Практична робота 1. Дослідження образу диска (Linux ext4) в Autopsy

Мета роботи

- Виконати аналітичний огляд образу диска в Autopsy
- Теоретично ознайомитися з інструментами The Sleuth Kit (TSK) та їх відповідниками в Autopsy.

Вимоги до середовища

- Встановлений Autopsy (остання стабільна версія).

Завдання 1. Створення кейсу та підключення образу

1. Запустіть Autopsy → Create New Case.
2. Case name: Lab1_<Прізвище>.
3. Add Data Source → Image File → оберіть файл образу (disk.img).
4. За потреби вкажіть файлову систему (ext4) і часовий пояс.

Завдання 2. Огляд структури файлової системи

1. Перейдіть у File System → Directory Tree.
2. Огляньте кореневі каталоги: /etc, /var, /home, /root, /tmp.
3. Зафіксуйте скріншоти дерева каталогів верхнього рівня з короткими підписами.

Завдання 3. Аналіз користувацьких та системних артефактів

1. Перевірте /home/<user> на наявність:
    - Історій оболонки: .bash_history, .zsh_history
    - SSH-артефактів: ~/.ssh/authorized_keys, known_hosts
    - Документів і завантажень: Documents, Downloads

2. Перейдіть до /var/log: перегляньте auth.log, syslog, dmesg, lastlog, wtmp, btmp.

Завдання 4. Пошук за ключовими словами

1. Results → Keyword Search або власні Custom Keywords.
2. Рекомендовані ключові слова: password, passwd, ssh, token, key, confidential, secret, gmail, login, sudo.
3. Зафіксуйте скріншоти знайдених збігів і контексту відображення в Autopsy.

Завдання 5. Ідентифікація видалених об’єктів

1. У Directory Tree увімкніть показ видалених елементів або скористайтеся відповідними Views.
2. Зробіть нотатки про наявність видалених файлів, їх розташування та ймовірну значущість.

Завдання 6. Аналіз метаданих образу в Image Details

1. Відкрийте панель Image Details для завантаженного диску.
2. Проаналізуйте наведені параметри та дайте короткі висновки щодо кожного з них:
3. Зробіть 1–2 скріншоти ключових частин Image Details з підписами.

Контрольні питання

- Яка роль суперблоку ext4? Які ключові поля варто перевіряти і як їх інтерпретувати в контексті цілісності ФС?
- Що таке групи блоків у ext4 і як вони впливають на розміщення даних та метаданих?
- Як організовані inode в ext4: що зберігають, які є часові мітки (atime, mtime, ctime, crtime) і чим вони відрізняються?
- Які типові mount-опції (наприклад, noatime, relatime, lazytime) впливають на часові мітки та слідову інформацію?

- Які обмеження і ризики при ідентифікації та відновленні видалених файлів у ext4 з точки зору затирання метаданих та перезапису extent-ів?
- Як інтерпретувати дані про файлову систему ext4 в Autopsy: де подивитися метадані ФС, розмітку розділів?