Criminalistică mobilă

Analiza de tip “forensic” pentru dispozitivele mobile.

Mihai GHITA

Universitatea Titu Maiorescu

CYBERX

Stagii de practică în centrul de excelență în securitate cibernetică în cloud

Program cofinanțat din Fondul Social European prin Programul Operaţional Capital Uman 2014-2020

CyberX

- Formare si pregatire tehnica de specialitate in domeniul securitatii cibernetice in vederea pregatirii de viitori specialisti.
- Acces liber la tehnologii de securitate cibernetica, de ultima generatie prin Centrul de Excelenta CyberX
- 11 solutii de securitate cibernetica – scannere de vulnerabilitati, cyber security analytics, UTM (Unified Threat Management), Priviledged Access Management
- **Sisteme expert de forensic in dispozitive fixe si mobile.**

CELLEBRITE MOBILE FORENSICS FUNDAMENTALS

cellebrite mobile forensics fundamentals

CMFF

certificate of completion

Certificate number:1973568000

Mihai GHITA

CELLEBRITE CERTIFIED LOGICAL OPERATOR

cellebrite certified CCLO logical operator

Certificate number:2033568000

Mihai GHITA

CELLEBRITE CERTIFIED PHYSICAL ANALYST

cellebrite certified CCPA physical analyst

Certificate number:20203568000

Mihai GHITA

CELLEBRITE CERTIFIED MOBILE EXAMINER

cellebrite certified CCME mobile examiner

Certificate number:9443568000

Mihai GHITA

has successfully completed an approved advanced level course of study in UFED Series hardware and software methodology and has successfully demonstrated knowledge, skills and proficiency to be recognized as a Cellebrite Certified Mobile Examiner

Awarded this 16 day of January, 2017

Cellebrite Certified Instructor

UFED series

Director of Global Training

MINISTERUL EDUCAȚIEI
UNIVERSITATEA „TITU MAIORESCU" DIN BUCUREȘTI
Calea Văcărești nr. 187, sector 4, București, cod 040051
tel.: 021 316 16 46, fax: 021 311 22 97, e-mail: rectorat@univ.utm.ro, www.utm.ro

Ce este criminalistica mobilă

- NIST descrie "știința criminalistică" ca fiind "aplicarea științei la lege". Criminalistica poate include examinarea științifică a fosilelor, a unei scene a crimei, a metalelor, a vehiculelor, a corpurilor postmortem și desigur, **datelor digitale în multe forme diferite**.
- **Criminalistica dispozitivelor mobile** este o ramură a **criminalisticii digitale** referitoare la recuperarea probelor digitale sau a datelor de la o **dispozitiv mobil** în condiții criminalistice conforme cu procedurile standard.
- Expresia dispozitiv mobil se referă de obicei la telefoanele mobile; cu toate acestea, se poate referi, de asemenea, la orice dispozitiv digital care are atât memorie internă, cât și capacitate de comunicare, inclusiv dispozitive PDA, dispozitive GPS și computere tabletă.

Istoricul dispozitivului mobil

- La 3 aprilie 1973, **Martin Cooper (Motorola)** l-a sunat pe Joel Engle de la Bell Labs, principalul concurent al Motorola, de pe un telefon portabil, de pe străzile din New York City.
- DynaTAC (DYNamic Adaptive Total Area Coverage) 8000x
- Acest dispozitiv a fost aprobat de Comisia Federală de Comunicații din SUA (FCC) pe 21 septembrie 1983 și a fost oferit comercial în 1984.

2014!

- În 2014, Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update a indicat că numărul de dispozitive mobile utilizate a depășit populația lumii.

- În februarie 2017, același studiu realizat de Cisco a arătat că "dispozitivele mobile și conexiunile în 2016 au crescut la 8 miliarde".

2024!

- În 2024, se estimeaza că există peste 16 miliarde de dispozitive mobile în lume, din care peste 7 miliarde sunt smartphone-uri. Aproape fiecare om de pe planeta are un smartphone.

- În 2024, se estimeaza că peste 60% din traficul internet mondial este realizat prin dispozitive mobile.

MINISTERUL EDUCAȚIEI
UNIVERSITATEA „TITU MAIORESCU" DIN BUCUREȘTI
Calea Văcărești nr. 187, sector 4, București, cod 040051
tel.: 021 316 16 46, fax: 021 311 22 97, e-mail: rectorat@univ.utm.ro, www.utm.ro

Terminologie și acronime în domeniul tehnologiei mobile

- AMPS/NMT/TACS
  - Advanced Mobile Phone System (AMPS) a fost standardul analogic utilizat în Statele Unite ale Americii
  - Nordic Mobile Phone (NMT) a fost standardul analogic în țările nordice
  - Total Access Communications Systems (TACS) a fost standardul analogic în Regatul Unit
  - Această tehnologie a fost numită mai târziu 1G, pentru prima generație
- TDMA/GSM/CDMA
  - Time Division Multiple Access (TDMA) și Code Division Multiple Access (CDMA) sunt tehnologii 2G (a doua generație), iar aceste dispozitive au intrat pe scena portabilă în anii 1990.
  - Principalele standarde pentru 2G sunt GSM, Interim Standard 95 (IS-95) (CDMA), IS-136 (amplificatoare digitale) și iDEN (Integrated Digital Enhanced Network).
  - Cea mai mare schimbare a fost de la analogic la digital, împreună cu criptarea digitală a transmisiei.
  - S-a născut SMS-ul

“MERRY CHRISTMAS”

- 3 Decembrie 1992. Primul SMS trimis vreodata.
- Neil Papworth i l-a trimis lui Richard Jarvis, unul dintre directorii Vodafone.
- Jarvis avea un telefon “mobil” Orbitel, care cântărea două kilograme.
- SMS-ul a fost vandut in 2022, ca NFT, pentru 132.680 de euro

MINISTERUL EDUCAȚIEI
UNIVERSITATEA „TITU MAIORESCU" DIN BUCUREȘTI
Calea Văcărești nr. 187, sector 4, București, cod 040051
tel.: 021 316 16 46, fax: 021 311 22 97, e-mail: rectorat@univ.utm.ro, www.utm.ro

Terminologie și acronime în domeniul tehnologiei mobile

- UMTS/CDMA2000
  - Universal Mobile Telecommunications System (UMTS) și IS-2000 (CDMA2000) sunt 3G sau a treia generație
  - Streaming video și de date

  UMTS a făcut upgrade la HSDPA (High-Speed Downlink Packet Access) și a fost combinat cu HSUPA (High-Speed Uplink Packet Access) pentru a forma HSPA (High-Speed Packet Access), care este încă cea mai răspândită tehnologie la nivel global. Ceea ce ar putea fi denumit 3.5G este dezbătut ca HSPA + și, de asemenea, LTE (Long Term Evolution). LTE este adesea menționat în ceea ce privește tehnologiile 4G, dar ratele de încărcare și descărcare a datelor nu îndeplinesc standardele stabilite de ITU (Uniunea Internațională a Telecomunicațiilor) pentru a o numi 4G.
- LTE-Avansat
  - (LTE-A) este, de asemenea, definit de ITU - un adevărat sistem 4G
- IMT-2020 (5G)
  - Sistemele internaționale de telecomunicații mobile (IMT) 2020 sunt, de asemenea, definite de ITU, iar în prezent este un sistem teoretic 5G.

  Specificațiile actuale de la ITU indică o capacitate de descărcare de cel puțin 20 Gbps (gigabiți pe secundă) pentru o singură celulă, cu suport pentru un milion de dispozitive conectate pe un kilometru pătrat

  Acest tip de conexiune wireless va avea un impact semnificativ asupra utilizării dispozitivelor purtabile și a altor dispozitive IoT.

Acul în Carul cu Fân

- Peste 10.000 de mesaje SMS
- Peste 30.000 de mesaje de chat
- Peste 5.000 de imagini
- Peste 10.000 de e-mailuri
- Calendarul a explodat cu date
- Istoric nesfârșit de navigare pe web
- Fișiere media: Video, Audio
- Jurnale de apeluri, aplicații
- Jurnale de călătorie, Contacte și multe altele

Exista cazuri cu mai multe dispozitive

Cum tratam un dispozitiv mobil

- Un dispozitiv mobil poate conține multe informații, de la contacte, SMS-uri și jurnale de apeluri în dispozitivele vechi, la documente complexe, aplicații, media, SMS, Serviciul de mesagerie multimedia (MMS), jurnale de apeluri, e-mail, calendar, note și contacte în dispozitivele moderne.
- Aplicațiile sau aplicațiile încorporate pot stoca tipuri de date suplimentare, pot comunica cu Internetul, pot lansa rachete, pot reda muzică, pot cartografia o casă, pot direcționa un vehicul către o destinație, pot determina parametri corpului omenesc și pot efectua tranzacții bancare.
- Dispozitivele mobile au toate formele și dimensiunile și au progresat de la circuite de memorie mici, la mai mult de 256 GB de spațiu de stocare.
- Modulele SIM și UICC Subscriber sau cartelele SIM au fost dezvoltate pentru a permite portabilitatea și, mai important, pentru a stoca informații pentru a permite autentificarea în rețeaua celulară.
- Cardurile SD media storage cards au fost create într-un efort de a extinde spațiul de stocare disponibil pentru dispozitivele mobile. SDXC, lansat în 2009, acceptă până la 2 TB de date, iar unele dispozitive mobile actuale vor suporta și recunoaște carduri în dimensiunea micro de peste 2TB.

- Pentru a fi un medic legist cu adevărat bun, examinatorul trebuie să înțeleagă specimenul.

Resurse educaționale

- Telefon Scoop (www.phonescoop.com/phones/finder.php)
  - Conține informații valoroase pentru a ajuta la identificarea și cercetarea dispozitivului care urmează să fie examinat.
- GSMArena (www.gsmarena.com/search.php3)
  - Este la fel ca Telefon Scoop, dar acest site conține numai dispozitive GSM și este în primul rând pentru dispozitive din afara Americii de Nord
- Mobile Forensics Central (www.mobileforensicscentral.com/mfc)
  - Utilizați Mobile Forensics Central căutând în baza sa de date pentru a găsi un raport de telefon care listează software-ul dispozitivului mobil și informațiile suplimentare necesare pentru procesare.
- Forensic Focus (www.forensicfocus.com/computer-forensics-forums)
  - Acest forum este destinat comentariilor și întrebărilor legate de forensic din Europa.
- Forumul dezvoltatorilor Android (developer.android.com/index.html)
  - În acest forum veți găsi informații despre dezvoltatori pe sistemul de operare Android
- XDA Developers Forum (www.xda-developers.com)
  - Acest site conține un forum împreună cu resurse de dezvoltare pentru dispozitive inteligente, în primul rând Windows și Android. În 2010, a fost lansat un site similar, iPhone-Developers.com.

Organizaţii

- Asociația Internațională a Specialiștilor în Investigații Informatice (IACIS)
  - IACIS este o corporație non-profit internațională bazată pe voluntariat, care oferă formare și educație în informatică criminalistică și acordă certificarea Certified Forensic Computer Examiner (CFCE).
- Societatea Internațională de Examinatori Criminaliști (ISFCE)
  - ISFCE este o organizație privată care desfășoară activități de cercetare și dezvoltare a tehnologiilor noi și emergente în știința criminalisticii informatice. ISFCE acordă certificarea Certified Computer Examiner (CCE).

- Aplicarea proceselor și procedurilor forensic:
  - Atât IACIS, cât și ISFCE urmează procese și proceduri similare în cerințele lor de competență, înainte ca un candidat să poată deveni certificat pentru a examina dovezile digitale computerizate.

Procese și proceduri de forensic

- Sechestru
  - Orice anchetă privind probele electronice trebuie să înceapă cu confiscarea legală a dispozitivului care deține, deținea, primea sau transmitea informațiile stocate electronic (ESI). Etapele legale corespunzătoare vor fi determinate de situație. ESI se află într-un loc care necesită obținerea unui mandat de percheziție, care este deținut de o corporație sau care necesită permisiunea proprietarului? În cazul în care confiscarea dispozitivului și datele ulterioare sunt afectate de întrebări privind legalitatea modului în care au fost obținute datele, informațiile colectate vor fi respinse în cadrul procedurilor ulterioare.

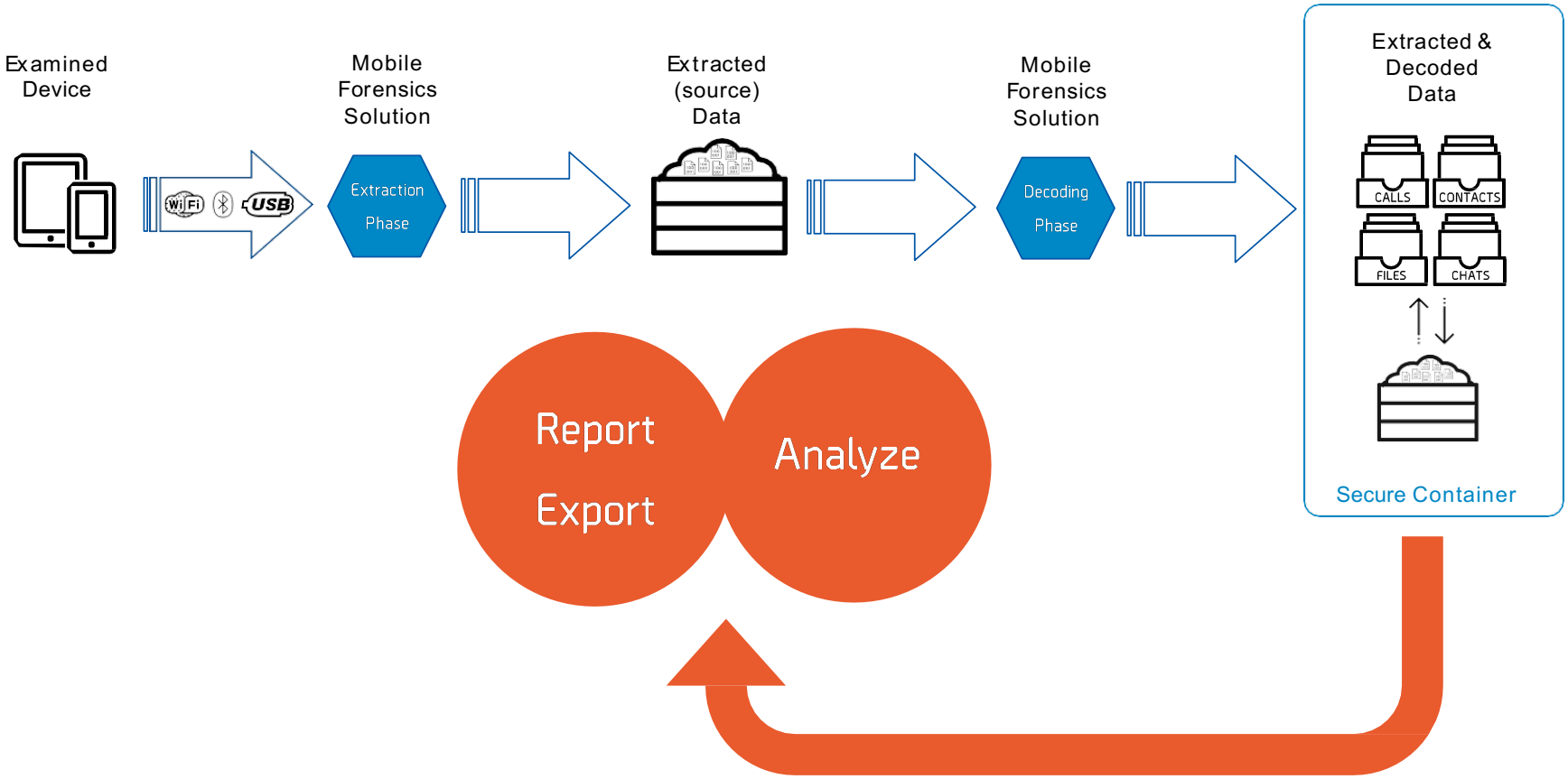
- Colectare
  - Trebuie să extrageți date de pe un dispozitiv digital într-un mod care vă permite să demonstrați că ESI nu s-a modificat, nu a fost modificat și este același ca atunci când a fost colectat. Datele colectate conțin, de obicei, o amprentă electronică. Dacă orice date sunt modificate, adăugate sau eliminate din containerul de date colectat, amprenta electronică se va schimba. Integritatea colectării datelor digitale și validarea și verificarea software-ului care a colectat dispozitivul sunt responsabilitatea persoanei care efectuează colectarea.

Procese și proceduri forensic

- Analiză/Examinare
  - Analiza datelor care au fost colectate de la dispozitivul confiscat este adesea cea mai obositoare parte a unei examinări. Analiza multor GB de informații este o muncă dificila, chiar și cu instrumente automate.

- Prezentare
  - Odată ce analiza este finalizată cu privire la datele confiscate și colectate, examinatorul trebuie să prezinte informațiile, de obicei printr-un raport scris.
  - Prezentarea este cea mai importantă piesă pentru cei care vor revizui și cel mai probabil, vor acționa asupra informațiilor care au fost recuperate și analizate. Prezentarea trebuie să arate întregul proces, inclusiv orice probleme întâmpinate, de la sechestru la analiză. Partea de analiză trebuie să fie documentată în mod clar în ceea ce privește cererea, metodologia și constatările. Examinatorul poate avea cele mai multe dificultăți în acest stadiu, deoarece examinatorii tehnici adesea nu comunică bine cu persoanele non-tehnice.

Procese și proceduri forensic



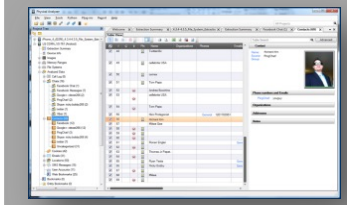
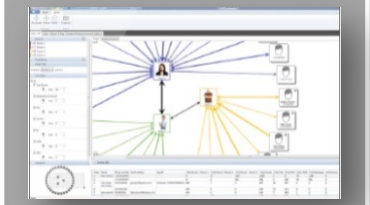
Extractia

Câteva exemple de Solutii utilizate in forensic.

Forensic Process

cellebrite
delivering mobile expertise

Universal Forensic Extraction Device (UFED)

Phone Identification	Extraction	Decoding/ Analysis	Link Analysis/ Reporting
UFED Phone Detective for Desktop/Mobile 	**UFED Touch**  **UFED 4PC**  **UFED TK**  **UFED CHINEX** 	**UFED Physical/Logical Analyzer** 	**UFED Link Analysis** 

The Right UFED for Me

cellebrite
delivering mobile expertise

UFED Touch

- Echipament dedicat
- Protejat la modificari si instalare de alte aplicatii
- Nu necesita administrare speciala
- Utilizat la extractii de date

UFED 4PC

- Solutie de tip All-in-one, continue toate instrumentele necesare
- Nu este nevoie de altceva in activitatea de forensic
- Hardware la alegerea analistului
- Flexibilitate maxina

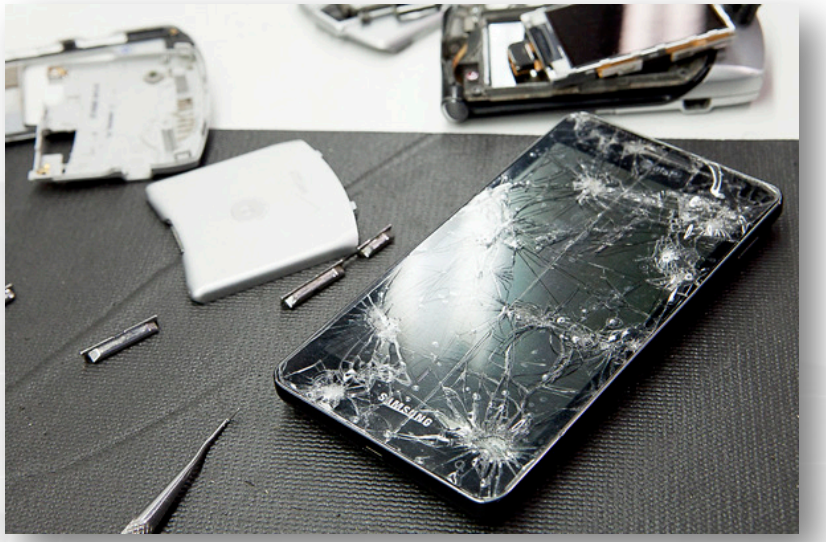
UFED TK

- Solutie de tip All-in-one, continue toate instrumentele necesare
- Nu este nevoie de altceva in activitatea de forensic
- Hardware adaptat si optimizat
- Protejat logic si fizic prin ruggedizare

JTAG (Joint Test Action Group)

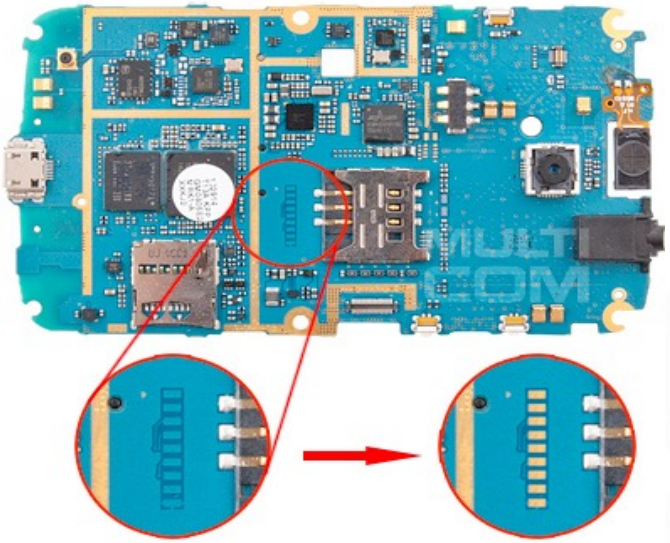
cellebrite
delivering mobile expertise

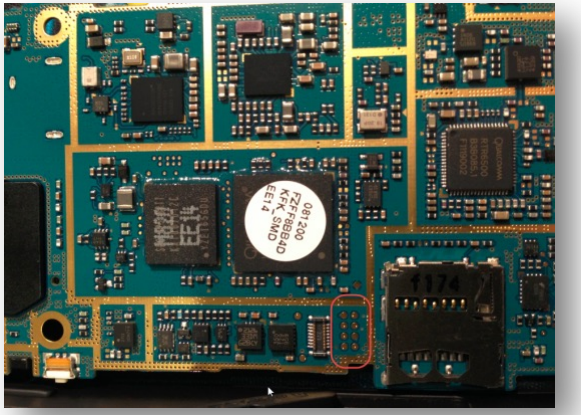
- Dezvoltat in 1990 este standard pentru testarea circuitelor.
- Permite metode avansate de extractive.
- Permite access la dispositive distruse, blocate, sau fara port de date.



JTAG

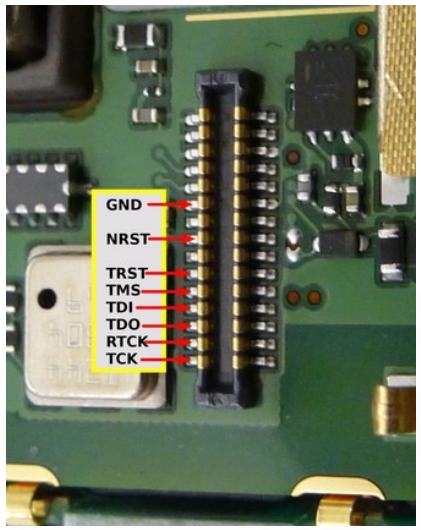
cellebrite
delivering mobile expertise

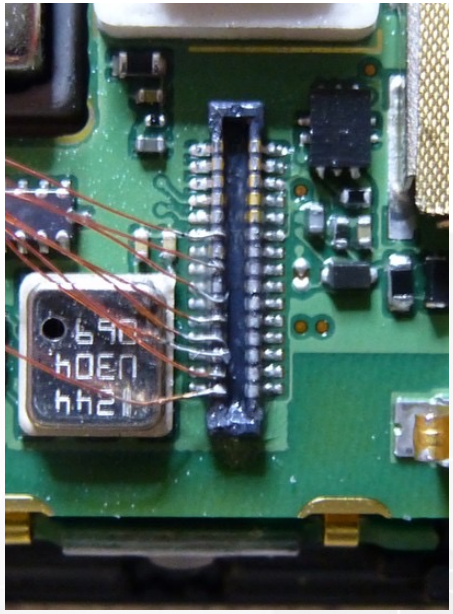




JTAG Data Extraction

cellebrite
delivering mobile expertise





cellebrite
delivering mobile expertise

Exact location and cloud tokens

Facebook

Twitter

KiK

Dropbox

Gmail

Google Drive

Analiza

Câteva exemple de solutii utilizate in analiza forensic.

Acul în Carul cu Fân

- Peste 10.000 de mesaje SMS
- Peste 30.000 de mesaje de chat
- Peste 5.000 de imagini
- Peste 10.000 de e-mailuri
- Calendarul a explodat cu date
- Istoric nesfârșit de navigare pe web
- Fișiere media: Video, Audio
- Jurnale de apeluri, aplicații
- Jurnale de călătorie, Contacte și multe altele
- Text, imagini, audio si video din Cloud si Social Media

Link Analysis

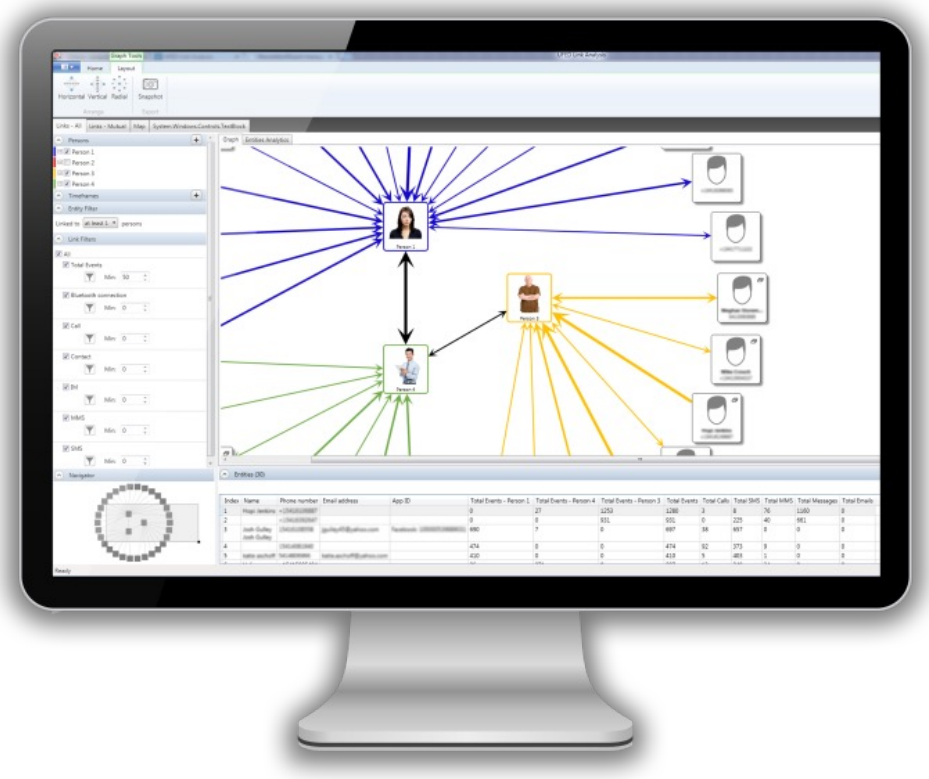
Descoperirea relatiilor intre mai multe dispozitive

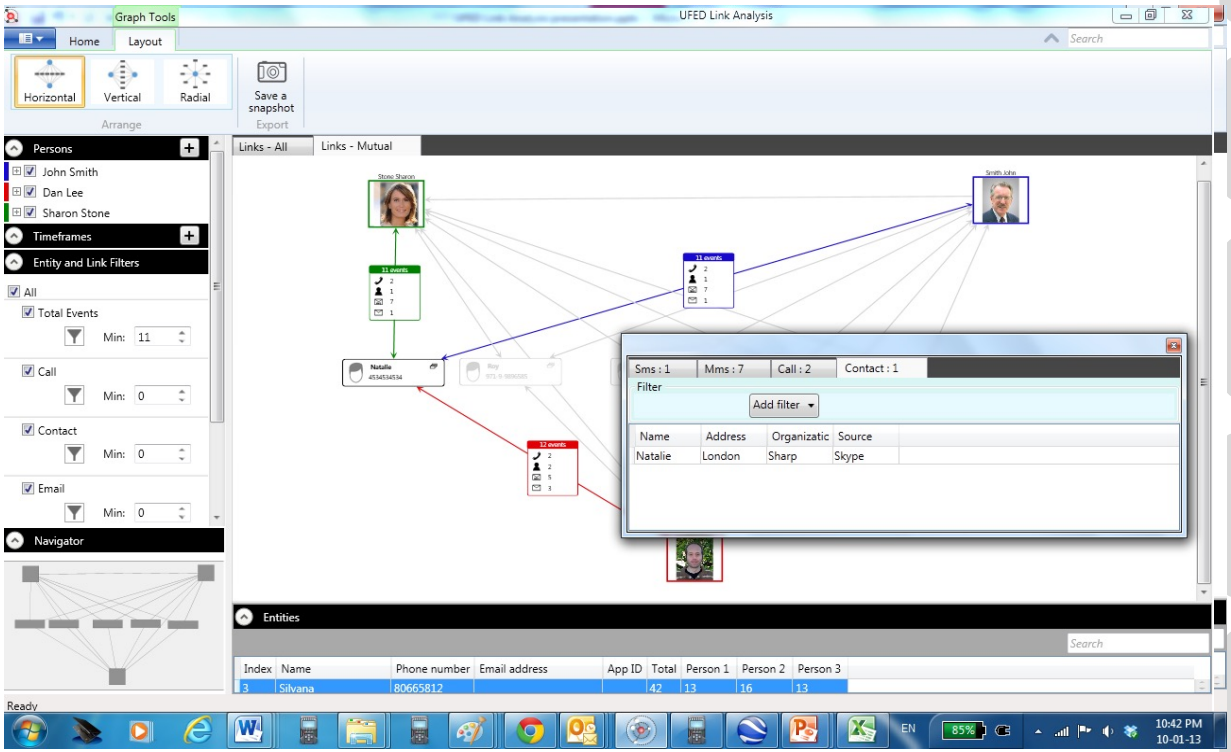
MINISTERUL EDUCAȚIEI
UNIVERSITATEA „TITU MAIORESCU" DIN BUCUREȘTI
Calea Văcărești nr. 187, sector 4, București, cod 040051
tel.: 021 316 16 46, fax: 021 311 22 97, e-mail: rectorat@univ.utm.ro, www.utm.ro

Link Analysis

Descoperirea relatiilor intre mai multe dispozitive.

- Cautari relevante pentru investigatii.
- Multiple device-uri si entitati.
- Descoperirea relatiilor dintre acestea.
- Analiza mai multor entitati/suspecti pe acceasi harta relationala.
- Analiza incrucisata cu baze de date existente.





Avem 3 suspecti

Se cunosc, sau macar au vorbit toti cu aceleasi persoane?

Care sunt conexiunile importante pentru investigatii?

Cat de frecvent comunica?

Cum putem raspunde in cel mai scurt timp?

AI / ML

Utilizarea NLP pentru Sentiment Analysis

MINISTERUL EDUCAȚIEI
UNIVERSITATEA „TITU MAIORESCU" DIN BUCUREȘTI
Calea Văcărești nr. 187, sector 4, București, cod 040051
tel.: 021 316 16 46, fax: 021 311 22 97, e-mail: rectorat@univ.utm.ro, www.utm.ro

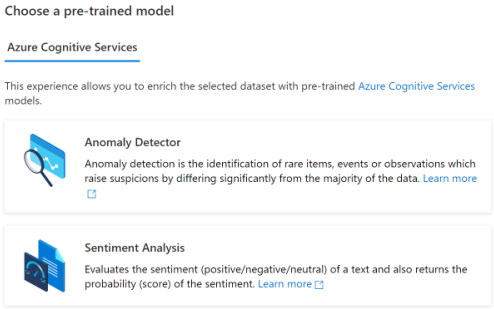
Utilizarea NLP pentru Sentiment Analysis

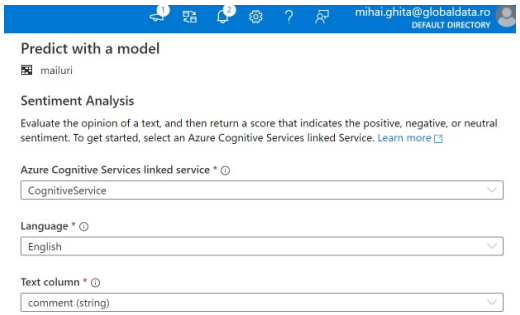
- Sentiment Analysis
  - Domeniu al procesarilor NLP care se ocupa in principal cu:
    - monitorizarea rețelelor sociale
    - analiza feedback-ului clienților
    - cercetarile de piață
  - In mobile forensic este dificil de aplicat din cauza mesajelor scurte si greselilor de tastare

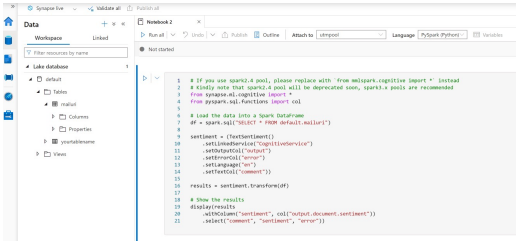
- Scenarii de utilizare
  - Investigații Criminale: Ajută la identificarea motivațiilor și intențiilor din spatele activităților infracționale.
  - Monitorizarea Amenințărilor: Detectarea mesajelor care conțin amenințări sau hărțuire.
  - Profilare Psihologică: Contribuie la profilarea psihologică a suspecților prin înțelegerea emoțiilor și stării lor mentale.

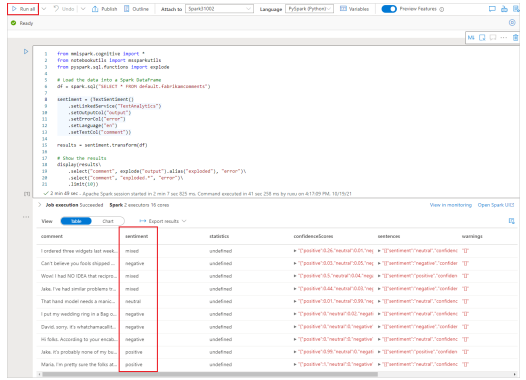
Utilizarea NLP pentru Sentiment Analysis

- Iata un exemplu de utilizare a Azure Cognitive Services, utilizand Synapse Studio.









AI / ML

Face Recognition si Photo/Video Analytics

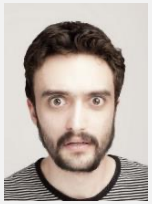
Ce este recunoasterea faciala?

1:1

Este aceeasi persoana?

- Imaginile reale au provocari – luminozitate scazuta, pozitie, expresie, diferenta de varsta, etc.
- Acuratetea algoritmului este importanta

1:n



Este persoana in baza de date de interes?

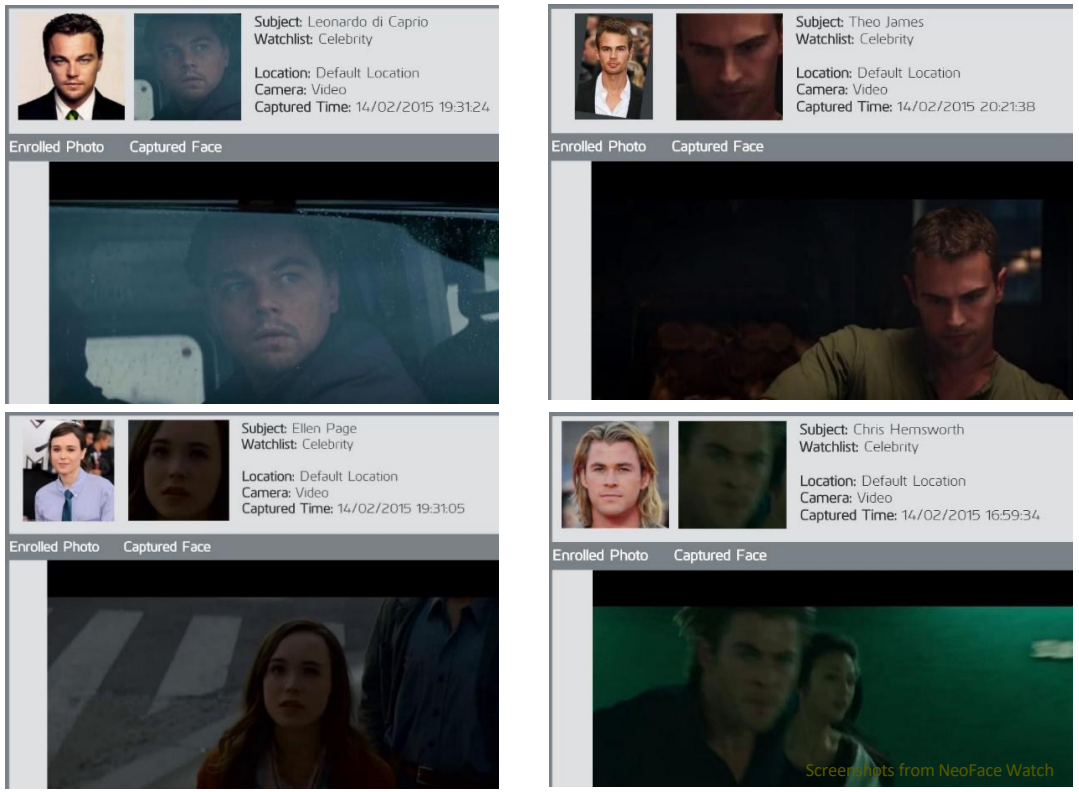
- La fel ca mai sus, dar viteza algoritmului este importanta.

n:n

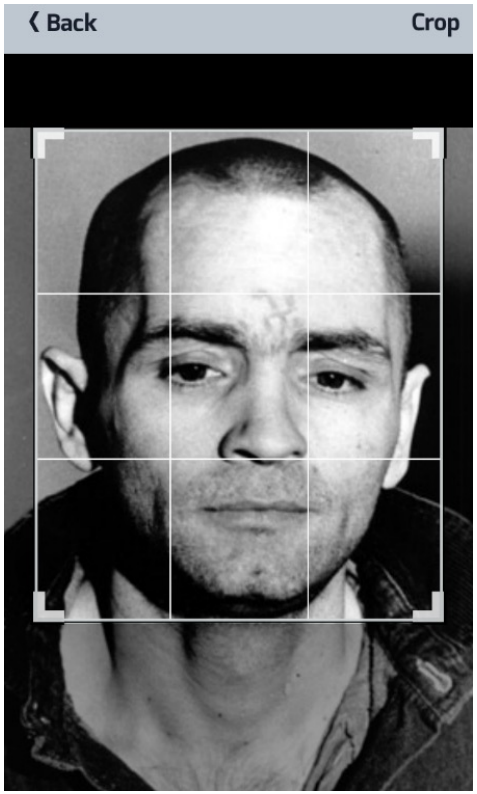
Verificari multiple simultan.

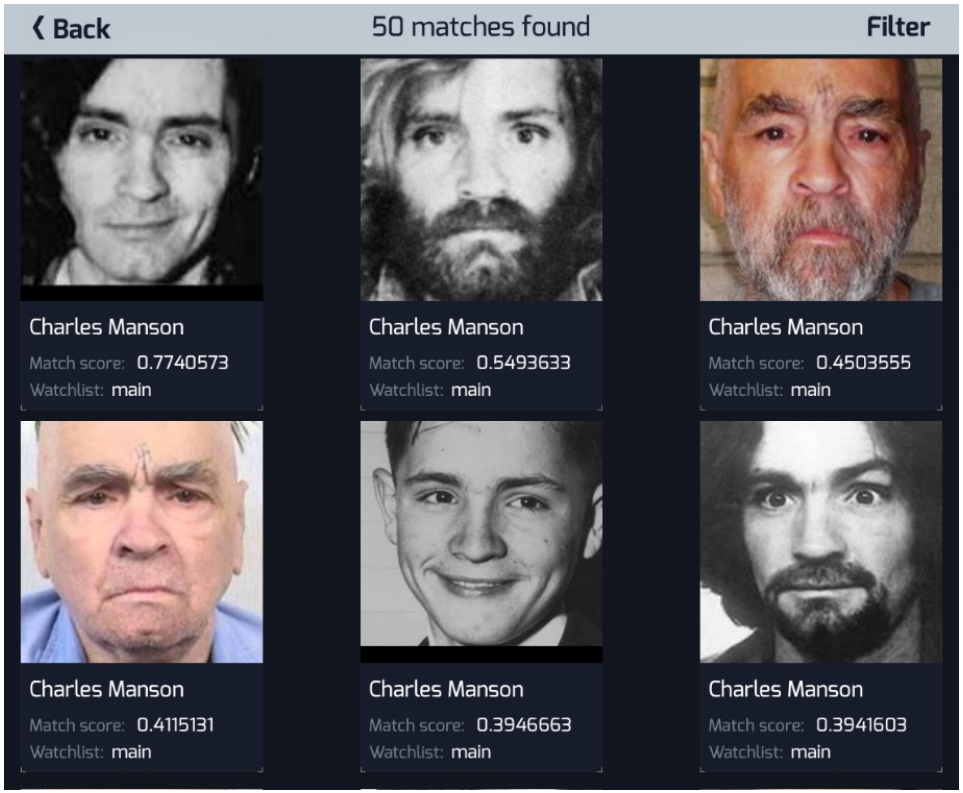
- La fel ca mai sus, dar viteza algoritmului este importanta.

Realitate = imagini de o calitate scazuta

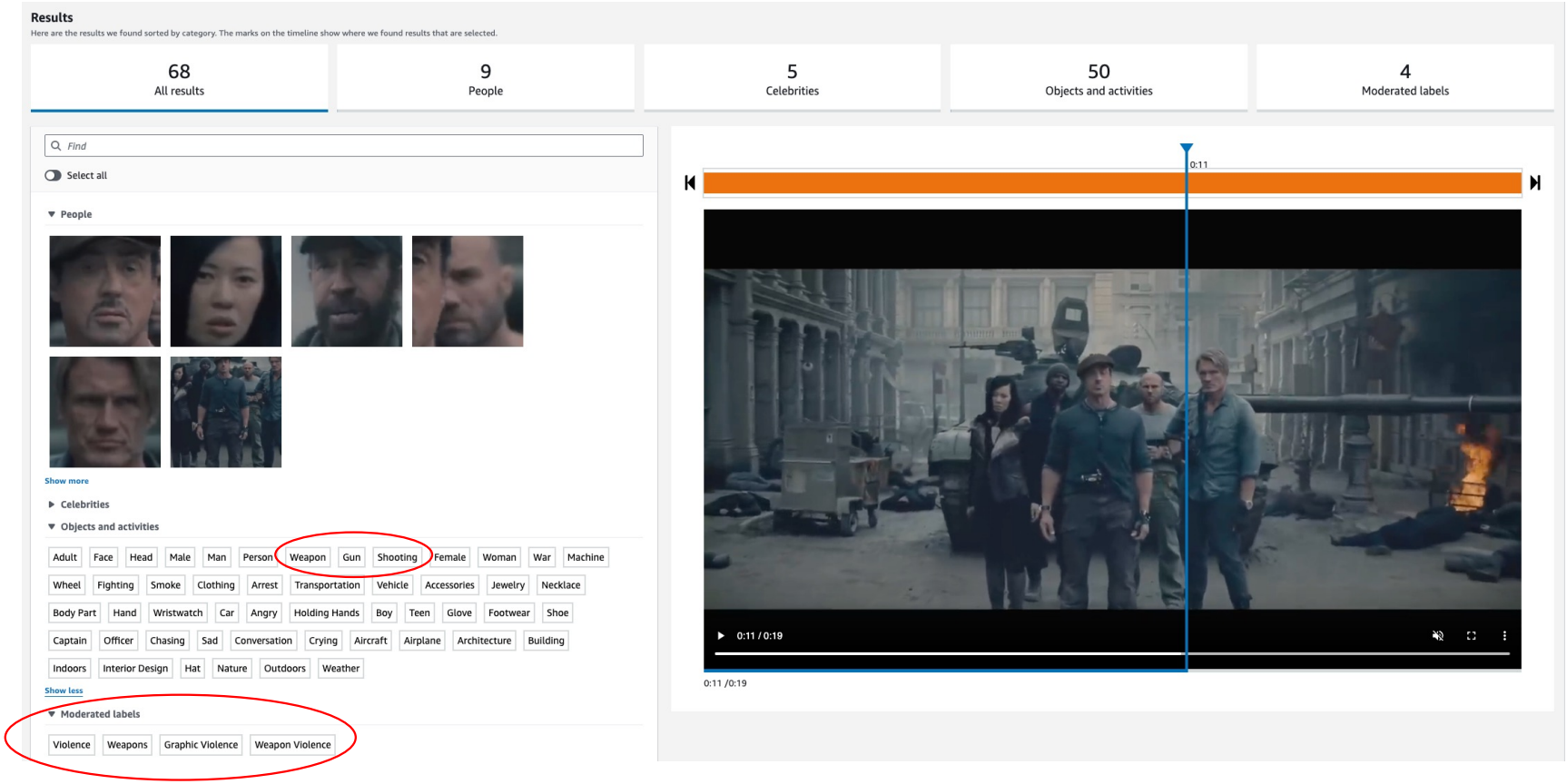


Provocari: calitate, luminozitate, varsta, fizionomie, expresie …





Analytics – detectarea automata a scenelor si obiectelor



Concluzie

- Din păcate, interesul pentru criminalistica digitală a explodat și a făcut ca mulți să intre în domeniu fără calificări adecvate.
- Pe langa utilizarea sculelor de forensic, este extrem de importanta cunosterea tehnologiei de comunicatie mobila, precum si intelegerea aspectelor constructive ale unui dispozitiv mobil.
- IA și ML aduc multiple avantaje în forensic, oferind unelte puternice pentru analiza datelor și identificarea activităților infracționale. Totuși, utilizarea acestor tehnologii trebuie să fie gestionată cu grijă, respectând normele etice și legale.

- **Performanta in activitatile de tip "forensic" se poate obtine doar printr-un proces continuu de invatare si perfectionare.**

Intrebari?

Mihai Ghita

Universitatea Titu Maiorescu