Informatyka śledcza

Laboratorium nr 7

Spis treści

Wstęp

Ostatnie laboratorium zaznajomi Państwa z artefaktami znajdującymi się w systemie mobilnym IOS. Przygotowane zadania mają na celu prześledzenie systemu plików oraz wychwycenie właściwych baz danych oraz plików plist przechowujących istotne informacje badanego urządzenia. Pierwszy krok składa się z ręcznej podstawowej analizy danych zabezpieczonego urządzenia. Na samym końcu zaprezentowane zostanie narzędzie do automatycznego pozyskiwania i raportowania zgromadzonych danych z badanego pliku.

Wykorzystywane narzędzia w trakcie laboratorium:

1. **SQLite**
2. **DB Browser for SQLite**
3. **Plistutil**
4. **iLEAPP**

Przygotowanie do laboratorium

1. Pobierz z platformy MS Teams plik 13-3-1.tar (pliki systemu IOS).
2. Zainstaluj na maszynie wirtualnej (Linux) program SQLite z repozytorium: *(sudo apt-get install sqlite3)*

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlite3
SQLite version 3.36.0 2021-06-18 18:36:39
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite>
```

3. Rozpakuj plik *13-3-1.tar* w systemie Linux (jeśli maszyna wirtualna nie posiada wystarczających zasobów spróbuj wykonać zadanie bez rozpakowywania pliku na dysk).
4. Pobierz program iLEAPP (*https://github.com/abrignoni/iLEAPP*). Program został napisany w języku Python, dlatego należy przygotować środowisko (w zależności od dystrybucji możne wymagać instalacji kilku a nawet kilkunastu dodatkowych bibliotek – informacje będą znajdować się w komunikacie z błędu).

5. Pobierz i zainstaluj program DB Browser for SQLite (*sudo apt install sqlitebrowser*).
6. Pobierz i zainstaluj program Plistutil (*sudo apt-get install libplist-utils*).

```
┌──(kali㉿kali)-[~/Desktop]
└─$ plistutil -h
Usage: plistutil [OPTIONS] [-i FILE] [-o FILE]

Convert a plist FILE from binary to XML format or vice-versa.

OPTIONS:
  -i, --infile FILE       Optional FILE to convert from or stdin if - or not used
  -o, --outfile FILE      Optional FILE to convert to or stdout if - or not used
  -f, --format [bin|xml]  Force output format, regardless of input type
  -d, --debug             Enable extended debug output
  -v, --version           Print version information

Homepage:    <https://libimobiledevice.org>
Bug Reports: <https://github.com/libimobiledevice/libplist/issues>
```

Proszę o przygotowanie raportu z zadania w formie pdf. Raport powinien składać się z zrzutów ekranu z wykonania poszczególnych podpunktów wraz z opisem uzyskanych rezultatów.

Zadanie 1 – Zawartość baz danych systemu IOS

1. Przejdź do folderu Accounts (*~/.../private/var/mobile/Library/Accounts*). Otwórz bazę danych znajdującą się w pliku Accounts3.sqlite:

```
┌──(kali㉿kali)-[~/…/var/mobile/Library/Accounts]
└─$ sqlite3 Accounts3.sqlite
SQLite version 3.36.0 2021-06-18 18:36:39
Enter ".help" for usage hints.
```

Przy pomocy zapytań SQLite wyświetl dane znajdujące się wewnątrz tabeli (SELECT*) i odpowiedz na pytania:
a. Ile adresów email znajduje się w analizowanej bazie danych (użytkownika)?
b. Podaj odszukane adres/y.
c. Czy któryś z adresów został podpięty do iCloud? Jeśli tak, to który?
d. Czy użytkownik tego systemu posiadał podpięte konto Gmail?
e. Podaj wartość z tabeli ZDATE. Jaką informacje skrywa ta wartość?
2. Przejdź do pliku lightspeed-100046799400843.db, otwórz go za pomocą programu DB Browser for SQLite i odpowiedz na pytania: *(/private/var/mobile/Containers/Shared/AppGroup/1F111E46-8DC5-4457-8C8A- 31470BAB279E/lightspeed-100046799400843.db* - wskazany plik zawiera informacje z portalu Facebook).
a. Odszukaj ID (thread_key) właściciela urządzenia.
b. Do kogo należy thread_key o nr 100030845613112?
c. Odszukaj z bazy informacje o emoji, ile ich tam się znajduje?
d. Wyświetl informacje z „messages”, czy w pliku znajdują się wiadomości tekstowe?
e. Dodatkowo określ liczbę osób biorących udział w rozmowie i podaj ich ID.
f. Rubryka *timestamp_ms* zawiera informacje o „czasie”. Podaj w jakie dni była prowadzona rozmowa pomiędzy użytkownikami, w tym celu napisz prosty program, który przekonwertuje wybrane wiersze i wskaże ich poprawny czas wykorzystując do tego np. konsolową wersje Pythona (może być PHP, JS, itp.)

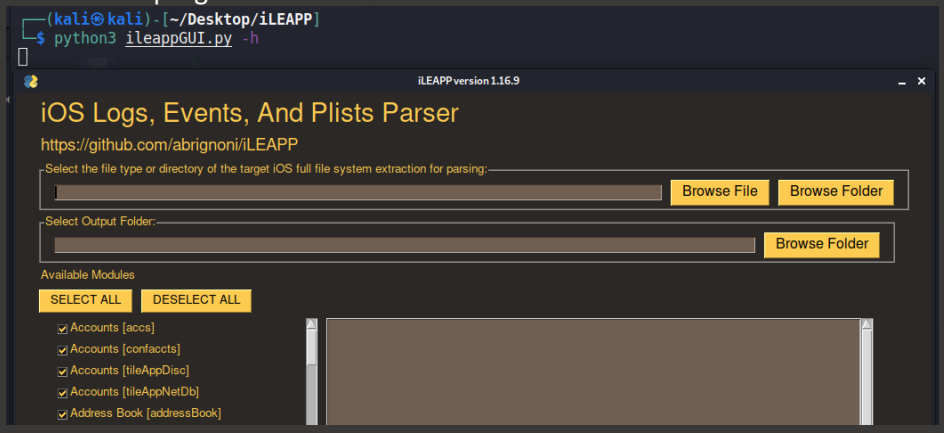
Zadanie 2 – Pliki plist

1. Opisz do czego służą w systemie IOS pliki o rozszerzeniu .plist?
2. Do jakiej postaci można konwertować ww. pliki?
3. Przy pomocy programu Plistutil wyświetl informacje zawarte w pliku i odpowiedz na pytanie, jakie informacje znajdują się wewnątrz badanego pliku (podaj kilka przykładów).

```
┌──(kali㉿kali)-[~/…/private/var/preferences/SystemConfiguration]
└─$ plistutil -i com.apple.wifi.plist
```

Zadanie 3 – Automatyzacja analizy plików systemu IOS

1. Uruchom program iLEAPP:



2. Wybierz z listy pobrany plik 13-3-1.tar oraz ustaw miejsce ekstrakcji pliku z programu.
3. Zaznacz wszystkie moduły ekstrakcji danych (default).
4. Uruchom proces.
5. Przejdź do folderu outputowego i odszukaj plik index.html (otwórz go), a następnie przeprowadź analizę raportu w oparciu o uzyskane dane. Analiza powinna składać się ze wszystkich najistotniejszych informacji m.in. o osobie, miejscu, czynności i czasie.

Rozwiązania zadań muszą zawierać zrzuty ekranów ze wszystkich wykonanych elementów oraz szczegółowy opis uzyskanych rezultatów.