MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

EXAMINAREA CRIMINALISTICĂ A DISPOZITIVELOR MOBILE

MOBILE DEVICE FORENSICS

Student: **Moloșag Nicolae**

Conducător: **Beșliu Victor**
conf. univ., dr. ing.

Chişinău, 2020

MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere, Șef departament: conf. univ., dr. Ion FIODOROV

_____

"__" _____2020

Examinarea criminalistică a dispozitivelor mobile

Teza de Master

Masterand: Moloșag Nicolae

Conducător: Beșliu Victor
conf. univ., dr. ing.

Chișinău, 2020

ADNOTARE

La proiectul de master: „Examinarea criminalistică a dispozitivelor mobile”, elaborat de Moloșag Nicolae, Chișinău, 2020.

Cuvinte cheie: smartphone, update, bootloader, forensics, kernel, software, hardware, OS.

Criminalistica dispozitivelor mobile, ca ramură a criminalisticii digitale, reprezintă entitatea ce vizează extragerea, recuperarea și analiza datelor conținute în memoria internă a dispozitivelor mobile, utilizând echipamente și metode prin care se respectă cadrul legal.

În teza de master s-a efectuat analiza situației în domeniul criminalisticii dispozitivelor mobile, analiza posibilităților programelor criminalistice, s-a descris procesul de extragere examinare și analiză a datelor. Au fost descrise regulile de ridicare a dispozitivelor, de elaborare a planșei fotografice, a unui raport de expertiză, iar în final a fost făcut un studiu comparativ ce ține de metodele utilizate la extragerea datelor și rezultatul final al acestora.

În conținut sunt: Introducere, 4 capitole, concluzii, și bibliografie (11 titluri). Conținutul este expus pe 63 de pagini și conține 38 figuri.

În capitolul 1 al tezei de master a fost descris domeniul criminalisticii dispozitivelor mobile, soluțiile software și hardware moderne utilizate în criminalistica dispozitivelor mobile, organizațiile specializate în domeniul dat.

În capitolul 2 sunt descrise din punct de vedere criminalistic modalitățile de securizare a dispozitivelor mobile, care sunt vulnerabilitățile lor și cum pot fi exploatate aceste vulnerabilități.

În capitolul 3 au fost descrise tipurile de dispozitive mobile, reguli tactice utilizate la ridicarea acestora, cadrul legal în activitatea expertului criminalist și etapele de pregătire spre examinare a dispozitivelor.

În capitolul 4 au fost analizate tipurile de date care pot fi extrase din memoria internă a dispozitivelor mobile, metode de extragere, au fost descrise regulile de efectuare a unei planșe fotografice și a unui raport de expertiză, iar în final a urmat partea practică a lucrării.

Lista de bibliografie include principalele surse de informare utilizate în procesul de proiectare.

ANNOTATION

At the master project: „Mobile device forensics", developed by Moloșag Nicolae, Chișinău, 2020.

Keywords: smartphone, update, bootloader, forensics, kernel, software, hardware, OS.

Mobile device forensics, as a part of digital forensics, represent an entity that is based on extraction, recovery and analysis of data stored in mobile devices internal memory, using equipment and methods of data collection which respects the law.

In the master's thesis, was analyzed the situation in the field of mobile device forensics, the forensics software opportunities, was described types of extractions and data analysis. Also was described the rules used for mobile devices confiscation, for photographic plan and report elaboration, and, at the end, it was made a comparison survey of a different data extraction methods.

The explanatory report contains: Introduction, 4 chapters, conclusions, and bibliography (11 titles). The content is exposed on 63 de pages and contains 38 figures.

In chapter 1 of the master's thesis, was made: the analysis of the studio domain, the detailed description of software and hardware modern solutions used in mobile device forensics, short description of national organizations involved in mobile device forensics.

Chapter 2 describes types of mobile devices security trough the forensics point of view, their weaknesses and how the expert can use them to gain data.

Chapter 3 describes types of mobile devices, rules used for mobile devices confiscation, legal limits of forensics expert activity and steps which are used before mobile devices examination.

In chapter 4 was analyzed types of data that can be extracted from mobile devices internal storage, types of extractions, also was described rules used for photographic plan and report elaboration, at the end, it was made a comparison survey of a different data extraction methods.

The bibliography list includes the main sources of information used in the thesis.

Cuprins

Introducere

Datorită evoluției avansate în domeniul tehnologiilor informaționale, precum și a dezvoltării rapide a dispozitivelor electronice, care și-au luat începutul din secolul XX până în prezent, suntem martori ai apariției și evoluției continue a dispozitivelor mobile. Astfel de dispozitive compacte îmbină caracteristicile de bază ale unui telefon celular cu posibilitățile unui calculator personal. Dispozitivele mobile moderne reprezintă o platformă bazată pe creșterea tot mai mare a posibilităților tehnice oferite de platformele hardware și a sistemelor de operare legate de acestea (Android și OS bazate pe acest sistem, 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.

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 dispozitiv de blocare a scrierii pentru carduri SD, un dispozitiv de colectare a datelor (hardware\software), un reader 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 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 file system, extracția fizică și extracția de tip ”Chip-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.

Concluzii

Revoluția în domeniul informațional cât și dezvoltarea rapidă a IT, sunt fenomenele caracteristice secolului al XXI-lea, moment cînd și-au făcut apariția și au evoluat continuu dispozitivele mobile. Aceste dispozitive de mărimi compacte, care îmbină mobilitatea și funcționalul unui laptop sau calculator, au evoluat de la primele telefoane cu butoane și funcții restrînse datorită avansării rapide a posibilităților tehnice oferite de platforme hardware și sisteme de operare dezvoltate pentru acestea (Android și sistemele de operare bazate pe această platformă, iOS, Windows Phone, BlackBerry).

Odată ce a crescut populația mondială, și dispozitivele mobile în fiecare an devin tot mai accesibile, crește și dependența oamenilor față de tehnologii, din motiv că prin dispozitivul mobil se poate de comunicat, de făcut achiziții, este acces la divertisment etc. În același timp, pas în pas cu evoluția tehnologiilor, este și dezvoltarea criminalității în spațiul internet, inclusiv cu utilizarea în aceste activități a dispozitivelor mobile. Aceste dispozitive care sunt în permanentă dezvoltare hardware și software, reprezîntă atât mijloace de comunicare, cât și mijloace de stocare a informațiilor personale, iar uneori și ca intermediari la manipularea de la distanță a altor dispozitive mobile (camere de luat vederi, drone, etc.).

Ca urmare a dezvoltării și utilizării în masă a dispozitivelor mobile, a apărut și se află în continuă evoluție criminalistica dispozitivelor mobile, ca ramură a criminalisticii digitale, și reprezintă entitatea ce vizează extragerea, recuperarea și analiza datelor conținute în memoria internă a dispozitivelor mobile, utlizând echipamente și metode prin care se respectă cadrul legal. Datele dobândite în urma manipulărilor cu dispozitivele ar fi recomandabil de reprezentat în format electronic, fără a fi efectuate modificări critice în dispozitivul mobil pe care sunt stocate.

Achiziția, examinarea și evaluarea fișierelor care se conțin în memoria internă a dispozitivelor mobile, reprezintă operațiunile de bază prin care se identifică și interpretează potențialele mijloace de probă care se regăsesc în acestea, iar pentru stabilirea corectă a autenticității datelor extrase, apare necesitatea de a elabora o arhitectură complexă ce va avea posibilitatea să coreleze aplicațiile care generează aceste date.

Practic, toate metodele moderne de extragere a datelor de pe dispozitivele mobile utilizează unul sau mai multe softuri specializate, care au fost create și dezvoltate pentru a selecta și transla mai departe pe un spațiu (în afara dispozitivului examinat) datele utilizatorului.

Aceste metode (logică, a sistemului de fișiere, fizică), în combinație cu diferitele modalități (de trecere peste măsurile de securitate) prin care pot fi dobândite privilegii la nivelul sistemului de operare a dispozitivului mobil, pot duce la rezultate impresionante, atunci când extragem datele din dispozitivele bazate pe Android, dar și în cazul când examinăm produsele Apple.

Ca urmarea a pătrunderii în viața de zi cu zi a tehnologiilor informaționale, inclusiv prin intermediul dispozitivelor mobile, criminalistica acestora, ca știința care se axează pe dovezi digitale,

este definită de o gamă destul de largă de posibilități, dispozitive și metode care sunt în permanentă dezvoltare, care permit achiziția datelor stocate pe un dispozitiv prezentat spre examinare.

Odată ce dezvoltatorii softurilor pentru dispozitivele mobile încearcă în permanență să actualizeze sistemele de operare, fapt ce duce la închiderea multor căi de utilizare a vulnerabilităților, producătorii de programe criminalistice sunt în căutarea altor posibilități de extragere a datelor, sau analizează noile actualizări pentru identificarea altor vulnerabilități (de asta se preocupă și dezvoltatorii de malware). Deci, între aceste două categorii există o permanentă ”cursă a înarmărilor”, iar uneori, pentru a face o achiziție de date dintr-un dispozitiv nou, este necesăr să așteptăm un update al programului crimininalistic.

Achiziția de date din dispozitiv este foarte importantă și uneori complicată, însă procesul de probare în totalmente este mult mai complex. Ca datele extrase din dispozitive să aibă valoare probantă este obligatoriu să ne menținem de cadrul legal și de un set de proceduri, ca ulterior, aceste date să poată fi incontestabile în instanță.

Bibliografie

1. Specialist hardware for all weathers, (online), [citat 25.11.2020]. Disponibil: https://ondatashop.com/msab-field/.
2. UFED Touch 2, (online), [citat 25.11.2020]. Disponibil: http://aimtech.ru/catalog/155.
3. Visual nand reconstructor kit, (online), [citat 25.11.2020]. Disponibil: https://rusolut.com/wp-content/uploads/2014/01/VNRkit.jpg.
4. USB SIM reader copier for GSM SIM card, (online), [citat 25.11.2020]. Disponibil: https://www.lelong.com.my/usb-sim-reader-copier-gsm-sim-card-newfroggyonline-214840878-2019-12-Sale-P.htm.
5. Digital Intelligence's Ultra Block Forensic Card Reader, (online), [citat 25.11.2020]. Disponibil: https://www.insectraforensics.com/Forensic-Card-Reader/es.
6. Xiaomi QIN 1S 4G Feature Phone 256MB RAM 512MB ROM Chinese & English Version, (online), [citat 27.11.2020]. Disponibil: https://gearvita.com/xiaomi-qin-1s-4g-feature-phone.html.
7. Смартфон Samsung Galaxy J3 SM-J320H Gold, (online), [citat 27.11.2020]. Disponibil: https://shop.kyivstar.ua/smartphones/sm-j320hzddsek.html.
8. Tableta Allview Viva C703 7 8GB Android 8.1 Black VIVAC703, (online), [citat 27.11.2020]. Disponibil: https://www.cel.ro/tablete/tableta-allview-viva-c703-7-8gb-android-8-1-black-pMyI6MTctNw-l/.
9. Κλωνοποίηση καρτών Sim, (online), [citat 30.11.2020]. Disponibil: https://www.gps-trackers.gr/klonopoiisi-karton-sim.html.
10. Ultra Block Forensic Card Reader, (online), [citat 30.11.2020]. Disponibil: https://www.insectraforensics.com/Forensic-Card-Reader.
11. DJI Phantom 4 Advanced Plus 4k Camera Drone, (online), [citat 30.11.2020]. Disponibil: https://hire.empire.as/shop/drones-gimbals/hire-dji-phantom-4-advanced-plus-melbourne/.