Aleksandra Boniewicz

ANALIZA ŚLEDCZA URZĄDZEŃ MOBILNYCH

TEORIA I PRAKTYKA

Helion

Redaktor prowadzący: Szymon Szwajger, Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/anaslv
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-8322-425-1

Printed in Poland.

Spis treści

4.3. Pozyskiwanie danych w praktyce

4.3.1. Przygotowanie narzędzi

Do pracy z urządzeniami mobilnymi będzie potrzebna stacja robocza, do której można podpiąć urządzenie. Może to być komputer stacjonarny lub laptop. Na stacji tej może być zainstalowany jeden z trzech dostępnych systemów operacyjnych: Windows, Linux lub macOS. W zależności od systemu operacyjnego użytego na komputerze trzeba będzie zainstalować inne narzędzia. Do wyboru są zarówno narzędzia komercyjne, jak i darmowe. Nie zawsze oprogramowanie do pobierania czy analizy danych jest dostępne dla każdej wersji systemu operacyjnego, dlatego wybór stacji roboczej w dużej mierze będzie zdeterminowany narzędziami, które są w posiadaniu osoby przeprowadzającej analizę. Również rozmaite urządzenia mobilne będą wymagały zainstalowania dodatkowych narzędzi do pracy z nimi. Zostaną one omówione w podrozdziałach opisujących urządzenia wybranego producenta.

Niezależnie od systemu operacyjnego podstawowym narzędziem pracy jest *Android Software Development Kit*[27] (SDK), który oferuje wersje instalacyjne na wszystkie trzy systemy operacyjne. Dodatkowo narzędzie to zawiera w pakiecie komponent *Platform Tools*, który oferuje polecenia takie jak `adb` i `fastboot`.

Stacja robocza z systemem Windows

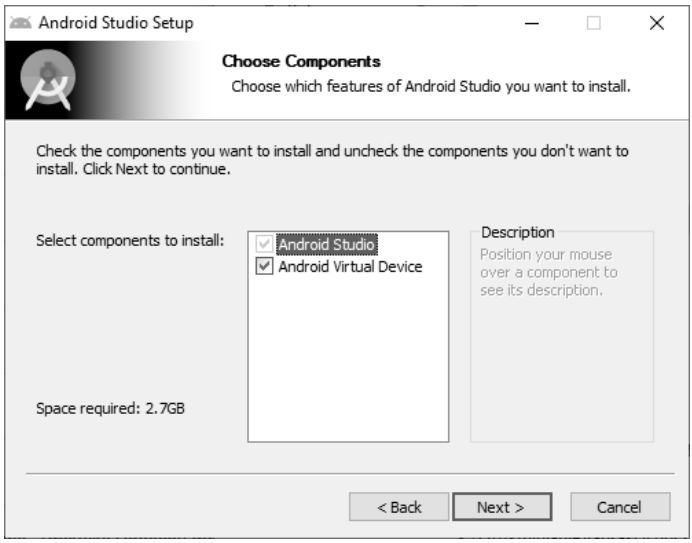
Obecnie dostępną i najbardziej popularną wersją systemu jest Windows 10, choć powoli wkracza na rynek wersja jedenasta. Większość nowych urządzeń mobilnych współpracuje z wersją dziesiątą. Problemy mogą pojawić się jedynie w przypadku starszych urządzeń pracujących z pierwszymi wersjami systemu Android. Wtedy można spróbować podłączyć urządzenie do stacji roboczej z niższą wersją Windowsa. Do pracy przydadzą się następujące aplikacje:

1. SDK

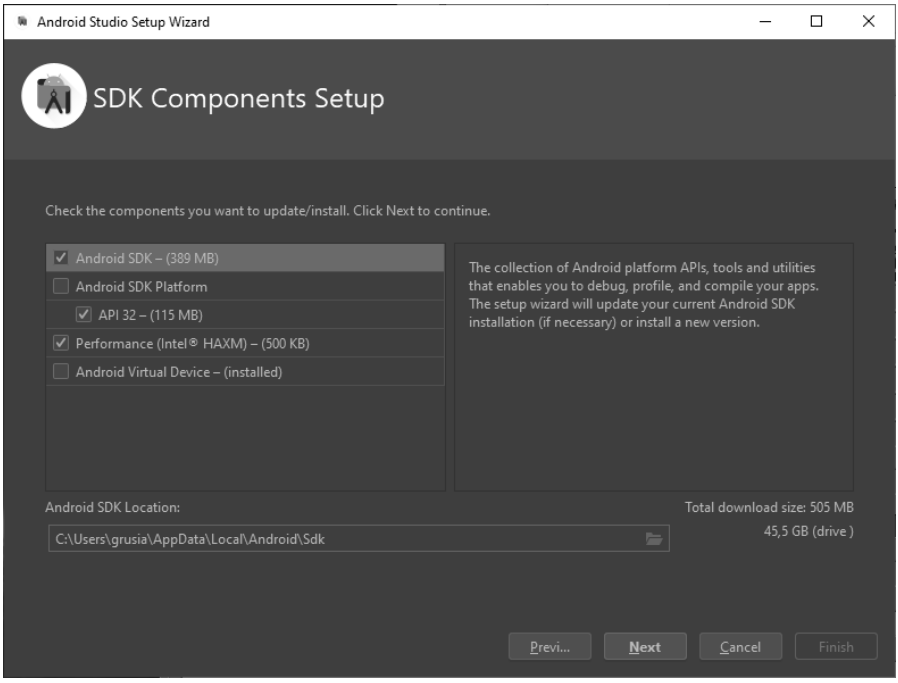
W przypadku systemu operacyjnego Windows 10 (lub starszego) należy pobrać plik instalacyjny SDK ze strony i go uruchomić. Nastąpi proces instalacji Android Studio. Pojawi się okno jak na rysunku 4.21.

Istnieje też możliwość instalacji wirtualnego urządzenia mobilnego, na którym można testować zachowanie różnych aplikacji oraz sposób przechowywania przez nie danych. Po instalacji należy uruchomić *Android Studio* w celu doinstalowania potrzebnych narzędzi (rysunek 4.22).

[27] *https://developer.android.com/studio*.



RYSUNEK 4.21. Instalacja Android Studio w systemie Windows



RYSUNEK 4.22. Android Studio — instalacja Platform Tools w systemie Windows

Wybór pierwszej opcji pozwoli na zainstalowanie zestawu narzędzi *SDK Platform-Tools*. Narzędzia te dostępne będą w oddzielnym katalogu:

LISTING 4.18. Pliki dostępne po zainstalowaniu SDK-Platform-Tools

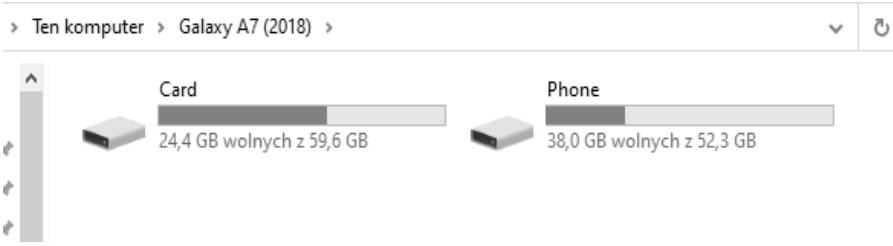
```
C:\User\username\AppData\local\Android\Sdk\platform-tools> dir

09.03.2022  13:12    <DIR>          .
09.03.2022  13:12    <DIR>          ..
09.03.2022  13:12         5 977 600 adb.exe
09.03.2022  13:12            97 792 AdbWinApi.dll
09.03.2022  13:12            62 976 AdbWinUsbApi.dll
09.03.2022  13:12           243 200 dmtracedump.exe
09.03.2022  13:12           441 344 etc1tool.exe
09.03.2022  13:12         1 648 640 fastboot.exe
09.03.2022  13:12            44 032 hprof-conv.exe
09.03.2022  13:12           231 594 libwinpthread-1.dll
09.03.2022  13:12           501 248 make_f2fs.exe
09.03.2022  13:12           501 248 make_f2fs_casefold.exe
09.03.2022  13:12             1 157 mke2fs.conf
09.03.2022  13:12           764 928 mke2fs.exe
09.03.2022  13:12         2 846 110 NOTICE.txt
09.03.2022  13:12                37 source.properties
09.03.2022  13:12         1 216 512 sqlite3.exe
09.03.2022  13:12    <DIR>          systrace
              15 File(s)     14 578 418 bytes
               3 Dir(s)  46 196 928 512 bytes free
```

2. Sterowniki

Aby móc pracować z urządzeniami, należy zainstalować również odpowiednie sterowniki zależne od producenta urządzenia. Z reguły dostępne są one na stronie producenta. Dzięki temu urządzenie będzie widoczne w komputerze jako zewnętrzny dysk, ale też będzie można łączyć się z nim za pomocą poleceń `adb` i `fastboot`.

Po podłączeniu urządzenia będzie ono widoczne jako dysk zewnętrzny (rysunek 4.23).



RYSUNEK 4.23. Telefon widoczny jako dysk zewnętrzny po podłączeniu do komputera

3. Aplikacja Odin

W przypadku urządzeń mobilnych firmy Samsung, aby używać trybu *fastboot* i móc wgrywać obrazy na wybrane partycje, należy skorzystać z darmowego programu *Odin*. W urządzeniach Samsunga nie jest obsługiwany protokół *fastboot*.

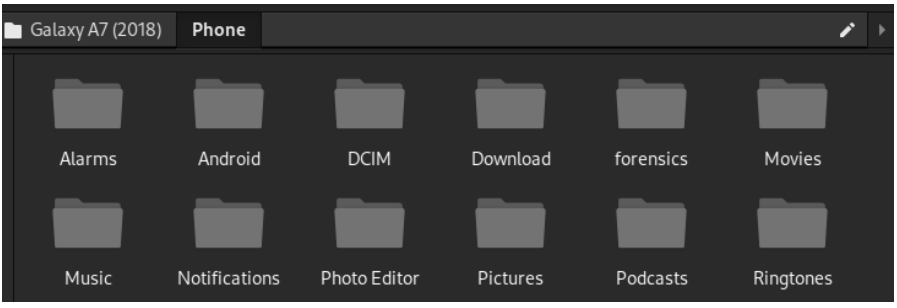
4. 7Zip

Bardzo przydatne narzędzie do rozpakowywania archiwów, w tym również plików obrazów, czy pobranych kopii danych z urządzeń.

Stacja robocza z systemem Linux

Obecnie jest dużo różnych dystrybucji systemu Linux, jednak najbardziej polecaną jest ta przeznaczona do pracy śledczej. Przykładem może być Kali Linux. Zawiera preinstalowane narzędzia, które pozwolą na analizę pobranych danych. Na systemach z rodziny Linuksa nie trzeba instalować żadnych sterowników, gdyż urządzenie jest wykrywane przez system od razu po podłączeniu. Zostanie ono zamontowane i będzie widoczne jako nowy nośnik danych (rysunki 4.24 i 4.25).

RYSUNEK 4.24. Telefon firmy Samsung widoczny po podłączeniu w systemie Linux



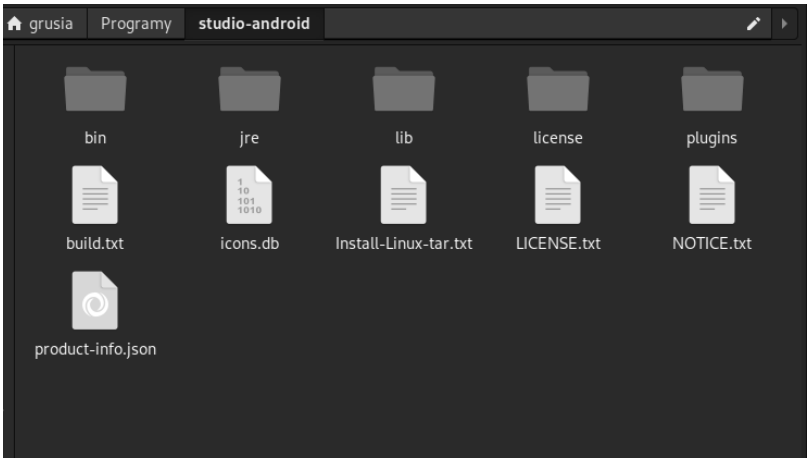
RYSUNEK 4.25. Dane dostępne z podłączonego telefonu w systemie Linux

Do pracy przydadzą się następujące narzędzia:

1. SDK

W tym celu należy ściągnąć odpowiedni plik i go rozpakować. Następnie należy uruchomić skrypt dostępny w katalogu *bin* (rysunek 4.26).

```
cd Programy/studio-android/bin
./studio.sh
```



RYSUNEK 4.26. Plik instalacyjny programu Android Studio w systemie Linux

Gdy narzędzie zostanie uruchomione pierwszy raz, zainstalowane zostaną dodatkowe narzędzia, czyli *Platform-tools* (rysunki 4.27, 4.28 oraz 4.29).

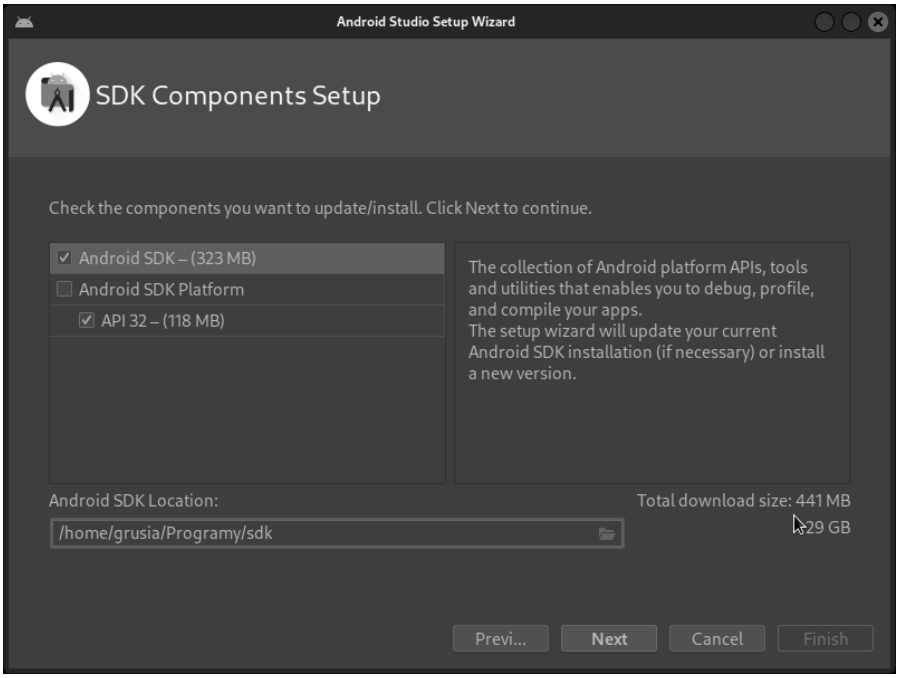
2. `adb` i `fastboot`

Aby móc korzystać z programów `adb` i `fastboot`, nie trzeba koniecznie instalować platformy SDK. Można pobrać te programy, używając menedżera pakietów:

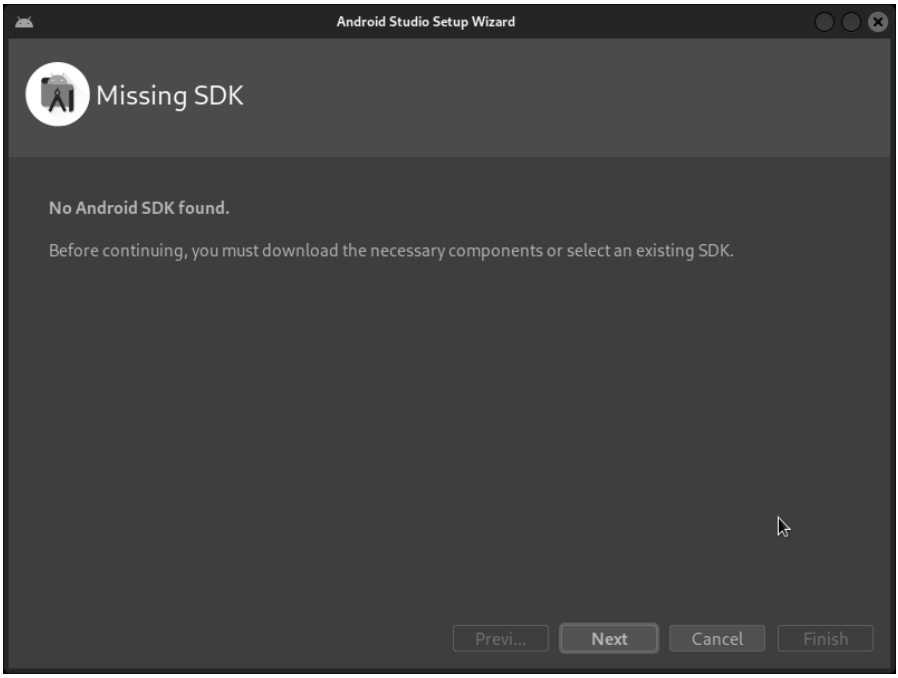
```
apt-get install adb
apt-get install fastboot
```

LISTING 4.19. Instalacja pakietu adb w systemie Kali Linux

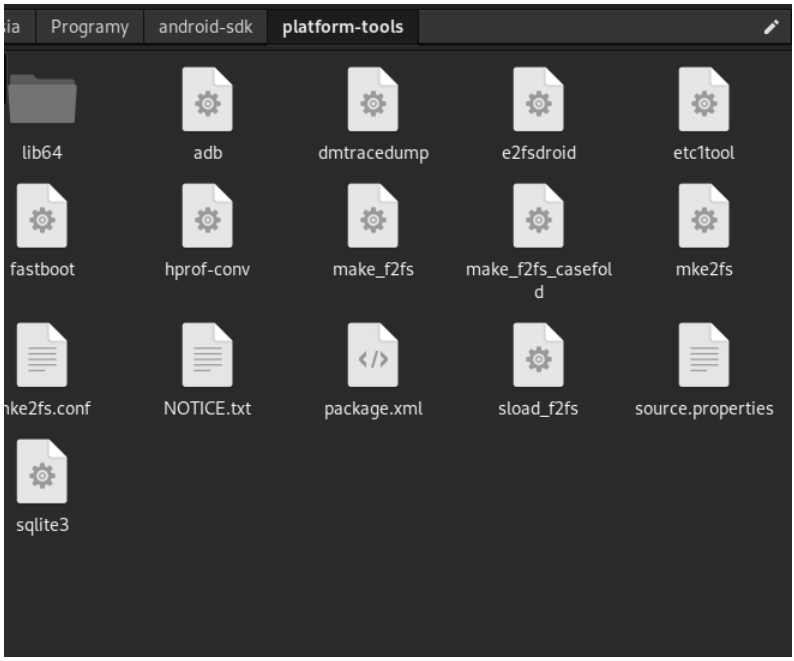
```
user@linux% sudo apt-get install adb
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Odczyt informacji o stanie... Gotowe
Zostaną zainstalowane następujące NOWE pakiety:
  adb
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 844 nieaktualizowanych.
Konieczne pobranie 0 B/599 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 1 795 kB miejsca na dysku.
Wybieranie wcześniej niewybranego pakietu adb.
(Odczytywanie bazy danych ... 311176 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu .../adb_1%3a29.0.6-6_amd64.deb ...
Rozpakowywanie pakietu adb (1:29.0.6-6) ...
Konfigurowanie pakietu adb (1:29.0.6-6) ...
Przetwarzanie wyzwalaczy pakietu man-db (2.9.4-4)...
Przetwarzanie wyzwalaczy pakietu kali-menu (2021.4.2)...
```



RYSUNEK 4.27. Instalacja Android Studio w systemie Linux



RYSUNEK 4.28. Brak możliwości uruchomienia Android Studio



RYSUNEK 4.29. Pliki narzędzia Platform-Tools w systemie Linux

LISTING 4.20. Instalacja pakietu fastboot w systemie Kali Linux

```
user@linux% sudo apt-get install fastboot
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności... Gotowe
Odczyt informacji o stanie... Gotowe
Sugerowane pakiety:
  android-sdk-platform-tools
Zostaną zainstalowane następujące NOWE pakiety:
  fastboot
0 aktualizowanych, 1 nowo instalowanych, 0 usuwanych i 844 nieaktualizowanych.
Konieczne pobranie 0 B/381 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 1 115 kB miejsca na dysku.
Wybieranie wcześniej niewybranego pakietu fastboot.
(Odczytywanie bazy danych ... 311178 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu .../fastboot_1%3a29.0.6-6_amd64.deb ...
Rozpakowywanie pakietu fastboot (1:29.0.6-6) ...
Konfigurowanie pakietu fastboot (1:29.0.6-6) ...
Przetwarzanie wyzwalaczy pakietu kali-menu (2021.4.2)...
Przetwarzanie wyzwalaczy pakietu man-db (2.9.4-4)...
```

Zgodnie z sugestią podaną na listingu 4.20 zamiast oddzielnie instalować pakiety `adb` i `fastboot`, można zainstalować cały pakiet `android-sdk-platform-tools`, korzystając z polecenia `apt-get`.

3. JOdin

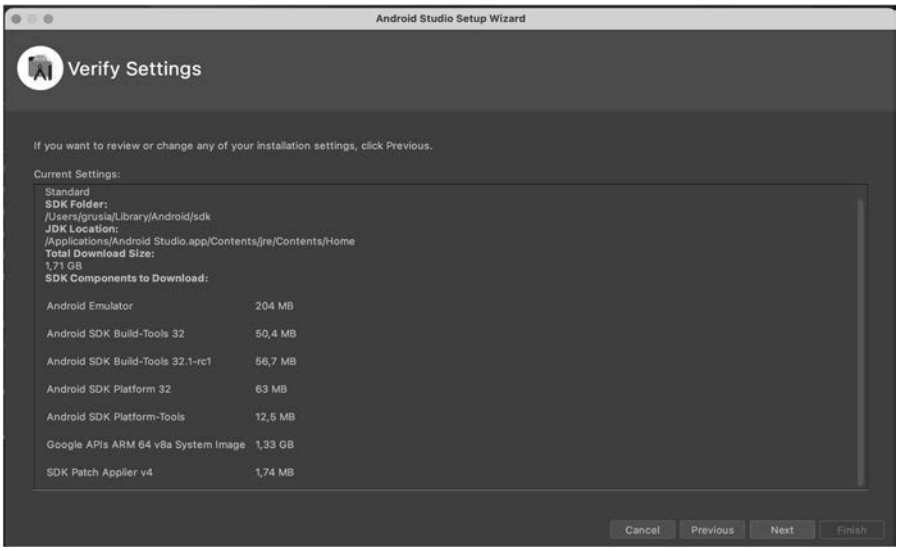
W przypadku komputerów z systemami Linux i macOS można pobrać odpowiednik programu Odin napisany w języku programowania Java o nazwie JOdin.

Program ten też powinien uruchomić się w systemie Windows. Warunkiem działania aplikacji jest zainstalowana Java na wszystkich tych systemach. JOdin opiera się na otwartoźródłowym, wieloplatformowym narzędziu **Heimdall**[28], utworzonym właśnie na potrzeby wgrywania firmowego oprogramowania na urządzenia firmy Samsung. Heimdall to narzędzie, którego komendy wykonywane są z linii poleceń.

Stacja robocza z systemem macOS

1. SDK

Należy pobrać ze strony plik przeznaczony na dany model komputera i uruchomić go. Podczas instalacji można wybrać opcję standardową, która doinstaluje również potrzebne narzędzia *Platform-Tools* (rysunek 4.30).



RYSUNEK 4.30. Instalacja Android Studio w systemie macOS

LISTING 4.21. Pliki Platform-Tools w systemie macOS

```
user@macbook % pwd
/Users/user/Library/Android/sdk/platform-tools
user@macbook % ls
NOTICE.txt  hprof-conf  package.xml
adb   lib64   sload-f2fs
dmtracedump  make_f2fs  source.properties
e2fsdroid  make_f2fs_casefold sqlite3
etc1tool  mke2fs
fastboot  mke2fs.conf
```

[28] *https://glassechidna.com.au/heimdall/*.

Po podłączeniu urządzenia można korzystać z zainstalowanych funkcji. Standardowo podpięcie urządzenia do komputera MacBook wymaga wyrażenia zgody na urządzeniu, aby można było używać opcji *Debugowanie USB.*

LISTING 4.22. Użycie polecenia adb na komputerze z systemem macOS

```
user@MacBook-Pro platform-tools % ./adb devices
* daemon not running; starting now at tcp:5037
* daemon started successfully

List of devices attached
b49d124 device

user@MacBook-Pro platform-tools % ./adb shell
lavender:/ $ su
lavender:/ #

user@MacBook-Pro platform-tools % ./adb reboot bootloader
```

LISTING 4.23. Dostęp do urządzenia mobilnego protokołem fastboot na komputerze z systemem macOS

```
user@MacBook-Pro platform-tools % ./fastboot devices
b49d124 fastboot
```

2. Aplikacje do pobierania danych użytkownika

Ponieważ Android nie jest kompatybilny z systemem macOS, po podłączeniu urządzenia poprzez USB nie jest ono widoczne jako oddzielny dysk zewnętrzny. Aby móc pobierać dane z niego bezpośrednio, nie za pomocą pakietu `adb`, należy zainstalować dodatkowe aplikacje. Dostępne są dwie:

- Android File Transfer[29] — aplikacja bezpłatna.
- MacDroid[30] — aplikacja płatna z siedmiodniową wersją testową.

Po pobraniu aplikacji i zainstalowaniu można podłączyć urządzenie poprzez USB do komputera. Zostanie wówczas wyświetlona zawartość urządzenia (rysunek 4.31).

Po zainstalowaniu aplikacji MacDroid i podłączeniu urządzenia staje się ono w niej widoczne (rysunek 4.32, rysunek 4.33).

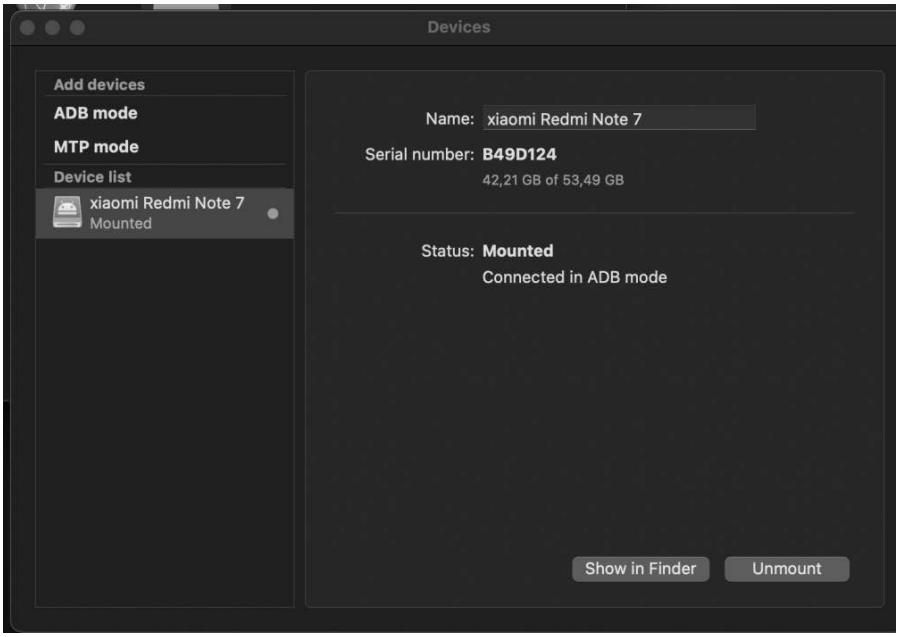
3. JOdin

Podobnie jak w przypadku systemu Linux, w celu pracy z urządzeniami firmy Samsung należy pobrać odpowiednią wersję aplikacji JOdin.

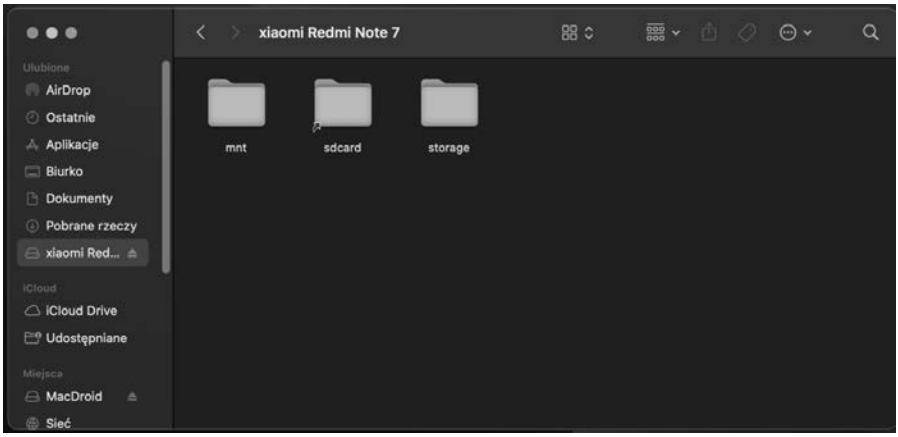
[29] *https://www.android.com/filetransfer/*.

[30] *https://www.macdroid.app/*.

RYSUNEK 4.31. Aplikacja Android File Transfer



RYSUNEK 4.32. Aplikacja MacDroid



RYSUNEK 4.33. Dane dostępne w aplikacji Finder po zamontowaniu urządzenia w aplikacji MacDroid

Pozostałe przydatne narzędzia, które mogą zostać wykorzystane na urządzeniu mobilnym:

1. Aplikacja Magisk

Ta aplikacja pozwala na uzyskanie uprawnień administratora, gdy urządzenie jest uruchomione w trybie normalnym. Umożliwia przygotowanie odpowiednio zmodyfikowanego obrazu urządzenia.

2. BusyBox

Jest to program, który zawiera zbiór powszechnie używanych poleceń systemu Linux.

3. Oprogramowanie firmowe urządzenia

Jeśli posiada się plik *boot.img* wyodrębniony z oprogramowania firmowego, można samemu przygotować nowy plik obrazu i wgrać go na urządzenie. Potrzebna tu będzie jednak specjalistyczna wiedza z zakresu systemów operacyjnych. W internecie dostępne są skrypty, które potrafią zdekompilować plik *boot.img* i wyodrębnić z niego jądro oraz ramdysk systemu, a następnie po zmianach ponownie utworzyć plik obrazu[31].

4. Niestandardowy tryb odzyskiwania danych — *recovery*

Jeśli nie uda się wyodrębnić pliku *boot.img* z oprogramowania firmowego, można poszukać zmodyfikowanego pliku obrazu *recovery* dla urządzenia. Obraz ten jest uruchamiany w trybie odzyskiwania danych. Często pliki te są przygotowywane przez społeczność informatyczną, która opracowuje je hobbystycznie i umieszcza w internecie. Po wgraniu pliku *boot.img* na urządzenie przy użyciu polecenia `fast ↪boot` można uzyskać pełen dostęp do urządzenia i wykonać fizyczną kopię danych.

[31] *https://github.com/aksalj/abootimg*.

ANALIZA ŚLEDCZA URZĄDZEŃ MOBILNYCH
TEORIA I PRAKTYKA

Jeśli myślisz, że dane w Twoim smartfonie są bezpieczne, prawdopodobnie się mylisz. I to bardzo!

Popularność urządzeń mobilnych z roku na rok rośnie. Nic dziwnego – nowoczesny telefon komórkowy można zabrać ze sobą wszędzie i skorzystać z niego praktycznie w każdej sytuacji, w zastępstwie komputera stacjonarnego czy laptopa. To także sprawia, że na swoich smartfonach gromadzimy coraz więcej danych, często osobistych, jak zdjęcia, filmy, hasła czy karty płatnicze. Mogą się one stać łakomym kąskiem dla osoby postronnej, której zamiarem jest wykorzystać je w nieuprawniony sposób. Ponadto urządzenia te bywają używane w działalności przestępczej. Pozostawione w nich ślady często okazują się przydatne podczas orzekania o winie podejrzanego.

Jak hakerzy włamują się do naszych urządzeń mobilnych? Z jakiego oprogramowania i z jakich metod w tym celu korzystają? Jakie słabe punkty ma system operacyjny Android, a jakie iOS? Czy i w jaki sposób możemy skuteczniej zabezpieczać nasze dane? Czym się zajmuje informatyka śledcza i na jakich przepisach prawa bazuje? To tylko kilka z licznych pytań, na które stara się kompleksowo odpowiedzieć autorka tego podręcznika. Do kogo jest on skierowany? Do każdego, kto korzysta na co dzień ze smartfona. Każdy z nas bowiem powinien się uzbroić w podstawową wiedzę dotyczącą zasad bezpiecznego użytkowania urządzeń mobilnych.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-8322-425-1
9 788383 224251
Cena: 69,00 zł