Eines de "carving" i de "wiping"

Carving

Quan s'elimina un fitxer (amb *rm* o similar), en realitat no s'elimina "físicament" dels sectors de disc que ocupava sinó qui simplement s'elimina la seva referència en un índex gestionat pel sistema de fitxers (anomenat "taula d'inodes" en els natius de Linux o "MFT" en els de Windows), índex que és utilitzat precisament per saber la ubicació en disc de tots els fitxers reconeguts (a més d'allotjar les seves metadades relacionades, com ara permisos, propietari, mida, nom, dates de modificació-accés-canvi-creació, etc). És a dir, que en una eliminació estàndard el contingut en sí dels fitxers no s'esborra sinó només la referència de la seva existència (això és com si, per exemple, en una biblioteca, no traguéssim un llibre del prestatge però esborréssim la seva referència de la base de dades del bibliotecari...el llibre continuaria existint però ningú en sabria res de la seva existència i constaria com que al seu lloc no hi ha cap llibre).

> NOTA: Els directoris també són elements que es troben referenciats a la taula d'inodes (o MFT, segons el sistema). En el seu cas, les metadades que contenen son simplement el nom i el nombre identificador dels inodes (fitxers o subcarpetes) que hi són a dins

Això permet que, sense haver d'esborrar físicament aquests sectors prèviament (tasca que computacionalment és molt costosa i lenta), els sectors ocupats constin de nou com a "lliures" i es puguin sobreescriure amb contingut nou. I el que és més important per nosaltres: una conseqüència interessant d'aquest comportament és que, mentre no s'efectui cap sobreescriptura, serà possible recuperar el contingut d'aquests sectors "orfes" (és a dir, recuperar certs fitxers eliminats).

> NOTA: El reformatament d'una partició és un procés similar a l'eliminació de fitxers en el sentit que l'únic que fa és buidar de contingut la taula d'inodes (o MFT) però deixant els sectors sense tocar el seu contingut. Així doncs, una partició reformatada també seria susceptible de tenir dades antigues recuperables

La tècnica de recuperació de fitxers eliminats més comuna és l'anomenada "data carving". Aquesta tècnica consisteix en recórrer els sectors del disc en busca d'estructures (marcadors de seqüència, capçaleres binàries...), que identifiquen determinats tipus formats de fitxers (com JPG, PDF, AVI, DOCX, etc). La idea és obtenir el contingut de determinats fitxers cercant en el flux continu de bytes certs patrons específics reconeixibles per tal de detectar-los i extreure'l a partir del seu inici i l'estimació (o càlcul) del seu final.

> NOTA: Quant menys fragmentat estigui el sistema de fitxers (és a dir, en quants menys sectors disseminats pel disc estigui repartit el contingut de cada fitxer), més èxit tindrà el "data carving" ja que serà més fàcil trobar i ensamblar els diferents trossos que formen un determinat fitxer

---

Una eina molt habitual per fer tasques de "data carving" (sempre que el sistema de fitxers sigui FAT, exFAT, NTFS, ExtX o HFS+) és **Photorec** (https://www.cgsecurity.org/wiki/PhotoRec_ES). Tant a Fedora com a Ubuntu aquesta eina es troba disponible a través del paquet anomenat "testdisk" (que inclou altres comandes, que de seguida veurem també). Un cop instal·lada, el seu ús és tan senzill com fer:

> *sudo photorec imatgeDiskOimatgeParticioOimatgeE01Odispositiu*

> NOTA: La llista de formats de fitxers reconeguts per Photorec és aquesta:
> https://www.cgsecurity.org/wiki/Formatos_De_Archivos_Recuperados_Por_PhotoRec

A partir d'aquí, apareixerà una pantalla interactiva que ens preguntarà tot un seguit de coses:

*Confirmació del dispositiu/imatge on es començarà a buscar
*Confirmació de la partició (d'entre les reconegudes dins del disc anterior) on es començarà a buscar
*Després de pulsar l'opció "Search", confirmació del sistema de fitxers de la partició triada
*Tria entre si es vol fer el "carving" només en els sectors buits de la partició o bé en tota ella
*Confirmació (amb "C") de la carpeta destí on es guardaran tots els fitxers trobats i recuperats (dins d'una subcarpeta anomenada "recup_dir.*nº*")

NOTA: A la pantalla de confirmació de partició (la 2ª), es pot triar, sota l'opció "File Opt", els formats concrets de fitxers que es voldran recuperar. També està l'opció "Options" que permet modificar el comportament de Photorec a l'hora de realitzar la seva feina amb la configuració de diverses opcions, però no les tindrem en compte.

Una altra eina molt habitual per fer "data carving" sobre imatges de disc, punts de muntatge o directament dispositius fisics és **Bulk Extractor** (https://github.com/simsong/bulk_extractor). Aquest programa recorre tots els bytes des de l'origen fins el final de la imatge/dispositiu (obviant qualsevol tipus de sistema de fitxers) per buscar elements que coincideixin amb una llista de paraules o expressions regulars determinada. És, per tant, una eina molt adient per buscar adreces de correu, nombres de tarjetes de crèdit, URLs, signatures de malware, etc. Desgraciadament, no està disponible encara als repositoris oficials de les distribucions genèriques més importants, així que caldrà afegir-hi un repositori específic per poder descarregar-la i instal·lar-la. Concretament:

*A Fedora: *wget https://forensics.cert.org/cert-forensics-tools-release-36.rpm*
sudo rpm -Uvh cert-forensics-tools-release-38.rpm && sudo dnf install bulk_extractor
*A Ubuntu: *sudo add-apt-repository ppa:gift/stable*
sudo apt update && sudo apt install bulk-extractor

NOTA: Una altra opció per Ubuntu seria utilitzar el repositori de la distribució Kali, compatible amb distribucions de la família de Debian. Per més informació sobre els detalls es pot consultar https://miloserdov.org/?p=3609 però bàsicament els passos consistirien en executar les següents comandes:

wget https://archive.kali.org/archive-key.asc
sudo apt-key add archive-key.asc
echo "deb https://http.kali.org/kali kali-rolling main contrib non-free" | sudo tee /etc/apt/sources.list.d/kali.list
sudo apt update && sudo apt install bulk_extractor

A partir d'aquí, la manera bàsica d'utilitzar-la d'alguna de les següents dues formes, segons tinguem com a font de dades una image/dispositiu o bé una carpeta (en aquest darrer cas és on cal afegir el paràmetre *–R* per repassar-la recursivament), ...

bulk_extractor -o /ruta/carpeta imatgeDiskOdispositiu
bulk_extractor -o /ruta/carpeta -R puntMuntatge

...i on el paràmetre *-o* indica la carpeta on es guardarà tot el contingut trobat, classificat en forma de diversos fitxers segons el tipus de resultat obtingut. Per exemple, podem trobar els següents fitxers, entre d'altres:

* "*ccn.txt*" : Inclou nombres de tarjes de crèdit identificades
* "*domain.txt*" : Inclou dominis DNS trobats a URLs, emails, documents, etc
* "*email.txt*" : Inclou adreces de correu trobades en documents, pàgines web catxejades, fitxers d'hibernació, certificats SSL, etc
* "*rfc822.txt*" : Inclou metadades dels missatges de correu i de peticions/respostes HTTP
* "*ether.txt*" : Inclou adreces MAC trobades a partir del carving de paquets de xarxa allotjats en fitxers swap o d'hibernació
* "*exif.txt*" : Inclou metadades de fotografies
* "*ip.txt*" : Inclou adreces IP trobades també a partir del carving de paquets de xarxa
* "*telephone.txt*" : Inclou telèfons internacionals
* "*url.txt*" : Inclou adreces URL allotjades en la catxé del navegador, precompilades en executables o dins de correus. En aquest sentit també hi ha els fitxers "*url_services.txt*" i també "*gps.txt*"
*"*url_searches.txt*" : Inclou paraules usades en recerques a Internet via Google, Bing, etc.
* "*json.txt*" : Inclou els documents JSON trobats
* "*wordlist.txt*" : Inclou una llista de paraules extretes del disc (útil per fer cracking de contrasenyes)

La majoria d'aquests fitxers inclouen, al principi de cada línia corresponent a cada dada trobada, el seu "offset" dins del disc/imatge estudiat i al final de cadascuna d'aquestes línies també se solen afegir certes dades per donar context a la dada en qüestió. També es creen certs fitxers anomenats "**histogram.txt*", que inclouen una ordenació per freqüència d'aparició de l'ítem en qüestió (email, domini, etc), i el fitxer "*report.xml*", amb les metadades del propi escaneig. Més a https://github.com/simsong/bulk_extractor/wiki

Altres paràmetres (opcionals) de *bulk_extractor* interessants són:

* *-F fitxer.regex* : Indica el fitxer que inclou un conjunt d'expressions regulars (una a cada línia) que es faran servir per, amb els patrons allà indicats, personalitzar la recerca sobre el contingut de la imatge. Alternativament també existeix el paràmetre *-f regex*, que serveix per indicar directament una determinada expressió regular en lloc d'un fitxer. En qualsevol cas, els resultats obtinguts es guardaran específicament dins el fitxer "*find.txt*" i cal que s'utilitzi l'"scanner" "find" (veure a cont.)

* *-e nomScanner* : Indica que es farà servir un determina plugin (*bulk_extractor* els anomena "scanners"). Per exemple, l'scanner anomenat "wordlist" serveix per trobar específicament paraules a guardar a l'arxiu "wordlist.txt". En general, cada scanner serveix per trobar un tipus concret de contingut dins de la imatge/dispositiu a investigar i es poden indicar més d'un simplement afegint tants paràmetres *-e nomScanner* com calgui. De totes formes, *bulk_extractor* proporciona per defecte uns quants scanners ja llestos per utilitzar sense haver d'indicar el paràmetre *-e*, com ara l'anomenat "accts" (per trobar telèfons o nombres de tarjes de crèdit, entre altres), "aes" (per trobar claus AES a la memòria, fitxers swap i/o d'hibernació), "base64" (per trobar cadenes codificades en aquest format), "elf" (per trobar binaris en aquest format), "email", "exif", "net", etc, etc. Es pot conèixer la llista d'scanners activats per defecte (que són la gran majoria) llegint la sortida de *bulk_extractor -H* , on, a més, es pot veure que alguns scanners admeten l'ús de paràmetres propis per modificar el seu comportament, els quals s'han d'indicar així: *-S paramScanner -S unAltreParam...* D'altra banda, per desactivar un (o més!) scanner/s preactivat/s determinat/s (i així fer que l'escaneig sigui més ràpid i obtenir un resultat més concís) es pot utilitzar el paràmetre *-x nomScanner -x unAltre...* o, si es vol desactivar-ne tots de cop (per possiblement activar després només uns pocs scanners concrets), es pot escriure *-x all* També es pot desactivar tots els scanners excepte un en concret amb *-E nomScanner*

* *-w llistablanca.txt* : Indica el fitxer on hi haurà especificades una llista de cadenes (una a cada línia, amb la possibilitat d'incorporar comodins), les quals, si són trobades al disc/partició/imatge, es guardaran en fitxers concrets amb el nom de "email_*stopped*.txt", "url_*stopped*.txt", "exif_*stopped*.txt", etc (en lloc dels fitxers principals "email.txt", "url.txt", "exif.txt", etc)

* *-r llistavermella.txt* : Indica el fitxer on hi haurà especificades una llista de cadenes (una a cada línia, case-sensitive però amb la possibilitat d'incorporar comodins), les quals, si són trobades al disc/partició/imatge, es guardaran en fitxers concrets amb el nom de "*ALERT*_email.txt", "*ALERT*_url.txt", "*ALERT*_exif.txt", etc (en lloc dels fitxers "email.txt", "url.txt", "exif.txt", etc)

D'altra banda, de vegades, els discs durs es danyen, fet que pot provocar que la seva taula de particions estigui corrupta i, per tant, que no es reconegui l'existència de les possibles particions que hi puguin contindre ni, per tant, el seu sistema de fitxers i el seu contingut. En aquests casos més greus, l'eina que hem de fer servir per, si més no, fer el primer pas de reconèixer les particions i sistemes de fitxers d'un disc és **Testdisk** (https://www.cgsecurity.org/wiki/TestDisk), disponible al paquet homònim. Un cop instal·lada, el seu ús és tan senzill com fer:

sudo testdisk imatgeDiskOimatgeParticioOimatgeE01Odispositiu

A partir d'aquí, apareixerà una pantalla interactiva que ens preguntarà tot un seguit de coses:

*Confirmació del dispositiu/imatge on es començarà a buscar
*Confirmació del format de taula de particions del disc anterior (normalment serà "EFI GPT")
*Després de pulsar l'opció "Analyze", se'ns presentarà la llista de particions actualment reconegudes i l'opció "Quick search" que ens permetrà buscar (i mostrar) possibles particions que ara mateix no estiguin disponibles. A la pantalla resultant apareixerà de nou el llistat de particions trobades amb la possibilitat de realitzar diverses accions (com ara "P" -per llistar els fitxers inclosos en la partició sel·leccionada-, "T" -per canviar el seu GUID-, "A" -per afegir a mà una partició si no ha sigut reconeguda automàticament per l'eina, etc-). En pulsar "Enter" tornarem a una pantalla similar a de "Analyze" però amb l'opció afegida de "Deeper search" si volem seguir amb la recerca de més particions esborrades (a més d'altres opcions més avançades).

NOTA: A la pantalla d'opcions on apareix la d'"Analyze" (la tercera), es pot triar l'opció "Options" que permet modificar el comportament de Testdisk a l'hora de realitzar la seva feina amb la configuració de diverses opcions, però no les tindrem en compte. També apareix l'opció "Geometry", que és molt avançada i no la necessitarem i "Advanced", la qual ens porta o bé a l'opció "Image creation", la qual ens permet fer una imatge "raw" de la partició sel·leccionada (la qual es guardarà a la carpeta que escollirem a la pantalla posterior) o bé a l'opció "Type", la qual ens permet canviar el tipus de partició sel·leccionada (és a dir, el seu GUID)...depenent del sistema de fitxers reconegut (especialment si és FAT32, NFTS o Ext2) també podria aparèixer una tercera opció anomenada "Undelete" que ens permetria fer "data carving"

Wiping

El "wiping" (o posar a 0 tots els bytes d'un dispositiu/partició/imatge) és el 1r que es fa quan es vol:

a) Clonar en un futur aquest dispositiu/partició/imatge. Això és perquè tots els sectors que no hagin sigut modificats després de la instal·lació i ús del sistema allà present romandran encara a zero i, per tant, no es tindran en compte a l'hora de fer la clonació; fent que aquesta sigui més ràpida i que la imatge resultant sigui més petita.

b) Utilitzar aquest dispositiu/partició/imatge com a destí d'una clonació forense. Això és per evitar que la imatge resultant resulti "contaminada" amb dades que poguessin estar gravades anteriorment

c) Transferir el dispositiu físic a una altra persona o institució sense que aquesta pugui conéixer el contingut que aquest tenia anteriorment

Depenent del tipus de dispositiu físic (és a dir, si és el tradicional de tipus mecanico-magnètic o bé si és de tipus flash con els discos SSD), la manera concreta de fer el "wiping" variarà. En els primers, el "wiping" simplement consisteix en sobreescriure moltes vegades els sectors del dispositiu (ja sigui amb zeros o amb valors aleatoris) per tal d'assegurar-se que la dada original hagi desaparegut. En els segons, però, aquest sistema no és idoni perquè retallaria moltíssim la vida útil del dispositiu (ja que les SSD tenen un nombre màxim d'escriptures permeses abans de fallar, a més d'altres consideracions que es poden llegir a https://linuxhint.com/securely-delete-files-from-my-ssd). Per tant:

*En el cas de discos magnètics, la comanda més comuna per fer "wiping" és ***shred*** (del paquet "coreutils"), la qual per defecte fa tres passades d'escriptura de dades aleatòries (i una quarta opcional per omplir finalment de zeros) i es pot executar de la següent manera (on el paràmetre *-v* activa el mode verbós i el paràmetre *-z* fa la quarta passada addicional amb zeros abans comentada:

sudo shred -vz imatgeDiskOimatgeParticioOdispositiuOfitxerregular

NOTA: Es poden fer més de les tres passades d'escriptura per defecte amb el paràmetre *-n nº*. D'altra banda, si l'element a esborrar és un fitxer regular, es pot afegir el paràmetre *-u* per esborrar-lo (després d'haver fet les passades)
NOTA: Una comanda similar a *shred* però més agressiva i completa és *srm*, del paquet "secure-delete" (https://github.com/hackerschoice/THC-Archive/tree/master/Tools). Aquest paquet també incorpora altres eines, com la comanda *sfill* (per esborrar l'espai lliure d'un punt de muntatge o carpeta), *sswap* (per esborrar la memòria d'intercanvi) i *sdmem* (per esborrar la memòria RAM no utilitzada). No obstant, fa temps que no s'actualitza. Altres paquets alternatius, com *srm* o *wipe* o la ISO arrencable Dban també estan obsoletes...l'alternativa més actual i actualitzada (que veurem als exercicis) és "Nwipe" (https://github.com/martijnvanbrummelen/nwipe), disponible als repositoris de les distribucions més importants.

*En el cas de SSDs, la comanda més comuna és ***blkdiscard*** (del paquet "util-linux"), la qual elimina totes les dades guardades en el dispositiu indicat (bàsicament el que fa és enviar la comanda interna "TRIM" a tot el disc, la qual esborra tots els sectors).

sudo blkdiscard imatgeDiskOimatgeParticioOdispositiu

NOTA: La comanda anterior té diversos paràmetres interessants, com ara *-s* (realitza una eliminació extra de possibles metadades que poguessin romandre a la memòria catxé del dispositiu), *-z* (que omple de zeros els sectors eliminats) o *-v* (mode verbós), entre d'altres.

NOTA: Amb *dd if=/dev/urandom of=discSSD* es pot aconseguir quelcom similar, però *blkdiscard* és molt més ràpid. També existeix la comanda *fstrim*, la qual envia la comanda interna "TRIM" (és a dir, esborra el contingut) només, però, als sectors que estiguin marcats com "espai disponible" (és a dir, sense ocupar per cap fitxer actual)

NOTA: Independentment de si el disc és mecano-magnètic o SSD, si la seva connexió amb la placa base de la màquina és de tipus ATA/SATA, existeix una funcionalitat pertanyent al protocol (anomenada "Sanitize Device") que permet realitzar un esborrament eficaç del dispositiu a baix nivell; es pot saber com utilitzar-la (amb la comanda *hdparm*) a https://tinyapps.org/docs/ata_sanitize_hdparm.html En el cas de discos amb connexió NVMe, una funcionalitat similar també existeix (amb la comanda *nvme*) i està descrita a la pàgina https://tinyapps.org/docs/nvme-sanitize.html . També són interessants de llegir https://tinyapps.org/docs/wipe_drives_hdparm.html i https://tinyapps.org/docs/nvme-secure-erase.html

NOTA: A https://docs.google.com/spreadsheets/d/1GrQoZDAcsfVVP6jNnjiHUvIMPtolW3WHHKaxpZVfMIo es pot consultar el llistat de requeriments legislatius en diferents administracions sobre l'esborrament de dades, així com les diferents solucions, tant físiques com lògiques, disponibles. D'altra banda, teniu més informació sobre les tècniques existents i les diferents eines de "wiping" a https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf i més informació generalista a https://en.wikipedia.org/wiki/Data_erasure

EXERCICIS:

0.-a) Executa les següents comandes per tenir un disc de 100MB formatejat en Ext4:

sudo dd if=/dev/zero bs=1M count=100 of=disk.img
sudo mkfs.ext4 disk.img

...i comprova que efectivament ho hagis fet correctament observant la sortida de la comanda *file disk.img*

NOTA: Altres comandes que haurien obtingut el mateix resultat serien:
sudo dd if=/dev/zero bs=1M count=100 of=disk.img
sudo losetup /dev/loop0 disk.img
sudo mkfs.ext4 /dev/loop0
sudo losetup -d /dev/loop0

b) Crea la carpeta "~/hola" i fes que sigui el punt de muntatge del disc anterior. Això pots fer executant...:

sudo mount -o loop disk.img ~/hola
sudo chown -R $USER:$USER ~/hola

NOTA: Altres comandes que haurien obtingut el mateix resultat serien:
sudo losetup /dev/loop0 disk.img
sudo mount /dev/loop0 ~/hola
sudo chown -R $USER:$USER ~/hola

c) Crea dins de la carpeta "~/hola" un arxiu de text amb el nom de "a.txt" que tingui com a contingut la frase "Hola caracola". A més, copia una fotografia qualsevol (però que sigui de tipus JPG, important!) per exemple de la carpeta "/usr/share/backgrounds" (la dels fons de pantalla del sistema) també a "~/hola". Confirma que tots dos fitxers estiguin dins de "~/hola" abans de desmuntar-la (fent *sudo umount ~/hola*).

1.-a) Sabent que el "magic number" d'inici d'un fitxer JPG és FFD8, digues què mostra la comanda *dd if=disk.img | hexdump -C | grep "ff d8"* Apunta't el número de byte (és el valor que apareix a l'esquerra de la pantalla) corresponent a la posició del byte "ff" del "magic number" anterior. Suposarem en aquest enunciat que aquest número és 12345678

b) Sabent que el "magic number" de final d'un fitxer JPG és FFD9 (atenció perquè la majoria de formats no en tenen però el JPG sí), digues què mostra la comanda *dd if=disk.img | hexdump -C | grep "ff d9"* Apunta't el número de byte corresponent a la posició del byte "d9" del "magic number" anterior. Suposarem en aquest enunciat que aquest número és 9abcdef0

c) Utilitza la calculadora del Gnome (establerta en mode programació i amb la base hexadecimal configurada com la base de treball) per realitzar la resta *9abcdef0 – 12345678* (en el teu cas aquests números seran diferents). Tot seguit, observa quin és el valor del resultat en la base decimal Suposarem en aquest enunciat que aquest número és 24680. D'altra banda, observa també quin és el número en base decimal corresponent al valor trobat a l'apartat b). Suposarem en aquest enunciat que aquest número és 13579

> NOTA: Des del terminal, es podria haver fet la resta de números hexadecimals i obtenir el resultat en base decimal amb aquesta comanda: *printf %d $((0x9abcdef0-0x12345678))* . D'altra banda, per obtenir un valor decimal a partir d'un hexadecimal només caldria fer *printf %d 0x12345678* En qualsevol cas, si s'hagués volgut veure un resultat qualsevol en lloc de en decimal en hexadecimal, només hagués calgut canviar el "%d" per un "%x"

d) Executa la comanda *dd if=disk.img of=foto.jpg skip=13579 bs=1 count=24680* ¿Què obtens? Pista: recorda de PDFs anteriors per a què serveixen els paràmetres *skip=*, *bs=* i *count=* de la comanda *dd* Comprova-ho utilitzant un visor d'imatges sobre el fitxer obtingut.

2.-a) Executa la comanda *hexdump -C disk.img | grep "Hola caracola"* ¿Què mostra? Apunta't el número de byte (és el valor que apareix a l'esquerra de la pantalla) corresponent a la posició de la lletra "H" del missatge. Suposarem en aquest enunciat que aquest número és 00880400

> NOTA: Una altra comanda alternativa que mostraria el mateix que la indicada a l'apartat anterior és *strings -tx disk.img | grep "Hola caracola"*. Recorda que la comanda *strings* (del paquet "binutils") mostra les eventuals cadenes incrustades dins del fitxer binari indicat (és a dir, les seqüències de caràcters imprimibles que són dins d'un fitxer binari). El paràmetre *-t x* serveix per mostrar, al costat de cada cadena trobada, la seva posició (en bytes) des de l'inici del fitxer on es troba (es mostra en hexadecimal amb el valor "x"; si es vol en decimal, i així estalviar-nos l'apartat aII) següent, es pot indicar el valor "d")

aII) Utilitza la calculadora del Gnome (establerta en mode programació i amb la base hexadecimal configurada com la base de treball) per esbrinar quin és el valor en base decimal del número obtingut a l'apartat anterior (escrit en base hexadecimal). Suposarem en aquest enunciat que aquest nou número és 77675565

b) Executa la comanda *dd if=disk.img bs=1 count=13 skip=77675565 of=tros.bin* ¿Què obtens? Pista: recorda de PDFs anteriors per a què serveixen els paràmetre *skip=*, *bs=* i *count=* de la comanda *dd* Comprova-ho fent servir la comanda *cat* sobre el fitxer obtingut.

c) Edita el contingut del fitxer extret a l'apartat anterior com vulguis però mantenint la llargària de 13 caràcters del text.

> NOTA: En aquest cas concret, en ser contingut textual, pots fer servir un editor de text qualsevol, però en general, si el contingut fos binari, hauries d'utilitzar un editor hexadecimal. D'editors d'aquest tipus que siguin en mode gràfic podem destacar **GHex** (https://wiki.gnome.org/Apps/Ghex) o **wxHexEditor** (https://www.wxhexeditor.org) entre molts d'altres mentre que siguin en mode text en podem destacar **Hexedit** (https://github.com/pixel/hexedit); en concret, en aquest programa amb F1 es pot accedir a la seva pàgina del manual, on es mostra la referència de combinacions de tecles que es poden fer servir per treballar-hi (la més important, CTRL+X per guardar i sortir). Un altre editor hexadecimal similar (però que fa servir les combinacions de tecles similars al Vim) és **Hexer** (http://devel.ringlet.net/editors/hexer)

d) Executa la comanda *dd if=tros.bin bs=1 count=13 seek=77675565 of=disk.img conv=notrunc* ¿Què obtens? Pista: recorda de PDFs anteriors per a què serveixen els paràmetres *seek=* i *conv=notrunc* de la comanda *dd*

e) Comprova el que has deduït a l'apartat anterior executant les següents comandes. ¿Què ha passat, efectivament?

```
sudo mount -o loop disk.img ~/hola
sudo chown -R $USER:$USER ~/hola
cat ~/hola/a.txt
sudo umount ~/hola
```

Fixa't que, en l'exercici anterior, en cap moment hem hagut de muntar el sistema de fitxer per modificar els bytes d'un dispositiu: la comanda *dd* funciona "per sota" sigui quin sigui el format del disc o partició en qüestió. Aquest fet el podem aprofitar per realitzar coses tan curioses com "amagar" dades fora de qualsevol partició (és a dir, en llocs "lliures" del disc). A continuació es veurà una demostració

3.-a) Executa les següents comandes per tenir un disc de 200MB format per una partició de 100MB i espai lliure posterior d'altres 100MB:

sudo dd if=/dev/zero bs=1M count=200 of=unaltredisk.img
sudo fdisk unaltredisk.img <- Indicant les opcions *g n ENTER ENTER +100M w*
sudo losetup -P /dev/loop0 unaltredisk.img
sudo mkfs.ext4 /dev/loop0p1

...i comprova que efectivament ho hagis fet bé observant la sortida de la comanda *fdisk -l unaltredisk.img*

> NOTA: Recorda que les opcions interactives indicades a *fdisk* indiquen que, en un disc GPT (de mida de 200M) es vol crear una nova partició (per defecte, la primera i ubicada el més al començament possible del disc) de 100M.
> NOTA: El paràmetre *-P* de la comanda *losetup* indicat a la tercera línia anterior és molt important perquè obliga a fer un repàs del contingut del fitxer-disc en recerca de possibles particions internes (les quals s'anomenaran llavors loopXpY); si no s'indica, aquestes no es trobaran

b) Tenint en compte la disposició de particions/disc obtinguda a l'apartat anterior, ¿què estàs aconseguint amb les comandes següents?

echo "text_secret" | dd bs=1M seek=150 of=unaltredisk.img conv=notrunc
dd if=unaltredisk.img bs=1M count=1 skip=150 | strings

> NOTA: En lloc d'un text res no impediria haver amagat un binari. En aquest cas, però, per obtindre'l caldria tenir en compte la seva mida exacta i, en lloc de fer servir la comanda *strings* s'hauria d'utilitzar una altra eina, com per exemple el visor hexadecimal *hexdump*

A continuació estudiarem l'ús d'eines de "carving" especialitzades, com Photorec o Bulk_extractor

4.-a) Fes que ara "~/hola" sigui el punt de muntatge de la (única) partició del disc creat a l'exercici anterior. Això pots fer executant (tenint en compte que "/dev/loop0p1" encara existeix...això ho pots comprovar a la sortida de *lsblk*; si no fos així, caldrà que executis primer la comanda *sudo losetup -P /dev/loop0 unaltredisk.img*) les següents comandes:

sudo mount /dev/loop0p1 ~/hola
sudo chown -R $USER:$USER ~/hola

b) Copia de nou una fotografia qualsevol (per exemple de la carpeta "/usr/share/backgrounds") dins de la carpeta "~/hola" i tot seguit, esborra-la fent servir la comanda *rm* Finalment, desmunta "~/hola".

c) Instal·la el paquet "testdisk" al teu sistema i executa la comanda *sudo photorec unaltredisk.img*. Segueix les instruccions que se't marquen (descrites també a la teoria) per recuperar el màxim de fitxers esborrats de la partició Ext4 al disc indicat (els quals es guardaran amb noms aleatori -ja que la referència als noms originals ha desaparegut- dins d'una subcarpeta "recup_dir.nº" ubicada a la carpeta on s'ha executat la comanda). Hauràs de comprovar com, efectivament, has recuperat la fotografia esborrada a l'apartat anterior

> NOTA: De fet, si executes *dd if=unaltredisk.img | hexdump -C | grep "ff d8"*, encara es veu la referència en disc del començament de la fotografia esborrada. Aquest fet és un dels trucs que utilitza Photorec per recompondre el fitxer original

d) ¿Què s'explica a https://www.cgsecurity.org/wiki/Add_your_own_extension_to_PhotoRec o a https://github.com/cgsecurity/testdisk_documentation/blob/master/photorec_custom_signature.rst ?

5.-a) Instal·la el paquet "bulk-extractor" (a Ubuntu) o "bulk_extractor" (a Fedora) i executa la comanda *sudo bulk_extractor -o ~/hola -R ~/Baixades* Després d'esperar una estona fins que finalitzi l'execució de la comanda anterior, observa el contingut de la carpeta "~/hola" amb la comanda *ls -s ~/hola* ¿Quins fitxers, de tots els que hi ha allà presents, tenen contingut? Fes-hi una ullada a veure què hi trobes.

b) Elimina el contingut de "~/hola" (amb *rm ~/hola/**, per exemple) i ara executa la comanda *bulk_extractor -o ~/hola* ***-E email*** *-R ~/Baixades* . ¿Quin resultat obtens ara?

c) Elimina el contingut de "~/hola" (amb *rm ~/hola/**, per exemple) i ara executa la comanda *bulk_extractor -o ~/hola* ***-E find -f "@gmail.com"*** *-R ~/Baixades* . ¿Quin resultat obtens ara?

> NOTA: Un altre programa similar a Bulk_Extractor és **FastirArtifacts** (https://github.com/OWNsecurity/fastir_artifacts). La seva base de dades d'"artefactes" a trobar es troba disponible a https://github.com/ForensicArtifacts/artifacts
> NOTA: Un altre programa interessant que en aquest cas realitza (només) recerques de contingut textual de fitxers en un sistema d'escriptori és **Recoll** (https://framagit.org/medoc92/recoll). En aquest sentit, **Tracker** (https://tracker.gnome.org/overview) fa una funció similar en escriptoris Gnome

Fdupes (https://github.com/adrianlopezroche/fdupes) és una eina que compara el contingut de dues carpetes i informa de si n'hi ha fitxers repetits entre elles

> NOTA: Altres eines similars són **Rmlint** (https://rmlint.readthedocs.io/en/latest) o, el més complet de tots, **Czkawka** (https://qarmin.github.io/czkawka)

6.-a) Instal·la el paquet "fdupes" i copia un fitxer qualsevol que tinguis en la teva carpeta "Baixades" a la carpeta "Escriptori". Tot seguit, executa la comanda *fdupes ~/Baixades ~/Escriptori* ¿Què veus?

b) Consulta la pàgina del manual de fdupes per esbrinar per a què serveixen els seus paràmetres *--recurse*, *--recurse:* , *--time*, *--size* i *--delete* (aquest darrer paràmetre obre una consola interna amb comandes pròpies...les més importants són "prune", per esborrar els fitxers no seleccionats i "exit" per sortir, més ajuda trobareu a *man fdupes-help)*

c) Vés a https://www.bleachbit.org (o https://github.com/bleachbit/bleachbit) i digues per a què serveix el programa gràfic "Bleachbit". Pots instal·lar-lo i provar-lo, si vols.

L'eina *hdparm* (disponible en el paquet homònim) permet consultar i manipular una gran quantitat de configuracions de molt baix nivell relacionades amb els discs durs. Una d'elles ens permet en concret saber (gràcies a consultar-ho a la taula d'inodes) en quins sectors del disc dur està físicament escampat un determinat fitxer, i s'executa així: **sudo hdparm --fibmap /ruta/fitxer** . En el cas de sistemes Ext2/3/4, una altra comanda que ens pot donar la mateixa informació és **filefrag -b512 -v /ruta/fitxer** Cal tenir en compte, però, que la primera comanda mostra els números de sectors (els anomenat "offsets") començant-los a comptar sempre des del principi del disc (tot i que també s'informa del l'offset del primer sector de la partició particular en qüestió, a la línia "begin at LBA...", per tal de poder així treballar amb direccionament relatiu si es vol) mentre que la segona comanda mostra els "offsets" ja directament començant des del principi de la partició particular en qüestió.

D'altra banda, recordem que cal distingir entre el que és un "sector" (mínima porció de disc direccionable a nivell de hardware, quasi sempre de 512 bytes de mida -es pot confirmar veient la sortida de la comanda **sudo blockdev --getpbsz /dev/disp** o el valor de l'opció "Sector size" de la sortida de *fdisk -l* -) i el que és un "bloc" (mínima porció de disc direccionable a la pràctica perquè funciona a nivell lògic -és a dir, a nivell de sistema de fitxers-; la seva mida dependrà del valor establert en el moment de formatejar la partició en qüestió amb el sistema de fitxers escollit -o el seu valor per defecte- i es pot consultar veient la sortida de la comanda **sudo blockdev --getbsz /dev/disp** o el valor de l'opció "I/O Blocks" de la sortida de *stat*). La comanda **filefrag -v /ruta/fitxer** mostra, en aquest sentit, en quins blocs del disc dur està físicament escampat un determinat fitxer i l'opció "Blocks"de la sortida de *stat* mostra la seva quantitat)

7.-Després d'haver llegit el quadre anterior, digues quina diferència hi ha entre la informació que apareix a la línia que comença per "*File size of ...*" i a les columnes "logical_offset", "physical_offset" i "length" mostrades a la sortida de les comandes *filefrag -b512 -v /ruta/fitxerGRAN* i *filefrag -v /ruta/fitxerGRAN*

> NOTA: A la sortida de les comandes anteriors es menciona la presència d'"extents". Cal saber que un "extent" redueix la quantitat de metadades necessàries per fer el seguiment dels blocs dels fitxers grans: en lloc d'emmagatzemar una llista de cada bloc individual que componen el fitxer, la idea és emmagatzemar només l'adreça del primer i l'últim bloc de cada rang continu de blocs. Aquests intervals continus de blocs de dades (i els parells de números que els representen) són els "extents"

8.-a) Executa la comanda *sudo dd if=/dev/random of=block.bin bs=1M count=500 status=progress* i observa el resultat amb *hexdump -C block.bin*

b) ¿Quina informació es mostra en el següent quadre (extret del Github de l'eina Nwipe)?

Nwipe's erasure methods

- Fill With Zeros - Fills the device with zeros (0x00), one round only.
- Fill With Ones - Fills the device with ones (0xFF), one round only.
- RCMP TSSIT OPS-II - Royal Candian Mounted Police Technical Security Standard, OPS-II
- DoD Short - The American Department of Defense 5220.22-M short 3 pass wipe (passes 1, 2 & 7).
- DoD 5220.22M - The American Department of Defense 5220.22-M full 7 pass wipe.
- Gutmann Wipe - Peter Gutmann's method (Secure Deletion of Data from Magnetic and Solid-State Memory).
- PRNG Stream - Fills the device with a stream from the PRNG.
- Verify Zeros - This method only reads the device and checks that it is filled with zeros (0x00).
- Verify Ones - This method only reads the device and checks that it is filled with ones (0xFF).
- HMG IS5 enhanced - Secure Sanitisation of Protectively Marked Information or Sensitive Information

c) Instal·la el paquet "nwipe" i executa les comandes *sudo losetup /dev/loop0 block.bin && sudo nwipe /dev/loop0*. Després de seleccionar el disc en qüestió (tecla "SPACE") i de triar el mètode d'esborrament (tecla "m"), que serà "Fill with Ones", i el número de rondes (tecla "r"), que serà "1", inicia el procés d'esborrament (tecla "S"). Un cop finalitzat, observa el resultat del procés amb *hexdump -C block.bin*

> NOTA: L'eina Nwipe és més útil quan ve integrada dins d'una distribució "Live", per tal de poder treballar amb discos sencers desmuntats. En aquest sentit, una distribució que està dissenyada per executar Nwipe automàticament en arrencar és **ShredOS** (https://github.com/PartialVolume/shredos.x86_64)