УДК 343.1 + 004
Віталій Вікторович НОСОВ
кандидат технічних наук, доцент,
професор кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
ORCID ID: orcid.org/0000-0002-7848-6448

ОСОБЛИВОСТІ ОГЛЯДУ ТА ВИЛУЧЕННЯ ДАНИХ З МОБІЛЬНОГО ANDROID ТЕРМІНАЛУ

На сьогодні у рамках розслідувань кримінальних проваджень дуже часто виникає потреба невідкладно, силами оперативних працівників і за дорученням слідчого, здійснювати огляд мобільного терміналу, який було вилучено у підозрюваного на місці вчинення злочину, при обшуку або надано потерпілим. Метою такого огляду є виявлення і фіксація інформації в електронній (цифровій) формі, що містить дані щодо обставин вчинення кримінального правопорушення.

Оскільки оперативні підрозділи Національної поліції мають у своєму розпорядженні невелику кількість коштовних спеціалізованих апаратно-програмних засобів для вилучення даних з мобільних терміналів, наприклад Cellebrite UFED [1], то вочевидь існує необхідність розробки методики вилучення даних із використанням звичайного портативного комп'ютеру і безкоштовного програмного забезпечення.

Існує цілий ряд публікацій [2-4], де розглядаються окремі аспекти використання різноманітних програмних інструментів логічного вилучення і аналізу даних мобільних Android терміналів. Взявши за основу запропоновані рішення, з урахуванням практичної перевірки і їх доповненням, можна запропонувати окрему методику огляду та вилучення даних з мобільного терміналу для оперативних працівників Національної поліції України.

Коротко розглянемо основні фази такої методики огляду та вилучення даних з мобільного терміналу, на якому встановлена ОС Android і заблоковані права адміністратора, що є найбільш імовірним випадком [5,6]. Припускаємо, що термінал розблокований.

1. Візуально оглядається мобільний термінал, встановлюється його стан (чи включений), можливість доступу (чи заблокований), виробник, тип операційної системи. Через налаштування ОС визначається усі можливі ідентифікатори терміналу (IP, MAC, MEID, IMEI) та SIM картки (IMSI).
2. Вимикаються служби WiFi, Hotspot, Bluetooth. Термінал переводиться у режим польоту (відключається від стільникової мережі), відключається перехід у режим сну, відслідковується достатність заряду акумулятору.
3. У налаштуваннях терміналу вмикається режим розробника (Developer), дозволяється відладка по USB (USB Debugging).
4. Підготовлюється робоча станція для криміналістичного дослідження мобільного терміналу:
    a. ноутбук з ОС Windows 10;
    b. кабелі для підключення терміналу USB-microUSB, USB-Type C;
    c. безкоштовне програмне забезпечення:
        - SDK Platform Tools for Windows;
        - Android USB Drivers for Windows;
        - Java for Desktop;
        - Android Backup Extractor;
        - AFLogical OSE;
        - QuickHash;
        - DB Browser for SQLite;
        - LibreOffice;
        - Maltego CE.
5. Термінал підключається до робочої станції через відповідний кабель USB-microUSB (-Type C).
6. У командному рядку cmd робочої станції виконуються наступні команди (після символу # йде пояснення команди):

```
>adb start-server          # запуск adb серверу
>adb devices               # визначаються підключені пристрої
>adb shell su              # робиться спроба отримати права адміністратора
>adb shell pm list packages > C:\Terminal\list-packages.txt #  записується
                                                  у файл перелік встановлених застосувань
```

```
>adb shell service list > C:\Terminal\service-list.txt      # записується у файл перелік сервісів ОС
>adb shell dumpsys wifi > C:\Terminal\wifi-list.txt         # записується у файл перелік усіх точок доступу WiFi, до яких підключався термінал
>adb shell dumpsys account > C:\Terminal\account-list.txt   # записується у файл перелік наявних облікових записів
>adb backup -apk -shared -all -f C:\Terminal\backup.ab #    створюється і переноситься на робочу станцію резервна копія системи
```

7. Оскільки в резервній копії системи, що створена не з правами адміністратору, відсутня адресна книга контактів, то через відповідні опції адресної книги терміналу експортуються контакти у файл 00001.vcf, після чого цей файл разом із усім вмістом картки пам'яті терміналу копіюється на робочу станцію:

```
>adb pull /sdcard/00001.vcf C:\Terminal\
```

8. Також у створеній резервній копії системи відсутній журнал дзвінків і SMS повідомлень, тому у термінал встановлюється утиліта AFLogical OSE: Open source Android Forensics app and framework

```
>adb install C:\Terminal\AFLogical-OSE_1.5.2.apk
```

   Після чого відкривається у терміналі застосування AFLogical OSE і запускається збір відповідних даних.

   Зібрані AFLogical OSE дані копіюються на робочу станцію

```
>adb pull /sdcard/forensics/ C:\Terminal\
```

9. Для усіх отриманих файлів обчислюються хеш-значення (наприклад програмою QuickHash), які потім заносяться до протоколу огляду.
10. Отримані файли запаковуються під паролем в архів (пароль заноситься до протоколу), на який накладається електронний цифровий підпис (ЕЦП) посадової особи. Накладання і перевірка ЕЦП здійснюється через офіційний сайт Міністерства юстиції - ca.informjust.ua.
11. Отримані файли і підписаний архів записуються на цифровий носій, який долучається до протоколу огляду.

Далі, із використанням зазначених вище безкоштовних програм, здійснюється аналіз вилучених даних, за результатом якого може бути отримана наступна інформація:

- Телефонна книга;
- SMS, MMS повідомлення;
- Календар;
- Журнал дзвінків;
- Дані власника терміналу;
- Історія веб-браузера;
- Повідомлення, сповіщення Facebook;
- Контакти, дзвінки, повідомлення:
  - WhatsApp;
  - Viber;
  - Skype;
  - Telegram;
  - і т.п.;
- Історія місцезнаходжень;
- Історія голосового керування;
- Історія пошуку, переглядів YouTube;
- Збережені файли.

Слід зазначити, що за отриманими обліковими записами і наявним розблокованим терміналом з'являється можливість огляду віддалених мережних ресурсів володільця терміналу.

Запропонована методика вилучення даних з мобільних Android терміналів із використанням портативного комп'ютеру і безкоштовного програмного забезпечення для оперативних працівників Національної поліції України потребує подальшого розвитку щодо ефективного аналізу вилучених даних великого об'єму із застосуванням безкоштовних програмних інструментів.

Список бібліографічних посилань:

1. Cellebrite UFED Touch Ultimate. URL: http://forensictools.com.ua/sem-dannykh-s-mobilnykh-telefonov/ufed-touch-ultimate.html (дата звернення 26.10.2018).
2. Andrea Fortuna. Forensic logical acquisition of Android devices using adb backup. Posted on December 29, 2017. URL: https://www.andreafortuna.org/technology/android/forensic-logical-acquisition-of-android-devices-using-adb-backup (дата звернення 26.10.2018).
3. Android Forensics with ADB. Posted on 20/12/2017 by tm4n6. URL: https://tm4n6.com/2017/12/20/android-forensics-with-adb (дата звернення 26.10.2018).
4. ISAK MRKAIC. Android Forensics Using Some Open Source Tools. Posted on March 20, 2017. URL: http://cyberforensicator.com/2017/03/20/android-forensics-using-some-open-source-tools (дата звернення 26.10.2018).
5. iOS и Android занимают уже 99,9% рынка мобильных ОС. 24.02.2018. URL: https://www.ixbt.com/news/2018/02/24/ios-android-99-9.html (дата звернення 26.10.2018).
6. Как iOS и Android разделили мобильный рынок. 22.02.2018. URL: https://apptractor.ru/measure/app-store-analytics/kak-ios-i-android-razdelili-mobilnyiy-ryinok.html (дата звернення 26.10.2018).

Одержано _____ 2018.