ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Санкт-Петербургский государственный университет телекоммуникаций

им. проф. М.А. Бонч-Бруевича***»***

(СПБГУТ)

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Факультет ИКСС

Кафедра ЗСС

Отчет по лабораторной работе №7

по дисциплине:

**«Цифровая криминалистика»**

на тему:

**«Анализ реестра Windows с использованием RegRipper»**

Выполнили:

Студенты гр. ИКТБ-98м

Зеличенок И.Ю.

Щипцов Д.И.

Проверила:

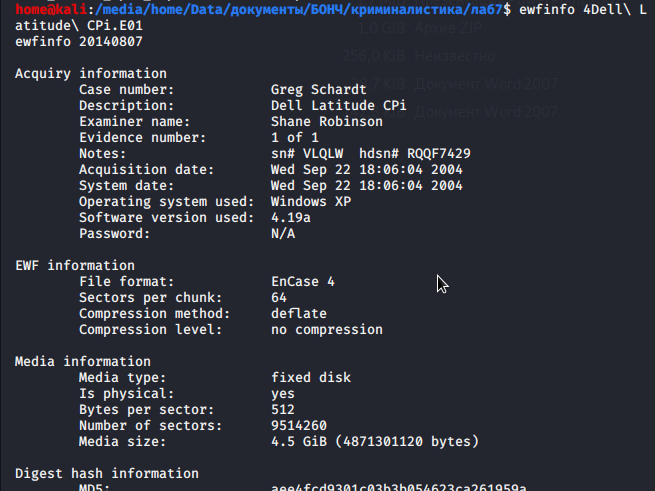
Федорченко Е.В

Санкт-Петербург

2020г.

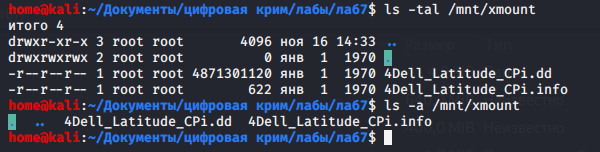
Цель: используя плагины просмотреть основную информацию в реестре.

Смонтировать образ.



Мета данные первого образа

Используя команду xmount -–in ewf ‘4Dell Latitude CPi.E01’ ‘4Dell Latitude CPi.E02’ /mnt/xmount/ монтируем образ в указанный каталог и проверим в каталоге и хэш сумму

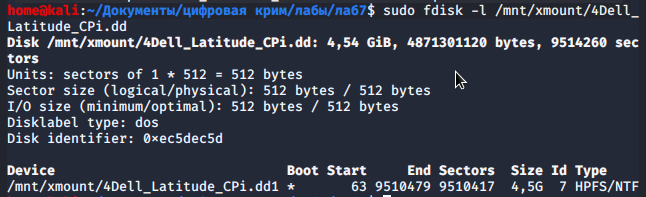


Проверка установки



Md5 хэш сумма

Получаем стартовое значение через fdisk

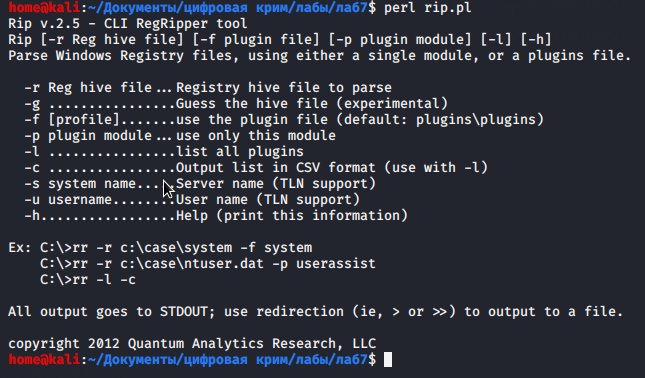


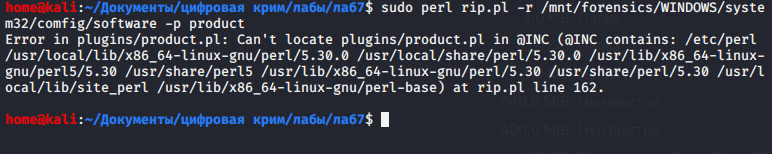
Информация о стартовом значении

Произведент монтаж со стартового значения(63\*512=32256)

mount -t ntfs -o ro,offset=32256 /mnt/xmount/4Dell Latitude CPi.dd /mnt/forensics/

используем скрипты RegRipper

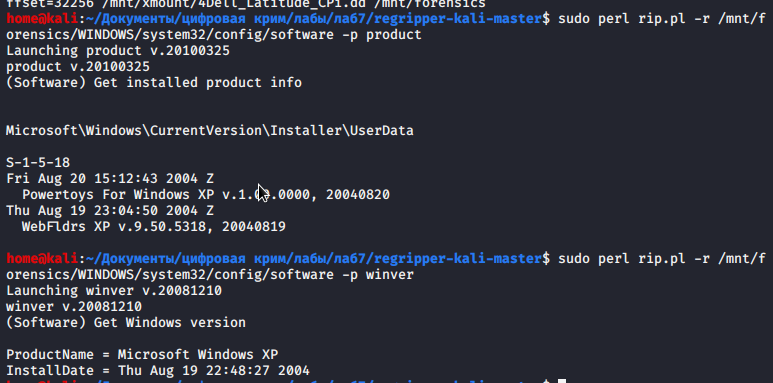




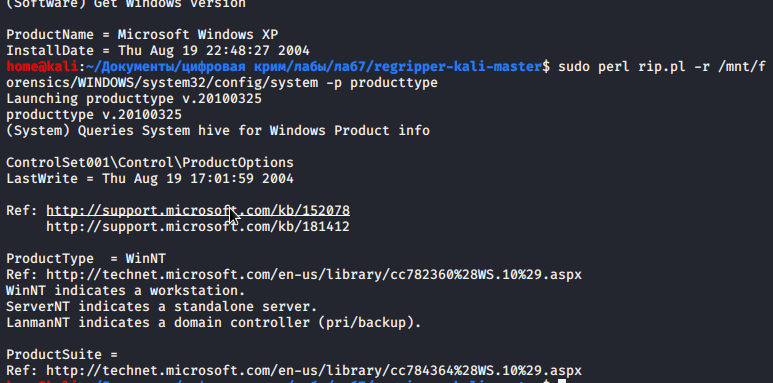
Решение проблем на весь каталог поставить разрешение чтение и выполнение



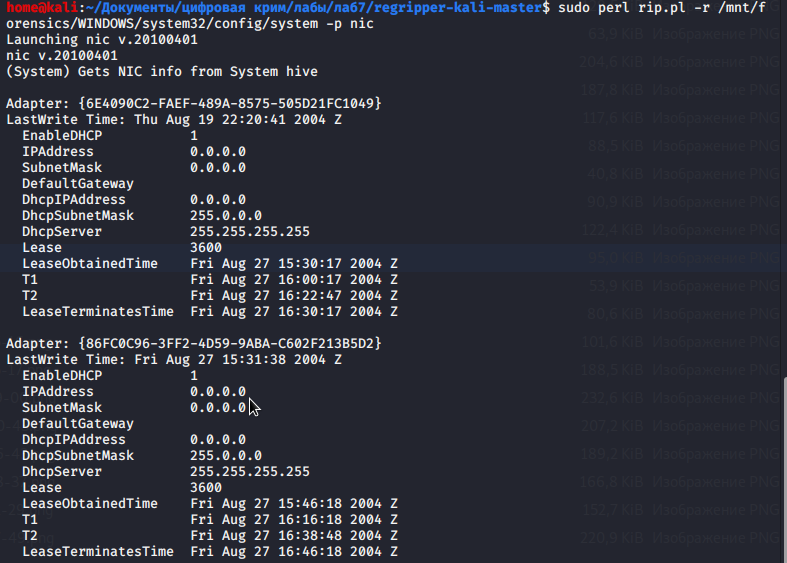
Получаем информацию о ОС и ее версии



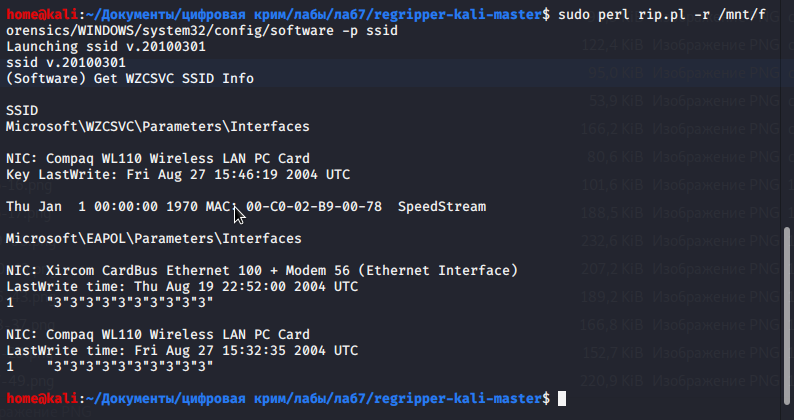
Определение типа



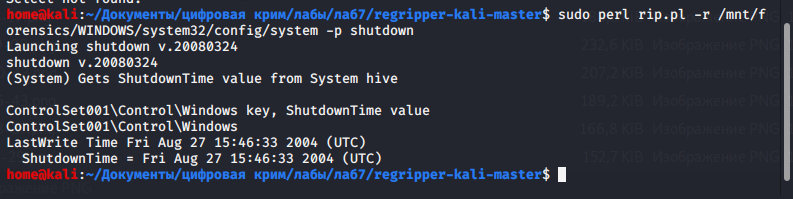
Получаем информацию о сетевых настройках



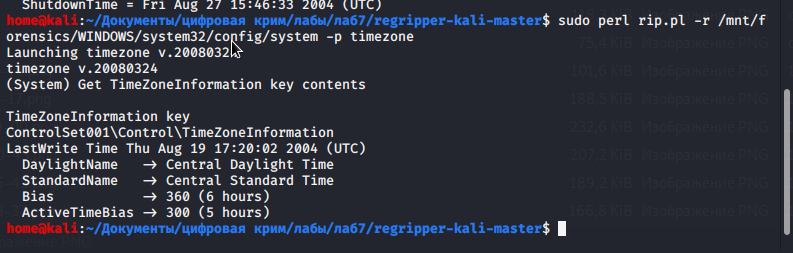
Получаем о беспроводных ТД



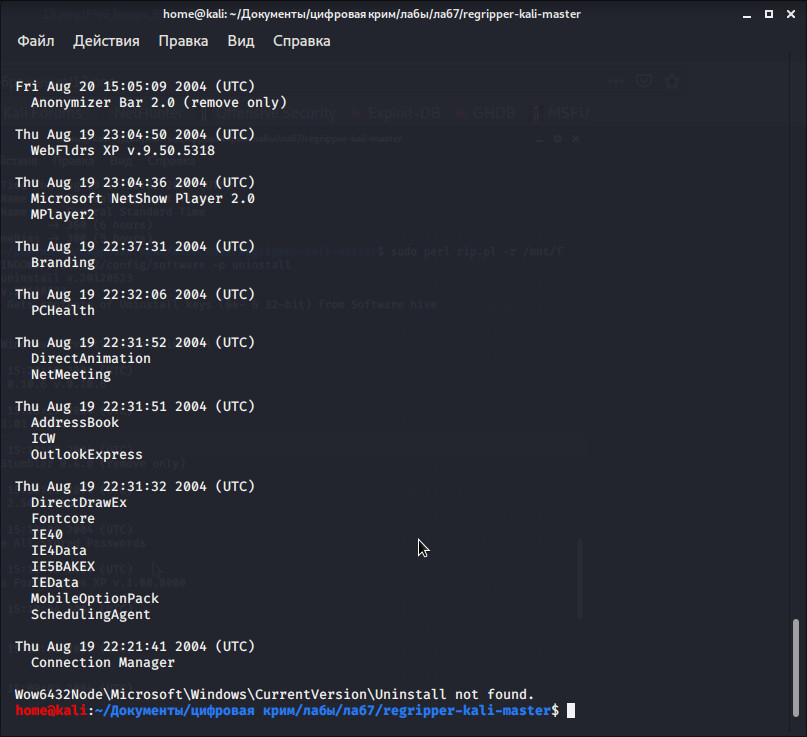
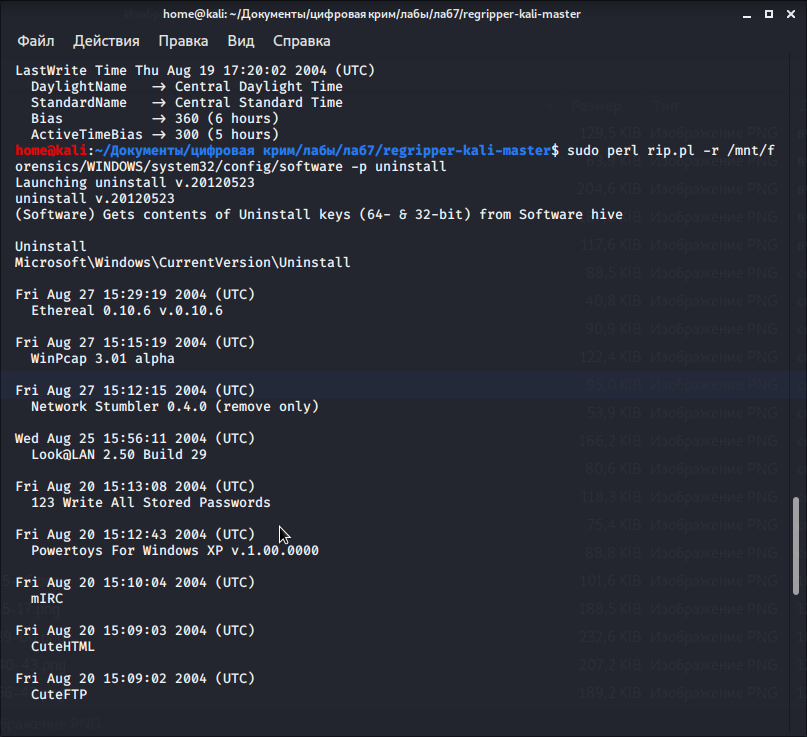
Определение отключения ПК



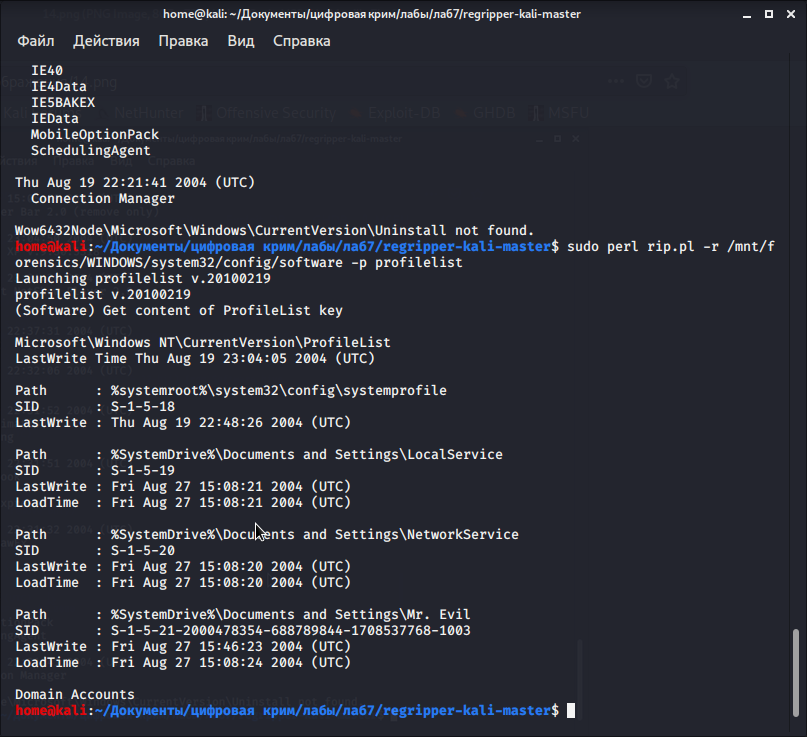
Определение настроек времени



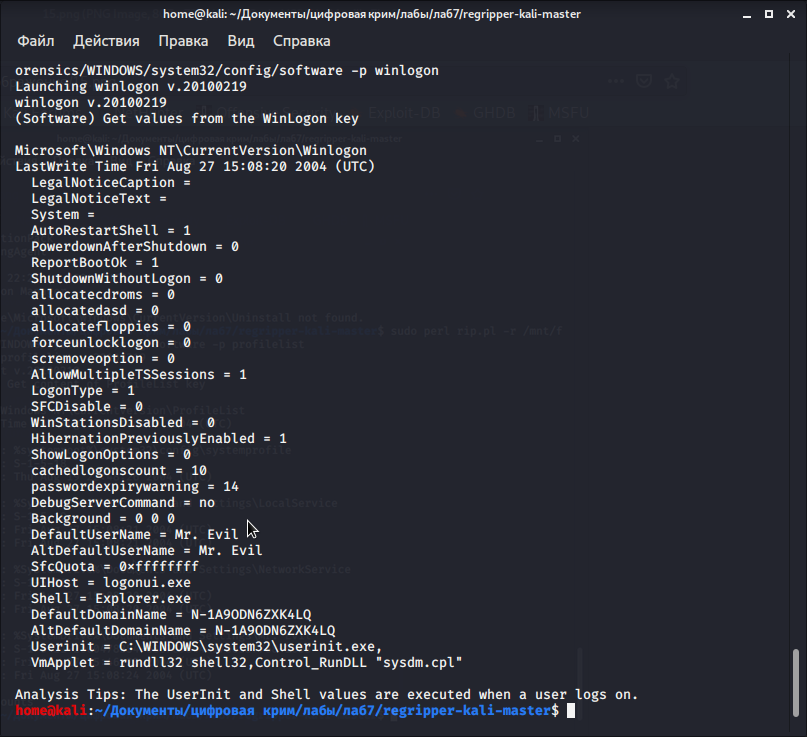
Определение установленных приложений



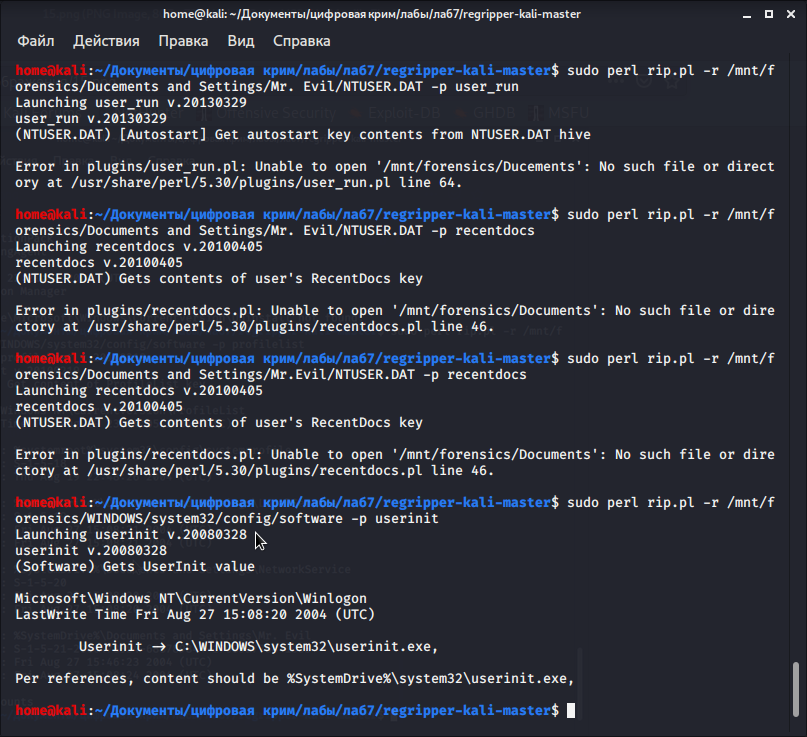
Определение унификаторов пользователей



Информация из ключа Winlogon



Определение значения раздела реестра userinit



Вывод: плагины позволяют получить ключевую информацию и реестра, избегая просмотра всех блогов данных.