

Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

Практическая работа №2
для слушателей программы повышения квалификации
«ОСНОВЫ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ
И МЕТОДИКИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»



Брянск
БГТУ
2022

Осмотр окончен:

Описание конфигурации устройств и программного обеспечения компьютера:

Дата и время осмотра г., системные часы компьютера показывают точное время часового пояса «Москва».

Объект осмотра:

Имя компьютера, на котором проводится осмотр (серийные номера и т.д.), оперативная память:

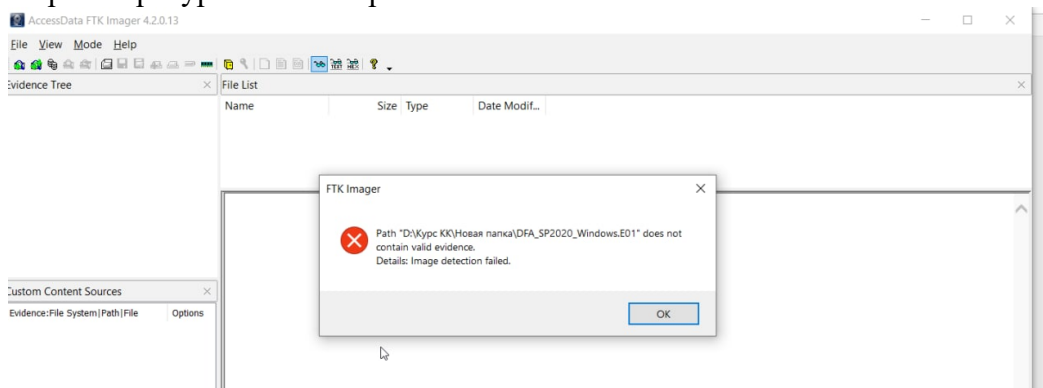
Программы участвующие в анализе образа жесткого диска:

Регистрация (наличие лицензии у программ):

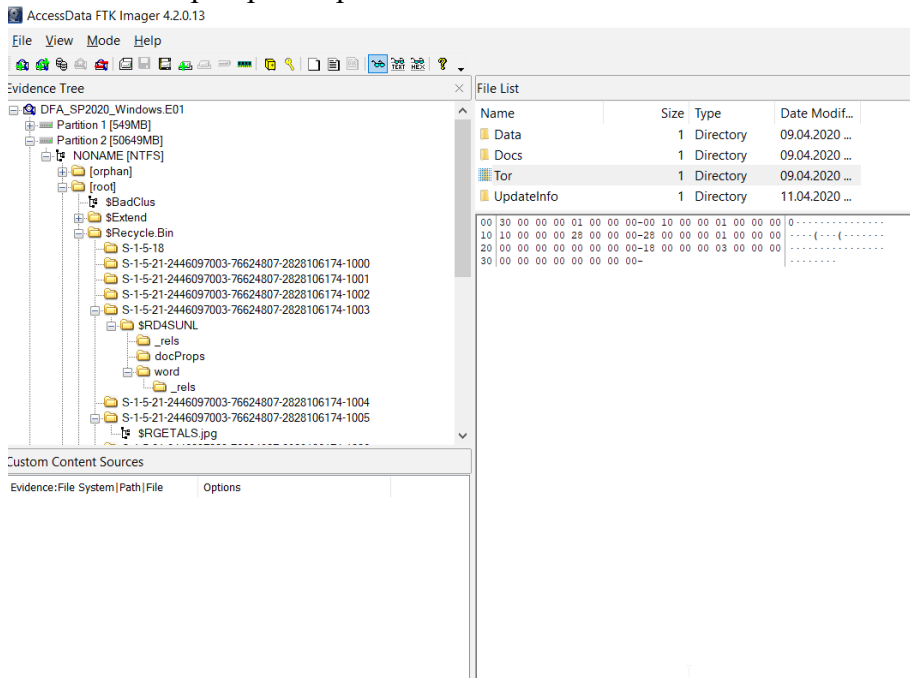
Перед комиссией поставлены следующие вопросы:

1. Является ли представленный образ работоспособным?

Образ из ресурса также нерабочий



Полный набор образа – рабочий:



2. Установить имя компьютера и его id.
Id = 16299

Values					
Поместите сюда заголовок колонки для группировки по этой колонке					
	Value Name	Value Type	Data	Value Slack	Is De
▼	Root	Root	Root	Root	
	SystemRoot	RegSz	C:\Windows	00-00-00-00-00-00	
	BuildBranch	RegSz	rs3_release	00-00-00-00	
	BuildGUID	RegSz	ffffffff-ffff-ffff-ffffffff	00-00	
	BuildLab	RegSz	16299.rs3_release_svc.180808-1748		
	BuildLabEx	RegSz	16299.637.amd64fre.rs3_release_svc.18080...	65-00-43-00-6F-00	
	CompositionEditionID	RegSz	Enterprise	00-00-00-00-00-00	
	CurrentBuild	RegSz	16299		
▶	CurrentBuildNumber	RegSz	16299		
	CurrentMajorVersionNumber	RegDword	10		
	CurrentMinorVersionNumber	RegDword	0		
	CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00	
	CurrentVersion	RegSz	6.3	00-00-00-00	
	EditionID	RegSz	Enterprise	00-00-00-00-00-00	
	EditionSubstring	RegSz			
	InstallationType	RegSz	Client	00-00-00-00-00-00	
	InstallDate	RegDword	1585879468		

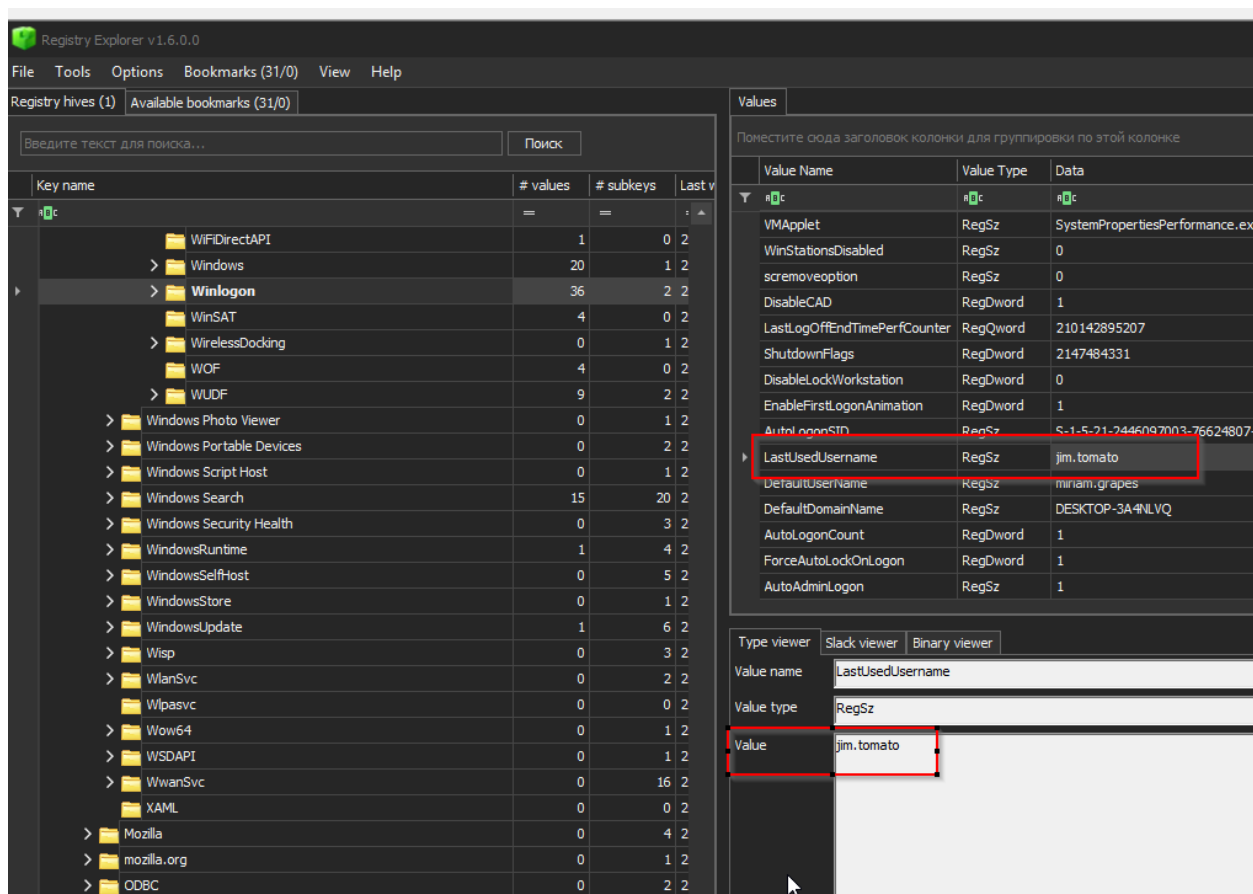
Type viewer	Binary viewer
Value name	CurrentBuildNumber
Value type	RegSz
Value	16299

Имя: DESKTOP-3A4NLVQ

Поместите сюда заголовок колонки для группировки по этой колонке					
	Value Name	Value Type	Data	Value Slack	Is T
▼	Root	Root	Root	Root	
	(default)	RegSz	mnmsrvc	DC-00-00-00	
▶	ComputerName	RegSz	DESKTOP-3A4NLVQ	00-00-00-00	

3. Какой из пользователей последний входил в систему?

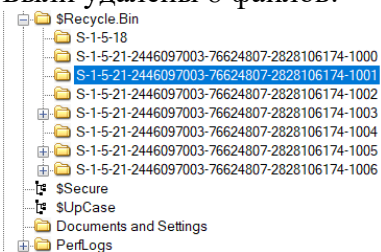
User: jim.tomato



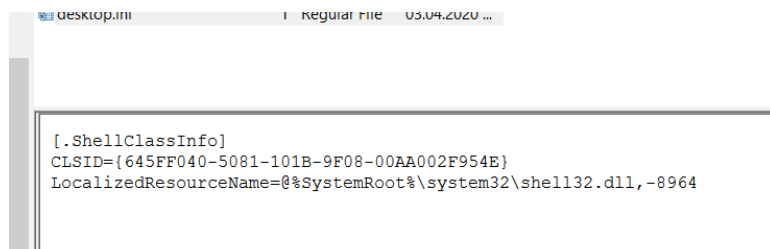
4. Присутствуют ли на образе факты удаления, уничтожения файлов(данных)?

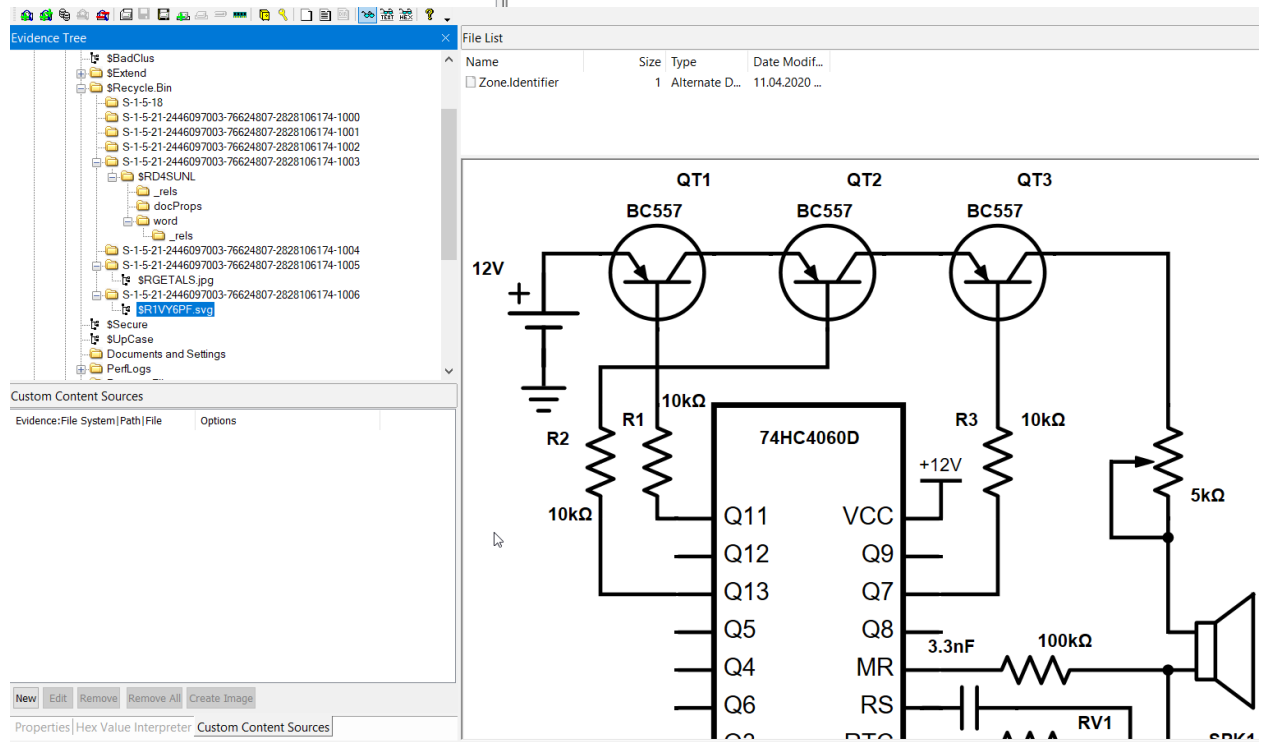
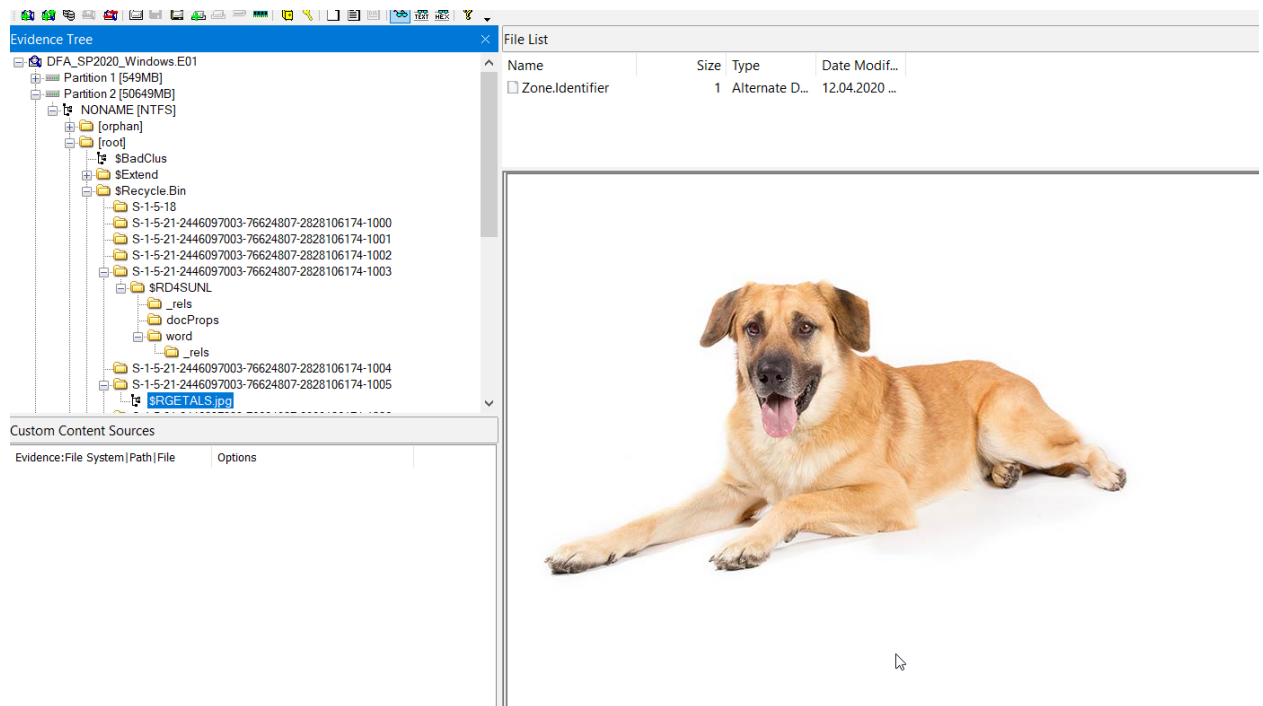
Да, присутствуют.

Были удалены 8 файлов:



Например:

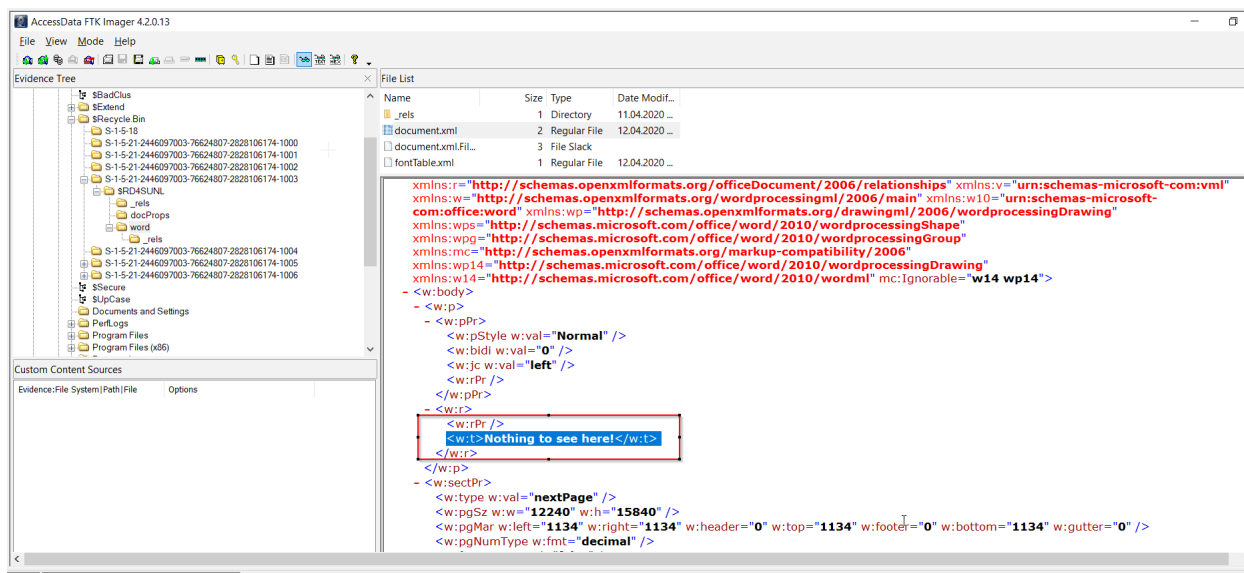




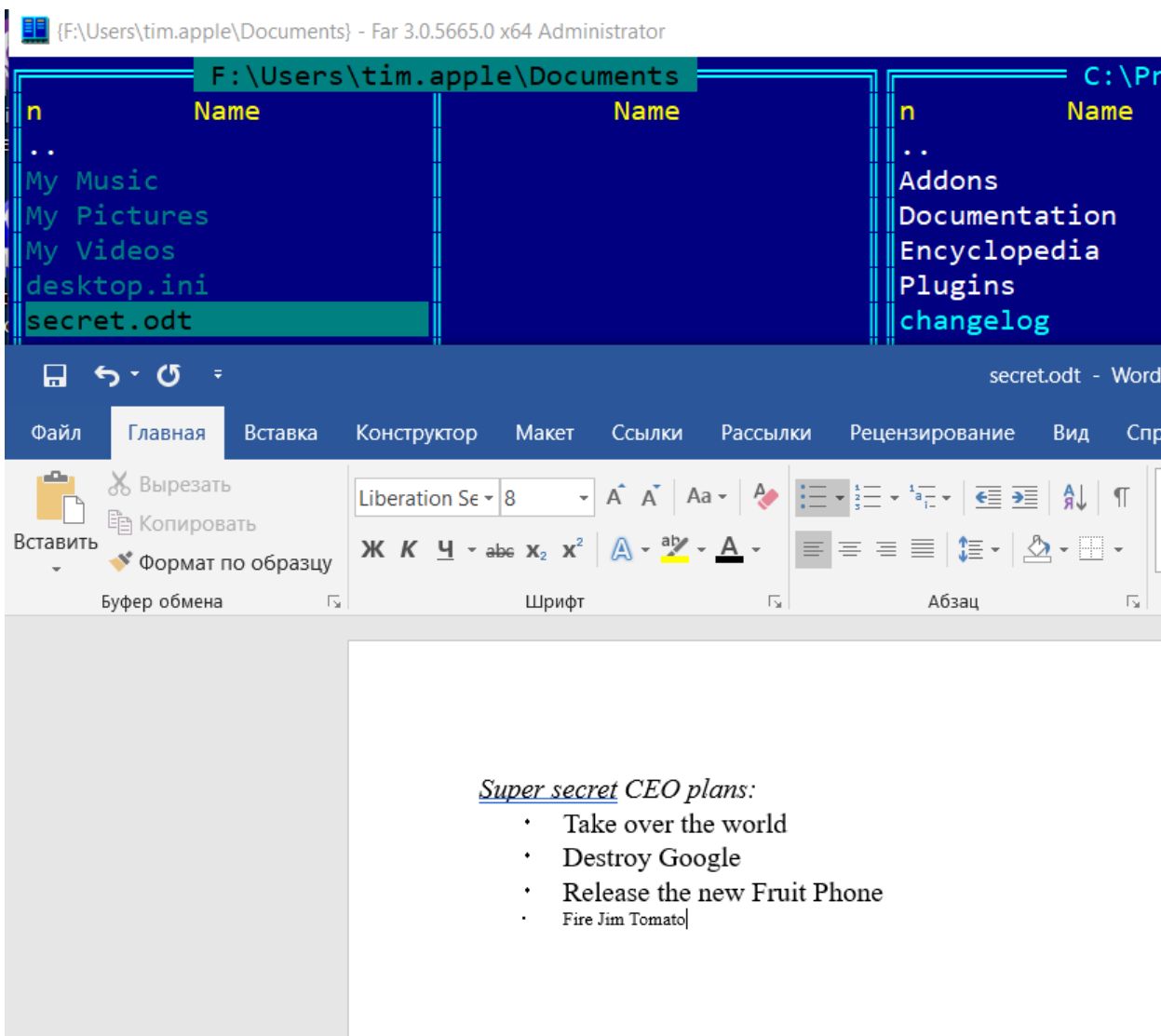
5. Содержат ли какие-то из файлов информацию конфиденциального назначения?

Вероятно, что принципиальная схема устройства выше может быть конфиденциальна

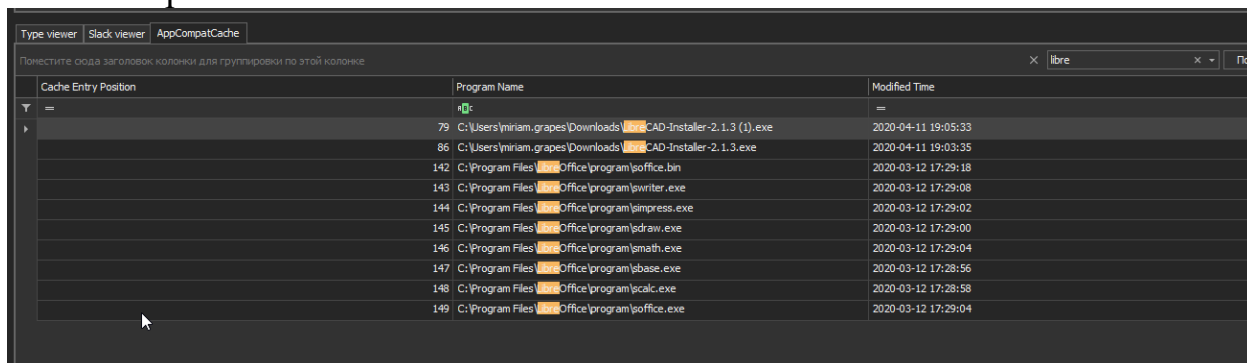
Вероятно, что удаленный файл *.doc может быть конфиденциальным



Также потенциально конфиденциальным может быть документ secret.odt пользователя tim.apple, в том числе скрытая строка «Fire Jim Tomato»



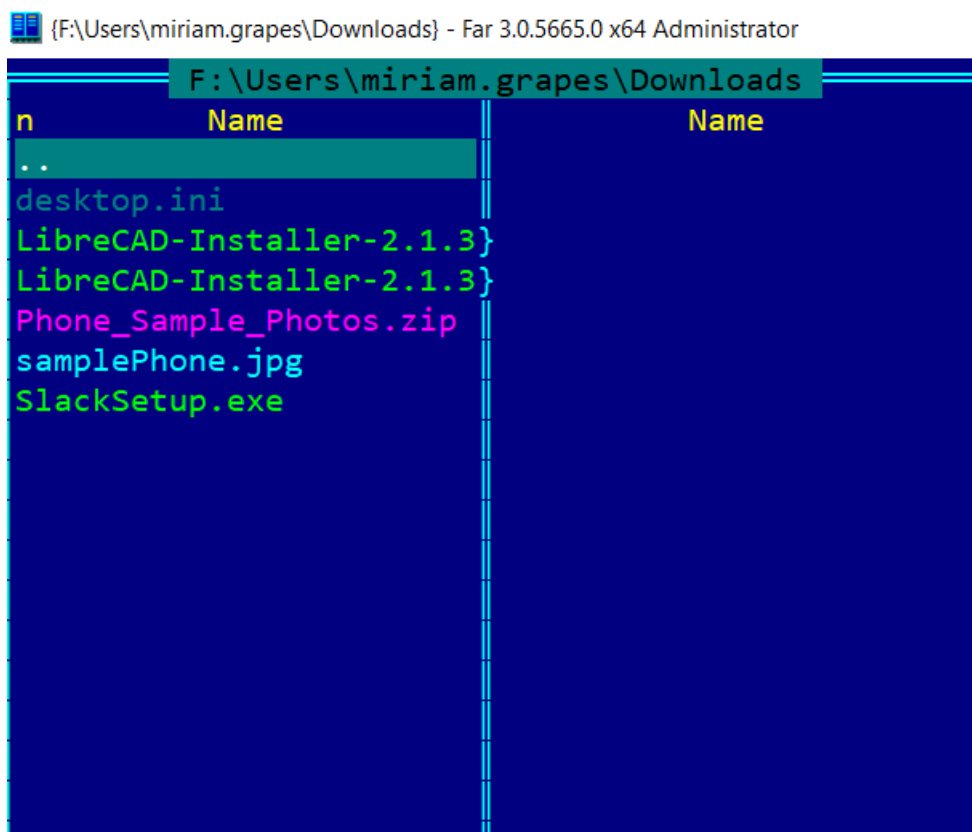
6. Возможно ли установить кто устанавливал программу LberCad на основной компьютер?



Cache Entry Position	Program Name	Modified Time
79	C:\Users\miriam.grapes\Downloads\LibreCAD-Installer-2.1.3 (1).exe	2020-04-11 19:05:33
86	C:\Users\miriam.grapes\Downloads\LibreCAD-Installer-2.1.3.exe	2020-04-11 19:03:35
142	C:\Program Files\LibreCAD\program\soffice.bin	2020-03-12 17:29:18
143	C:\Program Files\LibreCAD\program\swriter.exe	2020-03-12 17:29:08
144	C:\Program Files\LibreCAD\program\simpress.exe	2020-03-12 17:29:02
145	C:\Program Files\LibreCAD\program\draw.exe	2020-03-12 17:29:00
146	C:\Program Files\LibreCAD\program\smath.exe	2020-03-12 17:29:04
147	C:\Program Files\LibreCAD\program\sbrowser.exe	2020-03-12 17:28:56
148	C:\Program Files\LibreCAD\program\scalculator.exe	2020-03-12 17:28:58
149	C:\Program Files\LibreCAD\program\soffice.exe	2020-03-12 17:29:04

Установил пользователь: miriam.grapes

Также установочный файл в директории пользователя miriam.grapes:



В момент осмотра установлены:

Результаты осмотра:

Осмотром установлено:

Объектами осмотра являются:

