

Министерство науки и высшего образования Российской
Федерации

Брянский государственный технический университет

Практическая работа №5
для слушателей программы повышения квалификации
«Основы компьютерной криминалистики
и методики реагирования на инциденты информационной
безопасности»



Брянск
БГТУ
2022

Брянский государственный технический университет
241035, Брянск, бульвар 50 лет Октября, 7.
Кафедра «Системы информационной безопасности», тел. 58-82-16.

Выбрав один из дисков на рабочем компьютере, провести его анализ.

ПРОТОКОЛ № 5 2022 г.

Комиссия в составе:

Начала осмотр в:

Осмотр окончен:

**Описание конфигурации устройств и программного обеспечения
компьютера:**

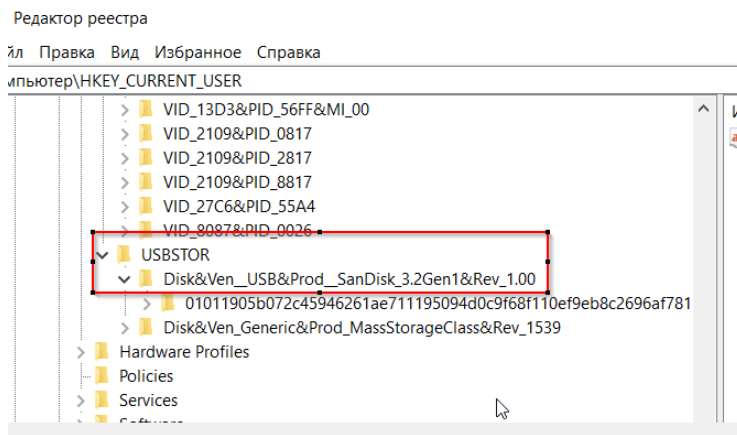
Объект осмотра:

**Имя компьютера, на котором проводится осмотр:
оперативная память:**

Программы участвующие в анализе памяти системы:

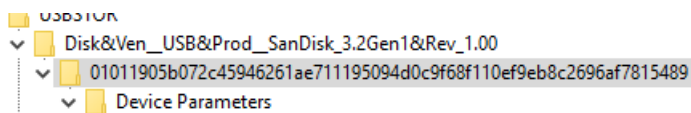
Перед комиссией поставлены следующие вопросы:

1. Присутствуют ли на носителе факты удаления, уничтожения файлов(данных)
(проверить минимум 2-мя программами)?
Да, содержат
2. Содержат ли какие-то из файлов информацию конфиденциального
назначения (вещественные доказательства по делу)?
Не содержат
3. Удалялась ли информация со съемного носителя в период с 01.07.2019 по
01.08.2019?
Не удалялась
4. Есть ли подключение USB с именем SanDisk?
Да, есть:



5. Если есть подключение, возможно ли вывести его дату последнего присутствия в системе?

Да, возможно: по серийному номеру через USBDev: 28.09.2021



USBDevView									
File Edit View Options Help									
	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number		Registry Time 1	Registry Time 2
Device D...	No	Yes	No	No				28.09.2021 10:45:14	28.09.2021 10:45:14
Device D...	No	Yes	No	No				28.09.2021 10:45:14	28.09.2021 10:45:14
Device D...	Yes	Yes	No	No				08.04.2022 17:19:05	22.09.2021 22:59:37
Device D...	Yes	Yes	No	No				08.04.2022 17:19:03	29.09.2021 16:08:02
Device D...	Yes	Yes	No	No				08.04.2022 17:19:05	08.04.2022 17:19:05
Device D...	Yes	Yes	No	No				08.04.2022 17:19:05	08.04.2022 17:19:05
Device D...	No	Yes	No	No		01011905b072c45946261ae711195094d0c9f68f110ef9eb8c2696af7815489	33a00000000000000000	28.09.2021 10:45:07	28.09.2021 10:42:35
Device D...	No	Yes	No	No		0000000001539		28.09.2021 10:45:11	28.09.2021 10:42:35
Device D...	No	Yes	No	No				28.09.2021 10:45:07	28.09.2021 10:42:35
Device D...	No	Yes	No	No				28.09.2021 10:45:14	28.09.2021 10:42:35
Device D...	No	Yes	No	No		0010000001		27.01.2022 20:00:34	28.09.2021 10:42:35
Device D...	No	Yes	No	No				28.09.2021 10:45:14	28.09.2021 10:42:35
Device D...	No	No	No	No		000000000000000001		28.09.2021 10:42:41	28.09.2021 10:42:35
Device D...	Yes	Yes	No	No				08.04.2022 17:19:03	22.09.2021 22:59:37
Device D...	Yes	Yes	No	No				08.04.2022 17:19:06	22.09.2021 23:00:49
Device D...	Yes	Yes	No	No				08.04.2022 17:19:05	22.09.2021 22:59:37
Device D...	Yes	Yes	No	No				08.04.2022 20:43:12	29.09.2021 16:59:02

USBDevView					
File Edit View Options Help					
	Driver InfPath	Instance ID	Capabilities	Install Time	First Install Time
Device D...	input.inf	USB\VID_046D&PID_C534&MI_00\7&2c97483d&0&0000	SurpriseRemovalOK	28.09.2021 10:42:41	28.09.2021 10:42:35
Device D...	input.inf	USB\VID_046D&PID_C534&MI_01\7&2c97483d&0&0001	SurpriseRemovalOK	28.09.2021 10:42:41	28.09.2021 10:42:35
Device D...	oem20.inf	USB\VID_13D3&PID_56FF&MI_00\6&3432745e&0&0000	Removable, SilentInstall, SurpriseRemovalOK	22.09.2021 22:59:37	22.09.2021 22:59:37
Device D...	usb.inf	USB\VID_0E8F&PID_00A8&MI_00\5&171d8861&0&0005	Removable, SurpriseRemovalOK	29.09.2021 16:08:02	29.09.2021 16:08:02
Device D...	input.inf	USB\VID_0E8F&PID_00A8&MI_00\6&39d6fe7&0&0000	SurpriseRemovalOK	29.09.2021 16:08:02	29.09.2021 16:08:02
Device D...	input.inf	USB\VID_0E8F&PID_00A8&MI_01\6&39d6fe7&0&0001	SurpriseRemovalOK	29.09.2021 16:08:02	29.09.2021 16:08:02
Device D...	usbstor.inf	USB\VID_0781&PID_5591\01011905b072c45946261ae711195094d0c9f68f110ef9eb8c2696af7815489a...	Removable, UniqueID, SurpriseRemovalOK	28.09.2021 10:42:35	28.09.2021 10:42:35
Device D...	usbstor.inf	USB\VID_05E3&PID_0749\0000000001539	Removable, UniqueID, SurpriseRemovalOK	28.09.2021 10:42:35	28.09.2021 10:42:35
Device D...	usbhub3.inf	USB\VID_2109&PID_0817\5&263bd205&0&0003	Removable, SurpriseRemovalOK	28.09.2021 10:42:35	28.09.2021 10:42:35
Device D...	usbhub3.inf	USB\VID_2109&PID_2817\5&171d8861&0&0003	Removable, SurpriseRemovalOK	28.09.2021 10:42:40	28.09.2021 10:42:35
Device D...	oem32.inf	USB\VID_0BDA&PID_8153\0010000001	Removable, UniqueID, SurpriseRemovalOK	28.09.2021 10:42:35	28.09.2021 10:42:35
Device D...	usb.inf	USB\VID_046D&PID_C534\6&157adb2b&0&0004	Removable, SurpriseRemovalOK	28.09.2021 10:42:41	28.09.2021 10:42:35
Device D...	winusb.inf	USB\VID_2109&PID_8817\0000000000000001	UniqueID	28.09.2021 10:42:41	28.09.2021 10:42:35
Device D...	usb.inf	USB\VID_13D3&PID_56FF\5&171d8861&0&0007	SurpriseRemovalOK	22.09.2021 22:59:21	22.09.2021 22:59:21
Device D...	oem35.inf	USB\VID_27C6&PID_55A4\5&171d8861&0&0009	SurpriseRemovalOK	22.09.2021 23:00:49	22.09.2021 23:00:49
Device D...	oem28.inf	USB\VID_8087&PID_0026\5&171d8861&0&0010	SurpriseRemovalOK	22.09.2021 22:59:38	22.09.2021 22:59:38
Device D...	oem8.inf	USB\VID_0529&PID_0620\5&171d8861&0&0001	Removable, SurpriseRemovalOK	29.09.2021 16:59:02	29.09.2021 16:59:02

Дополнительный вопрос:

*Присутствуют ли на компьютере скрытые файлы формата .db
(недавно удаленные)?*
Нет.

В момент осмотра установлены:

Результаты осмотра:

Комиссия постановила: