Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions

Anàlisi forense d'evidències digitals

Consultor: Josep Maria Arqués Soldevila
Estudiant: Esteban Bonachera López

12 de Gener de 2014

<< Yo os he elegido a
vosotros y os he
destinado para que
vayáis y deis fruto,
y que vuestro fruto
permanezca. >> Jn 15,16

Resum

L'objectiu principal d'aquest projecte consisteix en la realització de l'anàlisi forense del disc dur i de la memòria RAM d'un ordinador personal, en concret un Netbook, vinculat a una possible conducta delictiva. També s'inclou en l'anàlisi un base de dades del conegut programari Whatsapp extreta d'un smartphone. Per realitzar aquesta tasca s'utilitzaran eines específiques per localitzar les evidències digitals que puguin demostrar els presumptes delictes.

Les evidències localitzades s'han de recollir en un informe pericial que haurà de tenir en compte els requisits processals necessaris per a que l'anàlisi pugui tenir validesa en un procés judicial, a banda dels aspectes tècnics.

The primary goal of this project consists in the realization of forensic analysis of the hard disk and the RAM memory of a personal computer, in concrete a netbook, tie to a possible criminal conduct. Also is included in the analysis a data base of the well-known software Whatsapp extracted of a Smartphone. In order to make this task will use specfics tools to locate the digital evidences that can demonstrate the presumed crimes.

The located evidences are had to gather in an expert report that will have to consider necessary the procedural requirements so that analysis can have validity in a judicial process.

Índex

1. Introducció

Aquest document conforma la proposta d'un Treball d'investigació en l'àmbit de la seguretat de les Tecnologies de la Informació i la Comunicació.

Bàsicament es presentaran els diferents mètodes i eines disponibles per realitzar l'anàlisi forense d'un equip informàtic i de les comunicacions via telèfon mòbil de dues persones que van estar detingudes per portar al seu cotxe una quantitat considerable de drogues sintètiques i de targetes magnètiques en blanc.

Donat el caràcter dels objectes confiscats, les autoritats creuen necessari efectuar un registre al domicili dels detinguts.

La presència de targetes de banda magnètica, fa pensar que aquestes puguin ser utilitzades per falsificar targetes de crèdit o dèbit d'entitats financeres.

Així mateix, el fet de posseir tal quantitat de pastilles estupefaents pressuposa que no es tracti de simples 'camells de discoteca'.

Per tant, és necessari analitzar l'equip informàtic dels detinguts, i les seves comunicacions a través del telèfon mòbil, per intentar esbrinar l'abast dels delictes comesos.

D'una banda, es buscaran indicis de la participació dels detinguts en la falsificació de targetes bancàries i la realització d'activitats fraudulentes. D'altra banda, s'intentarà demostrar si els detinguts es dediquen a l'elaboració i/o distribució de pastilles estupefaents a gran escala.

Amb les evidències detectades, es redactarà un informe pericial que es farà servir per incriminar als detinguts davant d'un tribunal de justícia.

1.1. Estat de l'art de la informàtica forense

La informàtica forense [1] consisteix en l'aplicació de tècniques científiques i analítiques, molt especialitzades, a infraestructures tecnològiques que permeten identificar, preservar, analitzar i presentar dades que siguin vàlids dins d'un procés legal.

Així doncs, la informàtica forense recopila i fa servir les evidències digitals per aquells delictes informàtics i d'altres comuns en els quals les noves tecnologies tenen alguna implicació (l'ús d'Internet, d'un *PC*, d'un telèfon mòbil, etc.).

Les dades poden provenir de qualsevol tipus de dispositiu electrònic i de qualsevol mitjà d'emmagatzematge com, per exemple, discos durs, *memòria RAM*, targetes de memòria, arxius i correus electrònics.

1.1.1. Fases de la informàtica forense

Les forces de seguretat, davant el maneig d'evidències sobre un crim o delicte informàtic comés, hauran d'actuar com en qualsevol procés criminal comú. El primer pas és assegurar l'escena del delicte, restringint l'accés a la mateixa per evitar modificacions a les evidències. Els perits que manegin el cas hauran de posseir els coneixements adequats sobre les metodologies de l'anàlisi forense informàtic que s'han d'aplicar en funció del cas.

Per a dur a terme una investigació forense es necessari conèixer certs aspectes tals com:

- Conèixer les condicions sota les quals l'evidència serà considerada com:
  - Admissible
  - Autentica
  - Complerta
  - Confiable
  - Creïble
- Conèixer el procediment per dur a terme una investigació, quan es deuen considerar les qüestions legals a tenir en compte, depenent del país on es digui a terme.

Existeixen dos modes d'anàlisi per la informàtica forense, aquests són:

- **Anàlisi post-mortem (o en fred).** Es realitza amb un equip dedicat específicament per a fins forenses per examinar discos durs, dades o qualsevol tipus d'informació recaptada d'un sistema que ha sofert un incident. En aquest cas, les eines de les que es pot disposar són aquelles que existeixin al laboratori destinat a l'anàlisi de les evidències digitals.

- **Anàlisi en calent.** Es duu a terme quan un sistema ha sofert, o està sofrint, un incident de seguretat. En aquest cas, s'ha d'emprar un *CD*, o un *pendrive*, amb les eines de resposta a incidents i/o anàlisi forense compilades de manera que no realitzin modificacions en el sistema. Després de realitzar l'*anàlisi en calent*, s'haurà de fer una *anàlisi en fred*.

Cadena de custodia [2]. És el conjunt de passos o procediments a seguir per preservar la prova digital i que permeti convertir-la i utilitzar-la com evidència digital en un procés judicial. No existeix un estàndard reconegut públicament.

La cadena de custodia ha de:

- Reduir al màxim la quantitat d'agents implicats en el maneig o tractament d'evidències.
- Mantenir en secret la identitat de les persones implicades des de l'obtenció fins a la presentació de les evidències.
- Assegurar la fermesa de les evidències.
- Realitzar registres de temps, signats pels agents, de l'intercanvi entre aquestos de les evidències. Cada un d'ells serà responsable de les evidències en cada moment.

La seqüència de la cadena de l'evidència ha de seguir el següent ordre:

- Recol·lecció o identificació d'evidències.
- Anàlisi.
- Emmagatzematge.

- Preservació.
- Transport.
- Presentació en el jutjat.
- Retorn al propietari (si escau).

La cadena de custodia de l'evidència mostra:

- Qui va obtenir l'evidència.
- On i quan es va obtenir l'evidència.
- Qui va protegir l'evidència.
- Qui ha tingut accés a l'evidència.

L'evidència digital és el conjunt de dades en format binari, compren els fitxers, el seu contingut o referencia a aquests (*metadades*) que es trobin als suports físics o lògics del sistema atacat. Aquestes dades poden ser recopilats i analitzats amb eines i tècniques especials (veure l'Annex A).

1.1.2. Normativa i estàndards reguladors

Tot i no disposar d'un estàndard definit que reguli la recol·lecció i preservació d'evidències digitals, existeixen diversos manuals de bones pràctiques publicats per organismes internacionals que pretenen establir les pautes a seguir en aquestes fases del procés. Algunes d'aquestes normes son:

- **ISO/IEC 27037:2012.** *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. L'estàndard proporciona una guia detallada en la identificació, col·lecció i/o adquisició, emmagatzematge, transport i preservació d'evidències electròniques, particularment per mantenir la seva integritat.

Aquesta norma es basa en els següents principis:

- **Aplicació de mètodes.** Les evidències digitals s'han d'adquirir de la manera menys intrusiva possible per tal de preservar l'originalitat de la prova. Es recomana realitzar còpies de les evidències.

- **Procés auditable.** Els procediments emprats i la documentació que s'ha generat han d'haver estat validats i contrastats per les bones pràctiques professionals. S'han de proporcionar traces i evidències d'allò que s'ha realitzat i dels seus resultats.

- **Procés reproduïble.** Els procediments i mètodes aplicats deuen ser reproduïbles, verificables i argumentables al nivell de comprensió dels entesos en la matèria, que són els que poden donar validesa i respatller a les actuacions realitzades.

- **Procés defensable.** Les eines que s'han utilitzat han de ser esmentades i, a més, deuen haver estat contrastades i validades en el seu ús per a la fi que es vol aconseguir.

Publicada a l'octubre de 2012, aquest estàndard equival al britànic *BS 10008:2008* [3]. L'**ISO 27037** es complementarà amb la norma ISO 27043, quan aquesta es publiqui.

- I**SO/IEC 27041.** *Information Technology - Security techniques – Guidelines for the analysis and interpretation of digital evidence.* Aquesta norma encara està en fase de esborrany, es preveu la publicació definitiva l'any vinent. Bàsicament, **l'ISO 27041** tracta de garantir la investigació forense. Es a dir, aquesta norma el que pretén és assegurar la credibilitat, la integritat i la fiabilitat dels processos d'investigació de les evidències digitals.

  L'estàndard oferirà una guia per assegurar la conveniència i la idoneïtat dels mètodes necessaris per la investigació forense de les evidències digitals. També descriurà mètodes a través dels quals totes les etapes del procés d'investigació poden ser mostrades per ser les adequades.

- **ISO/IEC 27042.** *Information Technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence.* En fase d'esborrany, es preveu la seva publicació definitiva l'any 2014. **L'ISO 27042** proporcionarà directrius per l'anàlisi i la interpretació de les evidències digitals amb la finalitat d'estandarditzar el procés.

- **ISO/IEC 27043.** *Information Technology – Security techniques – Digital evidence investigation principles and processes.* En fase d'esborrany, es preveu la seva publicació l'any 2014. Aquest estàndard oferirà una guia amb els processos, i els passos a seguir, al llarg de la investigació forense de les evidències digitals. La finalitat d'aquesta norma és l'estandardització dels procediments forenses.

El propòsit fonamental d'aquestes quatre normes és promoure mètodes de bones pràctiques i processos en la investigació forense de les evidències digitals. La seva finalitat principal és aconseguir una estandardització dels mètodes, processos i controls involucrats en la investigació forense entre els diferents organismes, pertanyin o no a la mateixa jurisdicció.

1.1.3 Present i futur de la informàtica forense

Tot i tractar-se d'una disciplina relativament recent, la i*nformàtica forense* tal i com la coneguem en l'actualitat no està evolucionant al mateix ritme que la tecnologia. L'aparició dels discos durs *SSD* i el nivell de seguretat que aporten, d'una banda, i la cada cop més gran utilització de serveis de *Hosting* amb la conseqüent externalització d'equips i serveis, d'altra banda, fan cada cop més difícil la tasca de l'anàlisi forense. Cada cop és més difícil la tasca de l'investigador forense informàtic.

En el cas dels discos *SSD*, ja són molts els analistes forenses que afirmen que són la panacea dels delinqüents informàtics. El propi *Firmware* del disc s'encarrega d'eliminar definitivament les dades emmagatzemades un cop es rep l'ordre d'esborrat. Ja no es depèn del sistema operatiu i, aquest mètode, fa inútil tots els mètodes coneguts de recuperació d'arxius i dades.

Així mateix, l'ús dels serveis de *Hosting* per part de les empreses, fa quasi impossible les tasques d'informàtica forense. El fet de tenir les dades i serveis empresarials en servidors de terceres parts, complica molt la recol·lecció d'evidències en cas d'un atac o incident detectat. Es pràcticament impossible accedir als *logs* i registres dels servidors de l'empre-

sa proveïdora de serveis d'allotjament *web* sense una ordre judicial. Del mateix mode, el fet de compartir els servidors entre diversos clients, no garanteix que les dades es mantinguin intactes i no siguin alterades durant l'assignació de recursos o les tasques de manteniment dels servidors i dels *CPD*.

Un altre tema és la utilització de diversos dispositius per tractar i emmagatzemar la informació. La informàtica forense clàssica només tractava amb *PC* i amb servidors basats en emmagatzematge en discos durs. Actualment, cada cop és més habitual l'ús de dispositius mòbils com són les t*ableles* i els *smartphones*, tant a nivell empresarial com a nivell personal. Això implica una formació cada cop més específica i uns medis tècnics que no tots els professionals de la informàtica forense poden assumir.

A banda de les noves tecnologies i de la *globalització* de la informació, un dels principals problemes que es troba la informàtica forense és la constant evolució dels diferents tipus d'incidents que es poden produir. Les tècniques que fan servir els delinqüents són cada dia més sofisticades, apareixent cada dia noves formes d'atac més difícils de detectar i de combatre: nous *virus*, nous *troians*, etc. Així doncs, la informàtica forense està obligada a un reciclatge i a una preparació permanent per tractar d'afrontar amb èxit les noves formes d'atac.

Un altre punt a destacar de la informàtica forense és, tot i els esforços que actualment s'estan realitzant, la no existència d'uns estàndards dels diferents processos que intervenen en l'anàlisi forense. L'ús de diferents metodologies o guies suposa uns resultats diferents al analitzar les mateixes evidències digitals. Això és un problema que encara no està solucionat.

El factor humà també és molt important en la informàtica forense, a banda d'una formació cada cop més especialitzada, es requereix una objectivitat a l'hora d'analitzar i presentar els resultats de l'anàlisi de les evidències. No es pot permetre cap involucració personal amb l'incident o la informació investigada.

Finalment, no es podem oblidar dels aspectes legals, doncs és aquí on es troben les majors limitacions de la informàtica forense. En aquest món globalitzat existeixen diferents legislacions, fins i tots dins d'un mateix país, que dificulten enormement les tasques de l'anàlisi forense. Un exemple ben clar d'aquesta problemàtica és l'empresa *Google* [4] i el seu *'tractament'* a les dades de caràcter personal. Tot i ser una pràctica il·legal a molt països, el fet de tenir emmagatzemades les dades als Estats Units, amb una legislació més permissiva en aquest aspecte, amb la qual cosa, no es pot fer res al respecte.

2. Descripció del Treball

Amb aquest Treball el que es pretén és demostrar, d'una forma amena i molt complerta, mitjançant l'anàlisi de les evidències digitals obtingudes al domicili dels detinguts, els vincles existents entre les dades analitzades i la *presumpta* conducta delictiva de les dues persones detingues.

2.1. Objectius i resultats

A continuació s'enumeraran els objectius principals d'aquest Treball:

- Analitzar el disc dur d'un ordinador personal, i altres tipus de dades, per descobrir possibles irregularitats. En el nostre cas, es tracta de descobrir indicis d'activitats delictives relacionades amb la detenció de dues persones.

- Conèixer les eines i metodologies de les quals disposem per realitzar l'anàlisi forense d'un ordinador.

- Demostrar la culpabilitat dels delinqüents davant d'un tribunal de justícia. Aquest punt implica el coneixement de l'actual legislació i la familiarització amb el peritatge informàtic.

- Saber distingir entre informació rellevant per el cas que ens ocupa i altra informació important però no relacionada amb els delictes comesos. Per exemple, el fet de trobar plànols amb les instruccions de construcció d'una bomba atòmica a l'ordinador dels detinguts. Tot i ser un delicte molt greu, no està relacionat amb el cas que ens ocupa i, per tant, només caldria apuntar aquest detall a l'informe pericial o, el més lògic, obrir una altra causa judicial que queda fora de l'àmbit d'aquest Treball.

2.2. Anàlisi de riscos

Com succeeix a tots els projectes, els recursos són limitats al present Treball. S'ha de tractar de minimitzar el possible impacte que pugui produir una situació de risc no desitjada. A banda de les garanties de qualitat de tot el procés, es prendran les següents mesures preventives:

- Realització setmanal d'un seguiment de l 'estat del Treball complint els terminis establerts a la planificació inicial.
- Priorització de les tasques mantenint un ordre lògic i coherent. Per això s'haurà de respectar, amb molta cura, l'abast del Treball (Veure l'apartat següent).
- Garantia de la disponibilitat dels recursos necessaris: material bibliogràfic, disponibilitat de l'ordinador i programari ofimàtic imprescindible per cercar informació i redactar el Treball, connexió a Internet, etc.

3. Abast de la proposta

El Treball s'atendrà, de manera exclusiva, a l'anàlisi forense del disc dur d'un ordinador personal que presumptament està vinculat a uns actes delictius comesos per una parella que ha estat detinguda, de manera casual, en un control de carretera rutinari.

Així mateix, es disposarà d'altres evidències digitals. D'una banda, el bolcat de la *memòria RAM* de l'ordinador. La informació continguda a la memòria ens pot ser de gran utilitat a l'hora de cercar noms d'usuari i contrasenyes, entre d'altres dades. D'altra banda, una base de dades generada per una coneguda xarxa social extreta d'un *smartphone* propietat d'uns dels detinguts.

Finalment, les evidències detectades s'hauran d'incloure en un informe pericial que servirà per ratificar, davant d'un tribunal de justícia, l'autoria o la implicació en els fets delictius investigats per part de les dues persones que van ser detingudes. S'ha de tenir present que els càrrecs que s'imputen són el tràfic de substàncies estupefaents, d'una banda, i la possessió de targetes magnètiques en blanc, d'altra banda. Tot i no ser un delicte en si mateix, aquest darrer càrrec suposa hipotètiques activitats il·legals o fraudulentes futures.

4. Organització del Treball

Aquest apartat descriu amb detall els recursos que cal assignar per poder portar aquest Treball a bon termini.

Recursos Humans. Atès el caràcter educatiu d'aquest Treball, s'assignen tres grups diferents de rols a una mateixa persona: l'autor del Treball que, al mateix temps, és estudiant d'aquesta assignatura. Els diferents rols són: redactor, analista informàtic i pèrit informàtic.

Recursos Temporals. Tenint en compte el caràcter docent d'aquest Treball, el nombre de crèdits universitaris assignats i, a més, la càrrega lectiva de l'autor, el còmput global d'hores invertides **no hauria de superar en cap cas les 450 hores**.

Recursos Materials. Els recursos materials necessaris són:

● **Documentals.** Accés a la bibliografia (llibres, revistes, etc.) i consulta de diversos recursos a Internet. Tot aquest material formarà part de la font bibliogràfica del Treball.

● **Tecnològics.** Les eines tecnològiques, avui dia imprescindibles en qualsevol ambient de treball tecnològic, seran les eines ofimàtiques necessàries per realitzar les consultes a Internet, el programari que es farà servir per compilar i redactar el Treball, les eines que permetran investigar les diferents evidències digitals que s'han d'analitzar, un ordinador personal per emmagatzemar i tractar la informació, un *iPad* per consultar documents i textos i, finalment, una connexió de banda ampla. En concret, els recursos tecnològics que es faran servir són (veure l'apartat 8.1):

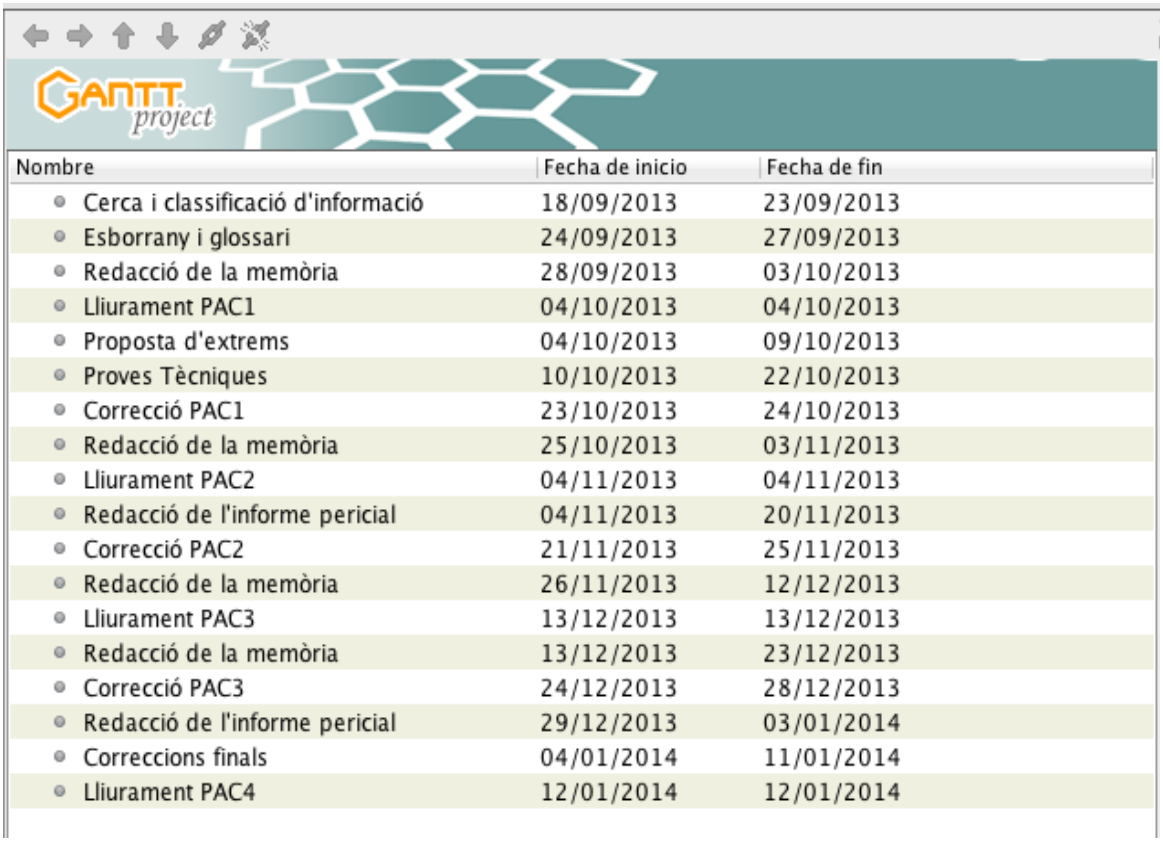
- **Programari:** Navegador web Safari v 6.0.5, OpenOffice 4.0.1, Adobe [8] Reader X, GanttProject 2.6.1 i VMware Fusion 5.0.3 Professional**.**
- **Maquinari:** Ordinador portàtil Apple [5] *MacBook Pro* 13.3” (mid 2012), Apple [5] *iPad* i connexió *ADSL* de Telefònica 10Mb.

5. Pla de Treball

Aquest capítol descriu la planificació temporal del present Treball així com les fites més importats.

5.1 Relació d'activitats

L'enumeració de les diferents etapes i tasques que conformaran aquest Treball es pot observar a la següent captura de pantalla:



Nombre	Fecha de inicio	Fecha de fin
Cerca i classificació d'informació	18/09/2013	23/09/2013
Esborrany i glossari	24/09/2013	27/09/2013
Redacció de la memòria	28/09/2013	03/10/2013
Lliurament PAC1	04/10/2013	04/10/2013
Proposta d'extrems	04/10/2013	09/10/2013
Proves Tècniques	10/10/2013	22/10/2013
Correcció PAC1	23/10/2013	24/10/2013
Redacció de la memòria	25/10/2013	03/11/2013
Lliurament PAC2	04/11/2013	04/11/2013
Redacció de l'informe pericial	04/11/2013	20/11/2013
Correcció PAC2	21/11/2013	25/11/2013
Redacció de la memòria	26/11/2013	12/12/2013
Lliurament PAC3	13/12/2013	13/12/2013
Redacció de la memòria	13/12/2013	23/12/2013
Correcció PAC3	24/12/2013	28/12/2013
Redacció de l'informe pericial	29/12/2013	03/01/2014
Correccions finals	04/01/2014	11/01/2014
Lliurament PAC4	12/01/2014	12/01/2014

Figura 1. Relació d'activitats

A la pàgina següent s'ofereix una breu descripció de les activitats o tasques anteriors:

Cerca d'informació: Compren la cerca de les eines necessàries per poder realitzar l'anàlisi i, a més, altres informacions complementaries (exemples d'informes pericials, metodologia, etc.)

Esborrany i glossari: Engloba el primer disseny del present document, la definició dels diferents apartats i la preselecció dels termes que caldrà definir al glossari.

Redacció de la Memòria i de l'Informe pericial: Aquestes dues tasques es refereixen, respectivament, a la redacció definitiva d'aquest Treball i de l'informe pericial resultant.

Proposta d'extrems: Aquesta activitat compren la definició i el plantejament dels extrems que conformaran l'informe pericial i, amb total seguretat, determinaran l'autoria dels fets delictius per part dels detinguts davant d'un tribunal.

Proves Tècniques: Compren l'anàlisi de les evidències digitals. S'examinaran el disc dur, el bolcat de la *memòria RAM* i una base de dades, generada per una popular xarxa social, extreta del *smartphone* d'un dels detinguts.

Correcció PACx: Al llarg del present Treball, s'aniran corregint els errors detectats als diferents lliuraments. D'aquesta manera s'evita l'acumulació de les possibles desviacions per al final del termini d'entrega i, a més, s'impedeix passar per alt les incorreccions detectades.

Correccions finals: Aquesta tasca és de vital importància, doncs implica la correcció dels dos documents finals que s'han de lliurar. Les correccions que s'aplicaran són: estil, redacció, lèxic, maquetació del document, links interns, etc.

5.2. Fites principals

L'autor del Treball garantirà que les fites principals quedaran assolides en els termes i terminis d'aquesta proposta.

A la següent taula es poden observar les fites més importants,

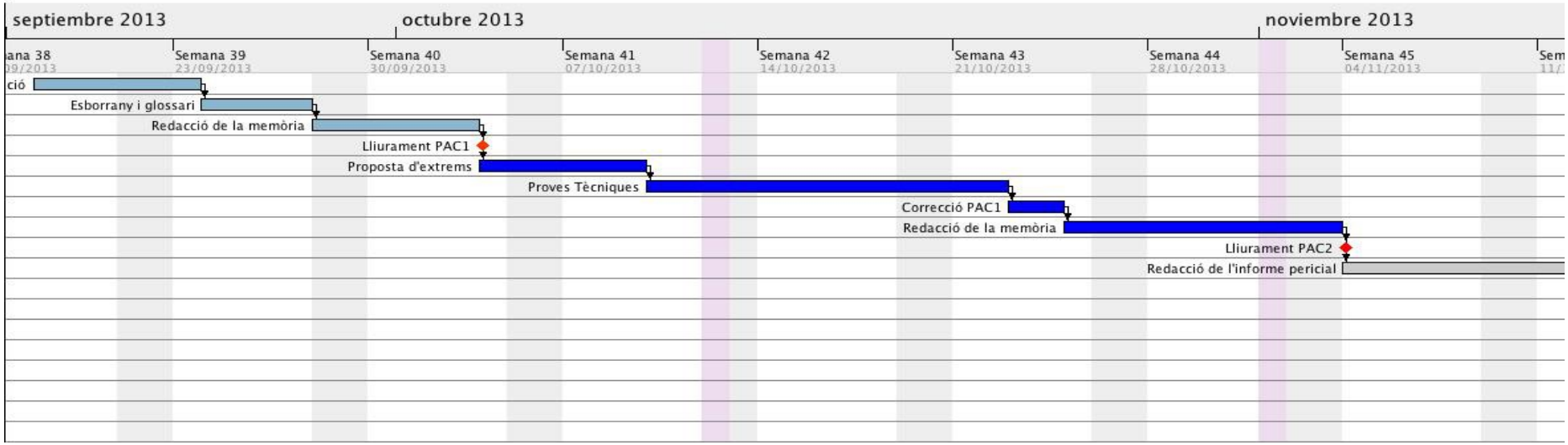
Fita	Descripció
04/10/2013	Data límit per lliurar la PAC1
04/11/2013	Data límit per lliurar la PAC2
11/12/2013	Data límit per lliurar la PAC3
12/01/2014	Data límit per lliurar la Memòria del Treball Final de Màster
12/01/2014	Data límit per lliurar l'Informe Pericial

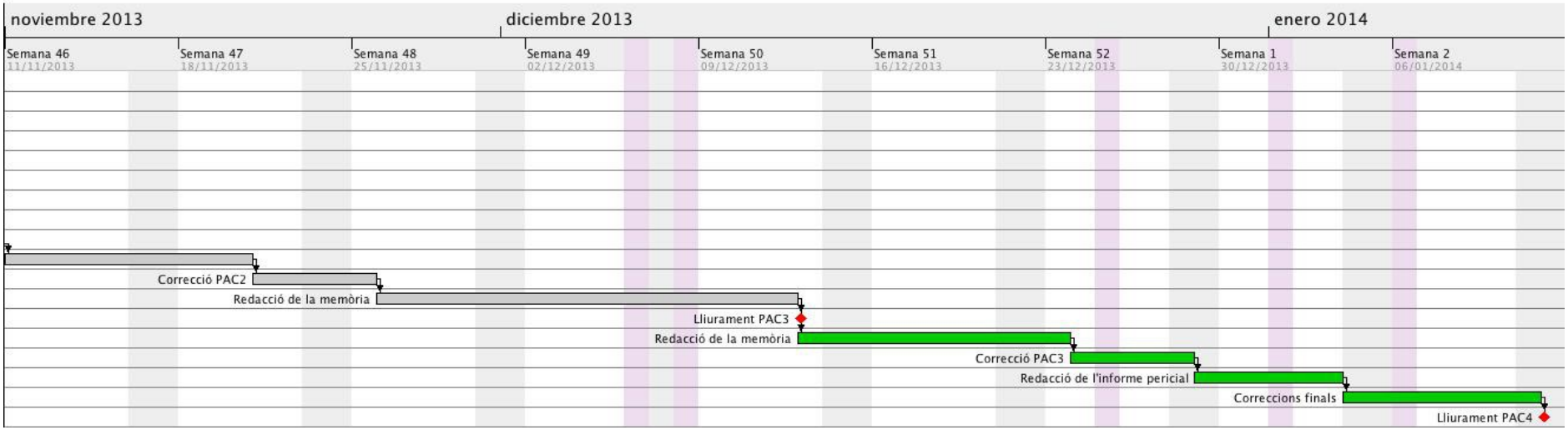
Taula 1. Fites principals

5.3. Calendari de treball

A continuació s'estableix el calendari laboral per a dur a terme el Treball. Aquest calendari estarà format per blocs setmanals, incloent els festius i caps de setmana. L'inici correspon al dimecres **18 de setembre de l'any 2013**, i l'acabament al diumenge **12 de gener del 2014**. Això comporta un total de **21 setmanes i cinc dies**. Tenint en compte que la dedicació al Treball depèn de la càrrega d'altra assignatura, es dedicaran un mínim de **20 hores** setmanals al present Treball. Així doncs, com a mínim, es disposaran de **420 hores**. En qualsevol cas, malgrat s'hagi d'afrontar algun imprevist, s'haurà de respectar el límit màxim de **450 hores** (veure l'apartat 5 d'aquest document).

A la següent pàgina s'adjunta un *diagrama de Gantt* on es mostren totes les activitats del Treball fins al seu lliurament. Es contemplen també les fites principals,


septiembre 2013
octubre 2013
noviembre 2013
Semana 38
09/2013
Semana 39
23/09/2013
Semana 40
30/09/2013
Semana 41
07/10/2013
Semana 42
14/10/2013
Semana 43
21/10/2013
Semana 44
28/10/2013
Semana 45
04/11/2013
ció
Esborrany i glossari
Redacció de la memòria
Lliurament PAC1
Proposta d'extrems
Proves Tècniques
Correcció PAC1
Redacció de la memòria
Lliurament PAC2
Redacció de l'informe pericial


noviembre 2013
diciembre 2013
enero 2014
Semana 46
11/11/2013
Semana 47
18/11/2013
Semana 48
25/11/2013
Semana 49
02/12/2013
Semana 50
09/12/2013
Semana 51
16/12/2013
Semana 52
23/12/2013
Semana 1
30/12/2013
Semana 2
06/01/2014
Correcció PAC2
Redacció de la memòria
Lliurament PAC3
Redacció de la memòria
Correcció PAC3
Redacció de l'informe pericial
Correccions finals
Lliurament PAC4

6. Valoració econòmica

Donat el caràcter educatiu d'aquest Treball, és gairebé irrellevant l'assignació de costos als diferents recursos, tant humans com materials. Podria considerar-se el consum energètic dels diferents equips informàtics, però aquest maquinari estaria funcionant independentment de la realització d'aquest Treball.

S'ha de tenir present, no obstant, que l'autor assumeix els diferents rols que calen per a dur a terme el present Treball. Així doncs, l'autor s'encarrega de les següents tasques:

- Cerca, recopilació i traducció, si escau, d'informació.
- Redacció dels diferents documents: Memòria i Informe pericial.
- Instal·lació de programari i anàlisi de les evidències digitals.

A continuació es pot veure una estimació dels costos d'aquest Treball desglossats per tasques o activitats,

Tasca	Preu/Hora	Hores dedicades	Total
Cerca d'informació	40 €	20 hores	800 €
Redacció Memòria	50 €	160 hores	8.000 €
Anàlisi d'evidències	60 €	60 hores	3.600 €
Peritatge informàtic	80 €	30 hores	2.400 €
Redacció informe pericial	50 €	100 hores	5.000 €
Correccions Finals	50 €	30 hores	1.500 €
Altres	40 €	20 hores	800 €
Total	**-**	**420 hores**	**22.100 €**

Taula 2. Costos totals del Treball

7. Proposta d'extrems

L'objectiu principal d'aquest Treball és l'anàlisi de les evidències digitals rebudes per tal de trobar indicis d'una conducta delictiva per part de les persones detingudes. En aquest apartat, es formulen unes preguntes o hipòtesis que s'hauran de respondre al llarg de la investigació forense i, especialment, amb el resultat final obtingut.

Les preguntes, en un cas judicial com el que ens ocupa, les formularà un jutge o secretari judicial emprant un formulari que el perit forense haurà de contestar mitjançant els resultats obtinguts a la investigació de les evidències digitals; és a dir: l'*informe pericial*.

Les hipòtesis inicials o preguntes a respondre són:

- Determinar si els usuaris de l'ordinador analitzat es dediquen al tràfic, distribució i/o venda de pastilles estupefaents.
- Determinar si els usuaris de l'ordinador analitzat elaboren pastilles estupefaents. En cas positiu, s'haurà de determinar el canal de distribució de les pastilles estupefaents.
- Determinar l'existència de terceres persones que col·laborin en el procés de producció, distribució o venda de les pastilles estupefaents.
- Determinar si existeixen activitats il·legals de falsificació i ús fraudulent de targetes de crèdit.
- Determinar la participació dels usuaris de l'ordinador analitzat en possibles activitats de frau amb targetes de crèdit.
- Determinar l'existència de terceres persones en activitats fraudulentes amb targetes de crèdit.
- Determinar si existeixen altres actes delictius comesos pels usuaris de l'ordinador analitzat.

A banda de les hipòtesis inicials, caldrà definir uns extrems i se'ls ha de trobar una resposta al llarg del procés judicial. Els extrems proposats són:

- Existeixen evidències que confirmen que els usuaris del *PC* analitzat han comés algun acte delictiu?
- Existeixen evidències que confirmen els tipus d'activitats il·lícites que han comés els usuaris de l'ordinador analitzat?
- Existeixen evidències que confirmen la participació de terceres persones en els actes delictius comesos?
- Existeixen evidències que confirmen que els usuaris de l'ordinador analitzat han amagat o destruït possibles proves incriminatòries?

La resposta a aquests extrems és de vital importància de cara al judici i als càrrecs als quals s'enfrontaran les persones detingudes, tot i que com ens indica l'enunciat, en el moment de la detenció es van trobar una gran quantitats de substàncies estupefaents, i es parteix de la premissa que els detinguts s'enfrontaran a una acusació relativament greu, segons la legislació espanyola actual.

8. Proves Tècniques

Aquest capítol descriu les diferents proves tècniques que es realitzaran a les evidències digitals proporcionades amb l'enunciat d'aquest Treball.

Primerament, es descriu amb detall el laboratori o entorn de treball on s'analitzaran les dades. A continuació es presentaran les evidències digitals rebudes i, finalment, les proves realitzades per resoldre aquest Treball i poder realitzar l'informe pericial.

8.1. L'entorn de treball o laboratori

Per realitzar aquest Treball, ha estat necessària la creació d'un mini laboratori forense amb els següents components:

- **Ordinador personal.** L'ordinador personal utilitzat ha estat un *Apple Macbook Pro* de 13.3" model mid-2012 (veure l'Annex B). Aquest ordinador desenvolupa dos rols ben diferenciats:

  - **Consulta d'informació i redacció de documents.** Aquesta tasca consisteix en la consulta, recol·lecció, traducció i classificació de la informació necessària per poder redactar tant aquest document com l'informe pericial resultant. El programari utilitzat ha estat el següent:

    - **Suite Apache OpenOffice 4.0.1.** Aquesta suite ofimàtica gratuïta és imprescindible per poder redactar els documents, en concret s'utilitzat el processador de text inclòs: l'aplicació *Writer*.
    - **Adobe** [8] **Reader X (v 10.1.8).** El visor de fitxers *PDF* per excel·lència. S'ha fet servir per llegir documents i per visualitzar els documents abans del seu lliurament.
    - **Navegador web Safari 6.0.5.** Navegador web desenvolupat per *Apple* [5], el seu ús es necessari per visualitzar les diferents pàgines webs consultades i per enviar els diferents lliuraments al director del Treball.

- **VMWare Fusion v 5.0.3 Professional.** Programari comercial que permet la creació de màquines virtuals. La seva utilització ha estat necessària per poder instal·lar l'entorn de proves. S'ha fet servir una màquina virtual amb *Microsoft* [6] *Windows 7 professional* 64 *bits* com Sistema Operatiu (veure el següent punt: *Realització de proves tècniques*).

- **Realització de proves tècniques.** Aquesta activitat representa la resolució del problema plantejat a l'enunciat d'aquest Treball, i consisteix en l'anàlisi de les evidències digitals que ens han proporcionat. Per realitzar aquesta tasca s'ha fet servir una màquina virtual configurada amb el Sistema Operatiu *Microsoft* [6] *Windows 7*, d'aquesta manera es garanteix la compatibilitat de les aplicacions destinades a l'anàlisi de les dades. Les aplicacions utilitzades són:

  - **Autopsy (i The Sleugh Kit) v 3.0.7.** Es tracta d'un entorn gràfic que facilita l'execució de les comandes de *Sleugh Kit*. És un programari gratuït molt potent a l'hora de realitzar l'anàlisi forense d'una unitat de disc. En el nostre cas, s'utilitzarà per analitzar la imatge del disc dur de l'ordinador dels delinqüents.

  - **Volatility Framework v 2.3.** Són un conjunt d'eines desenvolupades en *Python* amb llicencia *GNU*. Estan pensades per extreure d'una imatge de disc les dades volàtils que hi eren a la *memòria RAM*. En aquest Treball, es farà servir per analitzar el fitxer adjuntat amb el contingut del bolcat de la *RAM* de l'equip trobat al domicili dels detinguts.

  - **Whatsapp Xtract.** Es tracta d'un script desenvolupat en llenguatge *Python*, i gratuït, que permet obrir i consultar les bases de dades de la popular aplicació *Whatsapp.* S'analitzarà el fitxer de dades d'aquesta coneguda xarxa social extret d'un *smartphone* propietat d'un dels dos detinguts.

  - **Event Log Explorer v 4.2.** Aplicació que llegeix i analitza els fitxers d'events (logs) d'un sistema Windows. Es tracta d'una eina comercial, però es disposa d'una llicencia gratuïta per ús personal.

  - **WinMD5Free v 1.20.** Es tracta d'una eina molt senzilla que ens calcula el *Hash* de diversos fitxers i ens permet fer una comparació amb els *Hashes* que ens han proporcionat.

  - **John the ripper.** Eina molt coneguda que s'utilitza per *'crackejar'* les contrasenyes trobades fent servir força bruta.

- **Hacha v 4** i **Winzip v 16.0.** Aquest dos programes ens permetran extreure tant la imatge del disc dur com el bolcat de la *memòria RAM* que s'han d'analitzar per complir els objectius d'aquest Treball.

- **Windows Registry Recovery v 1.5.2.0.** Eina molt útil per llegir els diferents arxius que formen el registre de Windows i que permet navegar per les diferents claus d'una manera senzilla i clara.

- **USBDeview v 2.27.** Petita utilitat que mostra tota la informació possible dels diferents dispositius que han estat connectats als ports USB d'un ordinador.

- **ProDiscover Basic v 7.4.0.14.** Programa molt senzill molt similar a l'*Autopsy.* Té algunes opcions bàsiques molt més interessants i consumeix menys recursos.

- **SQLite Spy 1.9.6.** Programari *freeware* que permet la gestió de bases de dades: visualització, edició, creació, indexació i l'execució de sentències en llenguatge *SQL*. Eina molt senzilla i molt potent.

- **Apple iPad.** La seva funció principal és cercar informació i mostrar documents a l'hora de redactar aquest Treball. D'aquesta manera, ha estat possible treballar amb les 13.3 polsades de pantalla de l'ordinador principal de manera còmoda. Les aplicacions que s'han fet servir són:

  - **Navegador web Safari per a iOS 5.1.1.** Aquesta eina es imprescindible per la cerca d'informació a Internet.

  - **iBooks 3.1.3.** Aplicació d'*Apple* [5] que permet la lectura de llibres en format electrònic així com documents en format *PDF*.

- **Connexió de banda ampla a 10 Mbps, *ADSL*, de Telefònica.** Per a la cerca d'informació, comunicacions amb el director del projecte i lliurament de les diferents proves d'avaluació continuada i de la memòria i l'informe pericial, s'ha fet servir una connexió a Internet *ADSL* amb una velocitat teòrica de 10 Mbps.

8.2. Les evidències digitals

En aquest Treball es demana fer l'estudi de les evidències digitals procedents d'un *PC* que, presumptament, està vinculat una conducta delictiva. Juntament amb l'enunciat s'han rebut deu fitxers que hauran de ser analitzats amb la finalitat de trobar evidències dels delictes que s'han comés.

A continuació es pot observar una taula amb la descripció de cadascun dels fitxers que s'han d'analitzar,

Nom del fitxer	Mida (en bytes)	Grup o tipus de fitxer
hd_dd.zip.H00	49	Imatge del disc dur (fitxer principal)
hd_dd.zip.H01	672723296	Imatge del disc dur (dades)
hd_dd.zip.H02	672723296	Imatge del disc dur (dades)
hd_dd.zip.H03	672723296	Imatge del disc dur (dades)
hd_dd.zip.H04	672723296	Imatge del disc dur (dades)
hd_dd.zip.H05	672723296	Imatge del disc dur (dades)
hd_dd.zip.H06	672723295	Imatge del disc dur (dades)
Hash_MD5.ttxt	336	*Hashes* dels fitxers anteriors *
ram_adq.rar	163182910	Bolcat de la *memòria RAM*
whatsapp.db	26624	BBDD d'un xat extreta d'un *smartphone*

Taula 3. Fitxers d'evidències digitals a analitzar

Els fitxers a analitzar es poden classificar en tres grups que es complementen entre ells, de manera que a partir de les dades extretes d'un, es poden cercar proves als altres dos grups.

Les evidències digitals proporcionades són les que podem observar a la següent captura,

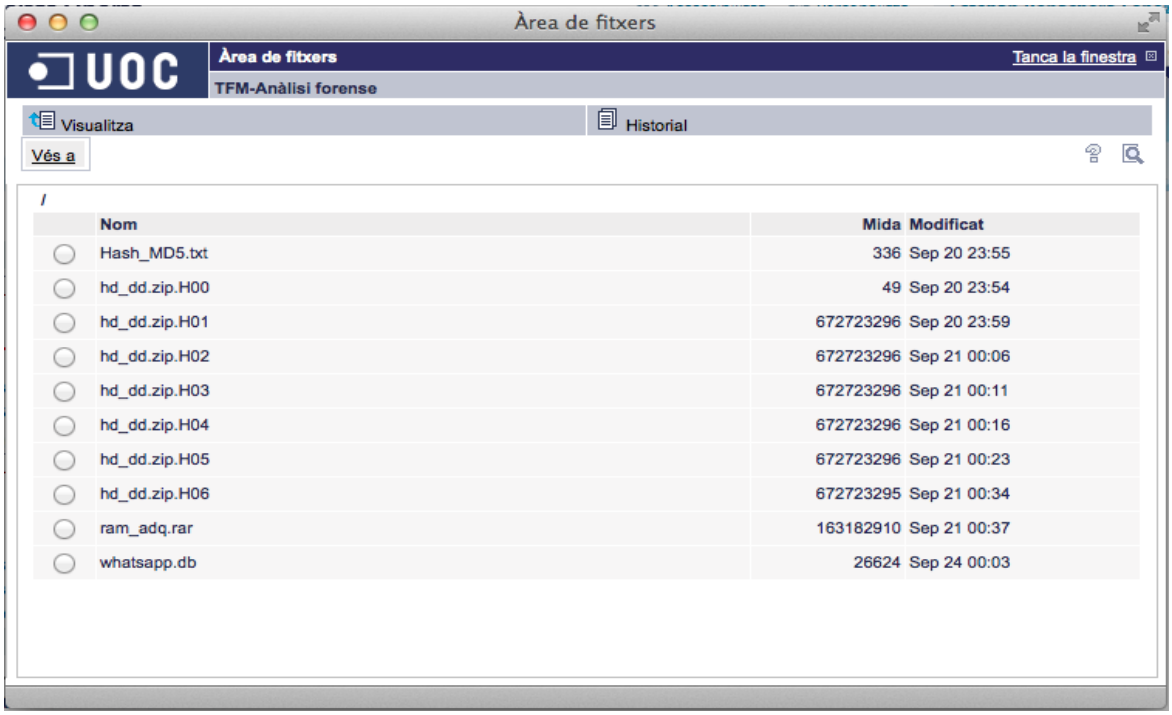


Figura 2. Fitxers proporcionats a l'aula per realitzar aquest Treball

***** El fitxer **Hash_MD5 txt** conté els *Hashes*, calculats fent servir l'*algoritme criptogràfic MD5*, que ens assegurarà que els arxius no han estat alterats. S'hauria de recalcular el *Hash* de cada fitxer i fer una comparació amb els *Hashes* proporcionats per tenir la certesa de treballar amb les dades originals.

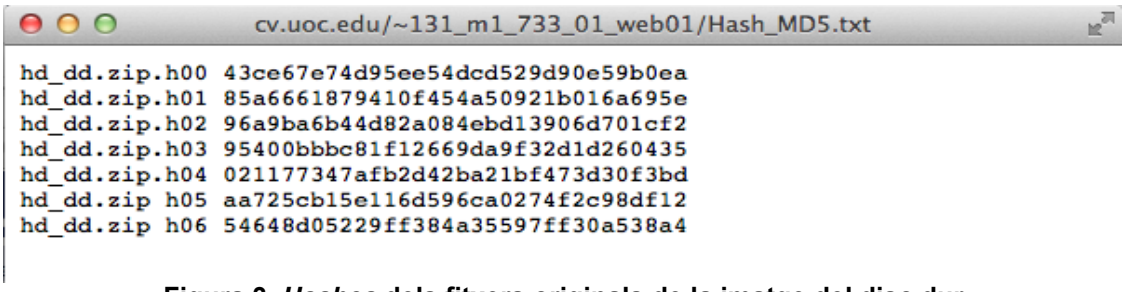


Figura 3. *Hashes* dels fitxers originals de la imatge del disc dur

8.3. Les proves tècniques realitzades

Aquest punt descriu els diferents tipus de proves que es realitzen al llarg de la investigació forense per poder donar resposta a les preguntes o hipòtesis inicials definides a l'apartat 7.

Per aconseguir l'objectiu d'aquest Treball, trobar evidències d'una conducta delictiva de les persones detingudes, s'hauran de realitzar una sèrie de proves tècniques a les evidències digitals. Aquestes proves es classifiquen en tres grans grups que es descriuen a continuació:

- **Estudi del sistema operatiu.** Inclou les següents informacions:

  - Identificació del sistema operatiu i la versió executada.
  - Identificació de la data d'instal·lació del sistema.
  - Identificació dels usuaris del sistema i permisos que té cadascun d'ells.
  - Data d'accessos a l'equip i als seus fitxers.
  - Identificació del hardware i del software instal·lat a l'equip.

- **Recuperació dels fitxers eliminats.** Realitzar la recuperació de la informació eliminada al disc dur examinat, doncs aquestes dades poden ocultar activitats il·lícites dels propietaris del sistema analitzat.

- **Anàlisi detallat de les evidències digitals.** Es realitzarà un estudi en profunditat dels fitxers d'evidències proporcionats amb l'enunciat:

  - **Anàlisi de la base de dades d'un popular programa de xat extreta d'un smartphone propietat d'una de les persones detingudes.** Aquest anàlisi es farà obrint la base de dades amb l'script *Whatsapp Xtract* i llegint les diferents converses per tal d'obtenir informació sobre qualsevol indici d'activitats delictives.

- **Anàlisi de l'imatge del disc dur de l'ordinador analitzat.** Es carregaran els fitxers resultants de la clonació del disc dur de l'equip propietat dels detinguts a l'entorn *Autopsy v 3.0.7*. i es realitzarà un exhaustiu anàlisi de les dades que conté. Es buscaran arxius que demostrin una conducta delictiva de les persones detingudes.

- **Anàlisi del fitxer de bolcat de la *memòria RAM.*** S'analitzarà l'arxiu de dades de memòria **ram_adq.rar** fent servir el programari *Volatility Framework v 2.3*. La finalitat d'aquest anàlisi es obtenir les credencials, contrasenyes i/o dades dels processos que s'executaven a l'ordinador propietat dels detinguts. També s'analitzaran els arxius d'hibernació, paginació i arxius d'intercanvi (*swap*) continguts a l'imatge del disc dur.

** **NOTA.** Tant l'apartat 8.2, Les evidències digitals, com l'apartat 8.3, Les proves tècniques realitzades, es troben àmpliament desenvolupats a l'informe pericial.

9. Conclusions

Un cop finalitzat el present Treball, és hora de fer una valoració de les tasques que s'han realitzat i dels resultats que s'han obtingut.

En referència a les tasques que s'han realitzat, ha estat força interessant conèixer les eines i els procediments que es fan servir en aquesta disciplina: la informàtica forense. Una mica més difícil ha resultat la realització i redacció de l'informe pericial, doncs el fet de tenir que enllaçar els descobriments que apareixien al analitzar els fitxers que se'ns van proporcionar per reconstruir uns fets que, a priori, semblaven evidents, mantenint un cert ordre i una certa coherència ha estat molt difícil. No obstant això, amb les evidències que es localitzen a les imatges analitzades

A nivell més personal, he gaudit molt realitzant aquest Treball Final de Màster, tot i que a priori, ho veia molt complicat. Per sort, el fitxer **whatsapp.db** ens ha facilitat molt la feina, ja que quedava molt clar que l'usuari Juan Solo havia comés un dels delictes i, a més ens proporcionava els col·laboradors i el *modus operandi* d'aquests delinqüents.

Pel que fa a la Nadine i la seva participació en aquest delicte, sempre he dubtat. Vaig pensar que l'usuari Juan Solo entrava al sistema amb les credencials de l'usuari Nadine per realitzar totes les tasques relacionades amb les targetes de crèdit falses: obtenir numeracions, ocultar les numeracions a dins d'un fitxer d'imatge, etc. Però el fet de trobar missatges de correu electrònic enviats per la Nadine a una tercera persona anomenada Irina Luhn (curiosament té el mateix cognom que l'inventor de l'algoritme de Luhn) i l'enviament de les numeracions de les targetes de crèdits, em va obligar a canviar d'opinió.

La trama es complica una mica més perquè, aquesta tercera persona, la Irina, apareix a un fitxer de xat del programari *Skype* i, la conversa, entre ella i l'usuari Juan Solo, és una compra de drogues, i la posterior cita per realitzar la transacció. Amb això, i amb les fotografies i fitxers *Word*, ja tenim les proves suficients per relacionar a l'usuari Juan Solo amb el delicte d'elaboració, distribució i venda de substàncies estupefaents.

Finalment, haig de dir que, tot i que ens proporciona molta informació, el fitxer **whatsapp.db** pot causar certa confusió. En alguns dels xats que conté aquest arxiu, apareix com propietari del telèfon mòbil un nom que no es correspon amb Juan Solo, a banda de tractar-se de missatges intercanviats entre estudiants i no guarden cap relació amb els fets investigats. També es va trobar una incongruència a la cadena de custodia: la data de copia del disc dur era molt anterior a la data de captura de la *memòria RAM*. Tot i que vaig pensar que s'havia de rebutjar aquest fitxer, vaig continuar i realitzar l'anàlisi, però he inclòs aquest fet a l'informe pericial.

10. Desviacions en la planificació original i dificultats trobades

Al llarg de la realització d'aquest Treball, no s'ha produït cap desviació temporal a l'hora de realitzar les tasques descrites a l'Apartat 5: Pla de Treball. La decisió d'anar aplicant les correccions i les recomanacions del Director del projecte en el mateix moment que eren rebudes, han evitat l'acumulació de feina *d'última hora*. Aquesta metodologia de treball ha permet que es compleixin tots els terminis establerts a la PAC1, fent possible el compliment dels objectius prefixats

Pel que fa a les dificultats trobades a l'hora de realitzar les proves tècniques, cal destacar la instal·lació i la posterior utilització de l'eina *Volatility.* Tot i disposar tant d'un maquinari com d'una versió de *Microsoft Windows 7* de 64 *bits*, algunes llibreries de *Python* no funcionaven correctament. Cercant a *Google* [4] es va localitzar una pàgina web que detallava la instal·lació, partint des de zero, de totes les eines necessàries per poder tenir operatiu el *Framework* de *Volatility*. La consulta dels paràmetres que cal utilitzar i l'estudi de diversos exemples a Internet van permetre, finalment, la cerca i extracció de la informació desitjada del fitxer que conté el bolcat de la *memòria RAM* de l'equip que s'ha analitzat.

Finalment, cal afegir que l'anàlisi del fitxer **whatsapp.db** ha facilitat enormement la feina, doncs a dins d'uns dels xats que conté queda molt clar que una de les persones detingudes ha comés un dels delictes que s'investiguen, entre d'altres delictes menors. Per tant, el fet d'analitzar aquest fitxer abans de començar, va servir de guia per cercar la informació necessària per poder realitzar aquest Treball amb èxit.

11. Annex A. Evidències digitals

Casey [9] defineix l'evidència digital com *"qualsevol dada que pot establir que un crim s'ha executat (commit) o pot proporcionar un enllaç (link) entre un crim i la seva víctima o entre un crim i el seu autor"*.

"Qualsevol informació, que subjecta a una intervenció humana o una altra semblant, ha estat extreta d'un mitjà informàtic".

Tipus d'evidència digital

Les evidències digitals es poden classificar en dos grans grups:

- **Constant.** És l'evidència emmagatzemada en un mitjà informàtic i que es manté preservada després d'apagar el sistema.

- **Volàtil.** Evidència que es troba emmagatzemada temporalment, a la *memòria RAM*, o a la memòria cau, i al interrompre l'alimentació elèctrica la evidència es perd. Aquest tipus d'evidència es deu recuperar d'immediat i ha de ser guardada a un fitxer, d'aquesta manera es convertirà en una evidència no volàtil.

És important considerar la diferència existent entre l'evidència electrònica i l'evidència digital, la primera es refereix als aparells electrònics (telèfons mòbils, *PDAs*, agendes electròniques, etc.) i la segona a la informació digital que aquests dispositius contenen.

Classificació de l'evidència digital

- **Evidència Física**

  - **Suports d'emmagatzematge**
    - Discos durs
    - Disquets
    - *CD-ROMs*, *DVD*
    - Cintes magnètiques, etc.

  - **Dispositius electrònics**
    - Telèfons mòbils
    - Agendes electròniques

  - **Dispositius de comunicacions de xarxa**
    - *Routers*
    - *Switches*
    - *Hubs*

- **Evidència lògica.** Qualsevol dada emmagatzemada o generada en un mitjà magnètic.

  - **Registres generats per ordinador.** Aquest registres són generats com efecte de la programació d'un ordinador i són inalterables per una persona, s'anomenen registres d'esdeveniments de seguretat (*logs*).

- **Registres emmagatzemats en un ordinador.** Aquests registres són generats per una persona i es guarden a un ordinador, per exemple, un document generat amb un processador de text.

- **Registres híbrids.** Aquests registres inclouen tant registres generats per ordinador com els emmagatzemats al sistema.

- **Registres de cada servidor.** Són els registres del sistema i els de cada programa en execució, per exemple, els registres del servidor *Web Apache*.

- **Registres de tràfic de xarxa.** Registres que emmagatzemen l'activitat de xarxa, i les comunicacions, del sistema.

- **Registres d'aplicació.** Són els registres que cada aplicació guarda sobre l'accés dels usuaris, els errors produïts i la informació sobre les activitats de cada usuari dins l'aplicació.

Fonts de l'evidencia digital

Les fonts d'evidència digital poden ser:

- **Sistemes de computació oberts.** Estan formats per ordinadors personals i servidors amb els seus perifèrics. Són una font d'evidència digital molt important ja que emmagatzemen gran quantitat d'informació als seus discos durs.

- **Sistemes de comunicació.** Engloben les xarxes de telecomunicacions, *Internet* i comunicacions sense fils.

- **Sistemes convergents de computació.** Formats per telèfons mòbils, *PDAs*, targetes intel·ligents, etc.

12. Annex B. Entorn de Treball

A continuació es poden observar les característiques de l'equip que s'ha fet servir per realitzar aquest Treball,

Figura 4. Característiques de l'ordinador

El rol principal d'aquest ordinador ha estat la redacció dels dos documents que conformen aquest *Projecte Final de Màster*: La *Memòria* (aquest document) i l'*Informe pericial*. Així mateix, s'ha utilitzat una màquina virtual amb sistema operatiu *Microsoft* [6] *Windows 7* per poder descarregar les evidències digitals des de l'àrea de fitxers de l'aula i instal·lar les eines que es fan servir per analitzar les dades.

Es pot consultar la pàgina web del fabricant per obtenir més informació de l'equip utilitzat: http://store.apple.com/es/buy-mac/macbook-pro

Detall de la redacció d'aquest document amb l'eina de codi obert *OpenOffice*,

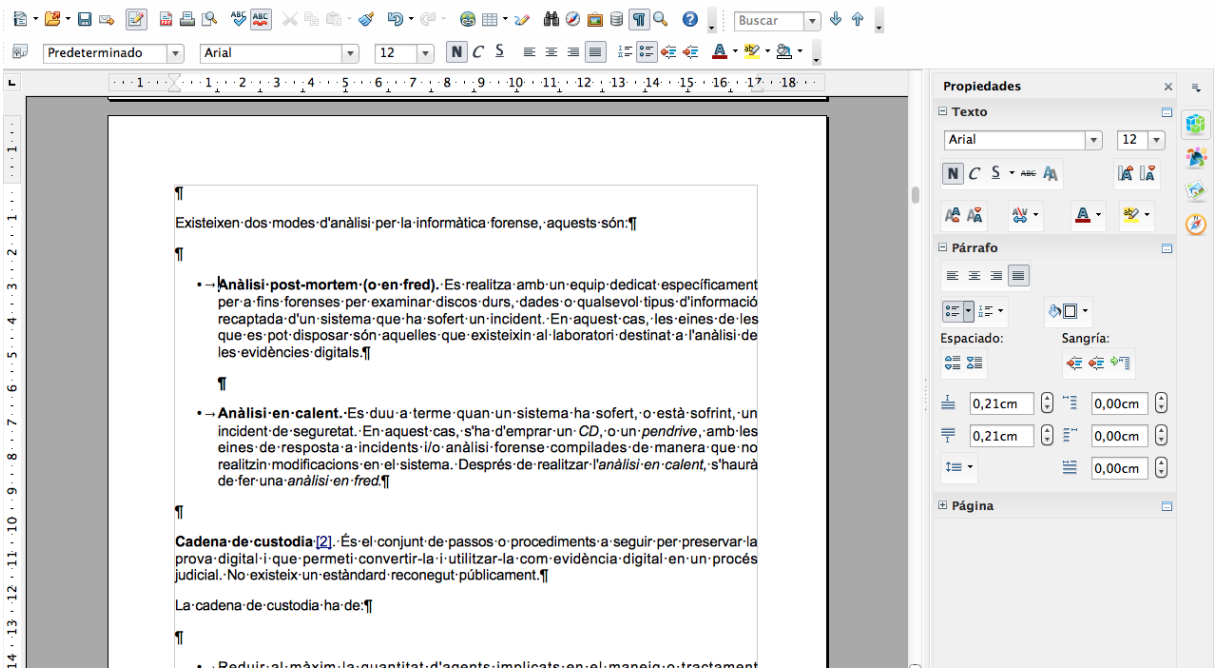


Figura 5. Vista de la redacció de la Memòria

Captura de la pantalla principal de l'aplicació de virtualització i característiques principals de la màquina que s'ha utilitzat per realitzar les proves tècniques,

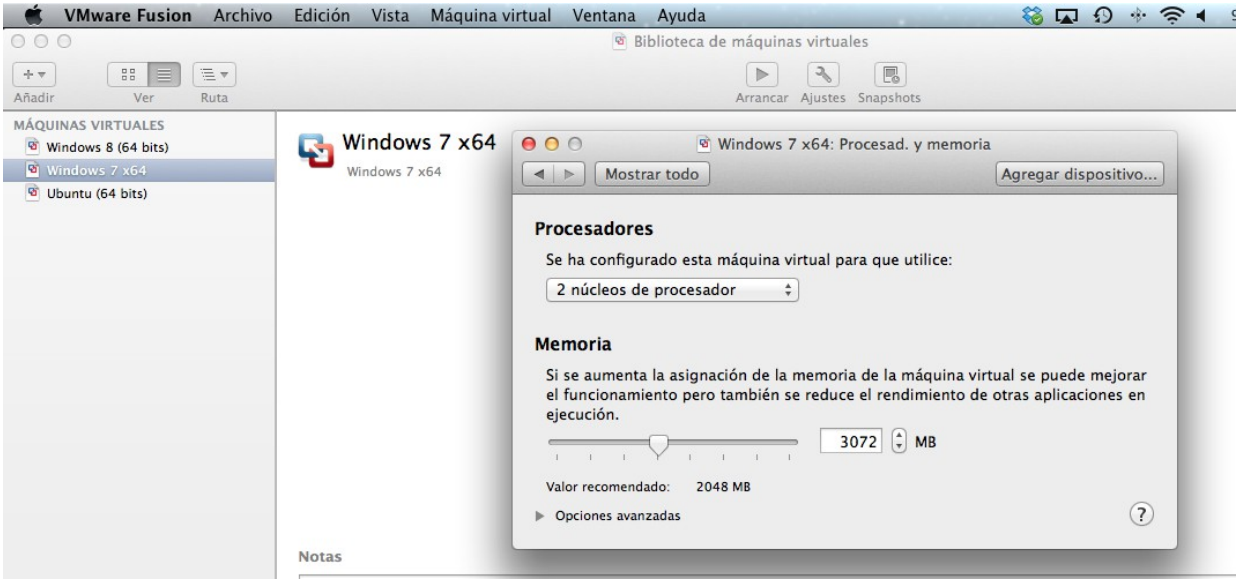


Figura 6. Característiques de la màquina virtual

A la següents captures es pot observar la màquina virtualitzada en funcionament, amb el sistema operatiu carregat, i la carpeta de treball amb les dades a analitzar,

Figura 7. Càrrega del sistema Windows a la màquina virtual

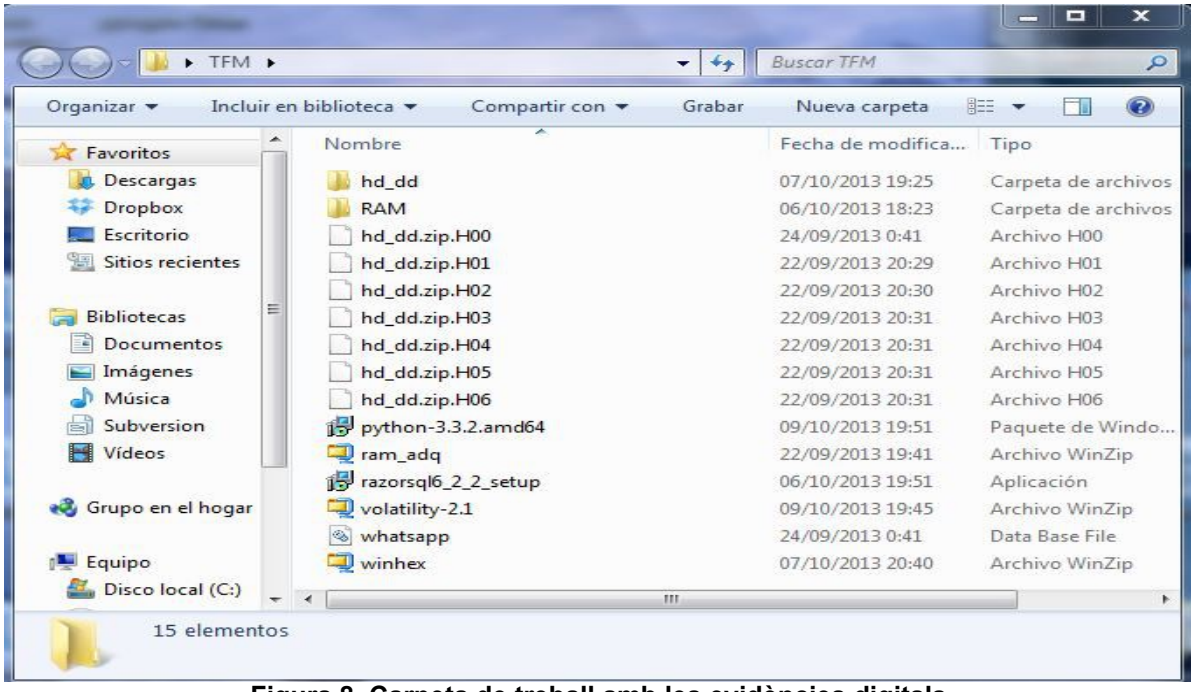


Figura 8. Carpeta de treball amb les evidències digitals

13. Annex C. Proves tècniques: Comprovació d'evidències

Per tal d'assegurar que les evidències digitals rebudes no han estat alterades, s'ha de calcular els *Hashes* dels arxius que ens han proporcionat i comparar-los amb els *Hashes* inclosos a la cadena de custodia. Aquests càlculs es realitzen amb l'eina gratuïta *WinMD5Free v1.20*.

A les següents captures es pot observar aquest procés amb els fitxers d'imatge del disc dur analitzat,

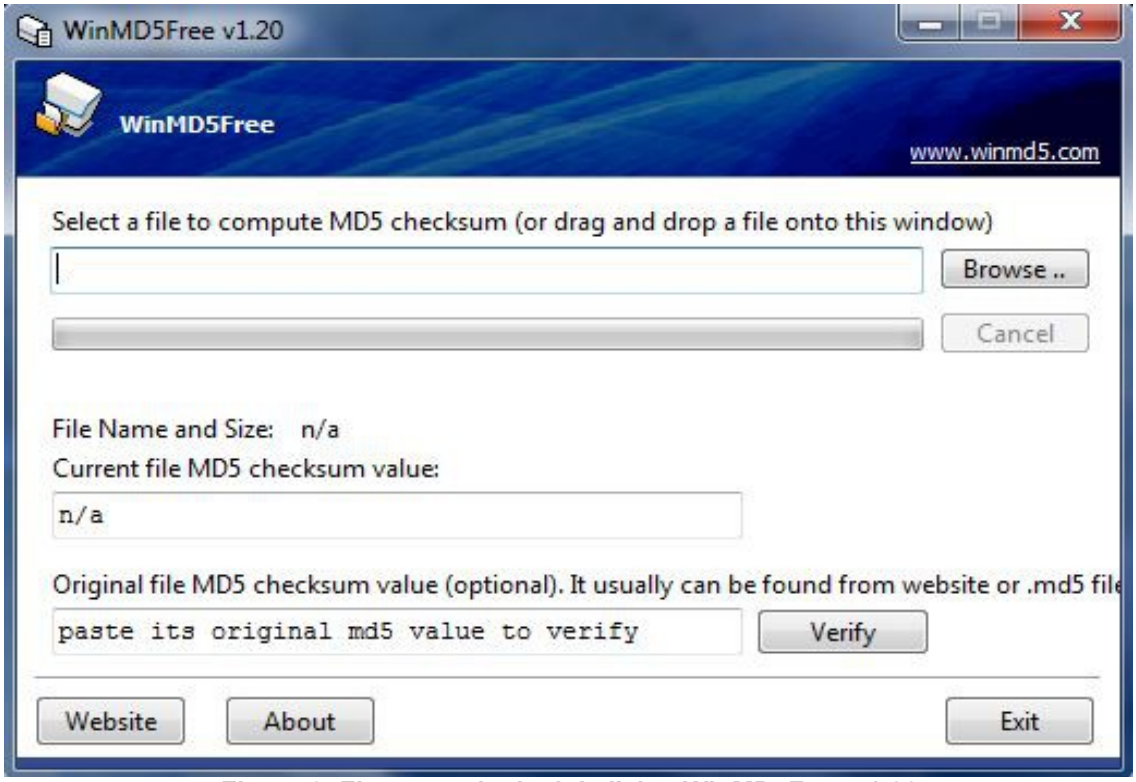


Figura 9. Finestra principal de l'eina WinMD5Free v1.20

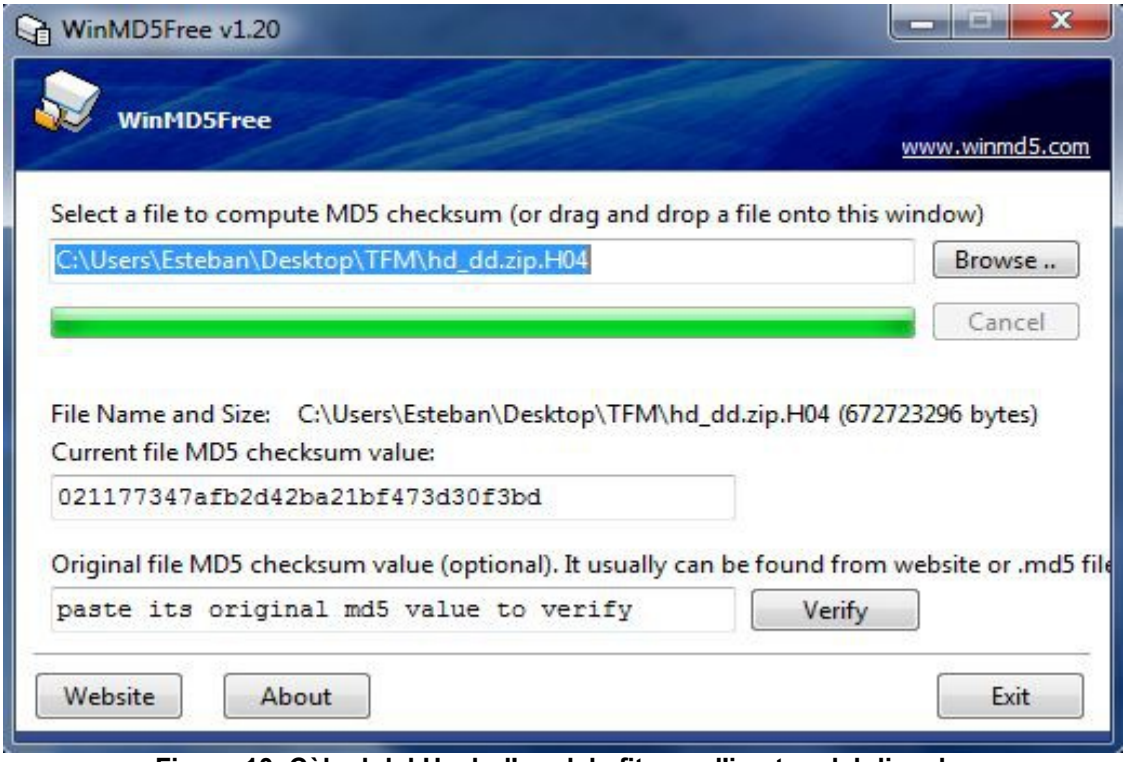


Figura 10. Càlcul del Hash d'un dels fitxers d'imatge del disc dur

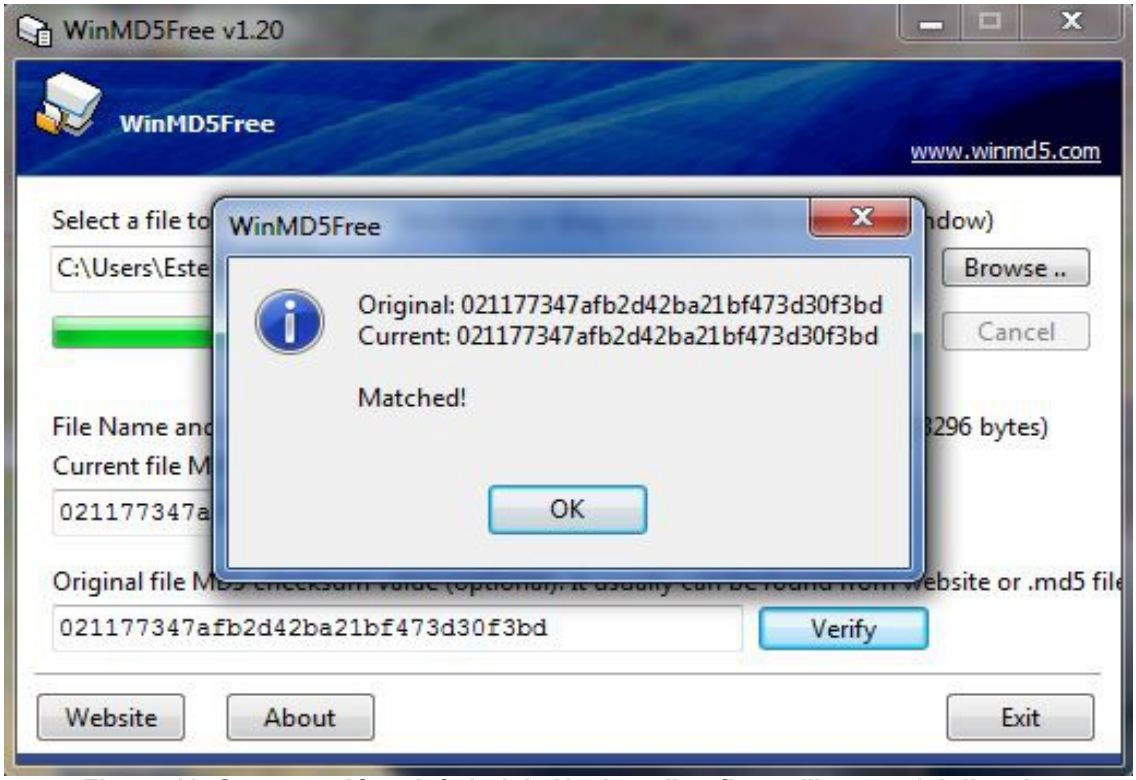


Figura 11. Comparació amb èxit dels Hashes d'un fitxer d'imatge del disc dur

Seguidament, es repeteix el procés amb el fitxer que conté el bolcat de la memòria RAM de l'ordinador analitzat,

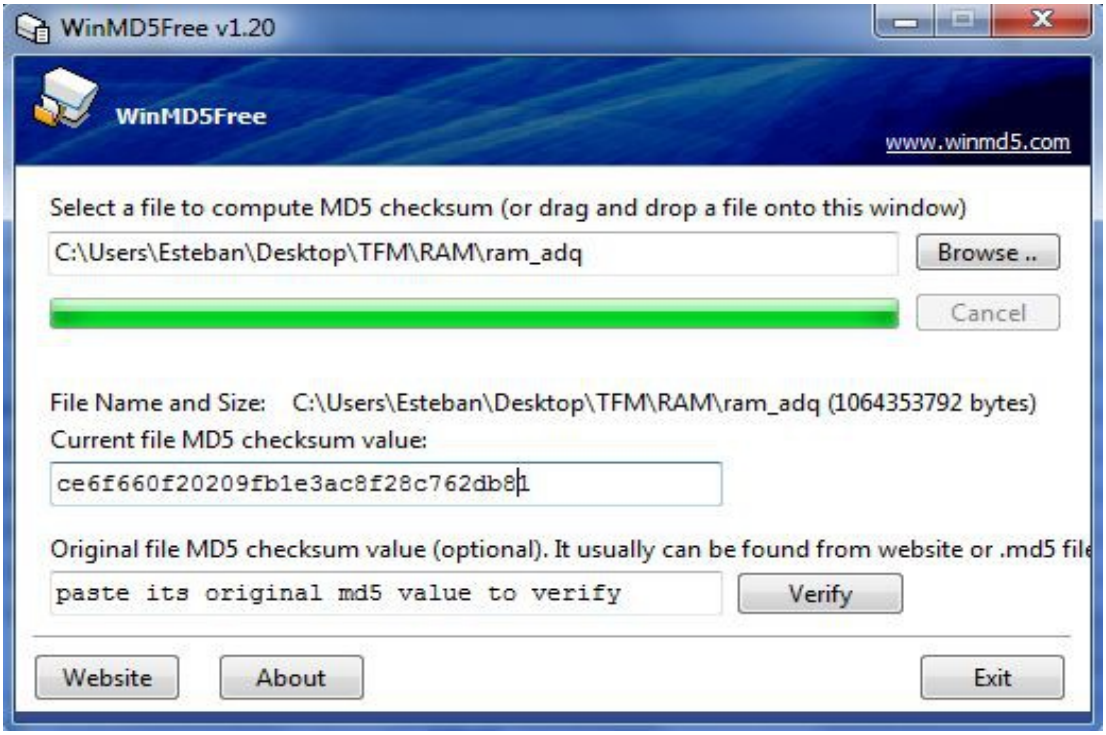


Figura 12. Càlcul del Hash del bolcat de la memòria RAM

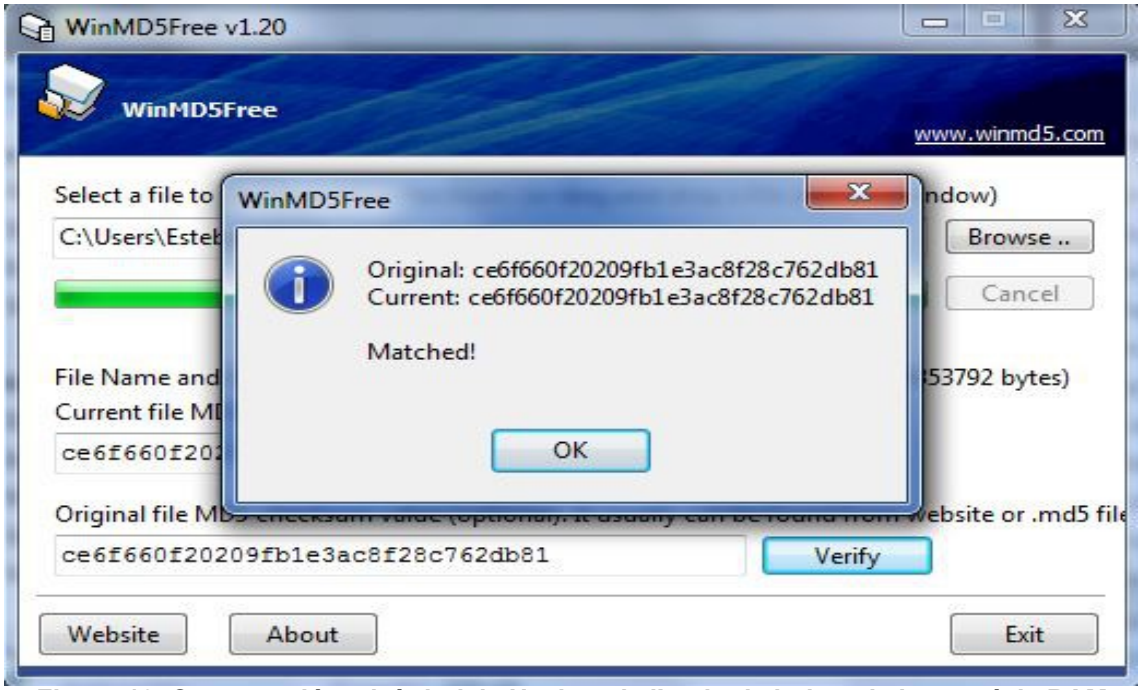


Figura 13. Comparació amb èxit dels Hashes de l'arxiu de bolcat de la memòria RAM

14. Annex D. Proves tècniques: Informació del sistema analitzat

Es realitza l'anàlisi del contingut de la *memòria RAM* emmagatzemat al fitxer **ram_adq**. Es fa servir l'eina *Volatility*, que permet extreure informació de l'activitat del sistema analitzat.

Primerament, s'obté la informació relativa al sistema operatiu executat,

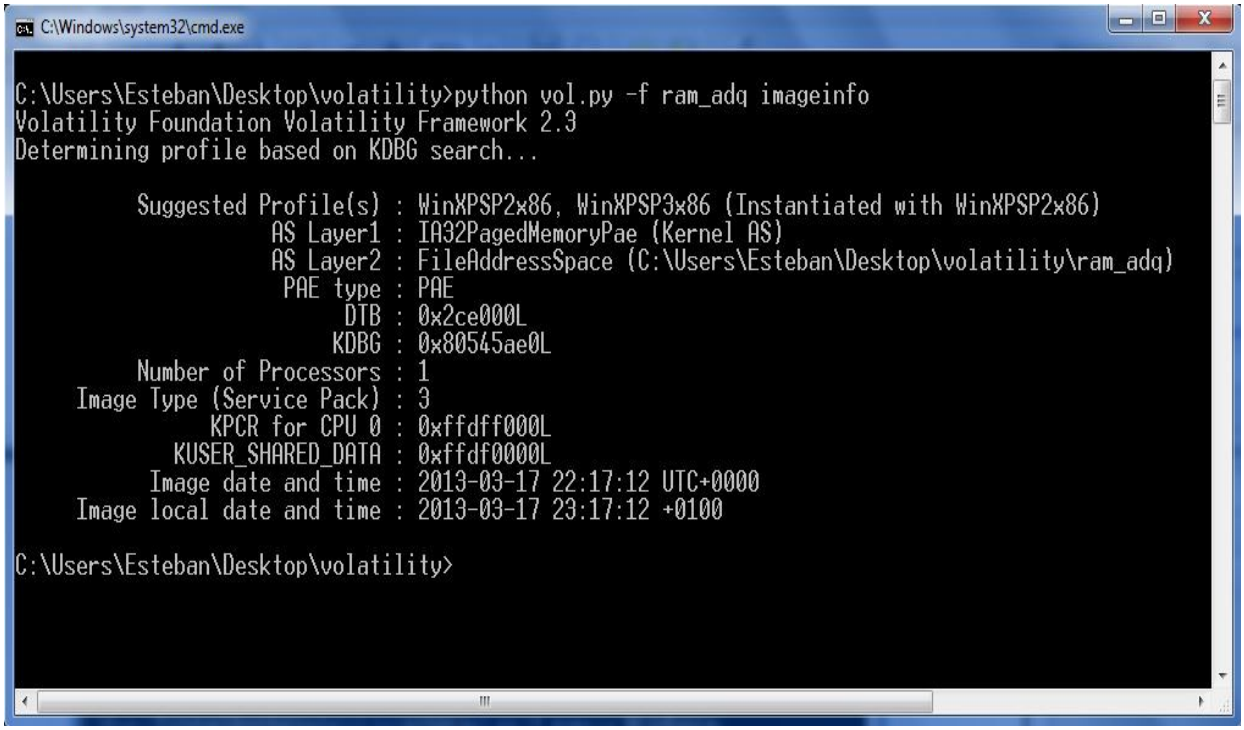


Figura 14. Informació del sistema operatiu executat a l'ordinador analitzat

A la imatge anterior es pot observar que el sistema analitzat executa la versió de 32 *bits* de *Microsoft Windows XP amb el Service Pack 3*. També es veu que es tracta d'un sistema amb només un microprocessador (i amb un sol nucli).

La següent captura mostra la informació anterior ampliada,

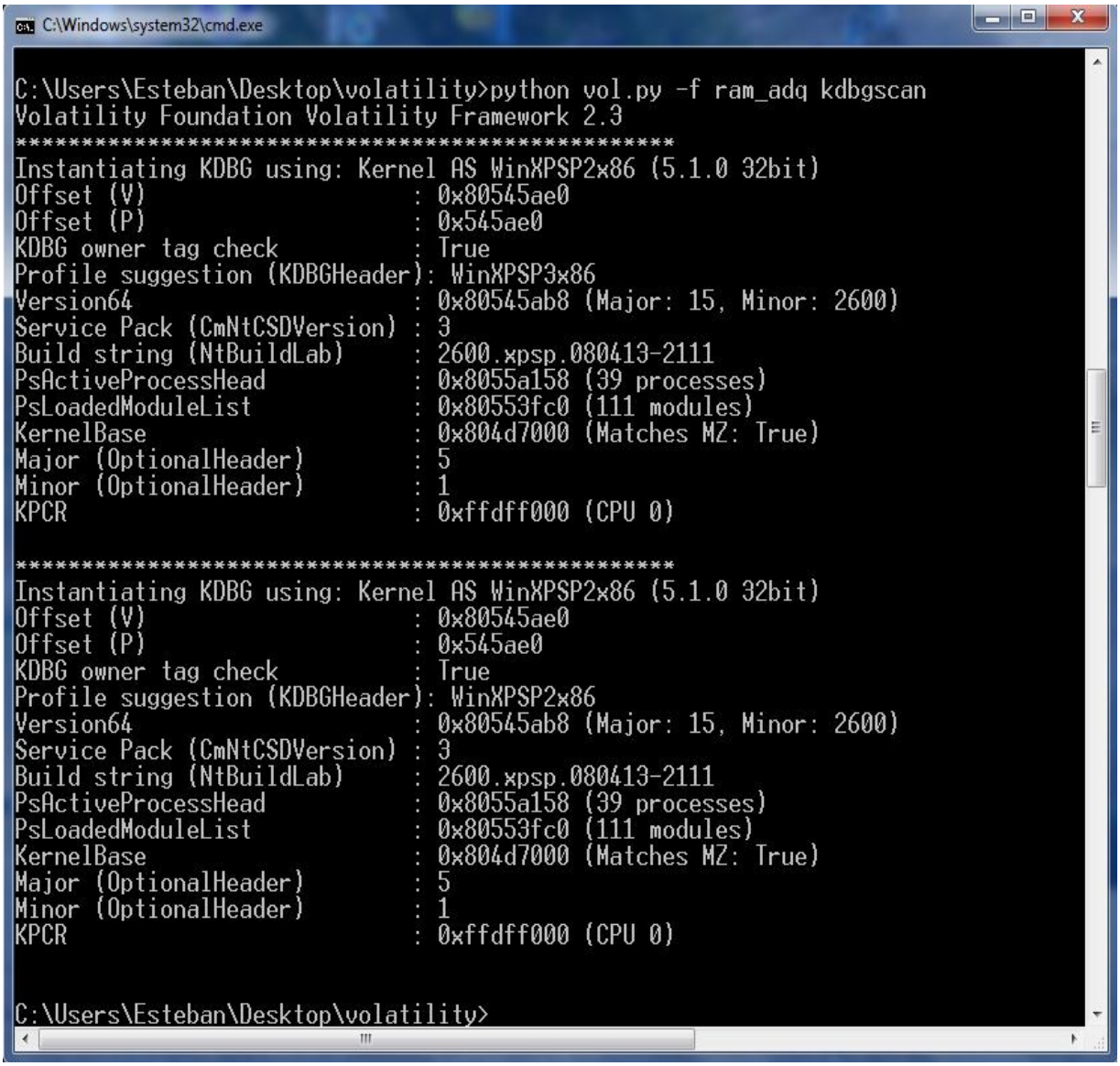


Figura 15. Informació ampliada del sistema

Seguidament, s'analitzen els processos en execució en el moment de realitzar el bolcat de memòria. Aparentment, no es troben processos estranys o rellevants en execució. Les dependències dels processos en execució, es poden observar a la següent captura,

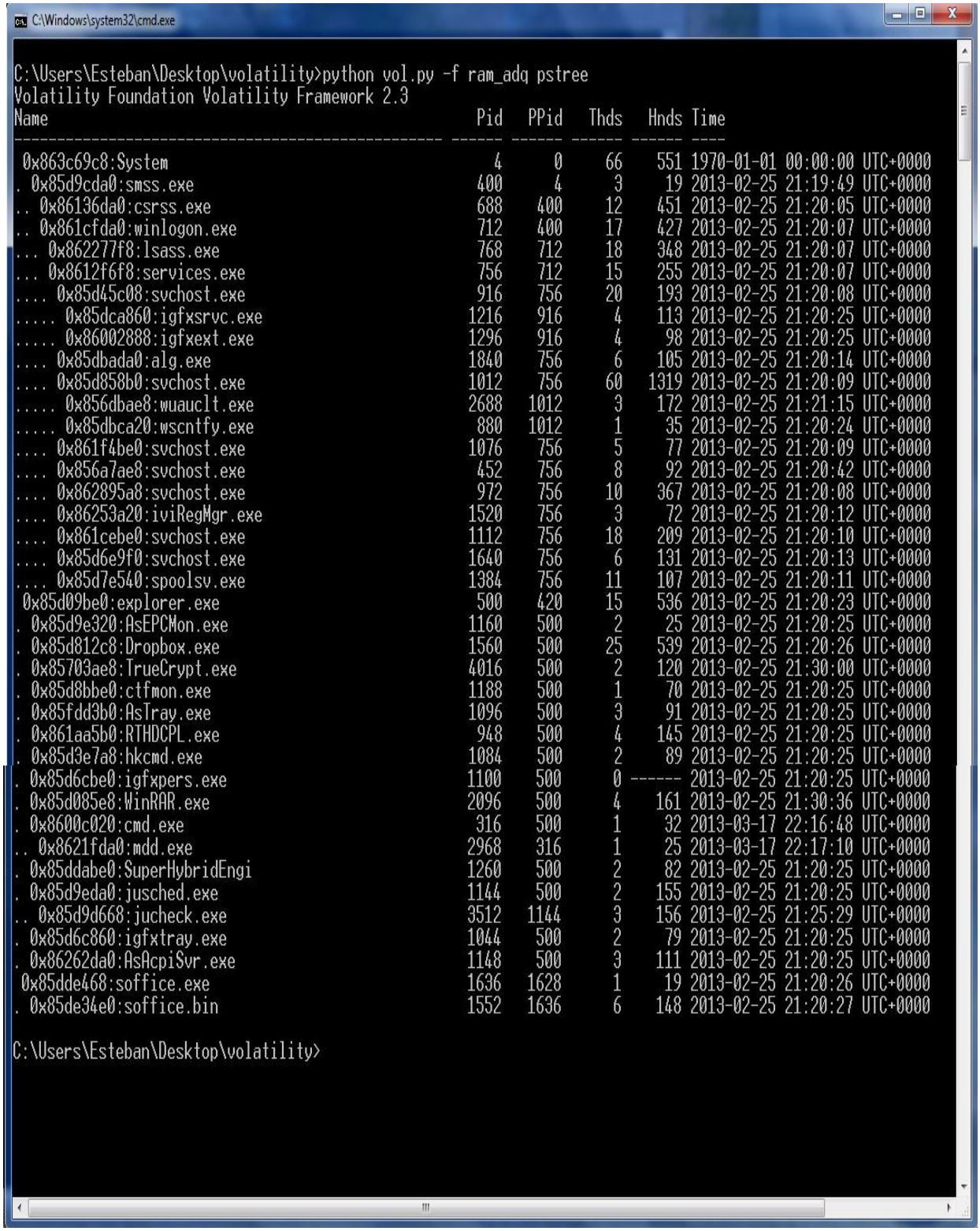


Figura 16. Arbre de processos en execució a la màquina analitzada

També s'analitzen les connexions i els serveis de xarxa, incloent els ocults. S'observa que l'ordinador analitzat té assignada l'*adreça IP* **192.168.1.12**, de tipus privada, i no s'aprecien signes de connexions remotes (intrusions, control remot, *botnet,* etc.).

Les *adreces IP* remotes pertanyen als servidors de *Dropbox* i a *Akamai Technologies*, l'empresa que permet distribuir continguts a *Google* [4], *Microsoft* [6] i *Yahoo!*, entre d'altres gegants d'Internet.

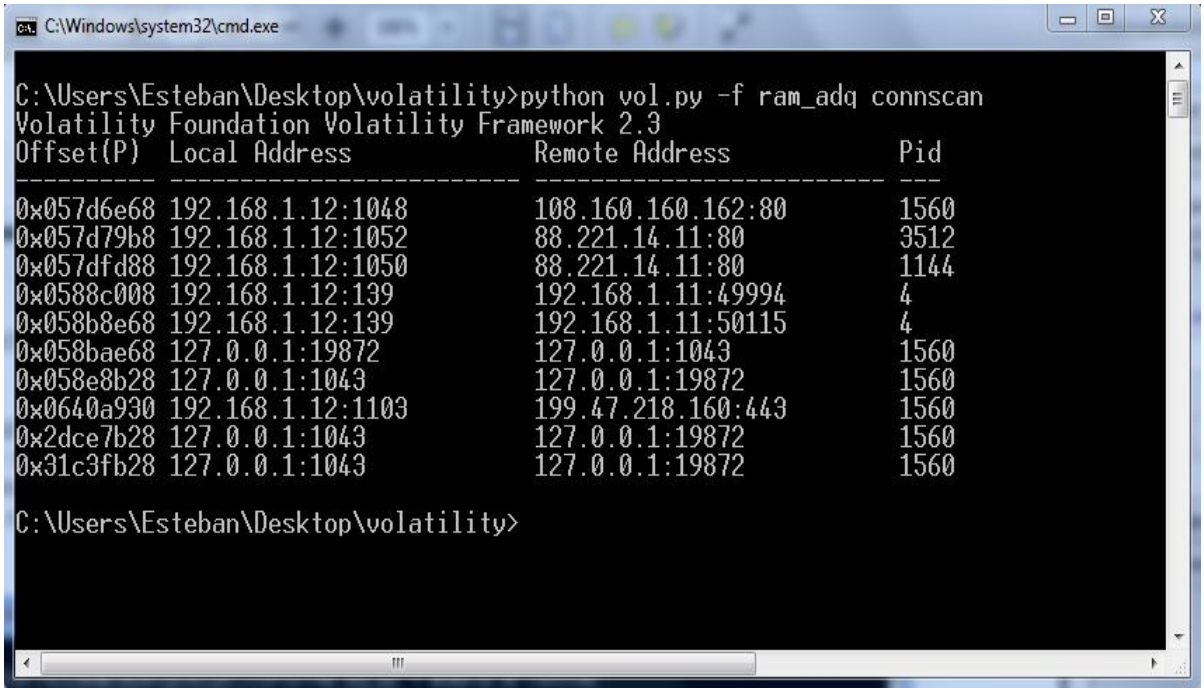


Figura 17. Detall de les connexions de xarxa

A continuació s'analitzen els *sockets* actius i aquells que, tot i haver estat tancats, han deixat rastres a la memòria del sistema. No s'observen evidències de connexions remotes tipus *netcat*. A les següents captures es mostren els *sockets,*

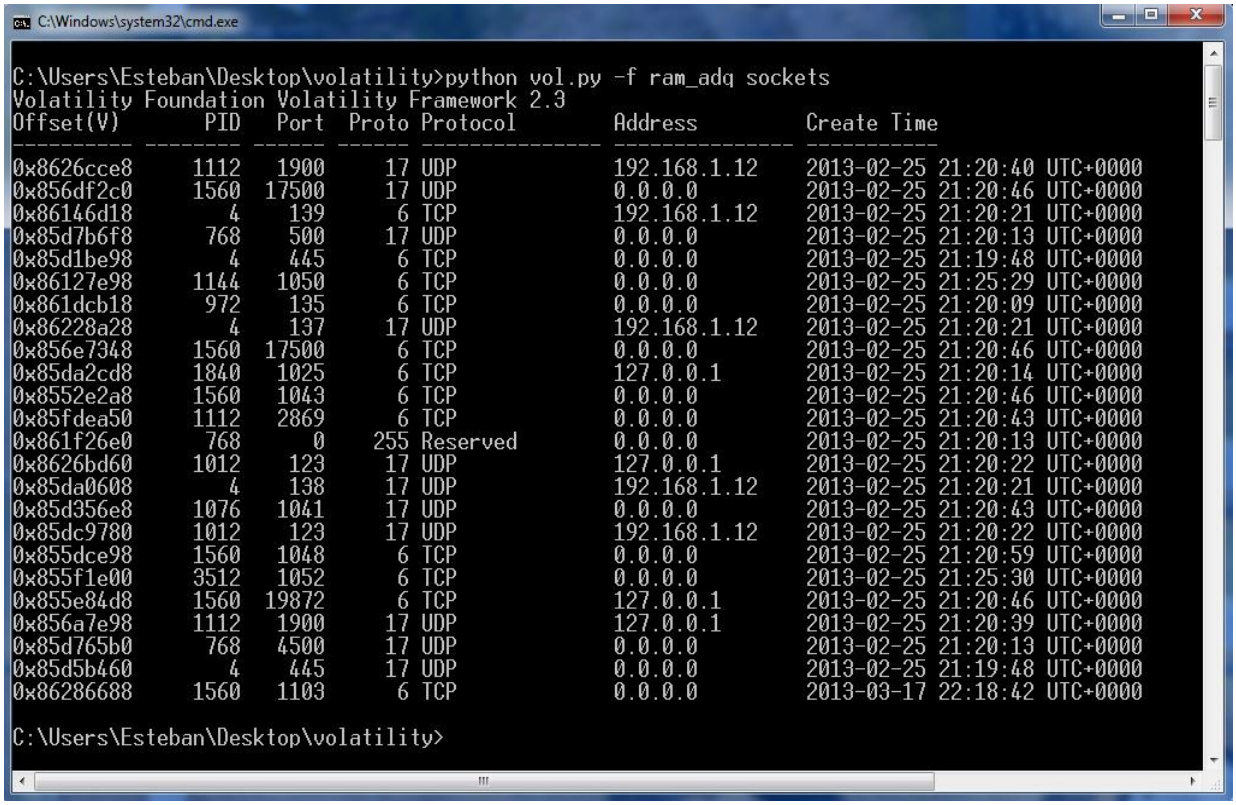


Figura 18. Detall dels *sockets* actius a l'ordinador analitzat

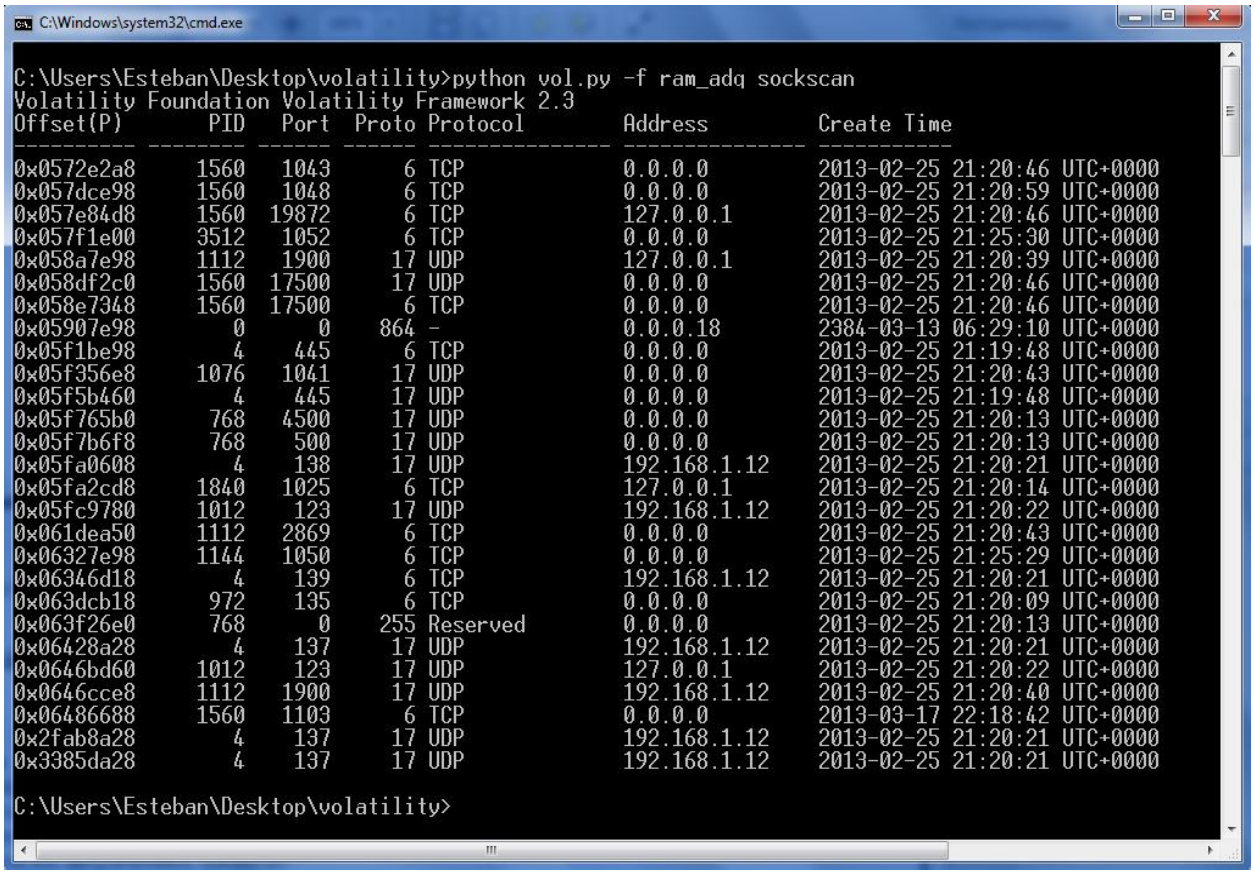


Figura 19. Obtenció de tots els *sockets* que s'han executat al sistema analitzat

15. Annex E. Proves tècniques: Usuaris de l'equip analitzat

Es fa servir l'eina *Volatility* per obtenir les credencials d'accés al sistema *Windows* instal·lat a la imatge de disc dur analitzada. Primerament, utilitzant els paràmetres *hivescan* i *hivelist* de l'eina *Volatility*, s'obtenen les adreces físiques de memòria on es pot trobar la informació que s'està cercant. A les següents captures de pantalla, es pot veure el procés de localització de les claus del registre de *Windows* que guarden els noms i les contrasenyes dels usuaris del sistema.

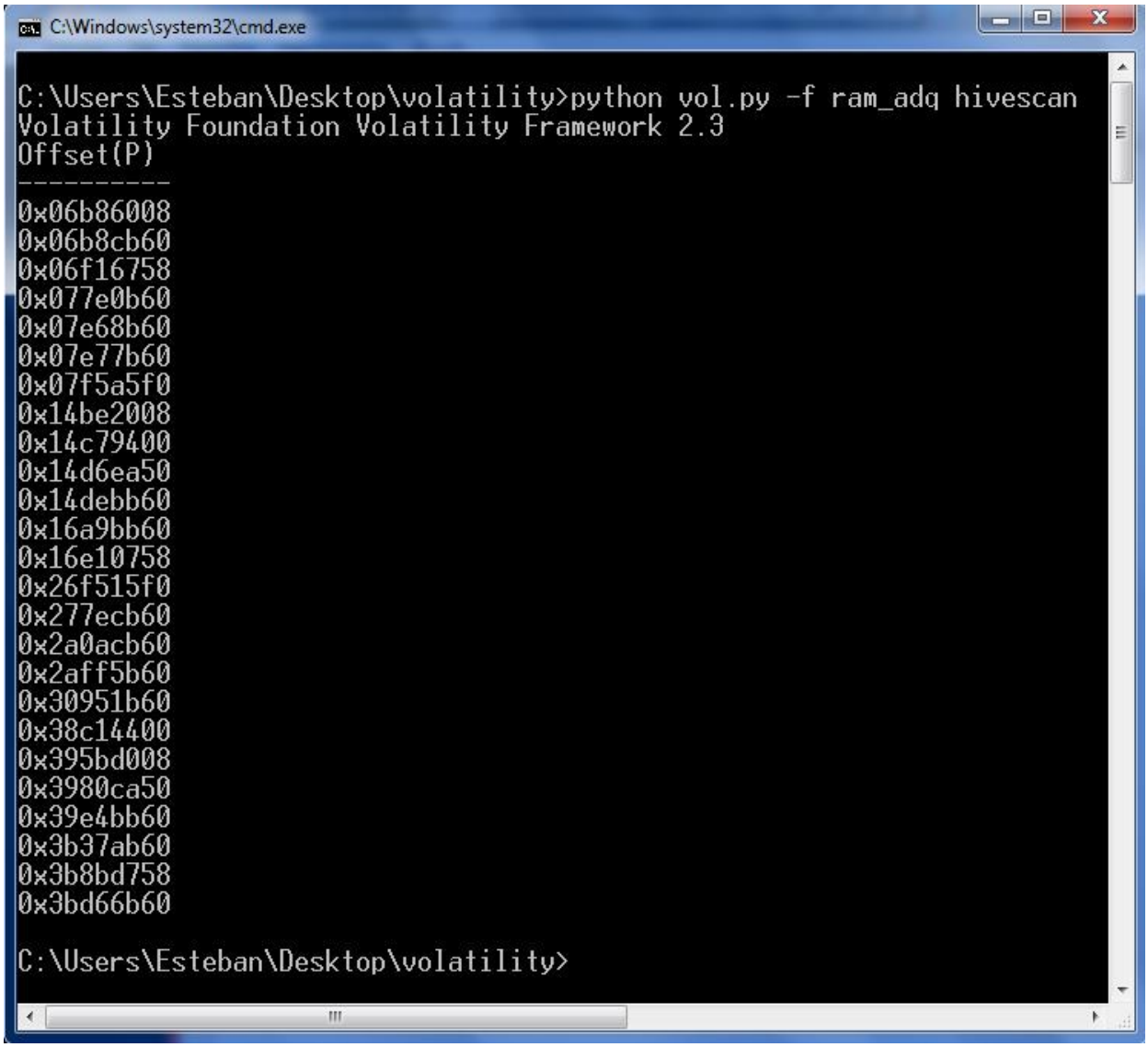


Figura 20. Llistat dels Offsets de memòria

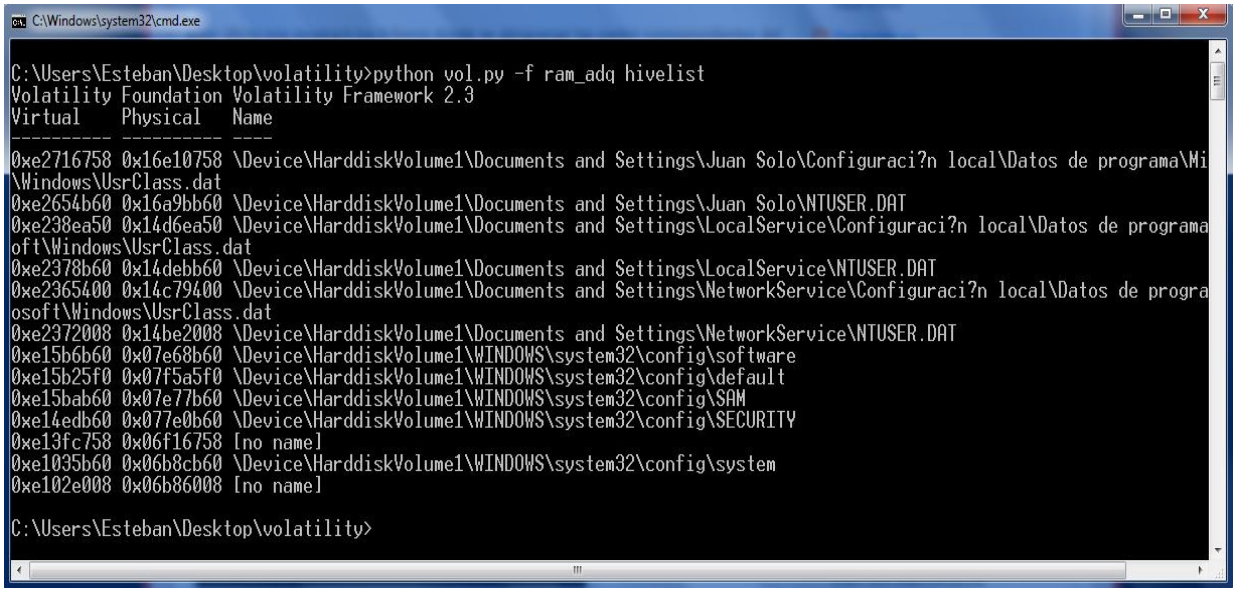


Figura 21. Localització de les claus del registre de *Windows* a la *memòria RAM*

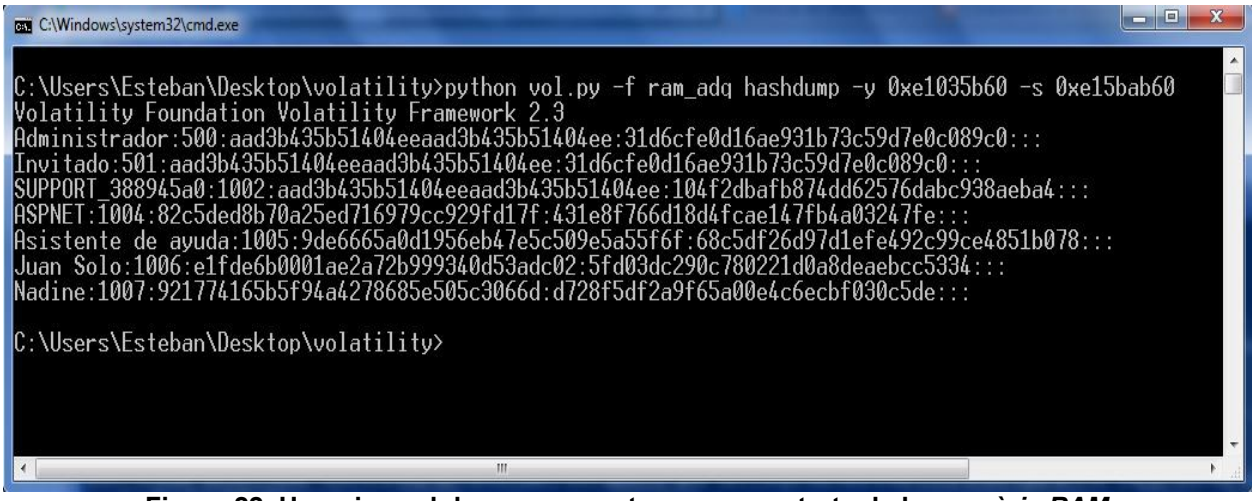


Figura 22. Usuaris, amb les seves contrasenyes, extrets de la *memòria RAM*

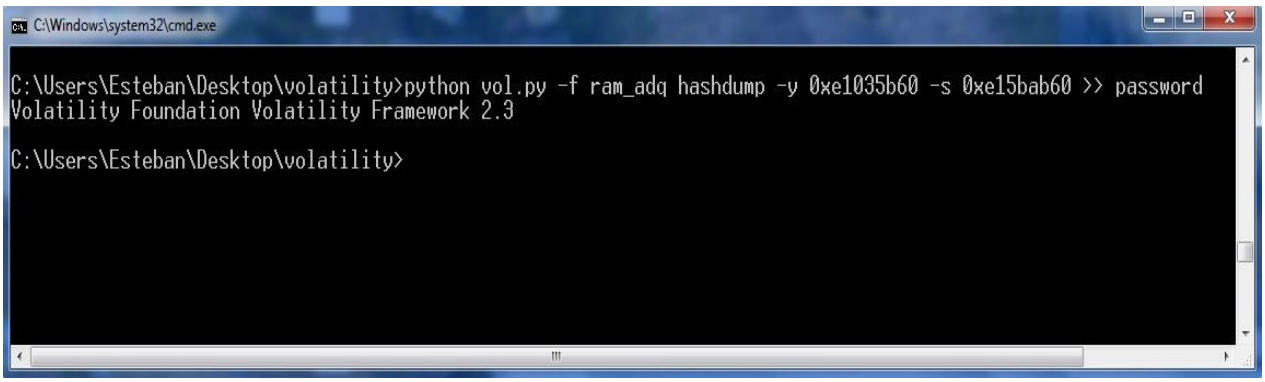


Figura 23. Copia dels usuaris i les seves contrasenyes encriptades a fitxer

Un cop s'extrauen les credencials dels usuaris de la memòria, i es bolquen en un fitxer de text, s'utilitza l'eina *John the ripper*, per '*crackejar*' els *Hashes* de les contrasenyes i obtenir-les en text clar,

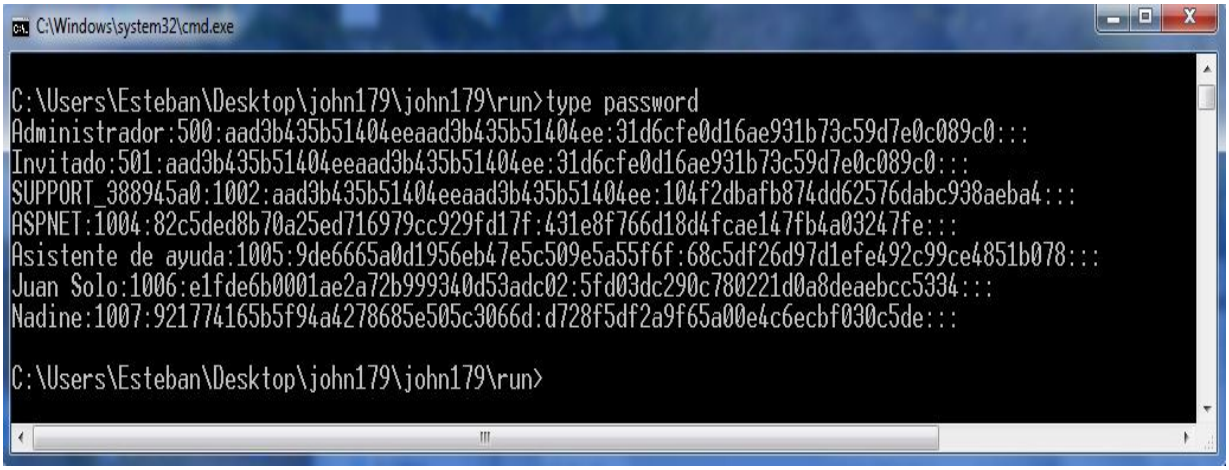


Figura 24. Detall del contingut del fitxer amb les contrasenyes

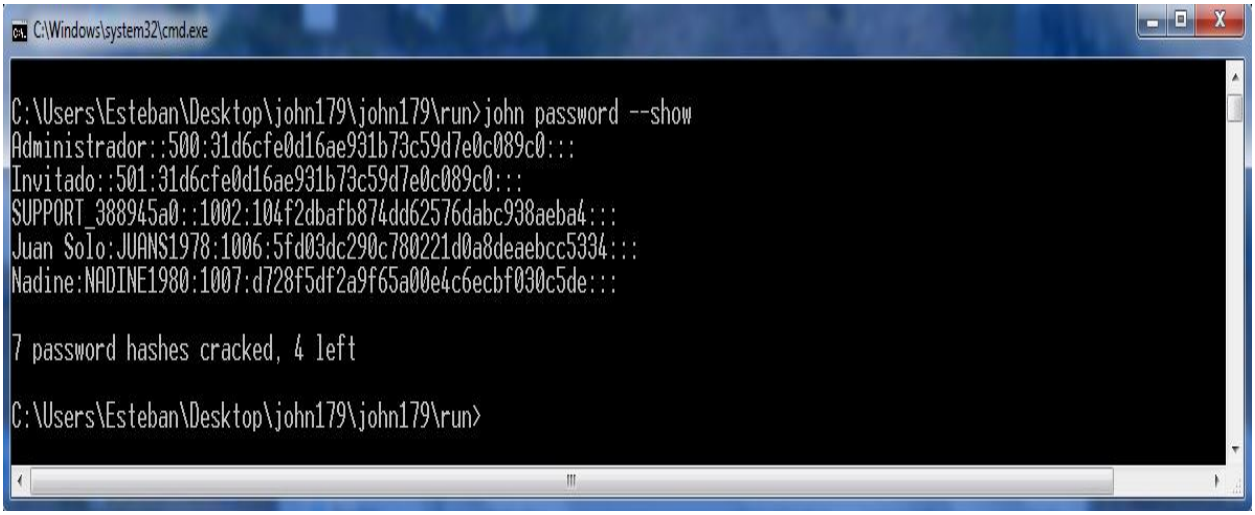


Figura 25. Extracció de les contrasenyes dels usuaris del sistema analitzat

16. Annex F. Proves tècniques: Extracció d'arxius ocults

Aquest annex conté l'anàlisi d'una fotografia sospitosa de contenir dades amagades al seu interior, esteganografia. Analitzant la carpeta dels documents personals de l'usuari **Nadine**, dins de la carpeta "*Mis imagenes/Vacaciones 2012*", existeixen dos fitxers molt peculiars. D'una banda es troba el fitxer *"Vacaciones_Budapest.jpg.odt"*, que conté les contrasenyes d'accés a diversos serveis de l'usuari **Nadine**. D'altra banda, es troba una imatge que, ni per la seva mida en bytes ni per l'extensió o tipus de fitxer, és coherent amb la resta d'arxius d'aquesta carpeta, el fitxer "*Budapest Verano 2012 424.bmp*".

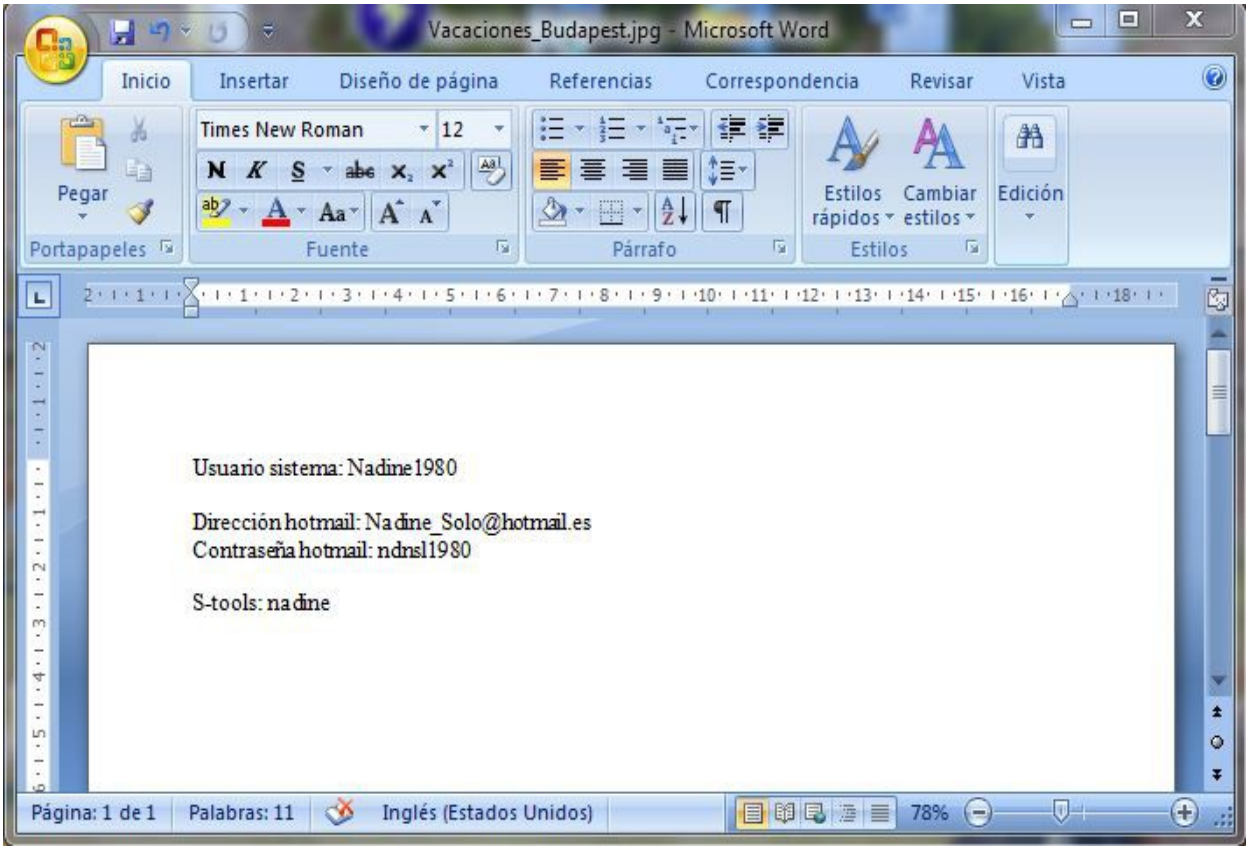


Figura 26. Contingut del fitxer sospitós *Vacaciones_Budapest.jpg.odt*

Es farà servir la contrasenya "*nadine*" que sembla utilitzar-se amb l'eina *S-tools*, un programari molt utilitzat per amagar informació dins de fitxers gràfics. Això es comprova obrint la imatge i introduint aquesta contrasenya.

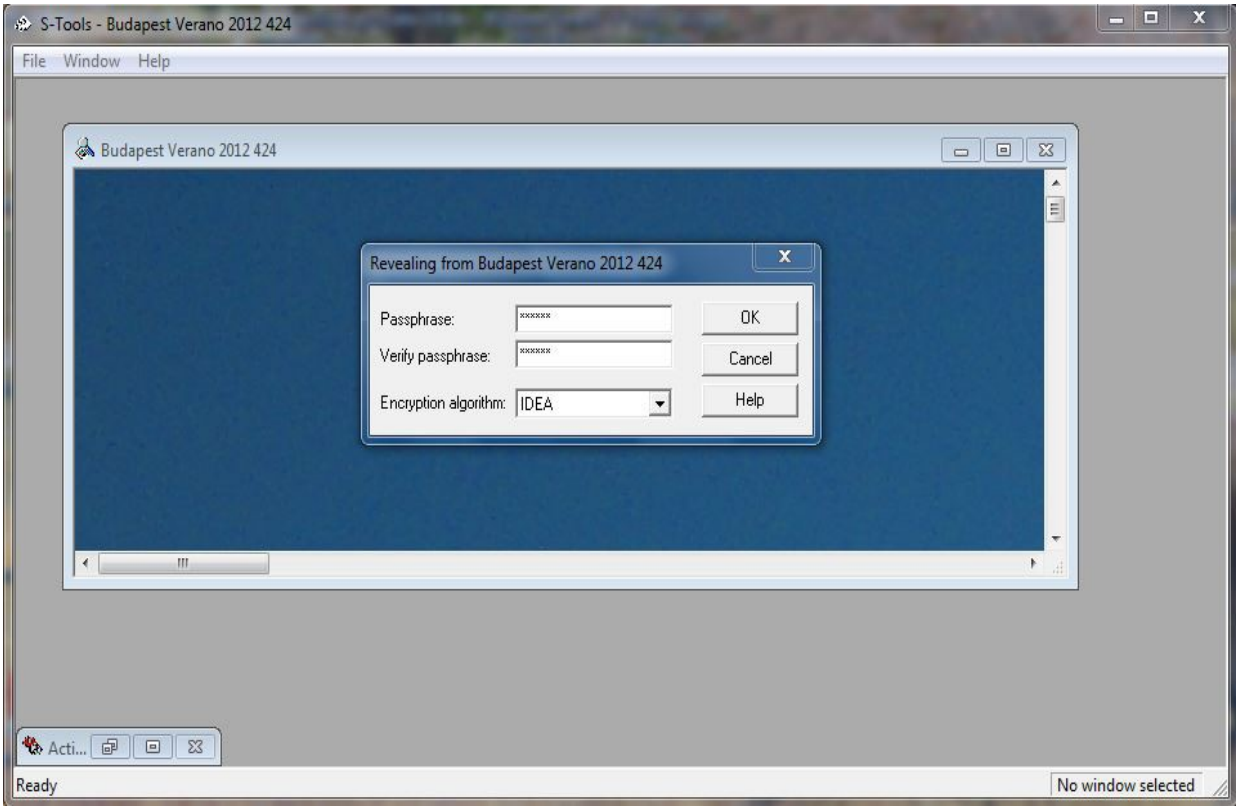


Figura 27. Procés d'extracció de fitxers ocults dins de la imatge

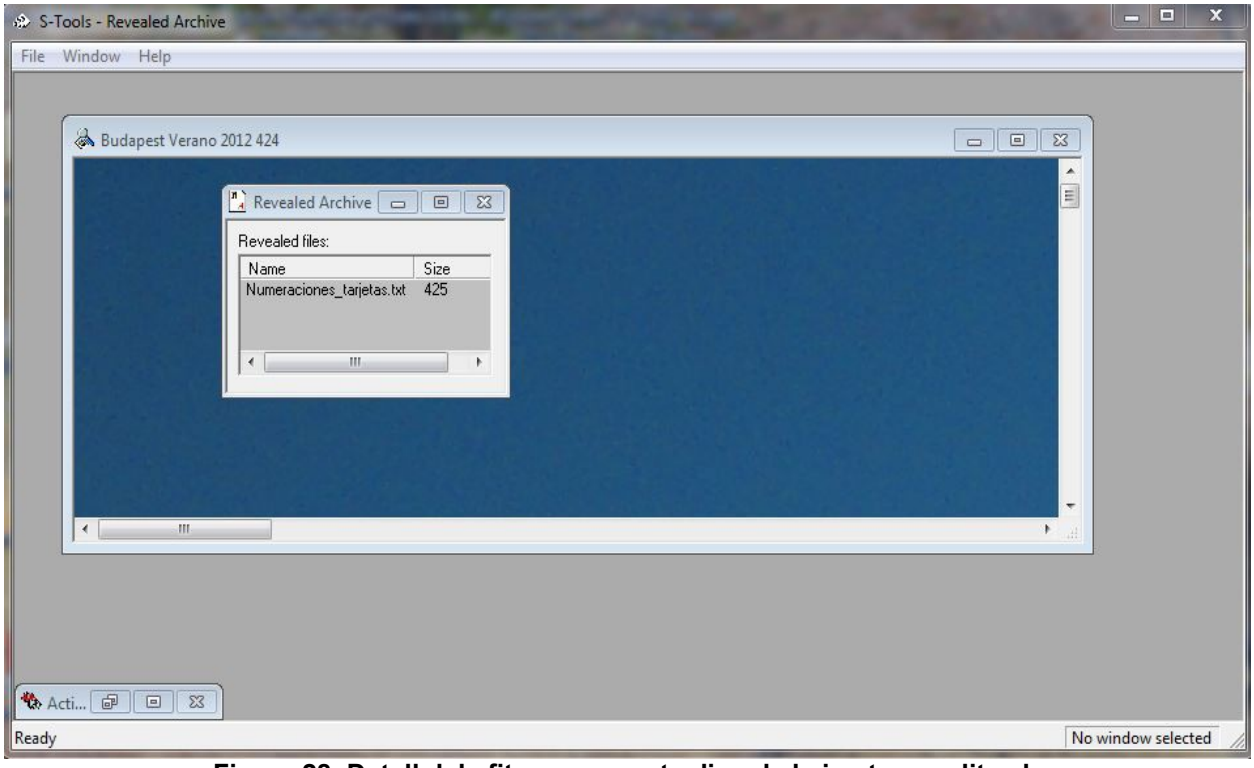


Figura 28. Detall dels fitxers amagats dins de la imatge analitzada

Com es pot observar a les captures anteriors, dins de la imatge sospitosa es troba un fitxer de text amb informació molt important per la investigació que es duu a terme,

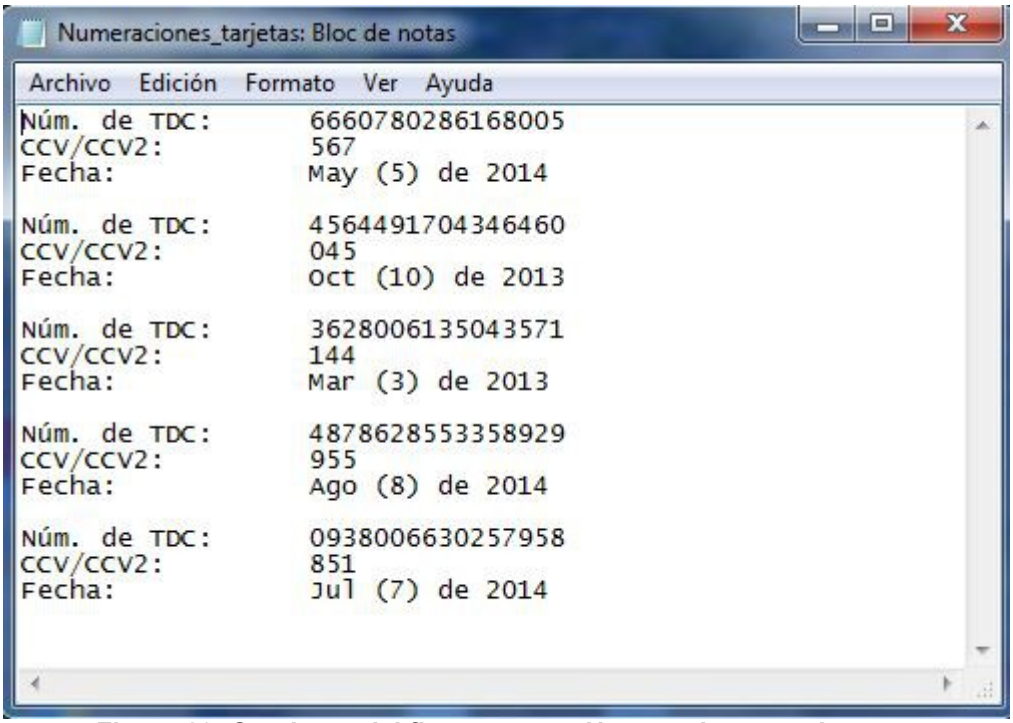


Figura 29. Contingut del fitxer amagat *Numeraciones_tarjetas.txt*

17. Annex G. Proves tècniques: Anàlisi del registre de Windows

En aquest annex s'analitza el registre de *Windows* del disc dur que s'està examinant. Primerament es localitzen els fitxers que contenen les claus del registre. Aquest fitxers són: "*SAM, SECURITY, software, system i userdiff*". Aquests arxius es troben a la carpeta "*Windows/System32/Config*".

Així mateix, s'analitzen també les claus dels dos usuaris de l'equip, que les podem trobar al fitxer *NTUSER.DAT* que es localitza a les carpetes personals de cada usuari, concretament a "*Documents and Settings/Juan Solo*" i "*Documents and Settings/Nadine*" Amb el programari *Autopsy*, es cercen aquests fitxers i es descarreguen al nostre equip.

Per extreure informació de les claus del registre, es fa servir el programari gratuït *MiTeC Windows Registry Recovery v 1.5.2.0*. Aquesta eina complementa la informació obtinguda amb l'eina *Volatility*, veure l'Annex D, d'una manera més gràfica.

A les següents captures podem trobar les informacions més rellevants que s'han trobat analitzant les claus del registre de *Windows*,

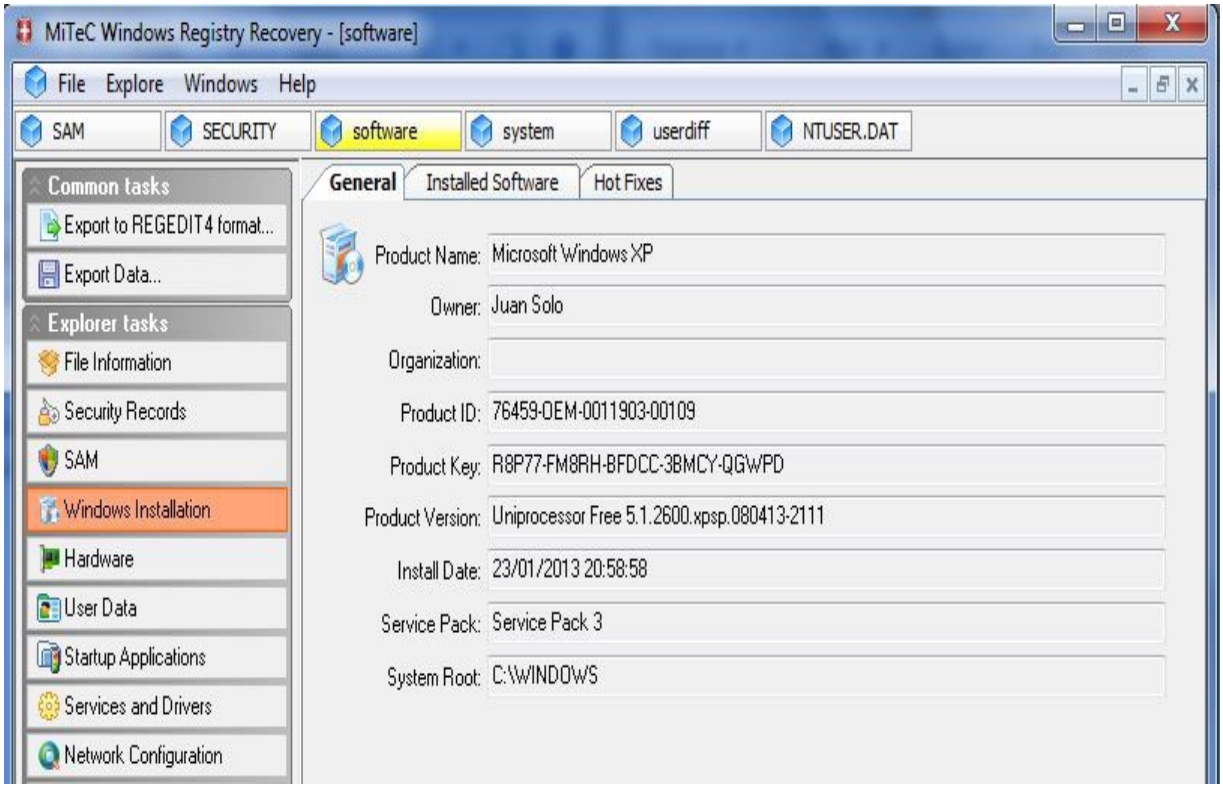
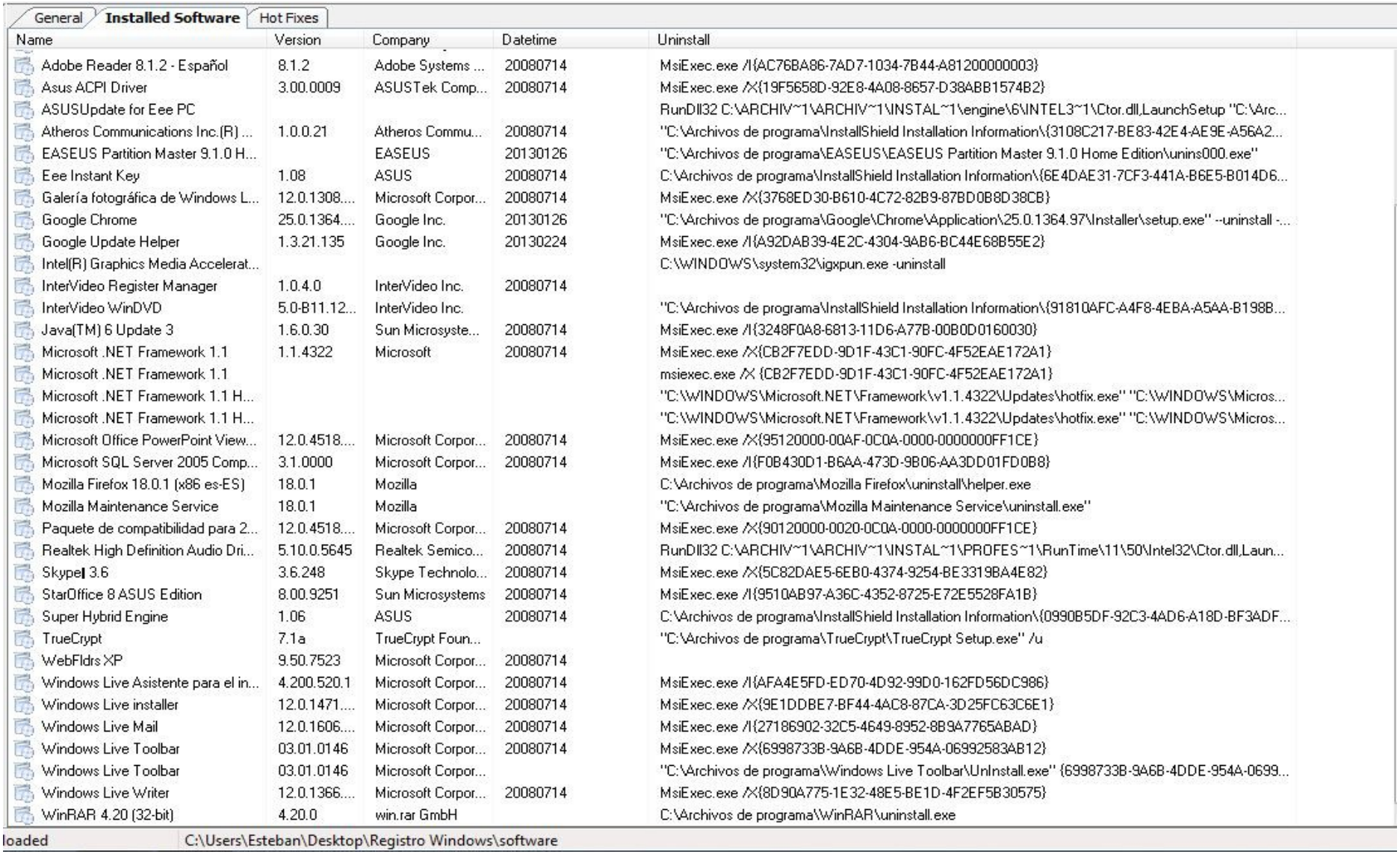


Figura 30. Detalls del sistema operatiu instal.lat



General | **Installed Software** | Hot Fixes

Name	Version	Company	Datetime	Uninstall
Adobe Reader 8.1.2 - Español	8.1.2	Adobe Systems ...	20080714	MsiExec.exe /I{AC76BA86-7AD7-1034-7B44-A81200000003}
Asus ACPI Driver	3.00.0009	ASUSTek Comp...	20080714	MsiExec.exe /X{19F5658D-92E8-4A08-8657-D38ABB1574B2}
ASUSUpdate for Eee PC				RunDll32 C:\ARCHIV~1\ARCHIV~1\INSTAL~1\engine\6\INTEL3~1\Ctor.dll,LaunchSetup "C:\Arc...
Atheros Communications Inc.(R) ...	1.0.0.21	Atheros Commu...	20080714	"C:\Archivos de programa\InstallShield Installation Information\{3108C217-BE83-42E4-AE9E-A56A2...
EASEUS Partition Master 9.1.0 H...		EASEUS	20130126	"C:\Archivos de programa\EASEUS\EASEUS Partition Master 9.1.0 Home Edition\unins000.exe"
Eee Instant Key	1.08	ASUS	20080714	C:\Archivos de programa\InstallShield Installation Information\{6E4DAE31-7CF3-441A-B6E5-B014D6...
Galería fotográfica de Windows L...	12.0.1308....	Microsoft Corpor...	20080714	MsiExec.exe /X{3768ED30-B610-4C72-82B9-87BD0B8D38CB}
Google Chrome	25.0.1364....	Google Inc.	20130126	"C:\Archivos de programa\Google\Chrome\Application\25.0.1364.97\Installer\setup.exe" --uninstall -...
Google Update Helper	1.3.21.135	Google Inc.	20130224	MsiExec.exe /I{A92DAB39-4E2C-4304-9AB6-BC44E68B55E2}
Intel(R) Graphics Media Accelerat...				C:\WINDOWS\system32\igxpun.exe -uninstall
InterVideo Register Manager	1.0.4.0	InterVideo Inc.	20080714	
InterVideo WinDVD	5.0-B11.12...	InterVideo Inc.		"C:\Archivos de programa\InstallShield Installation Information\{91810AFC-A4F8-4EBA-A5AA-B198B...
Java(TM) 6 Update 3	1.6.0.30	Sun Microsyste...	20080714	MsiExec.exe /I{3248F0A8-6813-11D6-A77B-00B0D0160030}
Microsoft .NET Framework 1.1	1.1.4322	Microsoft	20080714	MsiExec.exe /X{CB2F7EDD-9D1F-43C1-90FC-4F52EAE172A1}
Microsoft .NET Framework 1.1				msiexec.exe /X {CB2F7EDD-9D1F-43C1-90FC-4F52EAE172A1}
Microsoft .NET Framework 1.1 H...				"C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\Updates\hotfix.exe" "C:\WINDOWS\Micros...
Microsoft .NET Framework 1.1 H...				"C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\Updates\hotfix.exe" "C:\WINDOWS\Micros...
Microsoft Office PowerPoint View...	12.0.4518....	Microsoft Corpor...	20080714	MsiExec.exe /X{95120000-00AF-0C0A-0000-0000000FF1CE}
Microsoft SQL Server 2005 Comp...	3.1.0000	Microsoft Corpor...	20080714	MsiExec.exe /I{F0B430D1-B6AA-473D-9B06-AA3DD01FD0B8}
Mozilla Firefox 18.0.1 (x86 es-ES)	18.0.1	Mozilla		C:\Archivos de programa\Mozilla Firefox\uninstall\helper.exe
Mozilla Maintenance Service	18.0.1	Mozilla		"C:\Archivos de programa\Mozilla Maintenance Service\uninstall.exe"
Paquete de compatibilidad para 2...	12.0.4518....	Microsoft Corpor...	20080714	MsiExec.exe /X{90120000-0020-0C0A-0000-0000000FF1CE}
Realtek High Definition Audio Dri...	5.10.0.5645	Realtek Semico...	20080714	RunDll32 C:\ARCHIV~1\ARCHIV~1\INSTAL~1\PROFES~1\RunTime\11\50\Intel32\Ctor.dll,Laun...
Skype™ 3.6	3.6.248	Skype Technolo...	20080714	MsiExec.exe /X{5C82DAE5-6EB0-4374-9254-BE3319BA4E82}
StarOffice 8 ASUS Edition	8.00.9251	Sun Microsystems	20080714	MsiExec.exe /I{9510AB97-A36C-4352-8725-E72E5528FA1B}
Super Hybrid Engine	1.06	ASUS	20080714	C:\Archivos de programa\InstallShield Installation Information\{0990B5DF-92C3-4AD6-A18D-BF3ADF...
TrueCrypt	7.1a	TrueCrypt Foun...		"C:\Archivos de programa\TrueCrypt\TrueCrypt Setup.exe" /u
WebFldrs XP	9.50.7523	Microsoft Corpor...	20080714	
Windows Live Asistente para el in...	4.200.520.1	Microsoft Corpor...	20080714	MsiExec.exe /I{AFA4E5FD-ED70-4D92-99D0-162FD56DC986}
Windows Live installer	12.0.1471....	Microsoft Corpor...	20080714	MsiExec.exe /X{9E1DDBE7-BF44-4AC8-87CA-3D25FC63C6E1}
Windows Live Mail	12.0.1606....	Microsoft Corpor...	20080714	MsiExec.exe /I{27186902-32C5-4649-8952-8B9A7765ABAD}
Windows Live Toolbar	03.01.0146	Microsoft Corpor...	20080714	MsiExec.exe /X{6998733B-9A6B-4DDE-954A-06992583AB12}
Windows Live Toolbar	03.01.0146	Microsoft Corpor...		"C:\Archivos de programa\Windows Live Toolbar\UnInstall.exe" {6998733B-9A6B-4DDE-954A-0699...
Windows Live Writer	12.0.1366....	Microsoft Corpor...	20080714	MsiExec.exe /X{8D90A775-1E32-48E5-BE1D-4F2EF5B30575}
WinRAR 4.20 (32-bit)	4.20.0	win.rar GmbH		C:\Archivos de programa\WinRAR\uninstall.exe

loaded C:\Users\Esteban\Desktop\Registro Windows\software

Figura 31. Llistat de la majoria del programari instal·lat a l'ordinador analitzat

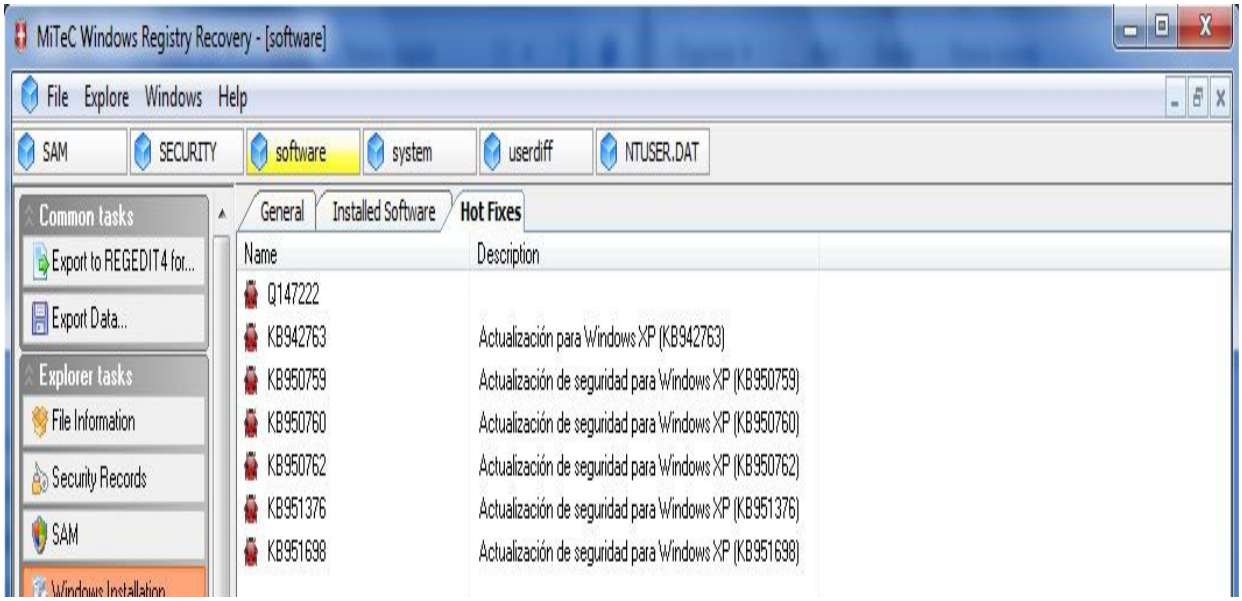


Figura 32. Detall de les últimes actualitzacions de seguretat del sistema operatiu

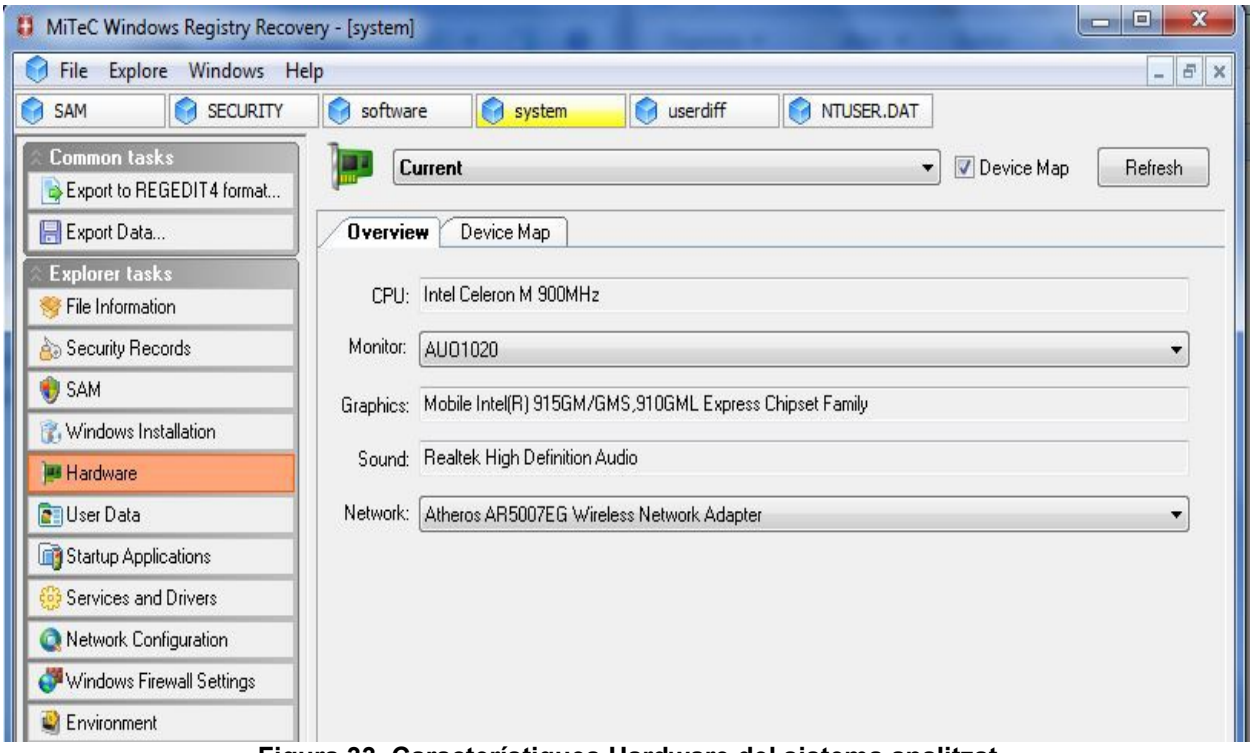


Figura 33. Característiques Hardware del sistema analitzat

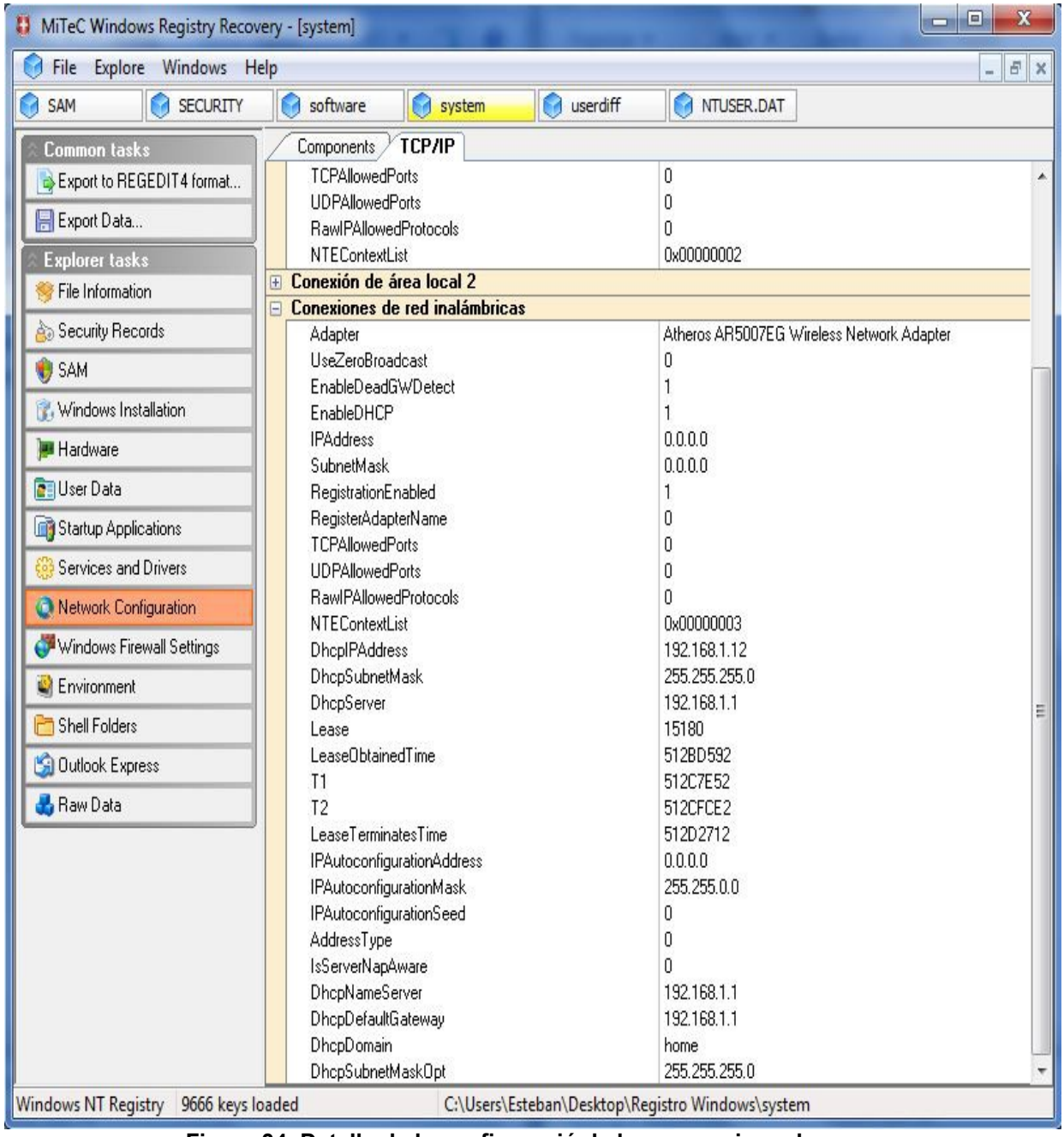


Figura 34. Detalls de la configuració de les connexions de xarxa

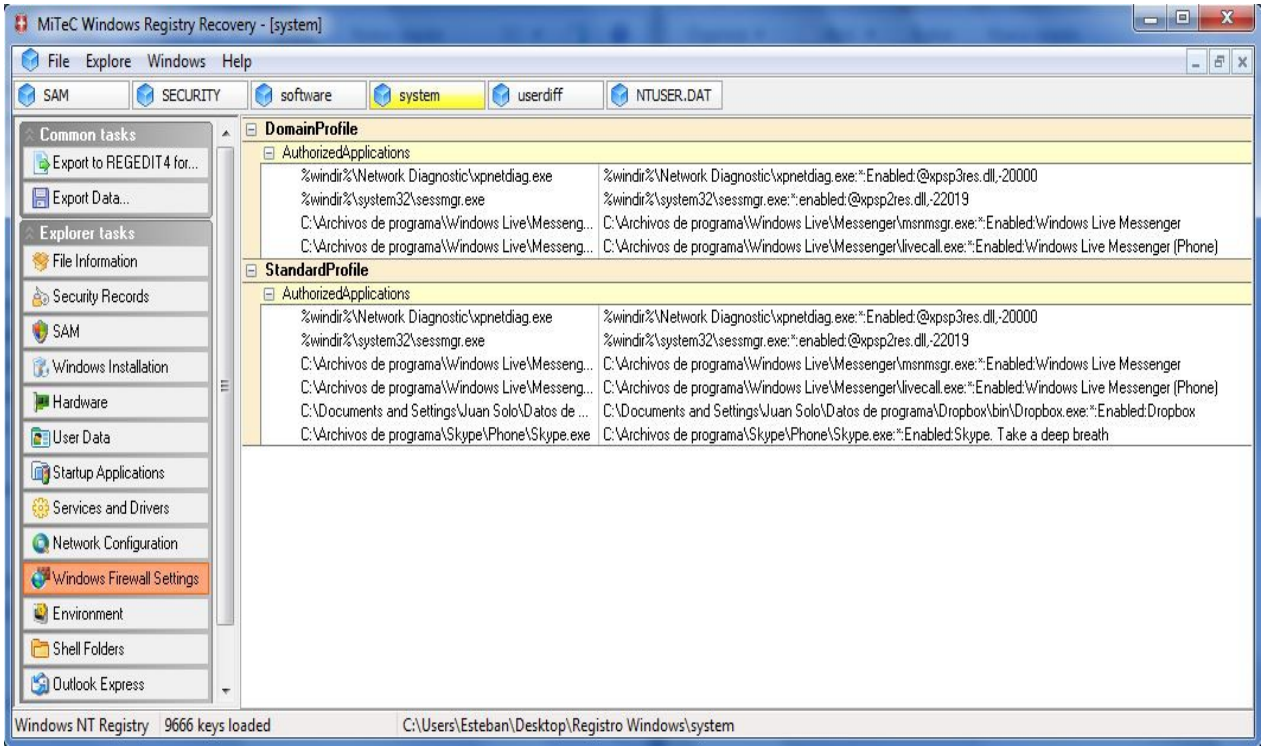


Figura 35. Configuració del Firewall de Windows

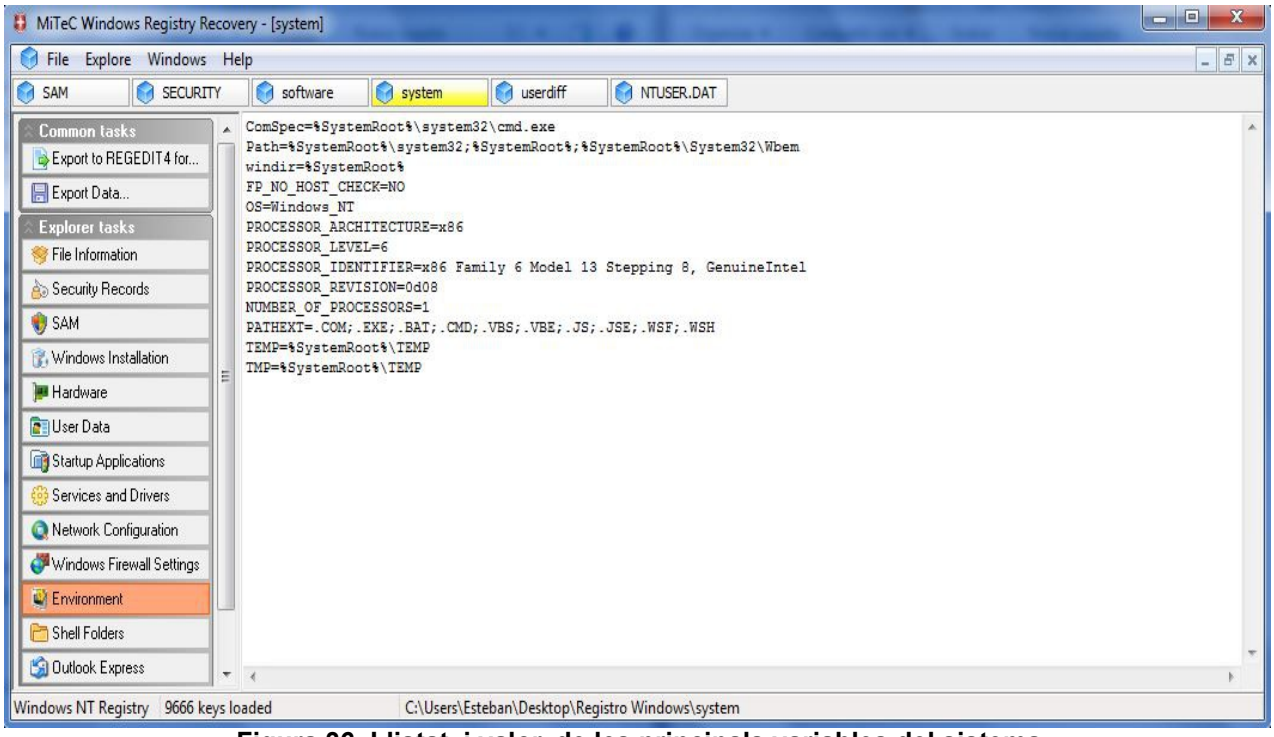


Figura 36. Llistat, i valor, de les principals variables del sistema

Complementant la informació dels usuaris del sistema analitzat, obtinguda a l'Annex E, les captures següents mostraran informació sobre l'ús de l'equip per part dels dos usuaris analitzats,

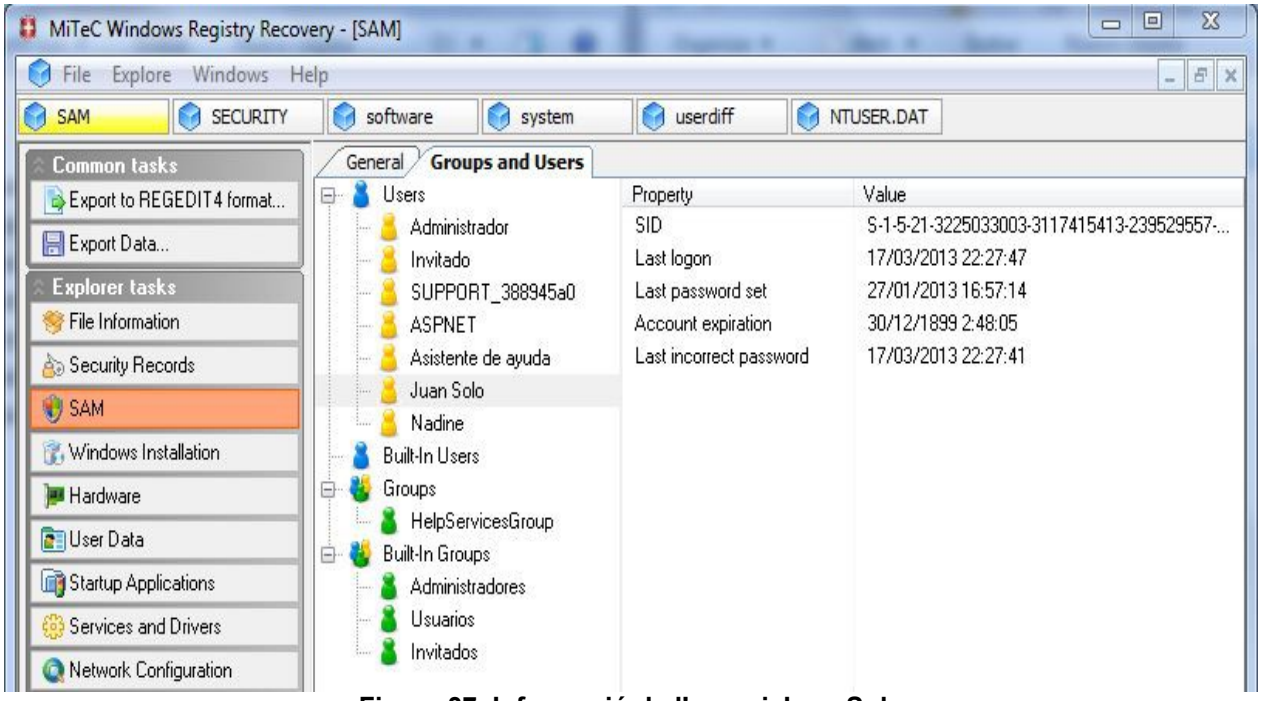


Figura 37. Informació de l'usuari Juan Solo

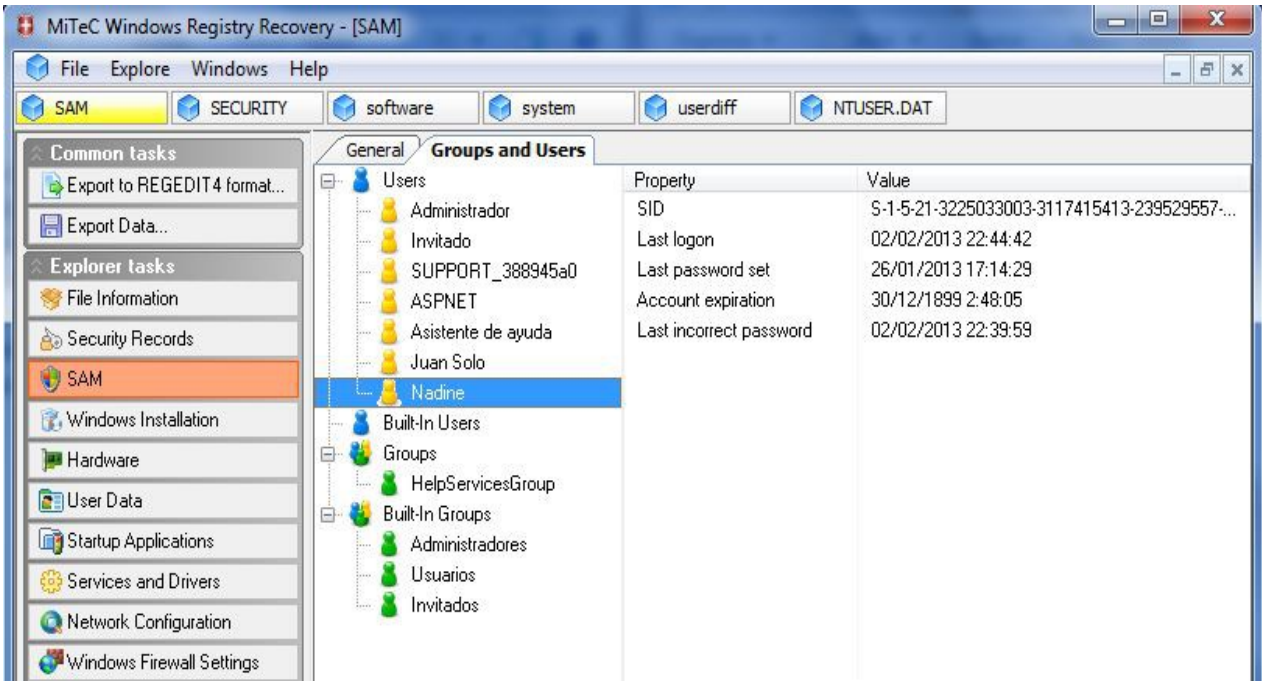


Figura 38. Detall de la informació del compte de l'usuari Nadine

18. Bibliografia

CASEY, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet 3rd Edition*. San Diego [etc.]: Elsevier Inc.

http://books.google.es/books?hl=es&lr=&id=6gCbJ4O4f-IC&oi=fnd&pg=PP2&dq=casey+eoghan+digital+evidence+and+computer+crime&ots=Wpw0cw1yd0&sig=VN7SqN9BQEFl3291DVKnOnt0-Co#v=onepage&q=casey%20eoghan%20digital%20evidence%20and%20computer%20crime&f=false

Anònim (2013). *ISO 27K infosec managament standards.* [en línia]. http://www.iso27001security.com [data de consulta: 11/10/2013].

SERRA, J.; COLOBRAN, M.; ARQUÉS, J.M.; GUASCH, A. (2009). *Anàlisis forense de sistemas de información: investigación de la evidencia digital*. Barcelona: Fundació UOC.

SÁNCHEZ, P. (2011). *101 utilidades forenses.* [en línia]. http://conexioninversa.blogspot.com.es/2011/11/101-utilidades-forenses.html [data de consulta: 06/10/2013].

GOOGLE PROJECT HOSTING (2013). *Volatility. An advanced fmemory forensics framework* [en línia] https://code.google.com/p/volatility/wiki/CommandReference23 [data de consulta: 03/10/2013].

CESICAT [12] (2010). *Manual d'usuari del TrueCrypt* [en línia]. https://www.cesicat.cat/media/files/Manual%20de%20l'usuari%20del%20TrueCrypt.pdf [data de consulta: 11/12/2013].

Bibliografia complementaria

NICOLAU, F.; CUENCA, M. J. (2010). *Competència comunicativa per a professionals de les TIC.* Barcelona: Fundació UOC.

19. Referències externes

[1] informàtica forense. http://es.wikipedia.org/wiki/Cómputo_forense

[2] cadena de custodia. http://es.wikipedia.org/wiki/Cadena_de_custodia

[3] BS 10008. http://www.bsigroup.com/en-GB/bs-10008-legal-admissibility-of-electronic-information/

[4] Google. https://www.google.com/

[5] Apple. http://www.apple.com/es/

[6] Microsoft. http://www.microsoft.com/es-es/default.aspx

[7] Intel. http://www.intel.es/

[8] Adobe Systems. http://www.adobe.com

[9] Casey, Eoghan. http://en.wikipedia.org/wiki/Eoghan_Casey

[10] Steve Jobs. http://allaboutstevejobs.com

[11] MIT (Massachusetts Institute of Technology). http://web.mit.edu

[12] CESICAT (Centre de Seguretat de la Informació de Catalunya). https://www.cesicat.cat

20. Glossari

ADSL. Acrònim, anglès *Asymmetric Digital Subscriber Line* (línia d'abonat digital asimètrica). És un tipus de tecnologia de línia *DSL*. Consisteix en una transmissió analògica de dades digitals recolzada en el parell simètric de coure que porta la línia telefònica convencional o línia d'abonat, sempre que la longitud de línia no superi els 5,5 km mesurats des de la central telefònica, o no hi hagi altres serveis pel mateix cable que puguin interferir.

Bit. Acrònim, anglès. *Binary digit* (digit binari). Unitat bàsica d'informació que pot representar dos valors assignant un dels valors a l'estat apagat (0) i l'altre a l'estat encès (1).

CD, CD-ROM, DVD. Són suports digitals òptics utilitzats per emmagatzemar qualsevol tipus d'informació: àudio, vídeo, imatges, documents i altres dades.

Diagrama de Gantt. És una popular eina gràfica que el seu objectiu és mostrar el temps de dedicació previst per a diferents tasques o activitats al llarg d'un temps total determinat. Malgrat això, el *diagrama de Gantt* no indica les relacions existents entre les activitats.

Firmware. És un bloc d'instruccions de màquina per a propòsits específics, gravat en una memòria, normalment de tipus *Flash* o *ROM*, que estableix la lògica de més baix nivell que controla els circuits electrònics d'un dispositiu de qualsevol tipus.

Hash. Els *Hashes* o *funcions de resum* són algoritmes que aconsegueixen crear a partir d'una entrada (un text, una contrasenya o un arxiu) una sortida alfanumèrica de longitud normalment fixa que representa un resum de tota la informació que se li ha donat (és a dir, a partir de les dades de l'entrada crea una cadena que solament pot tornar-se a crear amb aquestes mateixes dades). Aquestes funcions tenen els següents propòsits: assegurar que no s'ha modificat un arxiu en una transmissió, fer il·legible una contrasenya o signar digitalment un document.

Hosting. Anglicisme, allotjament web. És el servei que proveeix als usuaris d'Internet un sistema per poder emmagatzemar informació, imatges, vídeo, o qualsevol contingut accessible via web.

Hub. Anglicisme, concentrador. Es tracta d'un dispositiu que permet centralitzar el cablejat d'una xarxa i poder ampliar-la. Això significa que aquest dispositiu rep un senyal i repeteix aquest senyal emetent-lo pels seus diferents ports. Treballa en la *capa 1 del model OSI* o capa d'*Accés en el model TCP/IP*. Actualment estan desfasats i la seva tasca l'acostumen a realitzar els *switches* o commutadors.

iPad. És una línia de tabletes dissenyades i comercialitzades per *Apple Inc* [5]. La primera generació va ser anunciada el dia 27 de gener de 2010 per *Steve Jobs* [10]. Es situa en una categoria entre un telèfon intel·ligent, *smartphone*, i un ordinador portàtil, enfocat més a l'accés que a la creació d'aplicacions i continguts.

Macbook Pro. És una línia d'ordinadors portàtils d'alt rendiment d'*Apple Inc* [5]. I que té com a mercat objectiu els usuaris professionals. És el successor del famós model *PowerBook G4*. Va ser la primera línia de productes de l'empresa en incloure processadors *Intel* [7], i va ser presentada en la fira tecnològica *MacWorld* 2006 el dia 10 de gener de 2006.

Metadades. Es tracta de dades que descriuen unes altres dades. Generalment, un grup de *metadades* es refereix a un grup de dades anomenat recurs. El concepte de metadades és anàleg a l'ús d'índexs per localitzar objectes en comptes de dades. És a dir, ajuden a situar dades.

MD5. Acrònim, anglès *Message-Digest Algorithm 5* (algoritme de resum del missatge 5). És un algoritme de reducció criptogràfic de 128 *bits* molt utilitzat. Fou desenvolupat l'any 1991 al *MIT* [11] (*Massachusetts Institute of Technology*) per substituir l'*algoritme MD4* que era molt feble. Malgrat la seva àmplia difusió actual, Malgrat la seva àmplia difusió actual, la successió de problemes de seguretat detectats des de l'any 1996, es va anunciar una col·lisió de *Hash*, planteja una sèrie de dubtes sobre el seu ús futur.

OpenOffice. *Apache OpenOffice* és una suite ofimàtica lliure (codi obert i distribució gratuïta) que inclou eines com un processador de textos, full de càlcul, presentacions, eines per al dibuix vectorial i base de dades. Està disponible per a diverses plataformes, tals com *Microsoft* [6] *Windows*, *GNU/Linux*, *BSD*, *Solaris* i *Mac OS X*. Suporta nombrosos formats d'arxiu, incloent com predeterminat el format estàndard *ISO/IEC OpenDocument* (*ODF*), entre altres formats comuns, així com també suporta més de 110 idiomes.

PC. Acrònim, anglès. *Personal Computer* (ordinador personal). Es tracta d'una micro computadora dissenyada per ser utilitzada només per una persona. Va ser l'estratègia d'*IBM* per ingressar en el mercat de les computadores domèstiques.

PDA. Acrònim, anglès. *Personal Digital Assistant* (assistent digital personal). És un ordinador de ma, o de butxaca, originalment dissenyada com a agenda electrònica amb funcions típiques: calendari, llista de contactes, bloc de notes i recordatoris, i amb un sistema de reconeixement d'escriptura. Avui dia han estat substituïts pel fenomen *smartphone*.

PDF. Acrònim, anglès. *Portable Document Format* (format de document portàtil). És un format d'emmagatzematge de documents digitals independent de plataformes software o hardware. Aquest format és de tipus compost (imatge vectorial, mapa de bits i text). Inicialment, va ser desenvolupat per l'empresa *Adobe Systems* [8], i fou llançat de manera oficial com un estàndard obert l'1 de juliol de 2008.

Pendrive. Memòria USB. És un dispositiu extern, d'emmagatzematge, es connecta al port USB, que utilitza una memòria *Flash* per guardar informació. Aquestes memòries s'han convertit en el sistema d'emmagatzematge i transport personal de dades més utilitzat, desplaçant en aquest ús als tradicionals *disquets* i als *CD*. Es poden trobar al mercat fàcilment memòries que van des de un *Gigabyte* fins a un *Terabyte* de capacitat.

RAM. Acrònim, anglès. *Random Access Memory* (Memòria d'accés aleatori). És la memòria de d'on el processador principal rep les instruccions i guarda els resultats. S'utilitza com memòria de treball pel sistema operatiu, els programes i la majoria del software. Es denomina '*d'accés aleatori*' perquè es pot llegir o escriure en una posició de memòria amb un temps d'espera igual per a qualsevol posició, no sent necessari seguir un ordre per accedir a la informació de la manera més ràpida possible.

Router. Anglicisme, encaminador de paquets. És un dispositiu que proporciona connectivitat a *Nivell de xarxa* o *Nivell 3 en el model OSI.* La seva funció principal consisteix a enviar o encaminar paquets de dades d'una xarxa a una altra, és a dir, interconnectar subxarxes, entenent per subxarxa un conjunt de màquines *IP* que es poden comunicar sense la intervenció d'un *router* i que, per tant, tenen prefixos de xarxa diferents.

Smartphone. Anglicisme, telèfon intel·ligent. És un telèfon mòbil construït sobre una plataforma informàtica mòbil, amb una major capacitat d'emmagatzemar dades i realitzar activitats, semblants a una minicomputadora, i connectivitat que un telèfon mòbil convencional. El terme *intel·ligent* fa referència a la capacitat d'usar-se com un ordinador de butxaca, arribant fins i tot a reemplaçar a un ordinador personal en alguns casos. El terme *telèfon intel·ligent* és un terme merament comercial, ja que els telèfons no pensen ni raonen com els humans.

SSD. Acrònim, anglès. *Solid-State Drive* (unitat d'estat solid). És un dispositiu d'emmagatzematge de dades que utilitza una memòria no volàtil, memòria *Flash*, o una memòria volàtil con la *SDRAM*, per guarda les dades en comptes d'utilitzar els plats giratoris magnètics que es troben als discos durs convencionals.

Switch. Anglicisme, commutador. Es tracta d'un dispositiu digital lògic d'interconnexió de xarxes de computadores que opera en la *Capa d'enllaç de dades del model OSI*. La seva funció és interconnectar dos o més segments de xarxa, de manera similar als ponts de xarxa, passant dades d'un segment a un altre d'acord amb *l'adreça MAC* de destinació de les trames a la xarxa. Un commutador és el centre d'una xarxa amb topologia d'estel. Els commutadors s'utilitzen quan es desitja connectar múltiples xarxes, fusionant-les en una sola. Igual que els ponts, atès que funcionen com un filtre a la xarxa, milloren el rendiment i la seguretat de les xarxes d'àrea local.

USB. Acrònim, anglès. *Universal Serial Bus* (Bus universal en sèrie). És un estàndard industrial desenvolupat a mitjans dels anys noranta que defineix els cables, connectors i protocols utilitzats en un bus per connectar, comunicar i proveir d'alimentació elèctrica entre ordinadors i perifèrics i dispositius electrònics.

Altres

Adreça IP i adreça MAC. Una *adreça IP* és una etiqueta numèrica que identifica, de manera lògica i jeràrquica, a una interfície (element de comunicació/connexió) d'un dispositiu (habitualment una computadora) dins d'una xarxa que utilitzi el *protocol IP* (*Internet Protocol*) que correspon al *Nivell de xarxa del Model OSI*. Aquest nombre no s'ha de confondre amb l'*adreça MAC*, que és un identificador de 48 *bits* que identifica de forma única la targeta de xarxa i no depèn ni del protocol de connexió utilitzat ni de la xarxa.

OSI. Acrònim, anglès. *Open System Interconnection* (interconnexió de sistemes oberts). El model d'interconnexió de sistemes oberts (*ISO/IEC 7498-1*), també anomenat *OSI*, és el model de xarxa descriptiu, que va ser creat per *l'Organització Internacional per a l'Estandardització* (ISO) l'any 1980. És un marc de referència per a la definició d'arquitectures en la interconnexió dels sistemes de comunicacions.

Figura 39. Capes del model OSI