Министерство науки и образования РФ

Федеральное государственное автономное образовательное

учреждение высшего профессионального образования

«Санкт-Петербургский государственный электротехнический

университет «ЛЭТИ» им. В. И. Ульянова (Ленина)»

(СПбГЭТУ «ЛЭТИ»)

Кафедра вычислительной техники

Отчёт

по лабораторной работе № 2

на тему:

“Безопасность в Windows”

по дисциплине “Операционные системы”

Выполнил студент гр. 4306:

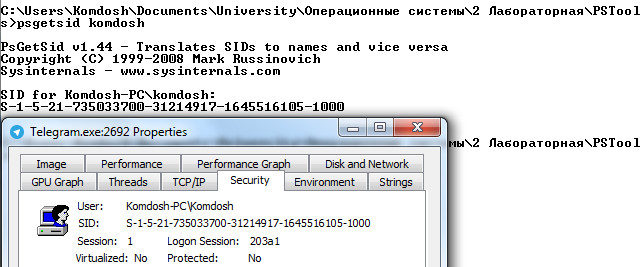
Табаков А.В.

Принял: Тимофеев А.В.

Санкт-Петербург  
2016

**Цель работы**: исследовать структуры данных Windows, используемые для обеспечения безопасности.

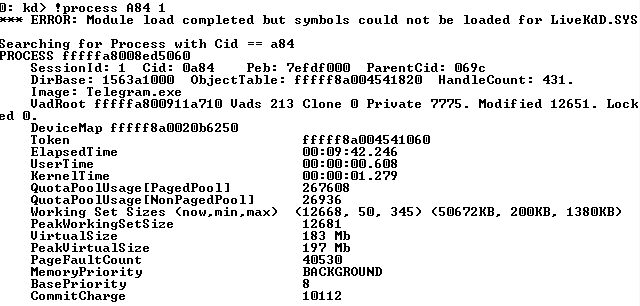
**Задание 2.1**: Определить идентификатор защиты SID текущего пользователя



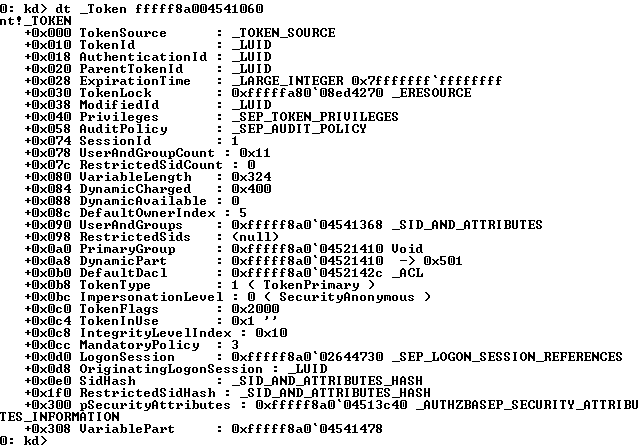
**Вывод**: процесс имеет такие же права, как и пользователь, который его запустил

**Задание 2.2**:исследовать маркер доступа (Access token)

Был выбран процесс Telegram.exe с pid 269210 = A8416



Модификатор доступа (Access Token):



Чтение атрибутов процесса:



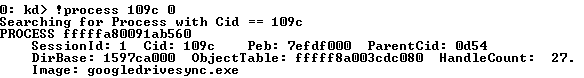
Чтение SID процесса:

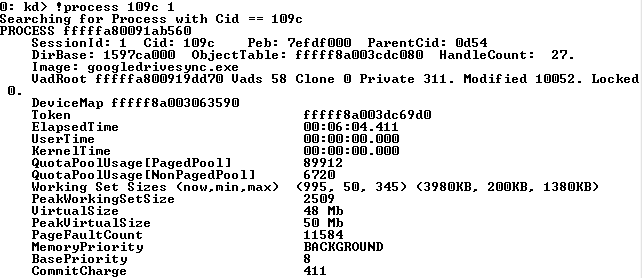


**Вывод**: Значение SID хранящееся в памяти совпадает с тем, что показал process explorer.

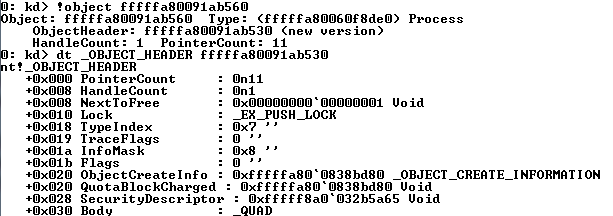
**Задание 2.3**: исследовать дескриптор защиты

Выведем краткую и полную информацию о googledrivesync.exe

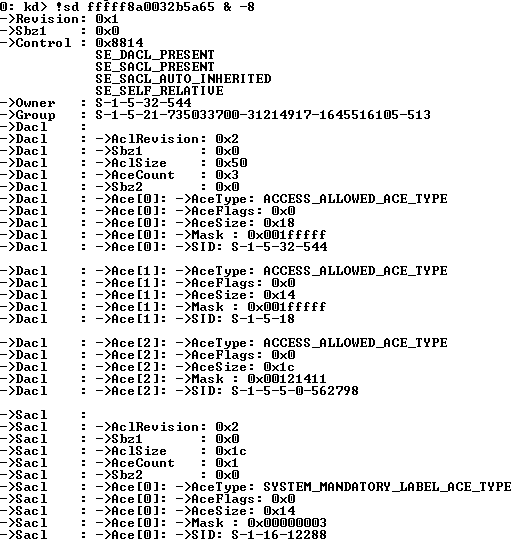




Определим заголовок объекта и читаем его



Просмотрим дескриптор безопасности



Дескриптор защиты содержит 3 элемента АСЕ «доступ разрешен» со следующими масками:

0х001fffff = 0000.0000.0001.1111.1111.1111.1111.1111

0x00121411 = 0000.0000.0001.0010.0001.0100.0001.0001

А также один элемент SACL.

Константы-маски прав доступа из winnt.h:

// The following are masks for the predefined standard access types

#define DELETE (0x00010000L)

#define READ\_CONTROL (0x00020000L)

#define WRITE\_DAC (0x00040000L)

#define WRITE\_OWNER (0x00080000L)

#define SYNCHRONIZE (0x00100000L)

#define STANDARD\_RIGHTS\_REQUIRED (0x000F0000L)

#define STANDARD\_RIGHTS\_READ (READ\_CONTROL)

#define STANDARD\_RIGHTS\_WRITE (READ\_CONTROL)

#define STANDARD\_RIGHTS\_EXECUTE (READ\_CONTROL)

#define STANDARD\_RIGHTS\_ALL (0x001F0000L)

#define SPECIFIC\_RIGHTS\_ALL (0x0000FFFFL)

#define ACCESS\_SYSTEM\_SECURITY (0x01000000L)

#define MAXIMUM\_ALLOWED (0x02000000L)

#define GENERIC\_READ (0x80000000L)

#define GENERIC\_WRITE (0x40000000L)

#define GENERIC\_EXECUTE (0x20000000L)

#define GENERIC\_ALL (0x10000000L)

Таким образом, рассматриваемый googledrivesync.exe имеет все стандартные права:

DELETE - Delete access

READ\_CONTROL - Read access to the owner, group, and DACL of the security descriptor.

WRITE\_DAC - Write access to the DACL.

WRITE\_OWNER - Write access to owner

SYNCHRONIZE - Synchronize access

И все object-specific

Вывод: дескриптор защиты имеет сложную структуру, с помощью которой производится тонкая настройка прав доступа.

Причём у 0 и 1 элементов следующие права:

0х001fffff = 0000.0000.0001.1111.1111.1111.1111.1111

DELETE

READ\_CONTROL

WRITE\_DAC

WRITE\_OWNER

SYNCHRONIZE

STANDARD\_RIGHTS\_REQUIRED

STANDARD\_RIGHTS\_READ

STANDARD\_RIGHTS\_WRITE

STANDARD\_RIGHTS\_EXECUTE

STANDARD\_RIGHTS\_ALL

SPECIFIC\_RIGHTS\_ALL

А у элемента 2 их меньше:

0x00121411 = 0000.0000.0001.0010.0001.0100.0001.0001

READ\_CONTROL

SYNCHRONIZE

STANDARD\_RIGHTS\_READ

STANDARD\_RIGHTS\_WRITE

STANDARD\_RIGHTS\_EXECUTE