CURS D'ESPECIALITZACIÓ EN CIBERSEGURETAT

ANÀLISI FORENSE INFORMÀTIC

Xavier Baubés Parramon - curs 2021/2022

Índex

1. QUÈ ÉS LA FORENSIA DIGITAL (O INFORMÀTICA)

És una disciplina que combina el dret i la informàtica per recopilar i analitzar dades de sistemes informàtics i xarxes d'una manera admissible com a prova en un tribunal.

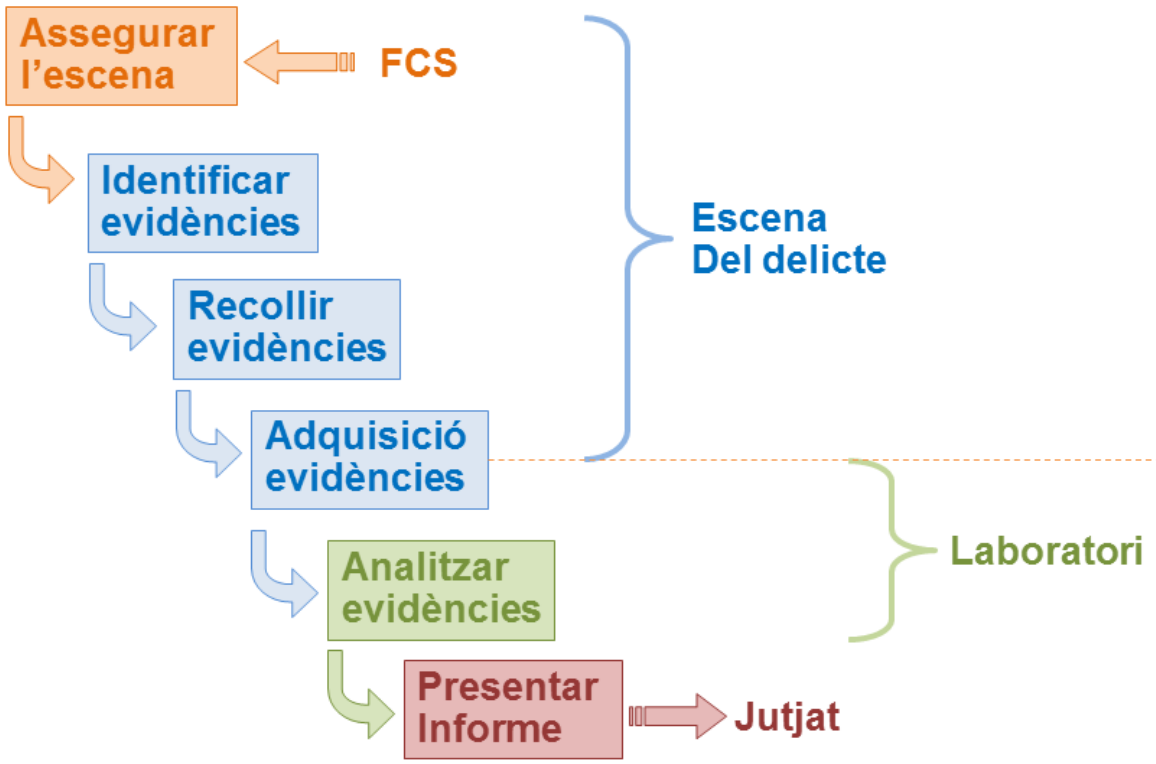
S'hi apliquen tècniques científiques i analítiques a infraestructures tecnològiques per permetre identificar, preservar, analitzar i presentar dades vàlides en un procés legal. Són també els estudis i investigacions usats en assumptes privats per a la recerca de proves i arguments que serveixin a una de les parts en discussió per decantar la discrepància al seu favor. Habitualment es recorre a proves pericials informàtiques en assumptes penals en què la infraestructura informàtica s'usa com a eina del delicte, per exemple la pornografia infantil a Internet. També intervé en la investigació contra delictes contra la propietat privada i intel·lectual, espionatge industrial, protecció de dades personals, fraus o sabotatges.

Les tècniques són reactives, s'accedeix al sistema un cop aquest ha sigut danyat: Reconstrucció de l'actiu informàtic, obtenció de dades residuals, autenticació de dades, etc

Segons el principi d'intercanvi de "Locard": Qualsevol accés a un element (informàtic en el nostre cas) deixa evidències.

La funció principal de la informàtica forense no és prevenir delictes, aquest és el marc d'actuació propi de la seguretat i l'auditoria informàtica.

1.1.ETAPES



Assegurar l'escena: Per part de les Forces i Cossos de Seguretat de l'Estat (FCS).

Identificació: Aquesta etapa consisteix en la recerca, reconeixement i documentació de l'evidència digital en l'escena de l'incident. Aquest procés ha de permetre la identificació dels mitjans d'emmagatzemament que puguin contenir evidència digital potencial rellevant relacionada amb l'incident ocorregut. Aquesta etapa hauria d'incloure un procés de tria que permeti prioritzar la recollida i/o adquisició de l'evidència en funció de la seva volatilitat o rellevància.

Recollida: Una vegada identificada l'evidència digital potencial, l'especialista haurà de decidir si recull l'evidència o bé si l'adquireix. Aquesta tria dependrà de diversos factors: circumstàncies, cost, temps i recursos disponibles. La recollida és la fase del procediment de gestió de l'evidència digital en la qual els dispositius que potencialment poden contenir evidència digital, són recollits i transportats a un laboratori per a una adquisició (aquesta operació també es pot fer in situ) i anàlisi posterior. L'evidència digital pot existir en dues condicions: quan el sistema es troba encès o bé apagat.

Adquisició: El procediment d'adquisició comporta la creació d'una còpia bit a bit de l'evidència continguda en els dispositius digitals, així com la documentació dels mètodes emprats i dels passos realitzats. Hi ha una gran varietat de mètodes d'adquisició i eines validades (tant de maquinari com programari). L'expert ha d'adoptar el millor mètode d'adquisició segons la situació, el cost i temps disponible, així com documentar qualsevol decisió que hagi pogut prendre. L'adquisició es pot dur a terme (segons circumstàncies diverses), tant a l'escena del delicte, com al laboratori d'anàlisi.

Anàlisi: En aquesta etapa, els pèrits o analistes (computer forensics analysts) estudien les evidències digitals obtingudes a l'etapa anterior i elaboren les seves hipòtesis. Aquesta etapa requereix personal molt tècnic, així com l'ús d'eines especialitzades. Aquesta etapa sempre es durà a terme en el laboratori.

Presentació: Finalment, a conseqüència de l'etapa d'anàlisi, s'elaborarà un informe pericial que pot tenir diversos destins. En aquest sentit, l'informe s'adreça sovint a persones no tècniques en la matèria (jutges, responsables d'empreses, etc.). Per aquest motiu, cal que l'informe contingui descripcions i indicacions clares (glossaris), així com les conseqüències i el desenvolupament dels fets succeïts. És molt important que es tingui en compte que les evidències digitals s'han d'haver adquirit a l'empara dels requisits legals per a ésser considerades vàlides.

En totes aquestes etapes cal tenir molt present la preservació de la integritat de les evidències, tant pel que fa a evitar la possibilitat que es puguin malmetre accidentalment (cops, arcs magnètics, etc.), com intencionadament.

1.2. OBJECTIUS

- Identificació de casos de frau
- Assessoria per minimitzar problemes de frau mitjançant la implementació de controls interns dins l'organització
- Expertesa en sistemes interns de control
- Recollida i anàlisi d'evidències digitals emmagatzemades en suports informàtics i electrònics per ser adreçades a l'autoritat judicial competent

1.3.PRESENT I FUTUR

Els sistemes informàtics formen part de les nostres vides tant a nivell personal com professional.

La importància de la informàtica forense creix ràpidament, passarà a ser més un mètode preventiu que una mera acció de reparació d'errors.

Cada vegada es requereix més personal preparat específicament per gestionar un crim informàtic.

1.4.POSICIONS I ESPECIALITATS

- Pèrit judicial (designat pel jutge)
- Pèrit de part (qualsevol pot sol·licitar-lo)
- Director de Seguretat de la Informació (CISO)
- Consultor de Seguretat de la Informació
- Cap de l'Oficina de Control de responsabilitat penal corporativa (RPC)
- Oficia de Compliment Normatiu (Compliance Officer)
- Auditor de Seguretat de Sistemes
- Complementar la formació de perfils no informàtics (com detectius o notaris) que necessitin mantenir la cadena de custòdia de la informació digital

1.5.TASQUES A REALITZAR

- Estudi de casos de robatori d'identitat, frau electrònic o phishing.
- Implantar sistemes informàtics i verificar del correcte establiment del sistema informàtic en el client.
- Verificar la responsabilitat penal de les empreses en incidents de ciberseguretat.
- Verificar la integritat i autenticitat de correus electrònics i missatgeria instantània.
- Analitzar el plagi en sistemes informàtics i espionatge industrial.
- Verificar l'autenticitat i integritat dels arxius digitals d'àudio, imatge o vídeo i transcripció de contingut.
- Estudiar l'espionatge industrial i la divulgació de secrets de l'empresa.
- Anàlisi del mal ús d'eines informàtiques durant l'activitat laboral.
- Clonació forense de discs durs i dispositius d'emmagatzematge.
- Observar la difusió a través d'internet de material privat de manera no autoritzada
- Valoració econòmica dels sistemes informàtics

2. LLEIS A CONÈIXER

2.1. REGULACIÓ ESTATAL

Cal conèixer la legislació vigent a la qual està sotmès l'exercici professional de la informàtica forense.

D'aquesta manera entendràs fins on poden arribar les teves investigacions, quines repercussions jurídiques poden tenir algunes accions o altres i actuaràs en conseqüència per no acabar sent acusat durant la investigació de qualsevol acte delictiu.

També ha de saber si els actes descoberts durant la investigació constitueien infraccions administratives o penals.

Lleis més importants en informàtica forense de la jurisdicció espanyola:

- Constitució espanyola
- Llei d'Enjudiciament Civil
- Llei orgànica de protecció de dades de caràcter personal
- Llei de Serveis de la Societat de la Informació i Comerç Electrònic
- Llei de conservació de les dades relatives a les comunicacions i les xarxes públiques
- Codi penal
- Regulació Internacional:
  - Directiva 2006/24/CE
  - Directiva 2013/40/UE
  - ISO 27037, UNE 71505, UNE 71506.

3. PROCÉS FORENSE

3.1. PASSOS A SEGUIR PER L'ANÀLISI

1) Mapejat de l'entorn de dades

2) Anàlisi de debilitats i vulnerabilitats

3) Auditoria de les pàgines web

4) Peritatge en informàtica forense

5) Anàlisi forense de dispositius mòbil

6) Recuperació de la informació

7) Protecció de la marca

8) Evidències de falsificació

9) Evidències d'infracció de marca

3.2. METODOLOGIA

3.2.1 Assegurar l'escena

Aquesta fase se centra més en els casos penals. No obstant això, és important en qualsevol anàlisi forense.

L'investigador no només ha de centrar-se en una anàlisi tècnica dels equips implicats en l'incident, sinó que també ha d'assegurar-se que a l'escenari on s'ha produït l'incident no s'ha alterat, des del descobriment dels mateixos fins a l'inici de la seva anàlisi.

Tots els implicats en la investigació han de ser conscients que qualsevol acte que duguin a terme pot tenir conseqüències, per la qual cosa no han de fer res que no els sigui clar i que pugui alterar els resultats.

El millor és treballar per consens en l'actuació i anotar tot el que es fa a l'escena. És recomanable fer fotografies de l'entorn de l'equipament per evidenciar l'estat original de l'escena, identificant així el perímetre de l'escena a analitzar i protegint-lo de l'accés per personal no autoritzat.

3.2.2 Identificar i recollir evidències

A Causa de la volatilitat de les dades i el període de temps en què romandran accessibles a l'ordinador. A causa d'aquests inconvenients, les proves més volàtils s'han de recollir de manera ordenada i ràpida, amb un ordre de volatilitat de major a menor.

Amb una primera còpia realitzada i comprovat que el contingut és idèntic usant el Hash, procedim a fer una segona còpia a la primera.

Lliurarem el primer a la secretària judicial o notari responsable del cas i mantindrem el segon per poder treballar.

La segona còpia serà la còpia de seguretat i no es treballarà directament amb ella.

Per realitzar l'anàlisi cal fer una tercera còpia, aquesta còpia es pot alterar. La firmarem amb un Hash mínim SHA-256.

Principis davant les evidències:

- Captura una imatge del sistema el més precisa possible
- Fer notes detallades, incloses les dates i les hores que indiquen si s'utilitza l'hora local o UTC
- Minimitzar els canvis en la informació que s'està recopilant i eliminar els agents externs que ho puguin fer
- Recopilar la informació abans d'analitzar-la
- Recopilar informació per ordre de volatilitat (de major a menor)
- La recopilació d'informació es realitza de forma diferent segons els dispositiu

3.2.3 Ordre de volatilitat

L'ordre de volatilitat es refereix al període de temps en què determinada informació és accessible. Primer s'ha de recopilar la informació que estarà disponible durant el període de temps més curt, és a dir, aquella que tingui una volatilitat més gran.

Segons aquesta escala es pot crear la següent llista per ordre de major a menor volatilitat:

- Registres i contingut de la caché. (memòria RAM)
- Taula d'encaminament, memòria cau ARP, taula de procés, estadístiques del nucli, memòria, etc.
- Informació temporal del sistema
- Disc
- Logs del sistema
- Configuració física i topologia de la xarxa
- Documents

3.3. PROCEDIMENT DE RECOL·LECCIÓ

El procediment de recaptació ha de ser el més detallat possible, assegurant que és inequívoc i minimitzant la presa de decisions.

3.3.1 Transparència

Els mètodes utilitzats per recollir proves han de ser transparents i reproduïbles. Estar preparats per reproduir amb precisió els mètodes utilitzats, i aquests mètodes han d'haver estat provats per experts independents.

3.3.2 Passos

- Indicar on és l'evidència. Llista quins sistemes intervenen en l'incident i des d'on s'han de prendre proves
- Recopilar molta informació i establir posteriorment que és rellevant
- Establir l'ordre de volatilitat de cada sistema i obtenir la informació segons l'ordre establert
- Comprovar i anotar el grau de sincronització del rellotge del sistema
- Documentar cada pas
- Anota les persones involucrades: Qui hi ha? Què fan? Què observen? Com reaccionen?

3.4. PRESERVAR LES EVIDÈNCIES

3.4.1 Accions a evitar

S'han d'evitar les següents accions per no invalidar el procés de recollida d'informació ja que s'ha de preservar la seva integritat perquè els resultats obtinguts puguin ser utilitzats en un judici:

- No tanquis l'ordinador fins que s'hagi recopilat tota la informació (la informació volàtil es perdria, igualment si el sistema conté un malware o rootkit).
- No confieu en la informació proporcionada pels programes del sistema, ja que pot ser que s'hagin vist compromesos. La informació s'ha de recopilar programàticament des de mitjans protegits
- No executis programes que modifiquin la data o hora d'accés de fitxers del sistema.

3.5. PROCEDIMENT D'EMMAGATZEMATGE

3.5.1 Cadena de custòdia

Consisteix en un informe detallat que documenta la manipulació i l'accés a les proves objecte d'investigació. La informació continguda en el document s'ha de conservar adequadament i mostrar les dades especifiques, en particular tots els accessos amb data i hora.

Cal conèixer tots els detalls sobre com es va gestionar l'evidència a cada pas del camí. Documentar per cada prova el "qui, quin, quan, on, per què i com".

- On? i qui? ha descobert i recollit les
- On? i qui? ha manipulat l'evidència
- Qui ha custodiat les proves? quant de temps? com les ha emmagatzemat?
- Quan? i com? es va realitzar un canvi de custòdia de les evidències

Recursos:

- Identificació de la evidència
- Fotografia i anotació de llocs i dades (número de sèrie, tipus, marca, etc)
- Etiquetatge de numeració única
- Acta notarial si és necessari
- Time-stamping
- Les evidències digitals cal que vagin signades (hash)
- Obertura i anotació de totes les dades del document de custòdia
- Qui integra la cadena de gestió de rols de custòdia
- M-A-C (modificació de l'accés) dels documents signats

3.5.2 On i com emmagatzemar-lo

La informació s'ha d'emmagatzemar en dispositius la seguretat dels quals hagi estat demostrada i que permetin detectar intents d'accés no autoritzats.

3.6. ANALITZAR EVIDÈNCIES OBTINGUDES

Determinar el com? i l'on? podem trobar l'evidència

3.6.1 Línia temporal

La cronologia, en les investigacions que duem a terme com a forenses, són importants, a l'hora d'analitzar les dades obtingudes l'ordre cronològic és crucial per conèixer la temporalitat de totes les accions, i s'ha de tenir en compte especialment quan sigui necessari analitzar diferents dispositius o informacions que es trobin en diferents usos temporals.

Les marques de temps dels arxius (M-A-C) poden ser canviades intencionadament per un atacant o usuari maliciós, utilitzant tècniques antiforenses amb les quals s'ha de tenir especial cura en l'anàlisi de les dades, ja que una hipòtesi podria ser sostinguda erròniament en esdeveniments modificats de manera maliciosa per obstruir la investigació.

Registrarem en el nostre propi document en qualsevol format (text, xls, csv, etc...) la crono-línia temporal de tots els esdeveniments o actuacions realitzades durant l'informe de presa de proves o enumeració dels equips implicats, inventari, etc.

3.6.2 Cerca d'informació

A través d'aplicacions utilitzades en la recollida d'evidències i extracció d'informació.

El procés de cerca ha de ser meticulós i ajustat al resultat final que esperem trobar a través d'evidències expertes.

Cada forense pot ajustar la recerca d'informació, com convingui, però un bon consell, és realitzar la recerca un cop finalitzada tota la col·lecció de proves.

3.7. REDACCIÓ DE L'INFORME DE RESULTATS

La importància d'uns bons informes que siguin clars, concisos i que serveixin, per exemple, en cas de judici, perquè una persona no entesa en el tema sigui capaç d'entendre el que va passar i el que li volem transmetre sense influir en una decisió posterior.

L'informe pericial és la presentació del treball de l'expert, d'una manera estructurada i perfectament comprensible per al lector no expert en la matèria. Aquest informe conclourà que es van produir o no una sèrie d'esdeveniments, per la qual cosa aquests informes són essencials en casos judicials d'especial complexitat tècnica, com els relacionats amb l'enginyeria informàtica.

Els informes pericials en l'àmbit de les tecnologies de la informació estan subjectes a la norma UNE 15/7001, que indica com redactar aquest tipus d'informes.

3.7.1 Què conté cada informe

Títol: Ha d'expressar de manera clara i inequívoca la finalitat de l'informe.

Documents: L'informe constarà, com a mínim, dels documents bàsics següents: Índex General, Informe i Annexos. Aquests documents bàsics es poden agrupar en diferents volums o en un sol volum.

Redacció: La primera pàgina de cadascun dels documents bàsics han d'aparèixer a la portada del volum:

- Número del volum
- Títol del volum
- Tipus de document unitari (índex general, memòria, annexos, etc)
- Organisme o client per al qual s'ha redactat l'informe
- Identificació i dades empresarials de cadascun dels autors de l'informe pericial
- Dades de la persona jurídica que ha rebut l'encàrrec de preparar-lo

Tots els documents s'han de presentar acuradament, de manera neta i ordenada. S'estructuraran en forma de capítols i seccions, que es numeraran d'acord amb la norma UNE 50132.

Índex general: La seva missió és localitzar fàcilment els diferents continguts de l'informe pericial.

Informe de l'informe: La seva missió és justificar les solucions adoptades i descriure de manera única l'objecte de l'informe pericial. L'informe ha de ser clarament comprensible, en particular els objectius de l'informe, les alternatives estudiades, els seus avantatges i inconvenients, i els motius que van conduir a les conclusions expressades.

Fitxa d'identificació: Un primer full on apareixerà: Títol de l'informe, i codi identificatiu si s'escau. Denominació social de la persona física o jurídica que hagi encarregat l'informe pericial i el seu C.I.F., nom i cognoms del seu representant legal i del seu DNL, adreça professional, telèfon, fax, correu electrònic, etc Nom i cognoms, associació professional a la qual pertany, número de Col·legiat, DNI, adreça professional, telèfon, fax, correu electrònic de cadascun dels autors de l'informe pericial. Data i signatura.

Índex de la memòria: Referencia cadascun dels documents.

Objecte: Finalitat i justificació de l'informe pericial informàtic.

Àmbit: Abast de l'informe pericial.

Antecedents: S'enumeren tots aquells aspectes necessaris per a la comprensió de les alternatives estudiades, i les conclusions finals de l'informe pericial.

Normativa i referències: Es relacionaran els documents i les normes legals i reglamentàries citades en els diferents apartats de l'informe.

Definicions i abreviatures: S'enumeren totes les definicions, abreviatures i expressions tècniques que s'han utilitzat al llarg de l'informe pericial, així com el seu significat.

Requisits: Es descriuen les bases de dades i dades d'inici establertes pel client i la legislació, normativa i normativa aplicables.

Anàlisi de solucions: S'indicaran les diferents alternatives estudiades, quins camins s'han seguit per arribar-hi, els avantatges i inconvenients de cadascuna i quina és la solució finalment triada i la seva justificació.

Resultats finals: Descriurà l'operació realitzada segons la solució triada juntament amb les conclusions de l'informe pericial informàtic.

Annexos a l'informe pericial informàtic: Començarà amb un index que farà referència a cadascun dels documents, els seus capítols i apartats, per tal de facilitar-ne l'ús.

Intervenció de l'evidència digital: S'hi ha de documentar amb gran detall la intervenció de l'evidència digital, el procés de la seva adquisició i la fonamentació de la seva cadena de custòdia.

Estudis d'experts: S'han de descriure les tècniques utilitzades i els resultats obtinguts després d'aplicar-los sobre l'evidència digital intervingut.

Visat col·legiat: El reconeixement que l'autor és un professional registrat i qualificat per a l'exercici de la professió, subjecte a l'ètica professional. Certifica l'autoria i titularitat de l'informe. Autenticació i registre de documentació de l'informe de visat. Que l'obra estigui formalment completa. Que l'autor hagi tingut en compte les disposicions legals i administratives aplicables a l'obra a realitzar. L'existència d'una corporació en virtut del dret públic que vetlla pels drets del destinatari de les obres

4. FRAMEWORKS I SUITES

Algunes eines útils per l'anàlisi forense:

Kali, **CAINE** o **DEFT:** Entorns per l'anàlisi forense creats amb distribucions GNU/Linux.

Autopsy: Anàlisi del sistema.

The Harvester: Permet recopilar informació pública de la web.

5. SISTEMES DE CLONACIÓ

5.1. MOTIU DE LA CLONACIÓ

La clonació de disc dur es realitza per certificar i mantenir la cadena de custòdia de les proves digitals contingudes en el dispositiu. Això és primordial i essencial en qualsevol procés judicial, si es fa malament, les proves pericials serien invalidades.

El deure de l'expert informàtic és certificar la cadena de custòdia, és a dir, que les proves es mantinguin inalterables des del moment en què són intervinguts, podent certificar la seva originalitat en qualsevol moment després de la intervenció.

5.2. QUÈ ÉS LA CLONACIÓ FORENSE D'UN DISC?

La clonació forense dels discs durs consisteix a copiar tot el contingut d'un disc dur, bit a bit, a un altre dispositiu d'emmagatzematge.

S'obté una còpia exacta de baix nivell de tots els continguts del disc dur a més de certificar el seu contingut amb una signatura hash.

6. EINES DE RECOPILACIÓ D'EVIDÈNCIES

Anàlisi de xarxa:

Snort: Detecció d'intrusions.

Wireshark: Filtratge i monitoratge d'una xarxa.

Nmap: Anàlisi de ports i serveis.

Xplico: Captura de dades.

Tractament d'unitats de disc:

Dcdd3: Copiar imatges grans a peces més petites.

Mount manager: Gestió d'unitats connectades al disc dur.

Guymager: Processament d'imatges.

7. EINES DE GESTIÓ I ANÀLISI DE MEMÒRIA

Volatility: Reconstrucció i anàlisi de memòria RAM.

RedLine: Captura i anàlisi de memòria

Memoryze: Captura de la memòria RAM.