Badania uszkodzonych urządzeń mobilnych – studium przypadku

podkom. Marcin Napiórkowski[1]
ORCID 0009-0009-3499-000X

1 Laboratorium Kryminalistyczne Komendy Wojewódzkiej Policji w Szczecinie, marcin.napiorkowski@sc.policja.gov.pl

Streszczenie

Artykuł porusza tematykę badania urządzeń mobilnych uszkodzonych w wyniku zalania. Urządzenia te w obecnych czasach towarzyszą nam niemalże bez przerwy i gromadzą wiele informacji, z tego powodu są cennym i często niezastąpionym rzeczowym źródłem dowodowym. Odczytane dane mogą pełnić szczególną rolę w procesie karnym, ich pozyskanie ze sprawnych i niezablokowanych urządzeń nie powinno przysporzyć większego problemu dla wprawnego informatyka śledczego. Nieco więcej wkładu pracy wymagane jest przy pozyskiwaniu danych z urządzeń, które zostały uszkodzone, np. umyślnie lub w wyniku nieszczęśliwego zdarzenia.

Słowa kluczowe: Informatyka śledcza, badania informatyczne, odzysk danych, urządzenia mobilne

Wstęp

Badania urządzeń mobilnych (telefony i tablety) w policyjnych laboratoriach kryminalistycznych z punktu widzenia biegłego często skupiają się na doborze odpowiedniej metody akwizycji danych. Ich odczyt w trybie logicznym niejednokrotnie jest ograniczony i niewystarczający, dąży się do pozyskania fizycznego obrazu pamięci, co umożliwia odtworzenie jeszcze większej ilości danych, np. usuniętych lub z obszarów systemowych. Tak pozyskane dane interpretuje się zgodnie z żądaniem zlecającego do odpowiedniego raportu. Producenci urządzeń mobilnych z oczywistych względów posiadania w telefonach i tabletach szeregu aplikacji finansowych, społecznościowych, komunikatorów, etc. dbają o ochronę danych swoich użytkowników i stosują coraz skuteczniejsze zabezpieczenia. Dlatego pozyskanie dostępu do informacji zawartych w urządzeniu staje się coraz trudniejsze. Nie jest tajemnicą, że współczesne urządzenia przechowują dane z wykorzystaniem algorytmów szyfrujących, ich skomplikowanie sprawia, że próba przełamania zabezpieczenia jest bardzo czasochłonna bądź praktycznie niemożliwa. Kolejnym utrudnieniem jest rozmiar przestrzeni pamięci urządzeń, aplikacje przechowują coraz to więcej danych, a treści multimedialne zapisywane są w wysokich rozdzielczościach. Na dzień dzisiejszy często zdarzają się w badaniach urządzenia o zasobach pamięci 512GB, których akwizycja i analiza zajmuje wiele czasu. Prawdziwe wyzwanie pojawia się gdy urządzenie jakie trafia do badań jest uszkodzone lub nie do końca sprawne. Opisywany poniżej przypadek przedstawia zastosowanie metody badawczej wobec telefonu i tabletu marki Apple.

Opis przypadku

Do pracowni badań informatycznych Laboratorium Kryminalistycznego Komendy Wojewódzkiej Policji w Szczecinie w celu wykonania badań trafiły dwa urządzenia, tj. telefon marki Apple model iPhone 6S i tablet iPad 2 tej samej marki. Ponadto zlecający poinformował, że przedmiotowe urządzenia zostały ujawnione na dnie rzeki Odry, w której znajdowały się przez około sześć miesięcy. Na pochwałę zasługuje fakt, że materiał dowodowy został zabezpieczony w opakowania papierowe, co pozwoliło na odprowadzenie części wilgoci. Z wydanego postanowienia wynikało, że ujawnione przedmioty zostały nadesłane w związku z podejrzeniem o dokonanie zabójstwa

i należały do ofiary. Samo postanowienie zawierało standardowe pytania dotyczące odczytania plików graficznych i wideo, korespondencji prowadzonej z użyciem wiadomości SMS/MMS oraz komunikatorów internetowych.

Badania rozpoczęto od rozpakowania materiału (Ryc. 1 i 2), fotograficznego utrwalenia ich stanu fizycznego (Ryc. 3-8), oczyszczenia z luźnych zanieczyszczeń oraz osuszenia w temperaturze pokojowej w przewiewnym i suchym pomieszczeniu. Suszenie urządzeń rozpoczęto od ich rozmontowania (Ryc. 9), odłączenia baterii i zdemontowania kluczowego elementu jakim jest płyta główna zawierająca nośnik pamięci.

Ryc. 1. Papierowe opakowanie zbiorcze materiału dowodowego.
Źródło: zasoby własne

Ryc. 2. Indywidualne opakowanie materiału dowodowego.
Źródło: zasoby własne

Ryc. 3. Tablet, widok z przodu.
Źródło: zasoby własne

Ryc. 4. Tablet, widok z tyłu.
Źródło: zasoby własne

Ryc. 5. Tablet, widok od strony złącza typu 30-pin.
Źródło: zasoby własne

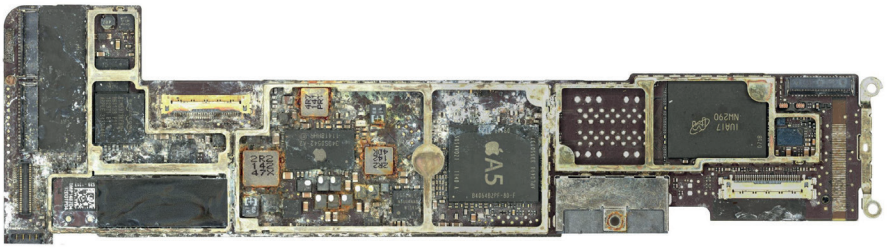
Ryc. 6. Telefon, widok z przodu.
Źródło: zasoby własne

Ryc. 7. Telefon, widok z tyłu.
Źródło: zasoby własne

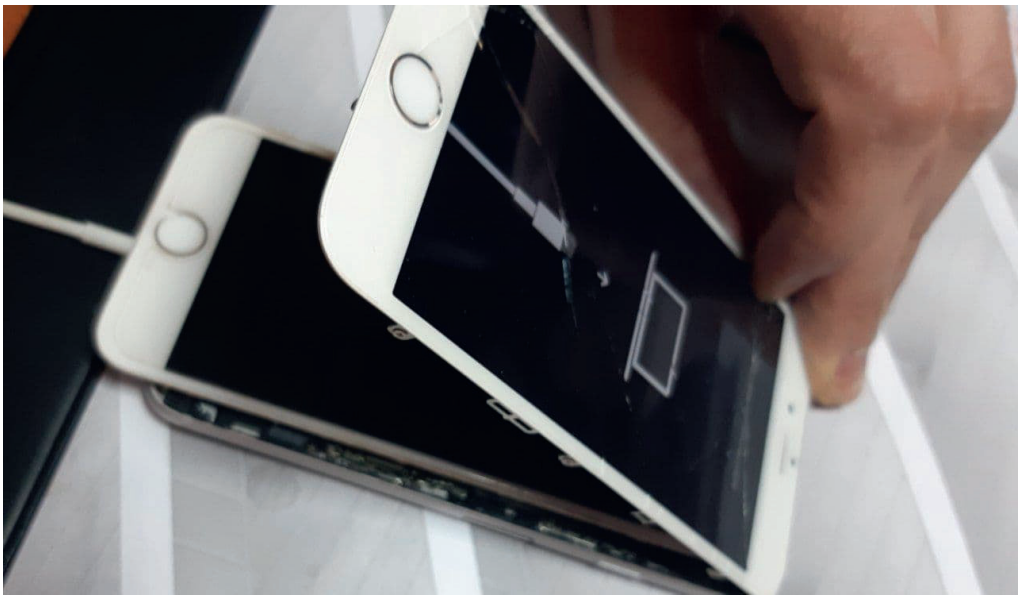
Ryc. 8. Telefon, widok od strony złącza typu Lightning.
Źródło: zasoby własne

W urządzeniu iPad 2 zauważyć można wybrzuszenie ekranu (Ryc. 5), które spowodowane jest zmianą objętości baterii. Nie jest to nic niezwykłego wśród niesprawnych ogniw litowo-jonowych, dzieje się tak w skutek nagromadzenia gazów w szczelnym pakiecie baterii. Do takiej sytuacji dochodzi np. w wyniku nadmiernego rozładowania bądź uszkodzenia kontrolera nadzorującego stan baterii. Na płytach głównych urządzeń znajdowały się również elementy ekranujące w postaci specjalnych etykiet samoprzylepnych i pokryw metalowych, które mogłyby utrudnić proces suszenia, dlatego zostały one zdemontowane (Ryc. 10). Przy użyciu miękkiej szczoteczki, 2% roztworu płynu do czyszczenia w myjkach ultradźwiękowych (Tech-Sonic) i wody destylowanej usunięto luźne zanieczyszczenia z obu płyt głównych urządzeń. Kolejnym krokiem może być dokładne oczyszczenie układu w wanience ultradźwiękowej, ale LK KWP w Szczecinie nie dysponuje osprzętem mogącym pomieścić tak duży element. Do ponownego suszenia użyto kolby hotair o nastawieniu temperatury 100°C i odległości od układu około 20cm. Ponadto do usunięcia wilgoci, która mogła zgromadzić się pod układami o dużej powierzchni użyto sprężonego powietrza. Metody tej należy używać bardzo ostrożnie w związku z niebezpieczeństwem oderwania i utraty naruszonych komponentów. Wzrokowo nie ujawniono żadnych uszkodzeń. Następnie na płycie głównej urządzenia iPad 2 zidentyfikowano główną linię zasilania, na której nie stwierdzono zwarcia z masą. Z Wydziału Łączności i Informatyki KWP w Szczecinie pozyskano tożsame urządzenie, w którym podmieniono płytę główną na zdemontowaną z urządzenia dowodowego. Tablet pomimo podłączenia zasilania nie uruchamiał się. W urządzeniach mobilnych marki Apple podłączenie wyłączonego telefonu bądź tabletu do źródła zasilania powoduje jego automatyczne uruchomienie. Dlatego dokonano dokładnej inspekcji płyty głównej z użyciem mikroskopu i tak np. tylko w obszarze złącza (J2201) stwierdzono destrukcyjne działanie wody, w miejscach styku cyny z polem miedzianym nastąpiło utlenienie ścieżki. Dzięki ogólnodostępnym w sieci Internet schematom płyty głównej istnieje możliwość mostkowania połączeń, kolejną metodą naprawienia tej usterki jest zdrapanie maski ochronnej z powierzchni ścieżki i przedłużenie jej. Z uwagi na brak lutownicy precyzyjnej w LK KWP w Szczecinie usterka ta nie może zostać usunięta, próba odczytu danych zakończyła się niepowodzeniem.

Ryc. 9. Widok wnętrza telefonu.
Źródło: zasoby własne



Ryc. 10. Widok zdemontowanej płyty głównej tabletu.
Źródło: zasoby własne



Ryc. 11. Telefon iPhone podczas uruchamiania.
Źródło: zasoby własne

W badaniach płyty głównej telefonu iPhone postępowano analogicznie jak w przypadku urządzenia iPad. Zdemontowano elementy ekranujące, przy użyciu miękkiej szczoteczki i roztworu usunięto luźne zanieczyszczenia. W celu dokładnego wyczyszczenia płyty głównej użyto wanienki ultradźwiękowej z roztworem o stężeniu jak powyżej, czas pracy ustawiono na trzy minuty. Wzrokowo nie ujawniono żadnych uszkodzeń. Na płycie głównej zidentyfikowano główną linię zasilania, na której nie stwierdzono zwarcia z masą. WŁiI KWP w Szczecinie nie był w stanie dostarczyć tożsamego urządzenia, dlatego tzw. dawcę pozyskano ze źródeł zewnętrznych, ale z uszkodzonym przyciskiem znajdującym się pod ekranem Home Button. Podmieniono płytę główną na zdemontowaną z urządzenia dowodowego, podłączono do zasilania i telefon uruchomił się. Na tym etapie pojawił się problem, o którym wspomniałem we wstępie, telefon wyświetlił monit z prośbą o podanie kodu PIN blokady użytkownika, który nie jest znany. Zawarte w telefonie dane zabezpieczone są przed nieuprawnionym dostępem przy pomocy sześciocyfrowego kodu PIN, co daje 1 000 000 możliwych kombinacji. Telefon iPhone 6S wyposażony jest w procesor Apple 9, podatny na atak słownikowy, którego można dokonać z wykorzystaniem specjalistycznego oprogramowania w trybie DFU (Device Firmware Upgrade). Wprowadzenie telefonu w tryb DFU wymaga użycia fizycznych przycisków, bocznych i znajdującego się pod ekranem Home Button (który w urządzeniu zastępczym jest uszkodzony). Konstrukcja panelu przedniego telefonu zbudowana jest z trzech podstawowych komponentów, tj. wyświetlacza, digitizera (elementu odpowiedzialnego za detekcję dotyku na ekranie) i przycisku Home Button. Każdy z nich połączony jest z płytą główną za pośrednictwem osobnego przewodu zakończonego wtyczką, dlatego istnieje możliwość wykorzystania przycisku Home Button znajdującego się na dowodowym ekranie (Ryc. 11). W tej konfiguracji telefon wprowadzono w tryb DFU i rozpoczęto procedurę przełamywania zastosowanego zabezpieczenia. Czynność ta odbywa się na telefonie z prędkością około sześciu haseł na minutę. Zaledwie po 17 godzinach właściwy PIN został ujawniony, co pozwoliło na ekstrakcję danych w trybach FFS (Full File System) oraz Checkm8.

Wnioski

Pomimo zastosowanych czynności badawczych, nie odczytano zawartości pamięci urządzenia. Tutejsze laboratorium nie posiada technicznych możliwości naprawienia urządzenia. W pamięci urządzenia iPhone ujawniono treści w postaci wiadomości SMS/MMS, korespondencji prowadzonej przy użyciu komunikatorów Facebook Messenger, Grindr, iMessages, Instagram, WhatsApp, a także pliki audio oraz wideo.