

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

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

Домашнее задание №2, 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 _____

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

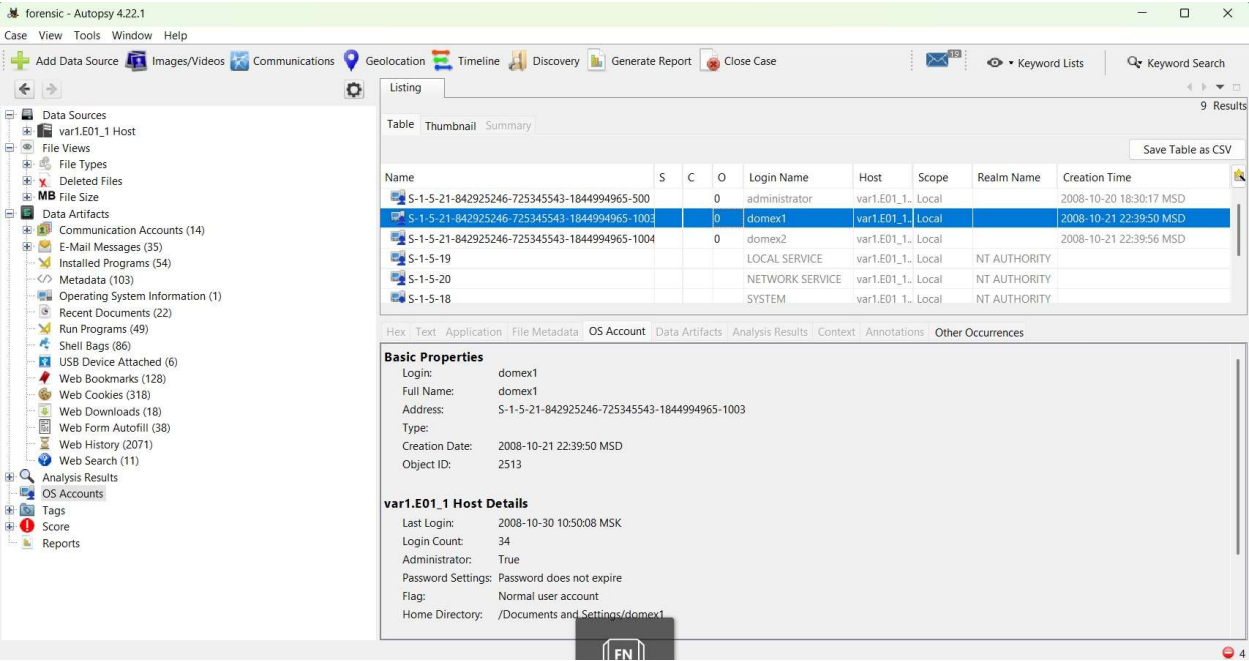


Рисунок 1. Windows версия «OS Accounts»

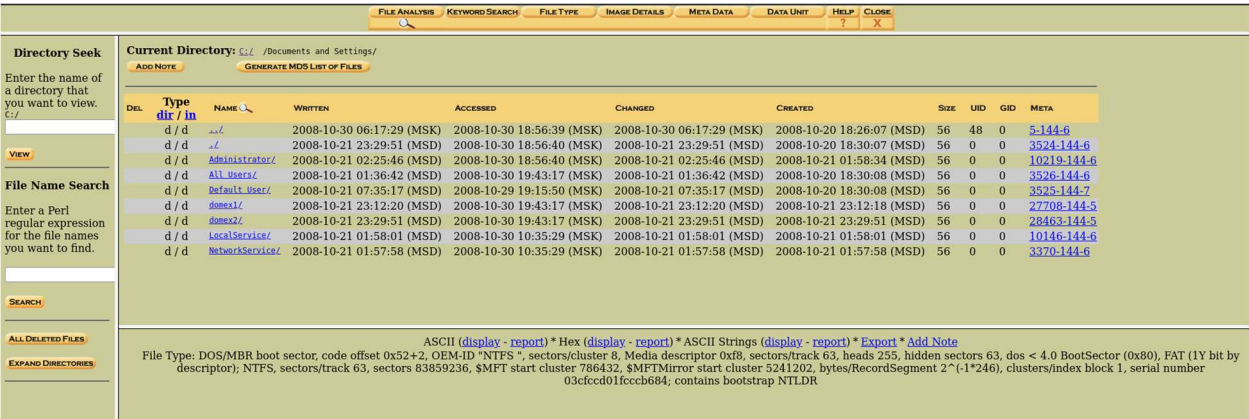


Рисунок 2. Kali Linux версия «Users»

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)

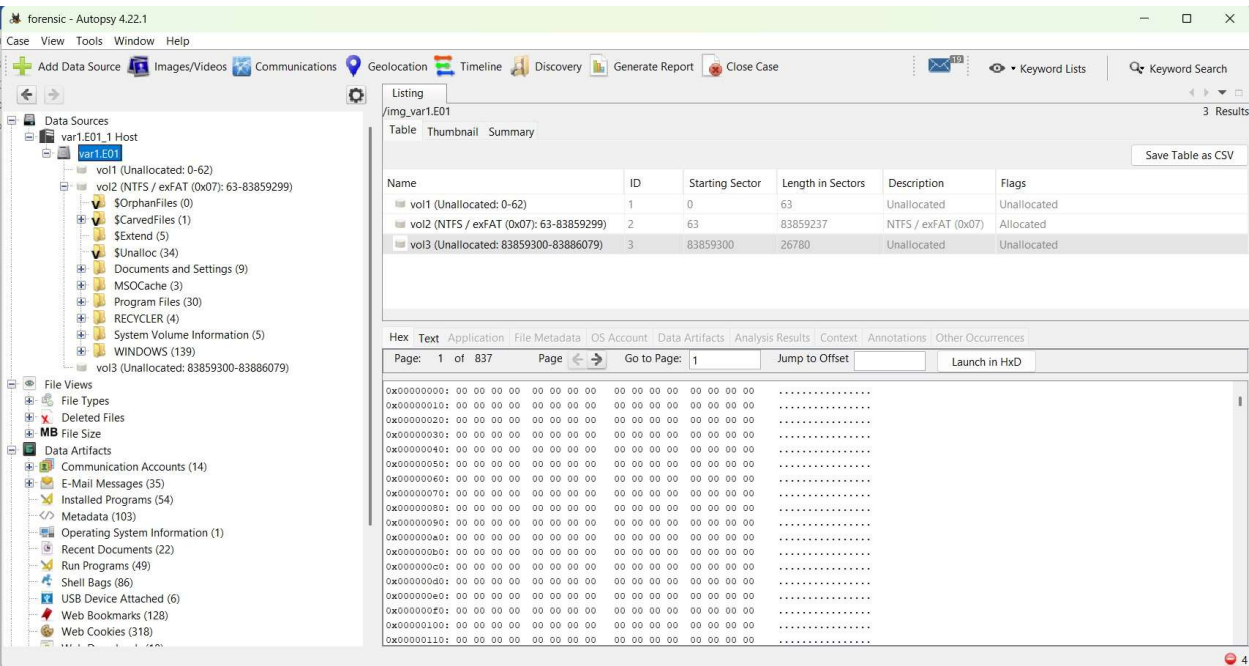


Рисунок 3. Windows версия «области диска»



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)

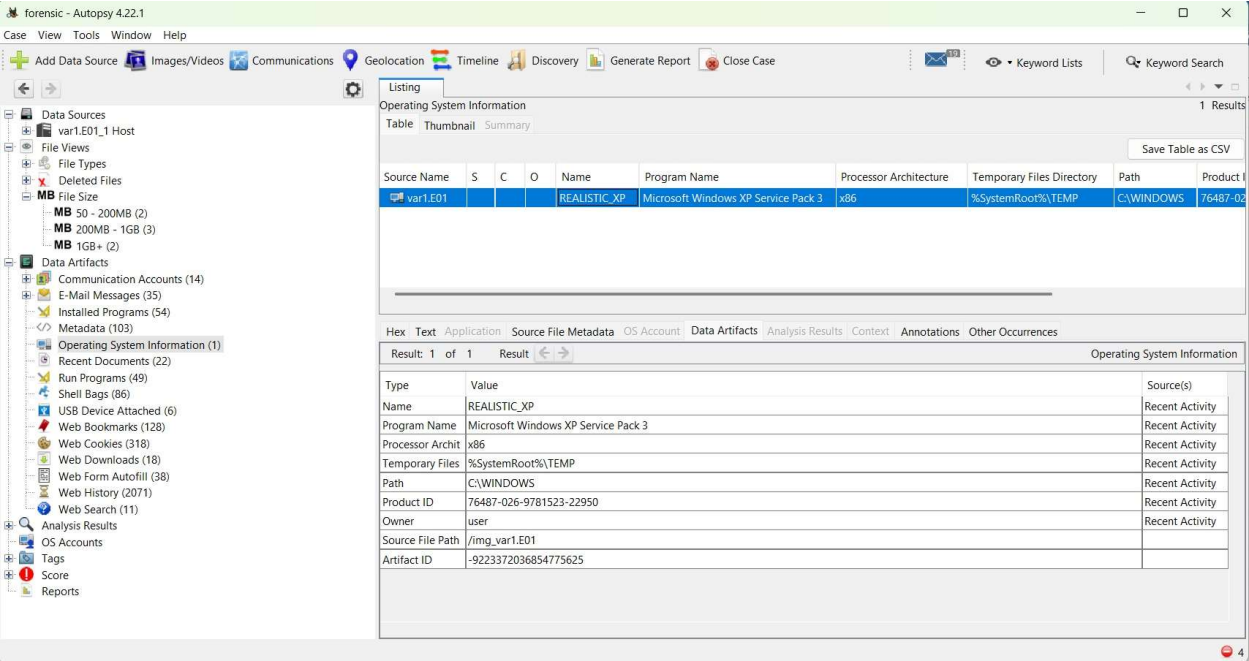


Рисунок 5. Windows версия «Operating System Information»

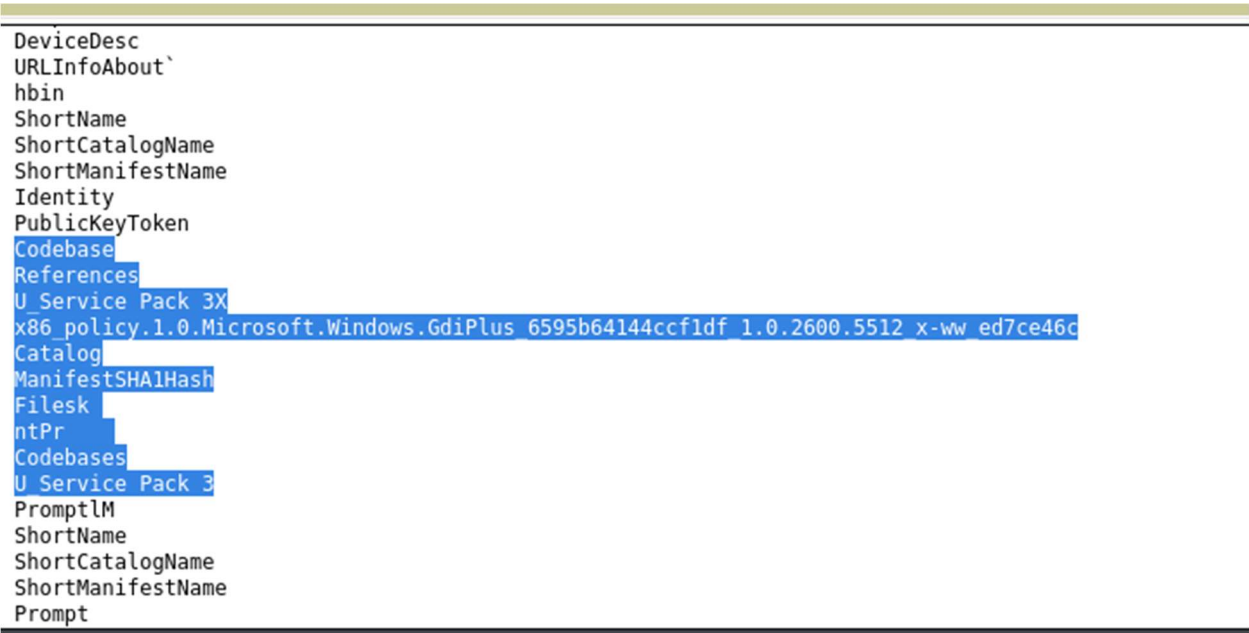


Рисунок 6. Kali Linux версия «анализ файла реестра SOFTWARE»

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

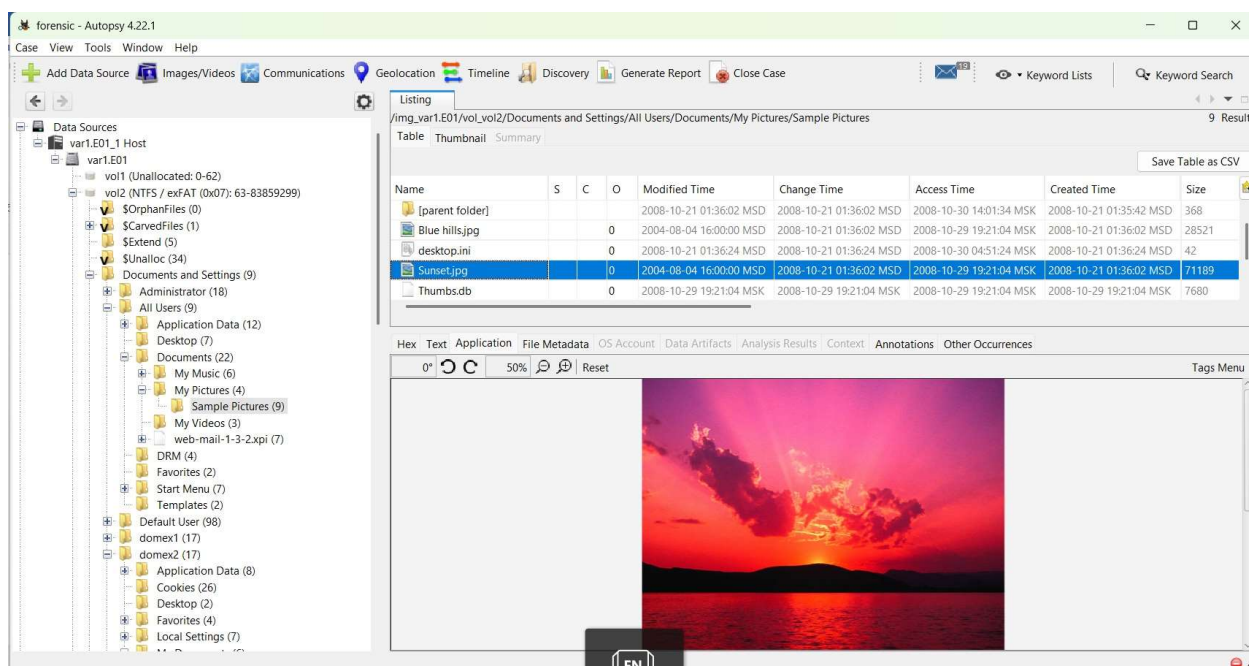


Рисунок 7. Windows версия «Sunset.jpg»

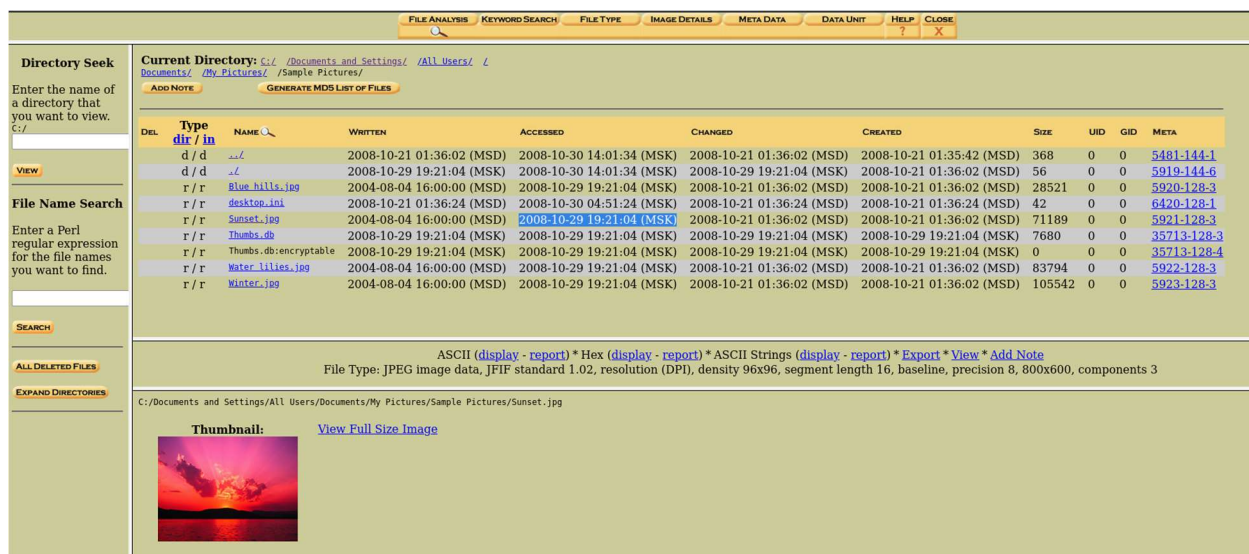


Рисунок 8. Kali Linux версия «Sunset.jpg»

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

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

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE											
Directory Seek	Error Parsing File (invalid characters?) : V/V 36880: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	DEL	Type dir \	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r		C:/Documents and Settings/domex1/Application Data/Microsoft/Office/Recent/This is a spreadsheet sent by domex user 1.xlsx	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:28 (MSK)	623	0	0	35391-128-4
	r / r		C:/Documents and Settings/domex1/Application Data/Microsoft/Office/Recent/This is a spreadsheet deleted by domex user 1.xlsx	2008-10-29 19:17:24 (MSK)	2008-10-29 19:17:24 (MSK)	2008-10-29 19:17:24 (MSK)	2008-10-29 19:17:24 (MSK)	663	0	0	11033-128-4
	r / r		C:/Documents and Settings/domex1/Application Data/Microsoft/Office/Recent/This is a spreadsheet sent by domex user 1.xlsx	2008-10-29 19:16:52 (MSK)	2008-10-29 19:16:52 (MSK)	2008-10-29 19:16:52 (MSK)	2008-10-29 19:16:52 (MSK)	648	0	0	35421-128-4
	r / r		C:/Documents and Settings/domex1/My Documents/This is a spreadsheet sent by domex user 1.xlsx	2008-10-29 19:16:28 (MSK)	2008-10-30 05:04:32 (MSK)	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:27 (MSK)	8230	0	0	35419-128-3
	r / r		C:/Documents and Settings/domex1/My Documents/This is a spreadsheet sent by domex user 1.xlsx	2008-10-29 19:16:52 (MSK)	2008-10-30 06:38:10 (MSK)	2008-10-29 19:16:52 (MSK)	2008-10-29 19:16:51 (MSK)	8203	0	0	35424-128-3
	r / r		C:/Documents and Settings/domex1/Recent/This is a spreadsheet sent by domex user 1.xlsx	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:28 (MSK)	2008-10-29 19:16:28 (MSK)	697	0	0	35420-128-4
	r / r		C:/Documents and Settings/domex1/Recent/This is a spreadsheet deleted by domex user 1.xlsx	2008-10-29 19:17:24 (MSK)	2008-10-29 19:17:24 (MSK)	2008-10-29 19:17:24 (MSK)	2008-10-29 19:17:24 (MSK)	737	0	0	11035-128-4
	r / r		C:/Documents and Settings/domex1/Recent/This is a spreadsheet sent by domex user 1.xlsx	2008-10-30 06:38:05 (MSK)	2008-10-30 06:38:05 (MSK)	2008-10-30 06:38:05 (MSK)	2008-10-29 19:16:52 (MSK)	722	0	0	28679-128-4
View											
File Name Search											
Regular expression or the file names you want to find.											
spreadsheet											
SEARCH											
All Deleted Files	ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note										
	File Type: ERROR:[gzip:] (Microsoft Excel 2007+)										
Expand Directories											
	ASCII String Contents Of File: C:/Documents and Settings/domex1/My Documents/This is a spreadsheet sent by domex user 1.xlsx										

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)

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE											
Directory Seek	All files with '.wma' in the name										
	SHOW ALL FILES										
	Error Parsing File (invalid characters?) : V/V 36880: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0										
	DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
VIEW		r / r	C:/Documents and Settings/All Users/Documents/My Music/Sample Music/Beethoven's Symphony No. 9 (Scherzo).wma	2004-08-04 16:00:00 (MSD)	2008-10-21 01:36:02 (MSD)	2008-10-21 01:36:02 (MSD)	2008-10-21 01:36:02 (MSD)	613638	0	0	5925-128-3
		r / r	C:/Documents and Settings/All Users/Documents/My Music/Sample Music/New Stories (Hiphop, RnB).wma	2004-08-04 16:00:00 (MSD)	2008-10-21 01:36:02 (MSD)	2008-10-21 01:36:02 (MSD)	2008-10-21 01:36:02 (MSD)	760748	0	0	5926-128-3
File Name Search		r / r	C:/Program Files/ATM/services/addressBookApp/ver1_1_28_1/content/dialogs/FanMailListList.bbox	2007-02-02 00:40:27 (MSK)	2008-10-21 19:09:01 (MSD)	2008-10-21 19:09:01 (MSD)	2007-02-02 00:40:27 (MSK)	6138	0	0	25858-128-4
		r / r	C:/Program Files/ATM/services/addressBookApp/ver1_1_28_1/content/dialogs/FanMailListList.is	2006-08-24 02:10:06 (MSD)	2008-10-21 19:09:01 (MSD)	2008-10-21 19:09:01 (MSD)	2006-08-24 02:10:06 (MSD)	8008	0	0	25859-128-4
Windows Media Player		r / r	C:/Program Files/ATM/services/addressBookApp/ver1_1_28_1/content/dialogs/newMailListList.bbox	2007-10-30 22:51:10 (MSK)	2008-10-21 19:09:01 (MSD)	2008-10-21 19:09:01 (MSD)	2007-10-30 22:51:10 (MSK)	2539	0	0	25869-128-4
		r / r	C:/Program Files/ATM/services/addressBookApp/ver1_1_28_1/content/dialogs/newMailListList.is	2007-07-11 18:46:35 (MSD)	2008-10-21 19:09:01 (MSD)	2008-10-21 19:09:01 (MSD)	2007-07-11 18:46:35 (MSD)	3042	0	0	25870-128-4
SEARCH											
ALL DELETED FILES											
EXPAND DIRECTORIES											
File Browsing Mode											
In this mode, you can view file and directory contents.											
File contents will be shown in this window.											

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.

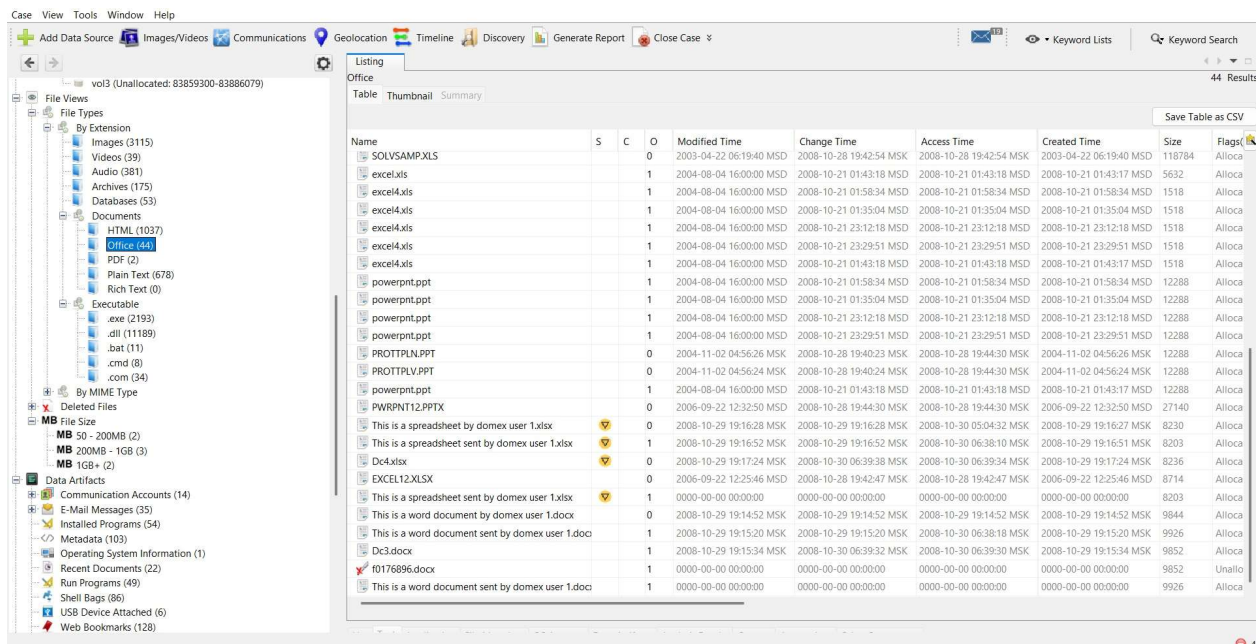


Рисунок 14. Windows версия «File Types -...- Office»

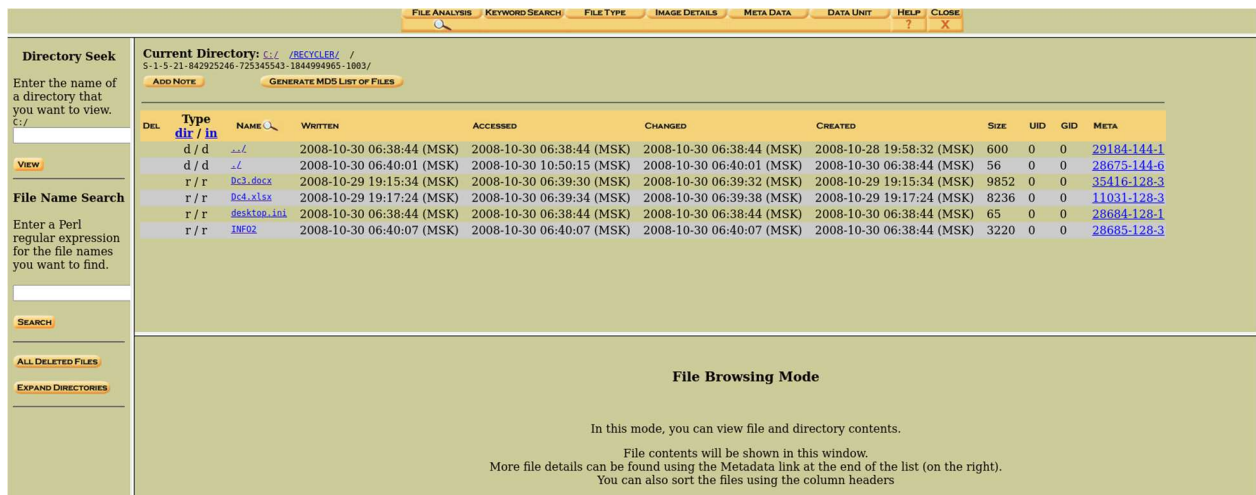


Рисунок 15. Kali Linux версия пример «RECYCLER»

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

Ответ: tcp port 119

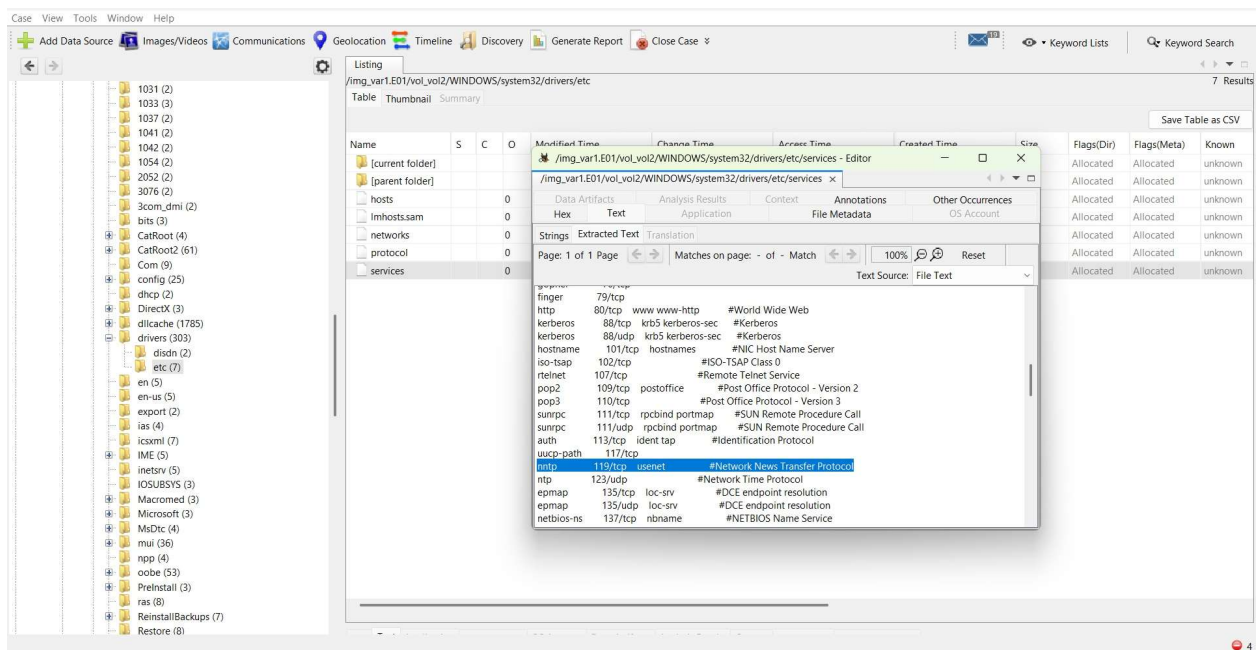


Рисунок 16. Windows версия «etc/services»

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@atdm.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.

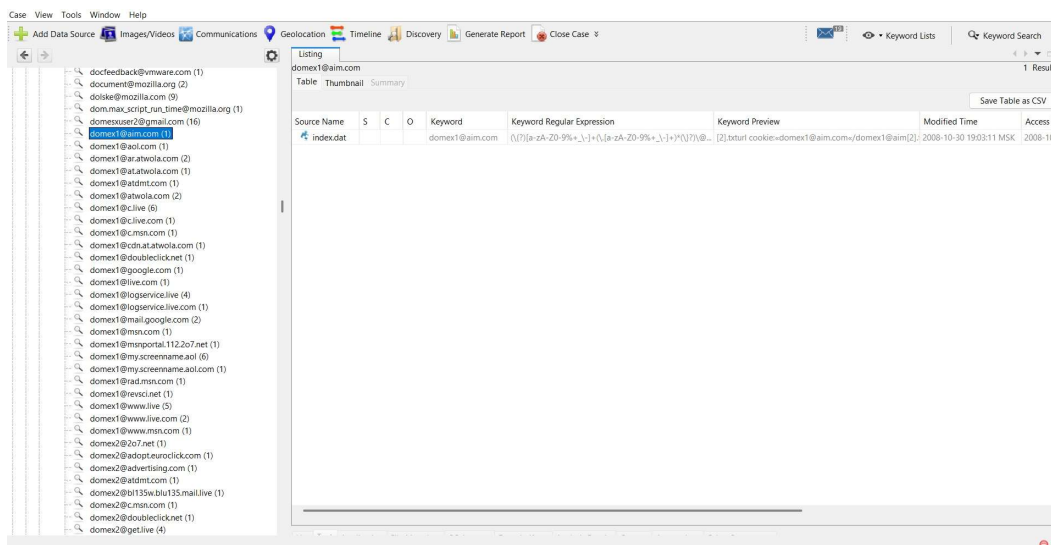


Рисунок 17. Windows версия «emails»