

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 телефону, який можна використовувати для виконання різних команд на пристрої.

Але якщо працювати з цією та іншими необхідними утилітами 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 роботи 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 даних на віддаленому телефоні;
- встановка різних пакетів за допомогою системи керування пакетами APT, відомої з Debian і Ubuntu GNU/Linux;
- пакети, доступні в Termux, встановить сторінки довідок на свій телефон;
- підтримка програмних пакетів Python, Perl, Python, Ruby та Node.js;

This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/deed.uk>)

– 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 – створить 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*.

```

Welcome to Termux!

Docs:      https://termux.dev/docs
Donate:    https://termux.dev/donate
Community: https://termux.dev/community

Working with packages:

- Search:  pkg search <query>
- Install: pkg install <package>
- Upgrade: pkg upgrade

Subscribing to additional repositories:

- Root:    pkg install root-repo
- X11:     pkg install x11-repo

For fixing any repository issues,
try 'termux-change-repo' command.

Report issues at https://termux.dev/issues
- $ █

ESC  /  -  HOME  ↑  END  PGUP
  ⌂  CTRL  ALT  ←  ↓  →  PGDN
  
```

Рис.1. Інтерфейс терміналу Termux

```

12:57 PM >_
jdpw          list pids of processes hosting a JDWP transport
logcat        show device log (logcat --help for more)

security:
disable-verity  disable dm-verity checking on userdebug builds
enable-verity  re-enable dm-verity checking on userdebug builds
keygen FILE    generate adb public/private key; private key stored in FILE,

scripting:
wait-for[-TRANSPORT]-STATE...
  wait for device to be in a given state
  STATE: device, recovery, rescue, sideload, bootloader, or disconnect
  TRANSPORT: usb, local, or any [default=any]
get-state      print offline | bootloader | device
get-serialno   print <serial-number>
get-devpath    print <device-path>
remount [-R]   remount partitions read-write. if a reboot is required, -R will
               will automatically reboot the device.
reboot [bootloader|recovery|sideload|sideload-auto-reboot]
  reboot the device; defaults to booting system image but
  supports bootloader and recovery too. sideload reboots
  into recovery and automatically starts sideload mode,
  sideload-auto-reboot is the same but reboots after sideloading.
sideload OTAPACKAGE
  sideload the given full OTA package
root          restart abdb with root permissions
unroot        restart abdb without root permissions
usb           restart abdb listening on USB
tcpip PORT    restart abdb listening on TCP on PORT

internal debugging:
start-server   ensure that there is a server running
kill-server    kill the server if it is running
reconnect      kick connection from host side to force reconnect
reconnect device
  kick connection from device side to force reconnect
reconnect offline
  reset offline/unauthorized devices to force reconnect

usb:
attach         attach a detached USB device
detach         detach from a USB device to allow use by other processes

environment variables:
$ADB_TRACE    comma/space separated list of debug info to log:
               all,adb,sockets,packets,rwx,usb,sync,sysdeps,transport,jdpw
$ADB_VENDOR_KEYS
  colon-separated list of keys (files or directories)
$ANDROID_SERIAL
  serial number to connect to (see -s)
$ANDROID_LOG_TAGS
  tags to be used by logcat (see logcat --help)
$ADB_LOCAL_TRANSPORT_MAX_PORT
  max emulator scan port (default 5585, 16 emus)
$ADB_MDNS_AUTO_CONNECT
  comma-separated list of mdns services to allow auto-connect (default adb-tls-conne
ct)

Online documentation: https://android.googlesource.com/platform/packages/modules/adb/+/refs/heads/main/docs/
user/adb.1.md

~ $ adb devices
List of devices attached

~ $ █
ESC          /          -          HOME        /          ↑          END          PGUP
            CTRL        ALT        -          ↓          →          PGDN
    
```

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].

```

Fetched 559 kB in 6s (87.0 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sqlite
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 580 kB of archives.
After this operation, 1417 kB of additional disk space will be used.
Get:1 https://mirrors.nju.edu.cn/termux/apt/termux-main/stable/main/aarch64/sqlite_aarch64_3.46.1 [580 kB]
Fetched 580 kB in 6s (101 kB/s)
Selecting previously unselected package sqlite.
(Reading database ... 21599 files and directories currently installed.)
Preparing to unpack ../sqlite_3.46.1_aarch64.deb ...
Unpacking sqlite (3.46.1) ...
Setting up sqlite (3.46.1) ...
~ $ sqlite3 contacts.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> CREATE TABLE IF NOT EXISTS users (
  id INTEGER PRIMARY KEY,
  name TEXT,
  age INTEGER
);
sqlite> INSERT INTO users (name, age) VALUES ('John Doe', 30);
sqlite> SELECT * FROM users;
1|John Doe|30
sqlite> SELECT name, age FROM users;
John Doe|30
sqlite> █

```

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 діагностиці та обслідуванні телефону, для перевірки 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).

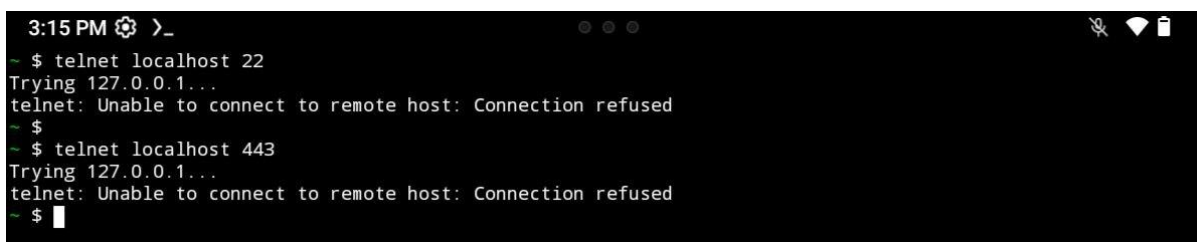
Для встановлення openssh застосовуємо наступні команди:

```
pkg update
pkg upgrade
pkg install openssh
```

Приклади, коли використовується протокол SSH [5]:

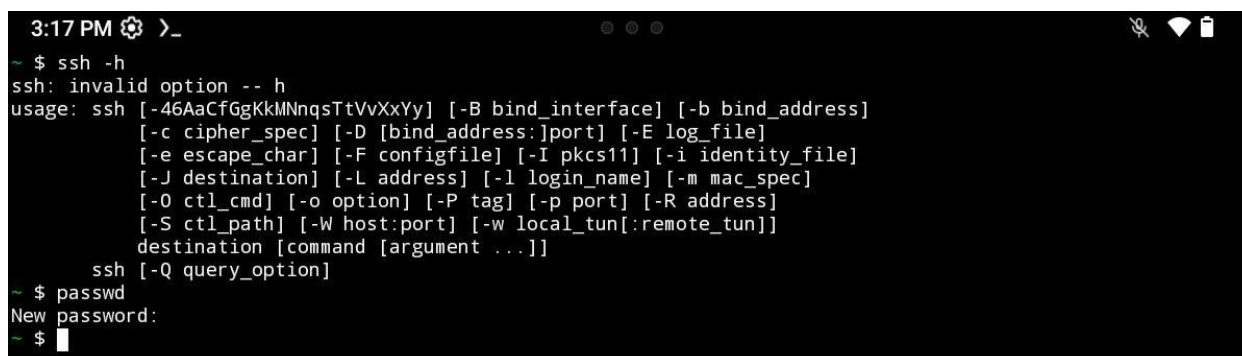
- Для входу в оболонку на віддаленому хості (заміняючи Telnet і rlogin).
- Для виконання однієї команди на віддаленому хості (заміна rsh).
- Для налаштування автоматичного входу (без пароля) на віддалений сервер (наприклад, за допомогою OpenSSH).
- У поєднанні з rsync для ефективного та безпечного резервного 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.



```
3:15 PM >_
~ $ telnet localhost 22
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
~ $
~ $ telnet localhost 443
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
~ $
```

Рис. 4. Модуль Telnet у Termux



```
3:17 PM >_
~ $ ssh -h
ssh: invalid option -- h
usage: ssh [-46AaCfGgKkMnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
[-c cipher_spec] [-D [bind_address:]port] [-E log_file]
[-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
[-J destination] [-L address] [-l login_name] [-m mac_spec]
[-O ctl_cmd] [-o option] [-P tag] [-p port] [-R address]
[-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
destination [command [argument ...]]
ssh [-Q query_option]
~ $ passwd
New password:
~ $
```

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