# 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-21 спеціальності 122 «Комп'ютерні науки» ОП «Прикладне програмування»*

%username%

*Викладач:*

проф. Сайко В.Г.

## Київ – 202

**1.Назва роботи**

Аудит і відновлення файлів з інформацією

1. **Тема роботи**

Аудит і відновлення файлів з інформацією

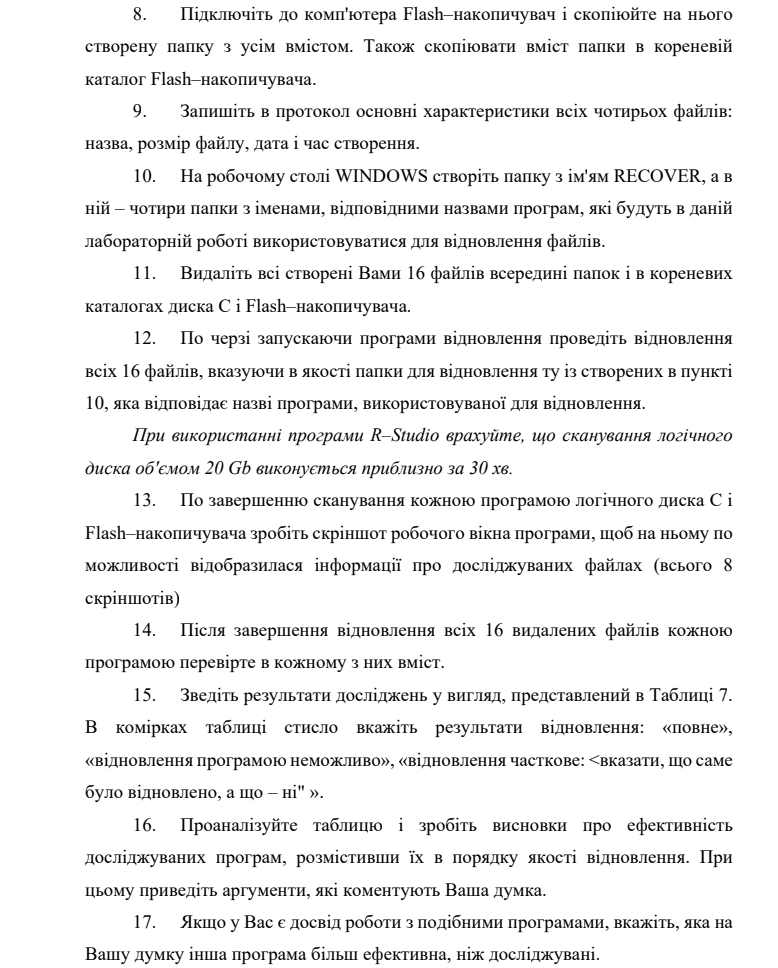
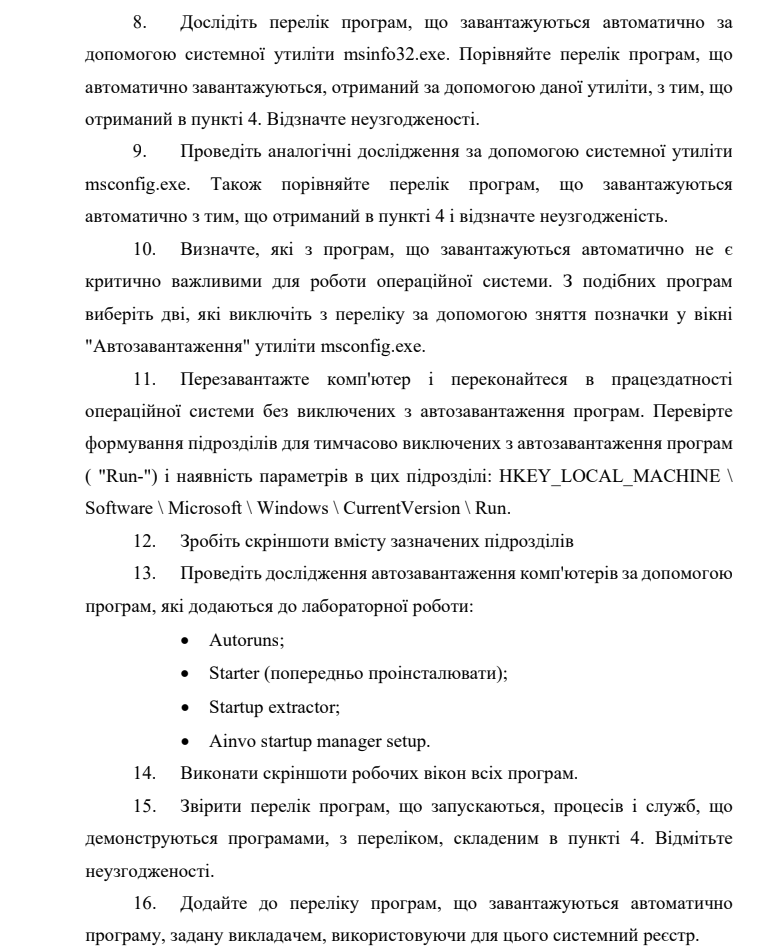
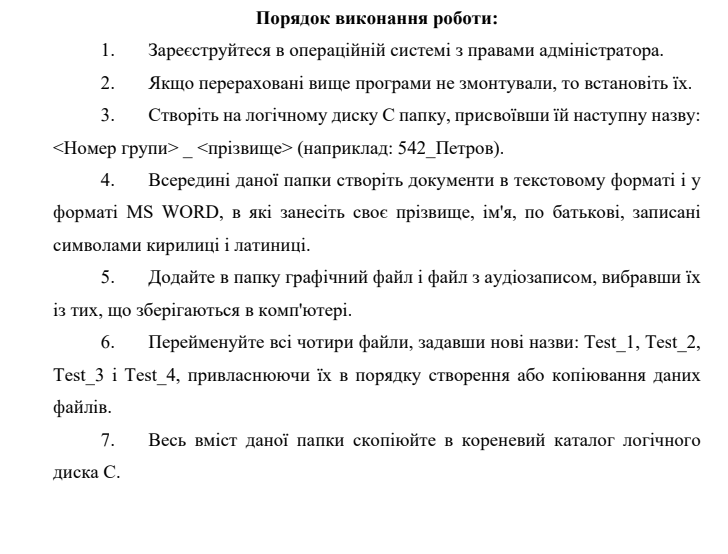
1. **Мета роботи**

Ознайомитися із файловими системами, вивчити принцип їх

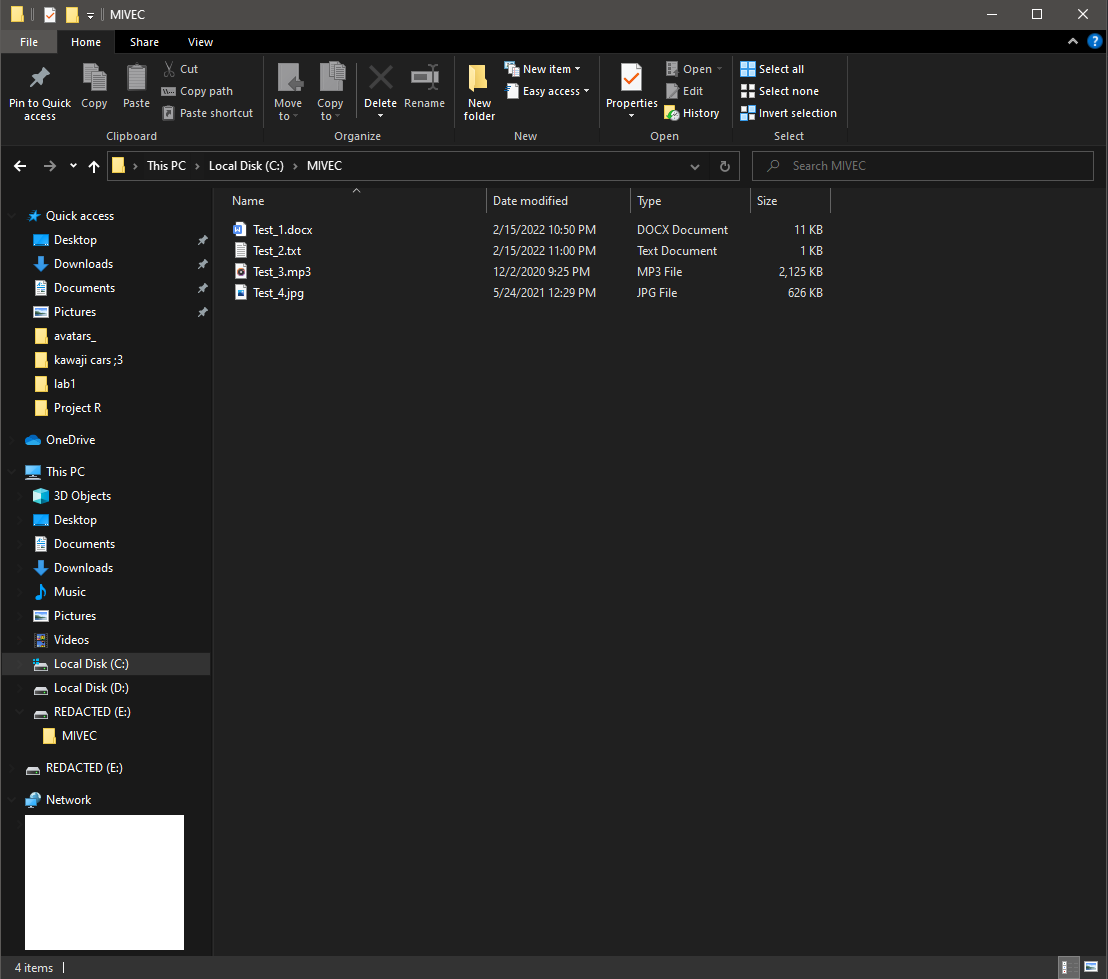
функціонування. Здійснити аудит та відновлення файлів за допомогою сучасних

інструментів.

1. **Умова завдання**

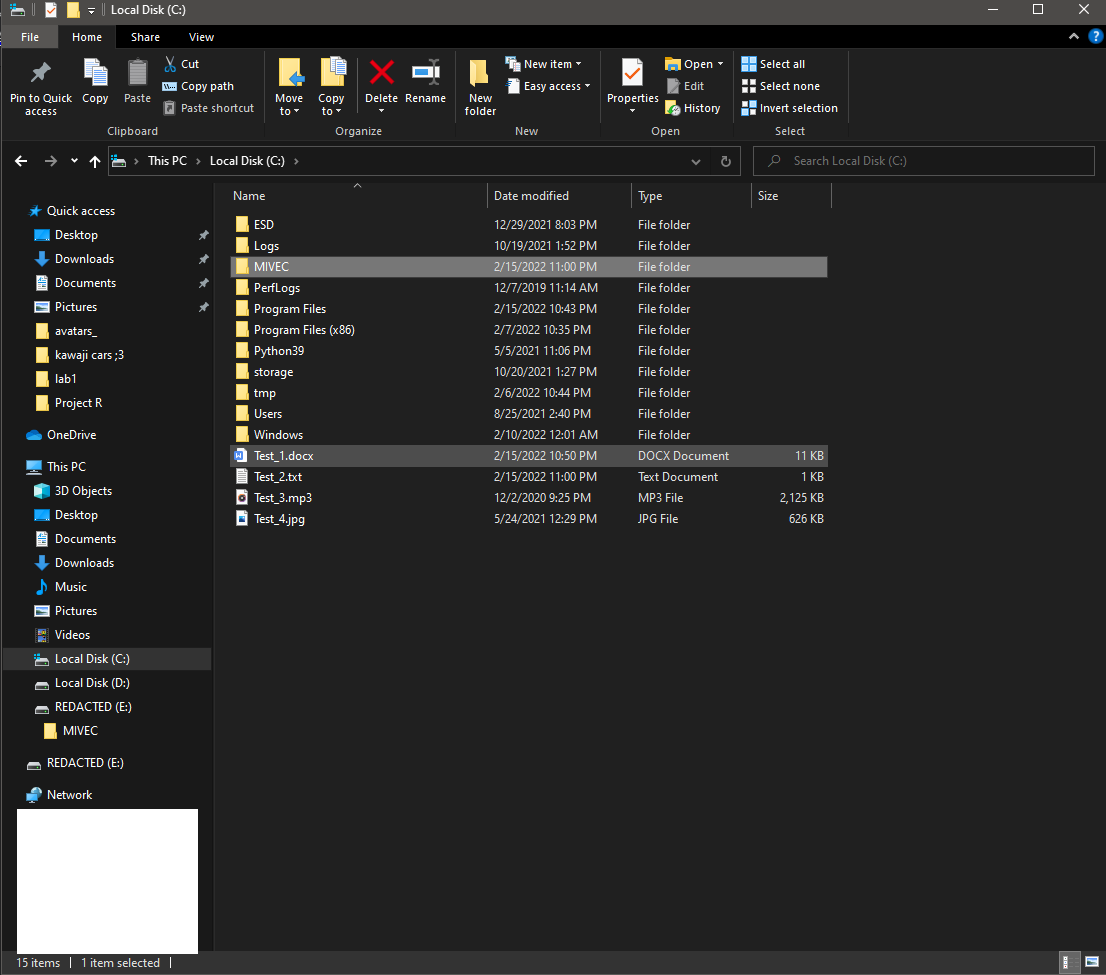


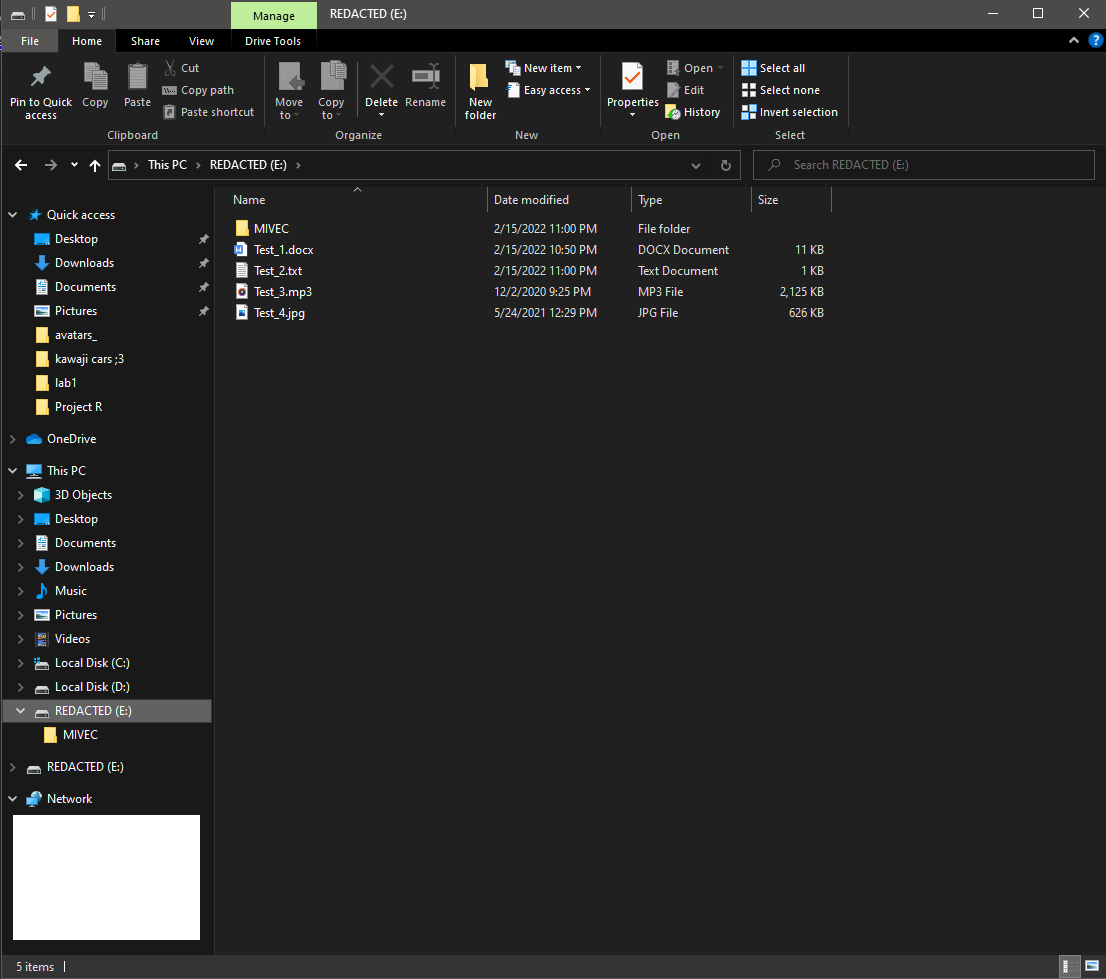
1. **Рішення**

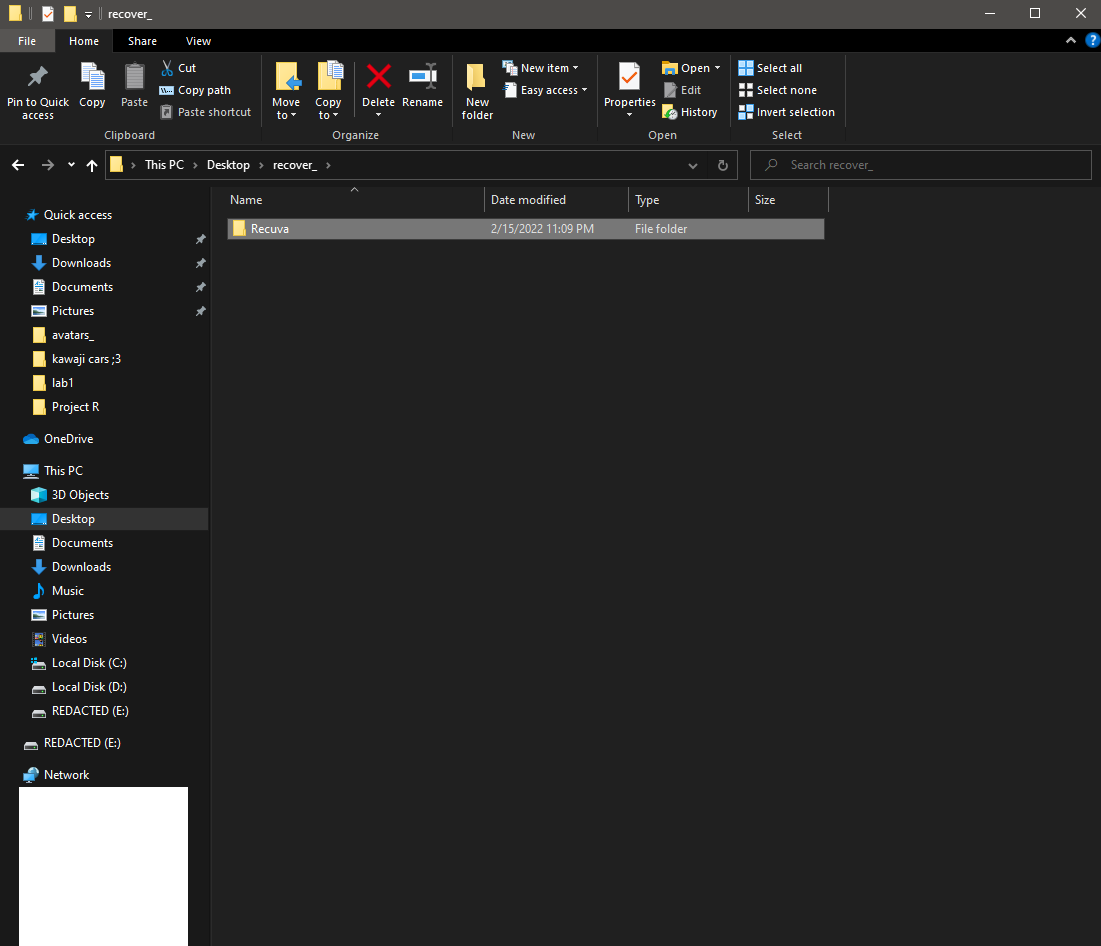


Створюємо потрібні файли

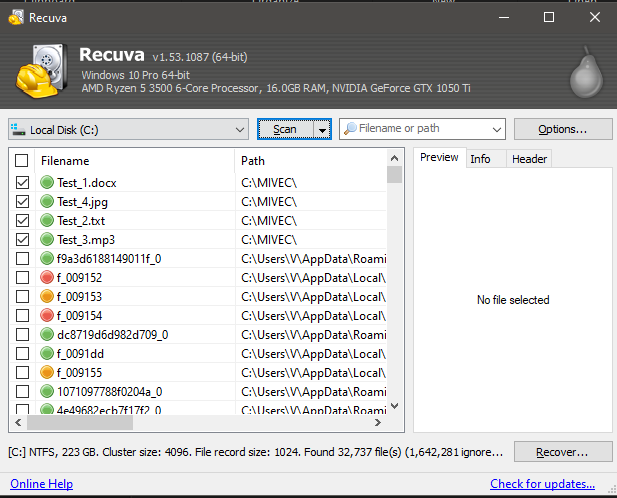
Копіюємо їх у корень диску С:/

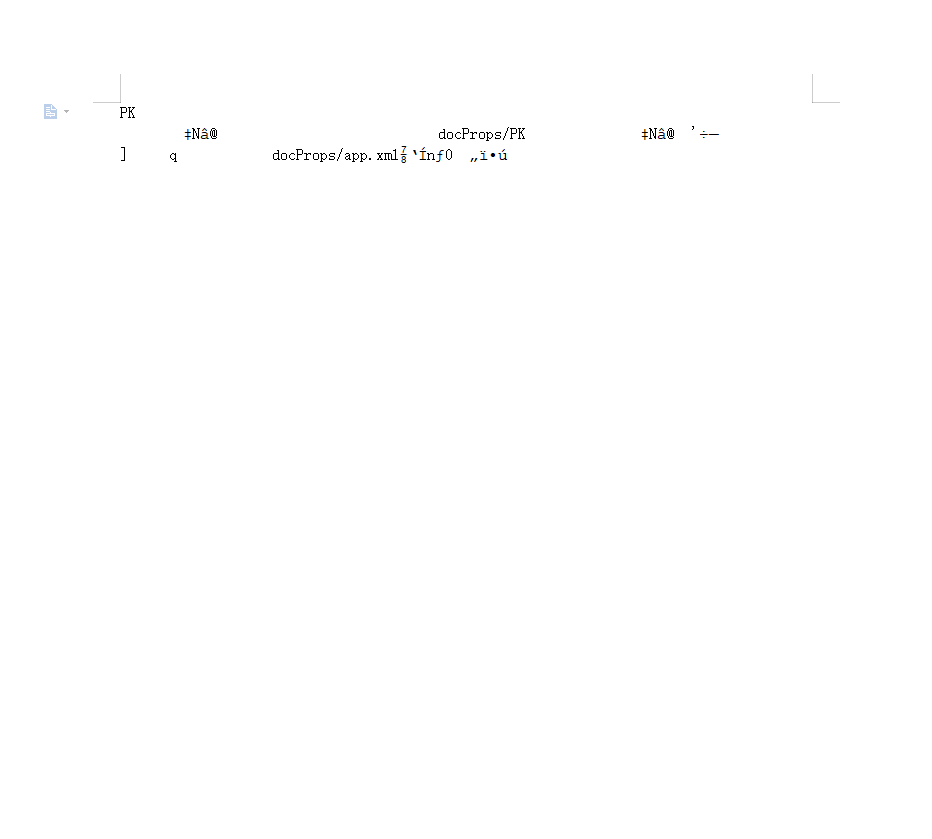


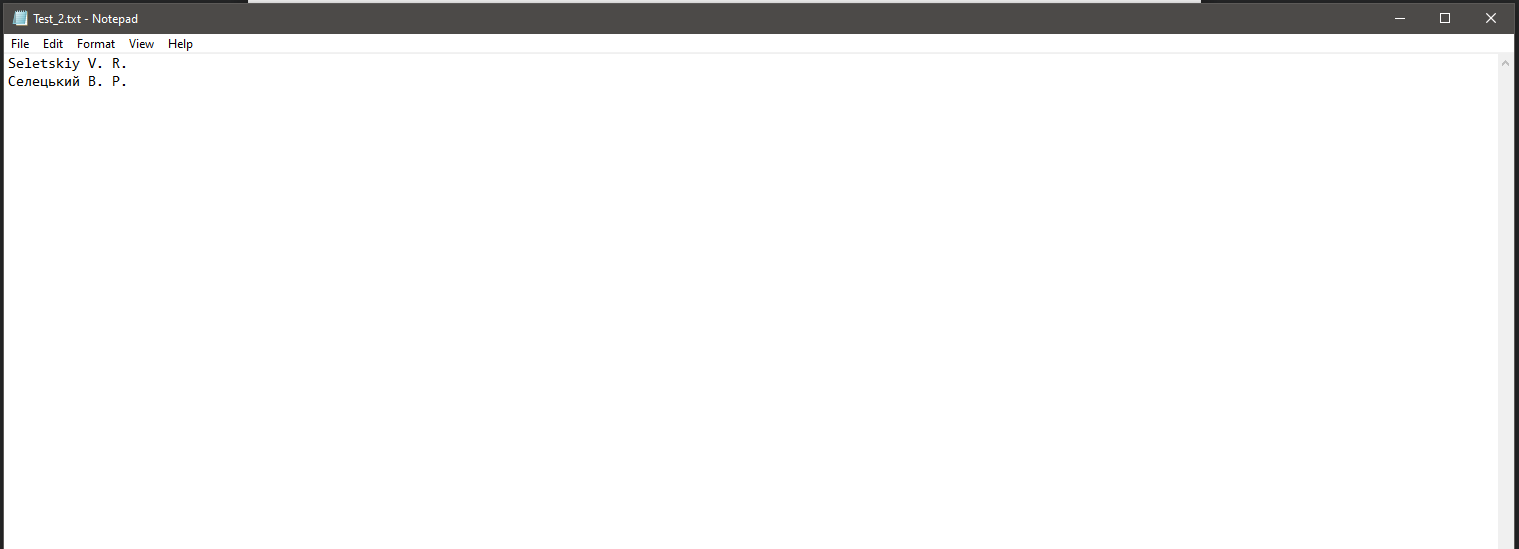
Копіюємо папку та файли в корінь флеш-накопичувача

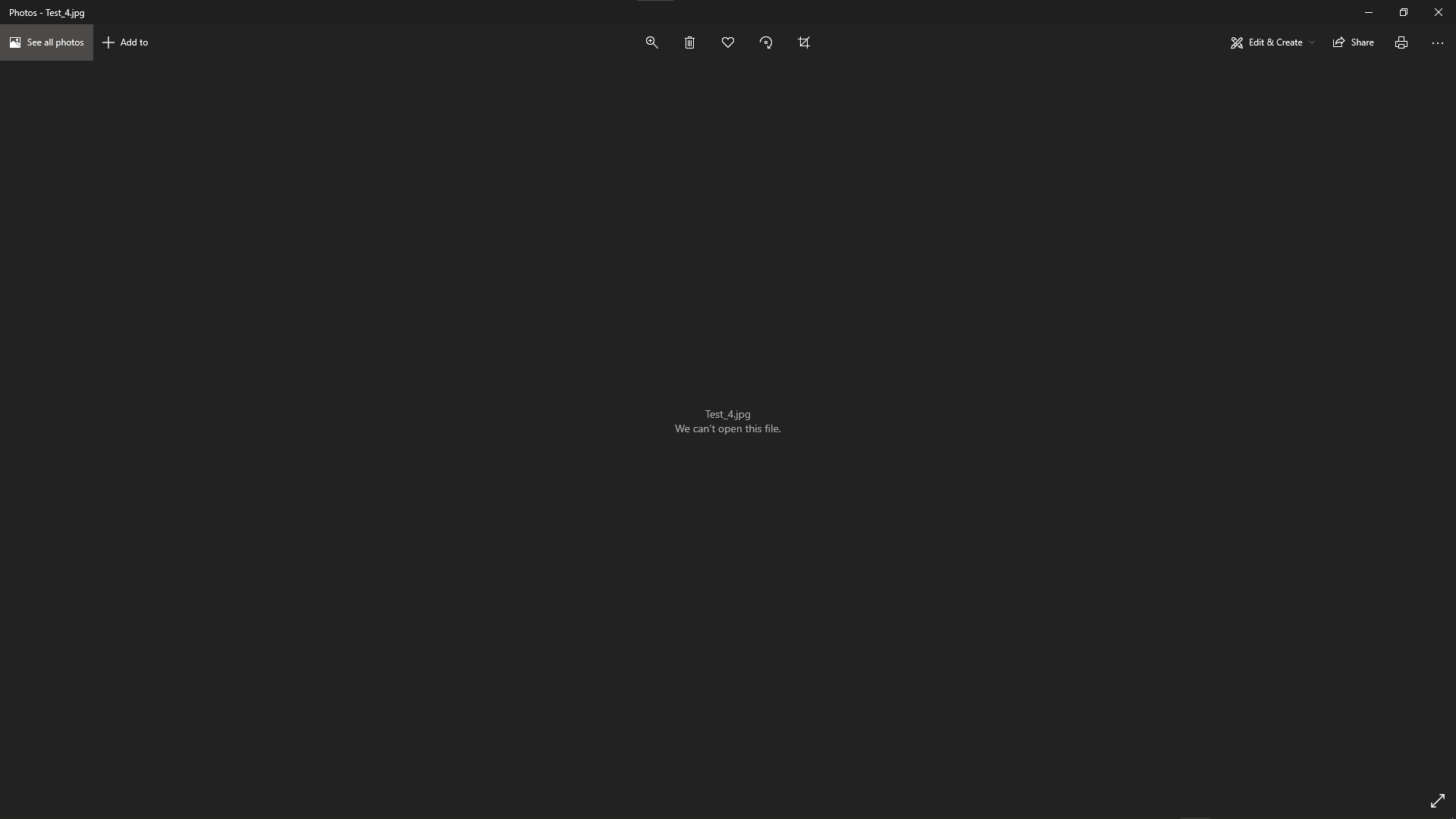


Створюємо папку на робочому столі, видаляємо файли та запускаємо програму:

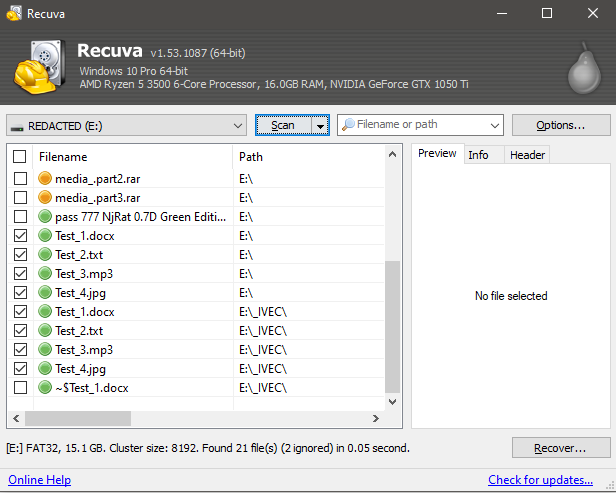


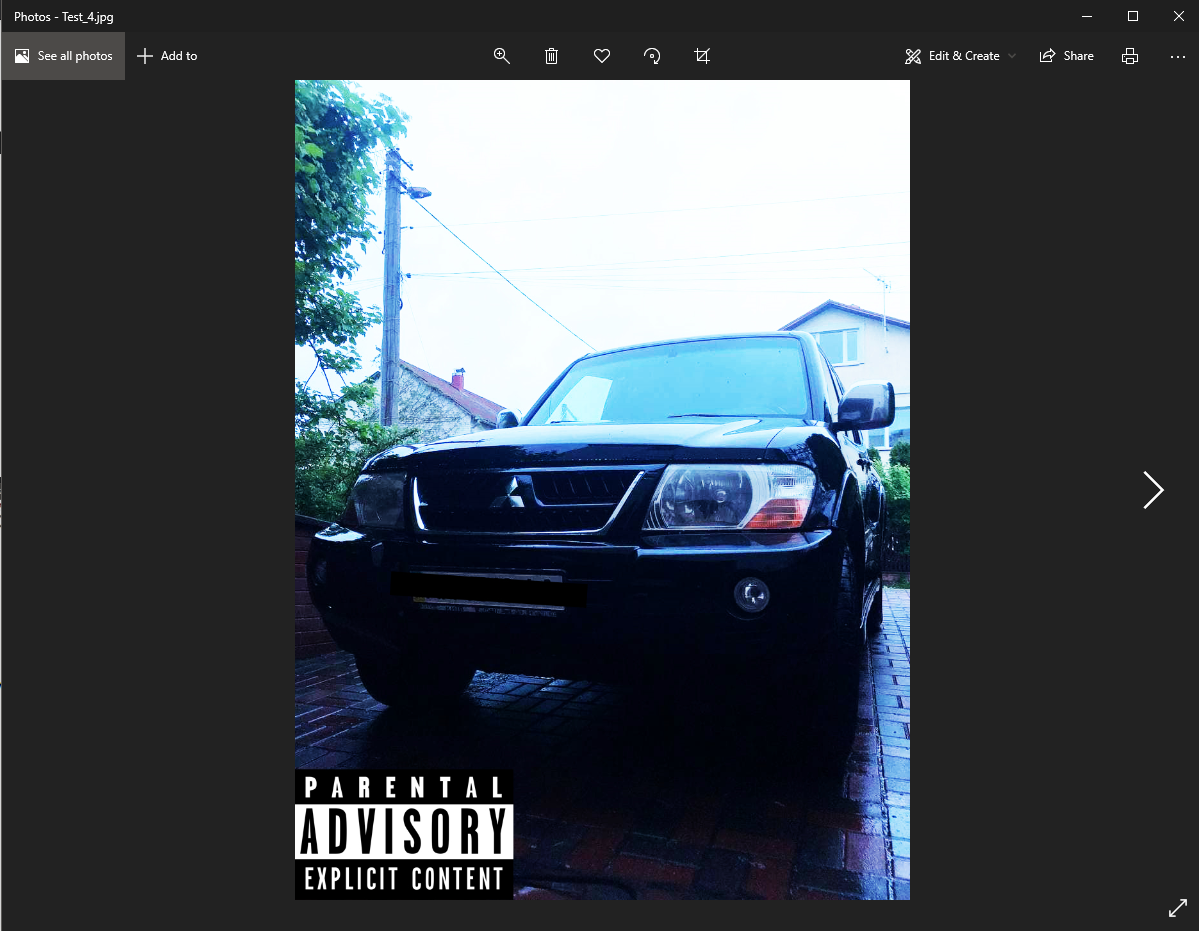
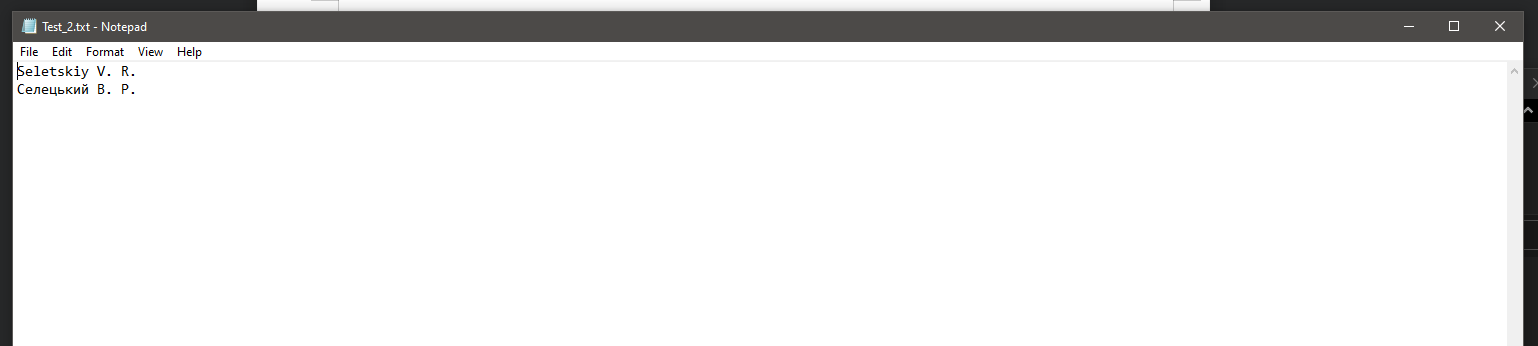


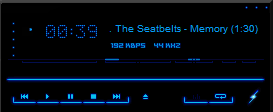




Результати для диску С:/. Аудіфайл відновлено лише частково: відтворюються перші дві секунди.







Результати для флеш-накопичувача

Як можна побачити, повністю відновились лише файли, що були записані на флеш-накопичувач. Це може бути пов’язано з тим, що папка, в яку було відновлено вміст папки в корені диску С:/, знаходиться на тому самому фізичному диску, що зменшує шанси на повне відновлення файлів.

**Контрольні запитання:**

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

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.

Кожна із зазначених системних областей є надзвичайно важливою для

нормального функціонування файлової системи і забезпечення безперешкодного доступу до файлів на логічному диску і їх руйнування робить цей доступ неможливим.

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

Тому що він виключно важливий для функціонування системи.

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

Число в абревіатурі вказує розмір елемента таблиці в бітах.

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

номера кластера?

Максимальний обсяг простору на диску має становити приблизно 8 терабайт з урахуванням таких змінних: Максимально можлива кількість кластерів на томі FAT32 становить 268 435 445, при цьому максимально допустимий розмір кластера становить 32 КБ разом із простором, який потрібен для таблиці розміщення файлів (FAT).

1. Де зберігається інформація про основні характеристики файлу?

В атрибуті $STANDARD\_INFORMATION

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

1. При запиті на дію з певним файлом відбувається звернення до його

запису в області ROOT, звідки зчитується номер початкового кластера даного

файлу.

2. В області FAT зчитується вміст запису, що відповідає номеру

початкового кластера цього файлу.

3. Якщо вміст не дорівнює коду EOF, то це означає, що файл не

завершується в даному кластері, а має продовження. Тоді з цього кластера

зчитуємо номер наступного кластера, і таким чином, йдемо по всьому ланцюжку, поки не буде виявлений код EOF.

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

неспроможність файлової системи розмістити пов'язані дані послідовно (неперервно)

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

Вільний - 00, дефектний - F7, останній - FF.

1. Які перетворення в системних областях відбуваються при видаленні файлу в FAT?

1. У відповідному файлу записі в області ROOT в поле імені файлу

NAME перший символ імені замінюється на код «Е5». В результаті цього файл

стає невидимий і недоступний засобами файл–менеджерів (Windows–Explorer,

FAR, Windows Commander і ін.). При цьому сам запис для даного файлу

зберігається в інших полях без змін.

2. Всі записи, відповідні кластерам файлу, що видаляються в області

FAT, заповнюються нулями, тобто ці кластери тепер розглядаються як вільні, і в

них може бути записана інформація будь–якого іншого файлу.

1. Чим відрізняється $MFTMirror від $MFT?

$MFT Mirror містить бекап перших чотирьох системних файлів NTFS:

$MFT, $MFT Mirror, $Log, $Volume

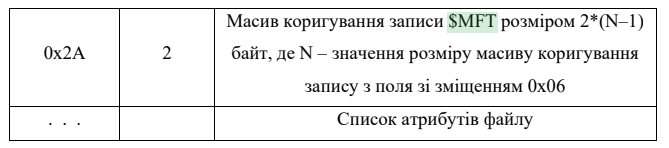
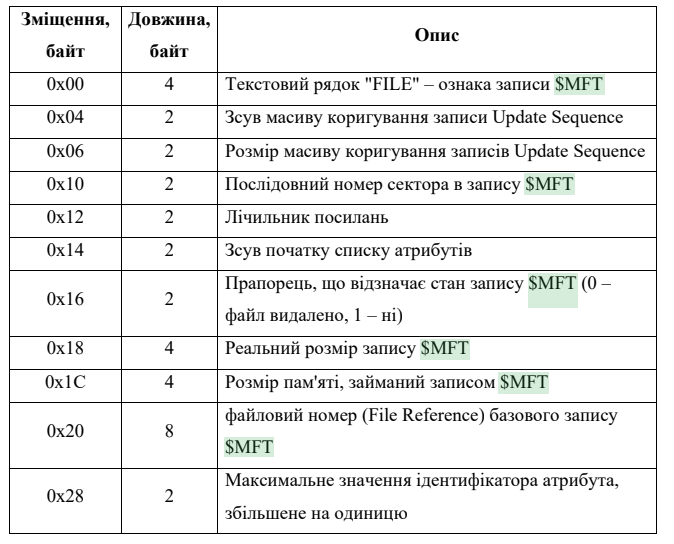
1. Де зберігається інформація про розташування $MFT і $MFTMirror на логічному диску?

В BootSector

1. Який обсяг запису в $MFT?

Зазвичай це 1кб

1. Які характерні ознаки має запис $MFT?

Запис має наступну структуру: 

1. Що називають атрибутом файлу в записі $MFT?

Заголовок та область змінної довжини запису.

15. Які перетворення в системних областях відбуваються при видаленні файлу в NTFS?

1. Коригується файл /$MFT: $BITMAP, кожний біт якого визначає

"зайнятість" відповідного файлового запису в MFT ( "0" – запис не

використовується);

2. Коригується файл /$BITMAP, кожний біт якого визначає

"зайнятість" відповідного кластера ( "0" – кластер не використовується);

3. У записі в MFT, що відповідає даному файлу, ставиться відмітка, що

файл видалений (поле FLAG, що перебуває по зсуві 16h від початку запису,

скидається в нуль);

1. Посилання на файл видаляється з двійкового дерева індексів;

5. Оновлюється атрибут $STANDART\_INFORMATION каталогу, який

зберігав видалний файл (коригується час останнього доступу і т.д.);

1. В /$LogFile оновлюється Sequence Number;

7. Update Sequence Number наступних файлових записів збільшується

на одиницю – сам файл, що видаляється, поточний каталог, /$MFT, /$MFT:

$BITMAP, /$BITMAP, /$BOOT, /$TRACKING.LOG.

1. З якої причини відновлення файлу не завжди можливо?

Сильна фрагментованість файлу, стертий запис в MFT, пошкодження диску, час після видалення.

**Висновки**

В результаті виконання даної лабораторної роботи я оволодів практичними навичками використання файлової системи Windows, користувався програмою Recuva. Налаштував відновлення файлів та папки з кореню диску C:/, з кореню флеш-накопичувача, скориставшись програмою для відновлення втрачених файлів Recuva. Отримав незадовільний результат при відновленні файлів з диску C:/, задовільний - при відновленні файлів з флеш-накопичувача. Вважаю дану лабораторну роботу виконаною в повному обсязі.