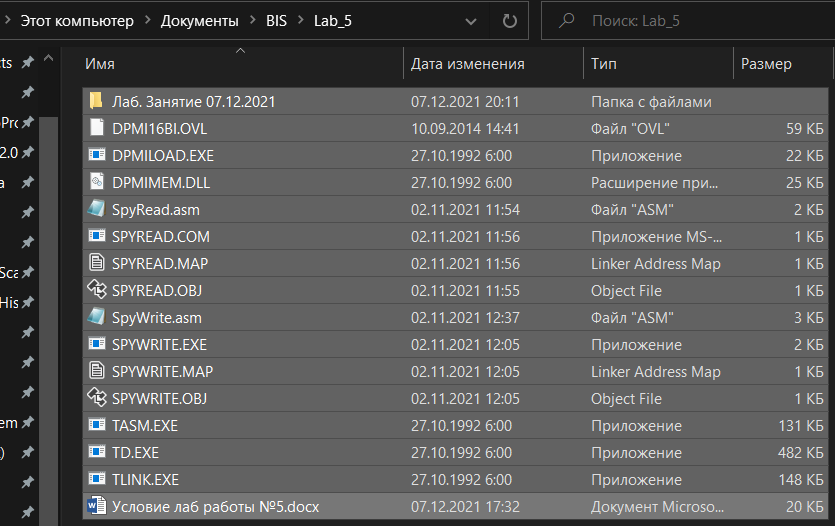
Жуковский Павел Сергеевич, 4 курс, 12 группа

Лабораторное занятие (14.12.2021)

5-ая лабораторная работа (продолжения)

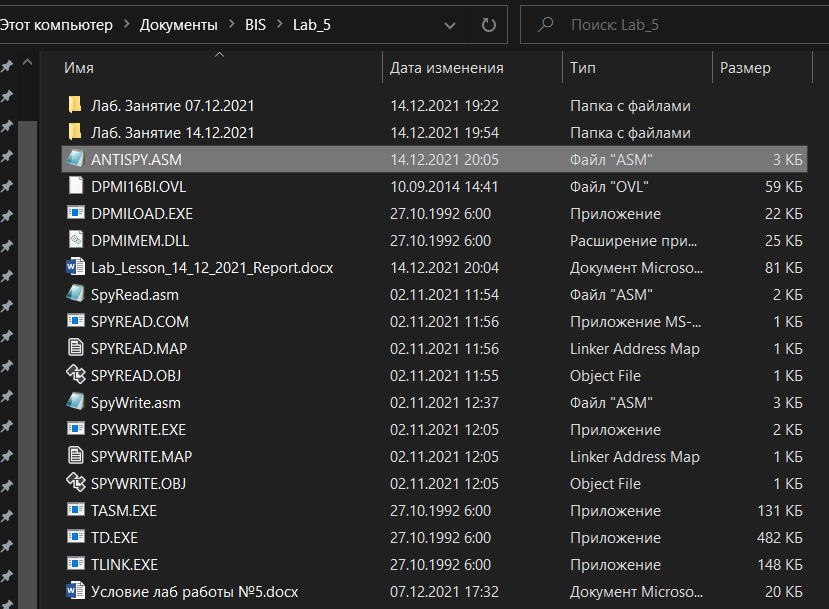
Так как на лабораторную работу ещё неделя, то я пока не торопился с получением конечного исполнимого модуля.

В прошлый раз (неделю назад, 07.12.2021) я создал папку **Lab\_5** и поместил туда такие исполнимые модули, как: TASM.EXE, TLINK.EXE, TD.EXE. А также DPMILOAD.EXE, DPMI16BI.OVL и DPMIMEM.DLL (на всякий случай). Также я поместил туда условие лабораторной, а также исходные текста, объектные и исполнимые модули клавиатурного шпиона (**SpyRead** отвечает за считывание нажатых клавиш, а **SpyWrite** – за их расшифровку).

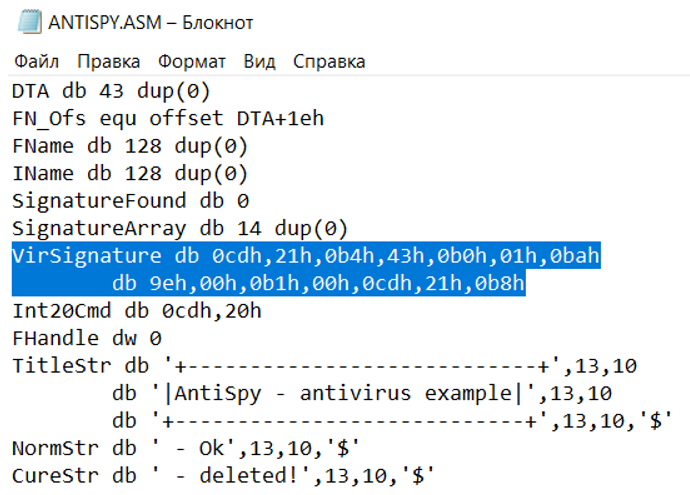


Так как у нас уже есть антивирус ANTIDHOG.ASM, то мы могли бы просто взять его для нашего ANTISPY, но при этом поменять сигнатуру «вируса» на другую – на сигнатуру шпиона.

Для этого возьмём исходный текст ANTIDHOG.ASM и сохраним его в файле **ANTISPY.ASM:**

****

В исходном тексте ANTISPY.ASM нас больше всего интересует вот это место:



Сейчас в этом месте записана сигнатура «свиньи». Нам следует заменить её на сигнатуру «шпиона». В одном из ответов на лекцию я уже как-то определял сигнатуру «шпиона».

Сигнатура осуществление доступа к файлам:

- создание подозрительного файла:

**b4 3c b9 01 00 ba 07 01 c7 06 16 01 01 00 cd 21**

mov ah, 3Ch

mov cx, 1

mov dx, offset FName

mov flag, 1

int 21h

- открытие подозрительного файла:

**ba 07 01 b0 01 b4 3d cd 21 eb b2 8b d8 b4 42 b0**

mov dx, offset FName

mov al, 1

mov ah, 3Dh

int 21h

jmp add\_position

mov bx, ax

mov ah, 42h

mov al, ...

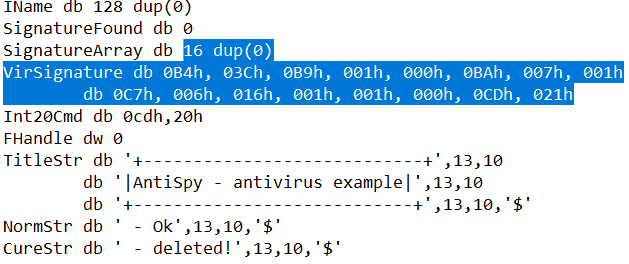
Есть ещё сигнатура оставления «шпиона» резидентной программой, но пока что не будем думать об этом. В качестве сигнатуры, возьмем, пожалуй первую, т.е. вот эту:

**b4 3c b9 01 00 ba 07 01 c7 06 16 01 01 00 cd 21**

Именно эта сигнатура соответствует созданию шпионом файла с информацией о нажатых клавишах (вторая сигнатура подразумевает, что такой файл уже существует, однако в нашем случае этого никогда не произойдёт, если «антишпион» сразу устранит «шпиона»).

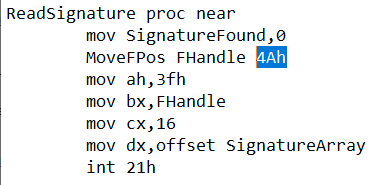
Стоит отметить, что данная сигнатура стоит из **16** байт.

По итогу, мы вносим в исходный текст ANTISPY.ASM следующие изменения:



Перед всеми байтами также были добавлены нолики.

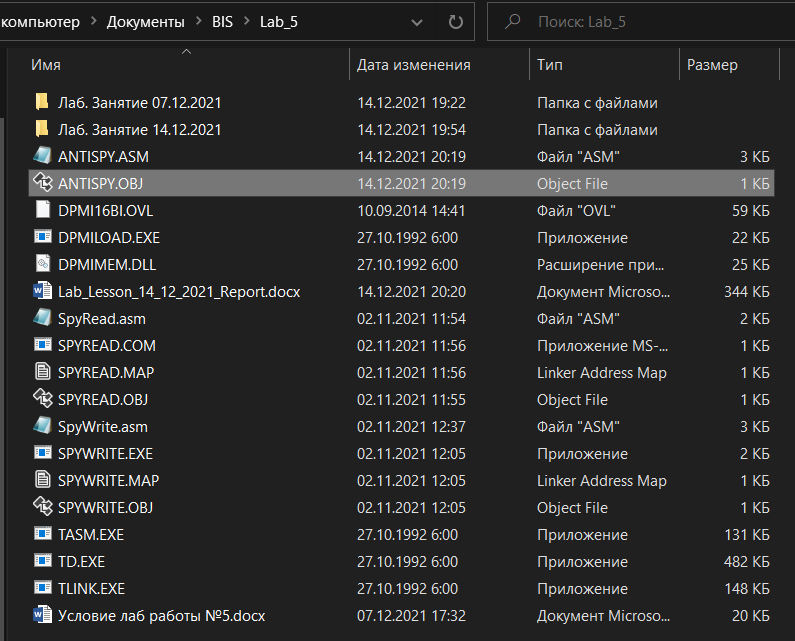
Также было сменено смещение для ReadSignature:



4Ah – это номер байта, начиная с которого в проверяемых исполнимых модулях будет искаться заданная сигнатура (это число было подобрано в процессе отладки, когда я искал ответ на один из вопросов с лекции №14)

Попробуем теперь получить сначала объектный модуль ANTISPY.OBJ:



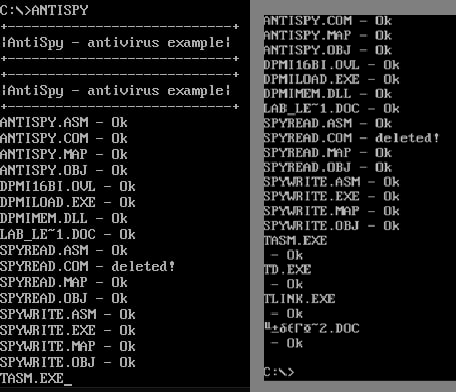


Теперь получим исполнимый модуль ANTISPY.COM:

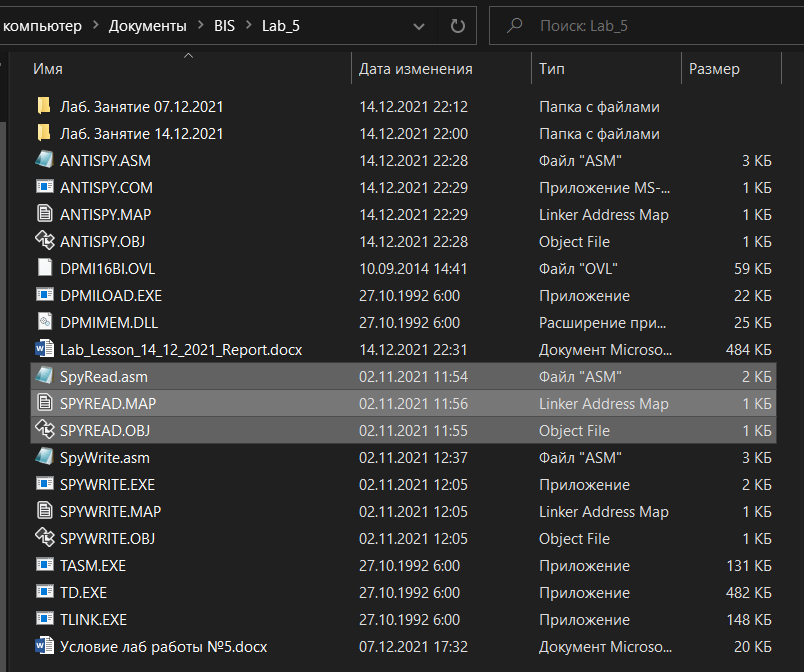


Теперь мы готовы загрузить ANTISPY.COM в оперативную память компьютера и проверить, посчитает ли он SPYREAD.COM опасным или нем.

Запуск ANTISPY:



После этого исполнимый модуль SPYREAD.COM, внутри которого была обнаружена сигнатура команды создания подозрительного файла, был удалён из папки:



Таким образом, текущая версия ANTISPY способна находить и удалять из папки исполнимые модуля, внутри которых находится сигнатура создания подозрительного файла (но пока что только сигнатура создания, а не просмотра уже созданного файла, и пока что без обнаружения сигнатуры «резидентности» программы)

На этом мои эксперименты касательно лабораторной работы №5 (14.12.2021) были завершены.

В архив я помещу следующие файлы: SpyRead.ASM, SPYREAD.COM, ANTISPY.ASM, ANTISPY.COM, а также этот отчёт.

Пароль от архива: **041** (на всякий случай, укажу пароль на самом верху этого отчёта тоже)