Роль дослідження *SquashFS*-пакетів операційних систем *Linux* в комп'ютерно-технічних експертизах

Роман Пташкін

Черкаський НДЕКЦ МВС України, м. Черкаси, Україна

Експерти з комп'ютерно-технічних досліджень вивчають сучасні файлові Live системи, хоча це доволі складний процес. Фактично для проведення дослідження таких систем експертам необхідно вміти ефективно працювати з SquashFS-пакетами в межах експертного експерименту.

Ключові слова: Linux; SquashFS; судова експертиза.

The Role of Investigating SquashFS Packages in Computer Forensics

Roman Ptashkin

Experts in computer forensics study modern Live file systems, although this is quite a complex process. In fact, to conduct investigations of Live systems, experts need to be proficient in working with SquashFS packages within the framework of forensic experiments.

Keywords: Linux; SquashFS; computer forensics.

Операційні системи (далі — ОС) сімейства *Linux* на сьогоднішній день домінують поміж серверних платформ. За даними *W3Techs*, понад 84% вебсайтів функціонують на *Unix*-подібних ОС, із яких майже 50% — на ОС *Linux*.

Розвиток сімейства *Linux* відзначається швидкими та постійними змінами у сферах організації даних і програмного забезпечення. Експерти з комп'ютерно-технічних досліджень змушені ставати новаторами у вивченні сучасних файлових систем і програмних засобів для забезпечення ефективної роботи в цьому напрямі.

Водночас *Live*-системи, які не потребують інсталяції для функціонування, отримали значну популярність, проте їх нова внутрішня структура та методи організації даних ускладнюють проведення досліджень та аналізування.

Важливо розрізняти фізичну та логічну файлові системи в ОС сімейства *Linux*. Фізична файлова система відповідає за керування дисковим простором і розміщенням файлів на диску, тоді як логічна файлова система визначає логічну структуру зберігання файлів і простір їх імен. Філософія «усе є файл» в Linux відображається в універсальному підході до роботи з даними, де багато взаємодій обмежуються зчитуванням і записом файлів, навіть якщо об'єкт не є традиційним файлом [1, 2].

Спеціальні файли пристроїв — це ключові компоненти ОС, які містять дані, необхідні для взаємодії з різноманітними фізичними пристроями (дисками, дисководами та принтерами). Ці файли є інтерфейсами для взаємодії з драйверами пристроїв, що забезпечують доступ до функціональності цих пристроїв у системі.

У *Linux*-подібних ОС, крім спеціальних файлів пристроїв, існує поняття *loop*-пристрій (англ. *loop device*) — це псевдопристрій, що забезпечує доступ до файлу у форматі блокового пристрою [2, 4].

Завантажувач операційної системи (англ. *bootloader*) є ключовим компонентом, який дає змогу користувачеві налаштовувати параметри завантаження системи та передавати їх у ядро ОС для подальшого оброблення. Сучасні завантажувачі мають багато функціональних можливостей, зокрема зберігання файлової системи в оперативній пам'яті та декодування її з певного носія інформації.

Популярним вибором для стиснення даних у *Linux*-середовищі є файлова система *SquashFS*, що надає доступ до свого вмісту у режимі «тільки для читання» (англ. *read-only*). Для неї характерні компактність і здатність зберігати дані у стислому форматі. Тобто, *SquashFS* — це файлова система зі стисненням даних, яку використовують в ОС із ядром *Linux*. Вона реалізує доступ до свого вмісту в режимі «тільки для читання», що означає, що дані в ній не можна змінити під час роботи ОС [3].

SquashFS — одна з найпоширеніших файлових систем у світі відкритого програмного

забезпечення, особливо в середовищі ОС із ядром *Linux*. Ця файлова система вирізняється своєю високою ефективністю стиснення даних, що робить її популярним вибором для використання у вбудованих системах, областях із обмеженим обсягом дискового простору та інших сценаріях, де важливою є економія місця на диску [2, 3].

Однією з ключових особливостей *SquashFS* є здатність зберігати дані у стислому форматі, що дає змогу ефективно використовувати місце на диску та зменшує ризик фрагментації диска. Ця файлова система забезпечує швидкий доступ до даних, оскільки їх можна зчитати безпосередньо з архіву без необхідності його розпаковування.

До того ж *SquashFS* підтримує різні методи стиснення даних (зокрема, *gzip, lzma* та *xz*), що дає змогу обрати оптимальний метод для конкретних потреб [3]. Вона також підтримує журналювання змін файлів і директорій, що робить її ідеальним вибором для використання у вбудованих системах та інших областях, де важлива надійність та стійкість до змін.

Тому *SquashFS* можна вважати потужним інструментом для зберігання та роботи з даними в ОС з ядром *Linux*.

Найтиповішими питаннями, що виникають в експертній практиці під час дослідження ОС, що використовують *SquashFS*-пакети, є питання зчитування вмісту пакета та зміна його інформаційного вмісту в межах експертного експерименту, що є одним із ключових методів дослідження у сфері комп'ютерно-технічних наук, який дає змогу глибоко вивчати внутрішні механізми та процеси, що відбуваються в операційних системах, програмах або пристроях. Цей метод полягає у проведенні систематичних та об'єктивних експериментів із метою виявлення внутрішніх залежностей, принципів роботи та можливостей досліджуваного об'єкта. В інструментарію судового експерта для дослідження *SquashFS*-пакетів існують три функціональні інструменти — *losetup, unsquashfs* та *mksquashfs* [3—5].

Losetup — це утиліта командного рядка в ОС на базі ядра *Linux*, яка дає змогу з'єднувати файлові системи та розпізнавати області даних у файлах як блокові пристрої: користувачі можуть працювати з файлами, як із дисками, відкриваючи широкі можливості для роботи з даними.

Завдяки *losetup* можна створювати і використовувати *loop*-пристрої, що є важливими для багатьох завдань. Наприклад, вони дають змогу монтувати образ диска, що зберігається у файлі, як звичайний диск, а також створювати та працювати з шифрованими образами дисків.

Unsquashfs — це утиліта в ОС на базі *Linux*, що дає змогу розпаковувати архівовані *SquashFS*-пакети та відновлювати вміст файлових систем. Програма надає можливість аналізувати та відновлювати дані зі *SquashFS*-пакетів, завдяки чому користувачі можуть досліджувати та працювати з архівованими файловими системами [5].

Іншим потужним інструментом в ОС на базі Linux, призначеним для створення *SquashFS*-пакетів, є *Mksquashfs*, що надає користувачам можливість створювати стислі архіви файлових систем, що є важливим для розробки та розгортання ОС, дистрибутивів *Linux* і вбудованих систем [5]. Основна функція *mksquashfs* — це створення *SquashFS*-пакетів із файлових систем, ураховуючи різноманітні параметри та налаштування (зокрема, рівень стиснення, виключення файлів і директорій та атрибути файлів).

Як свідчить практика, кожен дистрибутив *LiveCD* зберігає свою кореневу файлову систему в *SquashFS*-пакеті, який зчитується та частково розпаковується завантажувачем дистрибутиву [4, 5]. Із моменту завантаження системи, коли коренева файлова система вже визначена, алгоритми роботи ОС керуються наявними в цій файловій системі конфігураційними файлами. Маючи доступ до цих файлів, можна повністю керувати процесами завантаження та подальшого функціонування системи.

Тому отримання доступу до вмісту *SquashFS*-пакетів і їх модифікації дає підґрунтя для застосування такого важливого методу проведення досліджень, як експертний експеримент. Застосовуючи алгоритми роботи зі *SquashFS*-пакетами, у межах проведення експертного експерименту можна дослідити внутрішні процеси ОС, отримати доступ до динамічних файлових систем або захищених даних тощо.

Перелік джерел посилання

1. Cooper N. Linux for beginners. The ultimate practical guide to operating system, command line and programming. Improve your computer skills and become a computing expertise. 2020.
2. Negus C. Linux Bible: Thecomprehensive, tutorialresource. Indianapolis, 2015. 912 p.
3. Negus C., Clinton D. Ubuntu Linux Bible. Indianapolis, 2021.
4. Messier R. Operating system forensics. Waltham, 2016.
5. Ward B. How Linux works. 3rd ed. What every superuser should know. Early Access ed. San Francisco, 2021.