Investigații mobile – captură, analiză și stocare a datelor senzitive

Adrian Victor VEVERA, Deniss Bogdan ONOFREI-RIZA
Institutul Naţional de Cercetare-Dezvoltare în Informatică – ICI București
B-dul Mareșal Alexandru Averescu, Nr. 8-10, 011455, București, România
victor.vevera@ici.ro, deniss.onofrei@ici.ro

Rezumat: Dispozitivul mobil inteligent al zilelor noastre memorează contactele utilizatorului, deține date din rețelele sociale, mesaje „instant“, rulează aplicații de comunicare, reține informații despre apelurile telefonice, textul trimis și primit în mesaje, conține e-mailuri cu atașamente, jurnale de navigare și date tip "geolocație", stochează imagini și videoclipuri realizate cu camera foto proprie, "reține" parole pentru cloud, servicii, forumuri, portaluri online și site-uri de cumpărături, plus multe alte date stocate în memorie. Un astfel de dispozitiv inteligent (actualmente omniprezent) devine (urmare a celor exemplificate mai sus) un depozit complex de date sensibile. Colectarea acestor date (transformate în dovezi digitale) are o importanță deosebită, mai ales în situațiile în care telefonul (sau posesorul lui) pot fi subiectul (subiecții) unor investigații penale, civile, accidentale (informative) sau la nivel corporativ. Extragerea acestor informații, precum și "catalogarea inteligentă" a datelor cu scopul de a le transforma în dovezi solide și complexe sunt rezultantele finale ale aplicării unor algoritmi avansați de achiziție și analiză. Cu sisteme de operare diferite și expansiune tehnologică, criminalistica mobilă a evoluat în același ritm, dezvoltând noi metode practice de colectare a dovezilor conținute de către dispozitivele mobile.

Cuvinte cheie: Dispozitive mobile, criminalistica digitală, sisteme de operare, date senzitive.

Mobile investigations – capture, analyze, and store sensitive data

Abstract: Today's smart mobile device stores user contacts, social networking data, instant messaging, runs text messaging, retains information about phone calls, the text sent and received in messages, contains attachment emails, navigation logs, and geolocation data, stores images and videos made with your own camera, "holds" cloud passwords, services, forums, online portals, and shopping sites plus many other data stored in memory. Such a smart device (nowadays omnipresent) becomes (as exemplified above) a complex storage of sensitive data. Collecting these data (transformed into digital evidence) is particularly important in situations where the phone (or its owner) may be the subject (s) of criminal, civil, accidental (informative) or corporate investigations. Extracting this information, as well as „intelligently cataloguing" data to turn it into solid and complex evidence, is the ultimate result of applying advanced acquisition and analysis algorithms. With different operating systems and technological expansion, mobile forensics evolved at the same pace, developing new methods practical collection of evidence contained by mobile devices.

Keywords: Mobile device, mobile forensic, operating systems, sensitive data.

1. Introducere

Dispozitivele mobile, în continuă dezvoltare, au devenit un instrument principal în ceea ce privește combaterea criminalității digitale. Cu toate acestea, din ce în ce mai mulți specialiști ai domeniului se confruntă cu dificultăți tehnice generate pe parcursul procesului de investigare (lipsa metodologiilor clare, informații neordonate, împrăștiate, dispersate).

Extragerea dovezilor digitale conținute de către un dispozitiv mobil este un proces destul de complex, amplificat fiind și de viteza de schimbare a tehnologiilor IT prezente.

Diseminarea cunoștințelor criminalistice mobile generează investigații digitale dificile afectând nu numai calitatea rezultatelor cât și elaborarea de noi concepte reale ale acestui domeniu. O abordare elaborată tehnic dezvoltată practic în spiritul identificării și agregării metodologiilor comune de achiziție și analiză a datelor conținute de către dispozitivele mobile.

Dominând piața dispozitivelor mobile pe scară largă, platformele Android (Google) și iOS (Apple) atrag din ce în ce mai mulți consumatori și, implicit, o diversitate de dezvoltatori ai aplicațiilor dedicate acestor medii. Dezvoltat pe un Kernel Linux și susținut de serviciile Google, sistemul de operare mobil Android este cel mai răspândit, oferind totodată o flexibilitate mărită în a personaliza și utiliza dispozitivul pe care rulează. Cu un puternic suport către Cloud, Android rulează atât aplicații proprietare cât și terțe, modelul său de securitate permițând utilizatorului un anumit grad de flexibilitate. Viziunea Google asupra securității sistemelor de operare Android a determinat dezvoltatorii să aplice modele specifice de proiectare și dezvoltare a aplicațiilor în limbaj Java. Sistemul de operare are posibilitatea de a izola procesele ce rulează cu un identificator unic (UID). Un utilizator poate avea același identificator unic căruia îi sunt alocate drepuri diferite, de aceea Android poate aloca unui proces izolat mai multe permisiuni. Un alt aspect demn de menționat este modalitatea în care sistemul de operare preia atingerile și gesturile utilizatorului către ecran traducându-le în comenzi interne.

Dezvoltat de către Apple (în proprietatea căruia se află), iOS este un sistem de operare mobil ce funcționează numai pe hardware proprietar. Având la bază serviciile Apple și magazinul de aplicații AppStore, echipamentele mobile ce rulează iOS se declară a fi cu un grad de securitate ridicat, permițând utilizatorului controlul asupra resurselor de sistem (limitarea aplicată la niveul politicilor). Tehnicile avansate de criptare și decriptare precum și cheile hardware stocate în interiorul CPU (procesorului) fac din arhitectura acestui sistem de operare un concept robust, rezistent la atacurile din exterior.

2. Forensic mobil – date generale

Criminalistica dispozitivelor mobile face referire la procesele de recuperare a dovezilor digitale conținute de către dispozitivele mobile, utilizând metode cu acceptanță juridică. Cu alte cuvinte, procesele de tip forensic vizează colectarea, validarea, identificarea, interpretarea și memorarea datelor extrase din sursele digitale. Principalele categorii de date extrase din memoria dispozitivelor mobile sunt: contacte, poștă electronică, mesaje text, mesaje MMS, istoricul convorbirilor, fotografii, coordonate geolocative, date calendaristice, documente, convorbiri ale mesageriilor digitale, date conținute de către rețelele de socializare, identificatori ai dispozitivului mobil, date ale aplicațiilor, date ale jocurilor, fișiere aferente cardurilor de memorie SD etc.

Un rol foarte important în manipularea dispozitivelor mobile supuse anchetei cibernetice îl are integritatea dovezilor (ce ține nu doar de modul în care acestea au fost extrase ci, în aceeași măsură, de documentarea aferentă intrării în posesia dispozitivului mobil – dată și oră achiziție, nivel baterie, aplicații existente, starea fizică a dispozitivului, identificatori software și hardware proprietari etc.). De menționat, alături de pașii parcurși în timpul procesului de achiziție este și ușoara teamă a examinatorilor de a nu distruge dovezile digitale, teama de falsă percepere a acestor dovezi precum și eventuala ipoteză de expunere a acestora în fața instanțelor judecătorești.

Procesele complexe, total diferite de la caz la caz, extragerea și analiza datelor digitale conținute de către dispozitivele mobile parcurg următoarele etape:

- Cercetarea dispozitivului și identificarea tipurilor de date pe care le conține;
- Inspectarea aplicațiilor instalate manual (neimplicite);
- Identificarea dovezilor digitale conținute de către dispozitivul mobil;
- Identificarea locaților în care se află stocate informațiile;
- Adaptarea procedeelor de căutare personalizată a informațiilor senzitive;
- Identificarea și analiza aplicaților software ce execută transfer de informație către exterior;
- Corelarea jurnalelor de apeluri cu persoanele de contact;
- Identificarea informațiilor șterse din memoria dispozitivului mobil.

3. Forensic la nivel de cartelă SIM

Majoritatea telefoanelor mobile moderne au în componență o cartelă ce facilitează accesul în rețelele GSM, care poartă denumirea de SIM (Subscriber Identity Module). Modulul SIM are un spațiu mic de memorie ce poate stoca informații valoroase despre utilizatori (de la 8 la 256 de Kb). Elementul de bază fiind microcip-ul, cartela SIM rulează în interior asemeni unui sistem de operare cu o structură de fișiere aferente, fiind capabilă să controleze procesele de interacțiune cu exteriorul.

4. Forensic la nivel de card SD

Memoria volatilă, cardul SD și memoria internă a dispozitivului mobil sunt elemente ce conțin date sensibile, procese de executat, rezultate ale acestora, modele de date, credențiale etc. Utilizate cu precădere de către dispozitivele Android, Windows Phone și BlackBerry, cardurile SD stochează fișiere sistem create, modificate sau șterse. Analiza acestora poate fi făcută local, de la distanță, sau prin detașarea fizică a cardului ce mai apoi va fi supus unei analize atente nepermițând, în același timp, alterarea accidentală a informațiilor conținute de către acesta. Cardurile SD pot conține atât date lizibile, clare, cât și date inaccesibile procesele de achiziție normală (fișiere orfane, informații referitoare la sectorul de „boot“, date alterate, fișiere criptate, fișiere ascunse generate de aplicații ale sistemului).

5. Forensic la nivel de Android

Sistemul de operare Android, prin natura sa (open-source), a fost rapid asimilat de către dezvoltatorii de hardware și operatorii de telefonie ce simțeau nevoia unui sistem securizat, ieftin, rapid și funcțional.

Toate aceste caracteristici au adus Android-ul într-o poziție optimă vis-a-vis de dezvoltatorii ce își doreau utilizarea și particularizarea unei platforme, capabilă de a eficientiza lucrul cu dispozitivele inteligente.

Android, rulând peste un Kernel de Linux, este conceput pe Layere (nucleu de bază, abstractizare hardware, librării native de C și C++, librării de Core, framework-uri de Java, aplicații proprietare de sistem). La nivelul Kernel-ului, Google integrează managementul driverelor de sistem, generând, prin concept, un element de abstractizare între componentele hardware disponibile și software-ul dispozitivului mobil ce rulează Android.

Un rol important în cadrul analizei criminalistice a oricărui sistem de operare îl ocupă modalitatea în care acel sistem își organizează datele. Atâta timp cât vorbim despre sistemul de operare Android, discutăm de o ierarhie a fișierelor similară cu cea a Linux-ului, partiționarea fizică sau logică a acestora fiind reprezentate ca o structură unică (ROOT). Structura internă a fișierelor Android permite definirea clară a unor partiții proprietare:

– Boot – fiind o partiție de start este definitorie în buna funcționare a dispozitivului (conține Kernel-ul și Ramdisk-ul);

– Sistems (conține întreg sistemul Android plus aplucațiile preinstalate);

– Recovery – fiind o partiție alternativă de recuperare a dispozitivului mobil, aceasta conține fișiere destinate procedurii de back-up;

– Data – conține date ale utilizatorului dar și alte aplicații instalate de către acesta;

– Cache – conține date stocate în vederea accesibilității rapide;

– Misc – conține date importante referitoare la configurările avansate ale sistemului de operare mobil;

– Partiția logică/fizică de stocare a datelor (în cazul dispozitivelor cu o memorie internă limitată, aceasta împrumută comportamentul partiției Data).

În ideea unei achiziții complete și corecte a datelor senzitive conținute de către dispozitivele mobile Android, putem distinge o multitudine de metode de colectare (utilizate singular sau combinat, funcție de decizia examinatorului):

– Metoda agentului software instalat pe un dispozitiv mobil în vederea culegerii datelor;

– Metoda backup-ului, capabilă de a colecta date conținute de către copiile de siguranță incrementale sau nu, ale dispozitivului mobil;

– Metoda de tip ADB (Android Debug Bridge) executată din linie de comandă, ce rulează peste sistemul de operare mobil, permițând o conectare ușoară între acesta și sistemul informatic examinator;

– Metoda modificării rutinei de start a sistemului de operare mobil;

– Metoda de tip ROOT în care principalul rol îl joacă escaladarea drepturilor de administrator;

– Metoda achiziției datelor direct din cip-urile de memorie, din microcontrolere sau din magistralele de date;

– Metoda de tip JTAG (Join Test Action Group) ce implică accesul fizic la placa de bază în vederea colectării informațiilor stocate binar.

6. Forensic la nivel de iOS

Dezvoltat fiind de către compania Apple, iOS a fost lansat în anul 2007 ca și sistem de operare mobil ce utiliza primitive BSD și UNIX.

Modalitatea de start protejată, structura software gândită de așa natură pentru a nu fi modificată, coprocesorul criptografic și managementul integrității datelor sunt câteva dintre elementele definitorii ce anunță iOS ca și sistem sigur, puternic securizat.

Asemeni Android, ca și structură logică, iOS este construit pe baza unor layere de abstractizare:

– Baza sistemului de operare (fișiere și directoare, memoria, sistemul de gestionare al memoriei, managementul protocoalelor de rețea etc.);

– Serviciile de bază (baze de date interne, informații de tip geolocație etc.);

– Zona media (tot ceea ce ține de imagini, video, audio etc.);

– Layer-ul de management al proceselor paralele, a animațiilor de fundal precum și a altor elemente ce interacționează la acest nivel.

Dispozitivele ce rulează iOS conțin două partiții logice: partiția de sistem și partiția ce conține datele utilizatorului. Atât la nivelul partiției de sistem cât și la nivelul partiției ce conține datele utilizatorului, iOS stochează date sub forma fișierelor XML, a bazelor de date SQLite, a datelor de sistem, a jurnalelor de activități și a diferitelor fișiere temporare rezultate din rularea aplicațiilor.

Un rol foarte important în procesul de achiziție a datelor conținute de către dispozitivele mobile iOS îl are identificarea corectă a modelului unui astfel de dispozitiv (pentru a diminua riscul alterării datelor de examinat sau pierderii acestora).

Parte integrantă a lumii criminalității mobile, piața dezvoltatorilor de soluții comerciale dedicate acestei nișe, evoluează dinamic, dezvoltând atât aplicații cât și echipamente hardware din ce în ce mai performante și capabile de a extrage informații conținute de către dispozitivele mobile.

Companii precum MSAB, CELLEBRITE, MAGNET FORENSICS, COMPELSON, ACCESS DATA, vin și întregesc peisajul lumii digitale prin echipamente dedicate: UFED 4 PC, MAGNET AXIOM, MOBIL EDIT ENTERPRISE, XRY EXPRESS, FTK, OXYGEN (soluții complexe de forensic mobil capabile de a genera diversitatea metodelor de captură și analiză, care, la nivel primar, vor face obiectul prezentului suport de curs).

7. Concluzii

În contextul metodologiilor de recuperare a datelor cu referință către instrumentele de testare și implementare a acestor procese, criminalitatea mobilă, ca și disciplină digitală, tinde către generarea unei paradigme de validare și verificare în context unic a instrumentelor comerciale (și nu numai) destinate acestui sector. Aceste metodologii, derivate în timp, necesită testări intensive pentru a putea fi evaluate corect și a se contura ca și căi de urmat de către examinatori în procesele de extragere, stocare și analiză a datelor sensibile conținute de către dispozitivele mobile. Pentru a stabili corect autenticitatea datelor corelate este necesară dezvoltarea unei arhitecturi (în mare parte software) capabilă de a corela principalele entități generatoare de date, aplicațiile (versus utilitarele de sistem). Sistemele de operare mobile reprezintă, prin diferite particularități, elemente ajutătoare în identificarea metodelor de achiziție a datelor, precum și în procesul de selectare a soluțiilor (software/ hardware) ce vor fi utilizate pe parcursul anchetei digitale. Una dintre cele mai populare metode de achiziție a datelor conținute de către dispozitivele mobile constă în utilizarea soluțiilor comerciale, dezvoltate special pentru a colecta și transmite mai departe date senzitive. Aceste produse utilizează diverse combinații ale metodelor de colectare studiate în prezentul suport de curs, facilitând astfel atât achizițiile de tip logic cât și cele de tip fizic, cu scopul de a ușura considerabil nu numai procesul de extragere, dar și activitățile ulterioare acestuia. În paralel cu dinamica dispozitivelor mobile, criminalistica digitală (aferentă acestui sector), entitate ce vizează dovezile binare, acoperă o arie extrem de largă cu multe particularități, dar și cu metode, din ce în ce mai complexe, aplicate în procesele de colectare a datelor stocate, recepționate sau emise de către dispozitivul supus anchetei.

BIBLIOGRAFIE

1. Ablon L, Libicki MC, Golay AA., *Markets for Cybercrime Tools and Stolen Data*: Hacker's Bazaar, 2014;
2. Articles L, Webinars L., *Smartphone Users Worldwide Will Total Mobile users pick up smartphones as they become more. Best Practices in Digital Video Advertising. Go beyond the articles*?; *Hear from our clients?; Want to learn more?*, 2014;
3. Falk S., Shyshka A., *The Cloud Marketplace: a capability-based framework for cloud ecosystem governance,* 2014;
4. Hale-Ligh, M., Case, A., Levy, J., Walters, *The Art of Memory Forensics*, 2014;
5. Heider J., Boll M., *Lost iPhone? Lost Passwords!,* Fraunhofer Institute for Secure Information Technology (SIT), 2011;
6. Katalov V., *Apple iCloud Inside out,* HITBSecConf, 2013;
7. Li Y., Wang H., and Sun K., *A study of personal information in human-chosen passwords and their security implications*, 2016;
8. Mushcab R.A., Gladyshev P., *The significance of different backup applications in retrieving social networking forensic artifacts from Android-based mobile devices,* Second International Conference on Information Security and Cyber Forensics, 2015;
9. NIST, *Have Your Computer Forensics Tools Been Tested?,* Computer Forensics Tool Testing Handbook., 2015;
10. Shimonski R., *The Wireshark Field Guide: Analyzing and Troubleshooting Network Traffic,* 2013;
11. Voas J., Quirolgico S., Michael C., Scarafone K., *Technical Considerations for Vetting 3rd Party Mobile Applications (Draft),* NIST, 2014;
12. Wang D., Zhang Z., Wang P., Yan J. and Huang X., *Targeted online password guessing: An underestimated threat,* 2016;
13. Zhang Y., Monrose F., and Reiter M., *The security of modern password expiration: An algorithmic framework and empirical analysis*, 2010.

Adrian Victor VEVERA – este director tehnic, cercetător științific gradul II și membru în Consiliul Științific al Institutului Național de Cercetare-Dezvoltare în Informatică. Doctor în științe militare și informații, fiind la bază atât jurist cât și inginer specializat în fizică nucleară, deține o vastă experiență în ceea ce înseamnă securitatea națională, ocupând, de-a lungul timpului, numeroase poziții manageriale și de consiliere în diverse organisme ale statului. A publicat numeroase articole și lucrări pe teme de securitate națională și internațională, securitate energetică, criminalitate informatică, protecția infrastructurilor critice și a fost coordonatorul a numeroase proiecte de interes național.

Adrian Victor VEVERA – is a Senior Researcher II, the Technical Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics. Doctor of Military Sciences and Information, being both a lawyer and a nuclear physics engineer, Mr. Vevera has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counseling positions in different state organisms. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.

Deniss Bogdan ONOFREI-RIZA – este Specialist în Tehnologia Informațiilor și Comunicațiilor în cadrul departamentului RoTLD al Institutului Național de Cercetare-Dezvoltare în Informatică. A deținut numeroase poziții manageriale în diferite medii organizaționale private și de stat, academice și de cercetare-dezvoltare. A îndeplinit sarcini polivalente în diferite proiecte de cercetare – dezvoltare în domeniul IT&C, având expertiză în securitatea informațiilor și tehnologia comunicațiilor, auditor, atât la nivel de rețea informatică cât și la nivel de aplicații (desktop + mobile), în sisteme de securitate fizică, baze de date SQL și NOSQL. Complementar a desfășurat activități cu un grad ridicat de complexitate ca Auditor IT&C, dezvoltator, sau depanator pentru aplicații desktop (diferite sisteme de operare). Este specialist „ethical hacker“, având cunoștințe avansate în domeniul forensicului digital, fiind trainer în domeniul criminalisticii digitale avansate.

Deniss Bogdan ONOFREI-RIZA – is a Specialist in Information Technology and Communications within the RoTLD department of the National Institute for Research and Development in Informatics. He has held numerous managerial positions in various private, state, academic and research-development organizational environments. He has accomplished multifaceted tasks in various research and development projects in the field of IT & C, with expertise in information security and communications technology, auditor at both computer network and application level (desktop + mobile), physical security systems, SQL databases and NOSQL. Complementary he has performed highly complex activities such as IT & C Auditor, developer, or troubleshooter for desktop applications (various operating systems). He is an „ethical hacker“ specialist with advanced knowledge of digital forensics, being a trainer in advanced digital forensics.