ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н.Тихонова

Домашнее задание №3, вариант 1. Основы цифровой форензики.
По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Сорокин А. В.

Подпись _____

Выполнил:

Новиков В. С. МКБ 241

Подпись _____

Москва 2025

Задание «Вариант 1».

Перед Вами образ диска устройства (персонального компьютера). Установите следующие обстоятельства о нем.

1. Перечислите учетные записи пользователей (кроме существующих по умолчанию) на устройстве

2. Укажите все размеченные области диска

3. Укажите операционную систему устройства, включая тип, версию и архитектуру процессора

4. Укажите время последнего доступа к картинке с закатом

5. Определите, следы обработки набора разработчика (Developer Kit) какого поставщика ПО присутствуют на устройстве.

6. Во время сеанса какой из учетных записей созданы текстовые документы и таблицы Excel со словом spreadsheet в названиях?

7. Какая композиция прослушивается при демонстрации возможностей визуализации Windows Media Player?

8. Перечислите адреса, присутствующие в удаленных файлах формата doc

9. Определите номер порта, назначенного для сервиса nntp на исследуемом устройстве.

10. Укажите все адреса электронной почты, использованные пользователем с номером «1» в имени пользователя.

Решение

Отчет по анализу дампа диска var1.E01 с помощью Autopsy на Windows и Kali Linux

1. Перечислите учетные записи пользователей (кроме существующих по умолчанию) на устройстве

Ответ: domex1 и domex2

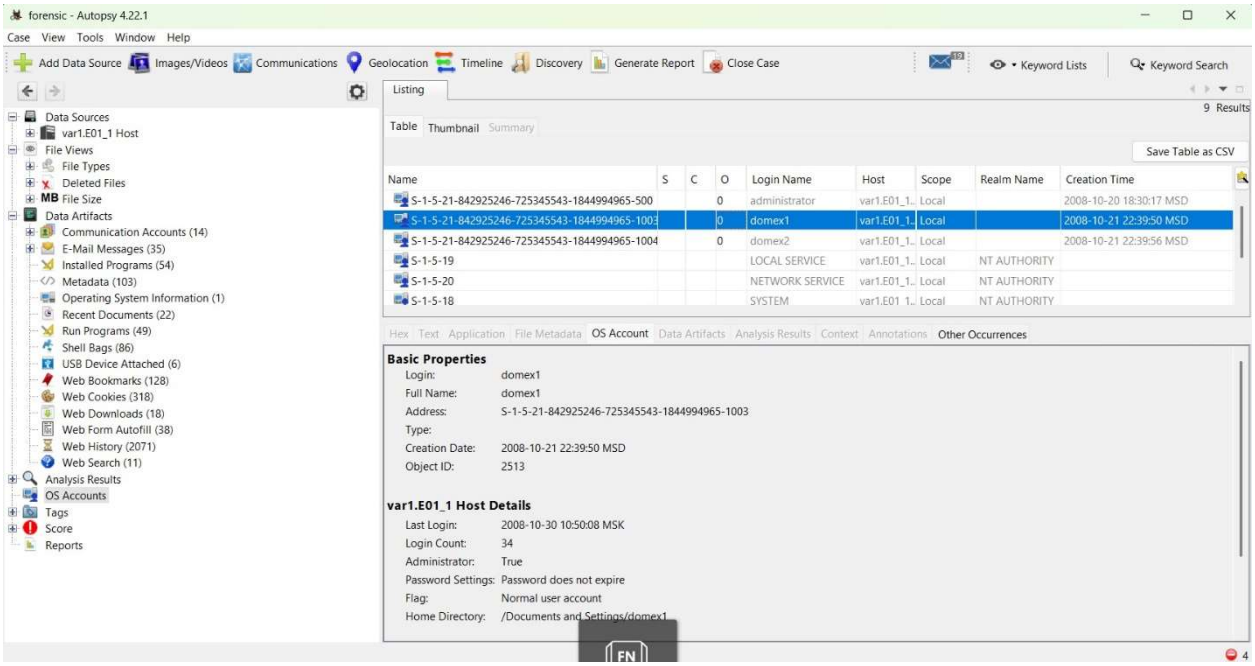

Рисунок 1. Windows версия «OS Accaunts»

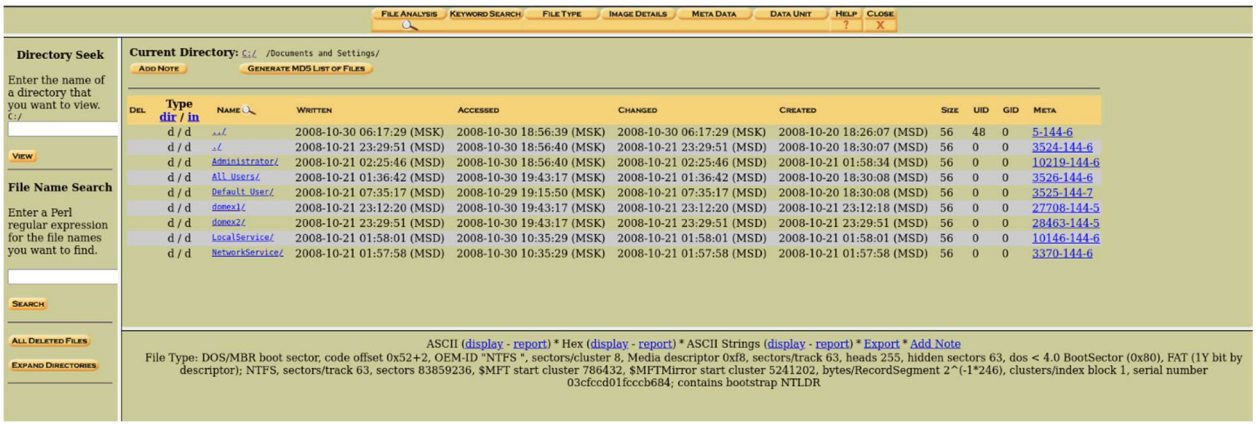

Рисунок 2. Kali Linux версия «Users»

2. Укажите все размеченные области диска

Ответ:

Размеченные области диска:

Vol1 (Unallocated: 0-62)

Vol2

Тип: NTFS (0x07)

Секторный диапазон: 63 – 83859299

Длина: 83859237 секторов

Монтируется как диск C:\

Описание: NTFS / exFAT

Vol3 (Unallocated: 83859300-838860079)

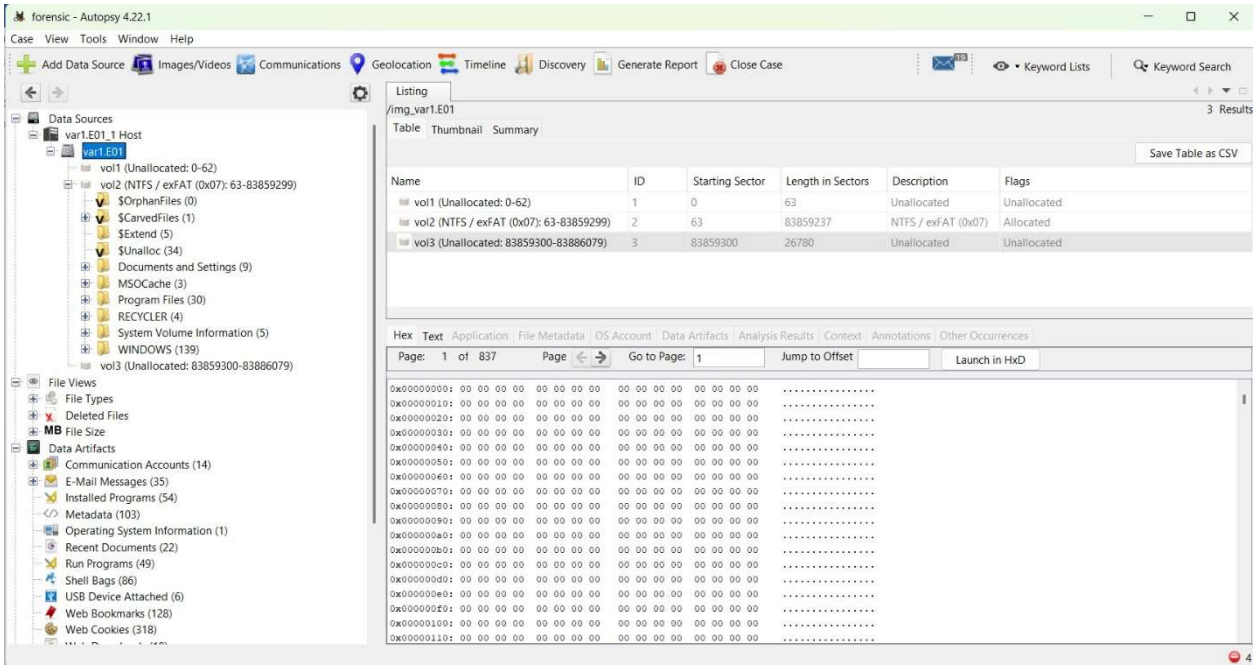

Рисунок 3. Windows версия «области диска»

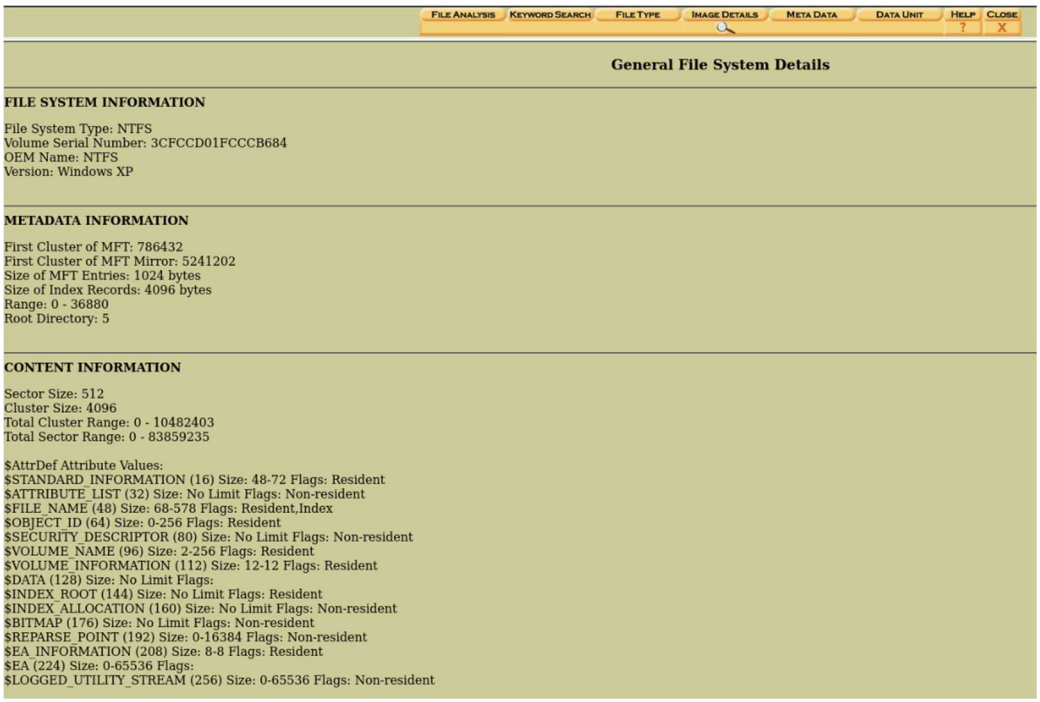

Рисунок 4. Kali Linux версия «General File System Details»

3. Укажите операционную систему устройства, включая тип, версию и архитектуру процессора

Ответ:

Version: Windows XP

В результате анализа файла реестра SOFTWARE были обнаружены следующие сведения:

Операционная система: Microsoft Windows XP

Версия: 5.1 (Build 2600.5512: Service Pack 3)

Архитектура процессора: x86 (32-битная)

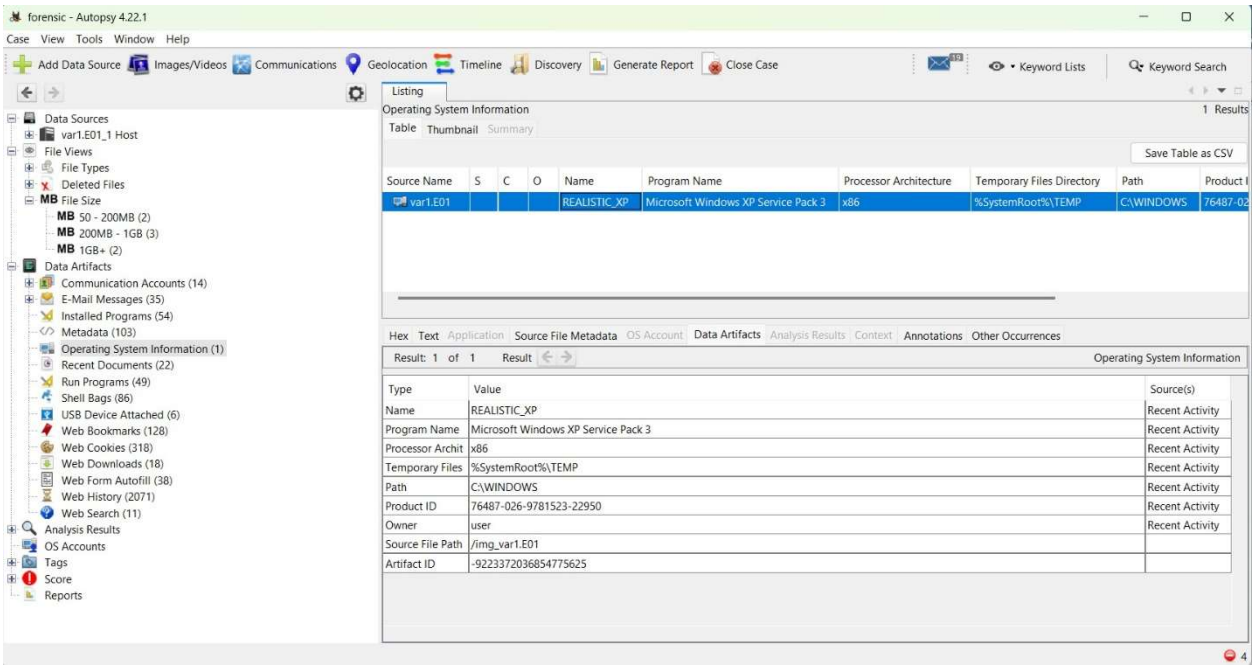

Рисунок 5. Windows версия «Operating System Information»

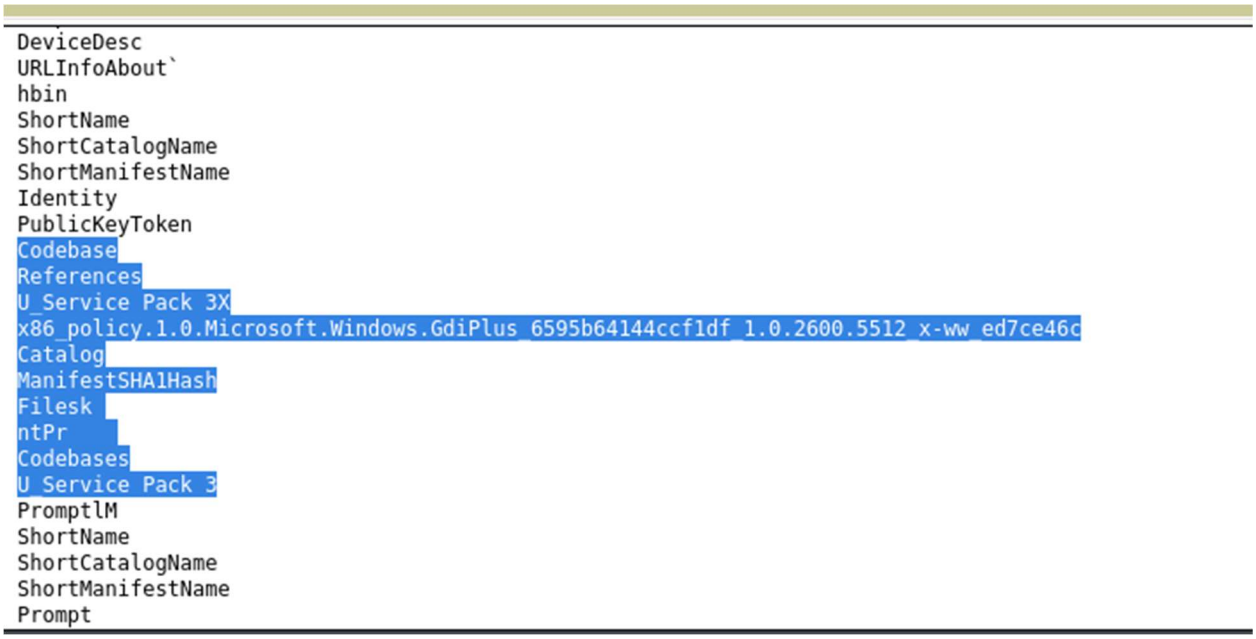

Рисунок 6. Kali Linux версия «анализ файла реестра SOFTWARE»

4. Укажите время последнего доступа к картинке с закатом

Ответ: 2008-10-29 19:21:04 (MSK)

C:/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Sunset.jpg

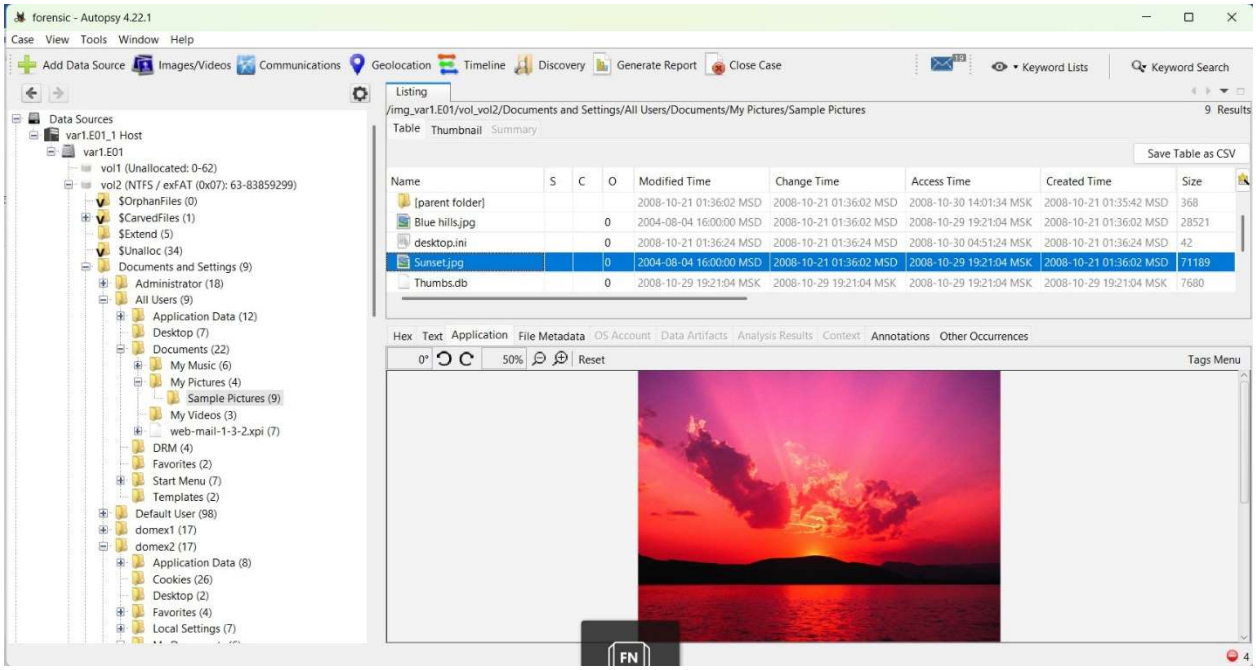

Рисунок 7. Windows версия «Sunset.jpg»

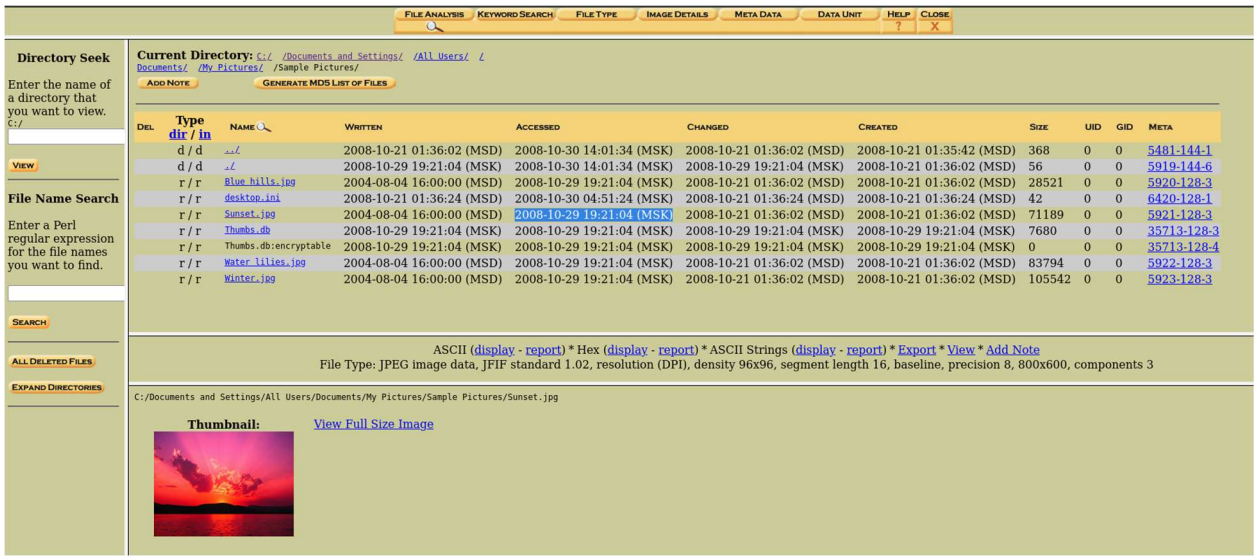

Рисунок 8. Kali Linux версия «Sunset.jpg»

5. Определите, следы обработки набора разработчика (Developer Kit) какого поставщика ПО присутствуют на устройстве

Ответ: VMware Guest SDK — это 100% Developer Kit от VMware

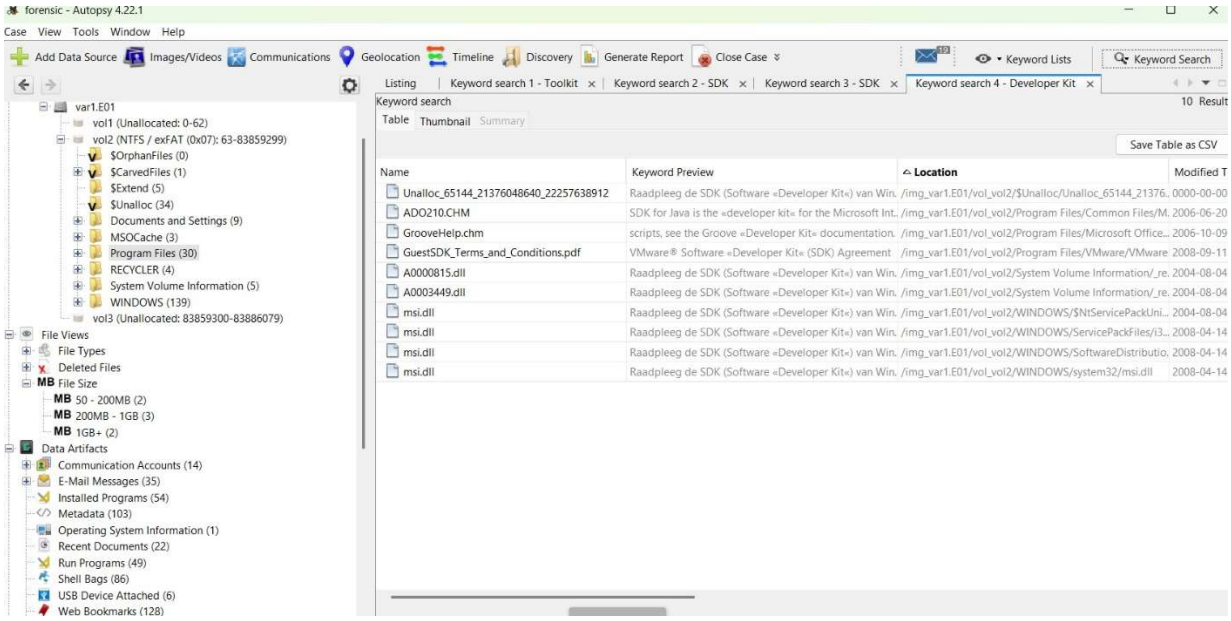

Рисунок 9. Windows версия «поиск по значению Developer Kit»

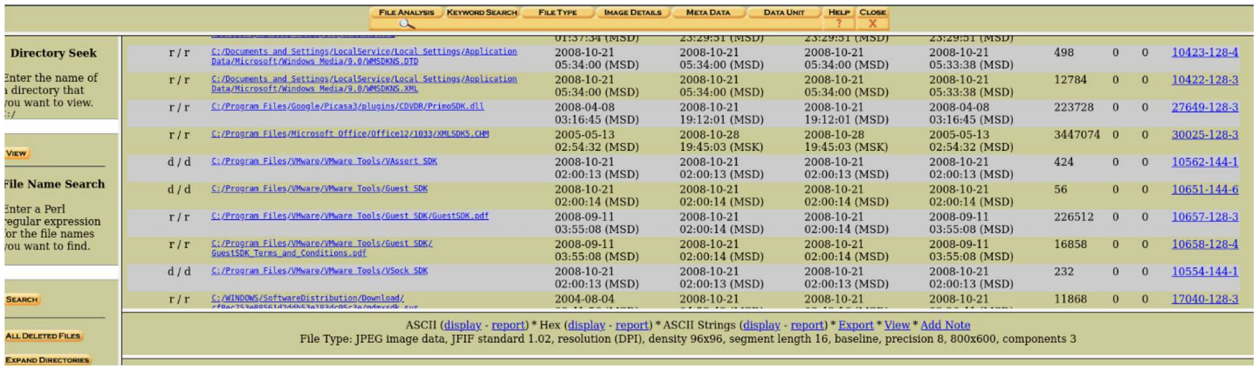

Рисунок 10. Kali Linux версия «поиск по значению Developer Kit и SDK»

6. Во время сеанса какой из учетных записей созданы текстовые документы и таблицы Excel со словом spreadsheet в названиях?

Ответ: учётная запись domex1.

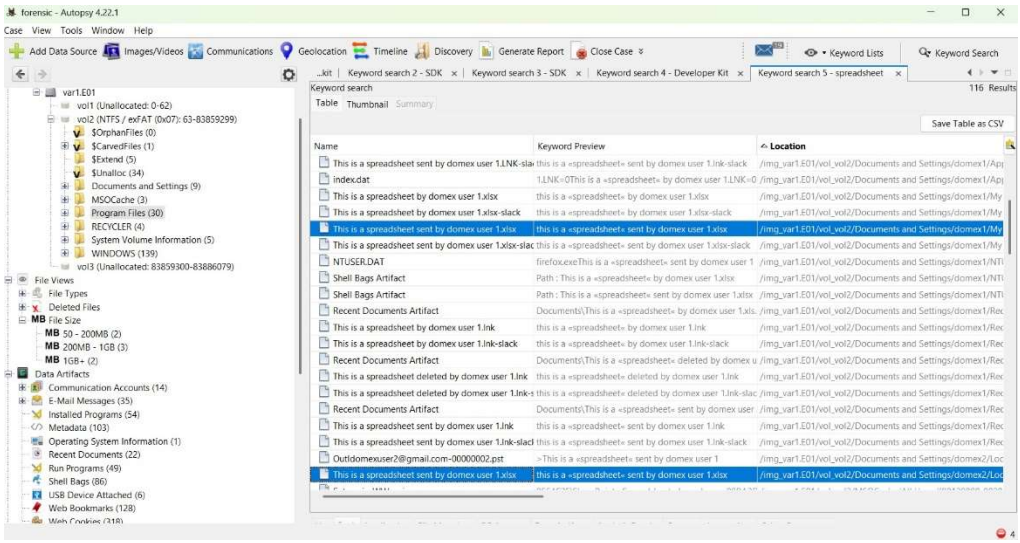

Рисунок 11. Windows версия «поиск по значению spreadsheet»

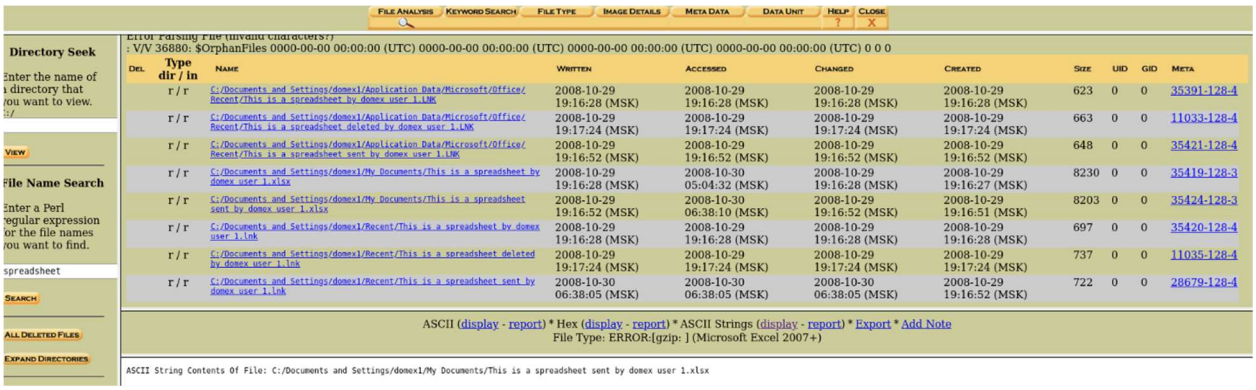

Рисунок 12. Kali Linux версия «поиск по значению spreadsheet»

7. Какая композиция прослушивается при демонстрации возможностей визуализации Windows Media Player?

Ответ: Beethoven's Symphony No. 9 (Scherzo)

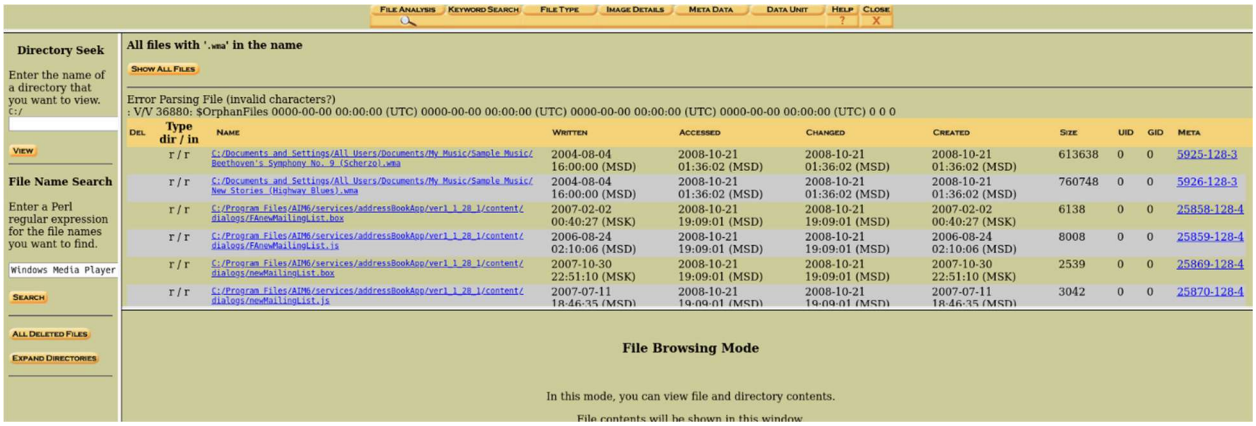

Рисунок 13. Kali Linux версия «поиск по значению .wma»

8. Перечислите адреса, присутствующие в удаленных файлах формата doc

Ответ: в ходе исследования файловой системы (C:/RECYCLER/; Delete Files) устройства были обнаружены следующие удалённые файлы в папке C:/RECYCLER/ - Dc3.docx и Dc4.xlsx.

1) в папке C:/RECYCLER/ найдены файлы Dc3.docx и Dc4.xlsx.

Эти файлы были экспортированы для последующего анализа.

Просмотр содержимого данных файлов показал, что в них отсутствуют упоминания почтовых адресов, уличных адресов или других идентифицирующих локационных данных.

2) в папке C:/Documents and Settings/domex2/My Documents/ был обнаружен файл TMP4352$.TMP, имеющий атрибут "удалённый". Попытка восстановления содержимого данного временного файла оказалась безуспешной: содержимое недоступно для просмотра, вероятно вследствие перезаписи данных на носителе после удаления.

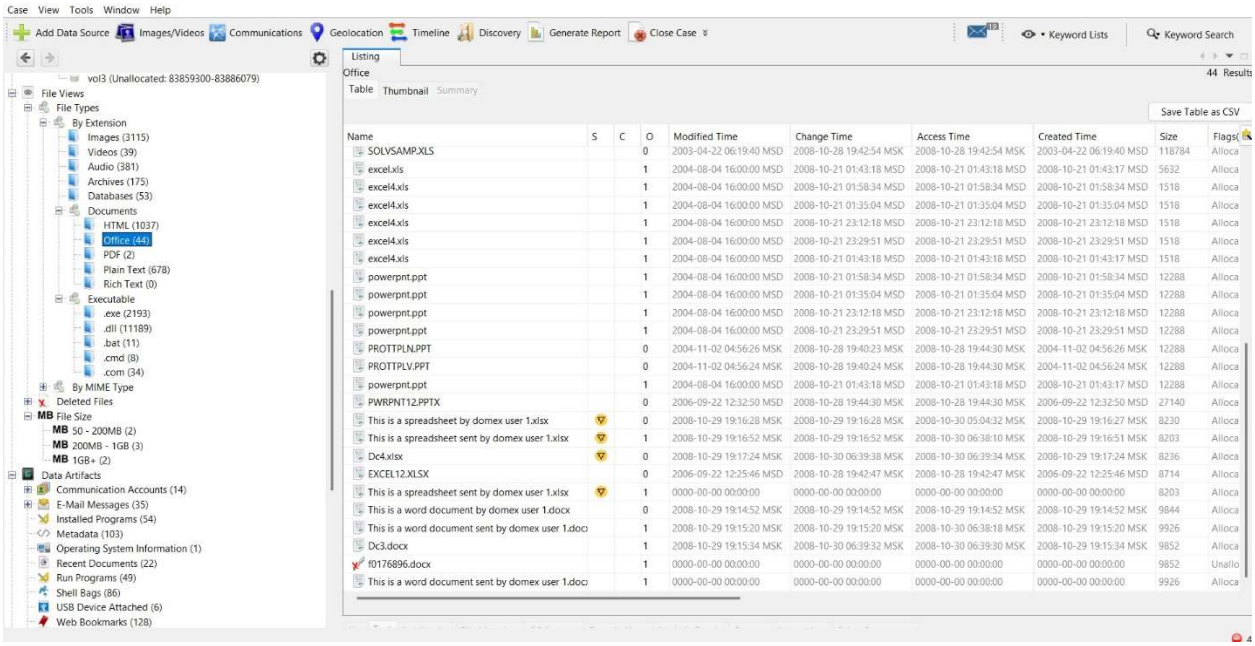

Рисунок 14. Windows версия «File Types -...- Office»

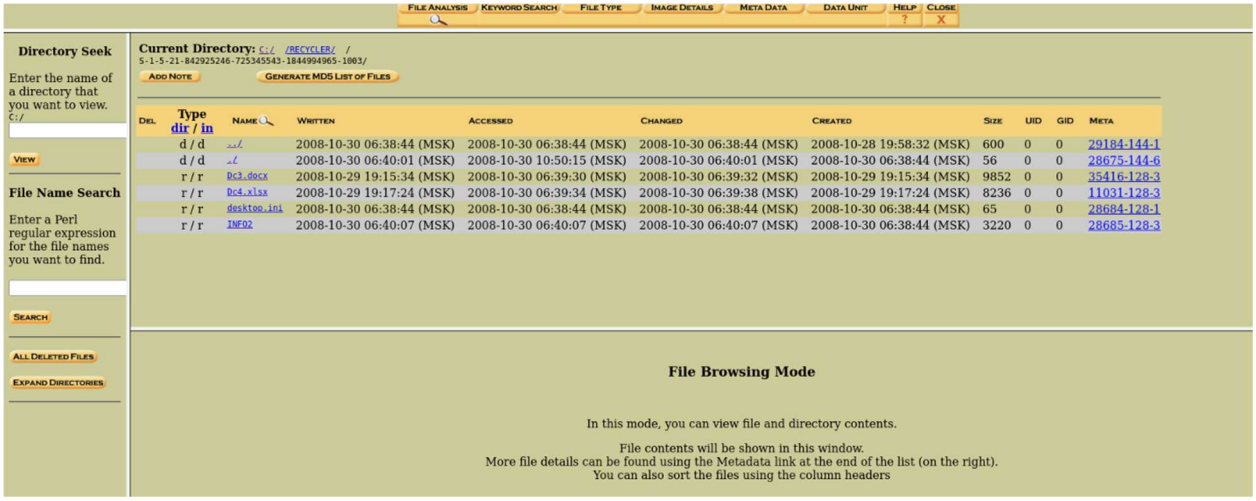

Рисунок 15. Kali Linux версия пример «RECYCLER»

9. Определите номер порта, назначенного для сервиса nntp на исследуемом устройстве.

Ответ: tcp port 119

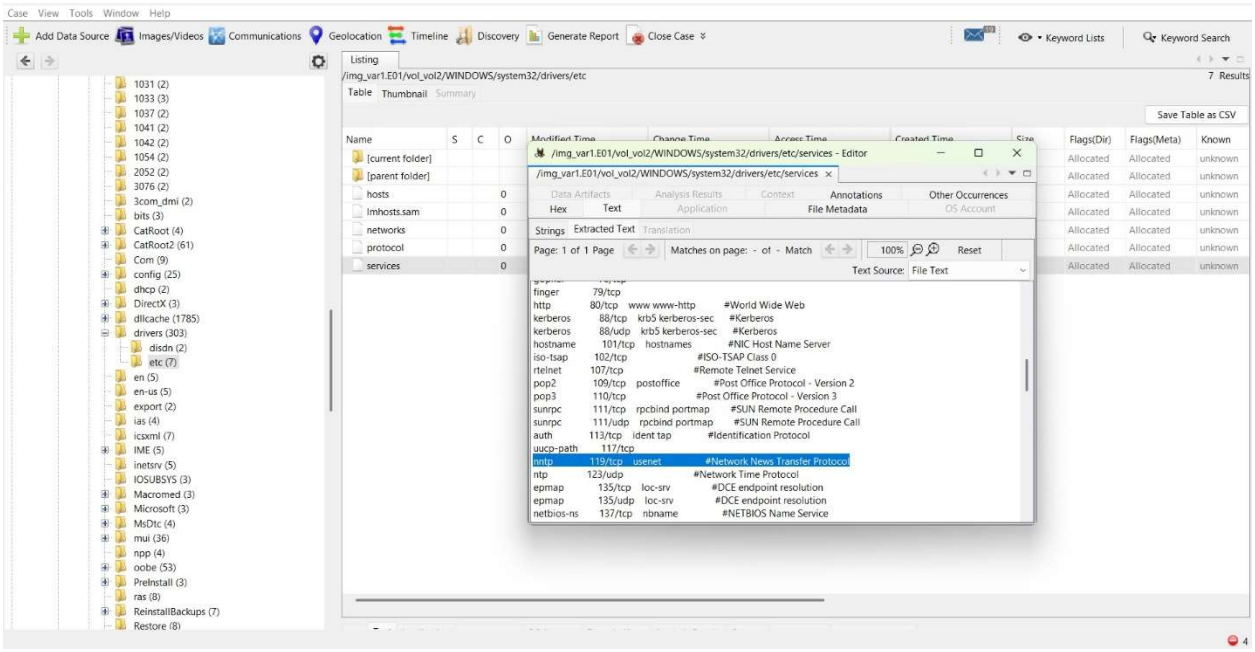

Рисунок 16. Windows версия «etc/services»

10. Укажите все адреса электронной почты, использованные пользователем с номером «1» в имени пользователя

Ответ:

domex1@aol.com; domex1@aim.com; domex1@ar.atwola.com; domex1@at.atwola.com; domex1@atdmt.com; domex1@atwola.com; domex1@c.live; domex1@c.live.com; domex1@c.msn.com; domex1@cdn.at.atwola.com; domex1@doubleclick.net; domex1@google.com; domex1@live.com; domex1@logservice.live; domex1@logservice.live.com; domex1@mail.google.com; domex1@msn.com; domex1@msnportal.112.2o7.net; domex1@my.screenname.aol; domex1@my.screenname.aol.com; domex1@rad.msn.com; domex1@revsci.net; domex1@www.live; domex1@www.live.com; domex1@www.msn.com.

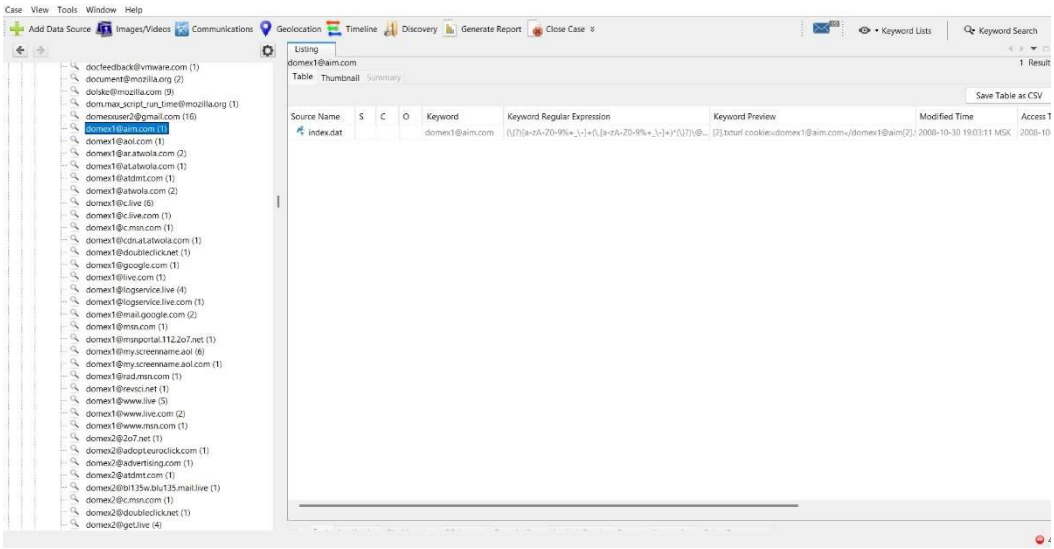

Рисунок 17. Windows версия «emails»