Анализ файла гибернации Windows 10

Выполнил: Медведев Андрей, 344 гр.

Научный руководитель:
Ст. пр. Губанов Ю. А.

Научный консультант:
Тимофеев Н. В.

Введение

Гибернация — энергосберегающий режим операционной системы компьютера, позволяющий сохранять её состояние при полном отключении энергии компьютера. В процессе гибернации оперативная память компьютера сохраняется в файле гибернации.

С выпуском каждой новой версии ОС Windows формат файла гибернации меняется, но задача анализа файла гибернации не теряет своей актуальности.

Постановка задач

- Провести обзор существующих решений для анализа файла гибернации Windows 10
- Изучить структуру файла гибернации ОС Windows 10
- Провести сравнительный анализ формата файла гибернации ОС Windows 10 и более ранних версий
- Разработать прототип программы на языке C++, позволяющей восстанавливать образ оперативной памяти из файла гибернации ОС Windows 10

Обзор существующих решений

В связи с изменениями в формате файла гибернации Windows 8 многие инструменты для анализа файла гибернации потеряли свою актуальность. На данный момент существует два инструмента, которые поддерживают новый формат

- Hibernation Recon
- Hibr2Bin

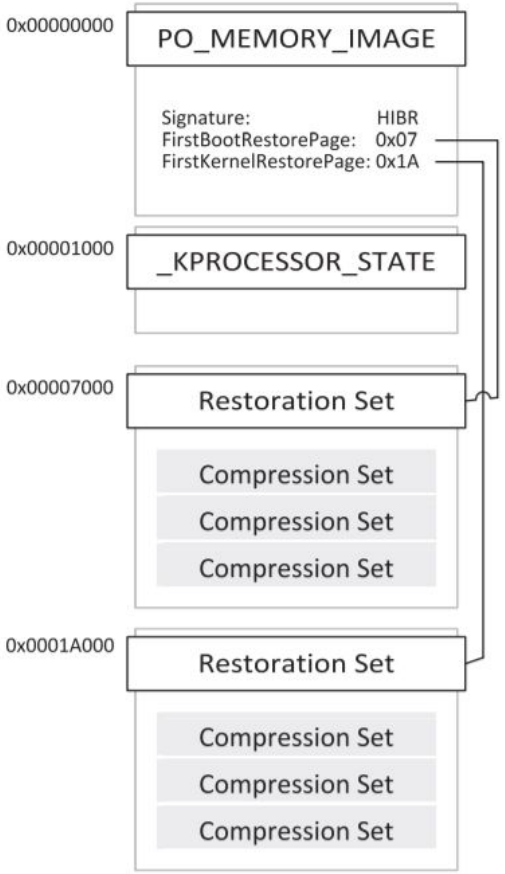
Исследование структуры файла гибернации

Структура файла гибернации ОС Windows является закрытой информацией Microsoft. Все структуры были восстановлены с помощью методов обратного программирования.

- Modern windows hibernation file analysis, Joe T. Sylve et. al, 2016
- WinDBG
  - Команда -dt (Display Type)

Структура файла гибернации

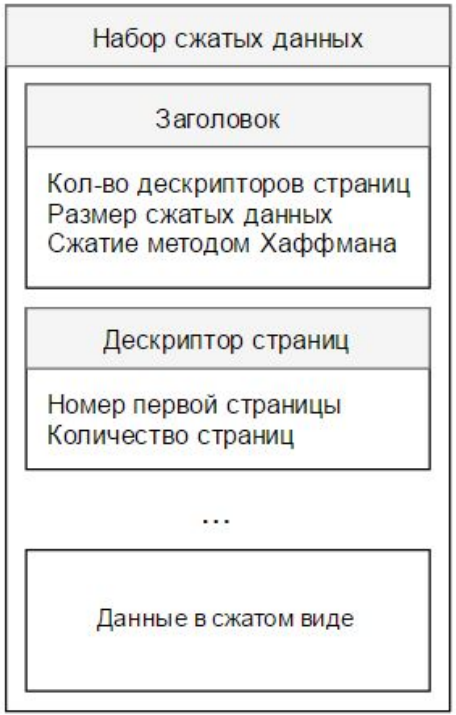
- Заголовок
  - Время сеанса гибернации
  - Адреса первых страниц наборов восстановления
  - Количество страниц в каждом из наборов восстановления
- Контекст процессоров



Структура файла гибернации

Набор восстановления представляет из себя последовательность наборов сжатых данных.

- Plain LZ77
- Huffman+LZ77



Сравнительный анализ

- Коренные изменения в формате файла гибернации с выходом Windows 8
- Отказ от формата, основанного на использовании XPRESS-блоков и таблиц адресации, и переход к использованию наборов восстановления
  - Упрощение процесса восстановления состояния системы
- Обнуление всех страниц кроме страницы заголовка и контекста процессора после успешного восстановления состояния системы

Разработка прототипа

Разработан прототип приложения позволяющий частично восстанавливать образ оперативной памяти по содержащимся в файле гибернации данным.

- Анализ заголовка
- Восстановление сжатых данных из файла гибернации

Тестирование прототипа проводилось путём сравнительного анализа оригинального образа оперативной памяти и образа, полученного с применением программы к соответствующему файлу гибернации.

Итоги

В ходе выполнения работы были достигнуты следующие результаты:

- Проведён обзор существующих решений для анализа файла гибернации Windows 10
- Изучена структуру файла гибернации ОС Windows 10
- Проведён сравнительный анализ формата файла гибернации ОС Windows 10 и более ранних версий
- Разработан прототип программы на языке C++, позволяющей частично восстанавливать образ оперативной памяти из файла гибернации ОС Windows 10

Спасибо за внимание