

Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
по Лабораторной работе
по дисциплине «Системное программирование»
по теме «Подсистема ввода-вывода в ОС Windows. Разработка драйверов»

Студент гр. БИБ201
Морин Д.А.
«9» мая 2023 г.

Руководитель
Преподаватель
Д.В. Смирнов
«___» _____ 2023 г.

Москва 2023

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ.....	3
2 ОСНОВНАЯ ЧАСТЬ.....	4
2.1 Ход работы.....	4
2.2 Дополнительное задание.....	8
3 ЗАКЛЮЧЕНИЕ.....	12

1 ВВЕДЕНИЕ

В операционной системе Windows существует множество подсистем. Одной из них является подсистема ввода-вывода, которая отвечает за обработку данных, поступающих с таких устройств, как клавиатура, мышь, принтер, сканер, и т.д.

Для работы с устройствами ввода-вывода в Windows используются драйверы, которые обеспечивают взаимодействие между операционной системой и устройством. От правильной работы драйвера зависит корректность работы устройства, поэтому разработка драйверов является важной задачей.

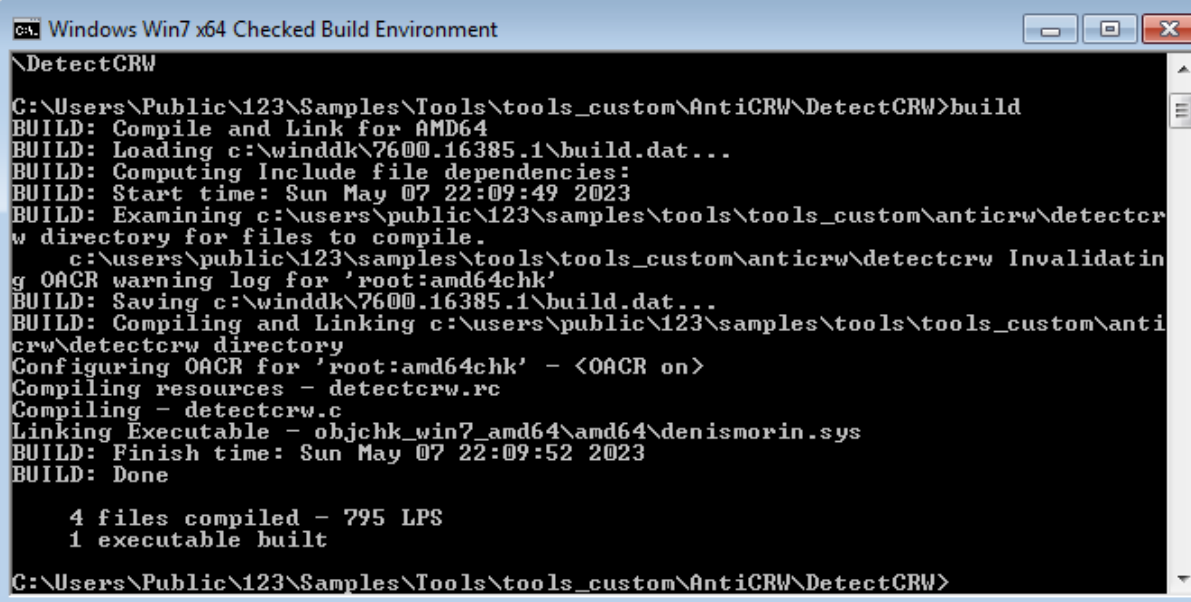
В данном отчете будет произведена подготовка операционной системы к загрузке драйвера режима ядра и программы пользовательского режима в память ОС, компиляция драйвера и программы, установка драйвера и мониторинг действий драйвера и программы.

2 ОСНОВНАЯ ЧАСТЬ

2.1 Ход работы

В ходе лабораторной работы была запущена виртуальная машина Windows 7 с установленными программами Windows Driver Kit (WinDDK) 7.1.0., Notepad++, Process Hacker, DebugView. Далее был разархивирован архив “AntiCRW.7z”, согласно заданию изменены некоторые значения в файлах внутри папки “AntiCRW” на DenisMorin. Далее была проведена перезагрузка виртуальной машины с целью отключения проверки цифровой подписи драйверов (в процессе включения/перезагрузки нажать клавишу F8, чтобы появились дополнительные параметры загрузки, и до того момента, как загрузится операционная система, после выбрать опцию “Disable Driver Signature Enforcement”).

Далее была произведена компиляция драйвера (Рисунок 1).



```
C:\ Windows Win7 x64 Checked Build Environment
\nDetectCRW

C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\DetectCRW>build
BUILD: Compile and Link for AMD64
BUILD: Loading c:\winddk\7600.16385.1\build.dat...
BUILD: Computing Include file dependencies:
BUILD: Start time: Sun May 07 22:09:49 2023
BUILD: Examining c:\users\public\123\samples\tools\tools_custom\anticrw\detectcr
w directory for files to compile.
c:\users\public\123\samples\tools\tools_custom\anticrw\detectcrw Invalidatin
g OACR warning log for 'root:amd64chk'
BUILD: Saving c:\winddk\7600.16385.1\build.dat...
BUILD: Compiling and Linking c:\users\public\123\samples\tools\tools_custom\anti
crw\detectcrw directory
Configuring OACR for 'root:amd64chk' - <OACR on>
Compiling resources - detectcrw.rc
Compiling - detectcrw.c
Linking Executable - objchk_win7_amd64\amd64\denismorin.sys
BUILD: Finish time: Sun May 07 22:09:52 2023
BUILD: Done

4 files compiled - 795 LPS
1 executable built

C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\DetectCRW>
```

Рисунок 1 – Выполнение команды build в папке DetectCRW

Кроме этого, была произведена компиляция программы (Рисунок 2).

```

C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\TerminateCRW>build
BUILD: Compile and Link for AMD64
BUILD: Loading c:\winddk\7600.16385.1\build.dat...
BUILD: Computing Include file dependencies:
BUILD: Start time: Sun May 07 22:21:30 2023
BUILD: Examining c:\users\public\123\samples\tools\tools_custom\anticrw\terminat
ecrw directory for files to compile.
      c:\users\public\123\samples\tools\tools_custom\anticrw\terminatecrw Invalida
ting OACR warning log for 'root:amd64chk'
BUILD: Saving c:\winddk\7600.16385.1\build.dat...
BUILD: Compiling and Linking c:\users\public\123\samples\tools\tools_custom\anti
crw\terminatecrw directory
Configuring OACR for 'root:amd64chk' - <OACR on>
Compiling resources - terminatecrw.rc
Compiling - terminatecrw.c
Compiling - tcrwlib.c
Linking Executable - objchk_win7_amd64\amd64\denismorin.exe
BUILD: Finish time: Sun May 07 22:21:32 2023
BUILD: Done

      5 files compiled - 1 Warning - 1,491 LPS
      1 executable built

C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\TerminateCRW>

```

Рисунок 2 – Выполнение команды build в папке TerminateCRW

Из появившейся директории в папке DetectCRW был найден файл DenisMorin.sys, который был перемещён к файлу DetectCRW.inf, находящийся в DetectCRW. Была произведена инсталляция драйвера командой `rundll32.exe setupapi,InstallHinfSection DefaultInstall 132 C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\DetectCRW\DetectCRW.inf` с правами администратора (Рисунок 3).

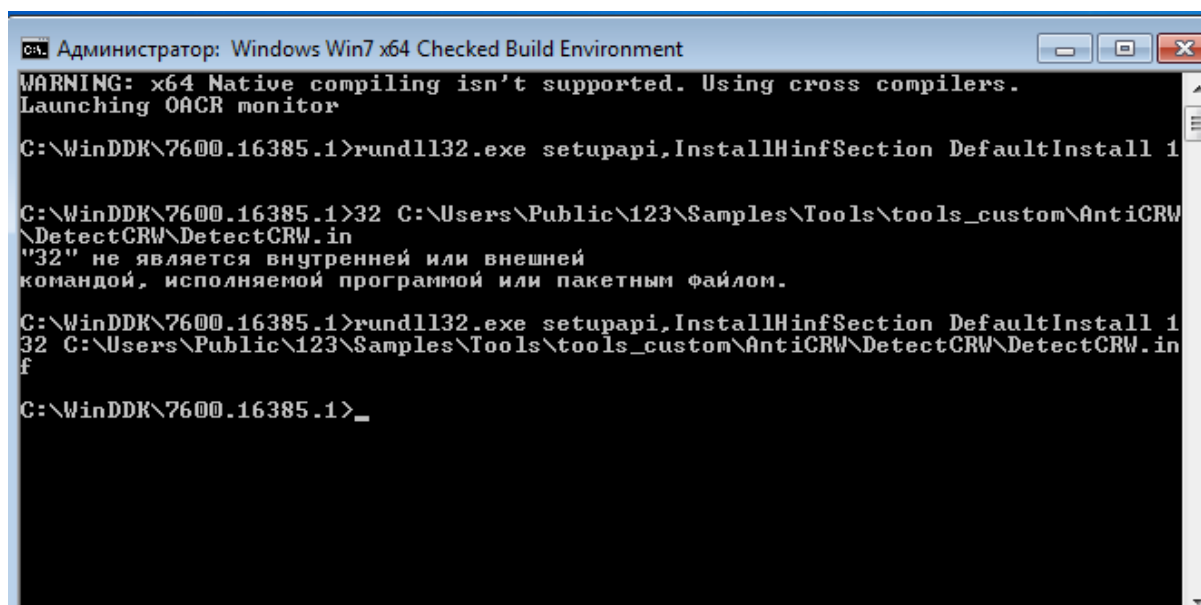


Рисунок 3 – Инсталляция драйвера

После была запущена программа DebugView с правами администратора.

В программе Process Hacker в разделе “Services” была найдена служба драйвера DenisMorin, которая позже была запущена (Рисунок 4).

Service	Автоматические файлы	Start process	Running	Auto start	600
DcomLaunch	Модуль запуска процессов DCOM-...	Share process	Running	Auto start	616
defragsvc	Дефрагментация диска	Own process	Stopped	Demand start	
DenisMorin	DenisMorin	FS driver	Running	Demand start	
DfsC	DFS Namespace Client Driver	FS driver	Running	System start	
Dhcp	DHCP-клиент	Share process	Running	Auto start	788
discache	System Attribute Cache	Driver	Running	System start	
Disk	Лайвер диска	Driver	Running	Boot start	

Рисунок 4 – Запущенная служба драйвера

В окне DebugView стали появляться отладочные сообщения драйвера при старте (Рисунок 5) и при дальнейшей работе драйвера (Рисунок 6).

#	Time	Debug Print
1	23:07:37	DetectCRW!DriverEntry: Entered
2	23:07:37	DetectCRW!DetectCRWCreateCommunicationPort: Entered
3	23:07:37	DetectCRW!DetectCRWCreateCommunicationPort: FltBuildDefaultSecurityDescriptor returns 00000000
4	23:07:37	DetectCRW!DetectCRWCreateCommunicationPort: FltCreateCommunicationPort returns 00000000
5	23:07:37	DetectCRW!DetectCRWInstanceSetup: Entered
6	23:07:37	DetectCRW!DetectCRWInstanceSetup: Entered
7	23:07:37	DetectCRW!DetectCRWInstanceSetup: Entered
8	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Entered
9	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: query file is "{3164e9cb-7c35-4438-9095-86427170c559}"
10	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Entered
11	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: query file is ""
12	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Entered
13	23:07:41	DetectCRW!DetectCRWSendMessage: Entered
14	23:07:41	DetectCRW!DetectCRWSendMessage: buf is "1192","2016","\Device\HarddiskVolume2\Windows\System32\wdi\{86...
15	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Entered
16	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Data isn't for DetectCRW
17	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: Entered

Рисунок 5 – Отладочные сообщения драйвера при старте в DebugView

12	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Entered
13	23:07:41	DetectCRW!DetectCRWSendMessage: Entered
14	23:07:41	DetectCRW!DetectCRWSendMessage: buf is "1192","2016","\Device\HarddiskVolume2\Windows\System32\wdi\{86...
15	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Entered
16	23:07:41	DetectCRW!DetectCRWPostDirectoryControl: Data isn't for DetectCRW
17	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: Entered
18	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: query file is "ARIAL.TTF"
19	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: Entered
20	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: query file is "ARIALI.TTF"
21	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: Entered
22	23:07:57	DetectCRW!DetectCRWPostDirectoryControl: query file is "ARIALBD.TTF"

Рисунок 5 – Отладочные сообщения драйвера при работе драйвера в DebugView

Открыв программу пользовательского режима с правами администратора, можно заметить, как DebugView последовательно отображает директории, которые находятся по пути к исполняемому файлу DenisMorin.exe (Рисунок 6).

```
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: query file is "AntiCRW"
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: query file is "TerminateCRW"
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: query file is "objchk_win7_amd64"
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:32 DetectCRW!DetectCRWPostDirectoryControl: query file is "amd64"
4... 23:40:44 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:44 DetectCRW!DetectCRWPostDirectoryControl: query file is "DenisMorin.exe"
4... 23:40:44 DetectCRW!DetectCRWConnect: Entered
4... 23:40:49 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:49 DetectCRW!DetectCRWPostDirectoryControl: Data isn't for DetectCRW
4... 23:40:49 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:49 DetectCRW!DetectCRWPostDirectoryControl: Data isn't for DetectCRW
4... 23:40:49 DetectCRW!DetectCRWPostDirectoryControl: Entered
4... 23:40:49 DetectCRW!DetectCRWPostDirectoryControl: Data isn't for DetectCRW

Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Windows\system32>cd C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\Te
rminateCRW\objchk_win7_amd64\amd64
C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\TerminateCRW\objchk_win7_
amd64\amd64>DenisMorin.exe
main: Entered
AllocAndZeroGlobalOpInfoMemory: Entered
AllocAndZeroRulesMemory: Entered
ReadRules: Entered
CommunicateWithFilter: Entered
AllocAndZeroMessageInfoMemory: Entered
CommunicateWithFilter: FilterConnectCommunicationPort is OK
DebugAndTerminate: Entered
```

Рисунок 6 – Запуск программы пользовательского режима с правами администратора

После в другой командной строке записывается команда dir и запускается, что вызывает предупреждение функцией AskUser (в файле TerminateCRW.c) о том, прекратить ли действие или нет (Рисунок 7).

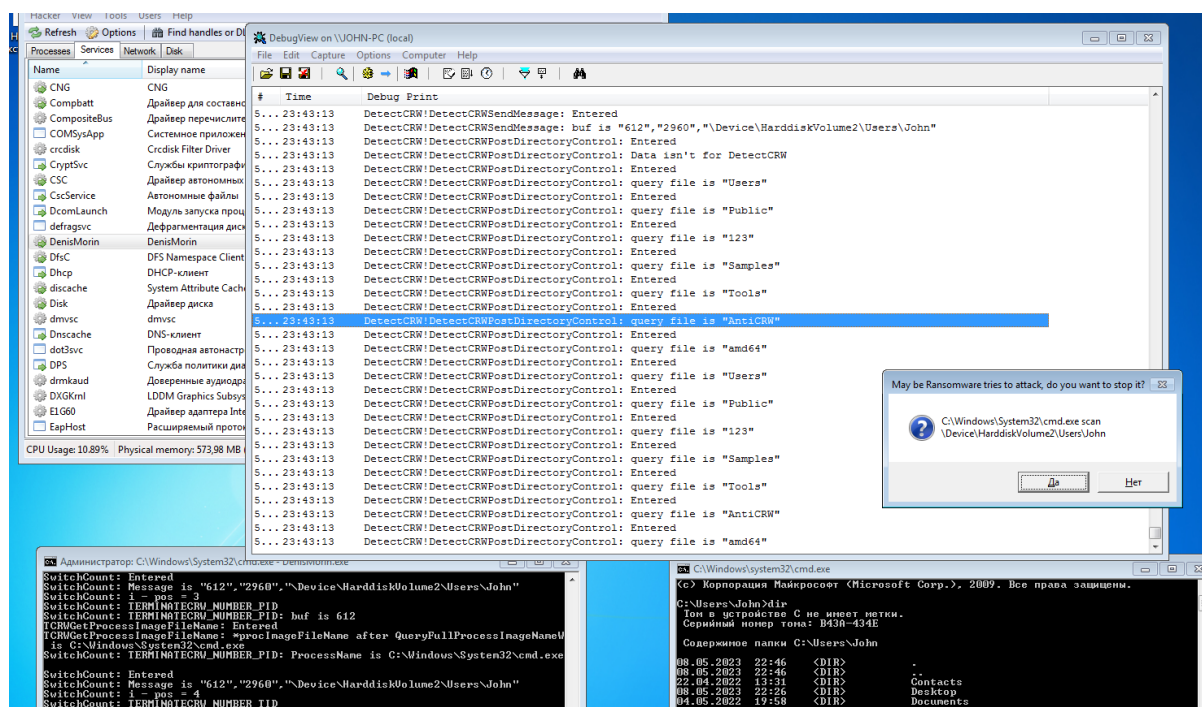


Рисунок 7 – Появление всплывающего окна

2.2 Дополнительное задание

1. Драйверы могут мониторить различные события в файловой системе с помощью различных кодов IRP_MJ (Major Function Code). В DetectCRW.c используется код IRP_MJ_DIRECTORY_CONTROL (шестнадцатеричный код 0x0C), который указывает, что драйвер должен реагировать на операции с директориями, такие как создание, удаление и переименование файлов внутри директории, с использованием функций DetectCRWPreDirectoryControl и DetectCRWPostDirectoryControl.

Драйвер файловой системы должен проверить дополнительный код функции, чтобы определить, какая операция управления каталогом запрашивается. IRP_MN_QUERY_DIRECTORY представляет собой операцию запроса содержимого директории в файловой системе. Она используется, например, для получения списка файлов и подкаталогов в указанной директории.

В DetectCRW.c файле IRP_MN_QUERY_DIRECTORY используется как один из критериев для проверки параметров операции ввода-вывода (I/O), переданных в структуру FLT_CALLBACK_DATA. Когда IRP_MJ_DIRECTORY_CONTROL завершается, DetectCRWPostDirectoryControl вызывается для обработки результатов операции (и используется проверка на IRP_MN_QUERY_DIRECTORY, чтобы убедиться, что операция запроса содержимого директории была успешно завершена).

Код IRP_MJ_DIRECTORY_CONTROL генерируется при обращении к директории файловой системы, когда необходимо выполнить какую-либо операцию с содержимым этой директории (например, когда приложение открывает директорию или запрашивает информацию о файлах, находящихся в этой директории).

2. Если операционная система устанавливает флаг isUsed для операции, то программа пользовательского режима сохраняет информацию об операции в глобальном массиве операций globalOpsInfo, чтобы в дальнейшем запросить пользователя на остановку процесса.

Когда пользователь запускает программ, она загружает правила из файла, вызывает функцию AskUserAndTerminate, которая ожидает запрос на остановку (и запускает функцию CommunicateWithFilter, которая устанавливает связь с драйвером через порт DETECTCRW_PORT_NAME).

Когда драйвер обнаруживает подозрительный процесс, он отправляет сообщение программе пользователя через порт DETECTCRW_PORT_NAME. Если подходящее правило найдено в загруженном массиве правил, программа выводит уведомление пользователю через диалоговое окно MessageBoxW, которое спрашивает, хочет ли пользователь остановить подозрительный процесс.

Для того чтобы остановить процесс, программа пользователя вызывает функцию `TerminateThread` с дескриптором потока, который был сохранен ранее в `globalOpsInfo`. Если пользователь отказывается остановить процесс, программа вызывает функцию `ResumeThread` для продолжения работы потока.

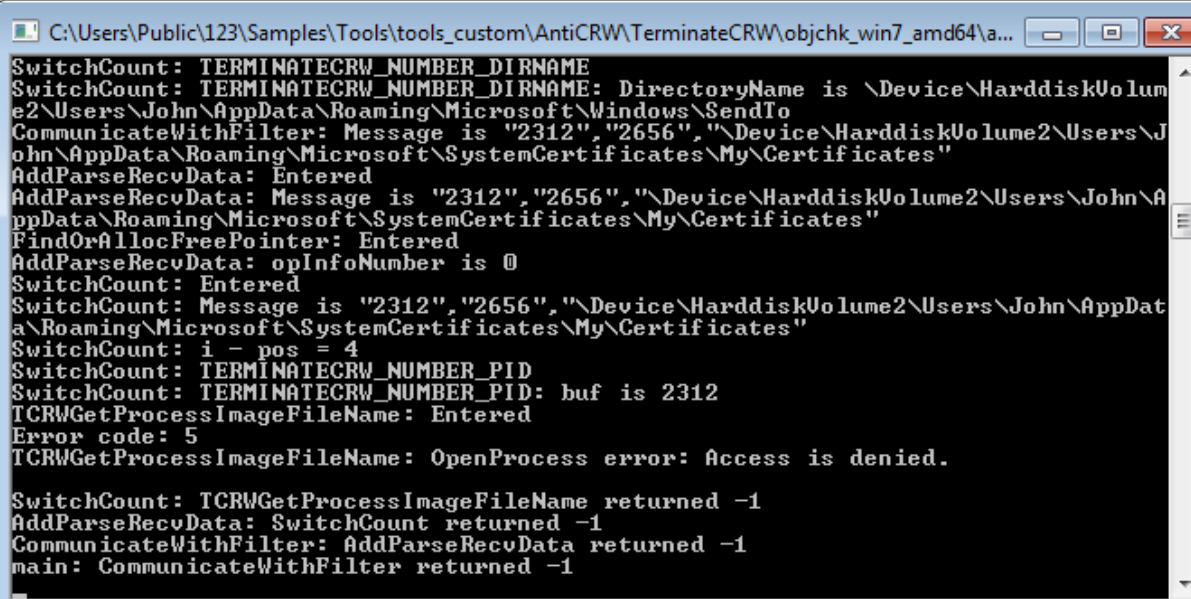
Вообще, функция `AskUser` (которая выводит диалоговое окно) вызывается всякий раз, когда в массиве `globalOpsInfo` есть хотя бы один элемент, который не равен `NULL` и используется (когда `isUsed == TRUE`, `DirectoryName != NULL` и `ProcessName != NULL`).

3. `DetectCRWPreDirectoryControl` и `DetectCRWPostDirectoryControl` являются функциями обратного вызова для перехвата и потенциального изменения операций файловой системы.

`DetectCRWPreDirectoryControl` позволяет прервать операцию файловой системы или изменить ее параметры до ее выполнения. Он вызывается до обработки операции драйвером файловой системы, но просто возвращает `FLT_PREOP_SUCCESS_WITH_CALLBACK` согласно коду (работа будет протекать в обычном режиме, без каких-либо изменений, вносимых фильтром).

`DetectCRWPostDirectoryControl` вызывается после завершения операции. Он проверяет, является ли операция операцией каталога запросов (`IRP_MN_QUERY_DIRECTORY`) и была ли она успешной (`STATUS_SUCCESS`). Затем он проверяет, является ли файловый объект, связанный с операцией, ненулевым и имеет ли операция запроса каталога ненулевое имя файла. Если эти условия выполнены, то вызывается `DetectCRWSendMessage` для отправки сообщения, указывающего, что в каталоге была выполнена операция запроса каталога. Если вызов этой функции завершается успешно, она возвращает `FLT_POSTOP_FINISHED_PROCESSING` (операция успешно завершена).

4. Ошибка, представленная на рисунке 8, вызывается, когда дескриптор при открытии процесса (функция `OpenProcess`) является пустым (`NULL`). Вызвав функцию `GetLastError` для получения дополнительных сведений об ошибке, она сообщила “Access is denied”. Таким образом, данная ошибка вызвана нехваткой привилегий доступа и может быть получена, если запустить приложение с правами администратора.



```
C:\Users\Public\123\Samples\Tools\tools_custom\AntiCRW\TerminateCRW\objchk_win7_amd64\...
SwitchCount: TERMINATECRW_NUMBER_DIRNAME
SwitchCount: TERMINATECRW_NUMBER_DIRNAME: DirectoryName is \Device\HarddiskVolum
e2\Users\John\AppData\Roaming\Microsoft\Windows\SendTo
CommunicateWithFilter: Message is "2312","2656","\Device\HarddiskVolume2\Users\J
ohn\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates"
AddParseRecvData: Entered
AddParseRecvData: Message is "2312","2656","\Device\HarddiskVolume2\Users\John\A
ppData\Roaming\Microsoft\SystemCertificates\My\Certificates"
FindOrAllocFreePointer: Entered
AddParseRecvData: opInfoNumber is 0
SwitchCount: Entered
SwitchCount: Message is "2312","2656","\Device\HarddiskVolume2\Users\John\AppData
a\Roaming\Microsoft\SystemCertificates\My\Certificates"
SwitchCount: i - pos = 4
SwitchCount: TERMINATECRW_NUMBER_PID
SwitchCount: TERMINATECRW_NUMBER_PID: buf is 2312
TCRWGetProcessImageFileName: Entered
Error code: 5
TCRWGetProcessImageFileName: OpenProcess error: Access is denied.

SwitchCount: TCRWGetProcessImageFileName returned -1
AddParseRecvData: SwitchCount returned -1
CommunicateWithFilter: AddParseRecvData returned -1
main: CommunicateWithFilter returned -1
```

Рисунок 8 – Некорректное завершение программы

3 ЗАКЛЮЧЕНИЕ

В процессе выполнения данной лабораторной работы были получены знания о том, как работает подсистема ввода-вывода в операционной системе Windows, а также о том, как создавать драйверы-минифильтры. Кроме того, были получены навыки компилирования драйверов с помощью Windows Driver Kits и анализа отладочных сообщений драйверов при помощи инструмента DebugView.