НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Информационная безопасность

Лабораторная работа № 4

Выполнили студенты:

Маслова Ксения, Группа № P34681

Неизвестная Екатерина, Группа № P34701

Морозова Екатерина, Группа № P34681

Вдовенко Мария, Группа № P34684

Преподаватель: Оголюк Александр Александрович

г. Санкт-Петербург

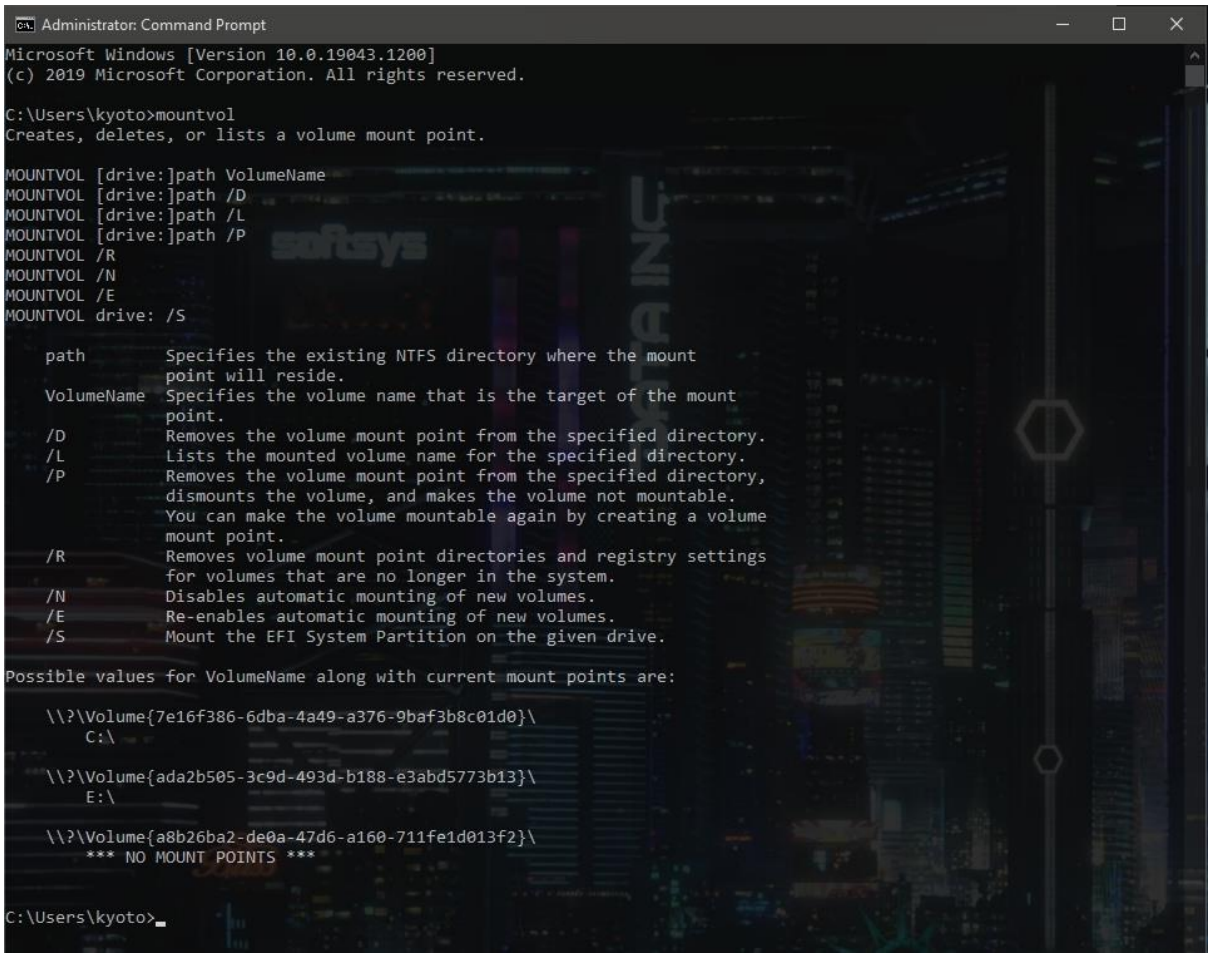
2022

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. 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:

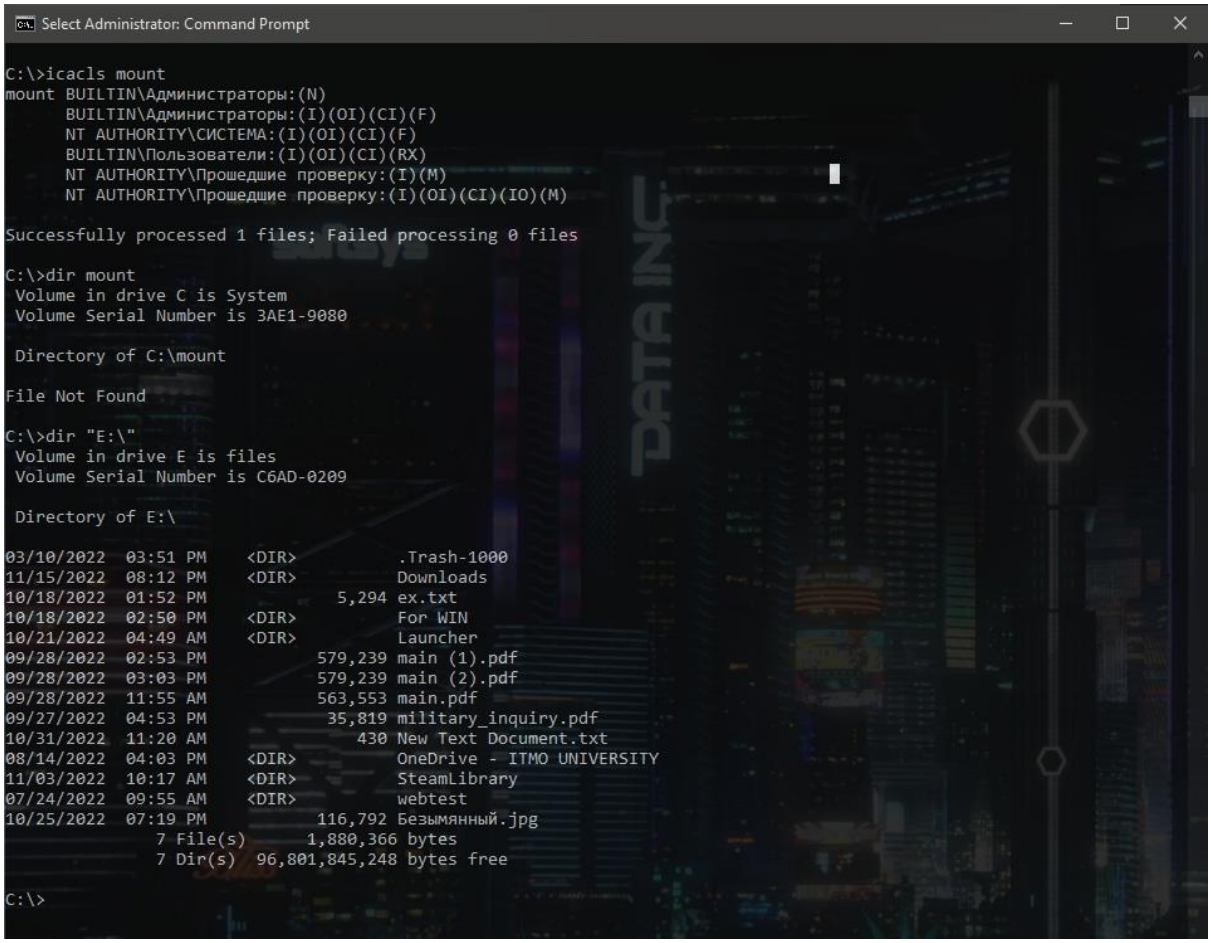
Подсказка



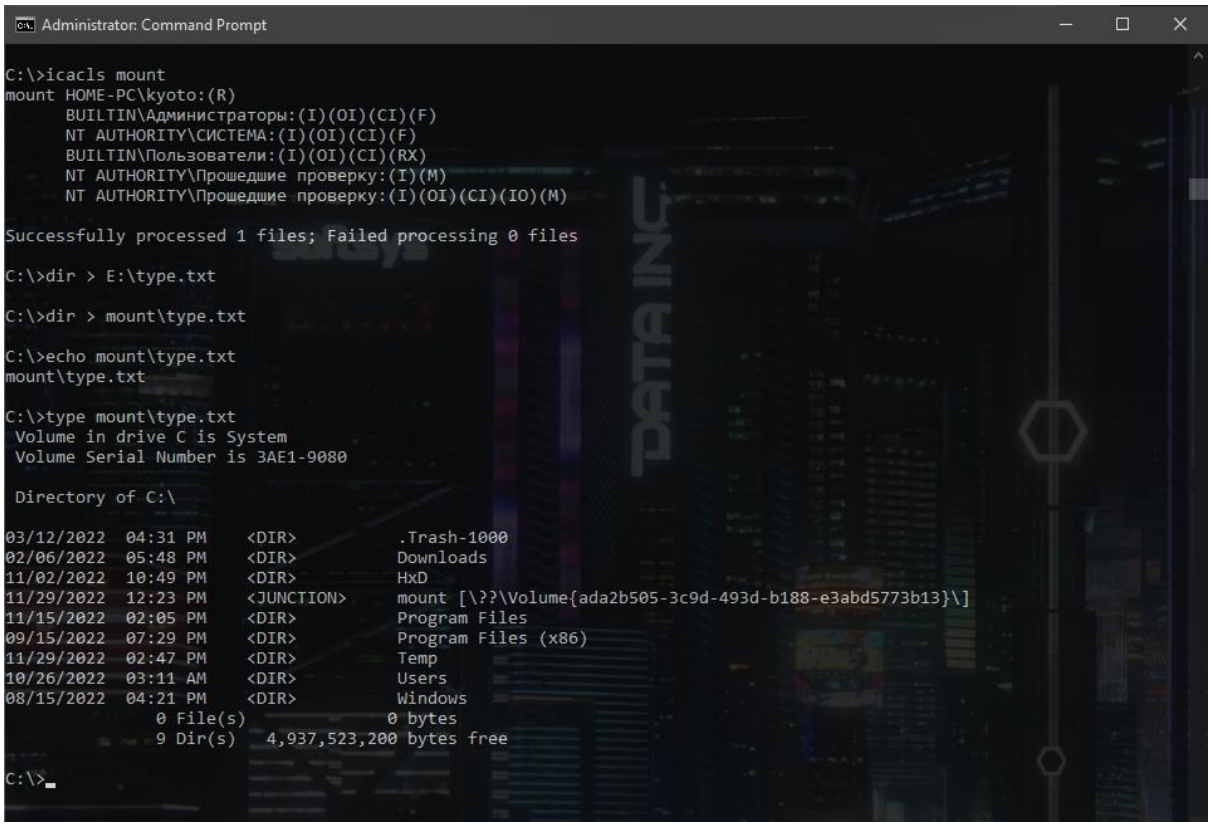
Маунт


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



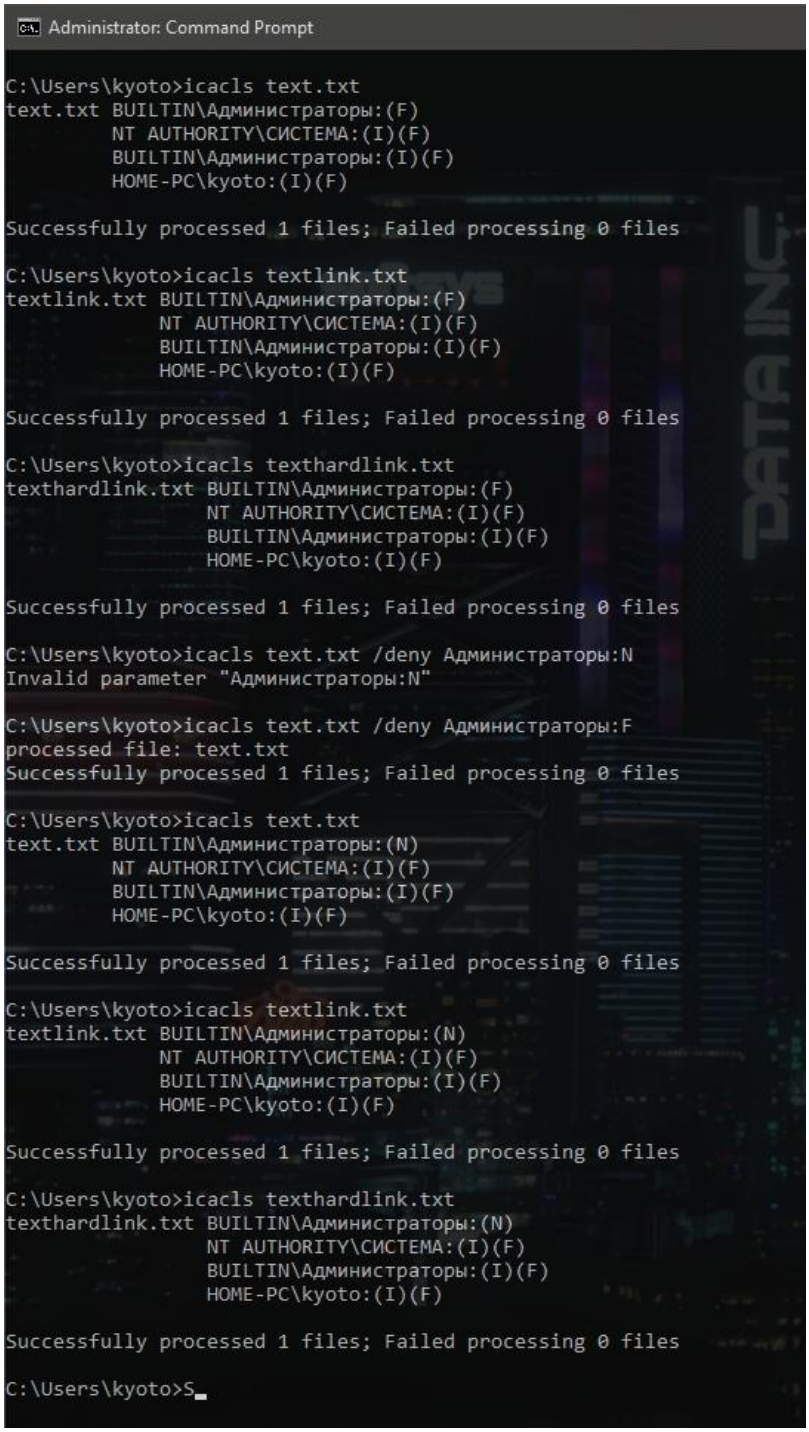
Редактирование файла с правами только чтение на маунт

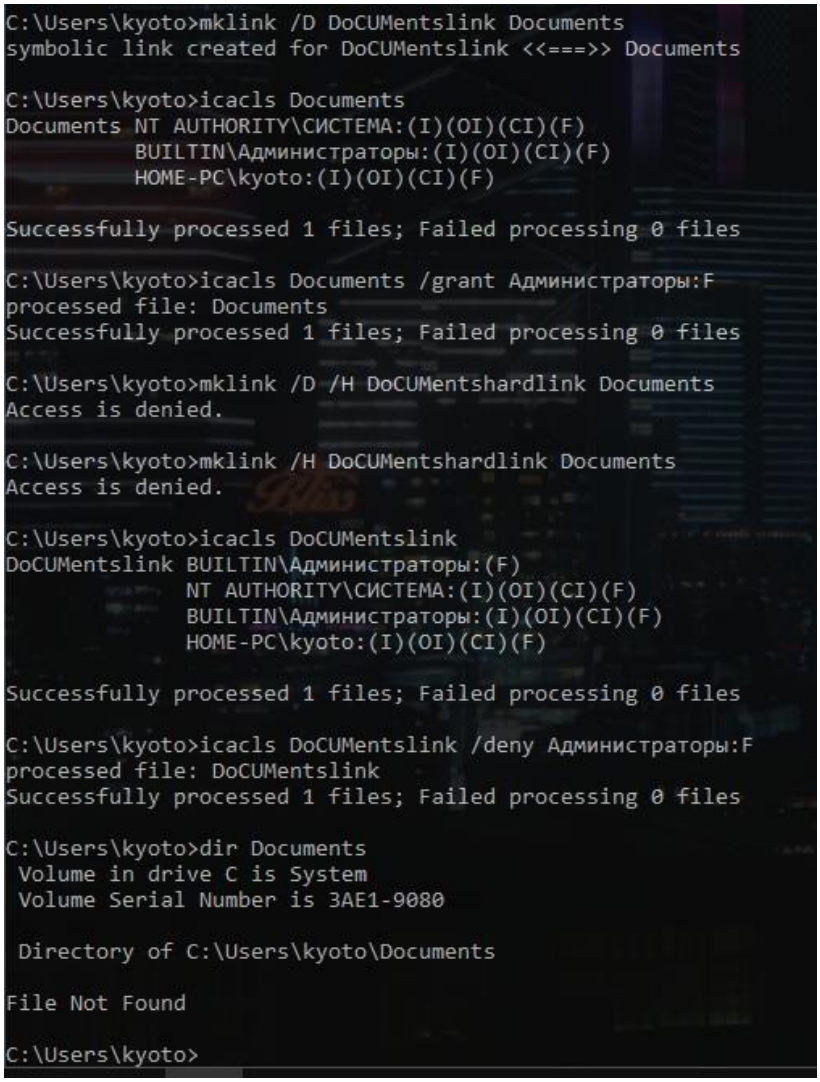


вывод: Если ты можешь прочитать маунт поинт, ограничения доступа на операции с файлами внутри берутся из исходной директории.

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




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>