СЪДЕБНИ ТЕХНИЧЕСКИ ЕКСПЕРТИЗИ НА iOS МОБИЛНИ УСТРОЙСТВА

Силвия Лецковска, Камен Сейменлийски
Георги Рачев, Елдар Заеров
Бургаски свободен университет

FORENSIC TECHNICAL EXPERTISES OF iOS MOBILE DEVICES

Silviya Letskovska, Kamen Seymenliyski
Georgi Rachev, Eldar Zaerov
Burgas Free University

Abstract: *The mobile device is now a part of our life and is a huge repository that stores sensitive and personal information about its owner. Because of this, mobile devices have become an object of study in forensics. A branch of digital forensics has been created that deals with the extraction of data from a mobile device. The aim of the present study is to investigate the methodology for extracting information from a digital device without changing the data present on it.*

Keywords: *mobile device, digital forensics, forensics.*

Въведение:

За да отговори на съвременните изисквания, криминалистиката трябва активно да проучва проблемите при проверката и изследване на мобилните устройства и да развива методите за анализ на информацията, съдържаща се в тях. Всъщност вече можем да се говори за развитие на подотрасъл *дигитална криминалистика*, който условно може да се нарече „мобилна криминалистика“ (криминалистика на мобилни устройства.

Криминалистиката на мобилните устройства като област на изследване датира от края на 90-те и началото на 2000-та година. Ролята на мобилните телефони в престъпността отдавна е призната от правоприлагащите органи. С нарастващата наличност на такива устройства на потребителския пазар и разширяването на гамата от поддържани от тях комуникационни платформи (например електронна поща, уеб сърфиране, приложения за комуникация, споделяне на файлове и използване на мобилното устройство като платежно средство), ролята на криминалистичните изследвания в областта значително нарастна [1].

Ранните опити за изследване на мобилни устройства използват методи, подобни на първите компютърни съдебни разследвания: анализиране на съдържанието на телефона директно през екрана и фотографиране на важното съдържание. Това обаче се оказа отнемащ време процес и тъй като броят на мобилните устройства започна значително да се увеличава и развива, изследователите бяха принудени да търсят по - ефективни средства за извличане на данни.

По-предприемчивите от тях понякога използват софтуер за резервно копие на мобилен телефон или PDA, за да „резервират“ данните на устройството в компютър за изображения, а понякога просто извършват компютърно изследване на твърдия диск на процесния компютър, с помощта на който данните са били архивирани. Този тип софтуер може да записва на телефона, както и чете, но не може да възстанови изтритите данни [2].

Криминалистическото изследване на мобилни устройства е раздел от цифровата криминалистика, свързан с възстановяването на цифрови доказателства или данни от мобилно устройство. Терминът „Мобилно устройство” обикновено се отнася за мобилни телефони, обаче може да се отнася и за всяко едно цифрово устройство, което има както вътрешна памет, така и комуникационни възможности, включително PDA (Personal digital assistant), GPS (Global Positioning System) и таблети.

Много често мобилни телефони, други мобилни устройства или техни части се намират на мястото на задържане на заподозрени или в тяхно присъствие. Мобилните устройства могат или да се използват по предназначение, или да бъдат елементи на други устройства, които се използват за извършване на престъпление (например взривни устройства, кражба на самоличност, детска порнография, разпространение на наркотични вещества и др.).

По време на статичния етап на проверка на мобилно устройство се изследват неговите размери, модел, цвят, установява се наличието на капак или други принадлежности върху него, които предпазват устройството от повреда, рисунки върху тях, следи и повреди.

На динамичния етап на първо място се определя възможността за включване на телефона (реакция на бутона за захранване, други бутони, сензор за пръстови отпечатъци и др.). Следващата стъпка е да се установи фактът на инсталиране на защита и ограничаване на достъпа до смартфона от неупълномощени лица (парола, цифров код, шаблон, достъп с пръстови отпечатъци, достъп след сканиране на лицето на потребителя или ретината на окото му). При липса на парола или други мерки за сигурност се извършва подробна проверка на информацията, съхранявана на телефона.

Информацията за SIM картата е от голямо значение за разследването. Съхранява информация за международния идентификатор на мобилния абонат; списък с номерата, на които е звънял; данни за номерата, разпределени в специални групи (бързо набиране, любими или други), както и последните набрани номера; информация за последното местоположение на устройството (означава местоположението спрямо обслужващите станции); информация за доставчика; информация за предпочитани езици; системна информация и др.

Софтуерното оборудване, с което разполагат криминалистите, дава възможност да се анализират обажданията, получени към и от изследвания смартфон, като се вземе предвид информацията, съхранявана на всички инсталирани SIM карти. Специалистите могат да изградят графична схема на контактната система. По този начин може да се установи структурата на престъпната група, източниците на информация и ръководство. При по-нататъшно откриване на други телефони е възможно да се обобщят получените данни и да се изградят разширени схеми.

Повечето съвременни смартфони имат приложение „Галерия“, което събира снимки и видеоклипове; и веднъж отворени, снимките и видеоклиповете, изпратени чрез различни приложения за комуникация, също оставят следа в паметта на мобилното устройство.

Съдържанието на „Галерия” може да бъде от съществено значение за целите на разследване на престъпления. Често представители на незаконни въоръжени групировки активно използват фото и видеозапис на своите действия, тормоз над жертви и т.н.

В допълнение към прякото съдържание на снимките (присъствието на определени лица, терен, сгради и съоръжения, други елементи на ситуацията). Криминалистичната стойност може да има допълнителна информация, отбелязана върху рамката: дата, час на заснемане и GPS координати.

Метаданните на фотофайла също съдържат информация за часа и датата на заснемане на снимката, а в много случаи и допълнителни опции за снимане: бленда, скорост на затвора, ISO ниво, светкавица, филтри и др.

Друг компонент от информационното съдържание на съвременните смартфони са сензорите за геолокация. Работата на тези сензори се използва в много програми. В допълнение към горните геотагове в снимките, повечето съвременни смартфони имат карти и навигатори.

В процеса на изучаване на тези програми могат да се определят най-новите заявки за търсене на адреси, положени маршрути, междинни точки на маршрута; в допълнение, ключови точки (дом, работа и т.н.) могат да бъдат зададени от потребителя. Отчасти такива данни ще помогнат за установяване на маршрута за номиниране на заподозрените, подхода към обекта и др.

Голямо количество информация може да бъде получено чрез изследване на приложенията Planner и Notes. В „Planner”, като правило, се отбелязват значими събития за потребителя (рождени дни на познати и роднини, определени дати), както и планове за деня.

„Бележките“, подобно на обикновените хартиени тетрадки, могат да съдържат всякакви записи – от телефонни номера до разпределение на ролите в групата, ключове към кода, използван от съучастниците, списък с необходимите покупки и т.н.

Всички браузъри, инсталирани на смартфона, също са обект на внимателно проучване. В тях, дори ако телефонът е изключен от мрежите, се съхранява информация за последните отворени страници, заявки за търсене, отметки.

Паметта на смартфона може да съдържа текстови, видео, аудио или други файлове, „изтеглени” от потребителя, или аудио файлове, записани от потребителя на диктофон. Съдържанието на папките, в които се съхранява информация, трябва да се проучи чрез приложението „Explorer” на смартфона или с помощта на специални софтуерни системи. На първо място, на изследване подлежат директориите „Изтегляне”, „Музика”, „Документи” или подобни.

При проверка на телефона на заподозрян могат да бъдат открити инсталирани на него специализирани програми, например за изчисляване на балистичните траектории на снаряд или обема и точката на поставяне на взривни устройства в сграда, за прихващане и управление на системи за контрол на достъпа и наблюдение и т.н.

По-сложните разследвания се извършват от експерти чрез логически, физически, файлов анализ, включително с помощта на специализиран софтуер, който дори позволява отключване на защитени с парола смартфони.

Тези обстоятелства предопределят важността на бъдещи теоретични разработки и изготвянето на практически препоръки за работа с мобилни устройства за най-пълно и ефективно разследване на престъпления.

Методът на клониране на мобилни телефони/устройства в криминалистиката е широко използван от няколко години, но криминалистичните изследвания на мобилни устройства са сравнително нова област.

Разпространението на телефоните (особено на смартфоните) и на другите цифрови устройства на потребителския пазар създаде условия за търсене, които не отговаряха на възможностите на съществуващите техники за компютърна криминалистика.

Мобилните устройства могат да се използват за съхраняване на няколко вида лична информация, такива като: контакти, снимки, календари и бележки, SMS (Short Message Service) и MMS (Multimedia Messaging Service) съобщения. Смартфоните могат допълнително да съдържат видео, имейл, информация за сърфиране в мрежата, информация за местоположение и съобщения и контакти в социалните медии.

Нараства нуждата от съвременна мобилна криминалистика поради няколко причини, основните от които са:

- Използване на мобилни телефони за съхраняване и прехвърляне на лична и корпоративна информация;
- Използване на мобилни телефони при онлайн транзакции;
- Използване на мобилни телефони от органи на реда и престъпници.

Криминалистичното изследване на мобилните устройства може да бъде особено предизвикателно на няколко нива. Например, когато са налице доказателствени и технически проблеми – анализът на местоположението на клетката в резултат на използването на покритие при използването на мобилен телефон няма необходимата точност и прецизност.

Следователно, въпреки че е възможно да се определи приблизително зоната на разположение на клетката, от която е направено или получено обаждането, все още не е възможно да се каже с каквато и да е степен на сигурност, че обаждането от мобилен телефон е произлязло от точно определено местоположение, като например, жилищен адрес, няма точност при определяне на местоположението по отношение и на надморската височина.

За да останат конкурентоспособни, производителите на често променят форм факторите на мобилните телефони, файловите структури на операционната система, съхранението, услугите, периферните устройства и дори конекторите и кабелите.

Обемът на паметта продължава да расте поради търсенето на по-мощни миникомпютърни устройства [4].

Не само типовете данни непрекъснато се променят, но и начините, по които се използват мобилните устройства. Важно е и поведението в хибернация, при което процесите се спират, когато устройството е изключено или неактивно, но остава активно в същото време [2].

В резултат на тези проблеми има голямо разнообразие от инструменти за извличане на доказателства от мобилни устройства, никой инструмент или метод обаче не може да се използва за получаване на доказателства от всички типове устройства.

Ето защо специалистите в областта, особено тези, които желаят да се квалифицират като експерти в съда, трябва да преминат през обучение, с цел:

- Да познават всеки инструмент и метод и да могат да ги използват за получаването на доказателства;
- Да спазват изискванията на стандартите при изследване Daubert или стандарта Fry. Стандартът на Фрай, тестът на Фрай или тестът за общо приемане е тест, използван в съдилищата на Съединените щати за определяне на допустимостта на научни доказателства. Той предвижда, че експертно мнение, основаващо се на научен метод, е допустимо само, ако методът е общопризнат за надежден в съответната научна общност. Във федералния закон на Съединените ща-

ти стандартът на Daubert е доказателственото правило по отношение на допустимостта на показанията на експертни свидетели.

Мобилните телефони в качеството на лични електронни устройства се използват за изпълнение на прости комуникационни задачи – провеждане на разговори, изпращане на текстови съобщения, сърфиране в интернет, изпращане и получаване на имейл, правене на снимки и видеоклипове, създаване и съхраняване на документи, идентифициране на местоположения с GPS услуги и управление на бизнес задачи.

Тъй като новите функции и приложения се вграждат в мобилните телефони, количеството информация, съхранявана на устройствата, непрекъснато нараства.

Мобилните телефони стават преносими носители на данни и те следят движенията на човека. С нарастващото им разпространение в ежедневието на хората и в престъпността данните, придобити от телефоните, се превръщат в безценен източник на доказателства за разследвания, свързани с наказателни и граждански дела. Рядко се провежда дигитално криминално разследване, което да не включва телефон. Дневниците за обаждания на мобилни устройства и GPS данните се използват при разследване на криминалистични престъпления.

Дигиталната криминалистика е клон на криминалистиката, фокусиращ се върху възстановяването и разследването на сурови данни от електронни или цифрови устройства. Целта на процеса е да извлече информация от дигитално устройство, без да променя данните, присъстващи на него.

През годините дигиталната криминалистика се развива интензивно наред с бързия растеж на в развитието на компютрите и различните видове цифрови устройства.

Има различни клонове на дигитална криминалистика, базирани на вида на цифрово устройство – компютърна криминалистика, мрежова криминалистика, мобилна криминалистика и т.н. Възстановяването на цифрови доказателства от мобилни телефони се нарича Mobile Forensics (мобилна криминалистика).

Цифровите доказателства се определят като информация и данни, които се съхраняват, получават или предават от електронно устройство, което се използва при разследвания.

Мобилната криминалистика е клон на дигиталната криминалистика, свързана с възстановяването на цифрови доказателства от мобилни устройства.

Основният принцип за стабилно криминалистично изследване на цифрови доказателства, който трябва да се спазва, е оригиналните доказателства да не бъдат променяни.

В случаите, когато изследването или придобиването на данни не е възможно без промяна на конфигурацията на устройството, процедурата и промените трябва да бъдат тествани, валидирани и документирани.

Следването на правилна методология и насоки е от решаващо значение при разглеждането на мобилни устройства, тъй като дава най-ценните данни. Неспазването на правилната процедура може да доведе до загуба или увреждане на доказателства или да го направи недопустим в съдебно дело.

Мобилната криминалистика включва три основни дейности:

- Изземване;
- Придобиване;
- Изследване/анализ.

Ако мобилното устройство е открито изключено, то трябва да се постави в специална опаковка /чанта/ Faraday, за да предотвратят промени, в случай че устройство-

то автоматично се включи. Чантите Faraday са специално предназначени да изолират телефона от мрежата.

Ако телефонът е намерен включен е от изключителна важност поставянето му в самолетен режим, ако е възможно.

Ако телефонът е заключен от ПИН код или парола, или е шифрован, от проверяващия ще се изисква да заобиколи заключването или да определи ПИН кода за достъп до устройството.

Мобилните телефони са мрежови устройства и могат да изпращат и получават данни чрез различни източници, като телекомуникационни системи, точки за достъп до Wi-Fi и Bluetooth. Така че, ако телефонът е в „активно” състояние, престъпник може сигурно да изтрие данните, съхранявани по телефона чрез изпълнение на дистанционно избърсване на команда.

Фиг. 1. Чанта на Faraday.

Когато е телефонът е включен, той трябва да бъде поставен в чантата Faraday. Ако е възможно, преди дасе постави мобилното устройство в чантата Faraday, той трябва да се изключи от мрежата, за да може да се защитят доказателствата, като се активира режим на полет и деактивират всички мрежови връзки (Wi-Fi, GPS, Bluetooth и др.).

Това ще запази и батерията, докато телефонът е в чантата Faraday.

Някои метали, обикновено мед, сребро или злато, са способни напълно да блокират радиосигналите и електромагнитните полета. Когато тези метали са вплетени във фина тъкан, чиито отвори не надвишават диаметъра на косъм, се осигурява пълно блокиране на сигналите.

Традиционният щит на Фарадей представлява метална проводяща мрежа, способна да блокира електромагнитните полета. Получава името си в чест на английския учен, който ги е изобретил през 1836 г., Майкъл Фарадей.

След като мобилното устройство бъде иззето правилно, проверяващият може да се нуждае от няколко криминални инструмента, за да придобие и анализира данните, съхранявани в телефона.

Поради специалната структура на защитната решетка електромагнитните заряди не могат да проникнат вътре в клетката. Това решение позволява да не се повреди и да се запази електрониката на устройството.

Ако телефонът е заключен от ПИН код или парола, или е шифрован, от проверяващия ще се изисква да заобиколи заключването или да определи ПИН кода за достъп до устройството.

За да се предотврати връзката, мобилните устройства често се транспортират и изследват от вътрешността на Фарадеева клетка (или чанта). Този метод обаче има два недостатъка. Първо, повечето чанти правят устройството неизползваемо, тъй като не може да се използва неговия сензорен екран или клавиатура.

Могат обаче да бъдат закупени специални клетки, за да може устройството да се използва с прозрачно стъкло и със специални ръкавици. Предимството на тази опция е възможността за свързване и с друго криминалистично оборудване, блокиране на мрежовата връзка, както и зареждане на устройството.

Ако тази опция не е налична, се препоръчва да се изолира мрежата, като се постави устройството в самолетен режим или като се клонира SIM картата си (метод, който може да бъде полезен и когато устройството е напълно без SIM) [3].

Мобилните телефони са мрежови устройства, които могат да изпращат и получават данни от различни източници – телекомуникационни системи, точки за достъп до Wi-Fi и Bluetooth. Затова преди да се постави мобилното устройство в чантата Faraday, трябва да бъде изключен от мрежата, за да бъдат защитени доказателствата в него, като се деактивират всички мрежови връзки (Wi-Fi, GPS, горещи точки и така нататък).

След като мобилното устройство бъде иззето правилно, проверяващият може да се нуждае от няколко инструмента, за да придобие и анализира данните, съхранявани по телефона. За тази цел могат да бъдат използвани различни методи, всеки от които влияе върху количеството на анализа.

Бързото увеличаване на броя на различните видове мобилни телефони от различни производители затруднява разработването на единен процес или инструмент за изследване на всички видове устройства. Освен това, мобилните телефони са проектирани с различни вградени операционни системи. Това изисква специални знания и умения от експертите по криминалистика, за да могат да придобият и анализират устройствата.

Модерните мобилни платформи съдържат вградени функции за защита на потребителските данни и личната неприкосновеност. Тези особености действат като препятствие по време на криминалистичното придобиване и изследване. Например, съвременните мобилни устройства идват с механизми за шифроване по подразбиране от хардуерния слой към софтуерния слой. Може да се наложи проверяващият да пробие тези механизми за криптиране, за да извлече данни от устройствата.

Едно от основните правила в криминалистика е проверяващият да се увери, че данните в устройството няма да се модифицират. С други думи, всеки опит за извличане на данни от устройството не трябва да променя данните, присъстващи на това устройство. Но това не е практически възможно с мобилни устройства, защото само включването на устройство може да промени данните на това устройство. Например, в повечето мобилни устройства будилникът все още работи, независимо че телефонът е изключен. Внезапният преход от едно състояние към друго може да доведе до загуба или промяна на данни.

Ако устройството е защитено с код за достъп, криминалистът трябва да получи достъп до устройството, без да увреждa данните на устройството. Цифровите доказателства могат лесно да бъдат променени или умишлено, или непреднамерено. Например, сърфирането в приложение по телефона може да променя данните, съхранявани от това приложение на устройството.

Мобилните устройства комуникират по клетъчни мрежи, Wi-Fi мрежи, Bluetooth. Тъй като комуникацията с устройството може да променя данните на устройството, възможността за понататъшна комуникация трябва да бъде премахната след изземване на устройството.

Тъй като броят на мобилните устройства се увеличава, се използват файлови системи от високо ниво, подобни на компютърните файлови системи. Различни софтуерни инструменти могат да извличат данни от паметта. Може да се използват специализирани и автоматизирани криминалистични софтуерни продукти или програми за преглед на файлове с общо предназначение, за да се търсят характеристики на заглавията на файловете. Предимството на шестнадесетичния редактор е по-задълбочено разбиране на управлението на паметта, но работата с шестнадесетичен редактор изисква много работа.

Обратно, специализираният криминалистичен софтуер улеснява търсенето и извличането на данни, но може да не открие всичко. AccessData, Sleuthkit, ESI Analyst и EnCase са само няколко криминалистични софтуерни продукти за анализ на памет. При изследването се предлага да се използванат на два или повече изследователски инструмента.

Устройството може да съдържа злонамерен софтуер, например вирус. Такива злонамерени програми могат да се опитат да се разпространят върху други устройства или по кабелен интерфейс, или безжично.

I. ИЗВЛИЧАНЕ НА ДОКАЗАТЕЛСТВА ЗА МОБИЛНИ ТЕЛЕФОНИ

Извличането на доказателства и криминалистичния преглед на мобилните устройства могат да бъдат различни. Всички методи, използвани при извличане на данни от мобилни устройства, следва да бъдат тествани, валидирани и добре документирани.

Криминалистичните средства за изследването на мобилно устройство включват няколко фази:

- *Фаза на прием (intake) на доказателства* – фазата на прием на доказателства е началната фаза и води до формулиране на заявка и документация, за да се документира информацията за собствеността и вида на инцидента, в който е участвало мобилното устройство. В нея се очертава видът на данните или информацията, която криминалистът търси. Иззема се устройството, като се внимава да не се модифицират никакви данни, присъстващи в него;
- *Фаза на идентификация (identification)* – трябва да идентифицират следните подробности при всеки преглед на мобилно устройство: правния орган, целите на прегледа, изработката, модела и идентифициращата информация за устройството, сменяемото и външно съхранение на данни, други източници на потенциални доказателства;
- *Фаза на подготовка (preparation)* – след като моделът на мобилния телефон бъде идентифициран, фазата на подготовка включва изследвания по отношение на конкретния мобилен телефон, който трябва да бъде разгледан, избор на подходящите методи и инструменти, които трябва да се използват за придобиване и изследване. Това по принцип се прави въз основа на модела на мобилното устройство, основната операционна система, неговата версия;
- *Фаза на изолиране (isolation)* – изолиращото устройство от комуникационни източници е особено важно. Изолацията на мрежата може да се направи например, чрез поставяне на телефона в режим „самолет“ или при използване на чанта Faraday;

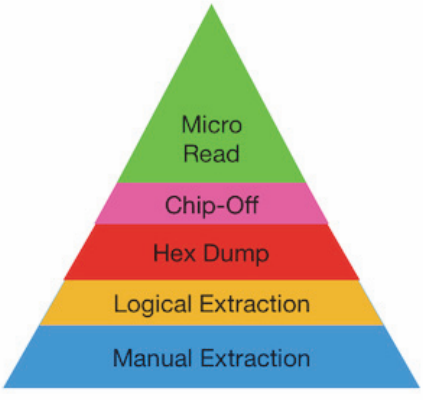
- *Фаза на обработка (processing)* – след като мобилния телефон е бил изолиран от комуникационни мрежи започва действителната обработка. Телефонът трябва да бъде придобит с помощта на тестван метод. Физическото придобиване е предпочитано, т.к. извлича суровите данни от паметта и устройството обикновено се захранва по време на процеса. Ако физическото придобиване не е възможно или е неуспешно, се прави опит за придобиване на файловата система на мобилното устройство;
- *Фаза на проверка (verification)* – по време на цялото разследване е важно да се знае, че информацията, извлечена и документирана от мобилното устройство, може ясно да бъде представена на всеки друг проверяващ или при съдебно дело. Създаването на криминален отчет за данните, извлечени от мобилното устройство по време на придобиването и анализа е важно. Това може да включва данни както в хартиени, така и в електронни формати;
- *Фаза на документиране и докладване (documentation and reporting)* – експертът криминалист е длъжен да документира всичко извършено през целия процес на изследване;
- *Фаза на архивиране (archiving)* – запазването на данните, извлечени от мобилния телефон, в подходящ формат е важна част от цялостното изследване.

II. СИСТЕМА ЗА КЛАСИФИКАЦИЯ НА ИНСТРУМЕНТИ ЗА КРИМИНАЛИСТИЧНО ИЗСЛЕДВАНЕ НА МОБИЛНО УСТРОЙСТВО

При избор на подходящите инструменти за съдебно придобиване и анализ на мобилен телефон се използва система за класификация на съдебни инструменти за мобилно устройство, разработена от Sam Brothers (Фиг. 2), която включва:

- Ръчно извличане (Manual Extraction);
- Логически анализ (Logical Analysis);
- Шестнадесетично зареждане (Hex dump);
- Чип екстрацкия (Chip-Off);
- Микро четене (Micro Read) [4].

Целта на системата за класификация на инструментите за криминалистическо изследване на мобилното устройство е да даде възможност на проверяващия да категоризира инструментите въз основа на методологията за изследване на инструмента.



Фиг. 2. Пирамида за изравняване на инструменти за клетъчни телефони (Sam Brothers, 2009).

Започвайки от дъното на класификацията и продължавайки нагоре (Фиг. 2), методите като цяло стават по-технически насочени, по-сложни и съдебно обосновани и изискват по-дълго време за анализ.

Има предимства и недостатъци на извършването на анализа на всеки един слой. Криминалистът трябва да е наясно с тези проблеми и трябва да продължи работа само с необходимото ниво на екстракция.

Доказателствата могат да бъдат унищожени напълно, ако даден метод или инструмент не се използват правилно. Този риск нараства при придвижване нагоре по стъпалата в пирамидата. Затова е необходимо обучение на специалистите, което да дава възможност за постигане на най-висок процент успеваемост при извличане на данни от мобилни устройства.

Всеки съществуващ мобилен криминалистичен инструмент може да бъде класифициран в едно или повече от пет нива.

***Ниво 1 – Manual Extraction*.**

Ръчното извличане включва преглеждане на информационното съдържание на телефона директно: какво се вижда на екрана му при използване на клавиатурата на устройството. Откритите данни се документират ръчно (обикновено с помощта на цифрова камера). На това ниво е невъзможно да се възстанови изтрита информация.

Разработени са някои инструменти, които помагат на специалиста лесно да документира ръчното извличане. Тези инструменти „улавят“ това, което се показва на устройството, което след това се заснема цифрово за бъдеща справка и съхранение.

Изследователят използва потребителския интерфейс, за да провери съдържанието на паметта на телефона. Така устройството се използва в нормален режим, докато проверяващият прави снимка на съдържанието на всеки екран. Този метод има предимството, че операционната система прави ненужно използването на специализирани инструменти или оборудване за преобразуване на необработени данни в информация, която може да бъде интерпретирана от човека. На практика този метод се прилага при мобилни телефони, PDA и навигационни системи [5].

Недостатъците на тази методика са:

- Могат да бъдат възстановени само данни, видими за операционната система;
- Всички данни са налични само като изображения;
- Процес на изследване отнема много време.

Извличането с „груба сила“ може да се извърши от инструменти, които изпращат серия от кодове/пароли към мобилното устройство. Това е трудоемък, но въпреки това ефективен метод. Този метод използва принципа на проба и грешка в опит да генерира правилната парола или PIN комбинация за удостоверяване на достъпа до мобилно устройство.

Въпреки че процесът отнема време, този метод все още е един от най-добрите в случай, че не може да се получи паролата.

С наличния в момента софтуер и хардуер стана сравнително лесно да се разбие криптирането на файл с парола на мобилно устройство, с цел получаване на паролата. Инструментите за груба сила са свързани към устройството и физически изпращат кодове до iOS (iOS е мобилна операционна система на компанията Apple Inc) устройства, започващи от 0000 до 9999 или 000000 до 999999 последователно, докато правилният код бъде въведен успешно. След успешно въвеждане на кода се дава пълен достъп до устройството и извличането на данни може да започне.

***Ниво 2 - Logical Extraction*.**

Свързването с мобилното устройство обикновено става чрез кабел към хардуер или работна станция, съдържаща специализиран софтуер. Проверяващият може също да предпочете да използва Bluetooth за свързване вместо кабел.

Веднъж свързан, софтуерният инструмент инициира команда, за да поиска след това да извлече разпределените файлове на дадено устройство. След това исканите данни се извличат от паметта на устройството и се изпращат обратно към работната станция, за да бъдат прегледани от проверяващия.

Повечето инструменти за съдебна експертиза на iPhone, налични в момента, работят на това ниво на подреждане.

Логическото извличане включва побитово копиране на логически обекти за съхранение (като директории и файлове), които се намират в логическо съхранение (като дял на файловата система). Ползата от логическото извличане е, че системните структури от данни са по-лесни за извличане и организиране. Логическото извличане извлича информация от устройството с помощта на API (Приложно-програмният интерфейс) на производителя на оригиналното оборудване за архивиране на съдържанието на телефона с персоналния компютър.

Ниво 3 - Hex Dump.

Известно е като *„физическо извличане“*, предоставя на изследователя повече данни, отколкото са били налични на по-ниските нива. За да се извърши този вид извличане, устройството се свързва към работна станция обикновено чрез кабел.

Получените данни се копират, прехвърлят и съхраняват като необработен дисков образ. Тъй като полученото изображение е в двоичен формат, за анализ на това ниво са необходими технически познания.

Физическото придобиване предполага копиране бит по бит на цялото физическо съхранение (като памет), следователно това е методът, който е най-близък до изследването на персонален компютър.

Предимството на физическото извличане на данни е, че позволява да се изследват изтрити файлове и остатъчни данни. Физическото извличане извлича информация от устройството чрез директен достъп до паметта.

Това обикновено се постига по-трудно, тъй като устройството на производителя на оригиналното оборудване трябва да бъде защитено срещу произволни четения на паметта, следователно устройството може да е заключено към определен оператор.

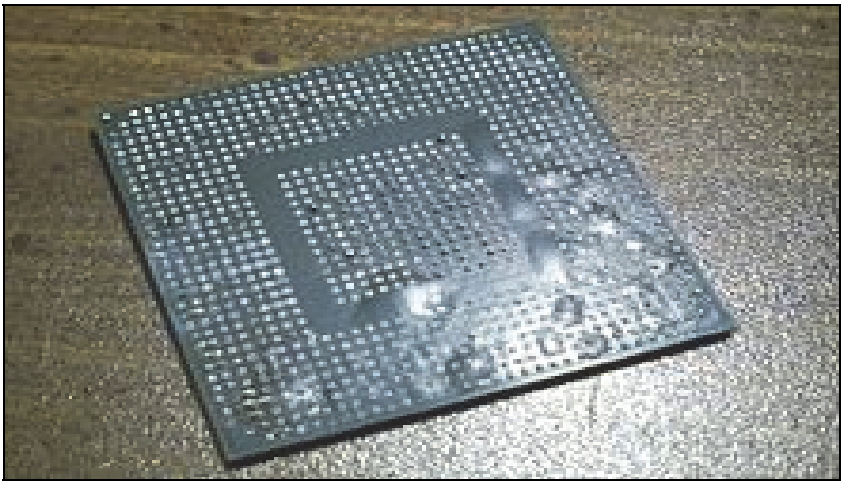
С цел да заобиколят тази сигурност, доставчиците на инструменти за мобилна криминалистика често разработват свои собствени програми за зареждане, позволявайки на инструмента за криминалистика да осъществява достъп до паметта (и често също така да заобикаля потребителските кодове за достъп или заключванията на шаблони) [6].

Ниво 4 *– Chip-Off.*

Chip-off се отнася до придобиването на данни директно от чипа на устройството. Чипът е физически отделен от устройството и данните, съхранени в него, се извличат от четец на чипове.

Редица от аспектите, които правят тази система толкова напреднала, включват голямото разнообразие от използвани типове чипове, безбройните необработени формати на двоични данни и риск от причиняване на физическа повреда на чипа по време на процеса на извличане.

Този метод съдържа потенциална опасност от пълно унищожаване на данните: възможно е да се унищожи чипа и съдържанието му поради топлината, получена при разпояване.



Фиг. 3. Влагата върху печатната платка се е превърнала в пара, при подлагането ѝ на висока температура. Това дава така наречения „Ефект на пуканките“.

Разпояването на чипа се извършва внимателно и бавно, така че топлината да не унищожи чипа или данните. Преди чипът да бъде разпоен, печатната платка се загрява в камера, за да се отстрани останалата влага. Това предотвратява така наречения ефект на пуканки, при който останалата вода/пара/ ще взриви пакета на чипа при разпояване.

Има три основни метода за топене на припой, които се използват:
- С горещ въздух;
- С инфрачервена светлина;
- С парно фазиране.

При технологията с инфрачервена светлина се използва за малки чипове с фокусиране на инфрачервен светлинен лъч върху специфична интегрална схема.

Методите с горещ въздух и пара не могат да се съсредоточат върху опрезелена зона толкова добре, колкото при използавено на инфрачервената техника.

Преди изобретяването на BGA (BGA е вид пакет за повърхностен монтаж използван за интегрални схеми), технологията позволяваше сензори да бъдат прикрепени към щифтовете на чипа с памет и паметта да бъде възстановена чрез тези сензори. Технологията BGA прикрепя чиповете директно към печатната платка чрез разтопени топки за припой, така че сондите вече не могат да бъдат прикрепени.

Ниво 5 – Micro Read.

Този процес включва ръчно преглеждане и интерпретиране на данни, наблюдавани на чипа. Методът отнема време, скъп е и изисква задълбочени познания по всички аспекти на паметта и файловата система.

III. ПОТЕНЦИАЛНИ ДОКАЗАТЕЛСТВА, СЪХРАНЯВАНИ НА МОБИЛНИ ТЕЛЕФОНИ

Данните на мобилен телефон могат да бъдат открити в на различни места – в SIM карта, във външна карта за съхранение и в паметта на телефона.

Освен това, доставчикът на услуги съхранява и информация, свързана с комуникацията. Инструментите за извличане на данни за мобилни устройства възстановяват данни от паметта на телефона.

Въпреки че данните, възстановени по време на криминалистично придобиване, зависят от модела на мобилното устройство, като цяло най-често срещани във всички модели са следните полезни като доказателства данни:

- *Видеоклипове*. Това са видеоклипове, които са заснети с помощта на мобилната камера, изтеглените от интернет, и прехвърлени от други устройства;
- *Музика*. Това са музикални файлове, изтеглени от интернет и тези, прехвърлени от други устройства;
- Документи. Това са документи, създадени с помощта на приложенията на устройството и изтеглени от интернет, както и прехвърлени от други устройства;
- *Календар*. Това е съдържание на записи в календара и срещи;
- *Мрежова комуникация*. Това е съдържание на GPS местоположения;
- *Карти*. Това е съдържание на места, посетени от потребителя, търсени упътвания, търсени и изтеглени карти;
- *Данни за социални мрежи*. Това съдържа данни, съхранявани от приложения като FaceBook, Viber, Telegram, Twitter, Linkedln, Google, WhatsApp и др.;
- *Изтрити данни*. Това е съдържание на информация, изтрита от телефона.

IV. МЕТОДИ ЗА ИЗВЪРШВАНЕ НА ЕКСПЕРТИЗИ С ВЪЗСТАНОВЯВАНЕ НА ДАННИ ОТ IOS УСТРОЙСТВА

IOS е една от двете най-големи платформи за смартфони в света заедно с Android. Потребителският интерфейс на iOS е базиран на концепцията за директна манипулация, използваща мулти-тъч движения. Контролните елементи на интерфейса се състоят от плъзгачи, ключове и бутони. Използва се „течен“ интерфейс (fluid interface), който реагира веднага на действията (input-a) на потребителя. Взаимодействието с операционната система включва движения на пръстите като плъзгане, потупване, натискане и др.

IOS устройство, възстановено от местопрестъпление, може да бъде богат източник на доказателства. Има различни начини за придобиване на криминални данни от iOS устройство. Независимо че всеки метод има своите положителни резултати и негативи, основният принцип на придобиване за всички методи е да се получи byt-bt-byt (побитово) или физическо копие на оригиналните данни, когато е възможно. С по-новите iOS устройства това е почти невъзможно.

Методи за придобиване за iOS устройства са следните:

- Режими на работа на iOS устройство;
- Защита с парола и потенциални байпаси;
- Логично придобиване;
- Придобиване на файлова система;
- Физическо придобиване.

Крайната цел при едно криминално изследване е да се получи физическия образ, а това е възможно за всички iOS устройства.Трябва да се избере най-добрия вариант на изследване.

- *Нормален режим*

Когато iPhone е включен, той се зарежда към операционната си система. Този режим е известен като нормалния режим. Повечето редовни дейности (обаждане, текстови съобщения и т.н.), извършени на iPhone, ще се изпълняват в нормалния режим.

Когато iPhone е включен, той преминава през сигурна верига за зареждане, както е показано на Фиг. 4.

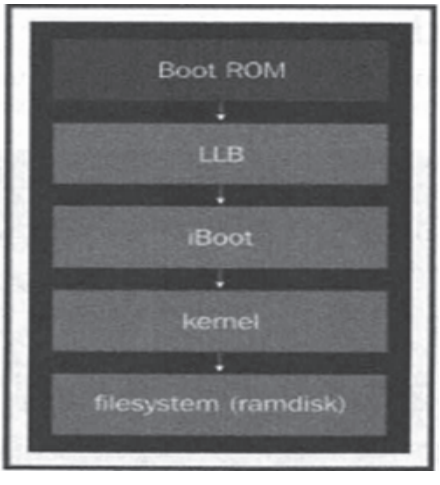
Всяка стъпка в процеса на зареждане съдържа софтуерни компоненти, които са криптографски подписани от Apple, за да се гарантира целостта.

- *Режимът DFU*

Режимът DFU (Актуализация на фърмуера на устройството) е режим на обновяване на фърмуера на iPhone от ниско ниво. Когато е включен, смартфонът ще бъде разпознат от компютъра за възстановяване на iOS. Самият iPhone няма да зареди графичната обвивка на системата и да реагира на натискане на бутони.

Много често режимът DFU се бърка с режима за възстановяване. Външно те са лесни за разграничаване, в режим DFU няма знаци на екрана на iPhone, а в режим на възстановяване се вижда индикатор за свързване към компютър.

Recovery Mode е режим за възстановяване на софтуер за iOS. В същото време данните остават на място и системните файлове се възстановяват от оригиналния фърмуер или архив.



Фиг. 4. Верига за зареждане на iOS устройство в нормалния режим на работата.

Режимът DFU е възстановяване на iOS в режим на зареждащо устройство, при което всички файлове се изтриват и презаписват с данни от оригиналния фърмуер.

Обикновено режимът на възстановяване може да се сравни с изтегляне на резервно копие на Time Machine, а режимът DFU с пълно преинсталиране на операционната система.

Всеки режим на работа на устройството може да спомогне за извличане на определени данни. Понякога е необходимо да преминете през всички опции, за да разберете състоянието на файловата система на устройството.

Но също така съдебният експерт трябва ясно да докладва за своите действия, така че въвеждането в един или друг режим на работа на устройството да не повреди данните.

- *Логично придобиване*

Логично придобиване улавя част от това, което е достъпно за потребителя, с други думи, това, което е включено в резервно копие. Това означава, че няма да се получат никакви изтрити файлове, но благодарение на SQLite бази данни безплатни списъци и неразпределено пространство, може да се възстановят изтрити записи, включително SMS и други чатове, хронология на сърфирането и така нататък.

Логичното придобиване е най-бързият, лесен и най-евтиният начин за получаване на достъп до данни, съхранявани iOS устройство. Има разнообразие от инструменти, повечето от които изискват устройството да бъде отключено или достъпът до plist файла от хост машината да бъде лесно достъпен.

Логичното придобиване е най-простият начин да се установи дали устройството е отключено, тъй като просто се използва вграденият резервен механизъм.

Повечето инструменти и методи, които поддържат логично придобиване на iOS устройства, ще се провалят, ако устройството е заключено.

Някои специалисти мислят, че ако физически диска е «заловен», няма нужда от логично придобиване. Въпреки това, не всички данни се анализират във физическия образ, поради което наличието на достъп до логическия образ, което води до получаване на четими данни, ще съдейства за навлизането дълбоко във физическия образ за артефакти в подкрепа на следствието.

Физическо придобиване

iOS устройства имат два вида памет – RAM и NAND Flash.

RAM се използва за зареждане и изпълнение на ключовите части на операционната система или приложението. Данните на Trie, съхранени в RAM паметта, се губят след рестартиране на устройство.

RAM обикновено съдържа много информация за приложението, като активни приложения, потребителски имена, пароли и ключове за шифроване. Въпреки че информацията, съхранявана в оперативната памет, може да бъде от решаващо значение в едно разследване, към момента няма наличен лесен метод или инструмент за придобиване на RAM паметта от действащ iPhone.

За разлика от RAM, NAND е запазва данните, съхранявани в нея дори след рестартиране на устройство. NAND е основната област за съхранение, съдържа системните файлове и потребителски данни [7].

Целта на физическото придобиване е да се извърши bit-by-bit (побитово) копие на NAND паметта, подобно на начина, по който компютърен твърд диск би бил придобит криминално. Докато съхранението на данни изглежда подобно, NAND се различава от магнитните носители, открити в съвременните твърди дискове. NAND паметта е по-евтина, по-бърза, и държи голямо количество данни. По този начин NAND е идеалното място за съхранение на мобилни устройства.

Физическото придобиване има най-голям потенциал за възстановяване на данни от iOS устройства, въпреки това настоящите и развиващите се защитни функции (сигурна верига за зареждане, криптиране за съхранение и код за достъп) на тези устройства могат да възпрепятстват достъпността на данните по време на криминалистичното придобиване.

Докато физическото придобиване е най-добрия метод за криминално получаване на по-голямата част от данните от iOS устройства, архивните файлове може да съществуват или да бъдат единственият метод за извличане на данни от устройството.

Физическото придобиване има най-голям потенциал за възстановяване на данни от iOS устройства, въпреки това настоящите и развиващите се защитни функции (сигурна верига за зареждане, криптиране за съхранение и код за достъп) на тези устройства могат да възпрепятстват достъпността на данните по време на криминалистичното придобиване.

Изследователи и търговци на криминалистични инструменти непрекъснато опитват нови техники за заобикаляне на защитните функции и извършване на физическо придобиване на iOS устройства.

Физическото придобиване на iOS устройство предоставя най-много данни в едно разследване, но може да намери и богатство от информация за резервни копия на iOS.

Потребителите на iOS устройства имат няколко възможности за архивиране на данни на своите устройства.

Потребителят може избере да архивира данни на компютъра си с помощта на софтуера Apple iTunes, или към услугата за съхранение в облака на Apple, известна като iCioud. Всеки път, когато iPhone се синхронизира с компютър или с iCioud, той създава резервно копие, като копира избраните файлове от устройството.

Потребителят може да определи какво да се съдържа в архива, може да архивира както на компютър, така и на iCioud и данните, получени от всяко местоположение, може да се различават.

Потребителят може да архивира снимки и контакти в iCioud, но може да направи пълно архивиране на всички данни на компютъра си. Физическото придобиване осигурява най-добрия достъп до всички данни на iOS устройството, въпреки това, резервните копия може да бъдат единствения наличен източник на цифрови доказателства.

iPhone архивни файлове могат да бъдат създадени с помощта на софтуера iTunes, който е наличен за платформите macOS и Windows.

iTunes е безплатна програма, предоставена от Apple за синхронизиране и управление на данни между iOS устройства и компютъра. iTunes използва патентования протокол за синхронизация на Apple, за да копира данни от IOS устройството на компютър.

Например iPhone може да се синхронизира с компютър с помощта на кабел или Wi-Fi. *iTunes* предоставя опция за криптирано архивиране, но по подразбиране създава нешифровано резервно копие винаги, когато iPhone се синхронизира. Шифрованите резервни копия осигуряват допълнителен достъп до данните, съхранявани на IOS устройството.

IOS устройства са способни да работят в различни режими на работа: ***нормален режим, режим на възстановяване и режим DFU***. Някои инструменти за криминализиране изискват от проверяващия да знае кой режим на устройството в момента да използва.

iTunes backup

Богатство от информация се съхранява на всеки компютър, който преди това е бил синхронизиран с iOS устройство. Тези компютри, обикновено наричани хост компютри, могат да имат исторически данни и сертификати за заобикаляне на код за достъп.

В наказателно разследване може да се получи заповед за обиск за изземване на компютър, който принадлежи на заподозрян за достъп до сертификатите за архивиране и заключване. За всички останали случаи се изисква съгласие или допустим достъп.

iOS архивиране файл криминалис главно включва анализ на офлайн резервно копие, произведено от iPhone, iPad, iPod докосване, и / или Apple Watch. Данните на Apple Watch ще се съдържат в рамките на архива на iPhone, към който се синхронизира.

Методът за архивиране на iTunes също е полезен в случаите, когато физическото, файловата система и логическото придобиване на iOS устройство не е осъществимо.

В тази ситуация, проверителите по същество създават iTunes резервно копие на устройството и да го анализират с помощта на криминален софтуер. По този начин е важно проверител да разбере напълно процеса на архивиране и участващите инструменти, за да се гарантира, че те са способни да създадат криминално резервно копие, без да замразяват устройствата с други данни.

iPhone архивни файлове могат да бъдат създадени с помощта на софтуера iTunes, който е наличен за платформите macOS и Windows.

iTunes е безплатна програма, предоставена от Apple за синхронизиране и управление на данни между iOS устройства и компютъра. iTunes използва патентования протокол за синхронизация на Apple, за да копира данни от IOS устройството на компютър.

Например, iPhone може да се синхронизира с компютър с помощта на кабел или Wi-Fi. iTunes предоставя опция за криптирано архивиране, но по подразбиране създава нешифровано резервно копие винаги, когато iPhone се синхронизира.

Шифрованите резервни копия, когато са накъсани, осигуряват допълнителен достъп до данните, съхранявани на IOS устройството.

Потребителите често създават архивни файлове, за да защитят данните си, в случай че устройството им е повредено или загубено. Или се създава резервно копие, за да се работи или просто се извличат данни от съществуващите архивни файлове на iOS, за да се търси наследена информация.

Например, ако имав процес на разследване и се изтриват файлове от iPhone, архивните файлове на iCloud и Mac все още съществуват. В зависимост от това дали са използвани iTunes или iCloud, може да съществуват няколко резервни копия за едно и също устройство.

Работа с iCloud резервни копия.

iCloud е услуга за съхранение и изчисления в облак от Apple. Стартирана през октомври 2011 г. услугата позволява на потребителите да поддържат данни като календари, контакти, напомняния, снимки, документи, отметки, приложения, бележки и други в синхрон на няколко съвместими устройства (iOS устройства, работещи с iOS 5 или по-нова версия, компютри с macOS X 10.7.2 или по-нова версия и Microsoft Windows), използване на централизиран iCloud акаунт.

Услугата също така позволява на потребителите да архивират безжично и автоматично своите iOS устройства в iCloud. iCloud също така предоставя други услуги,

като Find My iPhone (за проследяване на изгубен телефон и го избършете от разстояние).

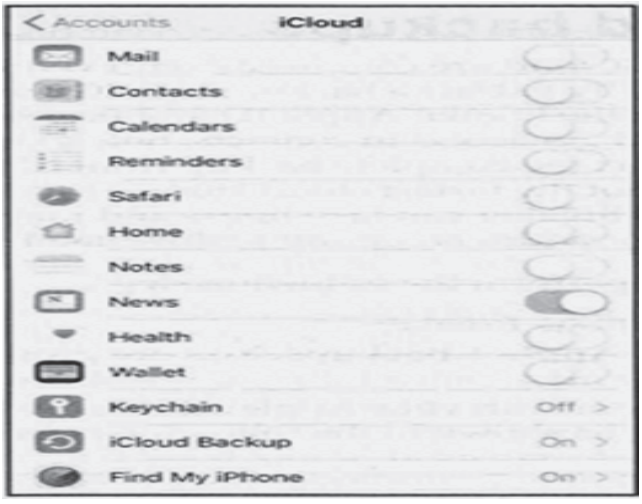
Записването с iCloud е безплатно и просто свързано с Apple ID. Когато има регистрация за iCloud, Apple предоставя достъп до пет гигабайта безплатно отдалечено хранилище. Ако има нужда от повече място за съхранение, може да се закупи план за надстройване.

За да поддържа данните защитени, Apple принуждава потребителите да изберат силна парола при създаването на Apple ID, която да използват с iCloud. Паролата трябва да има минимум осем знака, число, главна буква и малка буква.

iOS устройства, работещи на iOS 5 позволяват на потребителите да архивират настройките и данните на устройството в iCloud.

Архивираните данни включват снимки, видеоклипове, документи, данни за приложения, настройки на устройството, съобщения, контакти, календар, имейл, ключодържател и др.

Може да се включи архивирането в iCloud на устройството, като се навигира до „Settings/Accounts & Passwords/iCloud”, както е показано на Фиг. 5.



Фиг. 5

iCloud може автоматично да архивира данните, когато телефонът е включен, заключен и свързан към Wi-Fi. Така резервните копия на iCloud представляват свежо и близко до реално време копие на информацията, съхранявана на устройството, стига да е налично място за създаване на текущо архивиране.

Може също да се инициире резервно копие на iCloud от компютър, като се избере опцията iCloud. iCloud резервни копия са постъпкови, т.е. след като първоначалното архивиране на iCloud завърши, всички следващи архиви копират само файловете, които се променят на устройството.

iCloud подсигурява данните, като ги криптира, когато се предава по интернет, запазва ги в шифрован формат на сървъра и използва защитени маркери за удостоверяване.

Вградените приложения на Apple (например Имейл и контакти) използват защитен маркер за достъп до услугите на iCloud. Използването на защитени маркери за удостоверяване премахва необходимостта от съхраняване на паролата за iCloud на устройства и компютри.

IOS Анализ на данни

Ключов аспект в криминалната медицина на устройства iOS е да се изследват и анализират данните, придобити за тълкуване на доказателствата. Данните за повечето iOS устройства са шифровани и е необходимо да се дешифрира дялът с данни преди преглед.

Суровото дисково изображение, получено по време на физическо придобиване, дъмп на файловата система или логическия или архивния файл, съдържа стотици файлове с данни, които често са дешифрирани от криминалистите инструменти, описани в по-ранни глави.

Дори когато данните са анализирани и дешифрирани от инструмента за криминалистика, може да се изисква ръчен анализ за разкриване на допълнителни артефакти или за просто валидиране на вашите констатации.

SQLite бази данни

SQLite е отворен код, в процес на обработка библиотека, която внедрява самостоятелно, нула-конфигурация, транзакционен SQL база данни двигател. Това е пълна база данни с няколко таблици, тригери и изгледи, които се съдържат в един файл с кръстосана платформа. Тъй като SQLite е преносим, надежден и малък, той е популярен формат на базата данни, който се появява в много мобилни платформи.

Apple iOS устройствата, подобно на други смартфони, използват тежко базите данни На SQLite за съхранение на данни.

Много от вградените приложения, като телефон, съобщения, поща, календар и бележки, съхраняват данни в SQLite бази данни. Отделно от това, приложения на трети страни, инсталирани на устройството, също така SQLite бази данни за съхранение на данни.

SQLite бази данни се създават със или без разширение на файла. Те обикновено имат . sqlitedb или . DB файлови разширения, но някои бази данни са дадени други разширения, както и.

Данните в SQLite файлове се разбиват в таблици, които съдържат действителните данни. За достъп до данните, съхранявани в тези файлове, е необходим инструмент, който може да ги прочете. Повечето търговски криминалистически инструменти, SQLite Криминалист браузър, и Физически анализатор предоставят поддръжка за изследване на SQLite бази данни.

Обикновено данните за приложението в iOS се съхраняват в бази данни SQLite. От гледна точка на мобилната криминалистика тези бази данни са забележителни с това, че имат списъци със свободни зони и неразпределено пространство, в които доста често попада информация, изтрита от потребителя.

Благодарение на тях криминалистите имат възможност да възстановят например изтрита кореспонденция, въпреки че разполагат само с данни, извлечени на логическо ниво. Может да се анализират тези бази данни, например, като се използва SQLite Database Browser. За да се възстановят изтритите записи се ползва отличен и най-важното, безплатен инструмент – SQLite-Parser.

V. ПРАКТИЧЕСКИ ПРИМЕР ЗА ИЗСЛЕДВАНЕ НА МОБИЛЕН ТЕЛЕФОН IPHONE ЧРЕЗ СЪЗДАВАНЕ НА РЕЗЕВНО КОПИЕ И АНАЛИЗИРАНЕ ЧРЕЗ СОФТУЕРЕН ПРОДУКТ MOBILEDIT FORENSIC PRO

След като експертът получи инкриминирания телефон с конкретно поставени задачи, престъпва към изследването му.

Прави се първоначален оглед на получения обект, установява се марката и модела. Преди да започване изследването се остранява SIM картата.

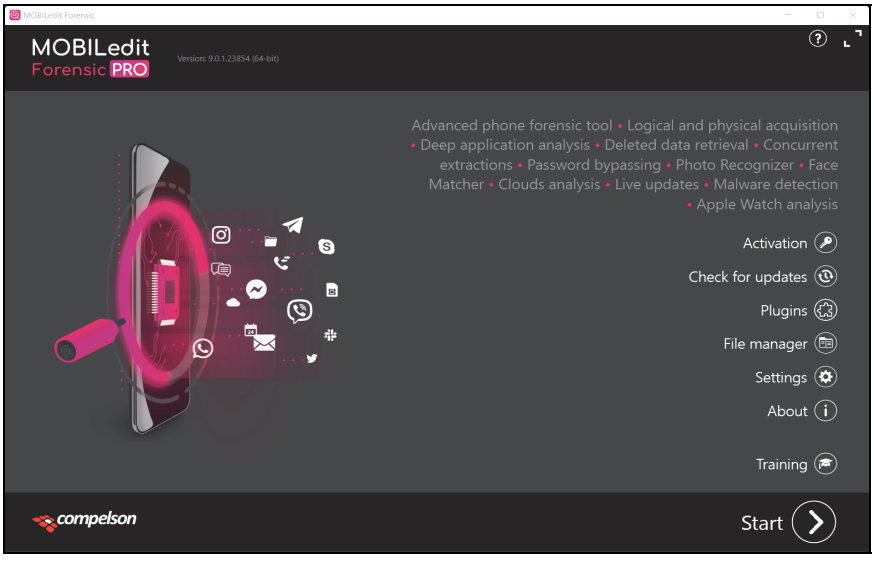
Целта на тази стъпка е при включване, ако в процеса на изземване мобилния телефон не е бил поставен в самолетен режим, да не се усъществява достъп до интернет, тъй като е възможно дистанционно да бъде изтрита информация от предоставения Обект.

След описаните по-горе действия се преминава към изследване посредством софтуерен продукт MOBILedit ForensciPro.

При стартиране на програмата се визуализира показания на Фиг. 6 интерфейс на програмния продукт.

След натиснака на бутона „Start” (Старт) програмата предоставя различни опции, с които може да се продължи.

В конкретния случай, автоматично е разпознала предоставения обект Apple iPhone 12 Mini, с IMEI: 353020117315458, ESN: 35302011731545 и IMSI: 284050072451005 (Фиг. 7).

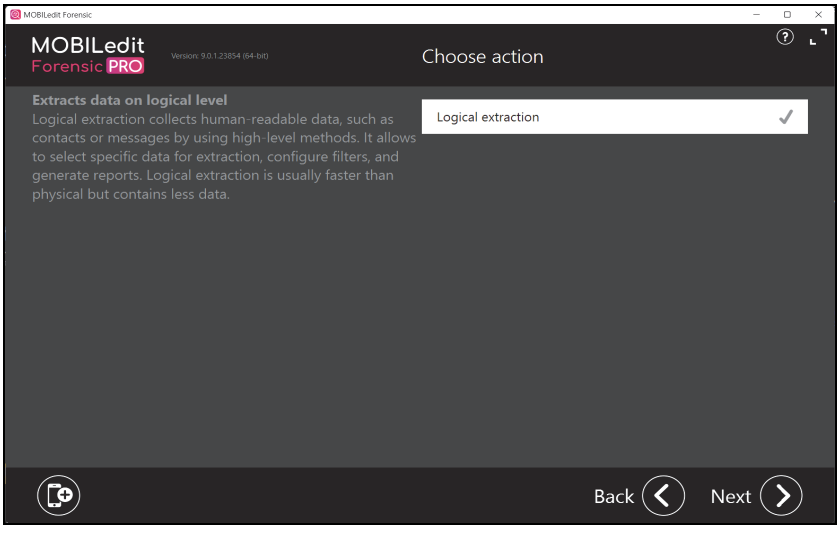


Фиг. 6. Визуализация на интерфейса на стартово меню на MobilEdit Forensic Pro.

Фиг. 7. Визуализация на интерфес с автоматично разпознат телефон на MobilEdit Forensic Pro.

След натискане на бутона „Next“ програмата показва различните методи, с които може да продължи изследването за този телефон.

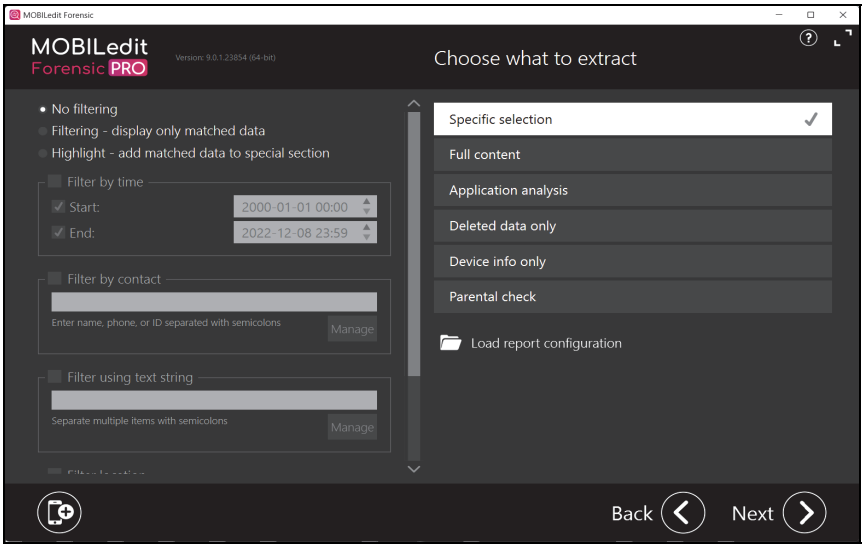
В конретния случай Logical extraction (Фиг. 8).



Фиг. 8. Визуализация на интерфес с възможни методи за изследване на MobilEdit Forensic Pro.

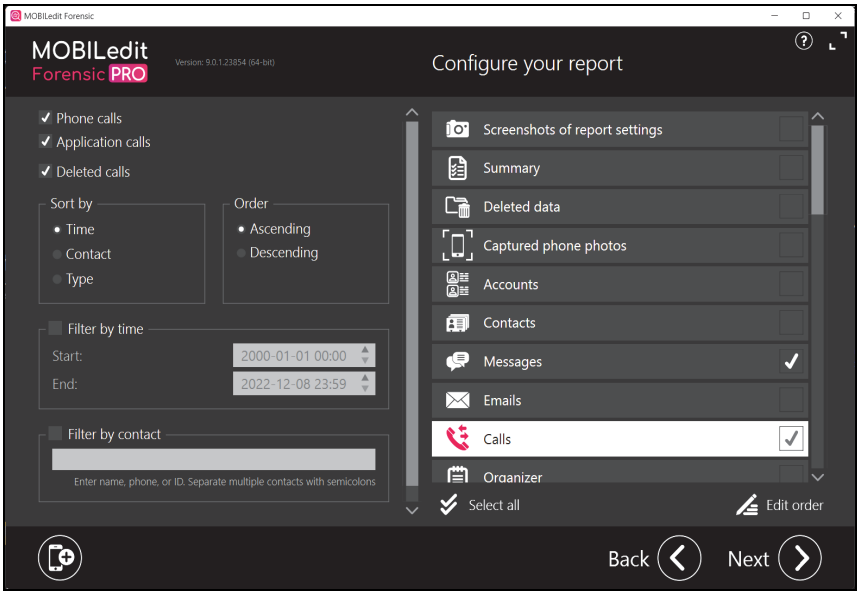
След активиране на бутона „Next“ (продължаване) се дава възможност да се избират различни подходи на работа: **Specific selection** (специфичен подбор), **Full content**

(пълносъдържание), **Application analysis** (анализ на приложенията), **Deleted data only** (само изтрити данни), **Device info only** (само информация за устройството) и **Parental check** (родителски контрол), както е показано на Фиг. 9.

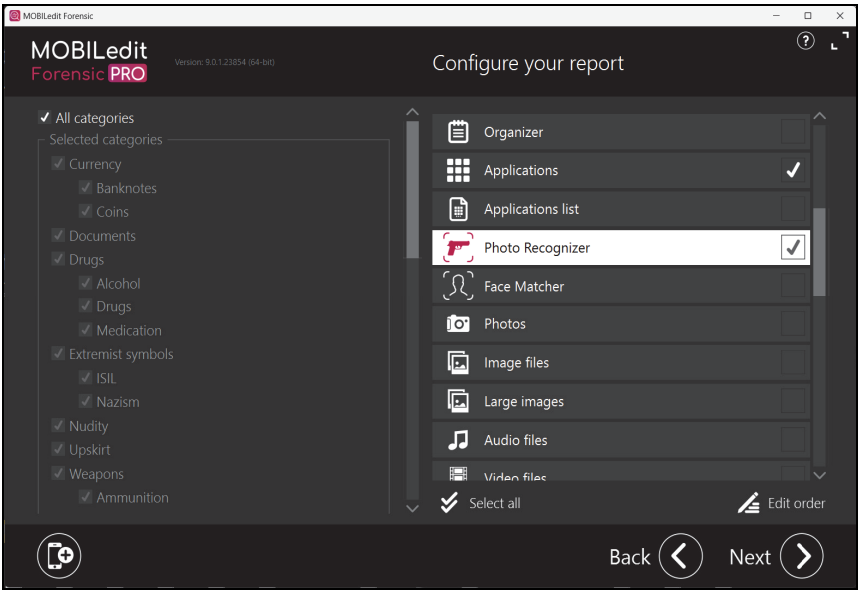


Фиг. 9. Избор на различни подходи на работа.

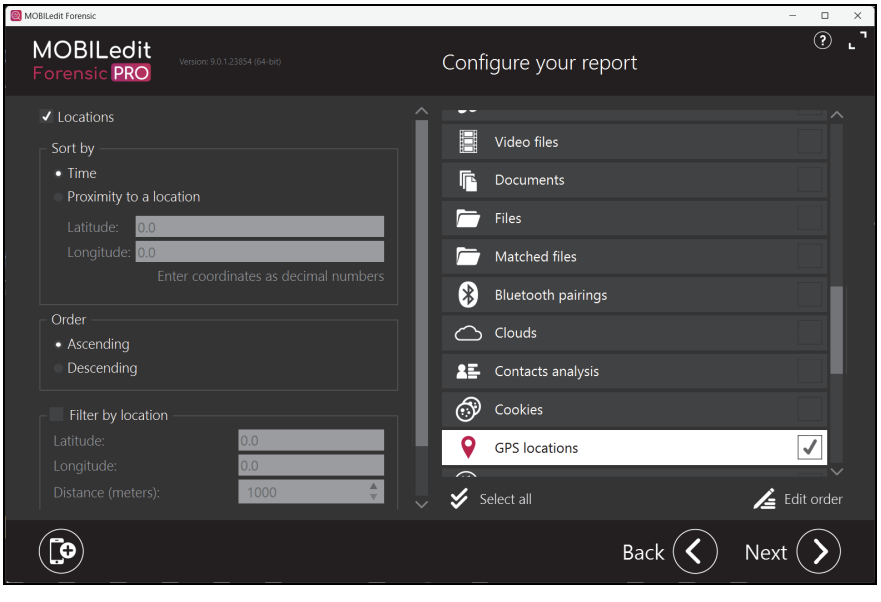
В конкретното изследване се избира **Specific selection**, като ръчно се посочват конкретни данни за извличане в зависимост от поставените задачи (Фиг. 10 ÷ 13).



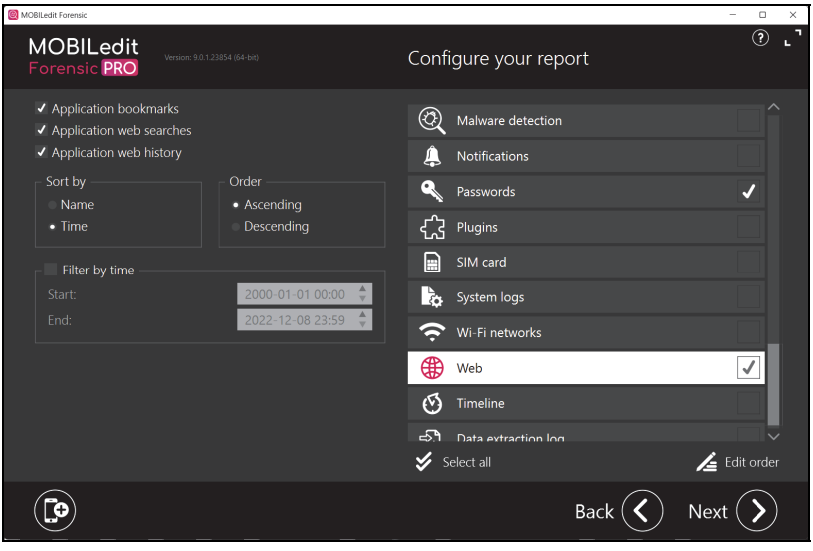
Фиг. 10. Визуализация на различни данни, които могат да бъдат извлечени чрез MobilEdit Forensic Pro.



Фиг. 11. Визуализация на различни данни, които мога да бъдат извлечени чрез MobilEdit Forensic Pro.



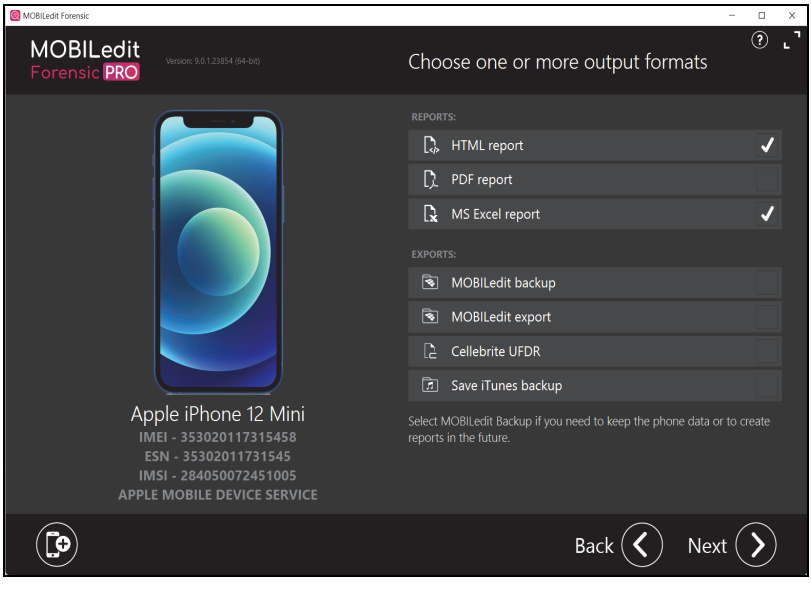
Фиг. 12. Визуализация на различни, данни които мога да бъдат извлечени чрез MobilEdit Forensic Pro.



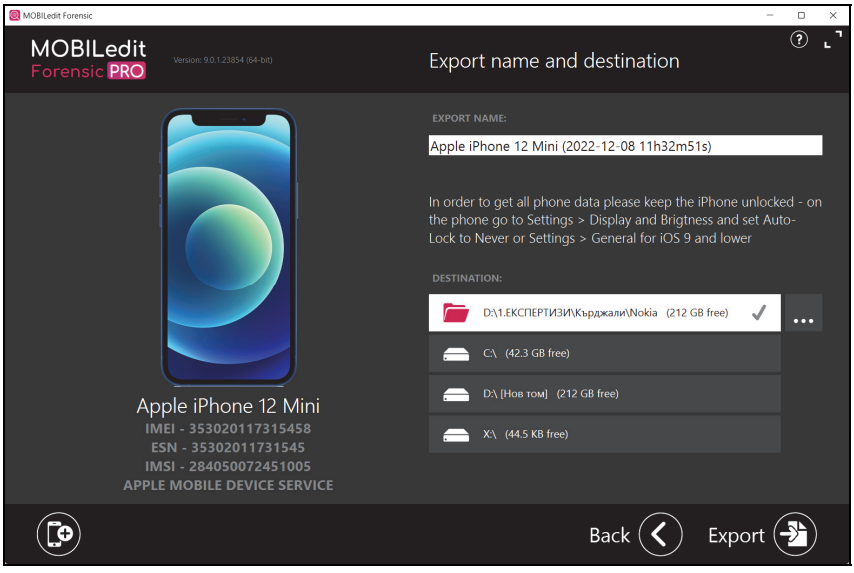
Фиг. 13. Визуализация на различни данни които мога да бъдат извлечени чрез MobilEdit Forensic Pro.

В тази стъпка има предоставени възможности на избор за извличане на акаунти, контакти, съобщения, имейли, повиквания, органайзер, прижения, фото разпознаване, снимки, видео файлове, аудио файлове, документи, GPS локация, пароли за достъп, Wi-Fi връзки и др в зависимост от нуждите на разследването.

След като се изберат нужните данни има възможност за избор на вида на предоставената информация: „**HTML report**”, „**PDF report**” и „**MSExcel report**”.

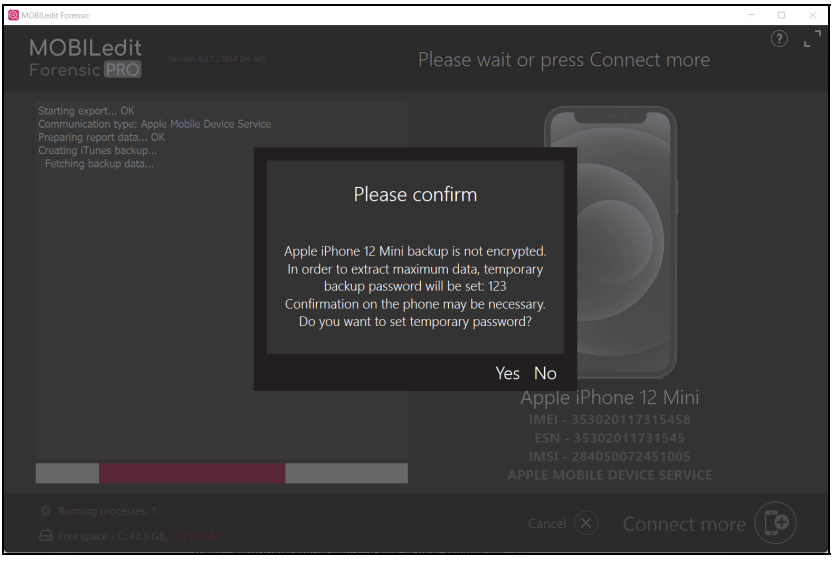


Фиг. 14. Визуализация на различни възможни опции за показване на резултата от извличане на данни чрез MobilEdit Forensic Pro.



Фиг. 15. Визуализация на интерфейст, показващ пътя за сваляне на информацията от MobilEdit Forensic Pro.

След активиране на бутона Export (износ) софтуерният продукт пресъпва към процес на работа. Създава резервно копие посредством iTunes, като за да бъдат извлечени максимално количество данни криптира мобилния телефон със стандартно заложена парола „123“ (Фиг. 16).



Фиг. 16. Визуализация на интерфейст, показващ процеса на извличане и възможност за криптиране.

След приключване на процеса се генерират файлове, с имена, съответстващи на тяхното съдържание виж. Фиг. 17.

В мобилния апарат /мобилен телефон, марка „Айфон“, черен на цвят с черен гръб, с изображение бяла отхапана ябълка, със СИМ карта на мобилен оператор „Йетел“/ бяха открити инсталирани приложения за интернет комуникация Facebook, Instagram, Messenger, TikTok, Twitter и WhatsApp

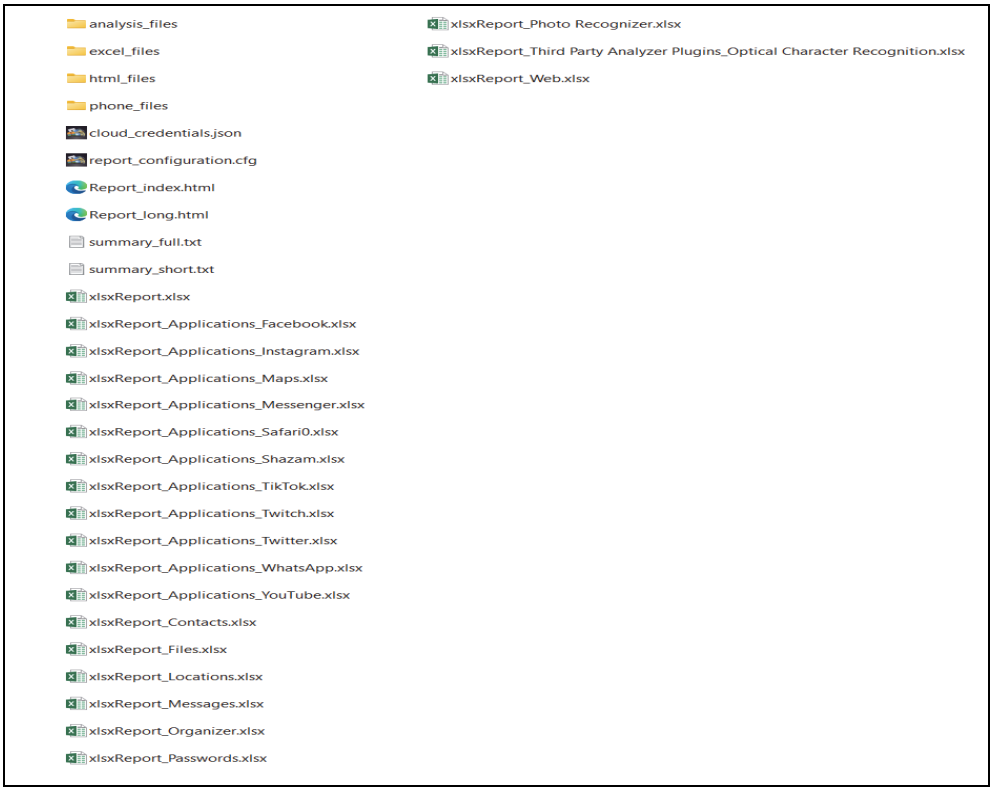
Файлове:

- xlsxReport_Applications_Facebook.xlsx;
- xlsxReport_Applications_Instagram.xlsx;
- xlsxReport_Applications_Messenger.xlsx;
- xlsxReport_Applications_TikTok.xls;
- xlsxReport_Applications_Twitter.xlsx;
- xlsxReport_Applications_WhatsApp.xlsx

съдържат Sheets/листове/ **„Conversation Messages”** и **„Messages”**, с подробна информация (Deleted, Type, To, From, Time, Body и др.) за всички съобщения, **„Calls”** с подробна информация за всички повиквания, **„Contacts”** с подробно информация за всички контакти и **„Accounts”** с информация за активния към момента на изготвяне на експертизата действащ акаунт и др.

В мобилния апарат беше открито инсталирано приложения за интернет достъп **„Safari”.**

Файл xlsxReport_Applications_Safari0.xlsx, съдържа Sheets/листове с подробна информация за интернет история, отворени сайтове и търсения в интернет.



Фиг. 17. Визуализация на извлечените вече файлове, предоставени във .xlsx формат и .html формат.

В мобилния апарат беше открито инсталирано приложения за навигация „Maps”.

Файл xlsxReport_Applications_Maps.xlsx съдържа Sheets/листове с подробна информация за GPS координати за „Searched Routes”/Търсени маршрути/, „Searched Positions”/Търсени позиции/ и „Pinned Positions“ /Закачени позиции/.

В мобилния апарат бяха открити всички запаметени контакти, съобщения и повиквания.

Файлове xlsxReport_Contacts.xlsx, xlsxReport_Messages.xlsx и xlsxReport.xlsx съдържат подробна информация за описаните по-горе данни.

Файл xlsxReport_Photo Recognizer.xlsx съдържа всички мултимедийни записи – изображения, анализирани и предоставени по вид (Валута, Документи, Дрога, Порнография и Оръжия).

Заключение

Разследващите органи и органите на съдебната власт могат по своя преценка да прегледат и/или разпечатат чрез общодостъпен софтуер необходимите им данни за нуждите на определено разследване.

Спецификата за изготвянето на този вид експертизи е индивидуална за всеки изследван обект. Подходът и методът на извличането на данни е различен според марката, модела, фърмуера, софтуера, зависи и от други фактори.

Актуализациите на софтуера, който се използва, ще променя и начина, по който трябва да се разглеждат намерените данни.

Работата на експерта е свързана с избора на най-ефективния метод за откриване на данни в мобилното устройство. При този вид експертизи не трябва да се разчита само на един инструмент, независимо от факта, че софтуера за мобилна криминалистика е скъп и труднодостъпен.

Литература:

1. Eoghan Casey (2004). Digital Evidence and Computer Crime, 2nd Edition - February 23, 2004, ISBN 978-0-12-163104-8
2. Янсен; и другие. «Преодоление препятствий для судебной экспертизы сотовых телефонов» (PDF) . Проверено 20 июля 2012 года .
3. Cynthia A. Murphy. 2013. Developing Process for Mobile Device Forensics. (PDF). 2013.
4. https://study.com/academy/lesson/mobile-device-forensics-tool-classification-system-definition-levels.html].
5. Eoghan Casey. Handbook of Computer Crime Investigation: Forensic Tools and Technology 2 Edition, 2003
6. Vance, Christopher. „Android Physical Acquisitions using Cellebrite UFED” 2012.
7. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST. SP.800-101rl.pdf).
8. Смушкин Александр Борисович, Криминалистическое исследование мобильных устройств, Электронное приложение к «российскому юридическому журналу» 2/2020, 48-52
9. Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices, 3th Edition – Rohit Tamma, Oleg Skilkin, Heather Mahalik, Satish Bommisetty, ISBN 978-1-83864-752-0.