

Технічні науки

УДК 004.008

Золотарьов Сергій Олександрович

*головний судовий експерт відділу
комп'ютерно-технічних та телекомунікаційних досліджень
Харківський науково-дослідний
експертно-криміналістичний центру МВС України*

Золотарёв Сергей Александрович

*главный судебный эксперт отдела
компьютерно-технических и телекоммуникационных исследований
Харьковский научно-исследовательский
экспертно-криминалистического центр МВД Украины*

Zolotarov Serhii

*Chief Forensic Expert of the Department of
Computer and Telecommunication Studies of
Kharkiv Scientific Research Forensic Center of the
Ministry of Internal Affairs of Ukraine*

РОЗУМНІ ГОДИННИКИ ЯК ОБ'ЄКТ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

УМНЫЕ ЧАСЫ КАК ОБЪЕКТ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

SMARTWATCH AS AN OBJECT OF COMPUTER FORENSICS INVESTIGATIONS

***Анотація.** У статті розглянуто поняття розумного годинника, наведено існуючі різновиди розумних годинників їх функціональні можливості та особливості. Проведено короткий аналіз популярних операційних систем (WearOS, Tizen OS, watchOS, Android) якими*

керуються розумні годинники, наведено дані, які зберігаються серед вмісту пам'яті розумних годинників та можуть бути використані у якості доказової бази під час розслідування правопорушень, визначено методи (логічні та фізичні) якими можливо вилучити та дослідити ці дані з урахуванням особливостей вилучення для кожного методу.

Ключові слова: розумний годинник, стільниковий (мобільний) телефон, операційна система, Android, iOS, функції, методи, дослідження, вилучення інформації.

Аннотація. В статті рассмотрено понятие умных часов, приведены существующие разновидности умных часов их функциональные возможности и особенности. Проведен краткий анализ популярных операционных систем (WearOS, Tizen OS, watchOS, Android), которыми руководствуются умные часы, приведены данные, которые хранятся среди содержимого памяти умных часов и могут быть использованы в качестве доказательной базы при расследовании правонарушений, определены методы (логические и физические), которыми возможно изъять и исследовать эти данные с учетом особенностей изъятия для каждого метода.

Ключевые слова: умные часы, сотовый (мобильный) телефон, операционная система, Android, iOS, функции, методы, исследования, извлечения информации.

Summary. The article deals with the concept of a smart watch, presents the existing varieties of smart watches, their functionality and features. A brief analysis of popular operating systems (WearOS, Tizen OS, watchOS, Android), which controls smart watches, lists data stored in the contents of memory of smart watches and can be used as evidence in the investigation of offenses, methods (logical and physical) that can be extracted and investigated, taking into account the specific features of the extraction for each method.

Key words: *smart watch, cellular (mobile) phone, operating system, Android, iOS, features, methods, research, retrieve of the information.*

Стрімкий розвиток інформаційних і комунікаційних технологій з кожним роком створює нові можливості для полегшення взаємодії між людьми, розширюючи засоби і способи для комунікації. З цим пов'язаний розвиток комп'ютерної техніки, розвиток мобільних пристроїв – стільникових (мобільних) телефонів, розвиток технологічного процесу у цілому, посилення інтеграції соціальних мереж у життя людей, все це прямо пропорційно впливає на розвиток цифрової криміналістики, кількість об'єктів, які можуть бути досліджені судовими експертами, які проводять дослідження за напрямком 10.9 «Дослідження комп'ютерної-техніки та програмних продуктів». До таких об'єктів можна віднести розумні годинники (англ. Smartwatch), про актуальність та значущість яких, як відносно нового об'єкта цифрової криміналістики піде мова у цій статті.

Розумний годинник (англ. Smartwatch) – комп'ютеризований наручний пристрій, який окрім вимірювання часу виконує додаткові функції: прийом сповіщень та дзвінків зі стільникового (мобільного) телефону (у разі наявності розніму для SIM-карт), відстеження маршрутів, збір інформації із вбудованих та зовнішніх датчиків, наприклад, акселерометра, відтворення мультимедіа контенту, тощо.

За цільовим призначенням розумні годинники умовно можна розділити на годинники для загальних потреб та спортивні годинники. Пристрої для загальних потреб можуть виконувати функції камери, GPS навігатора, мультимедійного плеєра, мати доступ до мережі Інтернет, тощо. Спортивні годинники, окрім названих функцій, мають додаткові, призначені для поглибленого контролю та аналізу фізичної активності

користувача, як приклад можна привести моніторинг серцевого ритму, підрахунок пройденої дистанції у кроках, кілометрах та інше.

Якщо на початку можливості розумних годинників були тісно пов’язані зі стільниковими (мобільними) телефонами, то вже на даному проміжку часу удосконалення існуючих функцій розумних годинників та впровадження нових все більше роблять ці пристрої повноцінними та незалежними від інших пристроїв. Більшість випущених після 2013 року розумних годинників керуються операційними системами Wear OS (раніше – Android Wear), Tizen, watchOS, а також збільшується кількість розумних годинників, які керуються повноцінною операційною системою Android. Керовані зазначеними операційними системами розумні годинники можуть містити унікальні дані мережевої активності користувача, файли користувача або їх фрагменти, інформацію про додатки та їх налаштування та іншу інформацію, яка може бути досліджена судовими експертами, які проводять дослідження за напрямком 10.9 «Дослідження комп’ютерної-техніки та програмних продуктів».

Розглянемо особливості деяких операційних систем, які використовуються на розумних годинниках:

- Wear OS (раніше відома як Android Wear) – версія операційної системи Google Android, створена для розумних годинників та інших переносних пристроїв. При з’єднанні смартфона на Android версії 4.3+ та розумного пристрою, Android Wear інтегрує в нього функціональність асистента Google і дозволяє отримувати вхідні повідомлення із смартфона на переносний пристрій;
- Tizen OS – операційна система розроблена у 2011 році для широкого спектру мобільних пристроїв, включаючи планшети, нетбуки, смартфони, телевізори та автомобільні інформаційно-розважальні системи, на даному етапі використовується на розумних годинниках

які виготовляються компанією SAMSUNG. Як і випадку з операційною системою Wear OS для повного доступу до функцій розумного годинника необхідна постійна взаємодія із стільниковим (мобільним телефоном).

— watchOS – операційна система від корпорації Apple, що була спеціально розроблена для розумних годинників Apple Watch. Операційна система підтримує сторонні додатки, має функцію голосового помічника, мапи, календар, нагадування, блокнот, і власне годинник. WatchOS розроблена виключно під розумний годинник Apple Watch і не пристосована для роботи на будь-якому іншому пристрої. Вперше випущена 24 квітня 2015 року [1].

Проведеним аналізом вищезазначених операційних систем, встановлено, що на даному етапі керовані операційними системами Wear OS, Tizen OS та watchOS розумні годинники тісно поєднані зі стільниковим (мобільним) телефоном власника, та без постійної взаємодії один із одним (синхронізації) розумний годинник має обмежений функціонал та не може самостійно приймати, або відправляти сповіщення, повідомлення, виклики, у деяких випадках має обмежений доступ до мережі Інтернет. Розумні годинники на базі операційних систем Wear OS, Tizen OS та watchOS окрім даних фізичної активності користувача можуть зберігати частину даних отриманих з стільникового (мобільного) телефону, або пристрою з яким проводиться синхронізація. Такими даними можуть бути:

- синхронізовані фотографії або їх фрагменти;
- частини повідомлень;
- налаштування деяких додатків;
- дані пересування користувача;
- дані службових журналів
- дані підключень.

Вилучити зазначені дані можливо шляхом створення резервної копії пам'яті розумного годиннику з подальшим її дослідженням за допомогою спеціального програмного забезпечення [2].

Окремо слід виділити розумні годинники, які керуються операційною системою Android [3]. Здебільшого розумні годинники на базі операційної системи Android позиціонуються як самостійний пристрій, який схожий у порівнянні зі стільниковим (мобільним) телефоном, адже також мають рознім для SIM-карт, бездротові інтерфейси Bluetooth та Wi-Fi, а також достатні об'єми внутрішньої пам'яті (у деяких випадках з можливістю розширення картами пам'яті формату microSD) тому незалежно від стільникового (мобільного) телефона можуть виконувати наступні функції:

- прийняття та здійснення дзвінків;
- створення, відправлення та прийняття текстових SMS, та мультимедійних MMS-повідомлень;
- доступ до мережі Інтернет;
- створення, обмін файлами та інше.

Всі ці функції необмежені обв'язкою синхронізацією з пристроями користувача, тому на відміну від розумних годинників з іншими операційними системами, розумні годинники на базі операційної системи Android можуть бути більш цікавими для ініціатора проведення експертизи, адже вони можуть містити серед вмісту внутрішньої пам'яті інформацію стосовно скоєння можливого правопорушення, яка може бути представлена у вигляді:

- листування засобами електронного зв'язку та іншої мережевої активності;
- файлів створених або отриманих користувачем, а саме: текстових файлів, файлів електронних таблиць, файлів електронних документів, графічних та відеофайлів, тощо.

Судовими експертами, які проводять дослідження за напрямком 10.9 «Дослідження комп’ютерної-техніки та програмних продуктів» можуть бути досліджені розумні годинники, які керуються операційною системою Android за наявності необхідних знань, наявності спеціального програмного забезпечення, спеціалізованого обладнання та за рахунок того, що більшість розумних годинників, які керуються операційною системою Android мають уніфікований інтерфейси підключення типу USB micro B, USB type C, рідше USB type B (Ілюстрація 1), а також процесорів компанії Mediatek, які широко використовують у розумних годинниках та стільникових (мобільних) телефонах.



Рис. 1. Уніфікований інтерфейси підключення типу USB type A, USB type B, USB type C, USB micro B

Як і у випадках із мобільними (стільниковими) телефонами, для проведення судовим експертом вищевказаного дослідження, у документі (ухвалі) про призначення судової комп’ютерно-технічної експертизи

ініціатором повинний бути наданий дозвіл на часткову або повну зміну властивостей об’єкта.

Для дослідження вмісту розумних годинників, які керуються операційною системою Android, як і у випадку із стільниковими (мобільними) телефонами, які керуються операційною системою Android для надання відповіді на поставлені ініціатором перед судовим експертом питання можуть бути використані наступні методи дослідження інформації, які відрізняються своєю ефективністю та складністю:

- логічне вилучення даних;
- знаття резервної копії даних Android;
- фізичний дамپ пам’яті пристрою;
- JTAG/Chip-off/ISP;

Метод «Логічне вилучення даних» – найменш ефективний, але найпростіший метод для витягування інформації із пам’яті розумного годинника. Зазвичай для читання даних пристрій, який надано на дослідження підключається до робочої станції експерта за допомогою кабелів передачі даних та досліджується за допомогою спеціального програмного забезпечення, яке автоматично встановлюється в пристрій, та автоматично видаляється після завершення процедури витягування інформації. Якщо з якої-небудь причини кабельне з’єднання було розірвано або програма закрилася з помилкою, процес необхідно повторити. В основному даний метод можна застосовувати для всіх пристроїв з ОС Android, але дає доступ тільки до основних розділів програми: контакти, повідомлення, календар, дзвінки, файли з карти пам’яті.

Метод «Резервна копія Android» (для пристроїв з ОС Android 4.0 і вище) – з пристрою витягуються дані, які зберігаються в резервної копії. Кожен виробник додатку сам вирішує, що буде збережено в резервної копії. Цей метод витягує менше, ніж фізичний, але на відміну від логічного методу дає доступ до додатків та у деяких випадках видалених даних.

Метод «Фізичний дамп» – один із найефективніших методів, але у свою чергу важкий за рахунок різноманіття особливостей починаючи від виробника пристрою, можливості та способу отримання рут-доступу (root права, або розширені права користувача), типу процесору та інше. З пристрою витягується повна копія пам'яті пристрою (і карти пам'яті, якщо вона присутня в пристрої). Для вилучення даних цим методом пристрій повинен мати рут-доступ (він може бути отриманий в ході вилучення). Витягуються наступні дані:

- веб з'єднання;
- журнал подій;
- файли користувача (текстові, графічні, відеофайли та інші файли, з можливістю відновлення видалених файлів);
- інформація щодо облікових записів користувача;
- об'єднані контакти;
- органайзер (нотатки, календар);
- збережені дані користувача (логіни та паролі);
- повідомлення (SMS/MMS/повідомлення клієнтів соціальних мереж/електронні листи);
- дані додатків.

JTAG/Chip-off/ISP – найбільш складні методи вилучення інформації із пристрою, які потребують розібрати пристрій (Ілюстрація 2) для отримання доступу до печатної (материнської) плати пристрою, а також наявності у розпорядженні експерта спеціального обладнання, набору інструкцій та поглиблених знань у області схемотехніки.

Joint Test Action Group (JTAG) – галузевий стандарт, розроблений для тестування друкованих плат (PCB) з використанням граничного сканування і був розроблений для швидкого та легкого тестування друкованих плат, що виходять з виробничої збірної лінії. JTAG Forensics – це процес, який використовує той самий процес і включає підключення

тестових портів доступу (TAP) на друкованій платі, та за допомогою набору інструкцій вилучає та обробляє дані з мікросхеми пристрою через JTAG Box (Riff, Z3X, ATF тощо) для отримання повного фізичного образу пристрою.



Рис. 2. Складові частини розібраного розумного годинника Samsung Gear S3

Chip-off Forensics – процес, під час якого чіп пам'яті BGA видаляється з пристрою та досліджується окремо за допомогою зчитувача мікросхем. Зчитувач мікросхем (програматор), необхідний для виконання зчитування та обробки вилучених даних, для цього потрібен певний адаптер залежно від конкретного типу мікросхеми. На відміну від JTAG, видалення мікросхеми є руйнівним процесом і пристрій більше не працюватиме.

Внутрішньосистемне програмування (ISP) – це практика підключення до мікросхеми флеш-пам'яті (eMMC або eMCP) з метою

завантаження повного вмісту пам'яті пристрою. eMMC та eMCP-пам'ять – це стандарт у сучасних пристроях (смартфонах), який дозволяє безпосередньо відновлювати повний дамп даних, не виймаючи мікросхему та не знищуючи пристрій, особливістю виступає той факт, що для проведення процедури внутрішньосистемного програмування необхідний аналогічний наданому на дослідження пристрій-донор, що робить цей метод одним із найскладніших, непрактичних та затратних методів.

Подальший розвиток розумних годинників, збільшення їх кількості, розмаїття та розширення цінового діапазону, вплине на коло ймовірних власників (у тому числі ймовірних злочинців), а тому, у майбутньому, може вплинути на частоту надходжень розумних годинників, як об'єкта дослідження комп'ютерно-технічної експертизи.

Удосконалення методичних рекомендацій, у тому числі поглиблений аналіз можливих проблемних питань, які можуть виникнути у процесі дослідження є актуальним вже зараз, а узагальнення вже існуючих напрацювань дозволить судовим експертам в повній мірі заповнити той інтерес у цифровій криміналістиці, та дозволить у майбутньому надати вичерпні відповіді на виникаючі питання, адже дослідження розумних годинників лише починається.

Література

1. Mattia Epifani. Learning iOS Forensics / Mattia Epifani, Pasquale Stirparo. Packt Publishing 2015. 220 p.
2. Mattia Epifani. Learning iOS Forensics - Second Edition / Mattia Epifani, Pasquale Stirparo. Packt Publishing 2015. 330 p.
3. Donnie Tindall. Learning Android Forensics: Analyze Android devices with the latest forensic tools and techniques / Donnie Tindall, Rohit Tamma. Packt Publishing, 2018. 328 p.