

# Informatika forensea

Mikel Egaña Aranguren

[mikel-egana-aranguren.github.io](https://mikel-egana-aranguren.github.io)

[mikel.egana@ehu.eus](mailto:mikel.egana@ehu.eus)



# Informatika forensea

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



# Zer da informatika forensea?

Diziplina kriminalistikoa

Informazioa lortzeko eta prozesatzeko informatika-sistemak ikertzea  
(ebidentzia digitalak):

- Balio juridikoa dutenak
- Ikerketa pribatu soilerako (baimenik gabeko sarbideak, informazio-lapurreten susmoak, etab.)

# Zer da informatika forensea?

Erantzuten saiatzen da:

- Zer?
- Nor?
- Zelan?
- Noiz?
- Zergatik?

# Zer da informatika forensea?

Nork erabiltzen du:

- Legearen agenteak
- Aseguru konpainiak
- Konpainia pribatuak
- Pertsona arruntak
- ...

# Zer da informatika forensea?

Zertan datza:

- Sistema baten informazioa erauzi
- Informazio zifratua/ezabatua/kaltetua berreskuratzea
- Sistema baten portaera monitorizatzea
- Enpresaren politiken ez-betetzeak detektatzea
- ...

# Zer da informatika forensea?

Locard-en trukaketa printzipioa:

- "Bi objektuk elkar ukitzen dutenean, zati bat transferitzen diote elkarri, beste objektuari eransten zaiona"
- Ekintza guztiek arrastoa uzten dute

# Zer da informatika forensea?

Heisenbergen ziurgabetasunaren printzipioa:

- "Sistema baten egoera neurtze hutsak aldatu egiten du"
- Ezin da sistema baten informazioa lortu sistema bera aldatu gabe
- Ahalik eta informazio gehien lortzea, aldaketak eta horien inpaktua minimizatuz



# Zer da informatika forensea?

Ebidentzia digital baten balio juridikoa epaileak erabakitzen du

Dokumentu, log, makina etab. manipulatuak izan ahal dira

Sinadura elektroniko aitortua duen dokumentuak balio juridikoa du?

# Zer da informatika forensea?

... Eta akusatuak ziurtagiria (txartela) lapurtu ziotela alegatzen badu?

Salaketarik bai? Ziurtagiria baliogabetzea (Errebokatzea) eskatu al zen berehala?

# Zer da informatika forensea?

Ebidentzia digitalek balio juridikoa izan dezaten, beharrezkoa da:

- Legea errespetatu da horiek lortzeko
- Informazioa zehazki jasotakoa da
- Aztertu bitartean ez da ezer aldatu/sortu/ezabatu
- Egindako analisiak erreproduzitzeko aukera izan behar du

# Zer da informatika forensea?

Forensic Examination of Digital Evidence: A Guide for Law Enforcement

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

UNE 71506 - Metodología para el Análisis forense de las evidencias electrónicas

# Zer da informatika forensea?

[Good Practice Guide for Computer-Based Electronic Evidence](#)

[RFC 3227 - Guidelines for Evidence Collection and Archiving](#)

[ISO/IEC 27037:2012 Information technology -- Security techniques --  
Guidelines for identification, collection, acquisition and preservation of  
digital evidence](#)

# Informatika forensea. Prozesua

1. Identifikazioa
2. Kontserbazioa
3. Analisia
4. Azalpena

# Informatika forensea. Prozesua

Ezinbestekoa da egiten den guztiaren oharak, grabazioak, argazkiak, bideoak eta abar hartzea, data eta orduarekin

Beharrezkoa izan daiteke prozesu osoa ahalik eta xehetasun gehienekin gogoratzea epaiketa batean (urte batzuk geroago)

# Identifikazioa

Ikerketan beharrezkoak izango diren sistemak (ebidentziak) identifikatzea

Gomendagarria da egiten den guztiaren fede ematen duen notarioa egotea

Komeni da argazkiak ateratzea, haien antolaera/konfigurazioa erakusteko



# Identifikazioa

Hasiera-hasieratik, zaintza-katea aktibatu behar da: bildutako ebidentziak nork erabiltzen dituen zehatz-mehatz erregistratu behar da, datak, orduak, non biltegitzen diren, zaintza-arduraduna nor den eta abar adieraziz

Martxan dauden sistemak badira, ez jarraitu erabiltzen eta informazio lurrunkor guztia jaso (sistema itzaltzean ezabatu egin daiteke): kanpoko programak erabili kopiak, sarbideak eta abar egiteko

# Identifikazioa

RAM memoriaren informazioa oso garrantzitsua da (kopiatu egin behar da, ahalik eta gutxien aldatuz):

- Gauzatzen ari diren prozesuak
- Gauzatzen ari diren moduluak
- Artxibo irekiak
- Datuen bertsio desenkriptatuak

# Identifikazioa

RAM memoriaren informazioa oso garrantzitsua da (kopiatu egin behar da, ahalik eta gutxien aldatuz):

- Emailen eranskinak, irudiak, chat-en zatiak
- Gako kriptografikoak
- Testu soileko pasahitzak
- ...

# Identifikazioa

RAMen edukia iraultzeko tresnak:

- pd Proccess Dumper
- FTK Imager
- Volatility
- EnCase

# Identifikazioa

Martxan dauden prozesuei, zerbitzuei, makinari konektatutako erabiltzaileei, portu irekiei eta abarri buruzko informazioa ere jaso beharko da

Kontuz!, notariorik ez badago, zer egin den eta zer informazio lortu den frogatzeko... Nork dio hori zela une hartan sisteman zegoena?

# Identifikazioa

Informazio lurrunkor guztia bildu ondoren, sistema itzali eta hegazkorra ez den informazio guztia kopiatzen da (disko gogorrak, USBak, etab.)

Write Blockers erabiltzea komeni da, informazioa eskuratzeko aukera ematen duten sistemak, baina diskoan idaztea saihesten dutenak

# Identifikazioa

Kopia bit mailan egiten da: kopia forensea (horrela kopiatzen dira arrastoak eta disko gogorretik dagoen ezkutuko informazioa)

Jatorrizkoaren eta kopiaren laburpen kriptografikoa kalkulatzen (eta biltegitratzen) da, berdinak direla ziurtatzeko

Kopiaren beste kopia forentse bat egiten da, kopiak kalterik izanez gero jatorrizkoarekin lan egin beharrik ez izateko

# Identifikazioa

Bit mailako klonazioa:

- dd (Linux)
- Helix3 Pro
- EnCase
- FTK Imager



# Kontserbazioa

Saihestu egin behar dira (zaintza-katea):

- Galerak
- Kutsadura
- Kaltea, alterazioa, manipulazioa

# Kontserbazioa

Bildutako informazio guztia zehatz-mehatz dokumentatzea

Jasotako gailu guztiak etiketatzea

Marka, modeloa, serie-zenbakia eta abar adierazi

# Kontserbazioa

Data, datuak eta lekualdatzen duten eta manipulatzeko duten pertsonen sinadura

Jatorrizkoa ondo bilduta geratu behar da (adibidez: notarioaren esku)

Kopia bana eman dakieke alderdi interesdun guztiei

Beti da gomendagarria babes-kopia izatea

# Analisia

Lortutako informazio guztia aztertzea lan aspergarria eta "ia ezinezkoa" da

Tresna mota asko erabiltzen dira:

- Ezabatutako elementuak berreskuratzea
- Pasahitza krakeatzea
- Log-en analizatzaileak
- ...

Ordenatua eta zehatza izan behar da; analistaren intuizioa funtsezkoa da

# Analisia

Informazioa bilatzeko ohiko guneak:

- Posta elektronikoak
- Mezu-tresnak
- Fitxategi ezabatuak
- Fitxategien metadatuak: sorkuntza, azken atzipena, etab.
- Nabigazioaren historiak
- Aplikazioen eta sistemaren logak
- Beste makina batzuekiko konexioak

# Analisia

Garrantzitsua da sistemaren denbora-lerroa kudeatzea:

- Noiz instalatu zen X
- Noiz eskuratu zen Y
- Noiz ezabatu zen Z

# Analisia

Ezinbestekoa da DBLO (LOPD) eta komunikazioen sekreturako eskubidea errespetatzea (ezin da mezu elektronikorik irakurri zure medikuarekin edo maitale batekin, ikerketarako garrantzitsuak ez badira)

# Analisia

Irtenbidea: bilaketa itsua (Analistaren intuizioa)

- Ez da informazio guztia aztertzen
- Bilaketak gako-hitzen bidez egiten dira
- Gako-hitz horiek agertzen diren informazioa baino ez da aztertzen

Peritu-txosten osoa ezeztatu daiteke hori egiteko legeren bat urratu bada



# Aurkezpena

Txostena egiten da prozesu osoa eta lortutako emaitzak azalduz

Nahiz eta prozesua eta lortutako emaitzak oso onak izan, txostenak behar bezala islatzen ez badu, ez dute baliorik izango

Txostena teknikariak ez diren pertsonen zuzenduta dago (epaileak, abokatuak, enpresaburuak, etab.). Ulergarria izan behar da

Txostenak inpartziala izan behar du. Perituak ez du iritzirik eman behar, frogak eta emaitzak baino ez ditu adierazi behar

# Aurkezpena

Informe baten zatiak:

- Aurrekariak
- Frogak
- Analisia eta tratamendua
- Emaizak
- Ondorioak

# Aurkezpena

**Aurrekariak:** Zein egoeratan egin den beharrezkoa peritu baten esku-hartzea

**Frogak:** Bildu diren ebidentziak eta bilketarekin, bikoizketarekin, kontserbazioarekin eta abarrekin jarraitu diren prozesuak

**Analisia eta tratamendua:** Informazioa aztertzeako erabilitako teknikak eta tresnak

# Aurkezpena

**Emaitzak:** argi eta ulertzeko moduan azalduko da erabilitako teknikak zer emaitza eman zituzten

**Ondorioak:** atalik garrantzitsuena. Bertan, adituak lortutako emaitzetatik zer ondoriozta daitekeen azaltzen du. Ondorio guztiak emaitzaren batetik eratorri behar dira, bestela suposizio hutsa da

# Aurkezpena

Epaiketarik badago, adituak lekuko gisa jardungo du

Bere garaian egin zuen txostena azaldu beharko du, eta abokatuen galderei erantzun

Justiziaren moteltasuna dela eta, hainbat urte igaro ahal izan dira. Komeni da txostena berrikustea epaiketa baino egun batzuk lehenago

# Aurkezpena

Batzuetan, peritu bati deklaratzera deitzen zaio, beste peritu baten txostena desegin dezan:

- Zaintza-katea hautsi zelako eta ebidentziak aldatu zitekeelako
- Txostenaren ondorioak ezin direlako lortutako emaitzetatik zuzenean eratorri
- Teknika desberdinak aplikatuta txostenean lortutakoekin kontraesanean dauden emaitzak lortzen direlako