

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

2022

## 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. Прodelать 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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1200]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\kyoto>mountvol
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

path          Specifies the existing NTFS directory where the mount
              point will reside.
VolumeName    Specifies the volume name that is the target of the mount
              point.
/D            Removes the volume mount point from the specified directory.
/L            Lists the mounted volume name for the specified directory.
/P            Removes the volume mount point from the specified directory,
              dismounts the volume, and makes the volume not mountable.
              You can make the volume mountable again by creating a volume
              mount point.
/R            Removes volume mount point directories and registry settings
              for volumes that are no longer in the system.
/N            Disables automatic mounting of new volumes.
/E            Re-enables automatic mounting of new volumes.
/S            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}\
C:\
\\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\
E:\
\\?\Volume{a8b26ba2-de0a-47d6-a160-711fe1d013f2}\
*** NO MOUNT POINTS ***

C:\Users\kyoto>
```

Маунт

Possible values for VolumeName along with current mount points are:

\\?\Volume{7e16f386-6dba-4a49-a376-9baf3b8c01d0}\  
C:\

\\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\  
E:\

\\?\Volume{a8b26ba2-de0a-47d6-a160-711fe1d013f2}\  
\*\*\* NO MOUNT POINTS \*\*\*

C:\>mkdir mount

C:\>mountvol mount \\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\

C:\>mountvol

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

path	Specifies the existing NTFS directory where the mount point will reside.
VolumeName	Specifies the volume name that is the target of the mount point.
/D	Removes the volume mount point from the specified directory.
/L	Lists the mounted volume name for the specified directory.
/P	Removes the volume mount point from the specified directory, dismounts the volume, and makes the volume not mountable. You can make the volume mountable again by creating a volume mount point.
/R	Removes volume mount point directories and registry settings for volumes that are no longer in the system.
/N	Disables automatic mounting of new volumes.
/E	Re-enables automatic mounting of new volumes.
/S	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}\  
C:\

\\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\  
E:\  
C:\mount\

\\?\Volume{a8b26ba2-de0a-47d6-a160-711fe1d013f2}\  
\*\*\* NO MOUNT POINTS \*\*\*

C:\>

## Проверка ограничений

```
CA: Select Administrator: Command Prompt

C:\>icacls mount
mount BUILTIN\Администраторы:(N)
      BUILTIN\Администраторы:(I)(OI)(CI)(F)
      NT AUTHORITY\СИСТЕМА:(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 mount
Volume in drive C is System
Volume Serial Number is 3AE1-9080

Directory of C:\mount

File Not Found

C:\>dir "E:\\"
Volume in drive E is files
Volume Serial Number is C6AD-0209

Directory of E:\

03/10/2022  03:51 PM  <DIR>          .Trash-1000
11/15/2022  08:12 PM  <DIR>          Downloads
10/18/2022  01:52 PM             5,294 ex.txt
10/18/2022  02:50 PM  <DIR>          For WIN
10/21/2022  04:49 AM  <DIR>          Launcher
09/28/2022  02:53 PM             579,239 main (1).pdf
09/28/2022  03:03 PM             579,239 main (2).pdf
09/28/2022  11:55 AM             563,553 main.pdf
09/27/2022  04:53 PM             35,819 military_inquiry.pdf
10/31/2022  11:20 AM             430 New Text Document.txt
08/14/2022  04:03 PM  <DIR>          OneDrive - ITMO UNIVERSITY
11/03/2022  10:17 AM  <DIR>          SteamLibrary
07/24/2022  09:55 AM  <DIR>          webtest
10/25/2022  07:19 PM             116,792 Безымянный.jpg
              7 File(s)          1,880,366 bytes
              7 Dir(s)          96,801,845,248 bytes free

C:\>
```

## Редактирование файла с правами только чтение на маунт

```
CA: Administrator: Command Prompt

C:\>icacls mount
mount HOME-PC\kyoto:(R)
      BUILTIN\Администраторы:(I)(OI)(CI)(F)
      NT AUTHORITY\СИСТЕМА:(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

C:\>dir > mount\type.txt

C:\>echo mount\type.txt
mount\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  <DIR>          .Trash-1000
02/06/2022  05:48 PM  <DIR>          Downloads
11/02/2022  10:49 PM  <DIR>          HxD
11/29/2022  12:23 PM  <JUNCTION>    mount [\\?\Volume{ada2b505-3c9d-493d-b188-e3abd5773b13}\]
11/15/2022  02:05 PM  <DIR>          Program Files
09/15/2022  07:29 PM  <DIR>          Program Files (x86)
11/29/2022  02:47 PM  <DIR>          Temp
10/26/2022  03:11 AM  <DIR>          Users
08/15/2022  04:21 PM  <DIR>          Windows
              0 File(s)          0 bytes
              9 Dir(s)          4,937,523,200 bytes free

C:\>
```



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

Ех. 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\СИСТЕМА:(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\СИСТЕМА:(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:(F)
                  NT AUTHORITY\СИСТЕМА:(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\СИСТЕМА:(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:(N)
              NT AUTHORITY\СИСТЕМА:(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\СИСТЕМА:(I)(F)
                  BUILTIN\Администраторы:(I)(F)
                  HOME-PC\kyoto:(I)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\kyoto>S_
```

```
C:\Users\kyoto>mklink /D DoCUMentslink Documents
symbolic link created for DoCUMentslink <=> Documents
```

```
C:\Users\kyoto>icacls Documents
Documents NT AUTHORITY\СИСТЕМА:(I)(OI)(CI)(F)
        BUILTIN\Администраторы:(I)(OI)(CI)(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\СИСТЕМА:(I)(OI)(CI)(F)
        BUILTIN\Администраторы:(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>
```