Особливості дослідження пристроїв з операційною системою macOS

Ірина Біловицька
старший судовий експерт, відділ комп'ютерно-технічних та телекомунікаційних досліджень,
Центр судових і спеціальних експертиз Інституту спеціальної техніки та судових експертиз
Служби безпеки України, м. Київ, Україна, e-mail: biiran@ssu.gov.ua

У тезах розглянуто особливості експертного дослідження пристроїв Apple з macOS. Проаналізовано вплив APFS, FileVault 2, Secure Enclave, T2 та Apple Silicon на процес вилучення й аналізу даних.

***Ключові слова**: цифрова криміналістика; macOS.*

Features of Examining Devices With MacOS Operating System

Iryna Bilovytska

This paper discusses features of expert research on Apple devices with macOS. The impact of APFS, FileVault 2, Secure Enclave, T2 and Apple Silicon on data extraction and analysis is analysed.

***Keywords:** digital forensics; macOS.*

Сучасні версії операційної системи macOS застосовують файлову систему Apple File System (APFS). Починаючи з macOS 10.15 Catalina, упроваджено групи томів APFS: системний том і том даних об'єднано в пару. Системний том містить лише системні файли й монтується лише для читання, тоді як користувацькі дані зберігаються окремо на томі Data [1]. Така структура підвищує безпеку й цілісність ОС, але потребує від експерта враховувати наявність кількох томів під час аналізу.

MacOS має вбудовані механізми безпеки [2], що ускладнюють несанкціонований доступ і модифікацію системи. System Integrity Protection (SIP) обмежує доступ до системних каталогів навіть з привілеями адміністратора, захищаючи важливі файли від змін. Із macOS 11 Big Sur введено концепцію Signed System Volume (SSV) — криптографічно підписаний та захищений системний том. Під час завантаження Big Sur і новіших версій кожен системний файл перевіряється за хешем SHA-256, і цілісність усього системного тому гарантована спеціальною «печаткою». У разі будь-якого втручання або пошкодження системного розділу macOS блокуватиме завантаження, що ускладнює модифікацію системи під час експертизи. Такі технології, як Secure Enclave (апаратний модуль безпеки в чіпах T2 та Apple Silicon), захищають чутливі дані та ізолюють їх від доступу з боку ОС.

Значна увага приділяється шифруванню дисків на комп'ютерах Mac [2]. Технологія FileVault 2 забезпечує повне шифрування системного диска, що робить злом сучасними методами практично неможливим. Увімкнений FileVault шифрує всі дані — ОС, застосунки й файли користувача — і розшифровує їх «на льоту» після введення пароля під час завантаження системи. Навіть якщо накопичувач вилучити з комп'ютера і під'єднати до іншого пристрою, дані залишаться недоступними без ключа розшифрування. Окрім пароля користувача, розблокувати том FileVault можна за допомогою ключа відновлення (Recovery Key), заданого під час шифрування, або інституційного ключа (для корпоративних Mac). У сучасних Mac із чіпами T2/M1 шифрування виконується апаратно: кожен пристрій має унікальний ключ, «зашитий» у Secure Enclave/T2. Це означає, що розшифрувати дані можна тільки на оригінальному пристрої, який містить цей ключ.

Основні проблеми при вилучені та аналізуванні даних macOS є [3]:

- зашифровані диски (FileVault 2). Повнодискове шифрування на Mac значно ускладнює отримання даних. Якщо FileVault активовано й пароль невідомий, прямий доступ до вмісту диска неможливий — всі дані на носії зашифровані криптографічним алгоритмом AES-256;
- аппаратний чіп безпеки T2. Найбільша проблема для експертів — унікальність ключів шифрування, прив'язаних до

T2. Дані на SSD постійно шифруються контролером T2, і навіть якщо FileVault формально вимкнено, носій має апаратне шифрування. T2 за замовчуванням не дає змоги завантаження з непідписаних носіїв: меню Startup Security потребує авторизації для перемикання в режим дозволу зовнішнього завантаження. Отже, експерт без пароля адміністратора не зможе просто завантажити свій інструмент з флешки на вилученому Mac з T2;

- Apple Silicon (чіпи M1/M2). На комп'ютерах з даними чіпами немає Target Disk Mode у класичному вигляді — доступ лише через Recovery (Share Disk) з авторизацією. Присутнє Secure Enclave та завжди увімкнене апаратне шифрування диска;
- відсутність стандартного доступу до даних. У macOS багато даних зберігається в закритих сховищах або форматах, що ускладнює аналіз уручну. Система прав доступу може перешкоджати відкриттю файлів навіть з образу, якщо інструмент аналізу неправильно інтерпретує їх. Деякі каталоги містять пісочниці застосунків із власною структурою. Також macOS не має загальноприйнятого реєстру — замість нього безліч plist-файлів, розкиданих по системі;
- сумісність інструментів та середовищ. Більшість традиційних криміналістичних інструментів історично працюють в Windows. Робота з образами macOS на Windows-станціях може ускладнюватися через відсутність драйверів APFS.

З даними обмеженнями є лише пара варіантів отримання інформації:

- логічне копіювання даних, яке передбачає отримання файлів і даних з працюючої системи засобами самої ОС або спеціального програмного забезпечення. Наприклад, можна скопіювати окремі папки, експортувати бази даних або виконати резервне копіювання засобами системи. Логічне копіювання не охоплює видалені файли та незайнятий простір, тому менш повне, але його перевага — менший обсяг даних і можливість працювати з уже розшифрованою інформацією (якщо система розблокована);
- фізичне копіювання дає змогу зберегти структуру файлової системи, усі файли та метадані. На старіших Mac (з HDD або без шифрування) фізичний знімок можна отримати, вийнявши диск і підключивши його через пристрій захисту від запису до робочої станції, або завантаживши Mac у спеціальний режим. Для комп'ютерів Mac на базі процесорів Intel традиційним є Target Disk Mode: під час запуску в даному режимі пристрій перетворюється на зовнішній диск, який можна під'єднати до іншого комп'ютера через Thunderbolt і зняти образ стандартними засобами. У разі шифрування FileVault цільовий диск буде видимий як зашифрований том — для монтування потрібен пароль. На нових Apple Silicon Mac застосовується режим спільного доступу до диска: завантажившись у Recovery, можна вибрати Share Disk і тим самим надати вміст диска іншому Mac по Thunderbolt. Це дає змогу отримати образ, проте так само потребує введення пароля для розблокування, якщо диск зашифровано. Окрім того, є проблеми з відповідністю версій ОС. У разі, якщо на досліджуваному ноутбуці та робочій станції не співпадають версії, існує ймовірність відмови при поширенні диска.

У разі ж коли система закрита паролем, можна спробувати декілька варіантів вирішення проблеми, але дуже обережно:

- підбір / відновлення пароля. Якщо пароль можна вгадати або перебрати, експерт може спробувати атаку методом повного перебору паролів на шифрованому образі. Для FileVault 2 доступні інструменти типу Hashcat або Passware, які, маючи копію заголовку тома, здійснюють перебір паролів. Проте через високу крипто-

стійкість це дієво лише при відносно простих паролях;

- отримання ключа відновлення. Під час ввімкнення FileVault користувачу пропонується зберегти Recovery Key. Якщо відомо Apple ID власника, можна запитати цей ключ в Apple або спробувати отримати з iCloud. Наявність ключа відновлення дасть змогу розблокувати том без основного пароля;
- експлойти апаратних вразливостей. Для чіпа Apple T2 у 2020 році було виявлено неусувне уразливе місце (checkm8), що дає змогу отримати низькорівневий доступ до чіпа. Якщо ввести Mac з T2 у DFU-режим і скористатись експлойтом, можна скинути лічильники введення пароля або навіть екстрагувати ключі шифрування. Деякі продукти (наприклад, Passware Kit та ін.) інтегрували ці можливості, даючи змогу обходити пароль EFI та пришвидшувати перебір паролів FileVault на Mac з T2.

На сьогодні основними інструментами для аналізу macOS є:

- Magnet AXIOM [4]. AXIOM вміє імпортувати образи APFS, розшифровувати їх за наявності ключів / паролів та автоматично аналізувати артефакти macOS;
- BlackBag BlackLight [5]. BlackLight може відкривати образи дисків Mac, відновлювати видалені файли, знаходити артефакти користувача. Його програмний модуль оптимізований під APFS і HFS+, підтримує декодування ключових сховищ macOS;
- Cellebrite MacQuisition [5]. Головна перевага MacQuisition — підтримка роботи з чіпом безпеки T2 та новими Apple Silicon. Це єдине рішення, що дає змогу створити фізичний дешифрований образ диска на Mac із T2-чіпом. Продукт застосовує можливості самого T2: під час завантаження з його носія MacQuisition домовляється з чіпом і здійснює дешифрування файлової системи на льоту під час копіювання.

Отже, дослідження пристроїв з macOS потребує комбінування різних підходів та інструментів. Особливості файлової системи APFS, розділення системних томів, шифрування та апаратні модулі безпеки становлять великі проблеми. Проте розуміння цих особливостей та застосування сучасних рішень дають успішно вилучати й аналізувати необхідні дані. Ключовим чинником є актуальність знань: технології Apple швидко розвиваються, тому судовий експерт має постійно оновлювати свій інструментарій і підходи.

Перелік джерел посилання

1. Big Sur's Signed System Volume: added security protection. *The Eclectic Light Company*. URL: https://eclecticlight.co/2020/06/25/big-surs-signed-system-volume-added-security-protection/#:~:text=Catalina%2010,only (дата звернення: 25.12.2025).
2. Apple Platform Security. *Apple Support*. URL: https://support.apple.com/uk-ua/guide/security/welcome/web (дата вернення: 25.12.2025).
3. Minoru Kobayashi. Workshop: An Introduction to macOS Forensics with Open Source Software. *Japan Security Analyst Conference*. 2022.
4. Magnet Forensics | Gain an Investigative Edge. *Magnet Forensics*. URL: https://www.magnetforensics.com/ (дата звернення: 25.12.2025).
5. Cellebrite Digital Collector. *H-11 Digital Forensics*. URL: https://h11dfs.com/macquisition_cellebrite/#:~:text=MacQuisition%20is%20the%20first%20and,data%20is%20collected%20or%20deices (дата звернення: 25.12.2025).