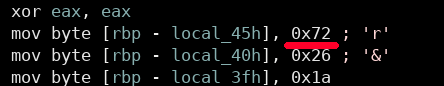
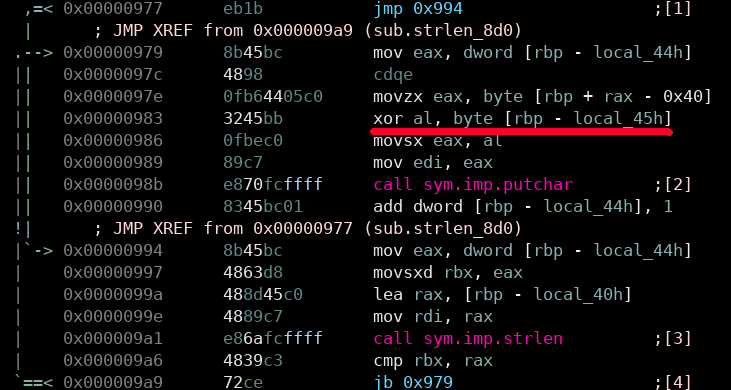
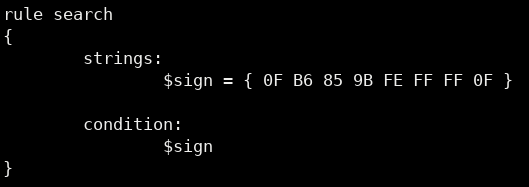
**WriteUP Reverse 300. KrasCTF 2017**

Выражение: “Поступи с ней, как другие поступают с подобными фразами.” говорит о том, что нужно посмотреть, как работают фейковые файлы. Вывод сообщения в фейковом файле происходит посимвольно. К каждому символу предварительно применяется исключающее ИЛИ с константой, она нам и нужна.

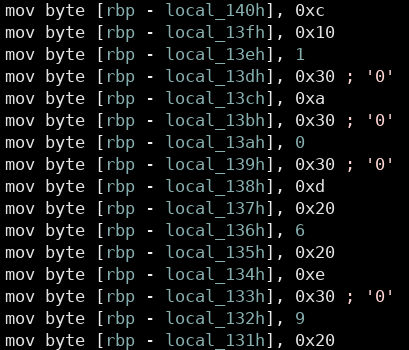


Применяем исключающее ИЛИ к HEX-строке, которая дана в формулировке задания, с константой 0x72. Получим строку “0F B6 85 9B FE FF FF 0F”. Это сигнатура искомого файла. Найдем этот файл с помощью YARA. Напишем следующее правило.

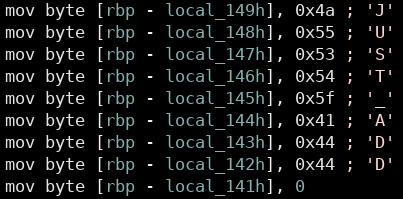


Номер искомого файла равен 679. Он принимает на вход файл длиной 32 байта. Также внутри программы инициализируются три массива:

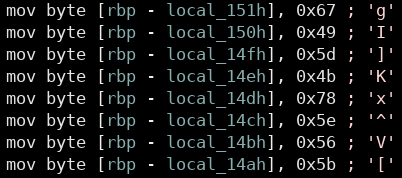
1. Массив вычетов. Из считанного значения из файла вычитается очередной элемент данного массива. Элементы массива – старшие и младшие половины значений из файла.



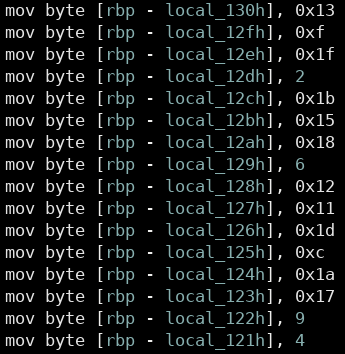
1. Массив с сообщением. После всех преобразований данные из файла сравниваются с элементами данного массива.



1. Массив с масками. К преобразованным данным из файла применяется исключающее ИЛИ с элементами из данного массива.



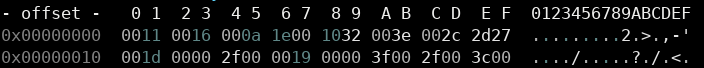
1. Массив со смещениями относительно конца файла.



Программа осуществляет следующий алгоритм проверки корректности файла:

1. Обнуление суммы;
2. Считывание первого значения;
3. Вычитание младшей части значения;
4. Добавление к сумме;
5. Считывание второго значения;
6. Вычитание старшей части значения;
7. Добавление к сумме;
8. Исключающее ИЛИ суммы и маски;
9. Сравнение полученного значения с соответствующим элементом сообщения;

Производя все действия в обратном порядке, получаем следующий файл.



Складывая по два значения из файла, используя таблицу смещений, получаем флаг - **IMHOTEPH**