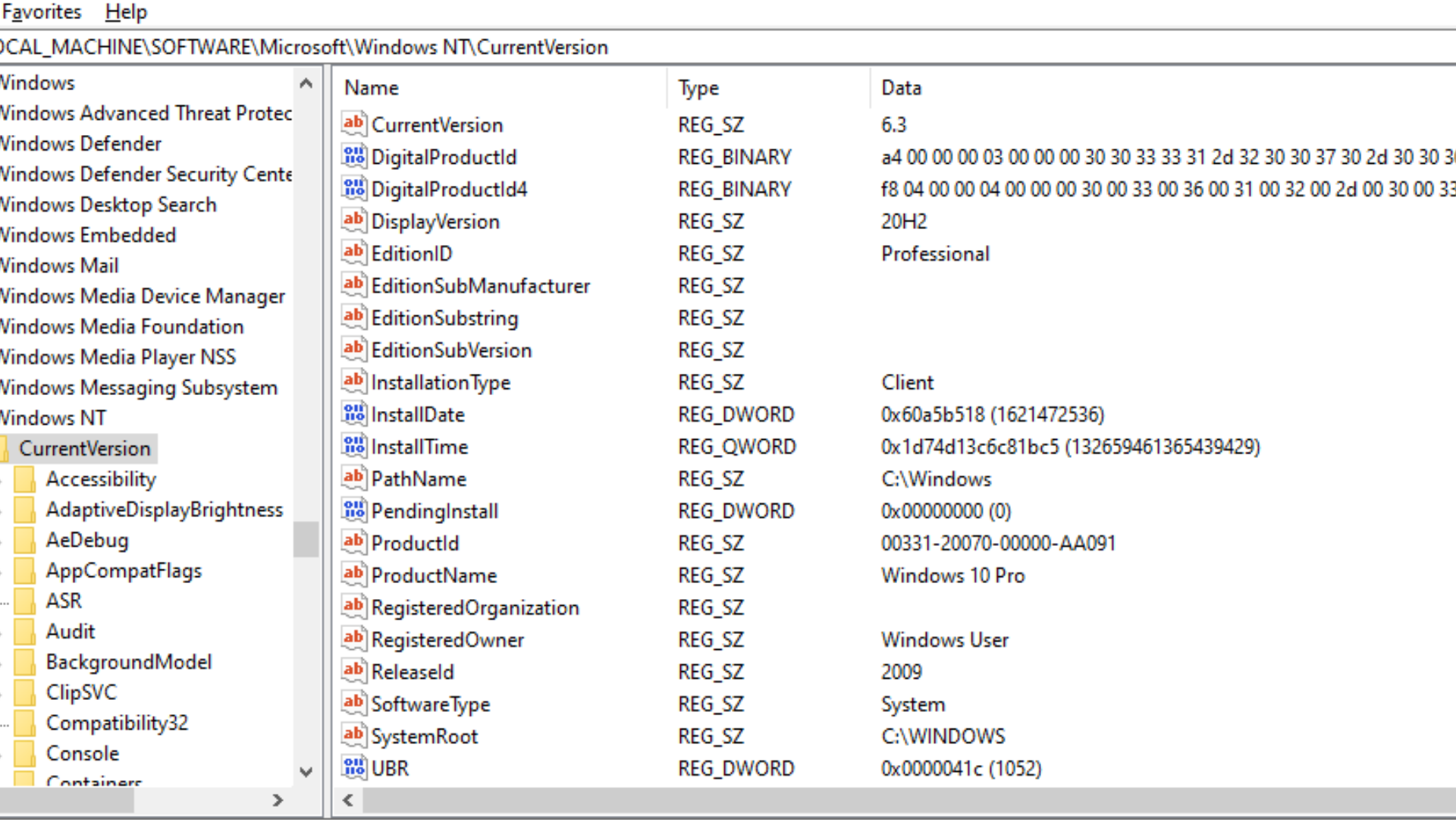
Для определения сведений об операционной системе следует использовать данные из реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion

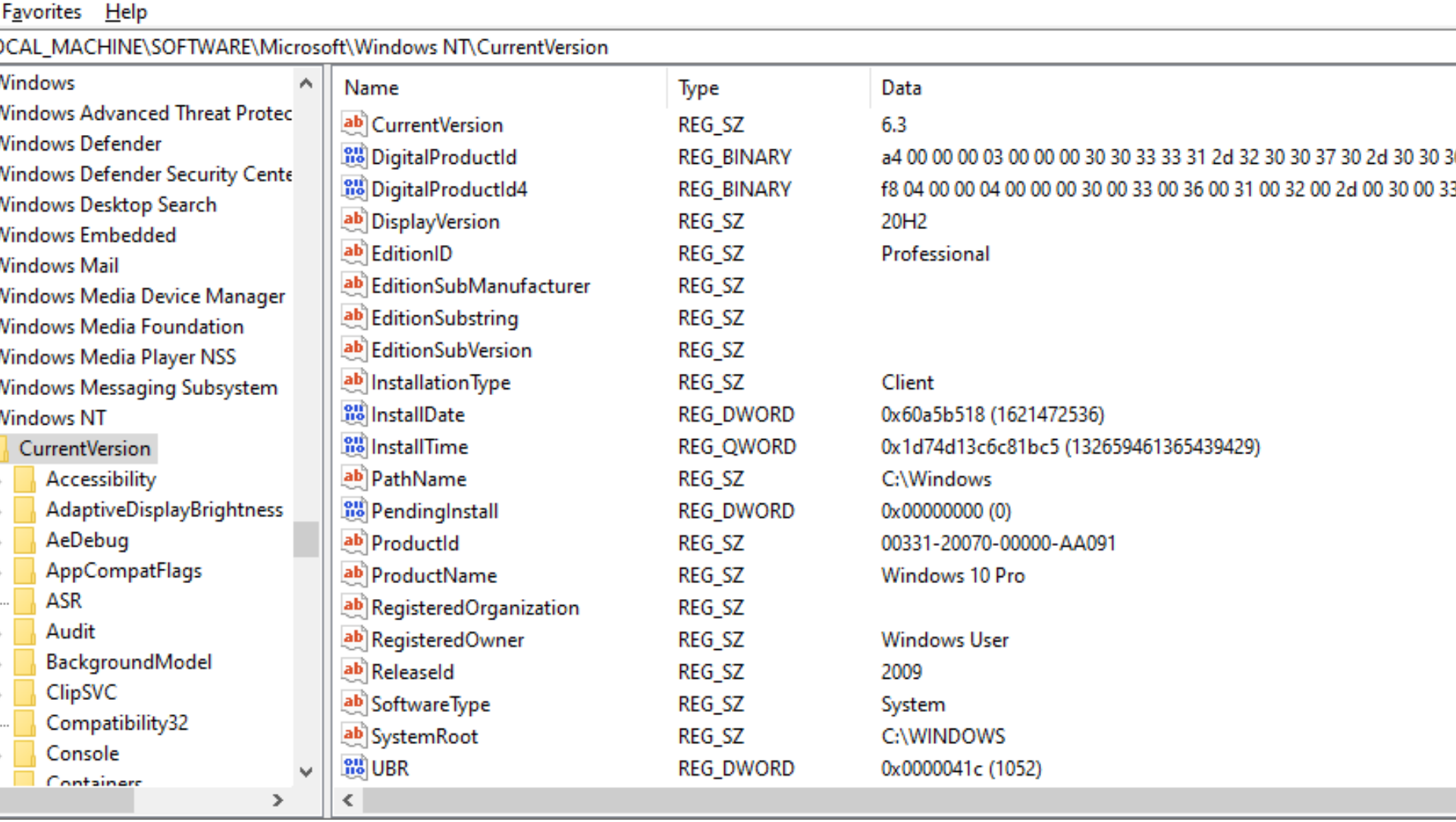
Дата инсталляции InstallDate (дата инсталляции дата установки операционной системы хранится в шестнадцатеричном и десятичном виде).
Параметр InstallDate показывает количество секунд, прошедших с 1 января 1970 г. до момента установки операционной систем.
Идентификационные номера продукта и пути установки.

Если система находится в активном состоянии, включена, то используют данные полученные с помощью команды: "systeminfo".

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion



systeminfo

Command Prompt

```
C:\Users\2>systeminfo

Host Name:                 DESKTOP-8L8DTPI
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-20070-00000-AA091
Original Install Date:     19.05.2021, 19:02:16
System Boot Time:          08.06.2021, 15:37:46
System Manufacturer:       HP
System Model:              HP Pavilion Laptop 15-cd0xx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 21 Model 101 Stepping 1 AuthenticAMD ~2700 Mhz
BIOS Version:              American Megatrends Inc. F.14, 20.07.2017
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             ru;Russian
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-06:00) Central America
Total Physical Memory:     11 735 MB
Available Physical Memory: 5 176 MB
Virtual Memory: Max Size:  23 511 MB
Virtual Memory: Available: 12 736 MB
Virtual Memory: In Use:    10 775 MB
```

systeminfo

Command Prompt

```
C:\Users\2>systeminfo

Host Name:                 DESKTOP-8L8DTPI
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-20070-00000-AA091
Original Install Date:     19.05.2021, 19:02:16
System Boot Time:          08.06.2021, 15:37:46
System Manufacturer:       HP
System Model:              HP Pavilion Laptop 15-cd0xx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 21 Model 101 Stepping 1 AuthenticAMD ~2700 Mhz
BIOS Version:              American Megatrends Inc. F.14, 20.07.2017
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             ru;Russian
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-06:00) Central America
Total Physical Memory:     11 735 MB
Available Physical Memory: 5 176 MB
Virtual Memory: Max Size:  23 511 MB
Virtual Memory: Available: 12 736 MB
Virtual Memory: In Use:    10 775 MB
```

El registro de acontecimientos

Para determinar las acciones realizadas por el sistema operativo de la familia "Windows", vea los registros de acontecimientos del sistema operativo

estos archivos se encuentran por defecto en el directorio " % SYSTEMROOT% \ System32\Winevt \ Logs\ "y tienen una extensión".Evtx"

Журнал событий

Для определения проведенных действий операционной системой семейства "Windows" производится просмотр журналов событий операционной системы

данные файлы по умолчанию расположены в директории "%SYSTEMROOT%\System32\Winevt\Logs\" и имеют расширение ".Evtx"

Al ver este registro se puede definir:

- marco de tiempo de trabajo del sistema operativo;
- marco de tiempo de ejecución de una serie de productos de software que se ejecutan en el registro de funcionamiento del sistema operativo "Windows";
- marco de tiempo de conexión: deshabilita los recursos de red (adaptador de red) que se ejecutan en el registro del sistema operativo Windows y una serie de otros parámetros.

Просмотром данного журнала возможно определить:

- временные рамки работы операционной системы;
- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале работы операционной системы "Windows";
- временные рамки подключения - отключения сетевых ресурсов (сетевого адаптера) запуск которых отображается в журнале работы операционной системы "Windows", и ряд других параметров.

Los siguientes son algunos códigos que muestran el funcionamiento del sistema para:

Código -6008- el cierre Anterior del sistema a las 17: 40: 08 el 18.09.2013 fue inesperado.

Código -12- Hora de Inicio del sistema operativo: 2013-09-19T07: 04: 12.125599400 Z.

Código -1- hora del Sistema cambiado de 2016-09-14T08: 20: 13.000000000 Z a 2016-09-14T08: 20: 13.000000000 Z.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

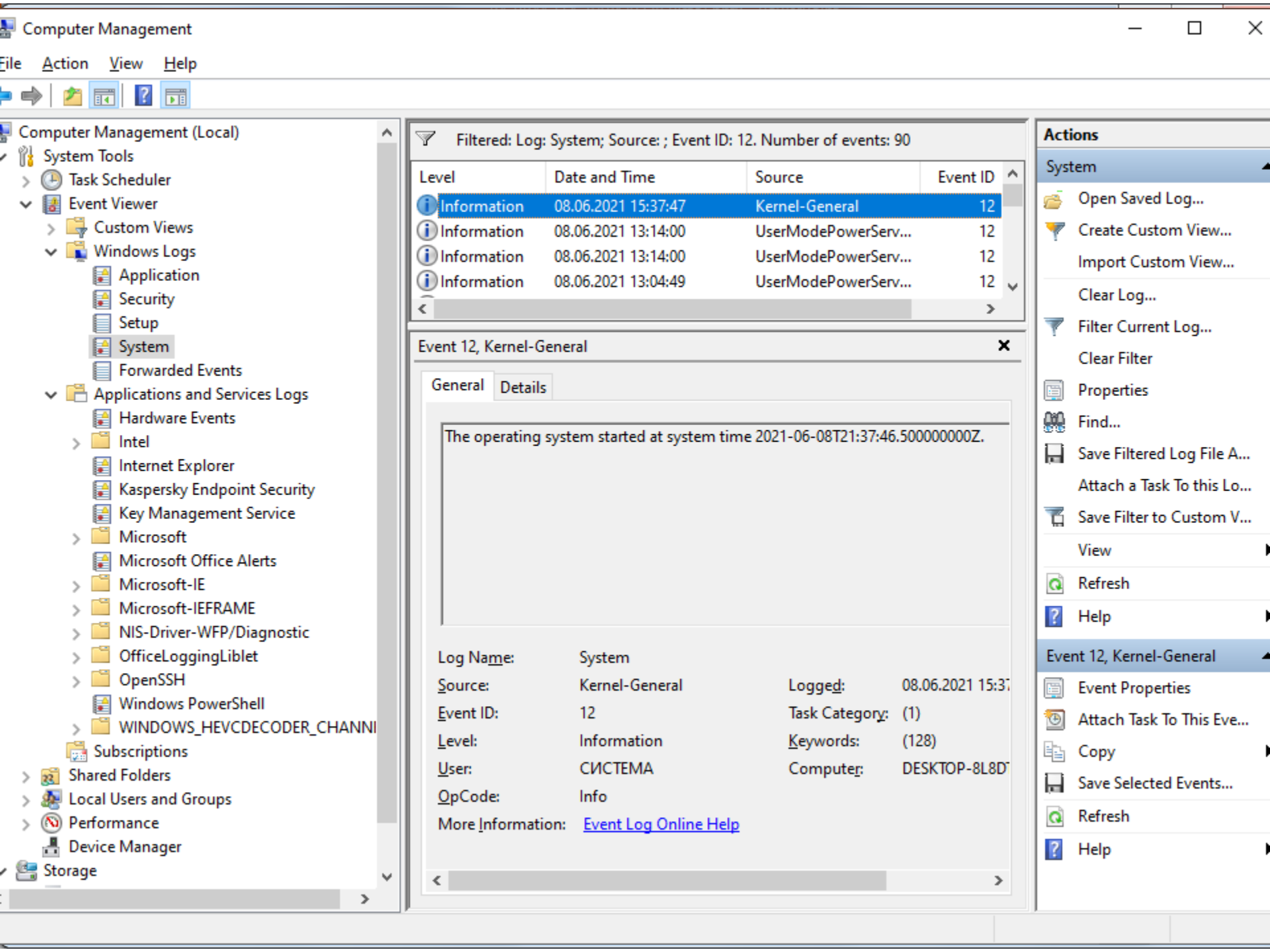
Ниже приведены некоторые коды отображающие работу системы:

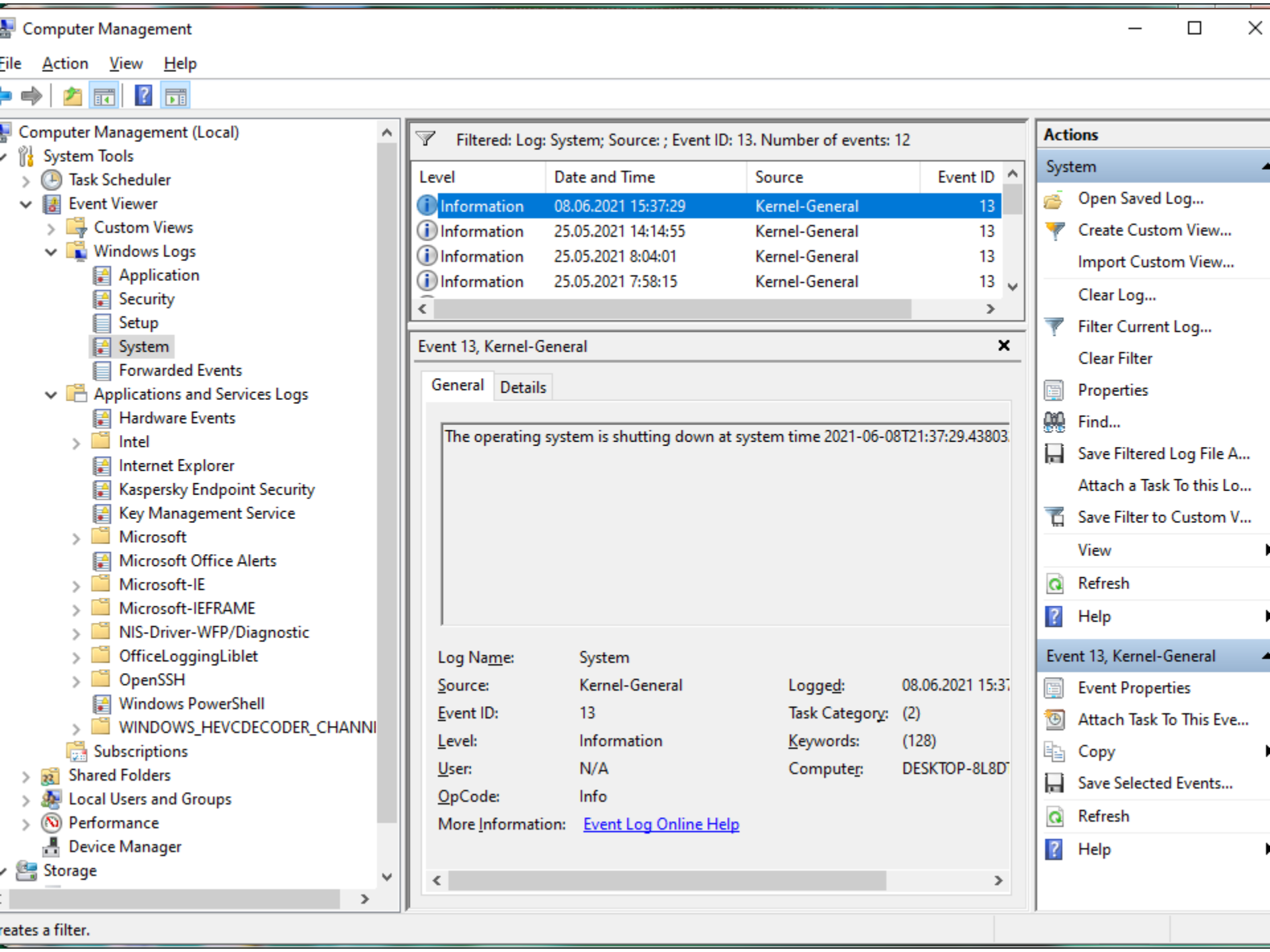
Код - 6008 - Предыдущее завершение работы системы в 17:40:08 на 18.09.2013 было неожиданным.

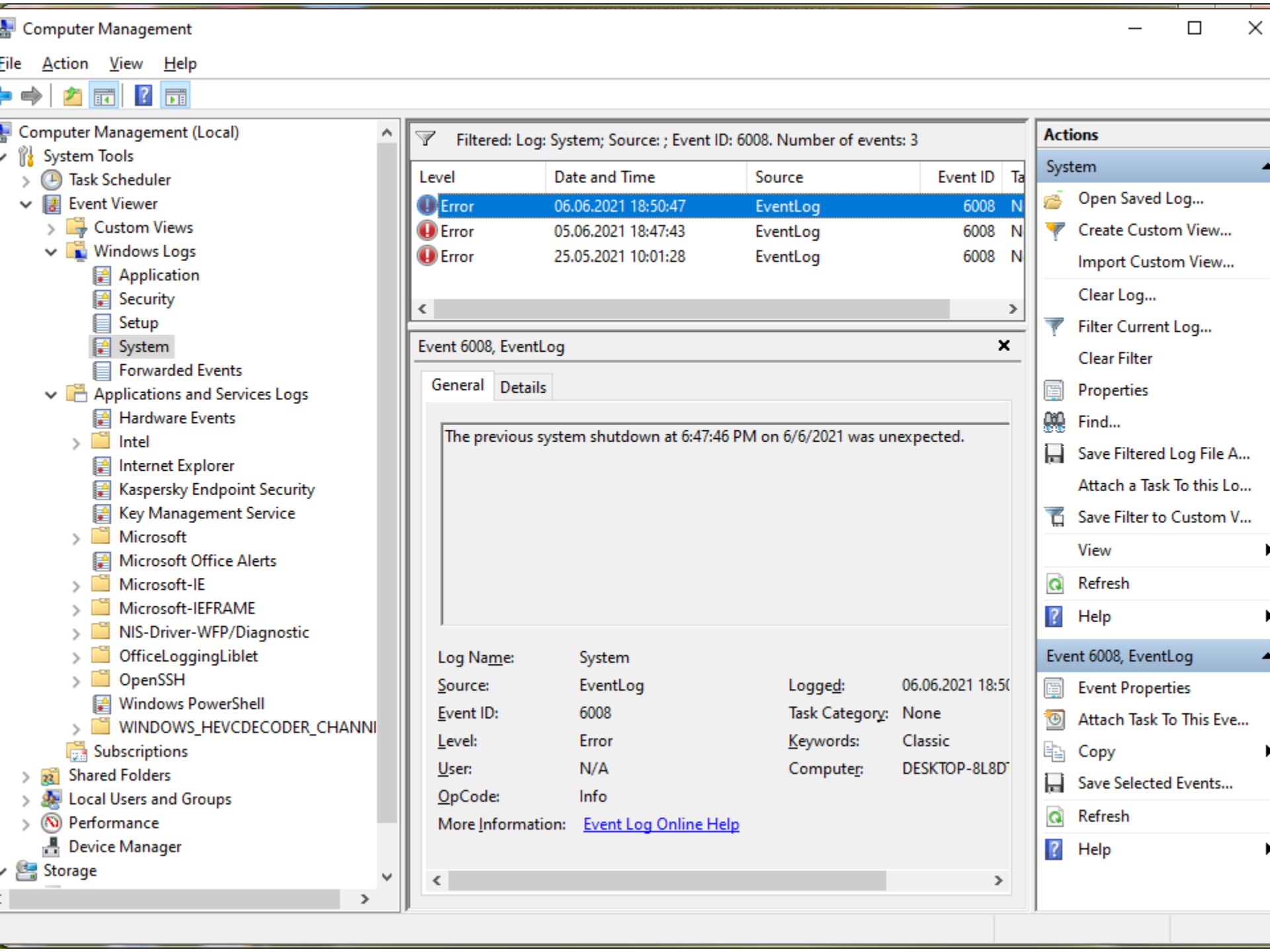
Код - 12- Системное время запуска операционной системы: 2013-09-19T07:04:12.125599400Z.

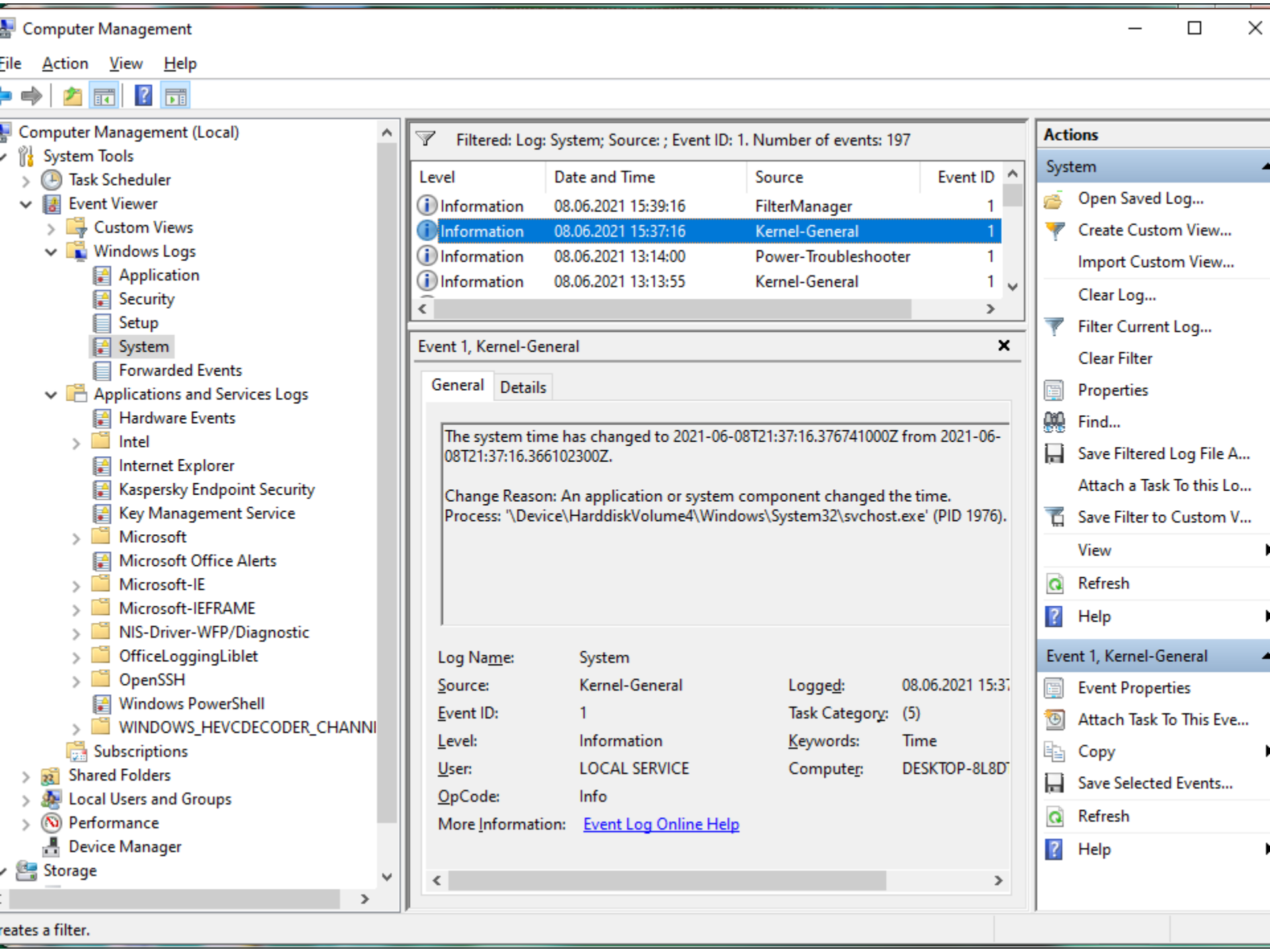
Код - 1- Системное время изменено с 2016-09-14T08:20:13.000000000Z на 2016-09-14T08:20:13.000000000Z.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Intel
Internet Explorer
Kaspersky Endpoint Security
Key Management Service
Microsoft
Microsoft Office Alerts
Microsoft-IE
Microsoft-IEFRAME
NIS-Driver-WFP/Diagnostic
OfficeLoggingLiblet
OpenSSH
Windows PowerShell
WINDOWS_HEVCDECODER_CHANNI
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Filtered: Log: System; Source: ; Event ID: 12. Number of events: 90
Level Date and Time Source Event ID
Information 08.06.2021 15:37:47 Kernel-General 12
Information 08.06.2021 13:14:00 UserModePowerServ... 12
Information 08.06.2021 13:14:00 UserModePowerServ... 12
Information 08.06.2021 13:04:49 UserModePowerServ... 12
Event 12, Kernel-General
General Details
The operating system started at system time 2021-06-08T21:37:46.500000000Z.
Log Name: System
Source: Kernel-General
Logged: 08.06.2021 15:37
Event ID: 12
Task Category: (1)
Level: Information
Keywords: (128)
User: СИСТЕМА
Computer: DESKTOP-8L8D
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File A...
Attach a Task To this Lo...
Save Filter to Custom V...
View
Refresh
Help
Event 12, Kernel-General
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Intel
Internet Explorer
Kaspersky Endpoint Security
Key Management Service
Microsoft
Microsoft Office Alerts
Microsoft-IE
Microsoft-IEFRAME
NIS-Driver-WFP/Diagnostic
OfficeLoggingLiblet
OpenSSH
Windows PowerShell
WINDOWS_HEVCDECODER_CHANNI
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Filtered: Log: System; Source: ; Event ID: 13. Number of events: 12
Level Date and Time Source Event ID
Information 08.06.2021 15:37:29 Kernel-General 13
Information 25.05.2021 14:14:55 Kernel-General 13
Information 25.05.2021 8:04:01 Kernel-General 13
Information 25.05.2021 7:58:15 Kernel-General 13
Event 13, Kernel-General
General Details
The operating system is shutting down at system time 2021-06-08T21:37:29.43803
Log Name: System
Source: Kernel-General
Logged: 08.06.2021 15:37
Event ID: 13
Task Category: (2)
Level: Information
Keywords: (128)
User: N/A
Computer: DESKTOP-8L8D
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File A...
Attach a Task To this Lo...
Save Filter to Custom V...
View
Refresh
Help
Event 13, Kernel-General
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
reates a filter.


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Intel
Internet Explorer
Kaspersky Endpoint Security
Key Management Service
Microsoft
Microsoft Office Alerts
Microsoft-IE
Microsoft-IEFRAME
NIS-Driver-WFP/Diagnostic
OfficeLoggingLiblet
OpenSSH
Windows PowerShell
WINDOWS_HEVCDECODER_CHANNI
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Filtered: Log: System; Source: ; Event ID: 6008. Number of events: 3
Level Date and Time Source Event ID Ta
Error 06.06.2021 18:50:47 EventLog 6008 N
Error 05.06.2021 18:47:43 EventLog 6008 N
Error 25.05.2021 10:01:28 EventLog 6008 N
Event 6008, EventLog
General Details
The previous system shutdown at 6:47:46 PM on 6/6/2021 was unexpected.
Log Name: System
Source: EventLog
Logged: 06.06.2021 18:5(
Event ID: 6008
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: DESKTOP-8L8D
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File A...
Attach a Task To this Lo...
Save Filter to Custom V...
View
Refresh
Help
Event 6008, EventLog
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Intel
Internet Explorer
Kaspersky Endpoint Security
Key Management Service
Microsoft
Microsoft Office Alerts
Microsoft-IE
Microsoft-IEFRAME
NIS-Driver-WFP/Diagnostic
OfficeLoggingLiblet
OpenSSH
Windows PowerShell
WINDOWS_HEVCDECODER_CHANNI
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Filtered: Log: System; Source: ; Event ID: 1. Number of events: 197
Level Date and Time Source Event ID
Information 08.06.2021 15:39:16 FilterManager 1
Information 08.06.2021 15:37:16 Kernel-General 1
Information 08.06.2021 13:14:00 Power-Troubleshooter 1
Information 08.06.2021 13:13:55 Kernel-General 1
Event 1, Kernel-General
General Details
The system time has changed to 2021-06-08T21:37:16.376741000Z from 2021-06-08T21:37:16.366102300Z.
Change Reason: An application or system component changed the time.
Process: '\Device\HarddiskVolume4\Windows\System32\svchost.exe' (PID 1976).
Log Name: System
Source: Kernel-General
Logged: 08.06.2021 15:37
Event ID: 1
Task Category: (5)
Level: Information
Keywords: Time
User: LOCAL SERVICE
Computer: DESKTOP-8L8D
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File A...
Attach a Task To this Lo...
Save Filter to Custom V...
View
Refresh
Help
Event 1, Kernel-General
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
reates a filter.

Dispositivos externos

La información sobre los dispositivos externos conectados se almacena en el registro del sistema operativo, los registros de acontecimientos y en el setupapi.dev.log

Datos del registro:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB
Y
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\
Enum\USBSTOR

Estas ramas contienen información sobre el tipo y el tipo de dispositivos conectados, así como su número de serie y un número único (Globally Unique Identifier - GUID) que identifica el dispositivo para el sistema.

Внешние устройства

Информация о подключенных внешних устройствах хранится в реестре операционных систем, журналах событий, файле setupapi.dev.log

Данные из реестра:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB

И

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

В данных ветвях содержится информация о типе и виде подключенных устройств, а так же их серийный номер и уникальный номер ClassGUID.

Contenido de la rama del registro con información sobre la unidad de almacenamiento