DOI: https://doi.org/10.15276/ict.01.2024.36
УДК 004.4

Використання мобільного додатку Termux при проведенні криміналістичної експертизи приладів з операційною системою Android

Ісаченко Ольга Володимирівна
Магістр каф. Інфокомунікаційної інженерії імені В. В. Поповського
E-mail: olha.isachenko@nure.ua
Харківський національний університет радіоелектроніки, пр. Науки, 14. Харків, 61166, Україна

АНОТАЦІЯ

Методи логічного вилучення даних з мобільного пристрою витягують дані, наявні на пристрої, шляхом взаємодії з операційною системою та доступу до файлової системи. Ці методи важливі, оскільки вони надають цінні дані, працюють на більшості пристроїв і прості у використанні. Знову концепція рутування з'являється під час вилучення даних. Логічні методи насправді не вимагають кореневого доступу для вилучення даних. Однак наявність кореневого доступу на пристрої дозволяє отримати доступ до всіх файлів, наявних на пристрої. Це означає, що деякі дані можуть бути витягнуті на нерутованому пристрої, тоді як root-доступ відкриє пристрій і надасть доступ до всіх файлів, наявних на пристрої. Отже, наявність кореневого доступу до пристрою значною мірою вплине на кількість і тип даних, які можна отримати за допомогою логічних методів.

Для логічного отримання даних з пристрою часто застосовують утиліту adb. Вона полегшує різноманітні дії з пристроєм, такі як встановлення та налагодження програм, копіювання даних, створення букапів системи. adb надає доступ до оболонки телефон, який можна використовувати для виконання різних команд на пристрої.

Але якшо працювати з цією та іншими необхідними утілітами з мобільного телефону, з використанням терміналу Termux, в деяких випадках це значно заощаджує час та зусилля. Termux дає змогу зчитувати, обробляти, налізувати дані з цільового пристрою за допомогою лише телефону, що надає дуже мобільний спосіб работи з даними.

Ключові слова: мобільна криміналістика; логічні методи; аналіз мобільних даних; термінал Termux

Актуальність. При проведенні криміналістичної експертизи мобільних пристроїв зазвичай використовується комп'ютер із встановленим спеціалізованим програмним забезпеченням. Проте, технології мобільних телефонів, що постійно вдосконалюються, на сьогоднішній день дали можливість використати навіть мобільний телефон для вилучення даних, за допомогою такого додатку як Termux.

Мета дослідження: розібрати можливості мобільного додатку Termux, його основні модулі, які можуть бути встановлені на телефон та корисні у криміналістичному дослідженні мобільних даних.

Termux – це термінальна програма Android і середовище Linux [1], емулятор терміналу Android, який працює безпосередньо, без необхідності рутування або налаштування. Мінімальна базова система встановлюється автоматично – додаткові пакети доступні за допомогою менеджера пакетів APT [2] (Рис .1).

Переваги застосування Termux:

– підтримування adb модулю;

– отримання доступу до віддалених серверів за допомогою клієнта ssh із OpenSSH;

– великий вибір модулів, таких як Bash, fish або Zsh і nano, Emacs або Vim. Доступ до API за допомогою curl, використання rsync для зберігання резервних копій діних на віддаленому телефоні;

– встановка різних пакетів за допомогою системи керування пакетами APT, відомої з Debian і Ubuntu GNU/Linux;

– пакети, доступні в Termux, встановіть сторінки довідок на свій телефон;

– підтримка програмних пакетів Python, Perl, Python, Ruby та Node.js;

– можливість підключити клавіатуру Bluetooth та зовнішній дисплей;

– підтримка компіляторів для Go, Rust, Swift або C за допомогою Clang, створювання проектів за допомогою CMake і pkg-config [2].

Деякі корисні команди adb, які використовуються у криміналістиці:

adb pull – стягнення одного файлу або цілого каталогу із пристрою.

adb restore <назва архіву> – створення резервної копії пристрою.

dumpsys - універсальна команда з кількома параметрами:

adb shell dumpsys package <назва пакету> – виведе всі дані про даний пакет

adb shell dumpsys activity – надає інформацію про Activity Manager, діяльність, провайдери, послуги, трансляції тощо.

pm list packages – покаже список усіх пакетів на пристрої

adb backup – створіть резервну копію телефону: *adb backup -apk -all -f backup*

adb restore <backup_name> – відновить резервну копію

adb help – список усіх команд

Роздивимось деякі необхідні у мобільній криміналістиці модулі Termux.

1) Модуль ADB на Termux перетворить телефон в термінал ADB, використовуючи root-доступ (Рис. 2).

На телефоні, який досліджується, потрібно ввімкнути перемикач «Налагодження USB» у параметрах розробника, щоб телефон приймав команди. Далі обидва пристрої підключаються до USB. І як тільки обидва телефони будуть фізично підключені, досліджувальний телефон повинен негайно отримати запит «Дозволити налагодження USB».

Щоб перевірити з'єднання, виконують команду: adb devices.

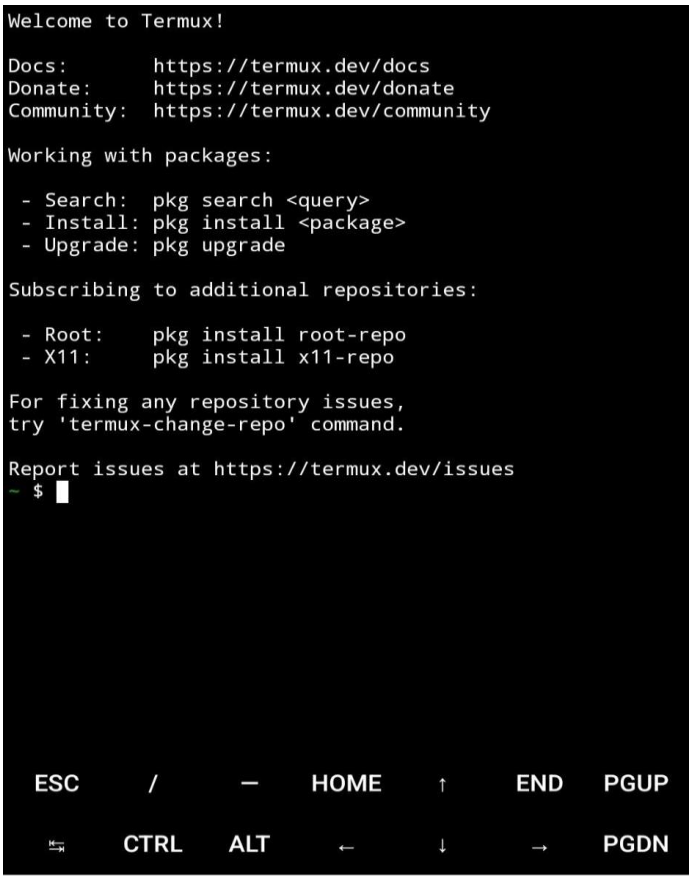

Рис.1. **Інтерфейс терміналу Termux**

Рис. 2. **Модуль adb на Termux**

Ця команда надсилає сигнал на телефон, щоб перевірити, чи може зв'язуватися з ним через ADB. У разі успіху з’являється спливаючий ідентифікатор пристрою під рядком «Список підключених пристроїв» Termux.

2) 7-zip – файловий архіватор з високим ступенем стиснення даних. Підтримує кілька алгоритмів стиснення та безліч форматів даних, включаючи власний формат 7z з алгоритмом стиснення LZMA.

Бекап – це важливий процес створення копії даних з телефону, для подальшого їх відновлення та криміналістичного аналізу.

Для встановлення 7-zip:
$ pkg install p7zip
$ cd storage/shared/Download

Використання:
$ 7z u <folder_name>.7z -pUnder -mx9 '<folder_name>'

3) SQLite [3] – це база даних, інтегрована в багато мобільних додатків. Однією з відмінних рис SQLite є відсутність клієнт-серверної структури.

SQLite, встановлена на Termux, дає можливість агалізувати sqlite бази даних додатків з телефону.

Так, для встановлення, необхідно виконати команди з терміналу:
pkg update
pkg upgrade
pkg install sqlite

Для отримання даних у SQLite застосовується команда SELECT (Рис.3). У спрощеному вигляді вона має наступний синтаксис:

1 SELECT * FROM users;
Якщо необхідно отримати дані не з усіх, а з якихось конкретних стовпців:
1 SELECT id, name FROM users;

4) Telnet (скорочення від «телетайпна мережа») – це клієнт-серверний прикладний протокол, який забезпечує доступ до віртуальних терміналів віддалених систем у локальних мережах або Інтернеті. Це протокол для двонаправленого 8-бітного зв’язку. Його основною метою було з'єднання термінальних пристроїв і термінально-орієнтованих процесів [4].

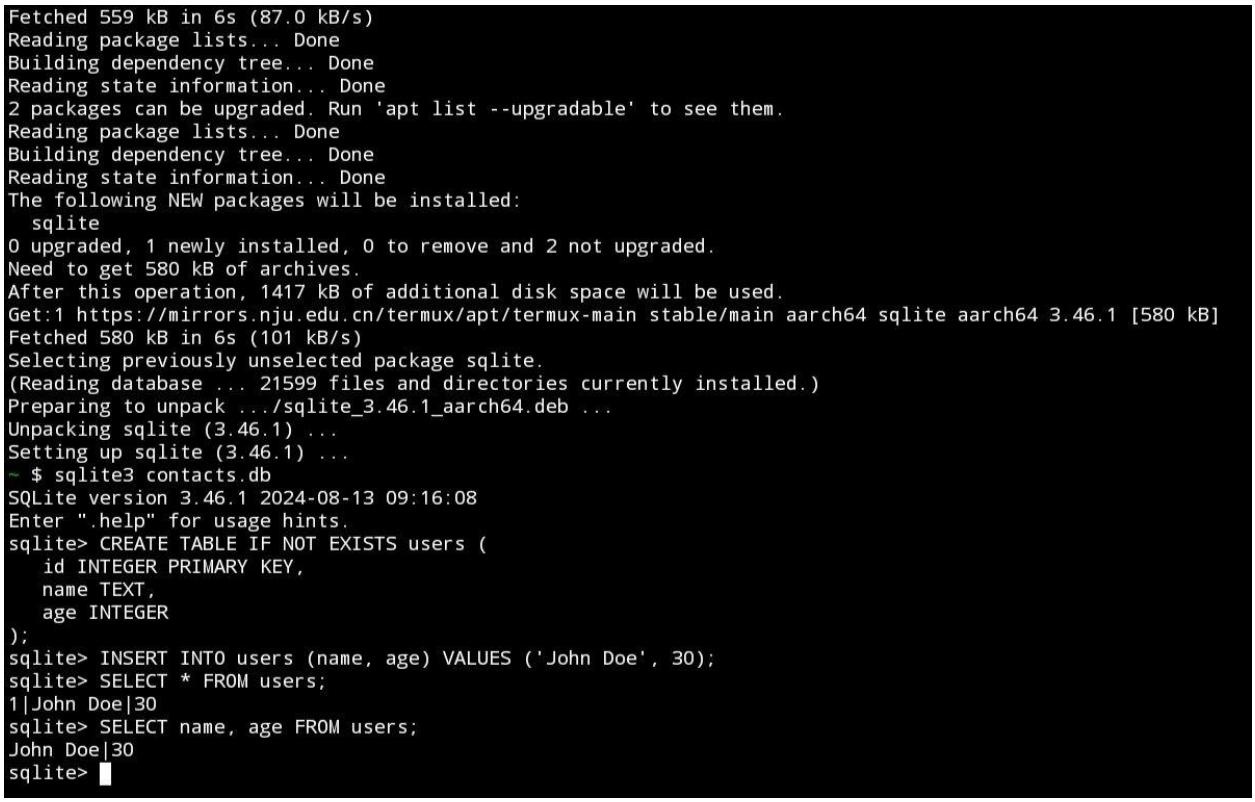

Рис. 3. **Модуль Sqlite у Termux**

Telnet складається з двох компонентів: самого протоколу та компонента служби. Протокол telnet – це клієнт-серверний протокол, заснований на надійному транспорті, орієнтованому на підключення.Цей протокол використовується для встановлення з'єднання з портом протоколу керування передачею (TCP) на 23 або 2323, де прослуховує сервер Telnet [3].

Так, утіліта Telnet (Рис. 4) є важливою при диагностиці та обслідуванні телефону, для провірки доступності портів та інше.

5) Secure Shell (SSH). Протокол Secure Shell (SSH) – це криптографічний мережевий протокол для безпечної роботи мережевих служб у незахищеній мережі. Його найбільш відомі програми – віддалений вхід і виконання командного рядка [5] (Рис. 5).

Для встановленния openssh застосовуємо наступні команди:

pkg update
pkg upgrade
pkg install openssh

Приклади, коли використовується протокол SSH [5]:

- Для входу в оболонку на віддаленому хості (замінюючи Telnet і rlogin).
- Для виконання однієї команди на віддаленому хості (заміна rsh).
- Для налаштування автоматичного входу (без пароля) на віддалений сервер (наприклад, за допомогою OpenSSH).
- У поєднанні з rsync для ефективного та безпечного резервного копіювання, копіювання та віддзеркалення файлів.
- Для перенаправлення порту [6], інші.

Висновки. Мобільний додаток для Android Termux розповсюджується під вільною GPL3+ ліцензією: емулятор терміналу для середовища GNU/Linux, яке працює безпосередньо без необхідності рутування. Мінімальний базовий функціонал встановлюється автоматично, розширені можливості підтягуються за допомогою менеджера пакетів та встановленням стороннього програмного забезпечення з гит-репозиторіїв, а просунута діяльність на телефоні досягається за рахунок рут-прав користувача та встановленням root дистрибутивів GNU/Linux.

Рис. 4. **Модуль Telnet у Termux**

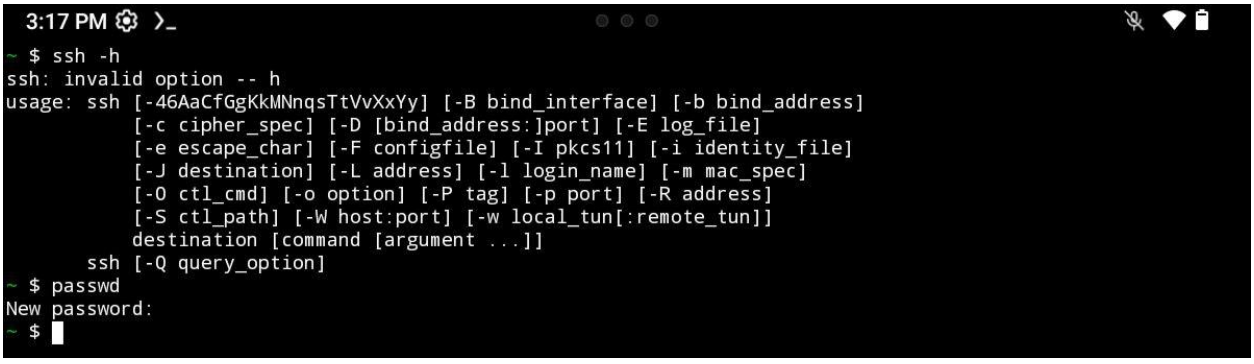

Рис. 5. **Модуль Openssh у Termux**

Таким чином, існує багато переваг при використанні Termux: мобільний додаток Termux дозволяє у будь-який час з телефону оброблювати дані, виконувати операції криміналістичної експертизи мобільних пристроїв, у тому числі запускати автоматизацію на основі Python скриптів.

СПИСОК ЛІТЕРАТУРИ

1. «Інформація з вебсайту “Termux application”». – Доступно з: https://github.com/termux/termux-app. – (Дата звернення: 22.08.2024).
2. Arbanas K., Spremic M., Zajdela Hrustek, N. “Holistic framework for evaluating and improving information security culture”. *Aslib Journal of Information Management*. 2021; 73 (5): 699–719. DOI: https://doi.org/10.1108/AJIM-02-2021-0037.
3. «Інформація з вебсайту “Termux”». – Доступно з: https://termux.dev/en. – (Дата звернення: 24.08.2024).
4. «Інформація з вебсайту “SQLite”». – Доступно з: https://www.sqlite.org. – (Дата звернення: 12.08.2024).
5. Georgiadou A., Mouzakitis S., Bounas K., Askounis D. A. “Cyber-security culture framework for assessing organization readiness”. *Journal of Computer Information Systems.* 2022; 62 (3): 452–462. DOI: https://doi.org/10.1080/08874417.2020.1845583.
6. «Інформація з вебсайту Wikipedia “Telnet”». – Доступно з: https://en.wikipedia.org/wiki/Telnet. – (Дата звернення: 22.08.2024).
7. «Інформація з вебсайту Wikipedia “SSH”». – Доступно з: https://en.wikipedia.org/wiki/Secure_Shell. – (Дата звернення: 24.08.2024).
8. «Інформація з вебсайту “Termux Wiki”». – Доступно з: https://wiki.termux.com/wiki/Getting_started. – (Дата звернення: 10.09.2023).
9. Dumitrescu M. “Fault tolerant control multiprocessor systems modelling using advanced stochastic Petri nets”. *Procedia Technology* 2016; 22: 623–626. DOI: https://doi.org/10.1016/j.protcy.2016.01.129.

DOI: https://doi.org/10.15276/ict.01.2024.36
UDC 004.4

Using the Termux mobile application for forensic expertise of Android devices

Olha V. Isachenko
Master, faculty Infocommunication Engineering named after V.V. Popovsky
E-mail: olha.isachenko@nure.ua
Kharkiv National University of Radio Electronics, 14, Nauky Ave. Kharkiv, 61166, Ukraine

ABSTRACT

Mobile device logical data extraction methods extract the data present on the device by interacting with the operating system and accessing the file system. These methods are important because they provide valuable data, work on most devices, and are easy to use. Again the concept of rooting comes into play when extracting data. Boolean methods don't actually require root access to extract data. However, having root access on the device allows you to access all the files present on the device. This means that some data can be extracted on a non-rooted device, while root access will unlock the device and give access to all files present on the device. Therefore, having a rooted device will greatly affect the amount and type of data that can be retrieved using the logical methods.

The adb utility is often used to logistically retrieve data from the device. It facilitates various actions with the device, such as installing and debugging programs, copying data, creating system backups. adb provides access to the phone shell, which can be used to execute various commands on the device.

But if to work with this and other necessary utilities from a mobile phone, using the Termux terminal, in some cases it significantly saves time and effort. Termux allows to read, process, analyze data from a target device using just phone, providing a highly mobile way of working with data.

Keywords: Mobile forensics; logistic methods; mobile data analysis; Termux terminal