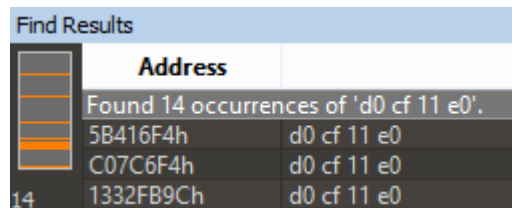


Перед тем, как использовать рекомендованную в задании утилиту Volatility, я решил попробовать найти в дампе нужный файл с помощью hex-редактора. Посмотрел, какие сигнатуры встречаются в doc-файлах. Выбор пал на сигнатуру «D0 CF 11 E0», встречающуюся в начале doc-файлов. Всего в файле дампа было обнаружено 14 таких сигнатур:



Find Results	
Address	
Found 14 occurrences of 'd0 cf 11 e0'.	
5B416F4h	d0 cf 11 e0
C07C6F4h	d0 cf 11 e0
1332FB9Ch	d0 cf 11 e0

Я проверил, что ворд умеет читать документы, в конец которых дописаны лишние байты, поэтому просто разбил файл на 14 частей, предварительно отрезав часть файла от его начала до первой найденной сигнатуры. Все полученные файлы ворд счёл битыми.

После этого я установил Volatility (быстрее всего получилось сделать это на виртуальной машине ubuntu с помощью apt-get install) и попробовал получить список процессов, предварительно почитав мануал и посмотрев пару примеров использования приложения. Для получения списка процессов необходимо было указать ОС. Тут я просто перебирал возможные варианты, указанные в справке программы. Список процессов удалось получить, выполнив команду `volatility -f 20190227.mem --profile=WinXPSP3x86 pslist`

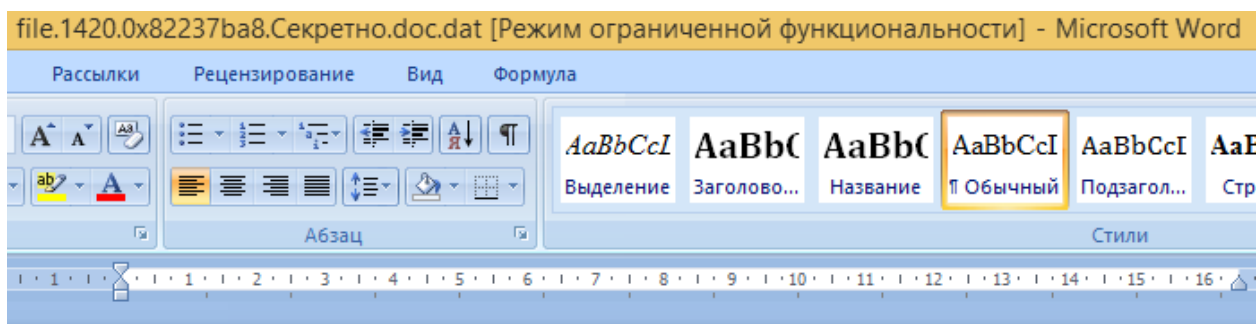
Нас интересовал процесс WINWORD.EXE. Информация о нем была в следующей строчке:

```
0x8227c6d0 WINWORD.EXE          1420  1760    4   206    0    0
2019-02-27 13:33:27 UTC+0000
```

Число 1420 является PID. Зная PID, с помощью Volatility можно извлечь все данные процесса. Выполняем команду

```
volatility -f 20190227.mem --profile=WinXPSP3x86 dumpfiles -n -p 1420 -
D xtra
```

Данная команда извлекает файлы нужного процесса в указанный каталог xtra. Среди всех извлеченных файлов видим файл с именем «file.1420.0x82237ba8.Секретно.doc.dat». Открываем файл и видим содержимое:



Мои поздравления, Вы справились!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Спасибо за интересное задание!