Fases i metodologia de l'anàlisi forense

PID_00273498

Josep Maria Arqués Soldevila
Miquel Colobran Huguet
Erik de Luis Gargallo

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Josep Maria Arqués Soldevila

Enginyer en informàtica per la Universitat Autònoma de Barcelona. Va fer el treball de recerca al Departament d'Enginyeria de la Informació i de les Comunicacions (DEIC) de l'esmentada universitat. Ha treballat, com a professor ajudant i associat, al DEIC, i ha exercit de professor docent col·laborador de diverses assignatures de la Universitat Oberta de Catalunya. Actualment, exerceix d'analista en informàtica forense i especialista en gestió de la qualitat en ciències forenses.

Miquel Colobran Huguet

Doctor en informàtica per la Universitat Autònoma de Barcelona. És professor docent col·laborador a la UOC i coautor de diversos materials centrats en l'administració i seguretat de sistemes i informàtica forense. La seva recerca s'emmarca dins de la seguretat i del *social computing*, és a dir, com els ordenadors influeixen i són influïts per la societat, i com intervé la seguretat informàtica en aquest procés.

Erik de Luis Gargallo

Enginyer en informàtica i Màster en Seguretat de la Informació per la Universitat Oberta de Catalunya. Té més de 10 anys d'experiència en seguretat de la informació, auditories informàtiques, informàtica forense i enginyeria de seguretat. Actualment, treballa establint línies estratègiques en l'àmbit de la seguretat de les TIC i desplegament de les tecnologies que les assegurin. També és professor col·laborador de diversos cursos i assignatures de la Universitat Oberta de Catalunya.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Jordi Serra (2020)

Primera edició: febrer 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

Introducció

La generalització de l'ús de les tecnologies de la informació en la societat ha incrementat el valor de la informació digital i ha creat, al seu torn, la necessitat de protegir-la davant dels atacs malintencionats o atribuïbles al desconeixement d'aquestes noves tecnologies. En tots dos casos, els rastres o les traces que podrien revelar l'execució d'un fet (tant si és constitutiu de delicte com no) estan emmagatzemats en suports digitals i es denominen genèricament **proves digitals**.

Delicte

Una conducta delictiva és la susceptible de ser sancionada pel dret penal.

La prova digital presenta, a grans trets, les propietats següents:

Proves digitals

En la comissió d'una conducta delictiva, es denomina **prova** qualsevol element que proporcioni informació que condueixi a alguna conclusió o troballa relacionada amb el fet que s'investiga.

- Es pot modificar o eliminar fàcilment.
- És possible obtenir una còpia exacta d'un fitxer sense deixar cap rastre.
- L'adquisició de la prova pot comportar l'alteració dels suports digitals.

L'**anàlisi forense** va sorgir de la necessitat de poder aportar elements rellevants en els processos judicials en els quals les noves tecnologies es trobaven presents, o bé com a objectiu (per exemple, una intrusió que comporti danys en un sistema informàtic) o bé com a mitjà (per exemple, l'enviament de correus electrònics amenaçadors a un personatge públic). En qualsevol cas, la prova digital és essencial per a trobar les respostes a les preguntes habituals que es plantegen en qualsevol investigació:

Preguntes clau

- **Què** s'ha comès?
- **Quan** s'ha fet?
- **On** s'ha comès?
- **Qui** ho ha fet?
- **Com** s'ha dut a terme?
- **Per què** s'ha comès?

Objectius

Amb el treball que s'ha de fer sobre aquests materials didàctics, pretenem que l'estudiant assoleixi els objectius següents:

1. Conèixer la definició de terminologia forense bàsica.

2. Conèixer el protocol de metodologia forense i els mecanismes de garantia de preservació de l'evidència digital.

3. Conèixer les bases de l'anàlisi forense digital.

4. Conèixer el maquinari i programari forense més emprat habitualment.

5. Aprendre a interpretar un informe pericial d'anàlisi forense digital.

1. Informàtica forense i prova digital

D'una manera més precisa que el concepte exposat en la introducció d'aquests materials, l'anàlisi forense es pot definir de la manera següent:

Definició d'anàlisi forense informàtica

Es denomina **anàlisi forense informàtica** el procés que resulta d'aplicar mètodes científics als sistemes informàtics i electrònics amb la finalitat d'identificar, recollir, adquirir, analitzar i presentar les evidències digitals, de manera que aquestes siguin acceptades en un procés judicial.

Hi ha moltes maneres de descriure les diferents subfases en què es divideix l'anàlisi forense. Totes al·ludeixen al mateix procediment, encara que de vegades s'empren noms diferents (la qual cosa pot arribar a ser bastant confusa).

No obstant això, els analistes no sempre aporten proves en processos judicials. Sovint, els seus informes s'elaboren amb finalitats privades o empresarials. En aquest sentit, la definició d'anàlisi forense que hem proporcionat té un cert tint delictiu, la qual cosa no s'ajusta, afortunadament, en la majoria dels casos, a la realitat que hem d'estudiar. L'anàlisi, d'una manera més genèrica, simplement ens permet reconstruir el que ha passat en un sistema informàtic després d'un incident de seguretat. Per tant, la finalitat de l'anàlisi pot ser simplement d'aprenentatge, una auditoria, la reconstrucció d'un sistema danyat, o l'adopció de mesures després de l'incident que minimitzin la probabilitat que aquest torni a ocórrer. Considerem, però, que el cas judicial és el més restrictiu i el que exigeix més mesures de preservació, la qual cosa pot ser molt didàctica i fàcilment extensible a tot tipus d'anàlisi forense informàtica.

Seguint amb l'enfocament criminalístic, l'informe de l'anàlisi forense, elaborat per un perit, podrà respondre en alguns casos les preguntes més directament relacionades amb l'àmbit tècnic com per exemple: **què** s'ha comès, en quines dates i hores (**quan**), i **com** s'ha dut a terme. No obstant això, especialment en les investigacions d'activitats delictives, trobar la resta de respostes requerirà una investigació policial i els mètodes que s'hi apliquen. Malgrat això, com ja s'ha advertit, no totes les anàlisis tenen com a destinació la seu judicial. Sovint, el receptor serà un client, normalment una empresa. En tots dos casos, però, l'analista ha de ser conscient que el receptor de l'informe potser no disposa de formació tècnica suficient i que, per tant, convé no abusar dels tecnicismes en l'elaboració de l'informe que ha de presentar.

1.1. Etapes de l'anàlisi forense informàtica

En general, les fases o etapes abans esmentades, de què consta tota anàlisi forense informàtica, són les següents (podeu trobar una descripció més acurada de les etapes d'identificació, recollida i adquisició a la norma ISO/IEC 27037):

- **Identificació**: aquesta etapa consisteix en la cerca, el reconeixement i la documentació de l'evidència digital a 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 posterior 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 (vegeu l'adquisició al paràgraf següent). Aquesta tria dependrà de diversos factors com poden ser: 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.

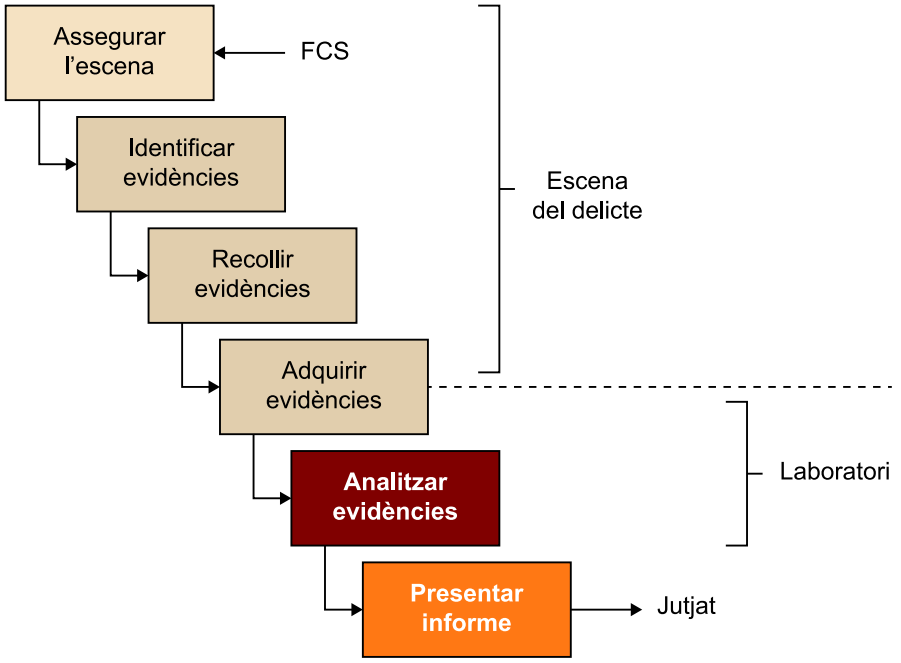
- **Adquisició**: el procediment d'adquisició comporta la creació d'una còpia bit a bit de l'evidència continguda en els dispositius digitals, així com la documentació dels mètodes emprats i dels passos realitzats. Hi ha una gran varietat de mètodes d'adquisició i eines validades (tant de maquinari com de 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.

- **Anàlisi**: en aquesta etapa, els perits 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, com per exemple: Encase, Autopsy, etc. Aquesta etapa sempre es durà a terme al laboratori.

- **Presentació**: finalment, com a conseqüència de l'etapa d'anàlisi, s'elaborarà un informe pericial que pot tenir diversos destinataris. 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 (per exemple, 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 un procediment judicial.

Figura 1. Etapes de l'anàlisi forense informàtica



La figura 1 mostra les etapes abans esmentades. El diagrama comença, en aquest cas, per l'assegurament de l'escena del delicte per part de les Forces i Cossos de Seguretat de l'Estat (FCS) i finalitza amb el lliurament de l'informe pericial al jutjat. Com a analistes i/o perits, les nostres tasques es circumscriuran, gairebé amb tota seguretat, a només un subconjunt de les etapes que us mostrem, però val la pena tenir en ment com seria el cas més complex en el qual podem participar.

Cal remarcar que, com ja s'ha apuntat anteriorment, l'adquisició es pot dur a terme (segons circumstàncies diverses), tant a l'escena del delicte, com al laboratori d'anàlisi. 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.

Hi ha multiplicitat d'institucions i manuals de bones pràctiques dedicats a la pràctica forense en l'àmbit digital. Nosaltres destaquem el manual de bones pràctiques (d'accés públic) elaborat per l'ENFSI (European Network of Forensic Science Institute). Aquesta institució va néixer oficialment el 1995 (encara que el seu primer congrés es remunta al 1993) i, entre altres objectius, procura que tots els països membres compleixin els estàndards de qualitat i segueixin les recomanacions dels manuals de bones pràctiques. L'ENFSI disposa de molts grups de treball segons l'àmbit forense (ADN, explosius, drogues, imatge digital, tecnologia digital, empremtes, etc.). A més de promoure l'intercanvi d'informació entre els membres, l'ENFSI fa congressos, molts de caràcter anual

(ordinaris i segons l'especialitat), als quals assisteix el personal dels laboratoris dels països membres. Espanya disposa de representants en l'ENFSI de diversos cossos policials (Policia Nacional, Guàrdia Civil, Mossos d'Esquadra i Ertzaintza), com també de l'Institut Nacional de Toxicologia i Ciències Forenses (òrgan adscrit al Ministeri de Justícia).

2. Assegurament de l'escena del succés

Aquesta fase sempre és preceptiva en el curs d'una actuació policial, encara que no sempre apareixerà en els casos reals d'anàlisis. No obstant això, tot i que difícilment ens trobarem amb aquests tipus de casos, les recomanacions sobre mesures de protecció del sistema i definició del marc de treball tenen un interès general i ens poden ser d'utilitat per a qualsevol cas. Amb massa freqüència, els analistes se circumscriuen als detalls tècnics del cas, eludint altres qüestions, com la protecció del sistema una vegada esdevingut el succés, la qual cosa podria arribar a invalidar la prova digital davant d'un tribunal.

La finalitat d'aquesta etapa consisteix, bàsicament, a assegurar l'escena del succés, restringint-ne l'accés perquè ningú no la pugui alterar. A més, en aquesta fase, els actuants també han de garantir que ningú no faci res sense estar segur de les conseqüències. El protocol proposat consta dels apartats següents:

- Identificar l'escena on s'ha produït el fet a investigar i establir un perímetre de seguretat.

- Restringir l'accés de persones i equips informàtics a l'interior del perímetre traçat.

- No permetre l'ús de cap dispositiu amb tecnologia sense fil per cap de les persones presents.

- Preservar les empremtes digitals mitjançant l'ús de guants de làtex.

- En aquest moment, s'ha de valorar la possibilitat de desconnectar les connexions de xarxa del sistema (dispositius sense fils, cables de xarxa, etc.). La desconnexió podria evitar que un determinat delicte o succés es continuï produint (per exemple, podria evitar l'eliminació remota de les proves digitals), però també cal valorar la utilització de la xarxa per a monitorar les connexions i investigar l'origen del succés (encara que cal tenir en compte que aquestes operacions sobre l'equip que s'ha d'investigar podrien implicar la pèrdua de la validesa de la prova davant d'un jutge).

- Si es troben impressores en funcionament, permetre que acabin la impressió.

- Anotar l'hora i la data del sistema[1] (marca horària o *timestamp*) abans d'apagar-lo (sempre que apareguin en el monitor, sense haver de manipular el sistema), i documentar aquests valors i fins i tot fotografiar-los o gravar-los en vídeo.

(1)La data i l'hora del sistema no ha de coincidir necessàriament amb la real. Aquest desfasament pot ser crucial per a l'analista i ha de ser documentat en aquest instant.

- Igualment, en cas que en el monitor apareguin processos rellevants (per exemple, els arxius que s'estan compartint en una aplicació d'igual a igual o P2P), és important fotografiar o gravar en vídeo aquesta informació. En general, s'ha de documentar qualsevol sortida del sistema que es consideri d'interès.

- Apagar[2] els dispositius encesos traient l'alimentació de la part posterior de l'equip[3] (especialment, en els casos en què es detecti destrucció d'informació). En cas de treure el cable directament de l'endoll, cal tenir present que el sistema podria disposar d'algun mecanisme de protecció en cas de caiguda del fluid elèctric, i es podrien escriure dades en el disc dur de l'equip. Així mateix, l'apagada «normal» de l'ordinador també podria ocasionar pèrdues greus d'informació si l'apagada activa algun procés d'eliminació de proves (per exemple, un *hacker* maliciós podria disposar de mesures de protecció d'aquest tipus). En general, no hi ha un procediment ideal per a resoldre la qüestió d'apagar els dispositius i, en cada cas, l'expert haurà de valorar quin mètode s'ha utilitzar en funció del resultat que es persegueix, l'equip que s'ha d'analitzar i el nivell de coneixements que se suposa a l'usuari de l'equip.

(2)No sempre és possible aturar el servei: imaginem, per exemple, el cas d'una fàbrica o d'una empresa proveïdora de serveis d'Internet, un hospital, etc.

(3)En el cas d'ordinadors portàtils apagats, cal extreure'n la bateria.

De vegades, l'assegurament de l'escena es produeix durant l'entrada i el registre en el lloc del succés amb l'ajuda dels membres de les FCSE. En aquest cas, l'entrada serà amb la presència del secretari judicial i el que s'hi esdevingui quedarà registrat en acta. Per tant, el secretari judicial registrarà en acta les comprovacions com, per exemple, l'hora i la data que puguin aparèixer en els monitors dels ordinadors, i no caldrà documentar la comprovació mitjançant fotografies o enregistraments. Així mateix, malgrat la presència del secretari judicial, de vegades pot ser pertinent aportar fotografies de l'escena o del que s'esdevingui en els monitors. Per exemple, continuant amb el cas ja descrit de les descàrregues de contingut il·lícit mitjançant aplicacions d'igual a igual (*peer-to-peer*), podria resultar d'interès fer una captura del contingut de la pantalla, encara que això impliqués l'alteració del sistema objecte d'anàlisi. En tot cas, el secretari judicial haurà de donar compte en acta de tot el que s'ha esdevingut durant l'entrada, especialment de les accions que hagin pogut alterar la prova digital.

3. Identificació de l'evidència digital

Es denomina així el procés d'identificació i localització de les proves que s'han de recollir per a analitzar posteriorment. Aquest procés no és trivial perquè, sovint, l'analista es trobarà en disposició d'empaquetar una quantitat ingent de material heterogeni: una xarxa sencera d'ordinadors, milers de DVD, dades al núvol, dispositius sense fil amagats, telèfons mòbils, etc. Per tant, l'analista ha de trobar una solució de compromís entre la qualitat, la validesa de la prova i el temps que hi ha invertit.

Com ja hem esmentat en apartats anteriors, podeu trobar més informació sobre la identificació, recollida, adquisició i preservació de l'evidència digital a la norma ISO/IEC 27037.

En primer lloc, l'analista ha d'identificar el sistema informàtic o dispositiu que ha d'analitzar amb la finalitat de saber on s'emmagatzemen les proves digitals que poden resultar útils per a la investigació. Així mateix, també ha de diferenciar entre les **proves volàtils** (memòria RAM, per exemple) i les que no ho són.

Proves volàtils

Essencialment, les que desapareixen en absència d'alimentació elèctrica.

El segon pas consisteix a valorar la necessitat d'obtenir les proves volàtils. Si és el cas, s'han de gravar com un fitxer en un dispositiu d'emmagatzematge extern al dispositiu que s'ha d'analitzar, de manera que en aquest moment es converteixen en proves no volàtils (la qual cosa implica l'obligatorietat d'accedir al sistema). Qualsevol tècnica que impliqui la manipulació del sistema original pot significar la invalidació de la prova en un procediment judicial (per exemple, n'hi ha prou d'obrir un arxiu per a modificar-ne la data de l'últim accés). En cas que sigui imprescindible accedir a un disc dur original, hi ha solucions de maquinari i de programari (hi aprofundirem en propers apartats) per a fer-ho evitant l'escriptura en el disc dur. Finalment, cal tenir en compte que, de vegades, els sistemes informàtics susceptibles de ser analitzats no es poden interrompre (per exemple, aturar un sistema informàtic podria implicar el cessament de l'activitat d'una fàbrica), de manera que les dades s'han d'obtenir a l'instant, per exemple, sol·licitant-les a l'administrador del sistema.

En tot cas, les manipulacions que es puguin fer del sistema informàtic original hauran de quedar clarament documentades. Sovint, aquestes manipulacions queden recollides pels secretaris judicials (per exemple, en diligències d'entrades i perquisicions en presència de les FCSE) o pels notaris. En cas que no disposem de cap d'aquestes figures, ho podrem fer nosaltres mateixos, estenent una acta de les accions que realitzem sobre el sistema informàtic.

Obtenció de proves

Altres vegades, les proves d'interès s'obtindran, per exemple, en monitorar una xarxa, la qual cosa pot significar, de nou, la invalidació de la prova davant d'un tribunal. Com ja s'ha esmentat, en cas de disposar de secretari judicial, serà imprescindible documentar en acta totes les manipulacions que s'hagin dut a terme per a arribar a obtenir la prova.

En general, l'analista ha de tenir en compte que les proves no solament es poden localitzar en els discos durs, i que actualment pràcticament qualsevol dispositiu electrònic (per exemple, un telèfon mòbil, un GPS, etc.) és susceptible d'emmagatzemar informació rellevant.

Exemples de dispositius electrònics susceptibles d'emmagatzemar informació rellevant (o de ser necessaris per a poder dur a terme l'anàlisi):

- Ordinadors i perifèrics connectats als ordinadors.
- Discos durs (no només els interns, sinó també els externs, NAS, etc.).
- CD o DVD.
- Dispositius en desús, com unitats ZIP o JAZ, disquets de 5 1/4", etc.
- Components de xarxa com, per exemple, un encaminador o un *switch*.
- Punts d'accés de les xarxes sense fil.
- Dispositius mòbils (telèfons, PDA, etc.) i els elements que contenen, com ara targetes SIM o de memòria.
- USB (notem que els USB poden tenir aspectes inesperats, com figures o joguets) i targetes de memòria.
- Impressores, escàners i fotocopiadores.
- Lectors/gravadors de targetes de banda magnètica (les targetes en si mateixes també són elements rellevants), cercapersones, etc.
- Motxilles (*dongles*). Aquests elements poden ser imprescindibles per a, per exemple, poder executar un determinat programari al laboratori.
- Dispositius per a fer còpies de seguretat o *backups*.
- Dispositius GPS.
- Sistemes de videovigilància (normalment, disposen de formats de sistema de fitxers propis, la qual cosa en dificulta o n'impossibilita l'anàlisi).
- Càmeres fotogràfiques i de vídeo digitals.
- Manuals, notes, paper imprès, etc.

Exemples de proves volàtils

Són proves volàtils les següents:

- Memòria RAM
- Fitxers temporals del sistema
- Estat de la xarxa
- Fitxers oberts
- Connexions de xarxa en ús
- Processos en execució, etc.

La tria dels elements o dispositius que s'hauran de recollir per a la seva anàlisi posterior dependrà en gran mesura de l'objectiu de l'anàlisi. Per exemple, és possible que necessitem agafar una impressora de l'escena del succés per a poder fer proves posteriors (de connexió amb un ordinador que s'està analitzant, per a poder comparar una impressió trobada amb les impressions que produeix una certa impressora, etc.). A més de discriminar els elements que seran analitzats, s'han de documentar aspectes generals del sistema, fins i tot d'aquells dispositius que no s'hagin de transportar al laboratori, així com tenir en compte les recomanacions següents:

- Fer una llista amb els sistemes (i la seva descripció) involucrats en el succés.

- Quant a les persones implicades, sol·licitar les dades que es considerin rellevants com, per exemple: nom, DNI, contrasenyes del sistema i d'usuaris, accions que s'hagin dut a terme des del coneixement de l'incident, etc.

- Fotografiar i/o gravar en vídeo l'escena del succés[4]. Sovint, també és desitjable representar esquemàticament el sistema que s'ha d'estudiar (per exemple, dibuixar la topografia d'una xarxa, identificant cadascun dels ordinadors que la constitueixen).

(4)Aquests esquemes o aquestes anotacions poden ser de molta utilitat en la fase d'anàlisi.

- Etiquetar els cables i els components. Molts dispositius, com els perifèrics lectors/gravadors de targetes magnètiques, poden necessitar un cablatge específic sense el qual el dispositiu no podrà funcionar i no es podrà analitzar posteriorment en el laboratori. Per tant, a més dels dispositius que s'analitzaran, també hem d'empaquetar tots els elements i el cablatge que, posteriorment, ens permetran utilitzar els dispositius en el laboratori, tant per a connectar-los a un sistema informàtic com per a proveir-los d'electricitat. Els cables han de ser etiquetats, de manera que es pugui identificar inequívocament el port del sistema informàtic en el qual estaven connectats.

- No encendre cap ordinador que estigui apagat.

- A part, cal esmentar els discos durs, en la majoria dels casos objectes principals d'anàlisi (el perit ha de considerar la possibilitat d'extreure'l per a la seva posterior anàlisi; sovint no cal l'ordinador, sinó només la informació continguda al disc dur). En aquestes circumstàncies, s'han de documentar tots els elements identificatius del disc dur (marca, model, número de sèrie, capacitat, etc.). Així mateix, hem d'extreure de les ranures de les unitats lectores de CD, DVD o qualsevol altre dispositiu, els suports digitals que puguin contenir, identificar-los i documentar-los adequadament.

- Fotografiar i gravar en vídeo els dispositius amb les etiquetes col·locades. Aquestes etiquetes també es poden anotar en els esquemes creats en el tercer punt d'aquesta llista de recomanacions.

4. Recollida de l'evidència digital

La fase de recollida implica la recollida dels dispositius físics (de la seva localització original) que poden contenir evidència digital, i documentar tots els dispositius recollits i els passos realitzats.

A l'hora d'efectuar la recollida cal evitar alterar, malmetre o destruir l'evidència digital. Així doncs, cal evitar utilitzar eines o objectes que provoquin electricitat estàtica o camps magnètics, per tal de mantenir intactes les evidències digitals (amb aquesta finalitat es poden utilitzar, per exemple, bosses i braçalets antiestàtics per al personal actuant).

Notem que hi haurà casos en què no es podrà efectuar la recollida dels ordinadors o dispositius diversos. Per exemple, no ens podrem emportar una xarxa complexa al laboratori (tot i que sempre tenim la possibilitat d'obtenir les evidències desitjades amb l'ajut de l'administrador del sistema). Per tant, les indicacions que mostrem en aquest apartat es refereixen més aviat als casos en què els ordinadors són dispositius aïllats (en cas de trobar-nos una xarxa d'ordinadors, el procediment pot ser força més complex, però en qualsevol cas haurem de tenir en compte les consideracions que tot seguit s'exposen).

Per tant, abans de procedir a la recollida del material caldrà tenir en compte:

1) Si l'ordinador està encès: en general, la forma més segura (tot i que normalment no és aquesta la que triarem) d'actuar davant d'un ordinador en funcionament, és **estirar el cable del corrent**. No obstant això, si l'evidència que estem cercant està, per exemple, ben visible a la pantalla, o sospitem que pot estar emmagatzemada a la memòria RAM, aleshores, en primer lloc, haurem de capturar i preservar la informació volàtil.

En les situacions següents **és recomanable** estirar el cable del corrent:

- Quan hi ha sospites o hi ha activitat a la pantalla que indica que la informació s'està esborrant o sobreescrivint.

- Quan hi ha algun procés que indica que s'està destruint algun dispositiu de emmagatzematge, com per exemple, el format d'un disc dur, la creació de noves particions o un procés d'esborrament segur (*wipe*) en funcionament.

- Cal valorar casos especials en els quals l'acció de prémer el botó *power* d'un dispositiu digital pugui estar configurada per iniciar un *script* que modifiqui o esborri la informació d'un sistema abans d'apagar-lo.

En les situacions següents **no és recomanable** estirar el cable del corrent:

- Quan a la pantalla es mostra informació clarament relacionada amb l'objecte de la nostra investigació.

- Quan hi ha indicis que hi ha algun dels programes següents en ús:
  - Clients de missatgeria instantània.
  - Documents oberts en pantalla.
  - Emmagatzemament de dades remot.
  - Programes d'intercanvi de fitxers amb continguts il·lícits.
  - Xifratge de dades (en aquest cas es pot valorar la possibilitat d'efectuar una adquisició lògica de la informació abans d'apagar l'ordinador).

En definitiva, quan l'ordinador està encès, abans de realitzar la recollida, caldrà valorar si primer hem de capturar o documentar (per exemple, amb una càmera fotogràfica o de vídeo) aquella informació que pot desaparèixer en apagar la màquina. De fet, el contingut de la memòria RAM pot ser cabdal en certes anàlisis, ja que hi podem trobar informació molt important, com ara contrasenyes de xifratge, llista dels processos en execució, ports oberts, etc.

En cas que la decisió presa sigui la de desconnectar l'ordinador de l'electricitat, aleshores s'ha de fer estirant el cable de l'extrem de la màquina (no pas de l'endoll). D'aquesta manera s'evitarà que si el dispositiu es troba connectat a un SAI (Sistema d'Alimentació Ininterrompuda) s'escriguin dades al disc dur i es pugui modificar l'evidència digital.

Cal tenir en compte, però, que a la gran majoria de casos no esperem tenir ni processos de xifratge, ni *hackers* preparats per a esborrar la informació. Per tant, amb una apagada normal de l'ordinador en podem tenir suficient.

2) Si l'ordinador està apagat: si tenim dificultats per a determinar si l'ordinador es troba apagat o en funcionament, podem engegar el monitor (en cas que no ho estigui), i moure el ratolí sense prémer cap botó. Si es produeix algun indici d'activitat, procedirem segons l'apartat anterior. Si efectivament comprovem que està apagat, seguirem les indicacions següents:

- Si no ho hem fet encara, cal documentar i fotografiar l'equip, totes les seves connexions i els perifèrics connectats. És possible que al laboratori necessitem reconstruir el sistema que s'ha d'analitzar.

- Desconnectar el cable del corrent des de la part posterior de l'ordinador. Si es tracta d'un portàtil, també cal extreure la bateria. Alguns portàtils s'engeguen en obrir la tapa. L'extracció de la bateria evita posar en funcionament el dispositiu de manera accidental.

- Desconnectar la resta de connexions tot indicant-les en la documentació.

- Si no ho hem fet encara, documentar el model i el número de sèrie de l'ordinador.

- Precintar l'ordinador, per exemple, dipositant-lo a l'interior d'una bossa tancada amb una brida. Si utilitzem etiquetes adhesives per a precintar, caldrà tenir en compte que els ports que permeten la connexió de l'ordinador han de romandre tapats i inaccessibles per evitar la modificació de les possibles evidències. Igualment, les etiquetes adhesives han d'evitar que es pugui extreure el disc dur o manipular l'interior de l'ordinador o dispositiu. En el cas d'utilitzar bosses precintades, és important col·locar dins la bossa tots aquells cables, carregadors d'electricitat, o elements diversos (*dongles*, etc.) que originalment estaven amb el dispositiu a l'escena de l'incident.

En cas que les condicions ho permetin, i si és necessari, es pot considerar la possibilitat d'extreure el disc dur (o discos durs) que pugui allotjar l'ordinador o dispositiu. En aquest cas, cal tenir present que l'extracció del disc dur facilita que es pugui malmetre en cas de no estar suficientment protegit. Per a evitar aquest problema, l'analista o perit que el manipuli pot emprar braçalets antiestàtics i bosses antiestàtiques per al disc dur extret.

Una vegada recollits els ordinadors o dispositius, caldrà empaquetar-los per a transportar-los al laboratori d'anàlisi. A l'hora d'empaquetar, precintar, transportar o emmagatzemar les evidències digitals cal tenir en compte que són fràgils i sensibles a temperatures extremes, humitats, cops, electricitat estàtica i camps magnètics. Per aquest motiu, s'hauran de prendre precaucions per preservar-les.

Finalment, a la fase de recollida també cal tenir en compte altres elements de mida més petita, com ara un DVD, USB, o fins i tot les evidències que puguem haver extret d'un sistema informàtic en funcionament, convenientment identificades i enregistrades en mitjans com ara un DVD, els quals s'hauran d'identificar, empaquetar i transportar amb les mateixes precaucions. Si cal, el secretari judicial (o el notari), identificaran unívocament a la seva acta els mitjans en els quals haurem extret les evidències que haurem considerat rellevants.

Cal tenir present que, segons el dispositiu que s'hagi de recollir, la metodologia emprada pot contenir matisos diferenciadors, en relació a la vista, molt importants. Tot seguit, veurem algunes recomanacions importants per al cas dels telèfons mòbils.

4.1. Recollida de telèfons mòbils

En els darrers anys, el número de telèfons mòbils ha registrat un increment espectacular fins arribar a superar els sis mil milions de dispositius l'any 2019, és a dir, al voltant d'un 70 % de la població mundial. Aquest fet ha afavorit un interès creixent en la ciència forense digital de telefonia mòbil en detriment

d'altres disciplines forenses digitals com ara l'anàlisi forense d'ordinadors o el de les xarxes de comunicacions. Actualment, s'estima que més del 75 % dels telèfons mòbils actius són intel·ligents. Aquests dispositius, realment són miniordinadors que poden enviar i rebre trucades, i que ens proporcionen una gran quantitat d'informació que podria resultar d'interès des d'un punt de vista forense.

A diferència dels ordinadors, vistos a l'apartat anterior, en el cas dels telèfons mòbils, la pròpia operativa de funcionament d'aquests dispositius pot comprometre la integritat de les dades que contenen. Així doncs, abans de traslladar el mòbil, en moltes ocasions, caldrà aïllar el terminal per a evitar que nous senyals entrants, com per exemple, SMS, puguin sobreescriure dades ja existents al mòbil i, per tant, es malmeti la integritat de l'evidència (no només poden desaparèixer dades, sinó que l'evidència s'altera, ja que no és exactament la mateixa que quan es va comissar el terminal). A més, si no s'aïlla, es podrien aprofitar remotament vulnerabilitats per a destruir evidències.

Abans d'emportar-nos un mòbil, doncs, cal valorar si és necessari aïllar el terminal i, si ho és, efectuar les operacions que calgui per a, efectivament, aïllar-lo de l'exterior. Per aconseguir-ho, podem triar diferents metodologies:

- **Posar el terminal en mode avió**: aquesta acció requereix interactuar amb el terminal emprant el teclat, la qual cosa implica assumir uns certs riscos, especialment si el perit o analista que el manipula desconeix la marca o el model. Mentre el mòbil està en mode avió no es podrà mantenir cap connexió sense fils. No obstant això, amb aquest mode d'operació també es pot emprar una xarxa wifi o Bluetooth, de manera que la connectivitat no es perd del tot.

- **Apagar el terminal**: si l'apaguem, per a encendre'l de nou podem necessitar conèixer diversos codis (PIN/PUK, patró de desbloqueig, mesures biomètriques), la qual cosa complicarà l'adquisició i en retardarà l'anàlisi).

- **Mantenir el mòbil en marxa, però aïllat (per exemple en una bossa de Faraday)**: aquesta opció escurça la càrrega de la bateria a causa de l'increment de consum d'energia que es produeix quan el dispositiu no es pot connectar a la xarxa i augmenta la força del senyal al màxim. D'altra banda, després d'un període en què el terminal no s'ha pogut connectar, alguns models poden esborrar dades de la xarxa que podrien ser d'interès per a la investigació. Finalment, és difícil garantir que les bosses de Faraday isolin completament el terminal, ja que poden estar mal tancades, o fins i tot els cables connectats a l'estació de treball podrien actuar d'antenes.

Si, per contra, decidim apagar el mòbil, caldrà tenir en compte que si no coneixem el PIN/PUK o el patró del dispositiu, l'anàlisi al laboratori es complicarà molt (o fins i tot no es podrà dur a terme).

Una vegada determinada i realitzada l'operació que el perit o analista hagi considerat, el terminal s'haurà de dipositar en un contenidor adequat i traslladar-lo al laboratori d'anàlisi.

Quan arribem al laboratori, si el mòbil l'hem deixat en funcionament, tant si es troba o no dins d'una bossa de Faraday, cal tenir present que caldrà mantenir la càrrega de la bateria per a evitar que es pugui apagar, perquè dificultarà o fins i tot impossibilitarà l'anàlisi posterior.

5. Adquisició de l'evidència digital

La facilitat amb la qual les proves digitals es poden modificar[5] i, fins i tot eliminar, determina un procediment acurat de preservació de la prova segons les lleis vigents i les solucions tecnològiques del moment. Aquest apartat és un dels més crítics de tota la seqüència, ja que un error en aquest punt podria arribar a invalidar una prova en el tribunal.

[5] Analitzar o observar un component del sistema n'alterarà d'altres.

No és possible obtenir una imatge congelada d'un sistema en un instant concret (és a dir, capturar la totalitat del sistema), si bé sovint les dades més rellevants per a la investigació es troben, simplement, en el sistema de fitxers de l'equip que s'ha intervingut, amb la qual cosa la pèrdua inevitable d'una part mínima de la informació (deguda a la impossibilitat esmentada) és un mal menor. D'altra banda, en cas que no sigui possible evitar l'alteració del sistema (és a dir, s'hagi de fer una anàlisi en viu del sistema), caldrà documentar el que ha passat mitjançant actes, fotografies o enregistraments de vídeo. Afortunadament per a nosaltres, sovint no cal actuar amb prestesa; tampoc no es requereixen mesures excepcionals per a protegir l'accés al sistema, ni es necessita l'obtenció de les proves volàtils, ja que amb les dades del sistema d'arxius és suficient per a desenvolupar l'anàlisi. En definitiva, en molts casos l'analista podrà dedicar el temps, amb tranquil·litat, a la tasca de duplicar la informació que contenen els suports (com ara discos durs) objecte d'estudi. Aquesta duplicació o clonació es podrà dur a terme, segons el cas, en el lloc de l'incident, o posteriorment al laboratori (si, per exemple, podem extreure els discos durs i transportar-los amb garantia al laboratori).

El procediment que s'ha d'observar per a adquirir l'evidència digital consta dels passos següents:

1) Còpia de bits dels suports originals. Qualsevol prova digital identificada com a rellevant per a la investigació s'haurà de copiar mitjançant programari o maquinari[6] que no n'alteri la integritat i que en permeti l'admissió en un tribunal de justícia. La còpia o **clon** s'ha de fer en l'àmbit dels bits, és a dir, el seu contingut ha de ser exactament el mateix que el del dispositiu original, incloent-hi els fitxers ocults, temporals, eliminats encara no sobreescrits i, fins i tot, ha d'incloure el denominat **espai desaprofitat** (s'anomena així l'espai entre el final lògic d'un fitxer i el final físic), com també la informació que conté l'espai no assignat del disc dur (en definitiva, el clon ha de ser una còpia exacta de l'original).

[6] Posteriorment, s'incidirà en les eines de programari o maquinari que es poden utilitzar per a crear una còpia de bits.

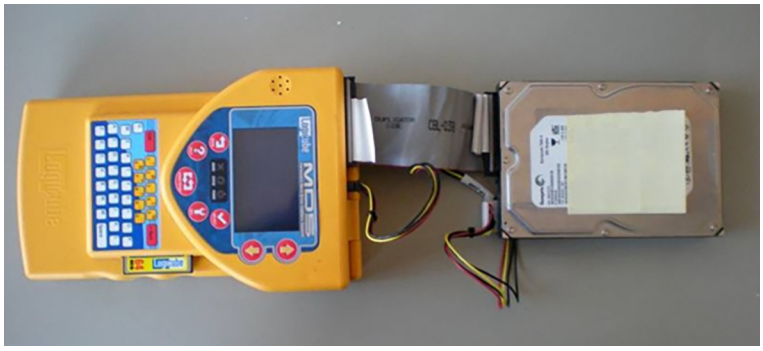
Anàlisi de dispositius

Hi ha procediments que permeten l'examen dels suports originals sense alterar-ne el contingut. De totes maneres, sempre que sigui possible és preferible treballar amb un clon.

El procés de clonació tindrà lloc sobre un dispositiu normalment aportat pel grup actuant: disc dur, CD-ROM, DVD, etc. L'elecció d'un mitjà o d'un altre dependrà de la quantitat d'informació continguda en els suports originals (nor-

malment s'empren discos durs). L'ús de CD-ROM o DVD presenta l'avantatge addicional que la informació que contenen no es pot modificar i, per tant, amb el seu ús es garanteix la integritat de la prova. Quant al **clon** o la **còpia**, es poden emprar mètodes de maquinari o de programari (LinEn, Acronis True Image, distribucions forenses de Linux, etc.). A la figura 2, podem apreciar un duplicador de maquinari.

Figura 2. Duplicador o clonador de discos durs (de Logicube)



Nota

Evidentment, la capacitat del disc dur de destinació ha de ser més gran o igual que la del disc dur original.

Aquest tipus de dispositiu ens permet generar un clon d'un disc dur sobre un altre d'aportat pels actuants. L'original es col·loca a l'exterior del duplicador, i el receptor (del qual s'haurà eliminat prèviament qualsevol rastre d'informació que pogués contenir mitjançant tècniques d'esborrament segur) a l'interior. Per descomptat, hem d'extremar la precaució en el moment d'efectuar la connexió dels discos durs, ja que l'intercanvi del disc d'origen pel de destinació provocaria la pèrdua irrecuperable de la informació original. La duplicació s'efectuarà de manera automàtica i transparent a l'operador. A més, fins i tot és possible dur a terme la cerca automatitzada de cadenes de caràcters (per exemple, la cadena literal «bomba») al mateix temps que es fa el duplicat.

Esborrament segur

Hi ha diferents eines, tant de programari com de maquinari (per exemple, els mateixos clonadors solen disposar d'aquestes funcions), per a dur a terme l'esborrament segur d'informació (*wipe*). Es basen en l'escriptura d'un determinat caràcter (efectuant diverses passades) en tots els sectors d'un disc dur.

Els dispositius duplicadors també poden generar **arxius d'imatges (imatges forenses)**, normalment de grandària més petita que el suport original, els quals també contenen tota la informació de l'original i en permeten l'anàlisi mitjançant l'ús d'eines de programari especialitzades, com Encase o Autopsy.

No solament els discos durs són susceptibles de ser duplicats, també ho és, per exemple, la informació que contenen els terminals de telefonia mòbil[7]. Així, tant les targetes que allotgen com les dades de la memòria es poden duplicar i emmagatzemar, per exemple, en una altra targeta de memòria aportada per l'analista forense (o abocar directament sobre el disc dur d'anàlisi). A la figura 4, podem veure un dispositiu utilitzat per a extreure la informació que conté un telèfon mòbil. Aquest tipus de dispositiu necessita una gran diversitat de cables per a garantir la connexió amb el màxim nombre possible de mòbils. Naturalment, la col·lecció de cables s'ha d'ampliar freqüentment per a poder accedir als nous terminals de telefonia que vagin sorgint en el mercat, i el seu cost econòmic de manteniment és molt elevat[8]. Les solucions actuals solen consistir en una combinació entre maquinari i programari.

(7)A part dels discos durs, hi ha molts altres dispositius electrònics que poden allotjar evidències digitals, com ara telèfons mòbils, GPS, dispositius lectors/gravadors de targetes de banda magnètica, etc.

(8)Cal recordar que cada fabricant pot emprar un tipus de cablatge diferent i, a més, els diferents models de cada fabricant solen disposar del seu propi cablatge específic. Sortosament, actualment els tipus de cablatge són més estàndards i principalment només se n'usen 2 o 3.

Evidència digital en la telefonia mòbil

Algunes proves que es poden localitzar en un telèfon mòbil:

- SIM (*subscriber identity module*)
- Número IMEI (*international mobile equipment identity*)
- Agenda telefònica
- Fotografies i àudio
- Configuració (data/hora, llenguatge, etc.)
- Executables emmagatzemats, etc.

Figura 3. Maleta de cablatge del dispositiu de la figura 4 (de Cellebrite)

Figura 4. Abocament d'informació d'un mòbil a un dispositiu USB (de Cellebrite)

A més d'aquestes solucions generalistes, la majoria de mòbils disposen de les seves pròpies aplicacions per a descarregar continguts i fer còpies de seguretat per a ús dels usuaris. Aquests programes es poden trobar en les pàgines web dels fabricants, encara que no solen oferir gaires prestacions com a eines forenses.

Per descomptat, hi ha molts altres dispositius tecnològics susceptibles d'emmagatzemar informació a l'interior. Per exemple, un dispositiu lector de targetes de banda magnètica. En aquest cas, en no haver-hi un dispositiu específic de duplicació, una estratègia possible a seguir consisteix a extreure la memòria del lector, fer-ne un abocament i interpretar el resultat obtingut. Aquesta operació pot revestir una gran complexitat, ja que la memòria pot estar protegida per una contrasenya, i fins i tot el contingut pot estar xifrat mitjançant algun algorisme.

Finalment, cal assenyalar que una de les diferències més importants entre les diferents pràctiques forenses és que, en l'àmbit de les ciències forenses habituals (ADN, drogues, explosius, etc.), la prova, encara que de vegades és divisible, no es pot duplicar, mentre que en l'àmbit de la tecnologia digital sí que es pot duplicar, la qual cosa és sens dubte avantatjós, encara que això pugui implicar problemes de verificació i preservació de la integritat de la prova.

2) Verificació de la integritat de la còpia o imatge. Una vegada generada la còpia o el clon del suport original, el programa o el dispositiu de maquinari emprat en aquest procés fa el càlcul del valor ***hash*** del suport original i de la destinació, amb la finalitat de garantir que tots dos són idèntics i que la còpia s'ha produït sense cap error (els dos valors han de ser coincidents). Aquest càlcul es fa sobre tot el conjunt de fitxers del suport clonat.

Funcions *hash*

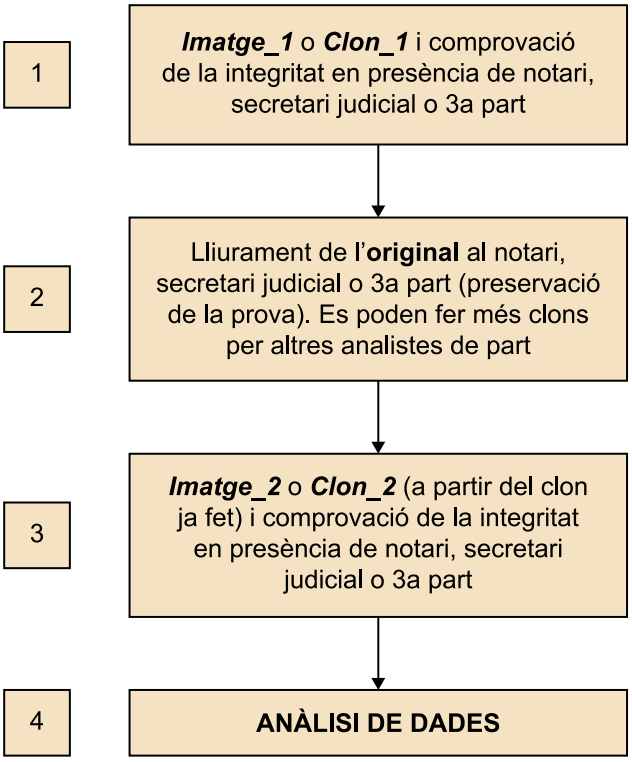
Per a més informació sobre les funcions *hash* podeu consultar l'apartat de preservació de les evidències digitals.

Funció *hash*

Funció matemàtica unidireccional que resumeix un missatge de grandària variable (per exemple, un arxiu) en una representació de grandària fixa. És poc probable que dos fitxers diferents tinguin la mateixa representació *hash*, la qual cosa significa que aquest valor es pot utilitzar per a comprovar la integritat d'un arxiu (o d'un sistema). Les funcions *hash* més conegudes són MD5 i SHA-1.

La figura 5 mostra el protocol d'actuació que ha de seguir l'analista per a adquirir les dades preservant la integritat de la prova. En aquest cas suposem que s'ha pogut extreure el disc dur del dispositiu. Si no s'hagués pogut extreure, en primer lloc s'haurien hagut d'obtenir les evidències (buidatge de memòria RAM, fitxers de registre, etc.) i després tractar-les seguint el protocol que s'exposa a la figura 5:

Figura 5. Protocol d'adquisició i preservació de la prova



En general, sempre haurem de mantenir les precaucions següents:

- L'anàlisi sempre s'ha de fer a partir d'una segona còpia (o imatge) del suport que s'ha d'analitzar. És a dir, en cas que aquesta segona còpia o imatge pateixi algun dany, sempre es podrà reiniciar l'anàlisi a partir de la primera còpia que tenim, de manera que obtindrem un nou clon o una nova imatge.

- En cas que el suport que s'ha d'analitzar sigui extraïble, cal que l'original (una vegada fetes les còpies pertinents) es lliuri a la tercera part del procés, és a dir, al fedatari de l'origen del suport. A més, amb aquesta acció permetem que es pugui produir un contraperitatge i garantim que les nostres hipòtesis es puguin reproduir, mitjançant un altre analista, a partir d'una còpia de l'original custodiat.

- Quant a la presència del secretari judicial durant el procés de clonació, hi ha diverses sentències que determinen que no és preceptiva, ja que no pot donar fe d'un procés tècnic que no està obligat a conèixer en l'exercici de les seves funcions.

El cas exposat és dels més senzills que es poden trobar, ja que sovint podem trobar problemes com els que es descriuen tot seguit:

- Heterogeneïtat de sistemes interconnectats.

- Configuracions complexes (sistemes RAID, per exemple).

- Programaris especialitzats (programes de comptabilitat, gravadors de vídeo, etc.): en aquests casos, encara que s'hagi clonat el disc dur que els conté, pot no ser senzill, durant la fase d'anàlisi, obrir els fitxers que tinguin un format propi (i veure'n el contingut), específicament dissenyat per a l'aplicació.

- Servidors ubicats en llocs distants a l'escena del crim.

- Dades al núvol: l'adquisició de les dades al núvol, que poden ser compartides per diversos usuaris, pot implicar la vulneració del dret a la intimitat (a més de necessitar una metodologia d'adquisició específica). Si les dades no s'han adquirit segons els preceptes legals vigents, poden no tenir validesa jurídica.

- Volum molt gran de dades: en aquest cas ens podem plantejar realitzar una adquisició lògica de les evidències rellevants, i triar només allò que sigui rellevant per al cas d'estudi.

- Dispositius SSD (*solid state drive*): el valor *hash* d'adquisició dels dispositiu SSD pot canviar (per causes inherents al seu funcionament) si es fan diverses clonacions consecutives, encara que la integritat de la prova no hagi estat compromesa.

- Sistemes crítics que no es poden aturar (hospitals, empreses, etc.): en aquests casos haurem d'obtenir les evidències amb el sistema informàtic en funcionament, sovint amb l'ajut dels administradors.

3) Retenció de temps i dates. Les dates i les hores de creació, accés i modificació d'un fitxer poden resultar de molta utilitat a l'hora d'elaborar un informe pericial. Aquestes dades estan vinculades a la data i l'hora del rellotge del sistema i, tot i que poden ser de molta utilitat forense, el cert és que es poden modificar amb facilitat i poden no ser significatives. La data i l'hora dels fitxers analitzats pot ser molt rellevant en algunes investigacions, com per exemple les intrusions en els sistemes informàtics. En aquest tipus d'anàlisi és molt important poder relacionar les dades horàries proporcionades pels fitxers de registre (o fitxers log) de connexió amb la informació localitzada en els dispositius confiscats. Finalment, sempre que sigui possible (per exemple, en el cas de l'anàlisi d'un ordinador aïllat en un domicili particular), és interessant comprovar l'hora i la data emmagatzemada a la BIOS del sistema.

GMT

Es pren com a base l'hora GMT (Greenwich Mean Time), que és el fus horari que passa pel meridià de Greenwich (hora 0). Segons aquesta convenció, la Terra està dividida en vint-i-cinc zones, de –12 a +12, amb l'hora 0 com a referència. El fus horari que correspon a Espanya és GMT+1.

4) Documentar qui va preservar la prova, on la va preservar, com ho va fer, quan i per què. Aquesta informació documental dona inici al que es denomina **cadena de custòdia**, la finalitat de la qual no és altra que la de permetre la traça de les proves adquirides.

5) Embalar els dispositius que contenen les proves. En cada paquet s'ha d'anotar, com a mínim, la informació següent:

- Identificador únic.
- Nom del tècnic responsable del material confiscat.
- Descripció del material (marca, número de sèrie, etc.).
- Propietari o usuari del material confiscat i lloc on s'ha confiscat (per exemple, es pot indicar l'habitació del domicili on es va trobar la prova).
- Dia i hora de la confiscació.
- Informació relacionada amb la causa que s'investiga (per exemple, les diligències prèvies de la causa).

6) Els suports magnètics o òptics (cintes de còpies de seguretat o *backups*, DVD, discos durs, etc.), s'han d'introduir en bosses antiestàtiques i posteriorment s'han d'acondicionar amb material protector contra possibles cops durant el transport[9].

[9]Si es troben suports, com per exemple un disc dur, submergits en líquids, s'han de conservar en el medi on s'han trobat, i no s'han d'extreure ni assecar.

7) Els tècnics que participen en aquest tipus d'anàlisi han de prendre precaucions per a preservar la prova de factors externs com, per exemple, la pluja o el pas dels embalatges a través d'un arc magnètic d'un jutjat.

8) Transport de les proves a un lloc segur i que tingui els factors ambientals que permetin conservar la integritat de la prova. L'embalatge i el transport dels dispositius també forma part de la **cadena de custòdia**, la qual permet garantir

la integritat de les proves des de l'obtenció fins a la posada a disposició de l'autoritat judicial (o l'arribada al laboratori). La documentació de la cadena de custòdia ha de registrar totes les baules per les quals circulen les proves; això ens permetrà saber on són emmagatzemades i qui hi ha accedit en qualsevol moment.

6. Preservació de l'evidència digital

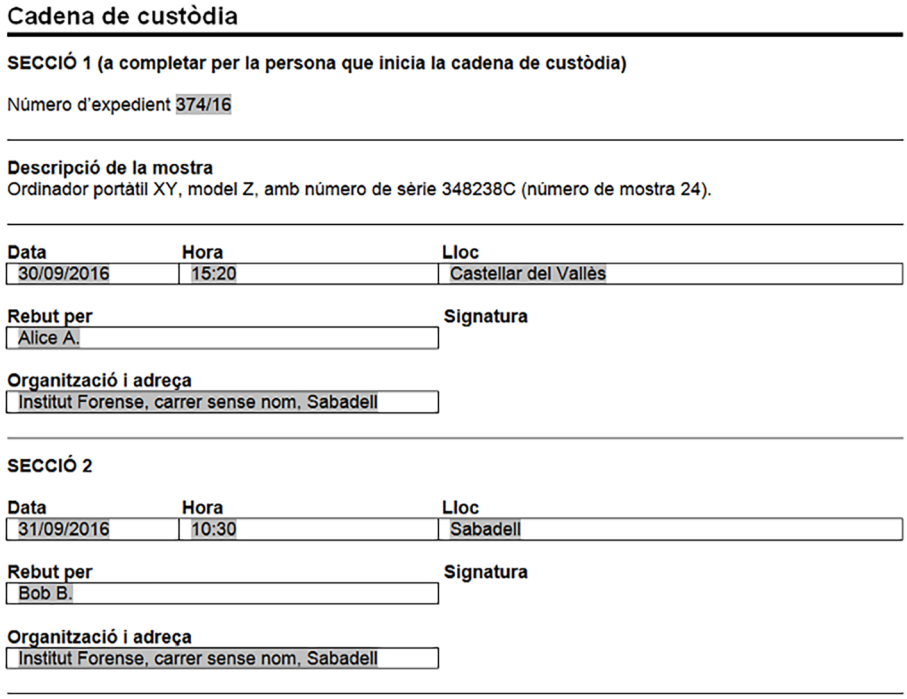
El procés de preservació implica la salvaguarda de l'evidència digital i dels dispositius que la poden contenir. El procés de preservació ha de començar en la primera fase del procés (identificació) i s'ha de mantenir durant la resta de fases de la gestió de l'evidència digital.

En un escenari òptim, no s'hauria de produir cap alteració o destrucció de les dades o de les metadades associades (per exemple, les dates de darrera modificació d'un arxiu). L'analista o perit ha de ser capaç de demostrar que l'evidència no s'ha alterat des que fou identificada, recollida o adquirida.

En qualsevol investigació, l'analista ha de poder donar compte de les dades i dels dispositius recollits i/o adquirits. Amb aquesta finalitat emprarà la **cadena de custòdia**, que és un registre (document físic o registre digital) que mostra, cronològicament, el moviment i la gestió de l'evidència en tot moment, des que fou recollida i/o adquirida. Per tant, la cadena de custòdia permet la identificació dels accessos i moviments soferts pels dispositius digitals i les evidències en qualsevol data i hora des que foren recollits. La cadena de custòdia hauria de contenir, com a mínim, la informació necessària per a identificar l'evidència, qui hi ha accedit, quan i en quin lloc s'ha realitzat l'accés, etc.

A la figura 6 es pot veure un exemple (un formulari en paper) de cadena de custòdia.

Figura 6. Exemple documental de cadena de custòdia



Cadena de custòdia

SECCIÓ 1 (a completar per la persona que inicia la cadena de custòdia)

Número d'expedient 374/16

Descripció de la mostra
Ordinador portàtil XY, model Z, amb número de sèrie 348238C (número de mostra 24).

Data	Hora	Lloc
30/09/2016	15:20	Castellar del Vallès

Rebut per | **Signatura**
Alice A.

Organització i adreça
Institut Forense, carrer sense nom, Sabadell

SECCIÓ 2

Data	Hora	Lloc
31/09/2016	10:30	Sabadell

Rebut per | **Signatura**
Bob B.

Organització i adreça
Institut Forense, carrer sense nom, Sabadell

En resum, el que és essencial en l'establiment de la cadena de custòdia és:

- La primera anotació en el document (vegeu la secció 1 de la figura 6) ha d'incloure la identificació amb què s'hagi etiquetat l'indici (entenent per indici un dispositiu informàtic qualsevol, una bossa precintada, etc.).

- La primera anotació ha d'incloure una descripció de l'indici, amb la data, l'hora de recollida, una identificació completa (telèfon, nom, persona/organització i adreça (o les dades que determini la institució com a preceptives) de qui ha recollit la mostra, així com la seva signatura.

- Seguidament, s'han d'anar documentant els transportistes següents o custodis de la mostra, amb la mateixa identificació indicada en el punt anterior (vegeu la secció 2 de la figura 6).

En cas d'emprar cadenes de custòdia en format paper, és habitual que la persona que es desprèn del formulari se'n guardi una fotocòpia abans de lliurar l'original al responsable de la cadena següent. En tot cas, el formulari original sempre es podrà localitzar juntament amb les evidències originals.

La tendència actual, quant a la cadena de custòdia, és que es digitalitzi progressivament, no només pel que fa a la desaparició del document en format paper, sinó també en relació a la traçabilitat i garantia d'integritat de les evidències, i fins i tot a l'auditabilitat de la cadena en si mateixa.

És important que la data i l'hora anotades siguin, exactament, en les quals es transfereixen els indicis, perquè indiquen en quin moment ha canviat la persona que n'és responsable i qui en té la custòdia a partir de llavors i, per tant, n'és ara el nou responsable.

A més d'indicar-ho en el document que registra les accions referents a la cadena de custòdia, els indicis o dispositius (ordinadors, portàtils, telèfons, discos, etc.) que eventualment contindran les evidències han de ser etiquetats (marcats de manera permanent) en ser recollits i, si escau, precintats adequadament per evitar-ne posteriors manipulacions no autoritzades. La persona que els ha recollit ha de poder assegurar en un judici que són els mateixos indicis que va aplegar en el seu moment. De la mateixa manera que es fa amb els indicis, les anotacions en el document de la cadena de custòdia s'han de fer amb algun dispositiu permanent.

Si la cadena de custòdia fos incompleta, o s'hagués produït algun error que el jutge considerés significatiu, podria determinar, segons la severitat d'aquest error o buit, que les evidències fossin inadmissibles, o bé admetre-les i atorgar-los un pes o significat diferent a l'inicialment previst per la part que pre-

senta les proves. Això pot, a més, portar a objeccions o apel·lacions per la part contrària. Per tant, encara que els indicis poguessin ser acceptats, aquests tipus d'errors poden arribar a disminuir fatalment el valor de l'evidència digital.

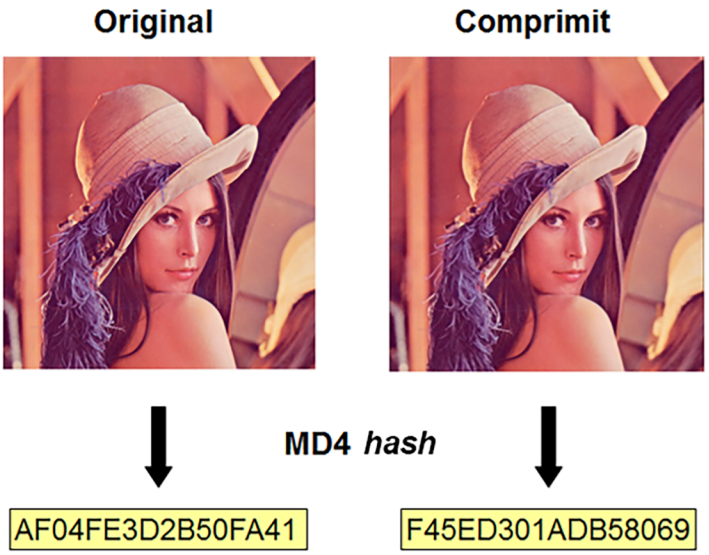
6.1. Verificació de la integritat mitjançant funcions *hash*

Quan hem introduït el concepte de clon s'ha definit què és un funció *hash* i com s'utilitzava per a verificar que el procés de clonació havia estat correcte. Per la mateixa raó, aquest tipus de funció també es pot emprar per a comprovar que la integritat d'una evidència digital no ha estat compromesa.

Des del punt de vista que ens ocupa, una funció *hash* és una funció matemàtica que, aplicada al contingut d'un suport informàtic (USB, disc dur, etc.), o fins i tot a un fitxer individual, genera un resultat únic, rellevant a efectes d'identificació del suport o fitxer. Val a dir que qualsevol petita alteració en el suport, fins i tot el canvi d'un sol bit, produiria, en calcular un nou valor *hash*, un resultat completament diferent del generat en primera instància.

El càlcul de la funció *hash* és realitza sobre els bits de l'arxiu i no pas sobre l'aparent contingut visual que aquest pugui tenir. Així doncs, dues fotografies poden ser visualment idèntiques, però si informàticament tenen formats diferents o presenten un sol bit de diferència, el càlcul de la funció *hash* donarà valors diferents per als dos fitxers. Aquesta característica es pot comprovar a la figura 7.

Figura 7. Exemple de funció *hash* (MD4)



Notem a l'exemple que encara que el contingut visual dels dos fitxers és igual, com a arxius informàtics (és a dir, quant a bits), les dues imatges són diferents, ja que les dues fotografies no tenen el mateix format (una és un arxiu compri-

mit JPG i l'altra un fitxer BMP). En aquest exemple s'ha emprat, amb finalitats didàctiques, la funció *hash* MD4, encara que les que actualment es fan servir en informàtica forense són les funcions SHA-2, SHA-1 i MD5.

A causa d'aquesta propietat d'identificació unívoca de les funcions *hash*, sovint s'incorporen els valors *hash* generats durant el procés de còpia bit a bit dels suports informàtics als informes pericials. Així, en principi, si es compara el resultat del valor *hash* del suport original amb el del suport copiat o clonat (per exemple, quan un perit fa un contraperitatge i obté una nova còpia d'anàlisi), tots dos valors haurien de ser idèntics, ja que el segon suport conté una còpia íntegra del primer. Si no s'obté el mateix resultat, podria voler dir que la cadena de custòdia ha estat compromesa i els suports informàtics alterats. Tot i que aquesta consideració pot ser absolutament errònia, com es veurà tot seguit, el cert és que des del vessant no tècnic, de vegades s'ha considerat, de forma completament errònia, el valor *hash* com una mena de precinte digital, garant de la cadena de custòdia.

Matemàticament parlant, la funció *hash* presenta, en qualsevol de les seves formes, un problema inherent de col·lisió, és a dir, és possible (encara que la probabilitat és molt petita) que dos suports informàtics o dos fitxers diferents, puguin tenir el mateix valor *hash*. També cal tenir present, com ja s'ha indicat, que el canvi d'un únic bit implica el canvi absolut del valor *hash*. Això implica que si el dispositiu original (un disc dur, per exemple) ha patit qualsevol cop durant el transport o el seu emmagatzemament, o qualsevol altre problema que l'hagi pogut danyar, és possible que les verificacions de les funcions *hash* produeixin valors diferents, sense que la informació rellevant hagi estat realment alterada (el dany pot no haver afectat les evidències d'interès). A més, en el cas dels discos durs dels ordinadors personals, és possible que amb el pas del temps la informació es malmeti sense que s'hagi produït cap tipus d'intervenció, fet que també produirà un valor *hash* diferent, tot i que no s'hagin compromès les evidències.

Finalment, el càlcul successiu de funcions *hash* sobre un dispositiu de tecnologia SSD, també pot generar resultats diferents, sense que ningú hagi tan sols accedit al contingut del dispositiu (i molt menys l'hagi modificat).

Per tant, cal ser molt curós a l'hora d'interpretar el valor *hash* associat a un dispositiu que conté evidències digitals i, en cas d'obtenir resultats divergents, cal tenir present que el fet pot ser explicable, sense que ningú hagi accedit o alterat l'evidència.

6.2. Digitalització de la cadena de custòdia

La tendència actual, quant a la cadena de custòdia, és que es digitalitzi progressivament, no només pel que fa a la desaparició del document en format paper, sinó també en relació a la traçabilitat i garantia d'integritat de les evidències, i fins i tot a l'auditabilitat de la cadena en si mateixa.

Aquesta proposta ja la podem veure, per exemple, a l'article de Ćosić i Bača (2010), on se suggereix la incorporació de *timestamps* (segells de temps) i la inclusió de mesures biomètriques dels analistes per tal de saber, de manera segura, qui té les evidències. Per tant, en aquest nou paradigma, l'evidència ja no viatja sola, sinó que anirà acompanyada de diverses dades que ens permeten auditar i traçar tots aquells aspectes d'interès en relació a la preservació de l'evidència durant tot el seu cicle de vida.

L'article ja esmentat descriu conceptualment els elements que ha de contenir aquesta cadena de custòdia, i que caldria tenir en compte a l'hora d'implementar-ne la digitalització:

- **Qui** té l'evidència: a l'exemple de la figura 8, l'analista s'identifica mitjançant una mesura biomètrica (una empremta dactilar).

- **Quina** és l'evidència: en aquest cas proposen el valor *hash* per a identificar-la.

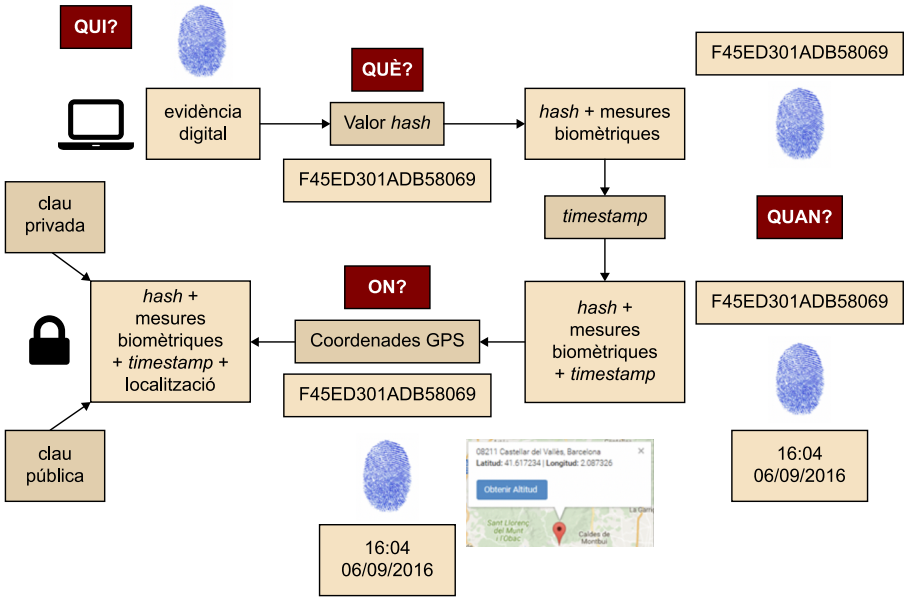
- **Quan** s'accedeix a l'evidència: es necessita establir la data i l'hora de cada accés a l'evidència.

- **On** s'accedeix a l'evidència: també serà necessari establir el lloc on s'ha produït l'accés (per exemple, les coordenades GPS on s'ha adquirit l'evidència o les del laboratori on s'hagi pogut transportar, etc.).

I ja per acabar, per a protegir la confidencialitat de la informació, l'esquema finalitza amb la introducció de mesures criptogràfiques.

Amb aquestes dades seria suficient per a poder gestionar la cadena de custòdia d'una evidència digital.

Figura 8. Digitalització de la cadena de custòdia



Altres estudis van més enllà, i proposen una implementació de l'esquema abans descrit, en què la cadena de custòdia ja s'ha digitalitzat completament i ha esdevingut informació que es transmet entre dos o més dispositius que controlen tot el procés (Marqués Arpa, T.; Serra Ruiz, J., 2014), i abasta des de la creació del propi document digital de la cadena de custòdia, fins a l'autenticació de les persones (procés de confirmació de les seves identitats) que poden accedir a les evidències, passant també per la geolocalització de l'evidència en tot moment.

El dispositiu conté el certificat personal que es transmet de manera segura a la central de dades, de manera que en tot moment es pot saber on és i qui té una determinada evidència, i així poder-ne revocar l'accés de manera remota, si es donés el cas. Una entitat de confiança proporciona el segell de temps en què les evidències són accedides o enviades a altres persones, de manera que la cadena de custòdia deixa de ser un formulari físic per a esdevenir un conjunt de dades que es van agregant a l'evidència de manera segura i on s'anirà desant de manera automàtica tot allò que està succeint i que, posteriorment, si escau, podrà ser auditat.

7. Anàlisi de la prova digital i investigació

Exemple de metadada

El contingut del camp «Autor» que apareix en tots els fitxers del Microsoft Word és un bon exemple de metadada.

En aquesta fase, el perit o l'analista ha de respondre les preguntes que s'han exposat en la introducció d'aquest mòdul, estudiant la prova digital recollida en les fases anteriors. Aquest estudi es basarà en l'anàlisi del contingut dels fitxers (**dades**) i de la informació sobre aquests fitxers (**metadades**).

En primer lloc, s'ha de revisar l'embalatge que conté les proves, amb la finalitat d'assegurar la integritat de la cadena de custòdia i documentar qualsevol anomalia que es pugui apreciar.

Normalment, les proves s'analitzen en funció dels extrems que ha de respondre el perit, ja que una anàlisi exhaustiva requereix, en la majoria dels casos, un esforç desproporcionat en relació amb l'objecte de l'anàlisi. Així mateix, en el cas de peritatges relacionats amb delictes, s'haurà d'analitzar un tipus concret de proves i en un ordre determinat en funció del delicte que s'hagi d'investigar. Finalment, els paràmetres de l'anàlisi també s'hauran d'ajustar al sistema operatiu (Mac OS, Windows, Linux, Android, etc.) del dispositiu que s'ha d'analitzar.

Justament, una de les màximes de l'anàlisi forense té a veure amb el funcionament intrínsec dels sistemes operatius i de les aplicacions que hi ha:

> Per molt expert i coneixedor que sigui un usuari d'un sistema operatiu o d'una aplicació, mai no podrà controlar i eliminar totes les traces provocades pel mateix funcionament d'aquests elements.

En la fase d'anàlisi poden aparèixer diferents categories de dades que s'han d'analitzar, bona part de les quals seran lògicament accessibles, és a dir, dades contingudes en fitxers, directament accessibles. En aquest procés d'anàlisi podem trobar diversos problemes, com els que esmentem tot seguit:

- **Massa informació**. Dispositius amb moltes gigues d'informació que s'han d'analitzar i dificultat per a destriar els fitxers amb un contingut que pot ser rellevant. Les eines d'anàlisi disposen de moltes possibilitats per a discriminar la informació rellevant (cerca de cadenes, exclusió de fitxers amb el valor *hash* conegut, etc.).

- **Fitxers troianitzats**. És a dir, fitxers que contenen un codi ocult l'execució del qual pot tenir conseqüències imprevisibles. Per a detectar aquest tipus de fitxers, es poden utilitzar eines de comprovació de la integritat i programes detectors de virus i *malware*. Per a comprovar l'efecte i el funciona-

ment d'aquest fitxers es poden emprar tècniques diverses, com ara l'anàlisi de la memòria RAM i l'execució d'aquest tipus de programari (*malware*) en entorns segurs que permeten ser monitoritzats fàcilment sense comprometre la seguretat del sistema. També existeix la possibilitat de pujar el fitxer maliciós a webs que contenen un ampli catàleg de fitxers *hash* i que poden generar-lo, i creuar el *hash* obtingut. D'aquesta manera, podem obtenir una descripció del fitxer, així com de les accions que realitza.

- **Fitxers xifrats o protegits**. El fitxers amb mètodes forts de xifratge (per exemple, GnuPG) no es poden analitzar (llevat d'excepcions puntuals). No obstant això, altres mètodes de protecció, com les contrasenyes d'accés a fitxers de text (per exemple, Microsoft Office) o fitxers comprimits, es poden analitzar utilitzant aplicacions desenvolupades per terceres parts i amb un cost de computació relativament baix per a contrasenyes relativament curtes.

Fitxers xifrats o protegits

Sovint els usuaris xifren els arxius sense eliminar els originals. Per tant, en tota anàlisi amb arxius xifrats és aconsellable localitzar els noms d'arxius iguals als xifrats. Així mateix, els arxius temporals generats per algunes aplicacions permeten accedir, de manera indirecta, al contingut (parcial o total) dels arxius xifrats. Per a tractar fitxers protegits amb una contrasenya, hi ha programes que la trenquen per força bruta utilitzant el càlcul distribuït entre diversos ordinadors.

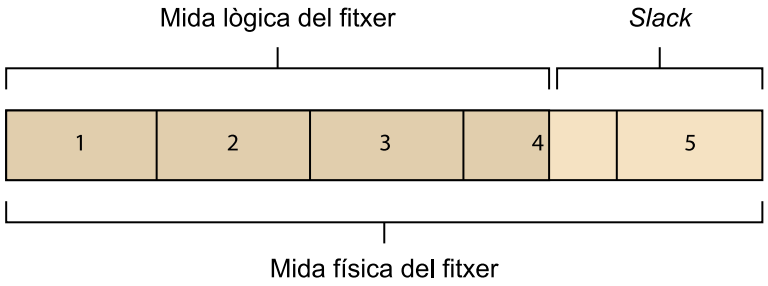
- **Dades ocultes mitjançant esteganografia**. A diferència de la criptografia, l'esteganografia amaga les dades entre altres tipus de dades (per exemple, un fitxer de text dins d'una fotografia). Així, el fitxer que conté la fotografia és lògicament accessible, però la seva visualització no ens permet ni tan sols intuir que conté un missatge ocult.

- **Arxius que s'han eliminat** i encara no s'han sobreescrit.

- **Dades localitzades en *ambient data***. Es denominen així les dades que apareixen en localitzacions que no són visibles directament i que requereixen un programari específic per a recuperar-les o visualitzar-les. Per exemple:
  - Espai desaprofitat: tal com ja hem definit, es denomina així l'espai que hi ha entre el final lògic d'un fitxer i el final físic.
  - *Unallocated cluster*[10]: clúster que, encara que no estigui associat a cap fitxer en concret, sovint pot contenir informació de caràcter residual (per exemple, parts d'un document de text que ja ha estat eliminat del disc dur o una versió antiga d'un fitxer ja existent, etc.).

(10)Un clúster és la unitat mínima d'assignació en un disc dur i pot contenir diversos sectors.

Figura 9. Representació gràfica de l'espai desaprofitat d'un arxiu



Els *unallocated clusters* i l'espai desaprofitat

Tant els denominats *unallocated clusters* com l'espai desaprofitat són susceptibles de contenir informació residual, procedent de fragments d'antics arxius. A més, l'espai desaprofitat és una ubicació excel·lent per a emmagatzemar informació deliberadament oculta. Si es troben proves en un espai desaprofitat, se n'ha d'extreure el fitxer atenent al límit físic o, en cas contrari, perdrem la informació en el procés d'extracció. Si les dades rellevants apareixen en els *unallocated clusters*, clarament no estan assignats a cap fitxer accessible; no obstant això, les eines d'anàlisi ens permeten situar les dades en un sector físic determinat del disc dur (aquesta dada és important, ja que ens permetrà situar la prova en el suport digital com si es tractés d'una ruta en el sistema de fitxers).

7.1. *Write blockers*

De vegades, caldrà manipular el disc dur original connectant-lo directament a l'ordinador d'anàlisi. Hi ha solucions, tant de programari com de maquinari, que permeten filtrar les peticions d'escriptura sobre el disc dur, de manera que l'examen del suport no alteri la prova[11].

[11]Aquests tipus de dispositius poden ser de molta utilitat per a fer tasques de preanàlisi i d'adquisició lògica de l'evidència *in situ*, sense alterar-la.

Tal com podem veure a les imatges, el disc dur es col·locaria en la connexió de la targeta i, mitjançant un cable USB, el dispositiu *write blocker* es connectaria a l'ordinador d'anàlisi (és a dir, entre l'ordinador i el disc dur) i filtraria qualsevol petició d'escriptura sobre el disc dur.

Figura 10. Dispositiu *write blocker* (FastBloc3, de Guidance Software)

Figura 11. *Write blocker* (FastBloc 3, de Guidance Software) amb el cable USB de connexió a l'ordinador d'anàlisi

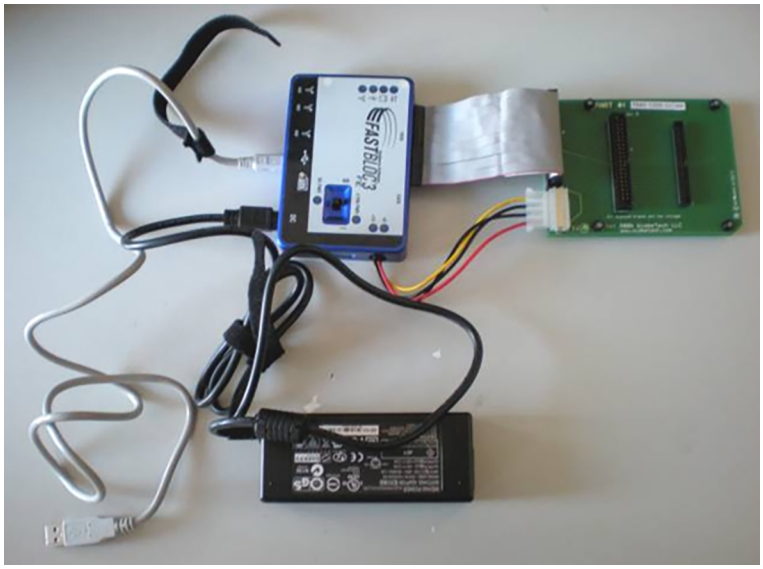


Figura 12. Maletí de targetes del dispositiu FastBloc

En definitiva, aquests dispositius poden ser de gran utilitat en els casos següents:

- Realització de preanàlisis urgents, en les quals no es disposa del temps necessari per a dur a terme una clonació i l'anàlisi posterior al laboratori.

- Adquisició de dades no invasiva en un entorn de sistema operatiu: mitjançant aquests dispositius, també es poden adquirir les dades dels suports sencers examinats o d'una part (per exemple, els que es consideren rellevants després de la preanàlisi efectuada).

7.2. Eines d'anàlisi informàtica: Encase, Autopsy, distribucions de Linux

Algunes de les eines ja esmentades, com Encase, permeten gestionar totes les fases de l'anàlisi forense, des de l'adquisició dels suports originals i l'anàlisi, fins a la generació automàtica de l'informe final. Moltes d'aquestes eines es basen en codi propietari i, malgrat oferir moltes garanties i ser molt amigables, de vegades és preferible la flexibilitat que ens permeten les aplicacions basades en codi obert (*open source*). Potser una de les eines més conegudes és la distribució de Linux CAINE (o, entre d'altres, SIFT, CAINE, DEFT, Kali, etc.). Aquest tipus de distribucions s'executen, directament, des d'un DVD o USB i inclouen un gran nombre d'eines al voltant del món de la seguretat informàtica. Una altra eina, amb una interfície a l'estil de l'Encase, però *open source*, és Autopsy.

No hi ha cap aplicació que pugui arribar a tots els aspectes d'una anàlisi forense. Normalment, les aplicacions que siguin més generals i amb interfícies amigables, seran de molta utilitat per a un percentatge de casos elevat; no obstant això, en determinades operacions (per exemple, en la recuperació d'arxius eliminats o altres de molt específiques) poden ser menys eficaces que les aplicacions dissenyades específicament per a una finalitat concreta. Altres vegades, com per exemple la gestió dels arxius criptogràfics, sempre s'haurà de recórrer a programes específics o dissenyats pel mateix analista. En definitiva, els laboratoris d'informàtica forense han de disposar necessàriament d'una gran varietat d'aplicacions, generals i específiques, de codi obert i propietari, adequades a diferents tipus de sistemes operatius i als sistemes respectius de fitxers.

Les extraccions de memòria RAM es poden efectuar amb l'eina Volatility, un entorn de treball de codi obert per a l'anàlisi forense, escrit en Python i compatible amb Microsoft Windows, OS X i Linux.

7.3. Virtualització i anàlisi en viu

Sovint, els analistes només disposen dels clons o de les imatges forenses que s'han d'analitzar i no tenen accés als ordinadors que allotjaven els continguts originals. Així doncs, de vegades, malgrat tenir accés lògic als fitxers del suport que hem d'analitzar, no en podrem examinar el contingut perquè aquests fitxers tenen un format propi, només accessible des de l'aplicació que els ha generat. En lloc d'adquirir l'aplicació específica, es pot intentar executar el sistema que hem d'analitzar per mitjà d'una màquina virtual.

Aquesta tècnica també ens pot ser molt útil, per exemple, per a analitzar un disc dur que conté algun troià. L'execució del sistema mitjançant una màquina virtual ens podria permetre, per exemple, esbrinar quin tipus d'accions du a terme el troià i a quines adreces IP envia la informació de l'ordinador local.

Per exemple, per a executar un clon, podem emprar eines com WMware o VirtualBox. Per a executar imatges forenses, podem emprar, per exemple, Live View.

7.4. Procediment general d'anàlisi

Una vegada rebem els dispositius que s'han d'analitzar, en primer lloc (i prèviament a qualsevol tasca d'anàlisi), serà necessari comprovar la correcció de les dades que figuren a la cadena de custòdia de les evidències susceptibles de ser analitzades.

Pel que fa a l'anàlisi en si mateixa, i malgrat que existeixen molts mètodes possibles i igualment vàlids, es podria tenir en compte el procediment que es detalla tot seguit.

1) Recuperació dels arxius esborrats

Consisteix en realitzar una recuperació parcial o total de la informació eliminada existent en els dispositius susceptibles de ser analitzats. Aquesta operació inclou les dades localitzades a les àrees sense assignar del disc dur, així com una recuperació de les dades d'arxius i directoris «orfes», la vinculació dels quals s'ha perdut. Aquest mètode de recuperació pot incloure procediments de recuperació d'arxius basats en *carving*.

2) Estudi del sistema operatiu

Pel que fa a l'estudi del sistema operatiu, des d'un punt de vista molt bàsic, es podrien efectuar les comprovacions següents:

- Identificació del sistema operatiu de l'equip i localització de la partició que allotja el sistema.
- Identificació de la data d'instal·lació del sistema.
- Identificació dels diferents usuaris definits al sistema.
- Última data d'accés a l'equip (per a cadascun dels usuaris).
- Identificació dels dispositius de maquinari i programari reconeguts pel sistema.

3) Estudi de la seguretat

En aquesta etapa, l'objectiu consistirà a estudiar si les evidències analitzades han estat compromeses (o fins i tot afegides deliberadament amb la finalitat de perjudicar una persona). En definitiva, s'haurà d'identificar qualsevol programari maliciós (virus, troià, etc.), avaluar el dany patit, identificar els arxius que han estat compromesos (eliminats, modificats, etc.), així com determinar la via d'accés al sistema.

4) Anàlisi detallada de les evidències digitals

Sense voler ser massa exhaustius, l'anàlisi detallada de les evidències podria incloure els apartat següents, alguns dels quals ja han estat tractats en apartats anteriors. Cada analista haurà de decidir, segons el cas, aquelles proves que ha de practicar necessàriament i aquelles que, potser, no siguin rellevants.

- Informació relativa al sistema analitzat: maquinari instal·lat i reconegut pel sistema operatiu, data, hora i usuari que va emprar el sistema per darrera vegada, data d'instal·lació.

- Estudi dels dispositius físics que en algun moment varen poder ser connectats al sistema analitzat: mòbils, USB, impressores, escàners, càmeres, targetes de memòria, etc.

- Estudi de l'escriptori i de la paperera de reciclatge.

- Connexions de xarxa, identificació de la MAC i adreces IP.

- Estudi del registre del sistema i logs d'auditoria del sistema operatiu i de les aplicacions instal·lades (si es disposa de logs).

- Estudi de la informació continguda en els *unallocated clusters* o en l'espai desaprofitat.

- Informació continguda en els arxius d'hibernació, paginació, particions i arxius d'intercanvi (*swap*).

- Anàlisi de la cua d'impressió.

- Visualització dels enllaços dels arxius i dels arxius als quals s'ha accedit recentment.

- Estudi dels directoris d'usuari.

- Estudi de les aplicacions instal·lades relacionades amb activitats de programació, gravació i tractament d'imatges, processament d'àudio i vídeo, programaris de comptabilitat, ofimàtica, etc.

- Estudi de les metadades dels arxius, si es considera que poden ésser rellevants per al cas.

- Estudi de les aplicacions de virtualització.

- Estudi de les bases de dades instal·lades i de les aplicacions que en permeten la gestió.

- Estudi dels programaris de xifratge, particions xifrades, etc.
- Estudi de la navegació per Internet, dels històrics i de les galetes.
- Anàlisi dels clients de correu electrònic i del correu web (suposant que l'analista disposi de l'autorització necessària).
- Anàlisi dels registres de missatgeria instantània, xats i contactes.

Algunes d'aquestes operacions poden ser difícils de dur a terme si no es disposa de l'ordinador original o de les aplicacions gestores de les dades (per exemple, programaris de gravació de vídeo, de comptabilitat, etc.). Cal tenir present que és possible que al laboratori només ens arribin els discs durs a analitzar, però no els ordinadors que els contenien.

7.5. Anàlisi i investigació

7.5.1. El marc legal

No solament els aspectes tècnics són rellevants en tot procés d'anàlisi informàtica. També cal tenir molt en compte que no tot allò que és tècnicament possible és legal. Suposem, per exemple, que en una empresa se sospita que un treballador envia i rep molts correus electrònics relacionats amb temes d'oci personal, que a més ocupen un volum de disc dur considerable. Tècnicament, el més senzill seria examinar els continguts del correu electrònic del treballador; no obstant això, tal com ja ens podem imaginar, estaríem incorrent en un delicte de greus conseqüències, inimaginables tenint en compte la senzillesa tècnica amb la qual un administrador del sistema podria efectuar aquestes comprovacions. De la mateixa manera, hi ha altres problemes, ja no tan evidents, que poden arribar a tenir conseqüències desastroses. Com en el cas que ens ocupa, sovint haurem d'investigar els fets mitjançant tècniques indirectes (constatant, per exemple, un consum desproporcionat d'amplada de banda).

Per tant, encara que no és l'objectiu d'aquest mòdul, sempre hem de tenir en compte el marc legal que ens limita i que, sovint, l'important no és obtenir una prova, sinó aconseguir presentar-la com a prova en un judici.

7.5.2. Anàlisi de correus electrònics

L'anàlisi de correus electrònics és un dels temes d'investigació més recurrents. La nostra intenció no és explicar com fer una investigació de les capçaleres d'un correu electrònic per a descobrir l'adreça IP d'origen, sinó més aviat descriure els problemes que comporta la seva anàlisi des del punt de vista legal.

L'obertura dels correus electrònics no oberts s'ha de fer algunes vegades davant del jutge. Això és perquè, en el marc legal, s'ha assimilat el correu postal al correu electrònic. Des del punt de vista estrictament tècnic, les diferències entre tots dos són apreciables i, en tot cas, el correu electrònic més aviat s'hauria d'assimilar a una postal (és a dir, a una carta sense sobre, amb les dades i el remitent a la vista). L'obertura dels correus davant del jutge comporta innombrables problemes:

- Hi pot haver un gran nombre de correus, potser milers, pendents d'obrir.
- L'obertura es du a terme en un ordinador d'anàlisi, preferentment portàtil, aportat pel perit. Atesa la gran diversitat de programes client de correu electrònic, és possible que l'obertura no sigui una tasca gens fàcil, especialment si no s'ha pogut preparar per endavant.
- Tècnicament, és molt difícil determinar si un correu ha estat obert o no.

Esment a part mereixen els correus electrònics de correu web (*webmail*). En aquest cas, els correus apareixen, residualment, en els directoris temporals d'Internet, d'on es podran recuperar amb relativa facilitat (l'usuari desconeix l'existència d'aquests documents, ja que s'emmagatzemen involuntàriament en els directoris temporals). A diferència dels anteriors, en aquest cas no hi ha cap dubte que l'usuari ha obert prèviament els correus, i analitzar-los, probablement, no hauria de comportar cap problema (no hem d'oblidar que el jutge serà qui decideixi, finalment, si l'obertura, malgrat tractar-se de correus web, es farà en la seva presència o no).

Correu

Per exemple, els indicadors de seguiment que determinen en els programes client si el correu ha estat obert o no, poden ser modificats fàcilment per l'usuari.

7.5.3. Els fitxers de registre i la investigació dels delictes informàtics

La investigació dels delictes informàtics es realitza, com ens podem imaginar, mitjançant l'estudi de les adreces IP involucrades en el presumpte delicte. L'adreça IP té consideració de dada personal i, per tant, els proveïdors de serveis d'Internet no podran efectuar la cessió d'aquestes dades sinó és mitjançant un manament judicial.

A fi i efecte de no impossibilitar la investigació dels delictes, **la llei de conservació de dades** determinarà l'obligatorietat que els proveïdors hagin de conservar els logs o fitxers de registre (article 4), així com la durada d'aquest període de conservació (article 5), que, com podem veure, es pot modular en funció de l'interès de la investigació.

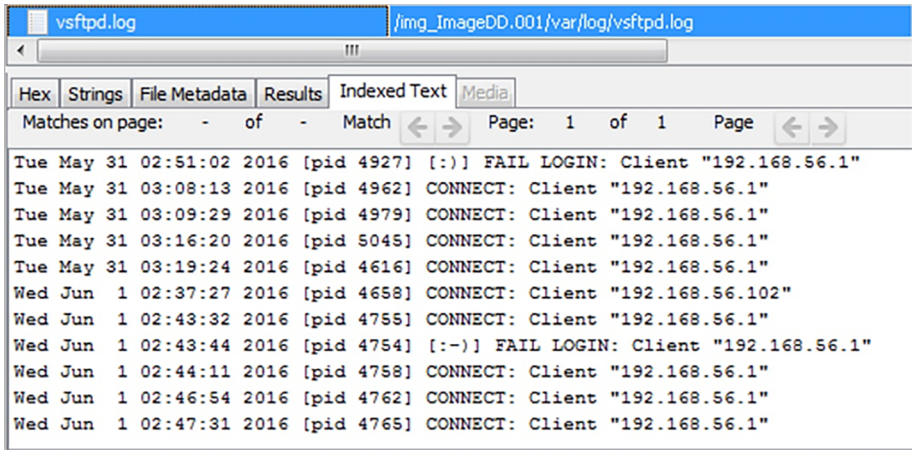
Article 5. Període de conservació de les dades.

1. L'obligació de conservació de dades imposada **cessa al cap de dotze mesos** a comptar des de la data en què s'hagi produït la comunicació. Per reglament, amb la consulta prèvia als operadors, es pot ampliar o reduir el termini

de conservació per a determinades dades o una categoria de dades **fins a un màxim de dos anys o un mínim de sis mesos**, tenint en compte el cost de l'emmagatzematge i la conservació de les dades, així com el seu interès per als fins d'investigació, detecció i enjudiciament d'un delicte greu, amb la consulta prèvia als operadors.

Tot seguit, podem veure un exemple de fitxer de registre (vsftpd.log), extret dels materials *Com s'ha de fer l'informe pericial d'un delicte informàtic?* «Col·lecció H2PAC» de la UOC:

Figura 13. Fitxer de registre del servei FTP



En aquesta captura de pantalla podem observar com, poc abans que es produïssin els fets investigats (aquesta dada l'obtindríem a partir de la feina feta pels investigadors del cas), es produeix una connexió amb èxit des de l'adreça IP 192.168.56.1 (una adreça local). Si s'examinés el fitxer de registre sencer, es veuria que s'han produït diversos intents d'accés, amb èxit i sense, en dates i hores properes als fets investigats. Val a dir que les adreces IP implicades en aquests tipus d'activitats es poden trobar en llocs geogràficament llunyans, en països estrangers, per la qual cosa la persecució del delicte (que sempre requerirà diversos manaments judicials per a poder esbrinar el camí fins al titular del telèfon) pot ser molt difícil, i fins i tot pot resultar impossible de traçar fins a l'origen. Notem, però, que sense les adreces IP, molts delictes informàtics no es podrien investigar.

8. Presentació i informe

En l'informe elaborat per l'expert es presentaran les proves relacionades amb el cas, les conclusions i també la justificació del procediment emprat. Sovint, aquest informe es ratificarà en presència del jutge, encara que sovint els peritatges aniran destinats a empreses. No obstant això, en tots dos casos no és necessari que el lector de l'informe tingui el bagatge tècnic suficient per a comprendre una anàlisi forense en profunditat. Per tant, en general no s'ha d'emprar el llenguatge tècnic de manera abusiva i, sempre que sigui necessari utilitzar-lo, convindrà posar notes aclaridores a peu de pàgina i, fins i tot, en forma d'annexos i glossaris. Atès que molts d'aquests informes s'han de presentar davant d'un tribunal, l'analista ha de tenir en compte que, a més d'aplicar el rigor tècnic, ha de ser prou hàbil per a comunicar-ne el resultat de l'anàlisi de manera concisa i clara.

Informes pericials

Podeu trobar més informació sobre el contingut i l'estructura dels informes pericials al mòdul «El peritatge. L'anàlisi forense i el sistema legal» d'aquesta assignatura.

9. El laboratori d'informàtica forense

Una de les aspiracions de qualsevol laboratori d'informàtica forense consisteix a obtenir algun tipus de certificació que n'avali la qualitat i la correcció pel que fa a la normativa vigent. Organitzacions com l'ENFSI promouen l'acreditació de tots els laboratoris oficials de criminalística que pertanyen als països adscrits. En concret, l'ENFSI promou l'adequació de tots els laboratoris oficials a la norma ISO/IEC 17025 de Requisits generals per a la competència de laboratoris d'assaig i calibratge. Notem, però, que aquesta norma no està específicament pensada per a laboratoris de criminalística (entre els quals hi ha els laboratoris d'informàtica forense).

La implantació d'aquesta norma a assajos tan dispars i allunyats dels propòsits inicials de la norma ISO/IEC 17025, com són l'estudi de projeccions de taques de sang o la clonació de discos durs, és una tasca complexa i amb molts buits que cal interpretar, per tal d'adaptar l'operativitat del laboratori al contingut de la norma. A diferència d'altres normes, la norma ISO/IEC 17025 no es pot certificar, sinó que només és susceptible de ser acreditada. En termes generals, i per no incidir excessivament en una qüestió tan aliena a l'objectiu d'aquest curs, l'acreditació abasta assajos concrets de cada laboratori (per exemple, «identificació i quantificació de cocaïna») i no té un abast tan «horitzontal» com les certificacions (que poden abastar l'activitat sencera d'una organització). Això no vol dir que les activitats d'un laboratori que es troben fora de l'abast es realitzin sense cap garantia, ja que els assajos sota la norma ISO/IEC 17025 poden coexistir amb altres normes o certificacions que assegurin que el laboratori sencer treballa correctament en termes de qualitat.

A més de l'acreditació sota la norma ISO/IEC 17025, també hi ha altres normes i manuals de bones pràctiques que el laboratori pot emprar per a definir els seus procediments interns de treball. De fet, el ventall de possibilitats és tan enorme que és causa d'una gran confusió entre tots els actors implicats; no obstant això, el camí cap a la normalització és una cosa que, en la nostra opinió, és inevitable i que marcarà el futur dels que decideixin fer d'aquesta feina la seva professió.

Al nostre entendre, qualsevol procés de certificació es basa en els quatre pilars següents:

Pilars del procés de certificació

- Normalització de les instal·lacions.
- Obtenció dels mitjans materials.
- Normalització dels procediments de treball.
- Formació certificada dels analistes.

Els mitjans materials necessaris i les metodologies de treball ja s'han estudiat en apartats anteriors, i la normalització de les instal·lacions segurament excediria el propòsit d'aquests materials. No obstant això, creiem que és necessari aportar alguna informació quant a la certificació professional.

9.1. Formació certificada dels analistes forenses

En primer lloc, cal assenyalar que moltes eines forenses disposen de les seves pròpies certificacions, la qual cosa ja ens pot orientar sobre la formació que ens interessa. També hi ha altres certificacions de caràcter generalista que poden ser d'interès per a iniciar-se en la matèria o per a acreditar els coneixements de l'analista. Quant a les universitats, atès el caràcter recent i multidisplicinari d'aquesta matèria, la informàtica forense encara no apareix reflectida en la majoria de plans d'estudi.

D'entre l'al·luvió de certificacions i cursos forenses, creiem oportú destacar les certificacions[12] següents (és molt interessant completar-les amb altres certificacions més relacionades amb la seguretat informàtica):

(12)Algunes de les certificacions tenen data de caducitat i requereixen noves proves per a mantenir la validesa de la certificació. Moltes ofereixen certificació a diferents nivells d'experiència.

- Computer Hacking Forensic Investigator Certification (CHFI): Certificació professional proporcionada per l'International Council of E-Commerce Consultants (EC-Council).

- Guidance Software (EnCe): La certificació EnCase Certified Examiner (EnCE) reconeix el domini de les metodologies pròpies de la informàtica forense emprant el programari Encase.

- IACIS Certified Forensic Computer Examiner (CFCE). IACIS (International Association of Computer Investigative Specialists) és una corporació sense ànim de lucre, formada per professionals policials, dedicats a la formació en el camp de la informàtica forense. Són als Estats Units.

- Certified Computer Examiner (CCE). Certificació oferta per la ISCFE (International Society of Computer Forensic Examiners) i dirigida tant al sector policial com al privat.

- SANS Certifications. El SANS (SysAdmin, Audit, Network and Security Institute), creat el 1989, ofereix multitud de certificacions i certificats, basats

en la superació de cursos de cinc o sis dies i un o dos dies (respectivament).

El seu àmbit d'actuació és enorme i una opció que s'ha de tenir en compte.

Resum

En aquest mòdul hem estudiat les diferents etapes que conformen una anàlisi forense. Aquests materials no busquen constituir-se en un compendi de fórmules per a gestionar qualsevol tipus d'anàlisi, sinó oferir una imatge molt generalista de la matèria, en la qual s'ha procurat dibuixar una part important de tot el ventall de possibilitats que ofereix aquesta ciència multidisciplinària, de recent creació.

A més de les tècniques i dels procediments associats a les etapes de l'anàlisi forense, s'han presentat algunes qüestions d'àmbit normatiu, essencials per a entendre com s'investiguen els delictes informàtics. En aquest sentit, és essencial comprendre que cal manipular amb molta cura les evidències digitals perquè puguin tenir validesa en un procediment judicial. De la mateixa manera, és important entendre que no tot allò que és tècnicament possible es troba conforme a la llei (per exemple, com a perits, podem obrir un correu electrònic, però si no en tenim l'autorització, és possible que la nostra acció no només invalidi la prova, sinó que fins i tot podria tenir responsabilitats penals).

Activitats

1. El càlcul del valor *hash* d'un fitxer es pot dur a terme en línia: http://onlinemd5.com/

Observació

Si l'enllaç anterior no funcionés, pots trobar a la xarxa altres llocs web amb funcionalitats similars.

Respon les preguntes següents:

a) Crea un fitxer amb el processador de textos que habitualment facis servir i escriu una frase qualsevol. Desa'l i calcula el valor *hash* MD5 en línia. Anota o copia el valor obtingut.

b) Torna a obrir novament el fitxer que has creat anteriorment, afegeix qualsevol text al fitxer i torna'l a desar. Calcula el valor *hash* del fitxer i compara'l amb l'anterior[13].

[13] Podeu usar el Fòrum de l'assignatura per a comentar aquestes activitats.

c) Són iguals tots dos valors? Si són diferents, quina creus que és l'explicació? En relació a les propietats d'integritat, confidencialitat i disponibilitat, quina creus que pot tenir alguna relació amb les funcions *hash*? (si no saps a què es refereixen aquestes propietats, pots cercar més informació a Internet).

2. Cerca a Internet informació sobre l'anomenat Machine Identification Code (*yellow dots, tracking dots* o *secret dots*), en relació a les impressores làser. Quin valor forense creus que tenen aquests punts? Quina relació tenen amb l'esteganografia?

3. Quina relació hi ha entre la gestió d'incidents de seguretat i la informàtica forense?

Exercicis d'autoavaluació

1. Quin és l'ordre lògic de les fases d'una anàlisi forense?

a) Adquisició, identificació, assegurament de l'escena, anàlisi i presentació.
b) Identificació, anàlisi, adquisició, assegurament de l'escena i presentació.
c) Assegurament de l'escena, adquisició, identificació, presentació i anàlisi.
d) Assegurament de l'escena, identificació, adquisició, anàlisi i presentació.

2. Es coneix amb el nom d'esteganografia:

a) Una tècnica de detecció i correcció d'errades d'integritat en sistemes de fitxers.
b) Un conjunt d'eines per a l'adquisició i anàlisi de memòria RAM.
c) Un *hash* avançat de 512 bits o més.
d) Una tècnica d'ocultació de la informació.

3. Enllaça cada definició amb el terme adequat:

Obtenir el clon d'un disc dur.	Assegurar l'escena
Trobar tots els documents ofimàtics relacionats amb la investigació d'un cas.	Identificar i recollir l'evidència
Restringir l'accés a l'escena del succés.	Adquirir l'evidència
Elaborar les conclusions d'una anàlisi forense.	Analitzar l'evidència
Decidir si es recullen o no uns dispositius USB trobats en un calaix de l'escena del succés.	Presentació i informe

4. A què es refereix el principi de Locard?

a) A que tot procés portat a terme, que no sigui repetible per un tercer perit, no tindrà validesa en un procediment legal.
b) És un conjunt de principis bàsics que cal tenir en compte en la fase d'adquisició d'evidències.

c) Ens diu que les evidències digitals són fàcilment alterables.
d) Quan dos objectes entren en contacte es produeix una transferència de material.

5. L'evidència digital pot ser...

a) Física i volàtil.
b) No volàtil.
c) Volàtil i no volàtil.
d) Volàtil.

6. Una funció *hash* és...

a) Una tècnica que ens permet identificar tots aquells fitxers que visualment presenten el mateix contingut.
b) Una funció matemàtica que genera un identificador resumit a partir d'unes dades d'entrada.
c) Una tècnica emprada per a generar clons d'una evidència forense.
d) Una funció matemàtica immune al problema de les col·lisions.

Solucionari

Exercicis d'autoavaluació

1. d

2. d

3.

Restringir l'accés a l'escena del succés.	Assegurar l'escena
Decidir si es recullen o no uns dispositius USB trobats en un calaix de l'escena del succés.	Identificar i recollir l'evidència
Obtenir el clon d'un disc dur.	Adquirir l'evidència
Trobar tots els documents ofimàtics relacionats amb la investigació d'un cas.	Analitzar l'evidència
Elaborar les conclusions d'una anàlisi forense.	Presentació i informe

4. d

5. c

6. b

Glossari

ambient data *n* Dades que apareixen en localitzacions que no són directament visibles i que requereixen un programari específic per a ser recuperades o visualitzades.

anàlisi forense informàtica *f* Procés resultant d'aplicar mètodes científics als sistemes informàtics amb la finalitat d'assegurar, identificar, preservar, analitzar i presentar la prova digital, de manera que aquesta sigui acceptada en un procés judicial.

clon *m* Còpia de bits del suport original. Per tant, ha de contenir, igual que l'original, els arxius ocults, els eliminats i no sobreescrits, el denominat espai desaprofitat, etc.

clúster *m* Unitat mínima d'assignació d'un disc dur. Un clúster pot contenir diversos sectors, segons el sistema de fitxers.

esteganografia *f* Conjunt de tècniques que permeten l'ocultació de qualsevol tipus de dades. A diferència de la criptografia, l'esteganografia amaga les dades entre un altre tipus de dades, però no les modifica perquè no siguin llegibles.

***file slack* o espai desaprofitat** *n* Espai entre el final lògic i el final físic d'un fitxer.

hash *n* Funció matemàtica unidireccional que resumeix un missatge de grandària variable (per exemple, un arxiu) en una representació de grandària fixa. És poc probable que dos fitxers diferents tinguin la mateixa representació *hash*, la qual cosa significa que aquest valor es pot utilitzar per a comprovar la integritat d'un arxiu (o d'un sistema sencer). Les funcions *hash* més conegudes són MD5 i SHA-1.

log o fitxer de registre *n* Un log o fitxer de registre és l'enregistrament seqüencial en un fitxer o en una base de dades de tots els esdeveniments o accions que afecten un procés particular (una aplicació, l'activitat d'una xarxa informàtica, etc.). El contingut d'aquests fitxers és molt important per a la investigació dels delictes informàtics.

logging *n* Procediment mitjançant el qual es registren, en un fitxer, les activitats que s'esdevenen en un sistema operatiu o en una aplicació. Aquest fitxer, denominat genèricament log, emmagatzema les traces de tot el que ha succeït en el sistema (per exemple, un atac de què hagi pogut ser objecte).

mac-time *n* Temps de modificació (*m*) i accés (*a*) d'arxius, i modificació de metadades (*c*) dels arxius.

marca horària *f* Vegeu *timestamp*.

prova *f* Element que proporciona informació que condueixi a alguna conclusió o troballa relacionada amb el fet que s'investiga.

prova digital *f* Prova emmagatzemada en suports digitals.

prova volàtil *f* Prova que desapareix en absència d'alimentació elèctrica.

timeline *n* Presentació dels *mac-time* en ordre temporal.

timestamp *n* Seqüència de caràcters que denota la data i/o hora en què s'ha produït un esdeveniment determinat.

unallocated cluster *n* Clúster que, malgrat no estar assignat a cap fitxer en concret, pot contenir informació, sovint de caràcter residual.

Bibliografia

AENOR (norma UNE) (2013). UNE 71505-1:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.

AENOR (norma UNE) (2013). UNE 71505-2:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.

AENOR (norma UNE) (2013). UNE 71505-3:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.

AENOR (norma UNE) (2013). UNE 71506:2013 Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.

AENOR (norma UNE) (2015). UNE 197010:2015. Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).

Arqués, J. M.; Colobran, M.; Iparraguirre, J. (2016). *Com s'ha de fer l'informe pericial d'un delicte informàtic?* «Col·lecció H2PAC». Editorial UOC. ISBN: 978-84-9116-584-2, 2016.

Arqués, J. M.; Guasch, A.; Serra, J. (2016). «La cadena de custòdia de les evidències digitals». A: *La ciberseguretat a Catalunya. Informe de l'Observatori del Risc* (pàg. 99-115). Institut d'Estudis de la Seguretat (IDES). ISBN: 978-84-617-7162-2.

Arqués Soldevila, J. M.; Colobran Huguet, M.; Guasch Petit, A. (2009). *Anàlisi forense de sistemes d'informació*. Barcelona: FUOC.

Blanquez, M. (2019). *Validació d'eines d'anàlisi forense digital sota la norma ISO/IEC 17025*. Treball Final de Màster MISTIC-UOC.

Colobran, M.; Morón, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC.

Ćosić, J.; Bača, M. (2010). A Framework to (Im)Prove «Chain of Custody» in Digital Investigation Process. Proceedings of the 21st Central European Conference on Information and Intelligent Systems. Faculty of Organization and Informatics. September 22-24 2010 (pàg. 435-438). Croàcia: Varaždin.

Cruz Allende, D. (2007). *Análisis forense de sistemas de información*. Barcelona: FUOC.

European Network of Forensic Science Institutes (ENFSI) (2015). *Best Practice Manual for the Forensic Examination of Digital Technology*. <http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf>

International Organization for Standardization/International Electrotechnical Commission (2012). ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.

Marqués-Arpa, T.; Serra-Ruiz, J. (2014). Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital. Reunión Española de Criptografía y Seguridad de la Información. Alicante.

NIST Special Publication 800-101 Revision 1, Rick Ayers, Sam Brothers, Wayne Jansen (2014). Guidelines on Mobile Device Forensics. <http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf>