Criminalistica mobilă

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

Rezumat: „Revoluția informațională“ precum și dezvoltarea fantastică a „lumii IT-ului“ vin și marchează Secolul al XXI-lea, un martor al apariției și evoluției continue a dispozitivelor mobile. Echipamente compacte ce combină caracteristicile tradiționale ale telefonului celular cu funcționalitatea calculatorului personal, dispozitivele mobile actuale sunt rezultatul unei creșteri tot mai mari a posibilităților tehnice oferite de platformele hardware și sistemele de operare aferente acestora (Android, iOS, Windows Phone, BlackBerry). Dispozitivele mobile inteligente ale zilelor noastre sunt utilizate din ce în ce mai puțin pentru apeluri și din ce în ce mai mult pentru socializare și informare! Astfel, dispozitivul mobil inteligent a devenit un depozit complex de date sensibile ce ajută la identificarea „comportamentului“ proprietarului / deținătorului său. Acest lucru a generat evoluția criminalistică a dispozitivelor mobile, o ramură a „forensicului digital“ care se ocupă cu recuperarea datelor stocate de către un dispozitiv mobil.

Cuvinte cheie: Sisteme de operare, criminalistica mobilă, date.

Mobile Forensics

Abstract: The "Informational Revolution" as well as the fantastic development of the "IT world" come and mark the XXI century, as a witness to the emergence and continued evolution of mobile devices. Compact equipment that combines traditional cell phone features with personal computer functionality, today's mobile devices are the result of a growing number of hardware and operating systems (Android, iOS, Windows Phone, BlackBerry). Today's smart mobile devices are being used less and less for calls and more and more for socializing and information! Thus, the intelligent mobile device has become a complex storage of sensitive data that helps identify the "behavior" of its owner. This has generated the forensic evolution of mobile devices, a branch of "digital forensics" dealing with the recovery of data stored by a mobile device.

Keywords: Mobile devices, mobile forensics, data.

Introducere

Creșterea populației mondiale și a dependenței de tehnologie se accelerează în fiecare zi. În aceeași măsură, bazată pe creșterea revoluționară a tehnologiei, este și dezvoltarea criminalității informatice. Dispozitivele mobile, în continuă expansiune hardware\software, sunt în aceeași măsură și mijloace de comunicare portabile, dar și echipamente ce stochează informații personale sensibile. Informațiile conținute de către un dispozitiv mobil descriu în mare parte acțiunile și faptele deținătorului, de aceea, ele sunt atât ținta atacurilor cibernetice tradiționale cât și a dezvoltatorilor de soft malițios (în încercarea de a le ‘altera’ sau manipula).

Datorită resurselor de procesare reduse, a multitudinii de arhitecturi CPU și a varietății sistemelor de operare protejate la acces, recuperarea dovezilor digitale conținute de către un dispozitiv mobil este un proces destul de complex.

La nivelul dispozitivului mobil, datele de colectat se află în 3 ‘locații’ distincte din punct de vedere hardware: SIM, memorie internă și card SD. Toate aceste trei componente conțin date valoroase, însă stabilirea corectă a autenticității acestora, precum și a lanțului logic de stocare în timp, necesită dezvoltarea unei arhitecturi de referință capabile de a corela aplicațiile ce generează aceste elemente cu utilitarele de sistem mobil.

În sprijinul stabilirii autenticității datelor vin și o serie de aplicații mobile ce, din dezvoltare inițială, generează jurnale de log și audit intern la nivel de entitate software. De asemenea, un alt element de luat în calcul este și sincronizarea fișierelor de sistem cu artefactele ce pot fi generate de către modificarea manuală a diferitelor date, precum și cu evenimentele de 'kernel mobil'. Mai mult decât atât, este necesar a fi atent analizate locațiile de memorie în care utilizatorul nu are acces (mod normal de lucru).

Un sistem capabil de a extrage și arhiva datele conținute de către aceste dispozitive, trebuie să includă: o cameră digitală, un suport de memorie extern (HDD, SSD, NAS, etc.), un blocator la scriere pentru carduri SD, un dispozitiv de colectare a datelor (hardware\software), un cititor de carduri SIM și un set de adaptoare aferent multitudinii de conectori aferenți structurilor hardware mobile.

Procesul de extragere și analiză a datelor digitale conținute de către dispozitivele mobile diferă de la caz la caz, însă, în general, sunt recomandate următoarele: cercetarea dispozitivului și identificarea tipurilor de date, documentarea aplicațiilor instalate manual, identificarea documentelor sau a notelor importante (scrise sau video) precum și a modalității de stocare locală sau transmitere la distanță a acestora, identificarea informațiilor senzitive cu ajutorul unor algoritmi de căutare dezvoltați personalizat, corelarea jurnalelor de apeluri cu persoanele de contact, calendar dar și note aferente acestor înregistrări, identificarea și analiza amănunțită a aplicațiilor ce permit transfer de bani, imagini, fișiere audio sau video, identificarea aplicațiilor sau a datelor șterse din memorie (corelate cu evenimentele la nivel de 'kernel-sistem' sau cu artefactele existente).

Din punct de vedere al instrumentelor și tehnicilor utilizate pentru achiziția datelor digitale conținute de către dispozitivele mobile putem defini următoarele: extracția manuală, extracția logică, extracția de tip HEX și\sau JTAG și extracția de tip 'Cip-Off'.

Din punct de vedere al metodelor utilizate pentru achiziția datelor digitale conținute de către dispozitivele mobile putem defini următoarele: achiziția manuală, achiziția logică și achiziția fizică.

Principalul factor decizional în identificarea metodelor și instrumentelor de achiziție și analiză a datelor este sistemul de operare. Sistemele de operare mobile prezintă diferite particularități prin care pot fi accesate dispozitivele pe care rulează, astfel, doar un nivel destul de ridicat al cunoașterii platformelor mobile poate duce la rezultate solide, concludente, de neatacat în domeniul criminalisticii mobile.

CRIMINALISTICA MOBILĂ APLICATĂ

a. Sistemul de operare mobil Android

Accesarea diferitelor tipuri de fișiere din dispozitivul mobil este restricționată în funcție de sistemul de operare rulat. Asfel, dispozitivele *Android* ofera acces la zona de stocare internă și\sau la cardul SD, dispozitivele *iOS* permit accesul doar la zona media (imagini și video), dispozitivele Windows permit accesul la memoria internă și card SD, iar BlackBerry suportă transferul nativ al diferitelor fișiere (audio, video, imagini, documente, fișiere sistem).

În cadrul procesului de analiză criminalistică a oricărui sistem de operare, un rol important îl ocupă modalitatea în care acel sistem își organizează datele. Din punct de vedere al structurii de fișiere, datele conținute de către dispozitivele mobile sunt grupate în trei entități: spațiul de stocare intern, spațiul de stocare extern și spațiul de stocare securizat.

Extragerea datelor conținute de un dispozitiv mobil utilizând protocoale proprietare și interogări, definesc în mare parte colectarea logică. Una dintre cele mai utilizate metode ale acestei categorii este utilizarea unui software ce rulează pe dipozitivul *Android*, capabil de a interoga bazele de date interne și de a le transfera către sistemul de calcul, sub forma unor elemente reprezentative ale conținutului fișierelor de achiziționat. Astfel, rezultatul exportului către sistemul de calcul nu conține doar fișierele și directoarele dispozitivului de analizat, ci și configurații ale sistemului de

operare, ale utilizatorilor, alături de informațiile stocate de către aceștia. Dispozitivele mobile moderne permit utilizatorilor transferul de astfel de date chiar și fără instalarea agentului colector, protocolul MTP (Media Transfer Protocol) permițând copierea, mutarea, înlocuirea și\sau ștergerea fișierelor de pe și pe dispozitivul mobil.

Un alt element important ce conține date senzitive este cartela SIM. La acest nivel putem identifica informații referitoare la caracteristicile SIM-ului, parametri ai rețelelor mobile, un număr limitat de contacte și\sau SMS-uri, precum și jurnale de apel.

Colecții importante de date și informații referitoare la utilizatorul dispozitivului mobil, precum și la informațiile senzitive conținute de acesta, pot fi extrase și cu ajutorul metodologiilor de back-up intern, local, extern sau în Cloud. Un dispozitiv *Android* cuplat la un sistem de calcul, poate genera copii de siguranță (back-up) ale conținutului dispozitivului mobil, în aceeași măsură în care acesta este capabil de a stoca aceleași date într-o structură de tip Cloud. Versionarea în timp a acestor copii de siguranță, precum și algoritmii complecși capabili de a detecta elementele modificate, pot furniza informații prețioase referitoare la tiparul comportamental al utilizatorului, la nivelul de utilizare al aplicațiilor de sistem, precum și la localizarea fizică a acestuia.

Un alt protocol de transfer al fișierelor este OBEX (Object Exchange). Utilizarea acestuia poate fi utilă pentru a colecta date la un nivel cantitativ nu foarte mare, însă, la un nivel de intervenție ce nu impune instrumente specializate.

ADB (Android Debug Bridge) este un utilitar puternic, de tip linie de comandă, ce permite comunicarea cu un dispozitiv mobil *Android*. Cu ajutorul acestuia pot fi instalate și depanate aplicații, pot fi date comenzi către kernel-ul Linux, pot fi accesate fișiere, pot fi vizualizate informații senzitive stocate pe dispozitiv, dar mai ales, dă posibilitatea garantării dreptului autorizat la nivel de rădăcină (‘root’).

Pentru a obține accesul la fișierele stocate în zone securizate (criptate sau nu) cea mai utilizată metodă de escaladare a drepturilor de administrator, poartă denumirea de rutare (‘root’-are). Speculând vulnerabilitățile diferitelor versiuni ale sistemului de operare *Android*, la nivel de ‘firmware’ sau ‘kernel’ se ‘injectează’ un fișier de tip ‘Exploit’ ce facilitează (temporar sau definitiv) accesul la aceste informații securizate.

Un alt procedeu care facilitează accesul la o plajă destul de mare de informații senzitive este reprezentat de modalitatea în care un proces de start al sistemului de operare este întrerupt, fluxul logic fiind preluat și interpretat cu ajutorul comenzilor ce introduc dispozitivul în starea de recuperare a sistemului de operare mobil.

În cazul dispozitivelor ce stochează criptat informații, cheile de criptare se pot afla atât într-un coprocesor matematic, cât și în spații special destinate de memorie securizată, practic inaccesibile. În cazul acestor sisteme, dezvoltarea algoritmilor matematici de decriptare a cheilor reprezintă singurele modalități prin care informațiile pot fi recuperate.

Pentru a adăuga plus valoare reală elementelor obținute în urma aplicării metodelor mai sus menționate, există posibilitatea achiziției datelor direct din cipurile de memorie aflate pe placa de bază a dispozitivului mobil. Accesarea acestor date poate fi făcută atât prin conectarea unor dispozitive externe la placa de bază, cât și prin extragerea memoriilor sau a procesoarelor de pe aceasta și examinarea lor cu ajutorul unor instrumente de citire ‘flash’. Prin urmare, această colectare fizică a datelor implică o comunicare directă între memoria internă și diferite tipuri externe de instrumente specializate.

b. Sistemul de operare mobil iOS

Spre deosebire de *Android, iOS* este un sistem de operare mobil "închis", compania dezvoltatoare neacordând licența niciunei instalări efectuate pe dispozitive non-Apple. Atât la nivelul partiției de sistem, cât și la nivelul partiției ce conține datele utilizatorului, *iOS* stochează local 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 procedeul de achiziție a datelor conținute de dispozitivele mobile *iOS*, îl are identificarea corectă a modelului unui astfel de dispozitiv (pentru a înțelege structura hardware, capabilitățile acesteia, precum și pentru a selecta corect instrumentele hardware\software de lucru). Există dispozitive moderne *iOS* capabile de a rula simultan procese și informații comune, neidentificarea hardware corectă a acestora ducând ori la alterarea datelor de examinat, ori la pierderea acestora.

Metodele și instrumentele utilizate pentru a achiziționa date din dispozitivele mobile ce rulează *iOS*, depind foarte mult de cunoașterea celor trei stări de operare ale acestor dispozitive: modul de operare normal; modul de operare în vederea restabilirii sistemului; modul de operare DFU.

Starea în care rulează dispozitivul, modalitatea de securizare a acestuia, versiunea sistemului de operare și/sau modelul acestuia, sunt câțiva dintre parametrii de luat în calcul în vederea abordării și execuției procedurii de achiziție a datelor.

Spre deosebire de echipamentele pe care rulează *Android*, dispozitivele mobile *iOS* nu facilitează accesul la componentele plăcii de bază, în plus, ele comportându-se total diferit chiar și la conectarea acestora la un sistem de calcul. Fiind un sistem închis, *iOS* nu expune pe magistrala serială date senzitive (chiar și în faza în care este recunoscut ca o memorie externă, utilizatorul nu are drepturi depline asupra spațiului accesat).

Pentru anumite variante ale sistemului de operare mobil *iOS*, există posibilitatea, utilizând structuri Linux, de a accesa anumite zone ce conțin date importante. Există distribuții de Linux special modificate pentru a comunica cu anumite dispozitive mobile *iOS*. În aceeași măsură, există dezvoltate o serie de aplicații ce utilizează biblioteci software clasice Apple, iar, prin sincronizarea acestora cu dispozitivul mobil *iOS*, creează un lanț de încredere, accesând fișiere sensibile. Prin natura acestei metode, tipurile de date accesate diferă substanțial de la o variantă *iOS* la alta.

Procedeul ce are ca și rezultat escaladarea drepturilor de administrator la nivelul sistemului de operare mobil *iOS* poartă denumirea de 'Jailbreak' (asemănător 'root'-ului de *Android*, acesta implică utilizarea rutinelor software capabile de a specula anumite vulnerabilități ale sistemului mobil). Aplicabil peste modul normal de lucru sau cel 'DFU', 'Jailbreak' facilitează accesul către fișierele senzitive stocate în memorie, dând posibilitatea chiar și interconectării dispozitivului cu sistemul informatic, printr-un terminal de comandă sau unul SSH.

Clientul software dezvoltat de Apple pentru sistemele informatice de tip 'desktop' poartă denumirea de iTunes. La nivelul acestui utilitar rulează un serviciu ce interacționează direct cu mediul mobil *iOS*, indiferent de versiunea sistemului de operare. Această magistrală de comunicare poartă denumirea de AFC (Apple File Connection).

Există posibilitatea de a dezvolta aplicații capabile de a prelua controlul asupra acestui protcol (AFC), în scopul obținerii de informații senzitive, prin garantarea accesului securizat. În funcție de cunoștințele dezvoltatorului, există chiar și posibilitatea de a dezvolta lanț de încredere peste această comunicare, fără a avea utilitarul iTunes instalat.

Un dispozitiv mobil *iOS*, ce are aplicată cu succes o metodă de tip 'Jailbreak' și este, în același timp, accesat cu ajutorul serviciului AFC, este cazul ideal de a efectua o colectare adecvată. Tot la acest nivel, urmare cercetării, pot fi remarcate mecanisme de securitate internă Apple (de tip 'file relay', 'house arrest') ce pot fi speculate în vederea achiziției datelor de transferat de pe un dispozitiv mobil *iOS* necriptat.

Asemenea *Android*, în mare parte, tipurile de date colectate din dispozitivele mobile *iOS* pot fi de tip contacte, jurnal de convorbiri, SMS-uri, MMS-uri, calendar, note, imagini, videoclipuri etc.

Într-o ierarhie securizată, sistemul *iOS* memorează date în format text ce conțin numere seriale, date hardware legate de dispozitiv, rezultate temporare ale anumitor servicii, încercări de

conectare reușite sau eșuate a dispozitivelor externe, tipuri de aplicații rulate, precum și terțe alte informații ce descriu activitatea utilizatorului.

Universal utilizate, fișierele de tip JSON (Java Script Object Notation) sunt și ele tipuri de fișiere utilizate de către aplicațiile *iOS* pentru a rula. Acest tip de fișier poate conține proprietăți ale unor forme, șiruri de caractere, matrici de date, colecții de cuvinte ordonate după anumite chei și/sau alte tipuri de variabile utilizate de către *iOS*.

Acordând posibilitatea utilizatorilor de *iOS* de a-și creea propriile copii de siguranță, Apple pune la dispoziția acestora două elemente capabile de a susține acest proces: iTunes și iCloud. Decriptarea copiilor de siguranță, precum și păstrarea conținutului acestora, permite recuperarea unei cantități mari de informații senzitive, stocate la nivelul memoriei flash.

În funcție de versiunea *iOS* ce securizează dispozitivul mobil, există posibilitatea dezvoltării unor aplicații ”native”, semnate ”forțat”, capabile de a decripta anumite fișiere sau porțiuni ale memoriei, instalarea acestora obligatoriu fiind făcută de pe suport extern, apobat de către lanțul de încredere, dar neverificat de Apple. Cu ajutorul acestor utilitare pot fi extrase parole, secvențe de parole, fișiere proprietare ale nucleului de securizare, fișiere ce stochează configurări ale mecanismelor de siguranță etc.

Spre deosebire de metodele mai sus menționate, cea mai complexă modalitate de a achiziționa date este cea fizică (obținerea conținutului memoriei interne). În cazul *iOS*, achizițiile fizice reușite se bazează pe specularea diferitelor vulnerabilități ce pot apărea pe parcursul procesului ce lansează sistemul de operare, de aceea, metode de acest gen sunt foarte eficiente în cazul dispozitivelor mobile de generație mai veche. În cazul dispozitivelor parolate, achiziția fizică pune în evidență doar datele a căror criptare nu depinde de modalitatea de securizare a dispozitivului.

c. Sistemul de operare mobil WindowsPhone

Sistemului de operare *WindowsPhone* are la bază un nucleu puternic securizat, aplicațiile ce rulează pe dispozitivele mobile aferente neavând acces la acest nivel. Mai mult decât atât, portalul Microsoft Store rulează în fundal mecanisme controlate și securizate, destinate auditului software, furnizând astfel aplicații de încredere cu arhitecturi interne omogene și sigure.

Analizând modelul securității *WindowsPhone,* de luat în calcul pentru studiul metodologiilor de achiziție a datelor sunt următoarele două aspecte: identificarea unor vulnerabilități ce ar putea permite rularea unor aplicații peste sistemul de operare cu drepturi de administrator și posibilitatea injectării de cod malițios printre secvențele de execuție rezidente în memoria dispozitivului.

Fișierele de sistem ale *WindowsPhone* sunt similare cu cele utilizate de sistemele Windows 7, Windows 8 sau chiar Windows 10. Cele mai importante locații ce stochează date la nivelul dispozitivului mobil sunt: MyDocuments; Applications; ApplicationData; Windows.

Achiziția datelor conținute de către un dispozitiv mobil *WindowsPhone* este destul de dificilă, deoarece cele mai multe din metodele prezentate anterior, în cazul acestor dispozitive, nu funcționează. Există totuși posibilitatea de a instala un agent software capabil de a ocoli procedura Microsoft de înregistrare și etichetare a aplicațiilor, aplicație nepublicată și implicit nesemnată.

Din punct de vedere al securității, nucleul sistemului de operare *WindowsPhone* este aproape identic la toate variantele. Această caracteristică facilitează dezvoltarea de soft capabil de a prelua secvența de start a dispozitivelor mobile și de a modifica drepturile asupra sistemului de operare.

Un aspect foarte important de luat în calcul este posibilitatea pe care o acordă dezvoltatorii sistemului de operare mobil Windows 10, de a dezactiva criptarea după ce, în prealabil, aceasta a fost activată.

Toată gama de dispozitive mobile *WindowsPhone* oferă posibilitatea efectuării copiilor de siguranță a datelor, acestea fiind stocate la nivelul portalului web ‘OneDrive’. Prin instrumente specializate, există posibilitatea interceptării traficului de date dintre un dispozitiv mobil și ‘OneDrive’, a decriptării și a extragerii, într-un anumit format, a datelor transferate.

În cazul preluării datelor de pe dispozitivele ce rulează *WindowsPhone*, soluțiile comerciale nu ușurează foarte mult munca, datorită modalității dificile de acces la dispozitiv.

d. Sistemul de operare mobil al dispozitivelor de tip BlackBerry

Chiar dacă *BlackBerry OS*, în esență, este un sistem de operare proprietar, acesta rulează aplicații bazate pe tehnologie Java, singurul element de securitate al acestora fiind semnătura digitală.

Cele mai uzitate metode utilizate în achiziția datelor conținute de către dispozitivele *Black Berry*, se rezumă la JTAG și/sau CIP-Off (dar numai pentru modelele vechi). Există posibilitatea colectării datelor cu ajutorul unei simulări ce 'introduce' dispozitivul într-o stare generatoare de copii de siguranță. Aceste copii de siguranță (criptate sau nu) vor fi analizate mai târziu, offline, cu instrumente specializate.

Ultimul sistem de operare *BlackBerry* OS 10, cu o nouă arhitectură a kernel-ului, oferă posibilitatea utilizatorului de a cripta informațiile pe cardul SD, criptare bazată pe niște chei stocate într-o zonă de memorie de nerecuperat.

Există posibilitatea (pe baza interceptării schimbului de date dintre dispozitiv și serverul de *BlackBerry*) de a dezvolta niște algoritmi capabili să decripteze conținutul informațiilor partajate, pe baza cheilor rezultate fiind posibilă garantarea accesului către copiile de siguranță criptate offline.

Un avantaj deosebit în dezvoltarea acestor algoritmi îl are faptul că modalitatea de criptare nu este în funcție de echipamentul hardware ce o generează, cheia, în sine, rămânând neschimbată chiar și în momentul în care utilizatorul își resetează parola.

Cu un suport tehnic aproape inexistent și o cotă de piață foarte scăzută, dispozitivele mobile ce rulează *BlackBerry* OS nu mai sunt o prioritate nici pentru dezvoltatorii de instrumente comerciale capabile de a colecta datele conținute de către acestea. Există totuși dispozitive mobile *BlackBerry*, asupra cărora, se aplică cu succes metodele dezvoltate pentru platforma *Android*.

Concluzii

Criminalistica mobilă, parte a criminalisticii digitale, este acea entitate ce vizează recuperarea datelor conținute de către dispozitivele mobile, în condiții ce respectă cadrul juridic. Rezultatele obținute este ideal a fi reprezentate prin cópii identice ale datelor senzitive, efectuate fără a aduce modificări majore dispozitivului ce le stochează.

Colectarea, investigarea și evaluarea datelor conținute de către dispozitivele mobile, sunt principalele operațiuni ce definesc identificarea și interpretarea potențialelor dovezi conținute de către acestea.

Pentru a stabili corect autenticitatea datelor colectate, este necesară elaborarea unei arhitecturi capabile de a corela aplicațiile ce generează aceste date cu utilitarele de sistem mobil.

Prin diferite particularități, sistemele de operare mobile reprezintă elemente definitorii în identificarea metodelor de achiziție, precum și în selectarea instrumentelor (software\hardware) ce vor fi utilizate pe parcursul analizei datelor conținute de către dispozitivele ce le rulează.

Analizând structura de nucleu a arhitecturii de bază, sistemele de operare mobile nu permit (implicit) accesul la partițiile de sistem (locații proprietare) sau la datele senzitive stocate intern.

În plus, majoritatea sistemelor de operare mobile nu au inclus în distribuția de bază un manager de fișiere propriu (ci doar un utilitar ce facilitează accesul la zone de memorie comune, neprotejate).

Una dintre cele mai utilizate metode de extragere a datelor de pe dispozitivele mobile se concretizează în utilizarea unui software special conceput pentru a colecta și transmite mai departe (către un client extern) date senzitive (funcție de accesul pe care îl are la nivel de utilizator). Această metodă, combinată cu diferitele modalități prin care pot fi escaladate privilegii la nivelul sistemului de operare mobil, poate genera rezultate spectaculoase, atât în cazul dispozitivelor Android, cât și în cazul celor iOS.

Ceea ce aduce cu adevarat un plus de valoare informațiilor extrase cu ajutorul metodelor enumerate mai sus, este posibilitatea achiziției datelor direct din cip-urile de memorie în care sunt stocate.

O astfel de metodă implică conectarea fizică la placa de bază a dispozitivului mobil și executarea de comenzi la nivelul 'memoriilor', instrucțiuni generate de către utilitare (hardware\software) externe, dedicate activității de service GSM.

Pe un val puternic al expansiunii dispozitivelor mobile, criminalistica mobilă, știința ce 'vizează' dovezile digitale, definește o arie extrem de largă, cu multe particularități, dar și cu metode din ce în ce mai sofisticate de a colecta date stocate, primite sau transmise de un dispozitiv supus investigării.

BIBLIOGRAFIE

1. Belenko A., *Overcoming data protection to re-enable iOS forensics*, Black Hat USA, 2011;
2. Bennett D., *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, 2012;
3. Cruz F, Moser A, Cohen M., *A scalable file based data store for forensic analysis*, 2015;
4. Damshenas M., Dehghantanha A., *A survey on digital forensics trends*, 2014;
5. Franke, K., Srihari, *Computational Forensics: Towards Hybrid-Intelligent, Crime Investigation*, 2007;
6. Fuente JD., Santiago J., Román A., Dumitrache C., Casasanto D., *When you think about it, your past is in front of you: How culture shapes spatial conceptions of time*, 2014;
7. Grobler, T., Louwrens, B., Solms V., *A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations*, 2010;
8. Halbronn C., Sigwald J., Lab S., *iPhone security model & vulnerabilities*, 2010;
9. Katalov V., *Advanced Smartphone Forensics*, 2014;
10. Links E., *Cybercrime moving to smartphones and tablets, say experts*, 2015;
11. Willassen S., *Forensics and the GSM mobile telephone system*, 2003.

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.