

Методичні вказівки  
до лабораторної роботи №1  
**«Програмне відновлення вилучених файлів»**  
з навчальної дисципліни вільного вибору  
**«Основи інформаційної та кібербезпеки»**

**Зміст практичного заняття:** Ознайомлення зі зберіганням і видаленням файлів у файлових системах FAT та NTFS операційних систем сімейства MS Windows, а також отримання навичок по відновленню видалених файлів програмним способом.

### **Загальні відомості**

При наведенні порядку серед файлів на комп'ютері можна випадково видалити "назавжди" важливий документ, фотографію або відео. Надійність файлової системи – це одне, а помилково вилучені файли – зовсім інше. Файлова система, навіть така потужна як NTFS, безсила захистити користувача від себе самого. Добре, якщо видалений файл зберігся в "Кошику". Якщо користувач натискає комбінацію shift + delete і після розуміє, що цей файл не потрібно було видаляти. Що робити? Головне – не панікувати. В цьому випадку залишається лише спробувати відновити видалений файл з файлової системи вручну або за допомогою спеціалізованих програм.

### **1. Зберігання та видалення файлів в файловій системі FAT**

У файловій системі FAT (File Allocation Table – таблиці розміщення файлів) суміжні сектори диска об'єднуються в структури, які називаються кластерами. Для зберігання даних файлу відводиться ціла кількість кластерів (мінімум один), так що, наприклад, якщо розмір файлу складає 40 байт, а розмір кластера 4 кбайт, реально зайнятий інформацією файлу буде лише 1% відведеного для нього місця. Для уникнення подібних ситуацій доцільно зменшувати розмір кластерів, а для скорочення обсягу адресної інформації і підвищення швидкості файлових операцій – навпаки.

Простір тому FAT32 логічно розділений на три суміжні області:

- зарезервована область. Містить службові структури, які належать завантажувального запису розділу і використовуються при ініціалізації тому;
- область таблиці FAT, що містить масив індексних вказівників («комірок»), що відповідають кластерам області даних. Зазвичай на диску представлено дві копії таблиці FAT з метою підвищення надійності зберігання інформації;
- область даних, де записано власне вміст файлів – тобто текст текстових файлів, кодоване зображення для файлів малюнків, оцифрований звук для аудіофайлів і т.д. – а також т.зв. метадані – інформація щодо імен файлів і папок, їх атрибутів, часу створення і зміни, розмірів і розміщення на диску.

Якщо кластер належить файлу, то відповідна комірка містить номер наступного кластера цього ж файлу. Якщо комірка відповідає останньому кластеру файлу, то вона містить спеціальне значення (FFFF<sub>16</sub> для FAT16). Таким чином вибудовується ланцюжок кластерів файлу. Невживаним кластерам в таблиці відповідають нулі. «Поганим» кластерам (які виключаються з обробки, наприклад, з причини нечитабельності відповідної області пристрою) також відповідає спеціальний код.

При видаленні файлу перший символ імені замінюється спеціальним кодом E5<sub>16</sub> і ланцюжок кластерів файлу в таблиці розміщення обнулюється. Оскільки інформація про розмір файлу (яка розташовується в каталозі поруч з ім'ям файлу) при цьому залишається недоторканою, в разі, якщо кластери файлу не були перезаписані новою інформацією, можливе відновлення видаленого файлу.

## **2. Зберігання та видалення файлів в файловій системі NTFS**

В процесі видалення файлу з NTFS (New Technology File System — «файлова система нової технології»)-розділу відбувається таке:

- коригується файл /\$MFT:\$BITMAP, кожний біт якого визначає "зайнятість" відповідного файлового запису (FILE Record);
- коригується файл /\$BITMAP, кожний біт якого визначає "зайнятість" відповідного кластера ("0" - кластер не використовується);
- файлові записи, що відповідають файлу, позначаються як видалені;
- посилання на файл видаляється з двійкового дерева індексів;
- оновлюється атрибут \$STANDARD\_INFORMATION каталогу, який зберігав файл (час останнього доступу і т.д.) тощо.

Каталоги видаляються практично точно так же, як і файли (з точки зору файлової системи каталог – той же файл, тільки особливий – з двійковим деревом індексів усередині).

Ні в тому, ні в іншому випадку фізичного видалення файлу не відбувається і він може бути легко відновлений до тих пір, поки не буде затертий FILE Record, що зберігає резидентне тіло файлу або список відрізків (run-list) нерезидентного вмісту. Втрата FILE Record дуже неприємна, оскільки в цьому випадку файл доведеться збирати по шматочках руками і чим сильніше він фрагментований, тим складніше це завдання. На відміну від FAT, NTFS не затирає перший символ ім'ям файлу, чим значно спрощує своє відновлення.

### 3. Відновлення видалених файлів

Якщо запис в сектори, що містять файли не проводився, то дані фізично залишилися на своїх місцях, але загубилися або спотворилися відомості про їх розташування. Таким чином, потрібно визначити, де саме знаходяться сектори, що містять потрібну інформацію, і відновити їх у правильній послідовності.

У разі, коли проводився запис на диск, наприклад, форматування з подальшою установкою операційної системи, ймовірність фізичного знищення потрібної інформації може бути досить велика. У подібних ситуаціях можливість успішного відновлення даних залежить від везіння і співвідношення обсягів втраченої і записаної інформації.

Також варто взяти до уваги, що при втраті даних через помилки у файловій системі, запуск програм типу ScanDisk істотно зменшує ймовірність успішного відновлення. Основне завдання цих утиліт – впорядкування службових структур файлової системи, що вони і роблять, не особливо дбаючи про долю призначених для користувача даних. При цьому знищуються «сліди», за якими можна було б реконструювати структуру файлової системи до пошкодження і врятувати дані.

У загальному випадку, програма для відновлення даних спочатку сканує всі носії. За результатами сканування, на основі виявлених службових записів, складається карта розташування фрагментів відновлюваних файлів і будується дерево каталогів. У карті містяться відомості про те, який кластер до якого файлу відноситься, розміри, назви та інші атрибути елементів файлової системи – все, що вдалося дізнатися на підставі залишків службової інформації. Якщо отриманих в результаті сканування відомостей мало, то використовуються певні методи екстраполяції. Потім файли і папки, які потрібно відновити, вибираються відповідно до складеної карти і переносяться на інший носій.

Найчастіше все, що в принципі можливо відновити зі справного носія інформації, дістається за допомогою спеціалізованих програм. І лише в меншій частині випадків, висококваліфікований фахівець, працюючи на більш фізичному низькому рівні, здатний відновити інформацію у більшому обсязі.

### 4. Програми для відновлення видалених файлів

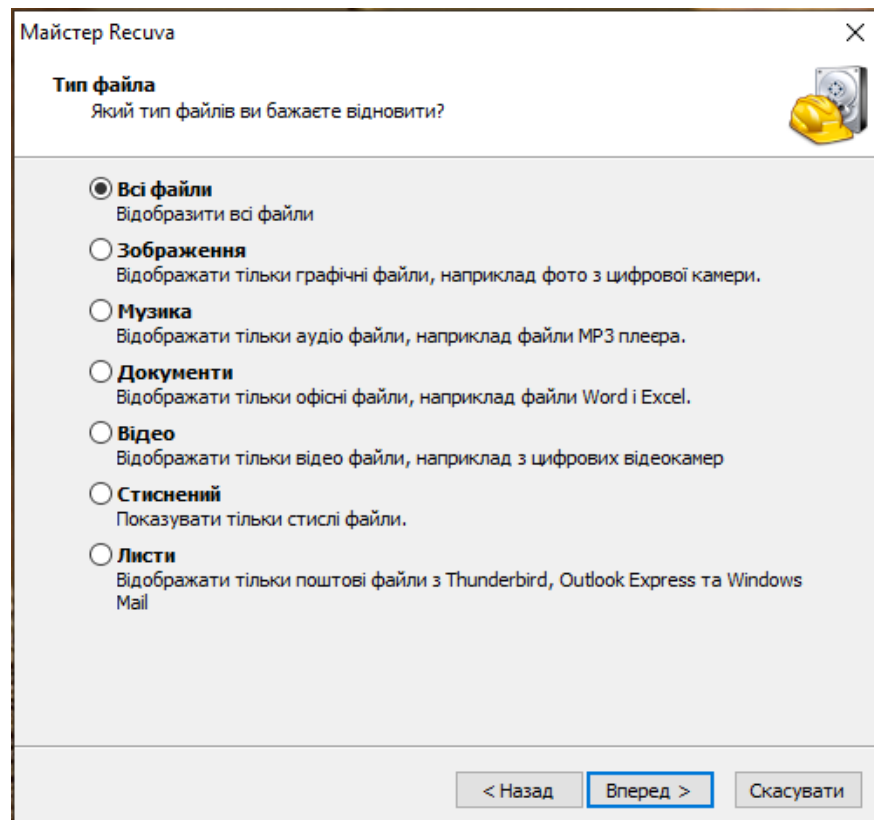
#### *Програма Rescuva*

**Rescuva** – одна з безкоштовних утиліт, розроблених компанією Piriform, відомої також такими програмними продуктами, як програма очищення системи **CCleaner**, засіб дефрагментації **Defragger**, і інструмент для відображення детальної системної інформації **Speccy**. Rescuva призначена для відновлення інформації після видалення файлів або каталогів, а також після швидкого або повного форматування розділів. Відмінними рисами даної програми, в порівнянні з аналогічними продуктами, є простота і зручність використання, а так само висока швидкість роботи. У сукупності з ефективністю відновлення, безкоштовністю, багатомовною підтримкою і зручним призначенням для користувача інтерфейсом, ці якості програми вивели її в лідери серед програмних засобів відновлення даних для домашніх користувачів.

Завантажити програму **Recuva** можна на сторінці завантаження з офіційного сайту <https://www.ccleaner.com/recuva>.

У програмі передбачена можливість використання спеціального майстра, за допомогою якого можна знайти і відновити вилучені файли, відповівши лише на кілька простих запитань. Користувач може відмовитися від використання майстра, натиснувши кнопку **Скасування**. При необхідності, можна взагалі відключити режим запуску майстра, встановивши відповідну позначку.

На наступному кроці необхідно визначити тип файлів, пошук і відновлення яких буде виконуватися програмою:



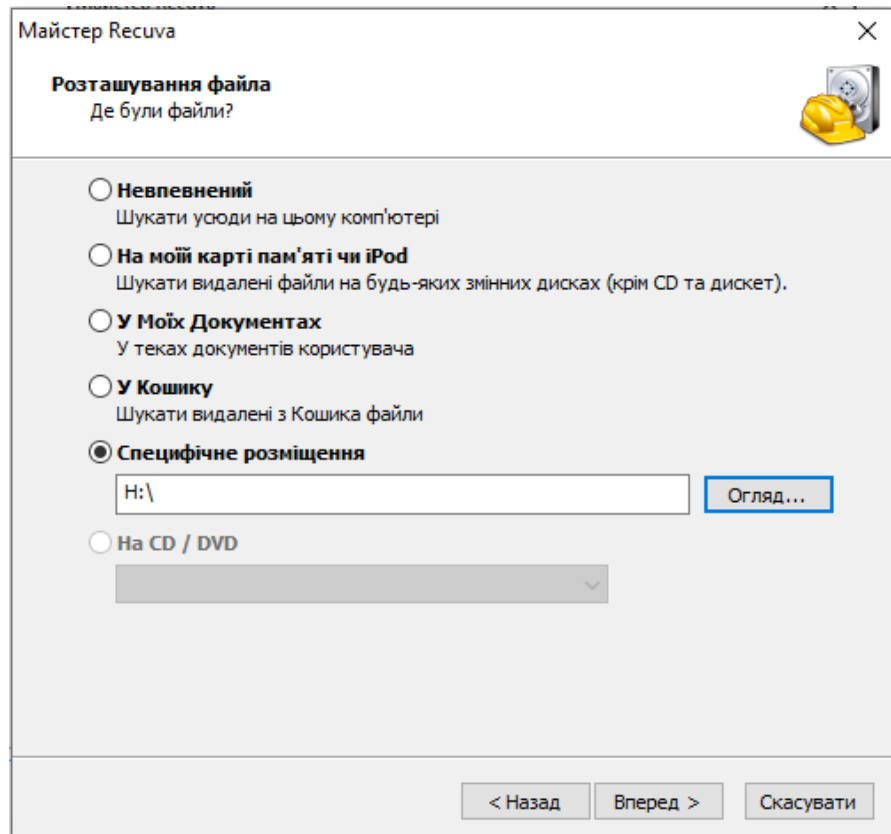
Майстер Recuva

**Тип файла**  
Який тип файлів ви бажаєте відновити?

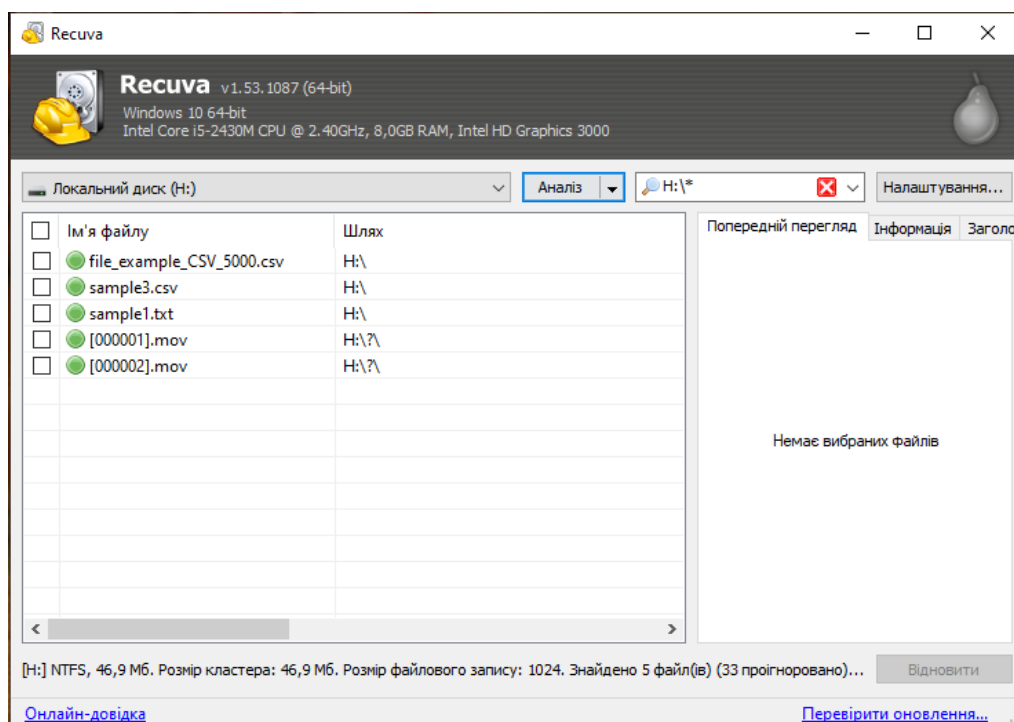
- ☒ **Всі файли**  
Відобразити всі файли
- ☐ **Зображення**  
Відображати тільки графічні файли, наприклад фото з цифрової камери.
- ☐ **Музика**  
Відображати тільки аудіо файли, наприклад файли MP3 плеєра.
- ☐ **Документи**  
Відображати тільки офісні файли, наприклад файли Word і Excel.
- ☐ **Відео**  
Відображати тільки відео файли, наприклад з цифрових відеоканер
- ☐ **Стиснений**  
Показувати тільки стислі файли.
- ☐ **Листи**  
Відображати тільки поштові файли з Thunderbird, Outlook Express та Windows Mail

< Назад    Вперед >    Скасувати

Потім визначається область пошуку файлів для відновлення:

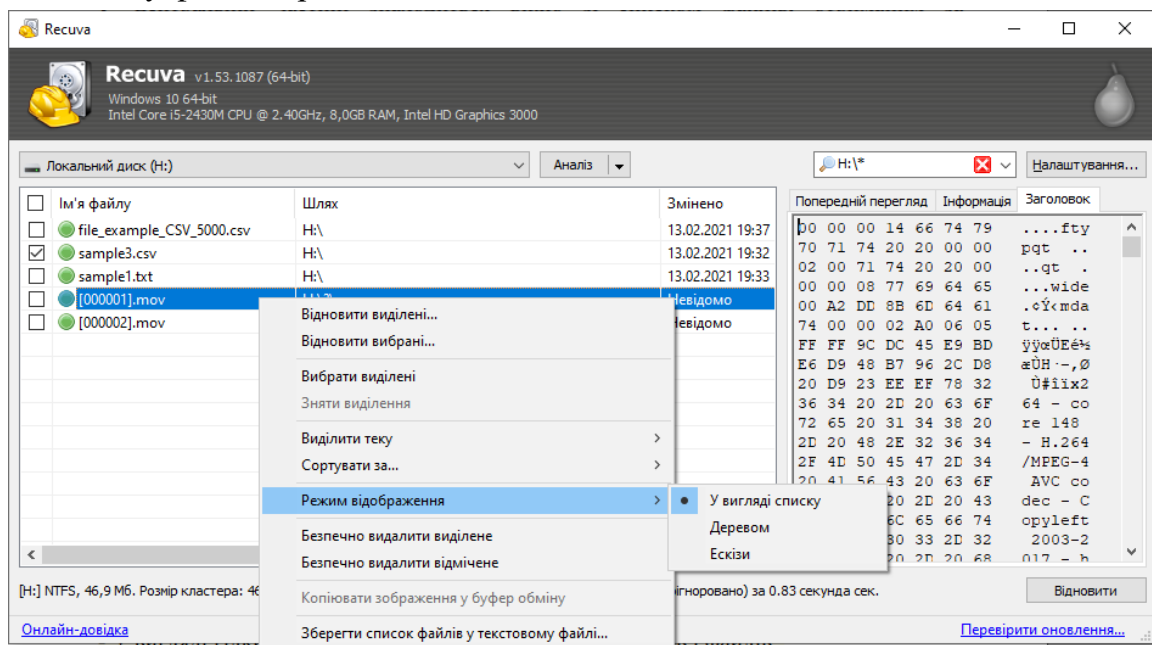


На наступному кроці програма виконує пошук і аналіз вмісту видалених файлів:



Вікно програми розділене на кілька частин. Зліва, у верхній частині, розташоване меню вибору дискових пристроїв, для яких буде виконуватися відновлення даних і кнопка **Аналіз** для запуску процесу сканування і аналізу даних. У правій частині розміщена панель пошуку і фільтрації файлів і кнопка **Налаштування**, в допомогу якої можна налаштувати деякі параметри Rescuva.

Праворуч - інформаційне вікно і кнопки для виконання дій над обраним файлом (**Попередній перегляд**, **Інформація**, **Заголовок** – початкова частина файлу в 16-му форматі). У нижній частині вікна відображається інформація про результати сканування і кнопка **Відновити** для запуску процесу відновлення вибраних файлів. Змінити режим показу можна за допомогою контекстного меню, що викликається в області списку файлів правою кнопкою мишки:



Користувачеві досить відзначити потрібні файли і натиснути кнопку **Відновити** в правій нижній частині вікна програми. Після чого потрібно вибрати папку для відновлених файлів і дочекатися закінчення процесу відновлення.

Можливість успішного відновлення видалених файлів визначається їх станом, що відображається в колонці **Стан**:

*Відмінний* – файл був видалений, але кластери, в яких знаходилися його дані, які не перезаписані новими файлами, запис яких виконувалася на даний диск після видалення. Такі файли відновлюються повністю, без будь-якої втрати даних.

*Втрачено* – файл повністю або частково був перезаписаний іншим файлом і його повне відновлення неможливо. Для таких файлів можна застосувати відновлення з подальшою оцінкою результату в ручному режимі. Так, наприклад, незначний перезапис частини відеофайлу може залишити поза увагою його формат і зробити його прийнятним для перегляду. Певною мірою про ймовірність відновлення можна судити по кількості і розміщенні перезаписаних кластерів обраного файлу, що відображається при натисканні на закладку **Інформація**.

Для відбору файлів зі списку зручно використовувати фільтр, розміщений у верхній правій частині вікна програми. Є можливість вибору типу файлу зі списку (**Графіка**, **Музика** ...) Або задати шаблон імені вручну, наприклад:

\*.jpg- всі файли з розширенням .jpg

IMG\*.jpg - всі файли з розширенням .jpg , імена яких починаються з IMG

\*2020.\* - всі файли, імена яких закінчуються рядком 2020

\*2020\*.\* - усі файли, в імені яких міститься 2020

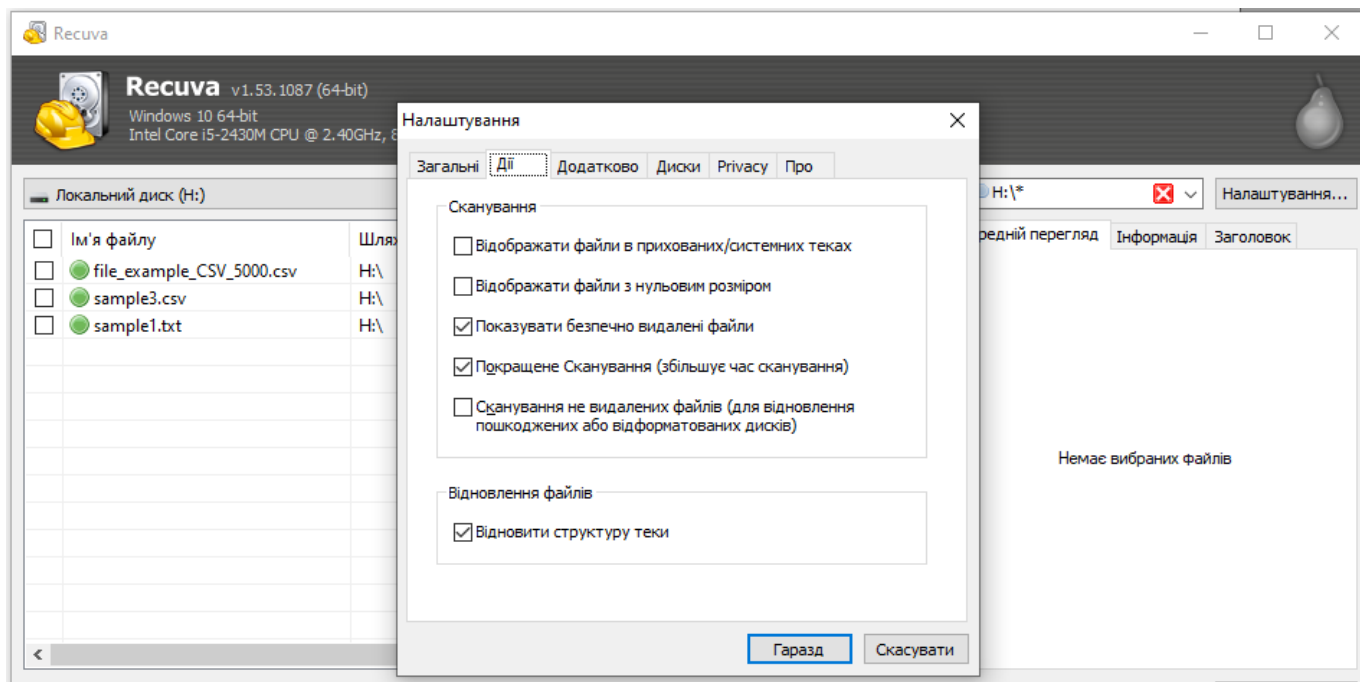
## ***Використання тіньових копій томів для відновлення файлів за допомогою Resuva***

Важливою особливістю Resuva є можливість роботи з тіньовими копіями томів, які автоматично створюються службою тіньового копіювання Windows з певною періодичністю. Для відображення тіньових копій, потрібно увімкнути даний режим - **Налаштування ... - Диски - встановити прапорець Показувати тіньові копії**. Тіньова копія являє собою знімок (snapshot, снапшот) файлової системи, створений на певний момент часу. Знімки автоматично створюються в фоновому режимі, без будь-яких дій з боку користувача і непомітно для нього. В операційних системах Windows з настройками за замовчуванням, зберігається кілька тіньових копій системного диска. Дані тіньових копій зберігаються в захищеному системному каталозі C: \ System Volume Information \ (для диску C :) і являють собою файли, в іменах яких міститься ідентифікатор GUID: {3808876b-c176-4e48-b7ae-04046e6cc752}

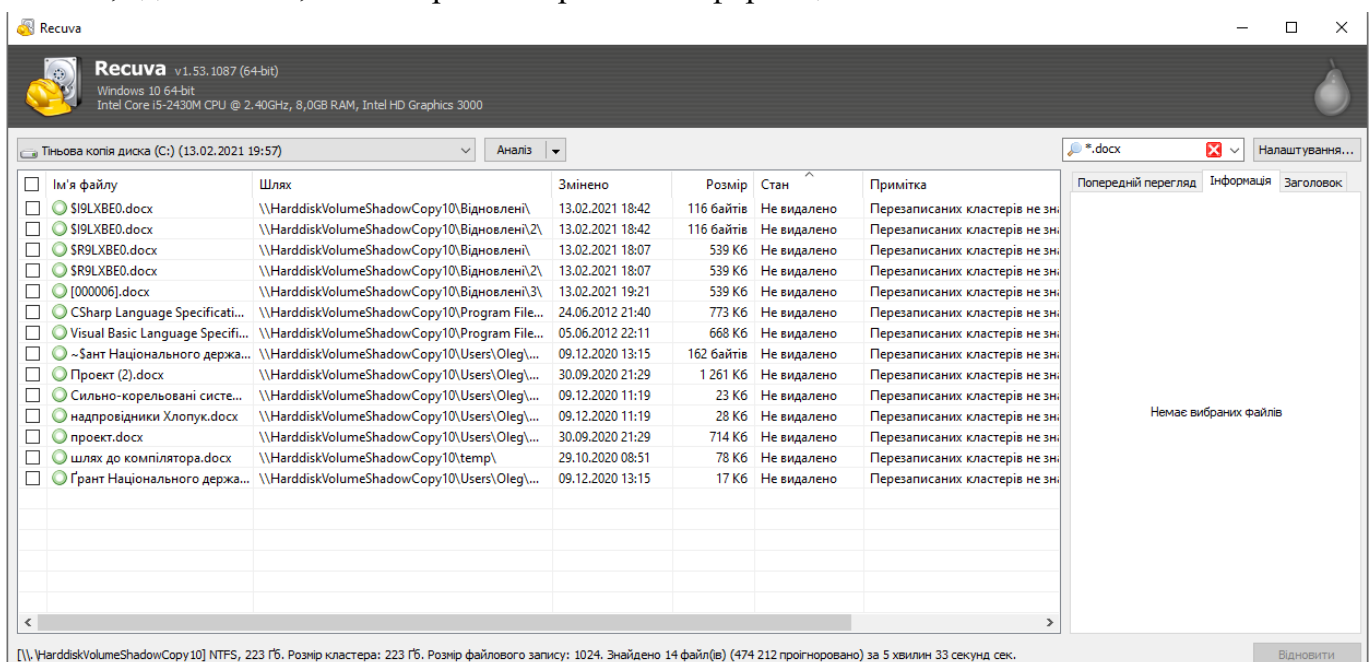
З використанням тіньових копій томів, в операційних системах Windows, реалізується проста і ефективна технологія відновлення попереднього вмісту файлів. Нерідко дана технологія дозволяє уникнути неприємностей, наприклад, якщо ви відредагували великий і складний документ, і раптом виявилось, що потрібно повернутися до його початкового стану, яке вручну відновити дуже важко або навіть неможливо. Повернення до попередньої версії файлу може врятувати ситуацію. Недоліком використання стандартних засобів системи для роботи з попередніми версіями файлів, є неможливість попереднього перегляду і вибору конкретного покоління попередньої версії файлу для відновлення. Крім того, повернення до попередньої копії знищує інформацію, відповідну поточному стану файлу.

Всі ці недоліки ліквідуються при використанні в режимі роботи з тіньовими копіями томів. Наявність файлу в будь-якій з тіньових копій, а також його вміст легко перевіряється за допомогою Resuva і копіюється в зручне, для зберігання, місце файлової системи. Єдиною перешкодою для витягання файлів і каталогів з тіньових копій томів, є їх відсутність, в тих випадках, коли використовуються змінні носії або логічні диски, для яких відключена функція спостереження за станом файлової системи з метою сумнівної економії дискового простору.

При роботі з тіньовими копіями необхідно вибрати для аналізу або **Всі тіньові копії**, або якусь конкретну копію зі списку дискових пристроїв. У Resuva тіньові копії відображаються таким же чином, як і реальні логічні диски. У налаштуваннях програми в закладці **Дії** повинен бути встановлений прапорець **Сканування не видалених даних** (відновлення з пошкодженого носія).



Після завершення аналізу, потрібно знайти файл для відновлення, який має стан **Не видалено**. Таким чином, ми будемо відновлювати **НЕ видалений файл**, а файл, збережений в знімку файлової системи. Тінювих копій, в залежності від версії Windows, розміру дискових томів, і системних налаштувань тінювого копіювання, може бути до 64 шт. І кожна з них може бути джерелом відновлення для утиліти Recuva, здавалося б, безповоротно втраченої інформації.



*Відновлення даних з тінювих копій, може бути єдиним способом вирішення проблеми, пов'язаної з втратою вмісту важливих файлів в результаті дій вірусів-шифрувальників, для яких не існує алгоритму дешифрування даних. Багато користувачів відновили більшу частину своїх даних, зашифрованих вірусом, використовуючи не дешифрацію, а можливості Recuva по відновленню файлів з миттєвих знімків файлової системи, що створюються службою тінювого копіювання Windows в автоматичному режимі.*



### ***Використання Resuva для копіювання системних файлів.***

Йдеться про файли, які неможливо скопіювати звичайним способом в середовищі операційної системи, таких як, наприклад, файли реєстру Windows. Це не зовсім стандартне використання утиліти Resuva, але даний прийом цілком можна застосувати в тих випадках, коли за допомогою Resuva відновлюються файли з тіньових копій томів. Для вирішення даного завдання можна використовувати будь-яку з існуючих тіньових копій, або створити нову, а потім витягти з неї необхідні дані за допомогою програми.

Тіньові копії створюються стандартним засобом Windows як автоматично, так і в ручному режимі, з використанням засобу створення контрольних точок відновлення для дисків з включеною захистом. Наприклад, в Windows 10 - **Параметри - Система - Про систему - Відомості про систему- Захист системи**. Або запустити від імені адміністратора додаток **systempropertiesprotection.exe**

Копійовані, таким чином, файли будуть повністю кондиційними, що забезпечується технологією створення точних копій Windows.

### ***Рекомендації по використанню утиліти Resuva***

- Не варто виконувати відновлення файлів на несправному обладнанні. Наприклад, коли неправильно визначається фізичний розмір носія даних. Це стосується не тільки використання Resuva, але і будь-якої іншої програми відновлення. Якщо ж потрібне відновлення файлів на носіях з пошкодженою логічною структурою, або з частково нечитабельними блоками, то потрібно включити режим відображення всіх файлів через **Налаштування ... - Дії - увімкнути режим Пошук не видалених даних ...**.

- Якщо у вас виникла необхідність відновлення видалених файлів, потрібно максимально виключити запис на диск. Чим менше виконаних операцій запису, тим вище ймовірність відновлення даних. Якщо дані на диску перезаписані, то їх не вдасться відновити жодною програмою і жодним з відомих методів. В ідеальному випадку, не використовуйте комп'ютер, на якому знаходилися втрачені файли. Зокрема, якщо потрібно відновити файл на системному диску, то потрібно зробити це якомога раніше, оскільки на нього записується інформація майже в постійному режимі. Не запускайте і не завершуйте ніякі програми, не користуйтеся інтернетом до тих пір, поки не відновите дані. По можливості навіть не вимикайте і не перезавантажуйте комп'ютер.

- У тих випадках, коли Resuva не може виявити шуканих файлів, слід використовувати поглиблений аналіз, включивши його через **Налаштування ... - Дії** поставити позначку **Глибокий аналіз** (збільшує час сканування).

- У тих випадках, коли зміст логічного диска пошкоджено настільки, що Resuva не знаходить розділи, не може визначити тип файлової системи і не виконує аналіз вмісту диска, відновлення даних все ж можливо, але з використанням інших програмних і апаратних засобів. Не виключено, що вам не потрібна Resuva, а

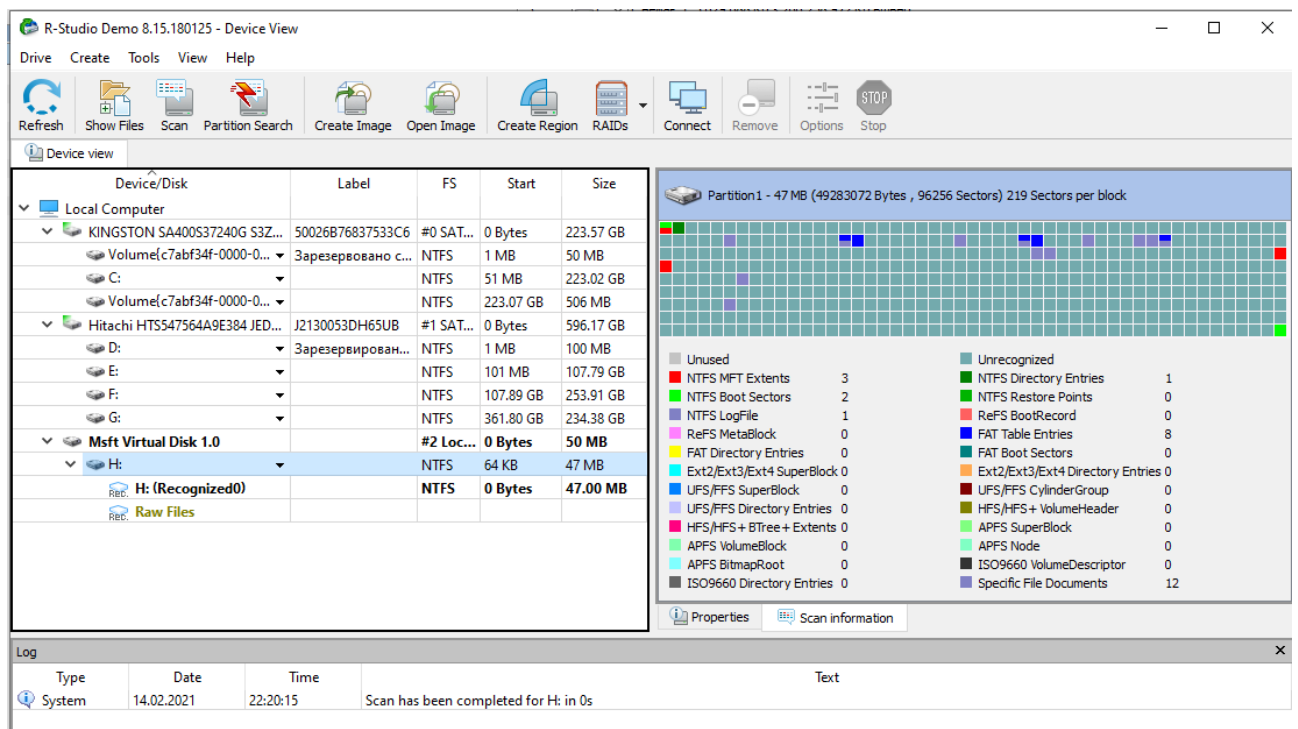
потрібна утиліта по відновленню видалених розділів жорсткого диска (безкоштовні EASEUS Partition Recovery і DM Disk Editor, платні продукти Acronis і т.п.). Якщо дані представляють певну цінність, то краще звернутися до фахівців з відновлення інформації. В крайньому випадку, на свій страх і ризик, можна спробувати таку методику:

- Створити посекторну копію пошкодженого носія даних, і в подальшому працювати тільки з нею, щоб мати повторні спроби відновлення.

- Спробувати створити розділ на носії з копією, і відформатувати його в той же тип файлової системи (NTFS, FAT32, exFAT ...), який використовувався до пошкодження носія. Якщо мова йде про карти пам'яті фотоапаратів, плеєрів, телефонів тощо, то краще за все виконати форматування вбудованими засобами пристрою. Якщо це зробити не вдається, то можна спробувати виконати цю операцію на комп'ютері, а потім - засобами пристрою.

## R-studio

R-STUDIO (умовно безкоштовна (пробна версія або ключ)) – це група надійних та ефективних утиліт для відновлення диску від компанії R-Tools Technology, Inc. Спершу ця програма була призначена для фахівців у сфері відновлення інформації, проте з часом R-Studio стала багатофункціональним, зручним і універсальним інструментом для відновлення даних. Поєднуючи передові технології відновлення файлів і диску зі зручним для користувача інтерфейсом, R-Studio дозволяє ефективно вирішувати задачі як компаніям і професіоналам, що займаються відновленням даних, так і початківцям.



Програма має дещо ширший функціонал в порівнянні з конкурентами: відновлює дані після форматування носія інформації, пошкодження або видалення

розділів, пошкодження секторів диска. Доступна функція створення образу диска і відновлення даних з нього.

На жаль, пробна версія має обмеження на розмір відновлюваного файлу (256 кБ), для більш широкого користування доведеться придбати платну версію.

### **Інші програми для відновлення даних**

FinalData Standard – швидка і ефективна програма, що вважається однією з кращих для відновлення видалених або пошкоджених даних.

Recover My Files – програма, що є потужним інструментом для відновлення видалених файлів на комп'ютері і портативних носіях.

Hetman Partition Recovery – це універсальна утиліта. Функціонал програми не обмежений відновленням якогось певного формату файлів або роботи з певним носієм інформації. Причина втрати файлу не має значення – алгоритми роботи інструменту дозволяють відновлювати файли в самих складних випадках.

Raise Data Recovery – має дуже зручний україномовний інтерфейс і працює практично з усіма поширеними файловими системами. Після відновлення зберігаються оригінальні імена файлів та структура каталогів. Дані можна витягти не лише із жорсткого диску, флешки, карти пам'яті чи мобільного пристрою, а й із дискового масиву (RAID) та мережевого сховища (NAS).

Ontrack EasyRecovery – програма, що дозволяє без особливих зусиль відновити дані після їх видалення з кошика, форматування диска або вірусного вторгнення.

Puran File Recovery розпізнає всі поширені системи та відновлює дані з вінчестерів, флешок, SSD карток та смартфонів із відтворенням оригінальних імен файлів та структури папок.

FreeUndelete сканує жорсткий диск для виявлення втрачених даних, при цьому можна встановити фільтр пошуку, вказавши ім'я і розширення файлу.

GetDataBack – програма для відновлення інформації, випадково або в результаті умисних дій видаленої з вашого комп'ютера.

R.saver – невелика, але потужна безкоштовна утиліта для відновлення даних із різних носіїв даних.

PC Inspector File Recovery – потужна утиліта яка з легкістю знайде і відновить втрачені з різних причин потрібні вам файли.

Unstoppable copier – потужна програма за допомогою якої можна відновлювати потрібні вам дані з пошкоджених носіїв.

Dead Disk Doctor – програма для відновлення файлів з частково пошкоджених оптичних дисків, дискет та інших носіїв інформації.

DiskInternals Uneraser – програма для відновлення файлів, загублених при очищенні Кошика, видаленні через командний рядок, після форматування і т.д.

Digital ObjectRescue Pro – програма для відновлення втрачених даних з цифрових фотокамер, MP3-плеєрів, диктофонів, цифрових камер, стільникових телефонів...

Search and Recover – це потужна програма, що дозволяє швидко і легко знайти на вашому комп'ютері втрачені, видалені, або пошкоджені дані.

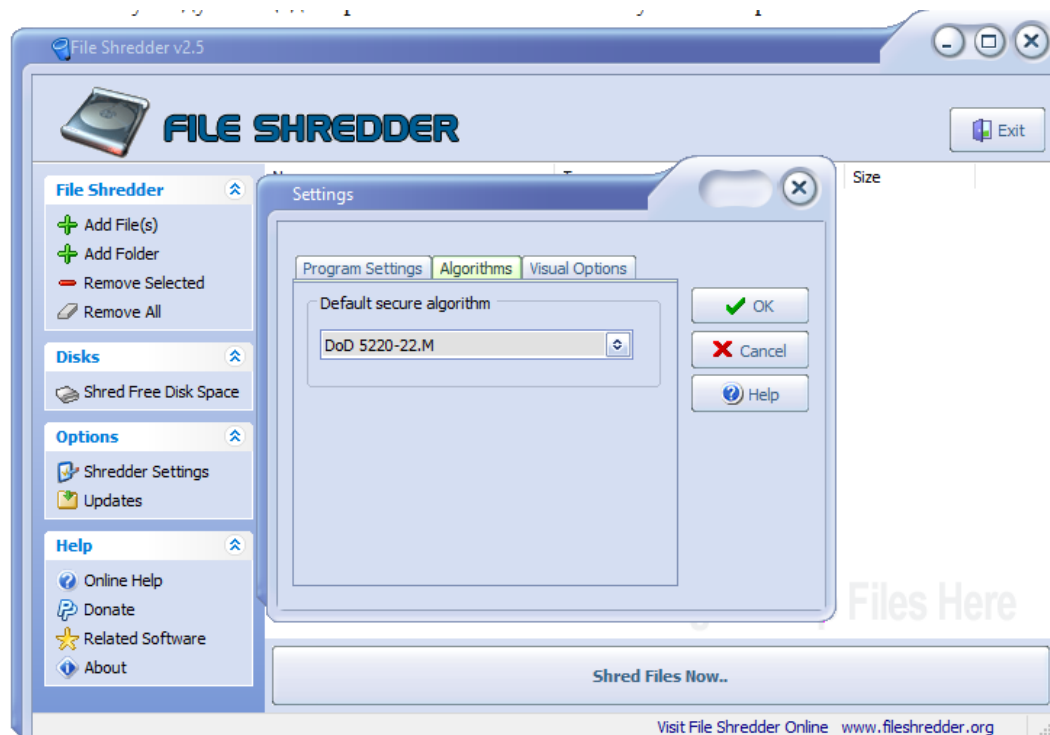
### Знищувачі інформації та програма File Shredder

Для безповоротного видалення даних є спеціальні програми – *файлові шредери*. Для тих, хто не знає, шредер це офісний пристрій, призначений для знищення паперових документів, шляхом розрізання їх на дрібні смужки. Принцип роботи файлового шредера заснований на тому, що інформація затирається іншими випадковими даними, записаними на них. Таким чином, стара інформація вже не підлягає відновленню. За допомогою файлового шредера слід видаляти дійсно важливу інформацію (файли), яка не повинна потрапити до рук сторонніх осіб.

Популярна безкоштовна програма Ccleaner має функцію затирання вільного місця на дисках, щоб не можна було відновити файли або повного безповоротного стирання всього вмісту дисків. Може бути виконано від 1 до 35 проходів за бажанням користувача.

Зараз існує безліч програм для безпечного видалення даних. Стільки ж існує і думок щодо ефективності тієї або іншої утиліти. В реальності ж твердження що одна програма-шредер видалляє дані краще, ніж інша це – не що інше, як міф. Видалляє інформацію не як така програма, а зашиті в неї алгоритми перезапису, а алгоритми у всіх цих утилітах використовуються одні й ті ж, просто в одній програмі може бути більш широкий набір алгоритмів, ніж в іншій. На думку фахівців, найбільш ефективним вважається алгоритм Пітера Гутмана, в якому використовується 35 циклів перезапису.

Однією з програм-шредерів є проста і зручна безкоштовна утиліта **File Shredder** (<https://www.fileshredder.org/>). Підтримується видалення даних з жорсткого диска, а також зі знімних носіїв.



Додавання файлів проводиться через головне меню, або прямим перетягуванням на робоче вікно програми. File Shredder можна використовувати і для затирання вільного дискового простору. Також є можливість видалення через контекстне меню Провідника. Програма має п'ять вбудованих методів видалення.

SSD – накопичувачі є більш новими, ніж жорсткі диски, і вони мають деякі унікальні властивості. Одна з них полягає в тому, що нові дані не замінюють старі, що робить старий метод видалення файлів марним. У них є функція *garbage collection*, яка періодично видаляє об'єкти, помічені як сміття. Більшість сучасних з них мають ще одну функцію – *TRIM*, яка дозволяє операційній системі повідомити диск, коли файл видаляється, і зазначає дані як непотрібні. Ці дві функції разом призводять до явища, яке називається випаровування даних. Випаровування даних описує здатність твердотільних накопичувачів назавжди видалити файл після того, як він буде видалений з файлової системи.

І це підводить до висновку про те, що файлові шредери не потрібні для SSD-накопичувачів, і насправді вони можуть пошкодити його за рахунок витрати обмеженого ресурсу кількості записів/перезаписів диска. Таким чином, при видаленні файлу на диску SSD, файл-шредер просто видаляє файл, а не перезаписує його.

## Завдання до лабораторної роботи

### Завдання А. Відновлення файлів засобами програми Recuva

1. Створюємо на жорсткому диску комп'ютера віртуальний диск розміром 50 Мбайт. Як створити віртуальний диск **див. Додаток 1**.
2. Створюємо дві вкладених одна в одну папки test\_прізвище у створеному віртуальному диску і записуємо в другу папку файли різних типів (мінімум 7 типів) – наприклад, презентація (ppt), 5 зображень – малого, середнього і великого розміру (jpg), таблицю ексель (xlsx), файл pdf, 5 файлів музики в mp3, 4 текстових файли різного формату і розміру (txt, doc, rtf), виконувані файли, відеофайли різних форматів.
3. Видалити файли у папках натисканням клавіш Shift + Delete (минаючи «Корзину») і спробувати їх відновити за допомогою Recuva.
4. Видалити файли разом з папками (Shift + Delete) і спробувати їх відновити за допомогою Recuva.
5. Відформатувати віртуальний диск (див. Додаток 1) і спробувати відновити файли за допомогою Recuva. **!Будьте обережними і випадково не відформатуйте якийсь інший диск з Вашими файлами.**
6. Видалити файли і записати в дані папки інші файли великого розміру. Спробувати відновити початкові файли за допомогою Recuva.
7. Видалити файли за допомогою програми File Shredder (<https://www.filesredder.org/>) в різних режимах і спробувати відновити.
8. У кожному з випадків 3-7 проведіть аналіз відновлених файлів на правильне відтворення їх вмісту і сформулюйте звіт за результатами виконаного завдання (зразок звіту додається).

Додаткові завдання (виконання не обов'язкове):

- виконати завдання А в іншій програмі на свій вибір (наприклад, R-studio) і порівняти отримані результати;
- навчитись відновлення попередніх версій не видалених файлів з тінювих копій.

**Завдання Б.** Напишіть програму, яка відновлює JPEG зображення з карти пам'яті.

### *Передісторія*

Уявимо себе в ролі хакера, який отримав доступ до карти пам'яті, яку необережно використовували. Карта пам'яті була використана фотоапаратом на яку були зроблені секретні фотографії, а потім вона була "обачливо" очищена (файли видалені). Ми отримали доступ до цієї карти пам'яті та зробили її цифровий відбиток замість вас. Цей відбиток являється лише послідовністю нулів та одиниць (байтів) що записані в один файл для зручності (RAW файл), він повністю відповідає стану цифрового носія після видалення файлів.

### *Теорія*

Незважаючи на те, що JPEG є більш складними, ніж BMP, JPEG мають "підписи", шаблони байтів, які можуть відрізнити їх від інших форматів файлів. Зокрема, перші три байти JPEG `0xff 0xd8 0xff` від першого байта до третього байта, зліва направо. Тим часом четвертий байт - це `0xe0, 0xe1, 0xe2, 0xe3, 0xe4, 0xe5, 0xe6, 0xe7, 0xe8, 0xe9, 0xea, 0xeb, 0xec, 0xed, 0xee` або `0xef`. Іншими словами, перші чотири біти четвертого байта - це `1110`.

Швидше за все, якщо ви знайдете цей шаблон із чотирьох байт на носіях, які, як відомо, зберігають фотографії (наприклад, на моїй карті пам'яті), вони визначають початок JPEG. Чесно кажучи, ви можете випадково зустріти ці закономірності на якомусь диску, тому відновлення даних не є точною наукою.

На щастя, цифрові камери, як правило, постійно зберігають фотографії на картах пам'яті, завдяки чому кожна фотографія зберігається відразу після зробленої раніше фотографії. Відповідно, початок JPEG зазвичай позначає кінець іншого. Однак цифрові камери часто ініціалізують картки файловою системою FAT, чий "розмір блоку" становить 512 байт (B). Наслідком є те, що ці камери записують на ці картки лише в одиницях 512 B. Фотографія розміром 1 МБ (тобто 1048 576 B), таким чином, займає  $1048576 \div 512 = 2048$  "блоків" на карті пам'яті. Але так само і фото, яке, скажімо, на один байт менше (тобто, 1048 575 B)! Даремно витрачений простір на диску називається «вільним місцем». Криміналісти часто розглядають вільний простір, щоб знайти залишки підозрілих даних.

Наслідком усіх цих деталей є те, що ви можете написати програму, яка переглядає копію моєї картки пам'яті, шукаючи підписи JPEG. Кожного разу, коли ви знайдете підпис, ви можете відкрити новий файл для запису і почати заповнювати цей файл байтами з моєї картки пам'яті, закриваючи цей файл лише після того, як ви зустрінете інший підпис. Більше того, замість того, щоб читати байти моєї картки пам'яті по черзі, ви можете для ефективності прочитати 512 з них за раз. Завдяки FAT ви можете довіряти, що підписи JPEG будуть "вирівняні за блоками". Тобто вам потрібно шукати ці підписи лише у перших чотирьох байтах блоку.

Файли JPEG можуть охоплювати суміжні блоки. Проте останній байт JPEG може не потрапити в самий кінець блоку. Згадайте про можливість вільного місця. Оскільки ця карта пам'яті була абсолютно новою, коли починали знімати фотографії, що спрощує нам завдання і означає що будь-яке вільне місце буде заповнене 0. Це нормально, якщо ці кінцеві нулі потрапляють у JPEG, які ви відновлюєте.

### *Практика*

Отже, ми створили «криміналістичне зображення» картки, зберігаючи її вміст байт за байтом, у файлі який називається “**card.raw**”. Ми зобразили лише перші кілька мегабайт карти пам'яті. Але в підсумку ви повинні виявити 50 JPEG зображень.

Щоб завантажити **card.raw** перейдіть за посиланням <http://cdn.cs50.net/2020/fall/psets/4/recover/recover.zip>

### *Завдання*

Створити програму, яка відновлює JPEG з криміналістичного зображення.

Програма повинна прийняти рівно один аргумент командного рядка, назва криміналістичного зображення, з якого можна відновити JPEG.

Якщо ваша програма не виконується рівно з одним аргументом командного рядка, вона повинна нагадувати користувачеві про правильне використання, та повинна повертати 1.

Якщо криміналістичне зображення не можна відкрити для читання, ваша програма повинна повідомити про це користувача, та повинна повернути 1.

Кожен створений файл повинен мати назву **###.jpg**, де **###** - трицифрове десяткове число, починаючи з 000 для першого зображення.

Після запуску ваша програма повинна відновити кожен із файлів JPEG із **card.raw**, зберігаючи кожен як окремий файл у вашому поточному робочому каталозі. Ваша програма повинна нумерувати файли, які вона видає, називаючи кожен **###.jpg**, де **###** - трицифрове десяткове число від 000 і вище. Вам не потрібно намагатись відновити оригінальні назви JPEG. Щоб перевірити, чи правильні JPEG-файли, просто двічі клацніть і подивіться! Якщо кожна фотографія здається цілою, ваша операція, мабуть, була успішною!

Однак є шанси на те, що JPEG, які повертає ваша програма, будуть неправильними. (Якщо ви відкриваєте їх і нічого не бачите, вони, мабуть, неправильні!).

### **УВАГА!!!**

**Якщо у Вас достатньо знань і навичок з програмування спробуйте виконати це завдання самостійно.**

У додатку 2 показано реалізацію цього завдання мовою програмування C. Ви можете скористатись готовою програмою і відновити файли із криміналістичного зображення “**card.raw**”.



У звіті про виконання **завдання Б** цієї лабораторної роботи потрібно надати один із 50 відновлених файлів зображень JPG.

Номер файлу у звіті визначається номером Вашої залікової книжки:

- якщо дві останні цифри номера залікової  $xx \leq 49$  то вибираєте файл **0xx.jpg**
- якщо дві останні цифри номера залікової  $xx = 50$  то вибираєте файл **000.jpg**
- якщо дві останні цифри номера залікової  $xx \geq 51$ , проведіть арифметичну дію  $yy = xx - 50$  і виберіть файл **0yy.jpg**

Тобто студент із номером залікової книжки 2119124С у звіті представляє файл 024.jpg, а студент із номером залікової книжки 3119086С – файл 036.jpg.