Digitální forenzní analýza mobilních zařízení

Tato práce se zabývá současnými technikami shromažďování elektronických stop přítomných v mobilních telefonech a zařízeních.
This work deals with current extraction technologies of data stored on mobile phone handsets and devices.

V současnosti je neustále zvyšován výpočetní výkon a rozšiřovány funkce mobilních telefonů při zachování jejich dostatečně malých rozměrů, aby se ještě „vešly do kapsy“. Lze říci, že se mobilní zařízení stala doslova digitálními svědky běžného života jejich vlastníků. Smartphone odhalí více podrobností o zvycích a chování uživatele než dříve stolní počítač nebo notebook. Právě díky tomu vzrostl potenciální význam dat uložených v mobilních telefonech, které mohou posloužit jako důkazy v trestním řízení.

Rapidní pokrok v technice mobilních telefonů představuje také jedinečnou výzvu pro kriminální policii a vyšetřování. Obor využití vědeckých metod pro extrakci dat uložených v mobilních telefonech a jejich periferních médiích pro kriminalistické účely se nazývá forenzní analýza mobilních zařízení. Článek vysvětluje, v čem spočívá její přínos pro vyšetřování trestných činů, uvádí její základní metody a nastiňuje trendy jejího budoucího vývoje, kdy již nebude stačit analýza samotného přístroje.

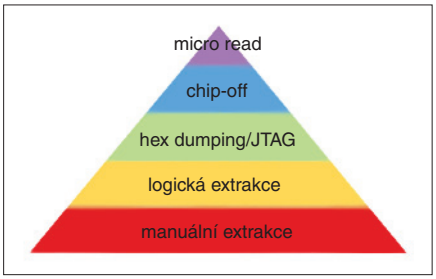
Zdroje důkazů

Zájmem kriminální policie jsou především zdroje údajů, jako je samotný přístroj, karta UICC (*Universal Integrated Circuit Card*)[1] a příslušná média. Přidružené periferie, kabely, napájecí adaptéry a další doplňky také mohou významně přispět k vyšetřování.

Potenciální zdroje kriminalistických stop mohou zahrnovat tyto položky:
- historie příchozích, odchozích a zmeškaných hovorů,
- telefonní seznam a kontaktní údaje,
- obsah textových zpráv SMS, aplikací a multimediálních zpráv,
- obrázky, videa a zvukové soubory a někdy i uložené hlasové zprávy,
- historie vyhledávání v internetu, obsah, cookies, analytické informace,
- datum a čas, jazyk a další nastavení,
- seznamy úkolů, poznámky, záznamy kalendáře, vyzváněcí tóny,
- dokumenty, tabulky, prezentační soubory a další data vytvořená uživatelem,
- hesla, přístupové kódy, pověření uživatelského účtu,
- historická geolokační data, údaje o poloze související se základnovými stanicemi mobilních telefonů, informace o připojení WiFi,
- data z různých nainstalovaných aplikací,
- systémové soubory, protokoly využití, chybové zprávy,
- smazaná data ze všech uvedených zdrojů.

V některých případech, jsou-li k dispozici správné údaje o autentizaci uživatele, lze rovněž obnovit data z cloudového úložiště aplikací.

Před zahájením vyšetřování mobilního telefonu je třeba zvážit, zda neexistují i jiné stopy. Mobilní telefony jsou cenným zdrojem DNA, otisků prstů nebo jiných biologických stop. Tyto druhy stop by měly být sejmuty před zahájením vyšetřování mobilního zařízení, aby se zabránilo jejich kontaminaci.



Obr. 1. Klasifikační systém metod pro digitální forenzní analýzu mobilních zařízení

Metody forenzní analýzy pro mobilní zařízení

Forenzní nástroje musí být navržené tak, aby bylo možné získávat data z paměti zařízení, aniž by došlo ke změně jejího vnitřního obsahu.

Analytické techniky digitálního vyšetřování se rozdělují na tzv. živé (tj. analýza v reálném čase) a mrtvé. V mrtvé digitální forenzní analýze je cílové zařízení vypnuté a vytváří se obraz celého pevného disku. To je právě zárukou reprodukovatelnosti důkazů analýzy. Ale v případě mobilních zařízení, která zůstávají aktivní, i když jsou vypnutá, je již nemožné dosáhnout bitové kopie celého obsahu paměti. Je to jeden z klíčových rozdílů mezi tradiční forenzní analýzou osobních počítačů a forenzní analýzou mobilních zařízení.

Na *obr. 1* jsou představeny metody pro digitální forenzní analýzu. Při pohybu pyramidou ze spodní části z úrovně 1 na vrchol k úrovni 5 stávají se metody zapojené do forenzní analýzy technicky komplexnějšími, invazivnějšími, časově náročnějšími a dražšími. Zvyšuje se také riziko změny až zničení dat.

Byl-li přístroj nalezen v aktivním stavu, měl by být obsah vnitřní paměti získán před vyjmutím a analýzou dat příslušného média (např. karty microSD). Jestliže je displej přístroje v zobrazovacím stavu, obsah na obrazovce by měl být vyfotografován, a je-li to nezbytné, zaznamenán ručně, se zachycením času, stavu poskytované služby, úrovně nabití baterie a s dalšími zobrazenými ikonami. Jestliže je zařízení ve vypnutém stavu, analýza dat vyměnitelného média by měla být provedena přednostně. Mnoho mobilních zařízení totiž podporuje kódy *master reset*, které mohou vymazat obsah zařízení do původního továrního stavu. *Master reset* může být proveden dálkově jednoduchým zasláním příkazu (např. v textové zprávě) do mobilního zařízení.

Manuální extrakce

Na této první úrovni jde o proces, který zahrnuje ruční ovládání displeje a klávesnice pro dokumentování údajů vnitřní paměti mobilního zařízení. Při něm vyšetřující ručně analyzuje mobilní telefon na místě činu bez použití vyšetřovacích nástrojů. Na této úrovni není možné obnovit smazané informace.

Příklady ručního vyšetřování zahrnují:
- procházení mobilním přístrojem a zobrazení dat uložených v telefonu na jeho displeji,
- fotografování nebo jiný záznam informací zobrazených na obrazovce telefonu.

Tato metoda má určitá rizika spojená s manipulací s mobilním zařízením. Umístění cizí SIM nebo paměťové karty do mobilních zařízení může vést k úpravě údajů. Nastartování mobilního přístroje s cizí UICC způsobí vymazání takových datových prvků, jako jsou záznamy o hovorech (zmeškané, příchozí a odchozí hovory), a SMS zpráv přítomných ve vnitřní paměti mobilního zařízení.

Hodně záleží na konkrétním případu. Nicméně manuální extrakce na místě činu má alespoň tu výhodu, že je zabráněno ztrátě informací v průběhu přepravy a skladování zařízení vyčerpáním baterie nebo poškozením přístroje.

Logická extrakce

Logická extrakce je pokročilejší technika s menším rizikem modifikace dat. U této metody se používá software nebo hardwarové zařízení určené ke stahování dat z mobilního zařízení. Mobilní zařízení a forenzní pracovní stanice jsou připojeny buď kabelem

[1] UICC, univerzální čipová karta, je inteligentní karta obsahující CPU, paměti ROM, RAM a EEPROM a obvody I/O. V sítích 2G se nazývala karta SIM, v sítích vyšších generací není toto označení přesné, protože jedna karta UICC obsahuje aplikace USIM (*Universal Subscriber Identity Module*) pro sítě GSM 2G, CSIM (*CDMA Subscriber Identity Module*) pro sítě CDMA i ISIM (*IP Multimedia Services Identity Module*) pro sítě UMTS.

(např. USB), nebo bezdrátově (např. IrDA, WiFi, Bluetooth).

Technika se používá k získání uživatelských přístupných údajů, jako jsou: kontakty, historie volání, textové zprávy (SMS, MMS), obrázky, videa, hlasová schránka, e-mail, údaje z aplikací, webová historie, informace o zařízení, kalendář, poznámky atd. Ale tento typ extrakce obecně neposkytuje přístup k údajům, které byly odstraněny. Také se vyskytují mobilní zařízení, která nemají žádný interface přístupný prostřednictvím počítače. To činí forenzní analýzu těchto mobilních zařízení na uvedené úrovni obtížnější až nemožnou.

Hex Dumping

Hex dumping je proces, který umožňuje zkoumat odstraněná data, jež ale ještě nebyla přepsána. Jde o vytvoření *bit-by-bit* kopie vnitřní paměti mobilního zařízení. Proces zahrnuje nahrání modifikovaného zavaděče do chráněné oblasti paměti přístroje. To se dělá prostřednictvím zapojení datového portu mobilního zařízení do tzv. flasher boxu, který je na druhé straně připojen k forenzní pracovní stanici. Série příkazů, která se odesílá z flasher boxu do mobilního zařízení, na něm spustí diagnostický režim. Následně v diagnostickém režimu flasher box zachycuje všechny sekce flash paměti a odesílá je do forenzní pracovní stanice.

JTAG

Mnoho výrobců mobilních zařízení podporuje standard JTAG (*Joint Test Action Group*). Standard využívající architekturu *boundary-scan* je primárně určen k testování plošných spojů a k programování pamětí flash po smontování zařízení. To je velmi invazivní technika: získání přístupu k zapojení často vyžaduje, aby byly demontovány některé části mobilního zařízení, popř. celé zařízení rozebráno.

Metoda spočívá v připevnění kabelu z pracovní stanice na rozhraní JTAG a realizaci přístupu k paměti mobilního zařízení přes jeho mikroprocesor. Potom pomocí diagnostických protokolů běží komunikace s paměťovým čipem. Tato komunikace může využívat operační systém mobilního zařízení, ale může ho i obejít a komunikovat přímo na čipu.

JTAG je zvlášť vhodná metoda forenzní analýzy pro zařízení, která jsou uzamčená, nebo zařízení, která jsou poškozená a nemohou být ovládána jinak. Některé softwarové nástroje poskytují funkci automatického obnovení hesla uzamčených mobilních zařízení. U určitých zařízení může být hodnota zámku snadno obnovena z výpisu paměti. JTAG a flasher box se často používají k tomu, aby bylo možné obejít mechanismy autentizace.

Chip-off

Chip-off je proces, který spočívá v odstranění paměťového čipu pro provedení analýzy uložených údajů přímo z paměti flash mobilního zařízení. Data z cílového zařízení jsou extrahována v binárním formátu pomocí speciálních algoritmů reverzního inženýrství. Extrakce *chip-off* je náročná, protože mobilní zařízení používají širokou škálu typů čipů a nesčetné množství nezpracovaných datových formátů. Současně hrozí fyzické poškození čipu během extrakčního procesu. Vzhledem ke složitosti provedení analýzy pomoci extrakce *chip-off* se častěji používá metoda JTAG.

Micro read

Micro read spočívá ve fyzickém sledování bran na čipu NAND nebo NOR s použitím elektronového mikroskopu. Tato úroveň shromažďování dat by připadala v úvahu pouze ve výjimečných případech, např. při ohrožení národní bezpečnosti, a to až poté, co byly vyčerpány všechny ostatní techniky sběru dat. Vyžaduje tým odborníků a špičkové vybavení, přičemž návody na použití této techniky nejsou zveřejněny.

Izolační fáze

V těch případech, kdy zařízení musí být pro potřeby kriminálního vyšetřování a využití vyšších úrovní digitální forenzní analýzy transportováno do laboratoře, je nezbytné je izolovat od okolních signálů. Izolace zařízení zabraňuje přidávání nových dat prostřednictvím příchozích hovorů a textových zpráv (mohou náhodně přepsat existující data), jakož i potenciálnímu záměrnému zničení dat prostřednictvím vzdáleného přístupu. Blokováním rádiových signálů však může dojít k vybití baterie, protože zařízení se snaží připojit k síti, zesílí svůj signál na maximum a jeho spotřeba roste. Proto musí být použity přenosné zdroje pro nabíjení.

Avšak žádná z používaných izolačních metod není dokonalá a je vždy spojena s určitými riziky.

Například prosté vypnutí mobilního zařízení může aktivovat autentizační kódy (PIN UICC nebo možné další bezpečnostní kódy), které jsou potom potřebné pro získání přístupu k zařízení.

Přechod do režimu letadla (*airplane mode*) vyžaduje interakci s mobilním zařízením pomocí dotykového displeje nebo klávesnice. Tento režim navíc nebrání systému používat další služby, jako je např. GPS.

Jamming/spoofing je metoda, při které se vysílá signál silnější než u mobilního zařízení nebo je rušen signál komunikační sítě. Metoda spočívá v tom, že zařízení si bude „myslet“, že z nejbližší vysílací stanice do něj přichází signál o tom, že není k dispozici žádná služba. Protože taková zařízení mohou mít vliv na komunikaci v blízkém veřejném okolí mimo zkušební oblast, nelicencované použití této techniky může být považované za protiprávní.

Faradayova klec je přenosný stíněný obal, který je určen k zeslabení rádiových signálů. Dovoluje bezpečné vyšetřování, jakmile se telefon nachází uvnitř. Kabely připojené ke kontejneru (od přenosného zdroje nabíjení nebo pracovní stanice) ale musí být zcela izolovány, aby se zabránilo průniku síťové komunikace. Tato metoda je jednou z nejčastěji používaných, ačkoliv účinnost izolace testovaných kontejnerů není vždy stoprocentní.

Pro mobilní telefony GSM lze izolaci provést vytvořením forenzního klonu SIM (SIM ID Clone). Tato CNIC (*Cellular Network Isolation Card*) funguje tak, že simultánně odmítá autentizaci mobilní sítě. SIM ID Clone není plně klonovaná kopie karty SIM mobilního telefonu, protože autentizační klíč a další uživatelská data nejsou v procesu klonování zkopírovány. Vytvoření CNIC může být dokonce nezbytné pro extrakci dat z mobilního zařízení, protože některé telefony nejsou schopné se spustit bez přítomnosti UICC.

Značka, model a identifikační informace

Až po transportu zařízení do forenzní laboratoře může začít pečlivější analýza. Obecně kriminální vyšetřování začíná identifikací typu mobilního zařízení, jeho operačního systému a dalších charakteristik.

Klasické mobilní telefony obvykle používají operační systém (OS) bez zveřejněné dokumentace, tj. uzavřený typ. Některé z OS jsou vyvinuty dobře známými výrobci, jako jsou např. Nokia nebo Samsung, zatímco některé jsou vyvinuty málo známými čínskými, korejskými či dalšími regionálními výrobci.

Na rozdíl od klasických mobilních telefonů používají smartphony otevřené operační systémy. Těmito operačními systémy jsou: Android, BlackBerry OS, iOS, Symbian, WebOS nebo Windows Phone.

Typ mobilního zařízení a dat, která mají být extrahována, obecně určuje, které nástroje a techniky by měly být při vyšetřování použity. Většina forenzních nástrojů pro mobilní zařízení poskytuje seznamy podporovaných telefonů podle značky a modelu telefonu.

Informace o mobilních zařízeních, která jsou neaktivní, mohou být získány uvnitř prostoru pro baterii, kam se obecně umísťuje štítek výrobce. Tam se uvádějí identifikátory zařízení, jako je IMEI (*International Mobile Equipment Identity*) nebo FCC ID (*Federal Communications Commission Identification*). Tyto informace jsou užitečné zejména v kombinaci s vhodnými databázemi. Zadání čísla modelu do vyhledávače na internetových stránkách výrobce může přinést odhalení značného množství informací o mobilním zařízení. Mohou např. obsahovat odkazy na elektronické verze manuálů pro téměř každou značku a model telefonu, stejně jako na ovladače ke stažení.

Výrobci obvykle nabízejí nějakou informační sadu o možných manipulacích s vlastnostmi a schopnostmi zařízení, včetně informací o prohlížení webových stránek, aplikací typu *Personal Information Management*

(PIM), správy zpráv a e-mailové schránky. Soubor vlastností a funkcí se liší v závislosti na datu, kdy bylo zařízení vyrobeno, verzi firmwaru, změnách provedených konkrétním poskytovatelem služeb a úpravách nebo aplikacích instalovaných samotným uživatelem.

Značka a výrobce mobilního zařízení mohou být také identifikovány podle vlastních pozorovatelných charakteristik (hmotnost, rozměry a tvar), zejména existují-li jedinečné konstrukční prvky. Synchronizační softwary nacházející se na přidruženém počítači rovněž pomáhají rozlišit skupiny operačních systémů.

Existují případy, kdy se zločinci pokoušeli zmařit vyšetřování maskováním mobilního zařízení. Upravit zařízení lze odebráním štítků výrobce a odstraněním log. Pokročilejší je modifikování operačního systému i aplikací nebo ve výjimečných situacích jejich nahrazení vlastními, které se potom mohou zobrazovat a chovat jinak, než by se od nich očekávalo.

Poškozená mobilní zařízení

Mobilní zařízení a přidružená média mohou být nalezena v poškozeném stavu, způsobeném náhodným nebo záměrným zásahem. Vnější viditelná poškození však nemusí nutně zabránit extrakci dat ze zařízení. Je možná oprava poškozených komponent mobilního zařízení a obnovení zařízení do provozuschopného stavu umožňujícího vyšetřování a analýzu. Z poškozeného zařízení mohou být rovněž vyjmuty nepoškozené paměťové komponenty, ale to není možné u všech přístrojů.

Poškozené zařízení už nesmí být připojeno ke zdroji elektřiny, protože by to mohlo způsobit další škody.

Jestliže byl mobilní přístroj namočen do kapaliny, je třeba ihned odstranit baterie (je-li to možné) a vypnout zařízení. Pokusy zapnout zařízení mohou mít za následek další poškození.

Jakákoliv tekutina poškozující zařízení musí být před balením pro transport do laboratoře důkladně vysušena. Vhodné je sušení stlačeným vzduchem. Naopak běžný vysoušeč vlasů by se v žádném případě neměl k vysušení přístroje používat.

Jestliže bylo zařízení vystaveno nekorozivní kapalině, mělo by být pečlivě vysušeno před tím, než se umístí do antistatického sáčku s látkou pohlcující vlhkost. Pro mobilní zařízení je doporučenou látkou silikagel.

Mobilní přístroje, které byly ponořeny do slaného roztoku, chlorované vody nebo jiných korozivních kapalin, by měly být urychleně demontovány. Jako neutralizační činidlo ke splachování solí a jiných nečistot se v takových případech běžně používá destilovaná voda, v nouzi čistá filtrovaná voda.

U zařízení, která byla vystavena tělesným tekutinám, je před zahájením jakéhokoliv čištění třeba zvážit zachování jiných kriminalistických stop (krev, otisky prstů atd.). Potom mohou být tyto tekutiny odstraněny ze zařízení destilovanou vodou a následně izopropylalkoholem. Izopropylalkohol by měl mít čistotu 99,8 % nebo vyšší, protože je vysoce hořlavý a musí se před reinstalací baterie nebo zapojením napájení zcela odpařit.

Poškození požárem obvykle zahrnuje kosmetické vady, vnitřní komponenty zůstávají nepoškozené a nebrání analýze vnitřní paměti zařízení.

Další možnosti pro sběr důkazů

Poskytovatelé služeb jsou povinni udržovat databáze s příchozími a odchozími hovory. Záznamy CDR (*Call Detail Records*) a jiné záznamy udržované poskytovatelem služeb lze vyžádat pomocí identifikátorů účastníka, mobilního zařízení či z UICC. Také mohou být získány nedodané textové zprávy SMS, multimédia nebo hlasové zprávy.

Dostupné údaje navíc mohou zahrnovat: účastnické záznamy, obsah e-mailových serverů (tj. nedoručené e-maily), protokoly e-mailových serverů nebo jiné protokoly IP adres, obsah serverů se zprávami SMS a MMS a obsah serverů hlasové pošty. Získání nebo poslech určitých typů nedoručených souborů třetí osobou bez náležité pravomoci může být považováno za nezákonné odposlouchávání.

Telefony zakoupené anonymně mohou mít také užitečné informace spojené s jejich účtem, např. číslo kreditní karty používané k dobíjení kreditu nebo e-mailovou adresu zaregistrovanou v online prodejně pro doručení pošty.

Identifikace geografického pokrytí specifických buněk v kombinaci s CDR může poskytnout další cenné informace, např. geograficky stanovit s určitým stupněm jistoty lokalitu, kde se nacházelo sledované mobilní zařízení v určitém čase. Profesionální zločinci jsou si ovšem těchto schopností vědomi a mohou se pokusit je obrátit ve svůj prospěch tím, že nechají někoho jiného používat svoje mobilní zařízení k vytvoření falešného alibi. Často používaným trikem je koupit, použít a rychle zlikvidovat telefon s předplacenou kartou. Aby se ještě více zatemnilo používání přístroje, lze měnit různé karty UICC mezi různými mobilními zařízeními.

Trendy

Již více než polovina světové populace užívá internet. Většinou jsou to aktivní uživatelé sociálních médií. Různorodá sociální média umožňují lidem udržovat přehled o aktuálních událostech, zprávách a zábavě. Pozoruhodné je, že uživatelé neváhají dobrovolně obětovat určitou úroveň soukromí tím, že zpřístupňují své osobní údaje. Za tuto realitu jsou částečně odpovědné cloudové aplikace, které poskytují možnost uložení a zpracování dat mimo mobilní zařízení. Tyto aplikace se staly tak běžnými, že si někteří uživatelé ani nevšimnou, že je používají.

Cloud computing je budoucností mobilní komunikace, ale zároveň je i budoucností elektronické trestné činnosti. Protože je to relativně nový obor, je problém zabezpečení dat v cloudu často diskutován. Jak poroste množství citlivých údajů v cloudu, očekává se, že se stanou upřednostňovaným cílem pro trestnou činnost.

Aplikace digitální forenzní vědy v prostředích cloud computingu je nyní velmi aktuálním tématem. Uživatelé se stále více spoléhají na cloudové služby, což snižuje počet forenzně relevantních dat uložených v samotných mobilních přístrojích. Ovšem většina zmíněných nástrojů má omezené možnosti pro zpracování dat hostovaných v cloudu.

Cloudová forenzní analýza je rozvíjející se disciplína, která je momentálně v raných fázích, proto zatím nejsou zpracovány standardy pro vyšetřování. Stále existuje velké množství problémů, které je třeba vyřešit. Zvláštní dilema v oblasti cloudové forenzní analýzy dat z mobilních zařízení se týká potřeby zajistit připojení zařízení do sítě během vyšetřovacího procesu, aniž by se riskovalo vzdálené vymazání nebo změna dat z jiného zařízení. Další překážku v práci vyšetřovatelů představuje nemožnost získat fyzický přístup ke cloudové infrastruktuře. Je to ještě více zhoršeno skutečností, že cloudová data jsou často šířena mezi různými místy v různých zemích s různými právními jurisdikcemi.

Na závěr

Budoucí digitální forenzní analýza musí překročit fyzické bariéry zařízení a zahrnovat zmíněné veřejné a soukromé domény cloudových služeb. To zvyšuje složitost a rozšiřuje hranice forenzního vyšetřování nad rámec tradičního vyšetřování.

Vzhledem k tomu, že technika a mobilní sítě se velmi rychle rozvíjejí a navíc se pravidelně zavádí další produkty a funkce, zachycuje tento článek jen momentální stav oboru kriminálního vyšetřování mobilních přístrojů. Další rozvoj techniky bude určitě vyžadovat nové forenzní metody pro kvalitnější analýzu.

Literatura:

[1] AYERS, Rick, Sam BROTHERS a Wayne JANSEN. *Guidelines on Mobile Device Forensics: NIST Special Publication 800-101*. U.S. Department of Commerce, National Institute of Standards and Technology, May 2014. ISBN 1548070866.

[2] BARMPATSALOU, Konstantia, Tiago CRUZ, Edmundo MONTEIRO a Paulo SIMOES. Current and Future Trends in Mobile Device Forensics. In: *ACM Computing Surveys*. 2018, s. 1–31. DOI: 10.1145/3177847. ISSN 0360--0300. Dostupné také z: https://dl.acm.org/doi/10.1145/3177847

[3] KRISHNAN, Sundar, Bing ZHOU a Min KYUNG AN. Smartphone Forensic Challenges. *International Journal of Computer Science and Security*. 2019, **13**(5), 183–200. ISSN 1985-1553.

Ing. Nikita Dovzhenko, Ústav počítačové a řídicí techniky Fakulty chemicko-inženýrské Vysoké školy chemicko-technologické v Praze