НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО Факультет Программной Инженерии и Компьютерной Техники

Информационная безопасность Лабораторная работа № 4

Выполнили студенты:

Маслова Ксения, Группа № Р34681

Неизвестная Екатерина, Группа № Р34701

Морозова Екатерина, Группа № Р34681

Вдовенко Мария, Группа № Р34684

Преподаватель: Оголюк Александр Александрович

г. Санкт-Петербург

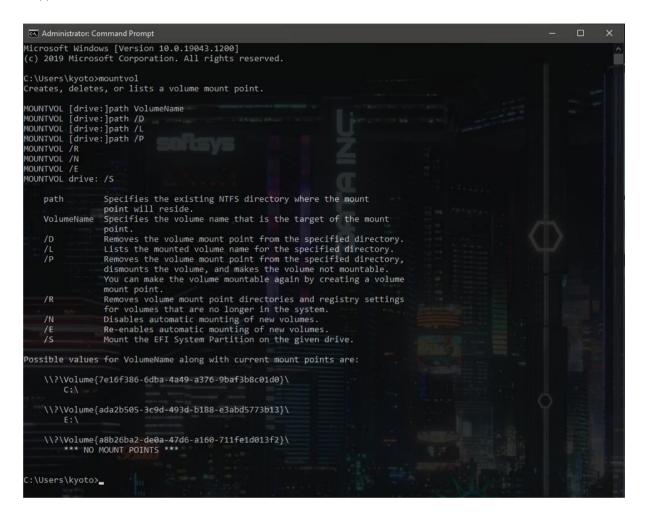
Лабораторная работа № 4 Ознакомление с утилитой монтирования томов mountvol и утилитами по созданию ссылок.

- 1. Запустить в ком. строке утилиту без параметров (посмотреть подсказку). Создать новую точку подключения для логич. диска с файловой системой NTFS.

 Установить разграничения (из RWXDPO) на саму папку D:\TEMP_E и отдельно (отличающиеся) на диск E: Проверить доступ, обращаясь к файлам через папку D:\TEMP_E и диск E: Привести различия в доступе (если есть). Использовать разные комбинации разграничений (RX<->RWPO и т.п.)
- 2. Проделать те же действия (Исследовать возможности разграничения доступа), но уже для ссылок на файловые объекты (каталоги и файлы: symbolic/hard link), используя утилиту makelink (или подобные) или FAR (ALT + F6)

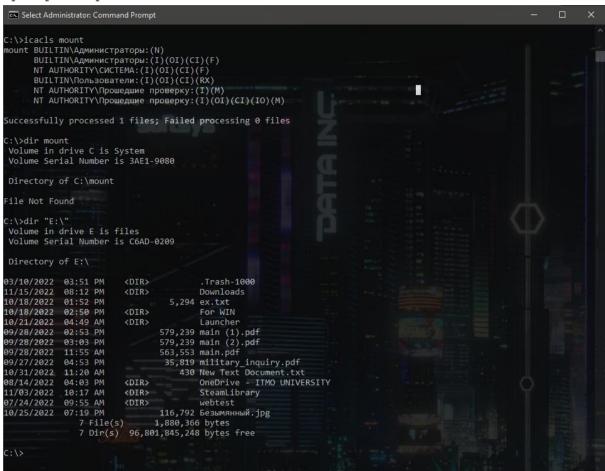
Ex. 1:

Подсказка



```
Possible values for VolumeName along with current mount points are:
    \\?\Volume{7e16f386-6dba-4a49-a376-9baf3b8c01d0}\
    \\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\
    \\?\Volume{a8b26ba2-de0a-47d6-a160-711fe1d013f2}\
         *** NO MOUNT POINTS ***
C:\>mkdir mount
C:\>mountvol mount \\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\ Documents
Creates, deletes, or lists a volume mount point.
MOUNTVOL [drive:]path VolumeName
MOUNTVOL [drive:]path /D
MOUNTVOL [drive:]path /L
MOUNTVOL [drive:]path /P
MOUNTVOL /R
MOUNTVOL /N
MOUNTVOL /E
MOUNTVOL drive: /S
                  Specifies the existing NTFS directory where the mount
    path
                  point will reside.
                 Specifies the volume name that is the target of the mount
    VolumeName
                  point.
                 Removes the volume mount point from the specified directory. Lists the mounted volume name for the specified directory.
    /D
                  Removes the volume mount point from the specified directory,
    /P
                  dismounts the volume, and makes the volume not mountable.
                  You can make the volume mountable again by creating a volume
                  mount point.
                 Removes volume mount point directories and registry settings
    /R
                  for volumes that are no longer in the system.
                 Disables automatic mounting of new volumes.
                 Re-enables automatic mounting of new volumes.
    /E
    15
                 Mount the EFI System Partition on the given drive.
Possible values for VolumeName along with current mount points are:
    \\?\Volume{7e16f386-6dba-4a49-a376-9baf3b8c01d0}\
    \\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\
        E:\
        C:\mount\
    \\?\Volume{a8b26ba2-de0a-47d6-a160-711fe1d013f2}\
*** NO MOUNT POINTS ***
```

Проверка ограничений



Редактирование файла с правами только чтение на маунт

```
Administrator: Command Prompt
 :\>icacls mount
 ::\>lcals mount

ount HOME-PC\kyoto:(R)

BUILTIN\Администраторы:(I)(OI)(CI)(F)

NT AUTHORITY\CUCTEMA:(I)(OI)(CI)(F)

BUILTIN\Пользователи:(I)(OI)(CI)(RX)

NT AUTHORITY\Прошедшие проверку:(I)(M)

NT AUTHORITY\Прошедшие проверку:(I)(OI)(CI)(IO)(M)
Successfully processed 1 files; Failed processing 0 files
C:\>dir > E:\type.txt
 ::\>dir > mount\type.txt
C:\>echo mount\type.txt
 nount\type.txt
 C:\>type mount\type.txt
Volume in drive C is System
Volume Serial Number is 3AE1-9080
 Directory of C:\
03/12/2022 04:31 PM
                                                             .Trash-1000
02/06/2022 05:48 PM
11/02/2022 10:49 PM
                                                           Downloads
HxD
                                    <DIR>
                                                           mount [\??\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\]
Program Files
Program Files (x86)
11/29/2022
                                     <JUNCTION>
11/15/2022
                  02:05 PM
09/15/2022
                 07:29 PM
                                    <DIR>
11/29/2022 02:47 PM
                                                             Temp
10/26/2022 03:11 AM
08/15/2022 04:21 PM
                                    <DIR>
                                                           Users
                                                           Windows
                                    <DIR>
                      0 File(s)
                                                          0 bytes
                       9 Dir(s)
                                     4,937,523,200 bytes free
  : \>_
```

вывод: Если ты можешь прочитать маунт поинт, ограничения доступа на операции с файлами внутри берутся из исходной директории.

Ex. 2:

Ссылки: права доступа дублируются между символической ссылкой, жесткой ссылкой и файлом

То же самое и с директорией, только на директорию создавать жесткие ссылки запрещено

```
Administrator: Command Prompt
C:\Users\kyoto>icacls text.txt
text.txt BUILTIN\Администраторы:(F)
                     NT AUTHORITY\CUCTEMA:(I)(F)
                     BUILTIN\Администраторы: (I)(F)
                    HOME-PC\kyoto:(I)(F)
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls textlink.txt
textlink.txt BUILTIN\Администраторы:(F)
                              NT AUTHORITY\CUCTEMA:(I)(F)
                              BUILTIN\Администраторы:(I)(F)
                              HOME-PC\kyoto:(I)(F)
Successfully processed 1 files; Failed processing 0 files
 C:\Users\kyoto>icacls texthardlink.txt
c. toser in fire the control of the
                                       NT AUTHORITY\CUCTEMA:(I)(F)
                                       BUILTIN\Администраторы:(I)(F)
                                       HOME-PC\kyoto:(I)(F)
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls text.txt /deny Администраторы:N
Invalid parameter "Администраторы:N"
C:\Users\kyoto>icacls text.txt /deny Администраторы:F
processed file: text.txt
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls text.txt
text.txt BUILTIN\Администраторы:(N)
                    NT AUTHORITY\CUCTEMA:(I)(F)
BUILTIN\Aдминистраторы:(I)(F)
                    HOME-PC\kyoto:(I)(F)
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls textlink.txt
textlink.txt BUILTIN\Администраторы:(N)
                              NT AUTHORITY\CUCTEMA:(I)(F)
                              BUILTIN\Администраторы:(I)(F)
                              HOME-PC\kyoto:(I)(F)
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls texthardlink.txt
texthardlink.txt BUILTIN\Администраторы:(N)
                                       NT AUTHORITY\CUCTEMA:(I)(F)
                                        BUILTIN\Администраторы: (I)(F)
                                        HOME-PC\kyoto:(I)(F)
Successfully processed 1 files; Failed processing 0 files
 :\Users\kyoto>S_
```

```
C:\Users\kyoto>mklink /D DoCUMentslink Documents
symbolic link created for DoCUMentslink <<===>> Documents
C:\Users\kyoto>icacls Documents
Documents NT AUTHORITY\CMCTEMA:(I)(0I)(CI)(F)
            BUILTIN\Администраторы: (Î)(OÎ)(CÎ)(F)
            HOME-PC\kyoto:(I)(OI)(CI)(F)
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls Documents /grant Администраторы:F
processed file: Documents
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>mklink /D /H DoCUMentshardlink Documents
Access is denied.
C:\Users\kyoto>mklink /H DoCUMentshardlink Documents
Access is denied.
C:\Users\kyoto>icacls DoCUMentslink
DoCUMentslink BUILTIN\Администраторы:(F)
                 NT AUTHORITY\CUCTEMA:(I)(OI)(CI)(F)
BUILTIN\Admunuctpatopы:(I)(OI)(CI)(F)
HOME-PC\kyoto:(I)(OI)(CI)(F)
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>icacls DoCUMentslink /deny Администраторы:F
processed file: DoCUMentslink
Successfully processed 1 files; Failed processing 0 files
C:\Users\kyoto>dir Documents
 Volume in drive C is System
Volume Serial Number is 3AE1-9080
 Directory of C:\Users\kyoto\Documents
File Not Found
C:\Users\kyoto>
```