КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра прикладних інформаційних систем

Звіт до лабораторної роботи №4

З курсу

«Безпека мереж і комп’ютерних систем»

студента 2 курсу
групи ПП-22
спеціальності 122 «Комп'ютерні науки»
ОП «Прикладне програмування»
Шевлюк Вікторії Віталіївни

Перевірив:
д.т.н, професор
Сайко В. Г.

Київ 2022

Тема:Аудит і відновлення файлів з інформацією

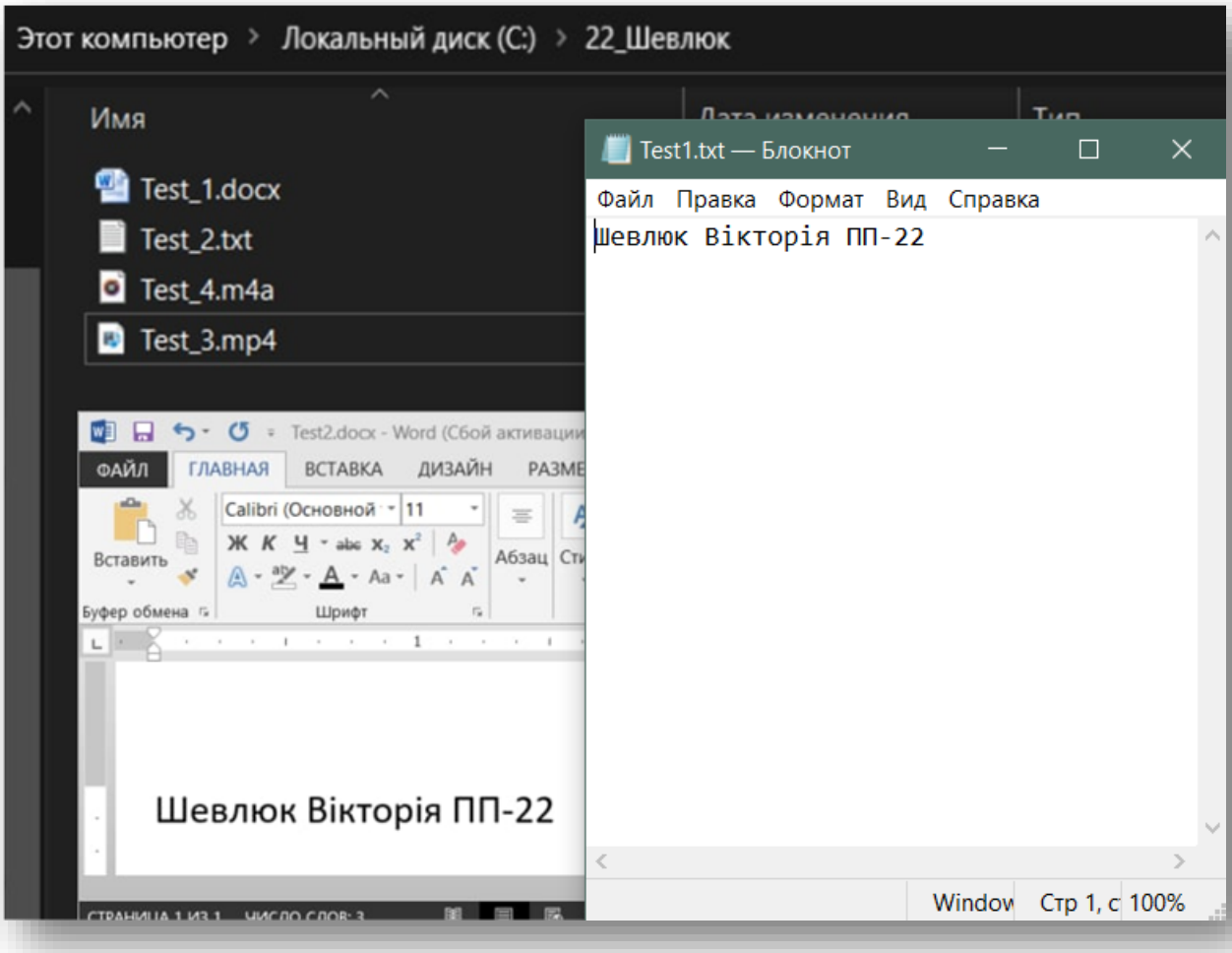
Мета роботи: ознайомитися із файловими системами, вивчити принцип їх функціонування. Здійснити аудит та відновлення файлів за допомогою сучасних інструментів.

Завдання:

Встановити та дослідити роботу кількох програм для відновлення файлів.

Хід роботи:

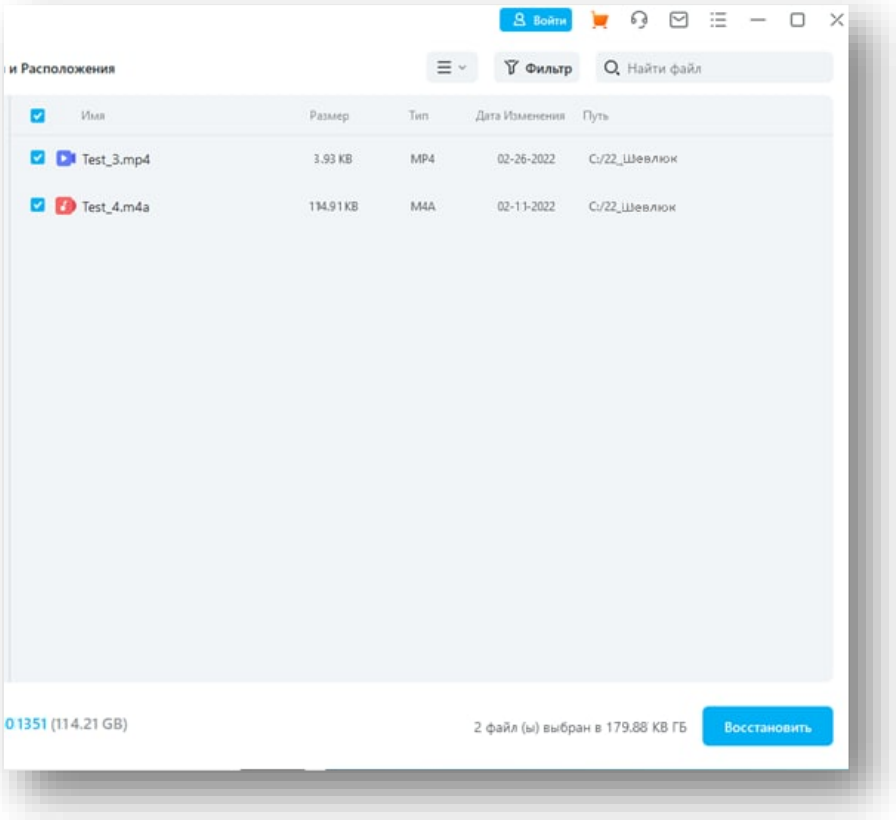
Спочатку створимо 4 файли з різними розширеннями у папці та у кореневому каталозі:



Встановлюємо необхідне програмне забезпечення для відновлення та видаляємо файли, які щойно створили.

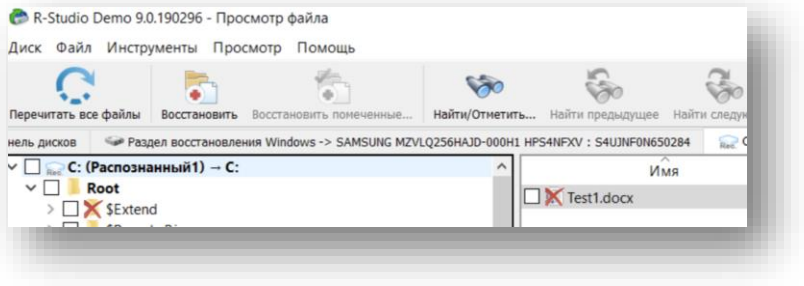
Далі по черзі за допомогою програм скануємо директорії, в яких зберігались наші файли та дивимось на результат роботи:

Спочатку програма Recoverit:



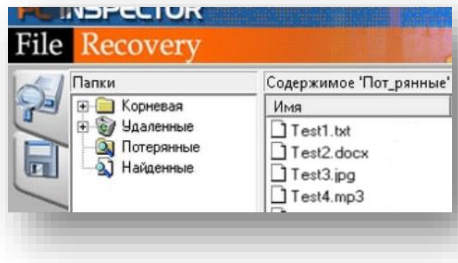
Ця програма знайшла тільки два файла у кореневому каталозі, а файли з папки не знайшла. Також щоб відновити ці файл, потрібно купити повну версію цієї програми.

Далі програма R-Studio:



Дана програма знайшла лише один файлу кореневому каталозі.

Тепер програма PC Inspector File Recovery:



Ця програма знайшла 4 файли, але відновились лише текстові. Файли з відео та аудіо відновились «битими».

Отже, таблиця з результатами роботи вищенаведених програм:

	Відновлені файли	**Recoverit**	**R-Studio**	**PC Inspector File Recovery**
Кореневий каталог	Test1	Не знайдено	*Знайдено*	*Відновлено*
	Test2	Не знайдено	Не знайдено	*Відновлено*
	Test3	*Знайдено*	Не знайдено	*Знайдено*
	Test4	*Знайдено*	Не знайдено	*Знайдено*
22_Шевлюк	Test1	Не знайдено	Не знайдено	Не знайдено
	Test2	Не знайдено	Не знайдено	Не знайдено
	Test3	Не знайдено	Не знайдено	Не знайдено
	Test4	Не знайдено	Не знайдено	Не знайдено

Висновок: В ході даної лабораторної роботи ми розглянули роботу кількох програм. В цілому ніяка з них не показала відмінний результат, хоча, можливо, перша програма працювала б краще, якщо її купити. Остання програма показала найкращий результат, тому, можу її порекомендувати для відновлення втрачених файлів.

Контрольні питання:

1. Назвіть основні розділи логічного диска в файлової системі FAT і охарактеризуйте їх вміст.

Розділи:

► *BootSector* - сектор з завантажувачем, в якому також розміщена інформація про структуру логічного диска.

► *ROOT* - кореневий каталог логічного диска, в якому розміщується інформація про ті файли і каталоги, що безпосередньо знаходяться в кореневому
каталозі логічного диска.

► *FAT* - таблиця розміщення файлів, в якій знаходиться інформація про послідовність тих кластерів, в яких зберігається даний файл. Через виняткову важливість даної таблиці вона представлена в двох примірниках: FAT-1 і FAT-2.

2. Чому розділ FAT представлений на логічному диску в двох примірниках?

Через виняткову важливість.

3. Що означають цифри в назві файлових систем FAT–12, FAT–16 і т. д.?

Розрядність файлових систем.

4. Чому максимальний обсяг логічного диска пов'язаний з довжиною номера кластера?

Кожен запис в таблиці FAT відповідає одному кластеру.

5. Де зберігається інформація про основні характеристики файлу?

Такая інформація зберігається у 32-бітній області.

6. Як відбувається процедура доступу ОС до файлу або папці?

Коли користувач входить в систему, він вводить своє ім’я, яким визначається його ідентифікатор і права доступу.

7. Що таке фрагментація файлів і які її особливості відображення в системі FAT?

Фрагмента́ція фа́йлової систе́ми (старіння файлової системи) — це неспроможність файлової системи розмістити пов'язані дані послідовно (неперервно), явище притаманне файловим системам, що дозволяють пряму модифікацію даних.

Відображається у кластерах.

8. Якими кодами позначаються вільний, дефектний кластер, останній кластер файлу?

- ► 000h – вільний
- ► 0F7h – дефектний
- ► 0F8h – 0FFh, останній

9. Чим відрізняється $MFTMirror від $MFT?

$MFTMirror – копія файлу $MFT, яка містить інформацію тільки про чотирьох службових метафайлів.

10. Де зберігається інформація про розташування $MFT і $MFTMirror на логічному диску?

Ця інформація зберігається у секції BootSector.

11. Який обсяг запису в $MFT?

Обсяг дорівнює 1Kb

12. Які характерні ознаки має запис $MFT?

Це є файл для зберігання даних.

13. Що називають атрибутом файлу в записі $MFT?

Області змінної довжини.

14. З якої причини відновлення файлу не завжди можливо?

• Минуло багато часу з видалення файлу.

• Через ступінь фрагментації видаленого файлу.