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

Informe Pericial

Consultor: Josep Maria Arqués Soldevila
Estudiant: Esteban Bonachera López

12 de Gener de 2014

Índex

AL JUTJAT Nº XXX DE BARCELONA

Procediment: *Treball Final de Màster*

A Barcelona el 12 de Gener del 2014

INFORME PERICIAL PEL PROCEDIMENT *TREBALL FINAL DE MÀSTE*R

Que emet el Pèrit D. **Esteban Bonachera López**, amb D.N.I. nº **XXXXXXXX-X** inscrit en el "*Col·legi Oficial d'Enginyers Tècnics Informàtics de Catalunya* (*COETIC*)", adscrit en Barcelona, amb nombre de col·legiat **436**.

Presta jurament en forma legal, jura dir veritat i manifesta que ha actuat amb la major objectivitat possible, prenent en consideració tant el que pugui afavorir com el que sigui susceptible de causar perjudici a qualsevol de les parts, i que coneix les sancions penals en les quals podria incórrer si incomplís el seu deure com a pèrit i assabentat de l'objecte de l'informe,

DIU:

Que complint l'ordenat pel Jutjat, ha examinat l'expedient que obra en autes, i en la seva conseqüència té a bé emetre el present informe pericial.

1. Abast de l'informe pericial

L'objectiu principal d'aquest informe pericial és la determinació de l'existència d'alguna evidència que confirmi que els propietaris o usuaris de l'equip analitzat han comés algun acte delictiu, relacionat o no, amb la seva detenció anterior per posseir una gran quantitat de pastilles estupefaents i un nombre elevat de targetes de banda magnètica en blanc.

El present informe s'ha realitzat en el període de temps que va des del dia **05/11/2013** fins al dia **12/01/2014**.

Les evidències digitals a analitzar que van ser proporcionades per les autoritats policials són les següents (veure l'annex A):

- Imatge del disc dur de l'equip.
- Bolcat de la *memòria RAM*.
- Base de dates d'una aplicació de missatgeria extreta d'un *smartphone*.

L'anàlisi de les evidències digitals permeten la identificació del sistema investigat amb gran precisió. L'equip objecte d'aquest anàlisi forense és un *netbook* de la marca *Asus* pertanyent a la sèrie *Eee PC* tamb el Sistema Operatiu *Microsoft Windows XP Professional*, actualitzat amb el *Service Pack 3*, instal·lat (veure l'annex I).

2. Antecedents

A continuació es presenten els antecedents previs a la investigació realitzada:

- En un control rutinari de vehicles es deté un conductor (Juan Solo) i la seva acompanyant (Nadine), i se'ls intervenen milers de pastilles estupefaents (èxtasi o MDMA) i desenes de targetes de banda magnètica en blanc (és a dir, sense cap impressió identificativa, logo, empresa o entitat bancària, etc.).

- En una posterior entrada i registre en el domicili de la parella detinguda, se'ls intervé un ordinador, el qual, en el moment d'efectuar l'entrada, es trobava en funcionament, per la qual cosa, els agents especialitzats que participen en la diligència decideixen realitzar una captura de la *memòria RAM* de l'ordinador. Així mateix, en l'esmentada diligència, i una vegada realitzada la captura de la *RAM*, els agents actuants realitzen una imatge del disc dur del portàtil comissat.

  Finalment, es troba un telèfon mòbil amagat a un calaix del dormitori. Els agents actuants realitzen un primer examen en presència del secretari judicial i decideixen extreure únicament una còpia d'una base de dades localitzada en una targeta de memòria del telèfon, vinculada a una coneguda aplicació d'ús molt comú en telefonia.

3. Resum executiu

El present informe pericial mostra el resultat de la realització de l'anàlisi forense a les evidències digitals proporcionades per les autoritats policials: imatge d'un disc dur, bolcat de la *memòria RAM* i una base de dades vinculada a una aplicació de missatgeria extreta d'un *smartphone*.

La necessitat d'aquest informe sorgeix de la detenció prèvia dels propietaris i/o usuaris de l'equip analitzat per un delicte de possessió de substàncies estupefaents i de targetes de banda magnètica en blanc.

Els objectius d'aquest informe pericial és donar resposta als extrems següents proposats pel Jutjat Nº XXX de Barcelona:

- 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.

El present informe pericial compta amb l'autorització i l'aprovació del tribunal encarregat del cas.

4. Relació de tasques realitzades

Aquest apartat descriu les diferents tasques que s'han efectuat sobre les evidències digitals aportades per les forces de seguretat i justifica la metodologia que s'ha seguit per dur a terme l'anàlisi forense i el present informe pericial. Les diferents tasques són:

Comprovació de les evidències digitals rebudes. Consisteix en la comprovació dels *Hashes* dels arxius que les autoritats policials ens han proporcionat, d'aquesta manera es tindrà la certesa de que les dades que s'han d'analitzat no han sofert cap modificació.

Anàlisi del fitxer whatsapp.db. S'analitzen les comunicacions, mitjançant una coneguda aplicació de missatgeria mòbil, entre els usuaris de l'equip analitzat i terceres persones per buscar evidències d'activitats il·legals.

Anàlisi de fitxers de dades. Es realitza l'anàlisi de tots els fitxers continguts al disc dur que les autoritats policials ens han lliurat amb la finalitat de trobar evidències que demostrin activitats il·legals comeses pels usuaris de l'equip analitzat.

Anàlisi de fitxers d'imatges. S'investiguen totes les imatges i fotografies localitzades a la imatge del disc dur analitzat per cercar evidències, ocultes o no, d'activitats il·lícites.

Recuperació de fitxers eliminats. Es realitza una cerca a la imatge de la unitat d'emmagatzematge dels elements que han estat eliminats i s'intenta la seva recuperació.

Programari específic. Es repassa el programari instal·lat en el disc dur investigat buscant aquell software que poden ser utilitzats per realitzar activitats il·lícites o amagar aquestes activitats per tal d'evitar la seva detecció.

Revisió dels historials web. S'analitzen els historials de navegació, els arxius temporals i descarregats mitjançant els navegadors web instal·lats a l'equip per a cadascun dels usuaris investigats.

Anàlisi de la memòria RAM. Consisteix en l'anàlisi del fitxer que conté el bolcat de la *memòria RAM* de l'equip investigat amb la finalitat d'obtenir informació útil per a la investigació que es duu a terme. Es presta especial atenció a l'anàlisi del sistema operatiu instal·lat al sistema analitzat i el seu ús per part dels usuaris detectats.

Altres. Es realitzen altres anàlisis necessaris per portar a bon termini la investigació: cerca de dispositius externs connectats a l'ordinador, transmissions de dades a altres equips, cerca de paraules clau, etc.

5. Conclusions (i una observació)

Un cop s'han analitzat les evidències digitals aportades per la part demandant, s'ha arribat a les següents conclusions i a una observació:

1ª) S'han localitzat dos usuaris actius a l'ordinador analitzat. D'una banda està l'usuari **Juan Solo** i, d'altra banda, l'usuari **Nadine** (veure l'annex H). Així mateix, s'han trobat dues adreces de correu electrònic gestionades, respectivament, pels esmentats usuaris: *juan_solo23@hotmail.es* i *nadine_solo@hotmail.es* (veure l'annex H).

2ª) En resposta als extrems proposats pel Jutjat Nº XXX de Barcelona, aquest pèrit afirma categòricament:

> **2ª.1)** *Determinar si els usuaris de l'ordinador analitzat es dediquen al tràfic, distribució i/o venda de pastilles estupefaents*.
>
> – S'han identificat una base de dades de l'aplicació de missatgeria i telefonia IP *Skype* (fitxer **chatmsg256.dbb**), que conté els missatges intercanviats entre l'usuari **Juan Solo** i una tercera persona. Aquesta conversa fa al·lusió a la venda de substàncies estupefaents (una droga sintètica denominada “cristal”), el preu acordat i el dia i el lloc per realitzar la transacció (veure l'annex C).

2ª.2) *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.*

– S'han identificat arxius de tipus *Microsoft Word*, propietat de l'usuari **Juan Solo**, amb contingut relacionat amb l'elaboració de substàncies estupefaents i també fotografies de productes químics, pastilles d'èxtasi i altres drogues sintètiques (veure l'annex C).

– S'han localitzat fotografies de laboratoris clandestins, mostrant eines i maquinaria, per produir substàncies estupefaents. Aquestes fotografies es troben a una carpeta del programari d'emmagatzematge i compartició *on line Dropbox*, propietat de l'usuari **Juan Solo** (veure l'annex D).

– En referència al canal de distribució de les pastilles s'han trobat dues possibilitats. D'una banda, existeixen evidències d'un canal de venda directa tal i com s'ha exposat a la resposta al extrem 2ª.1. D'altra banda, tot i haver trobat indicis de participació en el portal *Silk Road*, un supermercat de venda directa de drogues i substàncies il·legals a través d'Internet, als historials de *navegació web* de l'usuari **Juan Solo**, no es pot confirmar la realització de transaccions mitjançant aquest canal (veure l'annex G).

– S'han trobat tres adreces de correu electrònic que al·ludeixen al terme "*lab*" (laboratori en llengua anglesa): *happy_labs@hotmail.es*, *ppy_lab@hotmail.es* i *y_lab@hotmail.es* (veure l'annex H).

2ª.3) *Determinar l'existència de terceres persones que col·laborin en el procés de producció, distribució o venda de les pastilles estupefaents*.

– Després de realitzar l'anàlisi de les proves aportades per la part demandant, aquest pèrit no ha trobat evidències de la participació de terceres persones que col·laborin en el procés de producció, distribució i/o venda de substàncies estupefaents.

2ª.4) *Determinar si existeixen activitats il·legals de falsificació i ús fraudulent de targetes de crèdit.*

– S'han localitzat les numeracions vàlides de cinc targetes de crèdits a un fitxer de text ocultat, fent servir tècniques de esteganografia, dins de l'arxiu d'imatge **Vacaciones_Budapest 2012 424.bmp**, que és propietat de l'usuari **Nadine** (veure l'annex D).

– S'han localitzat visites a botigues *on line* mostrant interès en l'adquisició d'articles de luxe (abrics de pell i joies) a l'historial del *navegador web Mozilla Firefox* pertanyent a l'usuari **Nadine** (veure l'annex G).

– S'han localitzat visites a pàgines *web* que ofereixen informació, manuals, maquinari específic i petits programes utilitzats en el procés de generació de nombres de targetes de crèdit falses a l'historial del navegador *Google Chrome* de l'usuari **Nadine** (veure l'annex G).

– S'han localitzat pujades de fitxers relacionats amb els nombres de targetes falsos des del disc dur analitzat a un servei d'emmagatzematge i intercanvi d'arxius *on line: www.wetransfer.com*, a l'historial de navegació d'*Internet Explorer* de l'usuari **Nadine** (veure l'annex G).

– S'ha localitzat una conversa entre l'usuari **Juan Solo** i dues persones més al fitxer **whatsapp.db** descrivint el procés de compres fraudulentes amb targetes de crèdit falses (veure l'annex B).

2ª.5) *Determinar l'existència de terceres persones en activitats fraudulentes amb targetes de crèdit*.

– S'ha localitzat l'intercanvi d'un fitxer amb numeracions vàlides per falsificar targetes de crèdit entre l'usuari **Nadine** i una tercera persona anomenada **Irina Luhn** a l'historial de navegació de l'I*nternet Explorer* pertanyent a l'usuari **Nadine** (veure l'annex G).

– S'han localitzat dues persones, **Raul** i **Ivan**, a una conversa a l'interior del fitxer whatsapp.db que descriu la seva participació en la realització de compres fraudulentes amb targetes de crèdit falses. Així mateix, aquest usuaris incorren en altre delictes. D'una banda, **Raul**, l'encarregat de realitzar les compres, utilitza un DNI falsificat. D'altra banda, **Ivan**, l'encarregat de rebre les mercaderies, entra en un domicili sense autorització dels seus propietaris i usurpant la identitat d'aquestes terceres persones (veure l'annex B).

2ª.6) *Determinar si existeixen altres actes delictius comesos pels usuaris de l'ordinador analitzat*.

– L'anàlisi exhaustiu de les evidències digitals aportades pel Jutjat Nº XXX de Barcelona, indiquen que hi ha indicis raonables de la comissió d'un delicte de *pishing* (estafa o suplantació d'identitat amb la finalitat d'obtenir dades sensibles com dades personals, numeracions de comptes corrents, targetes de crèdit, etc.). Examinant el fitxer **whatsapp.db** es localitzen dos missatges enviats per l'usuari **Juan Solo** que confirmen la comissió d'un delicte de *pishing* (veure l'annex B, missatges *nº 4583* i *nº 10162*).

Aquest pèrit considera oportú realitzar una observació que s'hauria de tenir en compte pel Jutjat Nº XXX de Barcelona:

- S'han observat discrepàncies entre la data de captura de la imatge del disc dur i la data de captura de la *Memòria RAM*, aportades com a proves dins de la cadena de custodia. Mentre que la copia del disc dur de l'equip analitzat es va realitzar el dia **26 de Febrer de l'any 2013**, la data de realització de la captura del bolcat de la *Memòria RAM* indicada és el dia **17 de Març de l'any 2013**. (Veure l'annex H).

6. Recomanacions

A continuació s'inclouen algunes recomanacions addicionals que s'haurien de tenir en compte pel Jutjat Nº XXX de Barcelona:

- S'ha localitzat l'ús d'una unitat d'emmagatzematge encriptada per l'usuari J**uan Solo** que no ha estat aportada a la investigació (veure l'annex I).
- S'han localitzat varies contrasenyes dels dos usuaris investigats a l'interior dels fitxers hid1.tt.rtf i hid2.tt.rtf, ubicats al directori arrel (\) del disc dur analitzat (veure l'annex C).
- S'han localitzat dues conversacions a l'interior del fitxer **whatsapp.db** que presenta incongruències en el nom del propietari del *Smartphone*, identificat com "*me*" a l'aplicació *Whatsapp* (veure l'annex I).

Aquest és el meu lleial saber i entendre pericial per al Jutjat Nº XXX de Barcelona.

A Barcelona, 12 de Gener de 2014.

[Signatura]

D. Esteban Bonachera López, Enginyer Tècnic i pèrit judicial.

7. Annex A. Comprovació de les evidències digitals rebudes.

L'objectiu d'aquest informe pericial és determinar si existeix alguna evidència a l'equip analitzat que indiqui que els seus propietaris, o usuaris, han realitzat alguna conducta delictiva relacionada, o no, amb la seva detenció prèvia per possessió de pastilles estupefaents i targetes de banda magnètica en blanc.

Les autoritats policials ens proporcionen la imatge del disc dur i un bolcat de la *memòria RAM* de l'ordinador que estava en funcionament al domicili de les dues persones detingudes. Així mateix, també ens proporcionen una base de dades d'una coneguda aplicació de missatgeria procedent d'un smartphone, propietat d'una de les persones que van ser detingudes. Les dades que ens han proporcionat són:

- **Imatge del disc dur.** Es tracta d'un disc dur WD3200BPVT de la marca Western Digital, amb format de 2,5 polsades, una capacitat de 320 Gigabytes i amb nombre de serie: WX81E32FLU08

Figura 1. Fotografia del disc dur analitzat

Figura 2. Detalls identificatius del disc dur

Les dades que es van extreure del disc dur van ser truncades en set fitxers per facilitar la seva distribució i transport. Es va utilitzar el programari *Hacha* per crear aquests fitxers. A continuació es pot veure la informació relativa als fitxers que ens han proporcionat,

Nom del fitxer	Mida (en Bytes)	Hash
hd_dd.zip.H00	49	43ce67e74d95ee54dcd529d90e59b0ea
hd_dd.zip.H01	672723296	85a6661879410f454a50921b016a695e
hd_dd.zip.H02	672723296	96a9ba6b44d82a084ebd13906d701cf2
hd_dd.zip.H03	672723296	95400bbbc81f12669da9f32d1d260435
hd_dd.zip.H04	672723296	021177347afb2d42ba21bf473d30f3bd
hd_dd.zip.H05	672723296	aa725cb15e116d596ca0274f2c98df12
hd_dd.zip.H06	672723295	54648d05229ff384a35597ff30a538a4

Taula 1. Detalls dels fitxers que contenen la imatge del disc dur a analitzar

```
Hash values calculated during initial creation:
0 - 2097152000: f9a0beb5601ae7281d77b58a84e8f920
0 - 2097152000: 41c9b56c0bd97d74417cd7e14cf7d30c2c6cda67
2097152000 - 4194304000: 516c87230427b5f8905dd90c3d1ac522
2097152000 - 4194304000:
d0f0adf290c4baf633a9a2668cbb19ee62432fc3
4194304000 - 6291456000: ed2a0e3b0a7ec49f28f9c395d6530ae9
4194304000 - 6291456000:
56733b76897c27619677a7185dedfe0eb6a9b181
6291456000 - 8388608000: ba596bcf8aa53f2edd69fb98f1ce9475
6291456000 - 8388608000:
4778cacbf0e714c24576886a439d3faef577ed08
8388608000 - 10485760000: 9fb912ecf16a68cd4c7b8a209b459872
8388608000 - 10485760000:
09fda1a5242aed43332df042fd0ee359bbfb4657
10485760000 - 11062969344: 35b9ad61093849ff9dd20b3d2259cf01
10485760000 - 11062969344:
c9dff5570ac3fa376f19e800f2e14bbab9c425ed
Total (md5): 156223444d86a9a81e73018cafea087c
Total (sha1): 21558da3b475680deb726ff44a67e579717dd102


Hash values for verification started at 20130226 07:26:30:
Total (md5): 156223444d86a9a81e73018cafea087c
Total (sha1): 21558da3b475680deb726ff44a67e579717dd102


Completed verification process at 20130226 07:30:03
```

Figura 3. Detall dels *Hashes* obtinguts en el moment de copiar el disc dur

Es van recalcular els *Hashes* dels set fitxers d'imatge i es van comparar amb els *Hashes* que ens van proporcionat amb les evidències digitals que s'han d'analitzar. Totes les comprovacions van ser positives, és a dir, que cap dels fitxers van estar alterats des de la seva creació. Per comprovar els *Hashes*, es va fer servir l'eina *WinMD5Free v1.20*.

- **Memòria RAM.** Ens proporcionen un bolcat de la *memòria RAM* del sistema analitzat: el fitxer comprimit **ram_adq.rar** d'una mida de 163182910 Bytes. La captura de la *RAM* es va realitzar, fent servir l'eina *mdd*, de els resultats següents,

```
-> mdd
-> ManTech Physical Memory Dump Utility
   Copyright (C) 2008 ManTech Security & Mission Assurance
-> This program comes with ABSOLUTELY NO WARRANTY; for details use option `-w'
   This is free software, and you are welcome to redistribute it
   under certain conditions; use option `-c' for details.
-> Dumping 1015.05 MB of physical memory to file 'ram_adq'.
259843 map operations succeeded (1.00)
9 map operations failed
took 1375 seconds to write
MD5 is: ce6f660f20209fb1e3ac8f28c762db81
```

Figura 4. Bolcat de la memòria *RAM* del sistema analitzat

Per comprovar que el fitxer no ha estat alterat, es calcula de nou el seu *Hash* i es compara amb el *Hash* que podem veure a la captura anterior. S'utilitza l'eina *WinMD5Free v1.20*. Per tant, es pot afirmar que les dades procedents del bolcat de la *memòria RAM* no han estat alterades.

Nom del fitxer	Mida (en Bytes)	Hash
ram_adq	163182910	ce6f660f20209fb1e3ac8f28c762db81

Taula 2. Detalls del fitxer de bolcat de la *memòria RAM*

- **Whatsapp.db**. Fitxer de base de dades d'una coneguda xarxa social que va ser extreta d'un *smartphone* propietat d'una de les dues persones detingudes (veure l'Annex B)

Nom del fitxer	Mida (en Bytes)	Hash (no proporcionat)
whatsapp.db	26624	dd6764cbea3d21bcacf7c9da0f893024

Taula 3. Detalls de la base de dades analitzada

8. Annex B. Anàlisi del fitxer whatsapp.db

Es realitza l'anàlisi del fitxer **whatsapp.db** amb l'eina *Whatsapp Xtract.* Es tracta d'un script desenvolupat en llenguatge *Python* que mostra els missatges intercanviats en aquesta popular aplicació de missatgeria instantània. L'*script* presenta les dades en format *HTML*, mostrant, a més, altres dades d'interès com els nombres de telèfon dels remitents dels missatges i els *mactimes* d'aquests missatges.

De les cinc converses que interessen, només una aporta informació rellevant per la investigació que es duu a terme. Aquesta conversa, identificada amb el **nombre 21453**, proporciona informació molt rellevant sobre diverses activitats il·lícites de **Juan Solo i dues persones més**.

Les dades més rellevants extretes del xat són les següents:

- **Missatge nº 4545.** "*... Jo je aconseguit els numeros i els pins, raul tu fas les compres per internet i ivan t'enviem la mercancia al pis fals de tarragona amb el dni fals k tens...*".

- **Missatge nº 4546.** "*... tu pasam els numeros i pins i vaig al cybercafe de mataro i començo a fer compres a saco*".

- **Missatge nº 4549.** "*... que si fas comandes jo només puc anar al pis de tarragona quan sapigua que els propietaris no hi son!*".

- **Missatge nº 4583.** "*OK deixeu-me una mica per treballar el phising i les alternatives per conseguir més tarjetes...*".

- **Missatge nº 10162.** "*... Ja tinc tots el numeros i pins valids per fer el nostre negoci del segle!!!*".

- **Missatge nº 10176.** "*... perque ho tinc tot amagat al meu ordinador, no m'ho trobaria ni la poli*"

Chat session # 21453: 99999999543-9999999997

PK	Chat	Msg date	From	Msg content	Msg status	Media Type	Media Size
4524	99999999543-9999999997	2011-11-09 23:10:25	me	Bon dia nanos! parlem de com portem el tema de les tarjetes o ja no us atreviu...	4	0	0
4525	99999999543-9999999997	2011-11-09 23:14:09	me	💩	4	0	0
4527	99999999543-9999999997	2011-11-09 23:14:32	34635293190@s.whatsapp.net	Jajajajajajaja	0	0	0
4528	99999999543-9999999997	2011-11-09 23:14:33	34635293190@s.whatsapp.net	Si si! parlem que ja ho tenim tot mig preparadet no?	0	0	0
4544	99999999543-9999999997	2011-11-09 23:19:11	34660401445@s.whatsapp.net	Sip	0	0	0
4545	99999999543-9999999997	2011-11-09 23:20:06	me	bé, doncs tot com vam acordar, jo je aconseguit els numeros i els pins, raul tu fas les compres per internet i ivan t'enviem la mercancia al pis fals de tarragona amb el dni fals k tens. fins aqui tot clar com sempre...	4	0	0
4546	99999999543-9999999997	2011-11-09 23:20:08	34635293190@s.whatsapp.net	cap problema, tu pasam el numeros i pins i vaig al cybercafe de mataro i començo a fer compres a saco!!!	0	0	0
4547	99999999543-9999999997	2011-11-09 23:20:16	34635293190@s.whatsapp.net	Jajajaajajajaja	0	0	0
4548	99999999543-9999999997	2011-11-09 23:20:22	34635293190@s.whatsapp.net	Sk sin noo son nddd	0	0	0
4549	99999999543-9999999997	2011-11-09 23:20:31	34660401445@s.whatsapp.net	eps tranquil eh! que si fas comandes jo només puc anar al pis de tarragona quan sapigua que els propietaris no hi son! aixi que les entregues només poden ser els divendres pel matí!! o la cagem...	0	0	0

Figura 5. Detall de la conversa que proporciona dades rellevants per la investigació

4550	99999999543-9999999997	2011-11-09 23:20:33	34635293190@s.whatsapp.net	OK ivan, oido cocina! quan faci les compres totes les entregues seràn el mateix divendres a aquest horari, jo t'aviso!	0	0	0
4563	99999999543-9999999997	2011-11-09 23:23:54	me	Amén	4	0	0
4583	99999999543-9999999997	2011-11-09 23:27:09	me	OK deixeu-me una mica per trabajar el phising i les alternatives per conseguir més tarjetes.. us dic algo	4	0	0
10155	99999999543-9999999997	2011-12-27 00:20:56	me	 | Image	4	1	47663
10156	99999999543-9999999997	2011-12-27 00:23:06	34635293190@s.whatsapp.net	que es això	0	0	0
10162	99999999543-9999999997	2011-12-27 00:23:39	me	sóc el més fort!! ja tinc tots els numeros i pins valids per fer el nostre negoci del segle!!!	4	0	0
10163	99999999543-9999999997	2011-12-27 00:23:42	me	Jajajajaja	4	0	0
10164	99999999543-9999999997	2011-12-27 00:23:54	34660401445@s.whatsapp.net	jo estic llest que necessito pasta!!	0	0	0
10165	99999999543-9999999997	2011-12-27 00:23:55	34635293190@s.whatsapp.net	jo tb estic llest, quan vulguis m'ho envies }:X	0	0	0
10176	99999999543-9999999997	2011-12-27 00:32:22	me	a més sóc un crack, perquè ho tinc tot amagat al meu ordinador, no m'ho trobaria ni la poli ;p	4	0	0
10177	99999999543-9999999997	2011-12-27 00:32:27	me	som uns profesionals! mira k es facil fer pasta... viscan els sobresous!	4	0	0
10178	99999999543-9999999997	2011-12-27 00:32:30	me	Jajajaja	4	0	0
10179	99999999543-9999999997	2011-12-27 00:33:07	34660401445@s.whatsapp.net	amb tu estem tranquils, ets un crack!	0	0	0

Figura 6. Més missatges que detallen com actuen els interlocutors

10186	99999999543-9999999997	2011-12-27 00:34:14	34635293190@s.whatsapp.net	eres la ...	0	0	0
10188	99999999543-9999999997	2011-12-27 00:34:43	34635293190@s.whatsapp.net	💣	0	0	0
10189	99999999543-9999999997	2011-12-27 00:34:47	34635293190@s.whatsapp.net	Jajajjaajaja	0	0	0
10197	99999999543-9999999997	2011-12-27 10:21:55	me	raul ja ho tens al correu, el pwd del zip es somunscracks ... cordinat amb ivan i ja parlarem de repartir..	4	0	0
10200	99999999543-9999999997	2011-12-27 10:22:28	34635293190@s.whatsapp.net	OK	0	0	0
21442	99999999543-9999999997	2012-02-15 23:31:57	34635293190@s.whatsapp.net	estais aquí? mi vecina me ha dicho que ha venido la policia a mi casa pero no han dicho nada...sera una multa... pero por si acaso os aviso...	0	0	0

Figura 7. Detall del missatge número 10197, que ens informa dels noms dels interlocutors i d'una contrasenya d'un fitxer *sospitós*

9. Annex C. Informació trobada als fitxers del disc dur

Aquest annex conté el llistat de la informació rellevant que s'ha trobat a diversos arxius de la imatge del disc dur analitzat,

Nom del fitxer	Localització	Mida (en Bytes)
hid1.t.rtf	Directori arrel (\)	352
hid2.t.rtf	Directori arrel (\)	314
Contactos.rar	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\	4868
Vacaciones_Budapest.jpg.odt	\Documents and Settings\Nadine\Mis documentos\Mis imágenes\Vacaciones 2012\	7460
chatmsg256.dbb	\Documents and Settings\Juan Solo\Datos de programa\Skype\juan_solo23\	2640
Donna Leon – Altas esferas.doc	\Documents and Settings\Juan Solo\Mis documentos\eBooks\Novela de Suspense y Policial\Leon\	28973
Donna Leon – Justicia uniforme.doc	\Documents and Settings\Juan Solo\Mis documentos\eBooks\Novela de Suspense y Policial\Leon\	36318
Donna Leon – Muerte en la Fenice.doc	\Documents and Settings\Juan Solo\Mis documentos\eBooks\Novela de Suspense y Policial\Leon\	31399
Donna Leon – Veneno de cristal.doc	\Documents and Settings\Juan Solo\Mis documentos\eBooks\Novela de Suspense y Policial\Leon\	14109

Taula 4. Detalls dels fitxers que contenen informació rellevant

Nom del fitxer	Hash MD5	Modificació	Últim accés	Creació
hid1.t.rtf	23aee361948b00dcff14536ae681063e	25/02/2013 19:25:58	25/02/2013 19:44:32	25/02/2013 19:44:32
hid2.t.rtf	3ae803bfeb00f11ae767bfae72ae02d2	25/02/2013 19:26:44	25/02/2013 19:44:32	30/12/1899 00:00:00
Contactos.rar	2b02818561a1bb85feba176cd34fde96	31/01/2013 08:37:09	03/02/2013 22:47:32	31/01/2013 18:27:48
Vacaciones_Budapest.jpg.odt	80d8d2feb7c731d7c32023b994b5af0e	27/01/2013 12:07:21	27/01/2013 17:52:40	27/01/2013 12:04:50
chatmsg256.dbb	0558bb4b4afe22c28d1413ada0b16276	25/02/2013 20:29:49	25/02/2013 20:29:49	31/01/2013 22:54:29
Donna Leon – Altas esferas.doc	274dcc18618d42c2f303c92246a5d914	31/01/2013 20:22:06	25/02/2013 19:47:11	31/01/2013 20:36:54
Donna Leon – Justicia uniforme.doc	eba8b3eaf1b7860e6cc6fa80d5b14a03	31/01/2013 20:22:30	25/02/2013 19:47:11	31/01/2013 20:36:54
Donna Leon – Muerte en la Fenice.doc	7b0337849be5d17644a70ca9647893d3	31/01/2013 20:22:50	25/02/2013 19:47:11	31/01/2013 20:36:54
Donna Leon – Veneno de cristal.doc	f45f3370a7f27004ac14db6568c9fb0c	31/01/2013 20:23:18	25/02/2013 19:47:11	31/01/2013 20:36:54

Taula 5. Mactimes i Hashes dels arxius rellevants que s'han analitzat

A continuació es detallarà la informació continguda a cada un dels fitxers mostrats,

Hid1.t.rtf i hid2.t.rtf. Aquests dos fitxers es troben al directori arrel del disc dur analitzat. Crida l'atenció l'aparició d'aquests arxius a la partició principals de *Windows*, doncs no són fitxers estàndards del sistema operatiu, es tracta de fitxers de text que poden ser escrits o llegits amb qualsevol editor. El seu contingut s'observa a les següents captures,

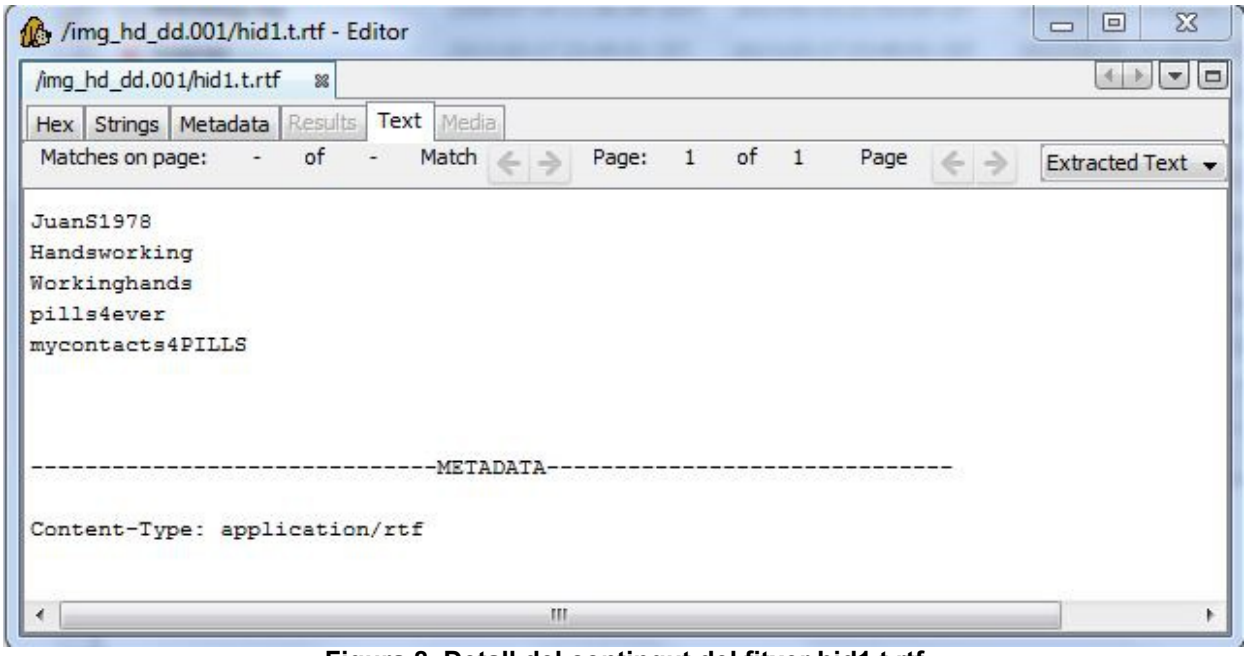


Figura 8. Detall del contingut del fitxer hid1.t.rtf

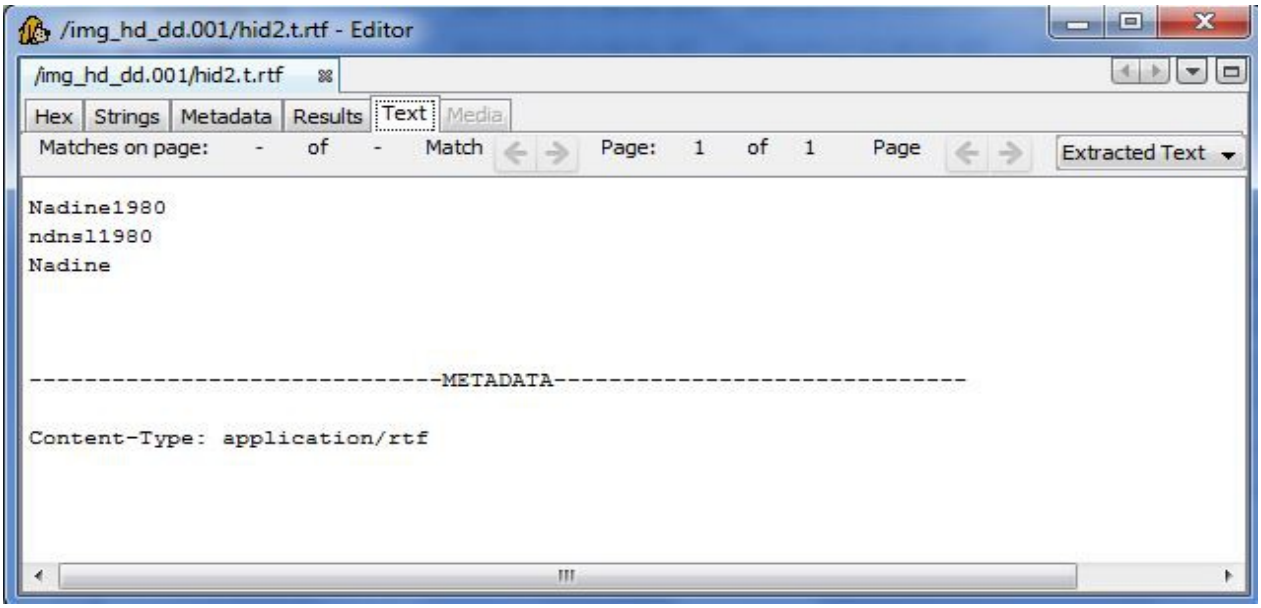


Figura 9. Contingut del fitxer hid2.t.rtf

Contactos.rar. Aquest fitxer comprimit es troba protegit amb una contrasenya que impossibilita la seva extracció i la visualització del seu contingut. Es va intentar obrir amb el programa *Winzip* fent servir les contrasenyes que apareixen al fitxer **hid1.t.rtf**. Un dels passwords, **pill4ever**, va possibilitar obrir i descomprimir l'arxiu. El resultat es una taula de *Microsoft Excel* que conté les dades de contacte de quatre persones,

	A	B	C	D
1	Enrique Ley	546373788	Avenida de la Industria, 2, 2-3	
2	María Hernández	917647733	C/Horticultura, 45	
3	Eladio Cifuentes	436778124	Calle de la Luz, 34, 5-6	
4	Mario Clua	934529977	Avenida de la Primavera, 3, 4-3	
5				
6				

Figura 10. Detall de les dades personals contingudes al fitxer Contactos.rar

Vacaciones_Budapest.jpg.odt. Es tracta d'un fitxer de text creat amb el processador de text de l'*OpenOffice*, el seu contingut és molt interessant,

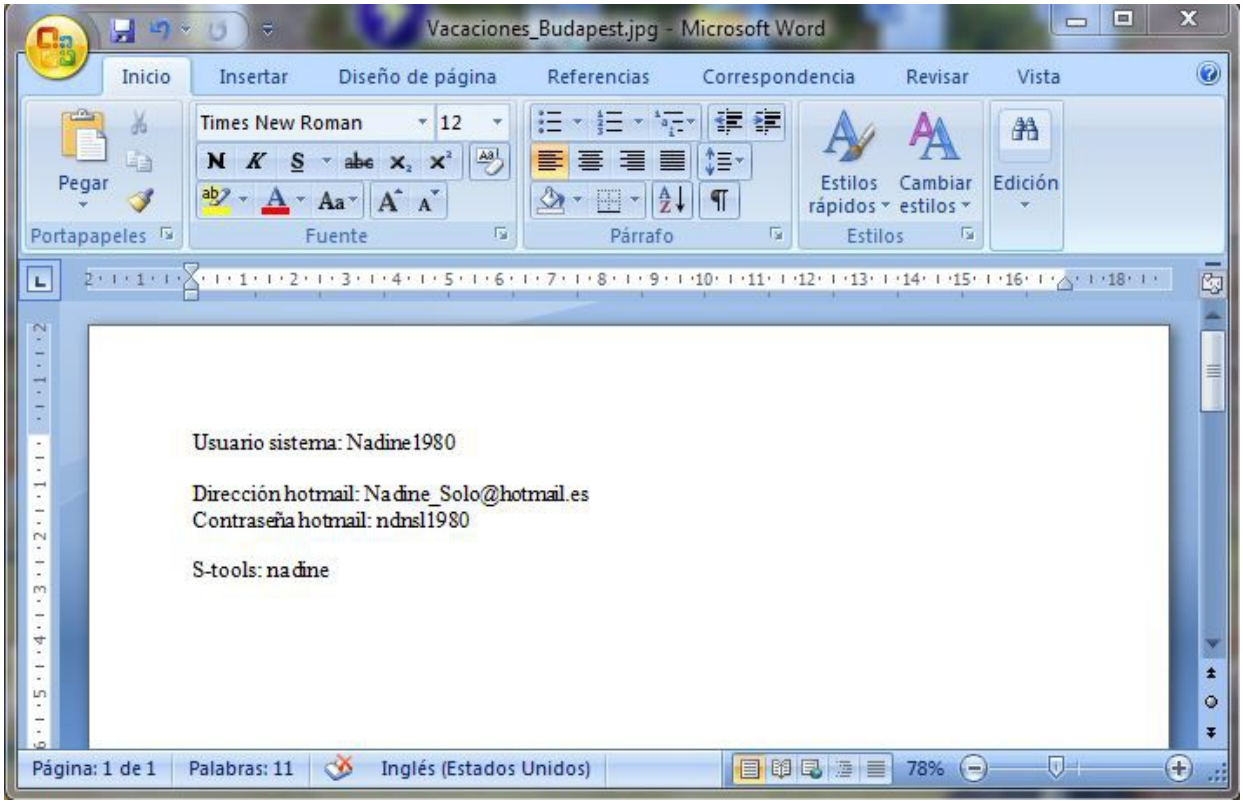


Figura 11. Detall de les contrasenyes amagades dins del fitxer analitzat

chatmsg256.dbb. Aquest fitxer conté l'historial d'una conversa, mitjançant el programari *Skype*, entre l'usuari de l'equip analitzat, **Juan Solo**, i una tercera persona anomenada l**rina Luhn**. Aquesta conversa va tenir lloc el dia 25 de febrer de 2013 i el seu contingut es pot observar a la següent captura,

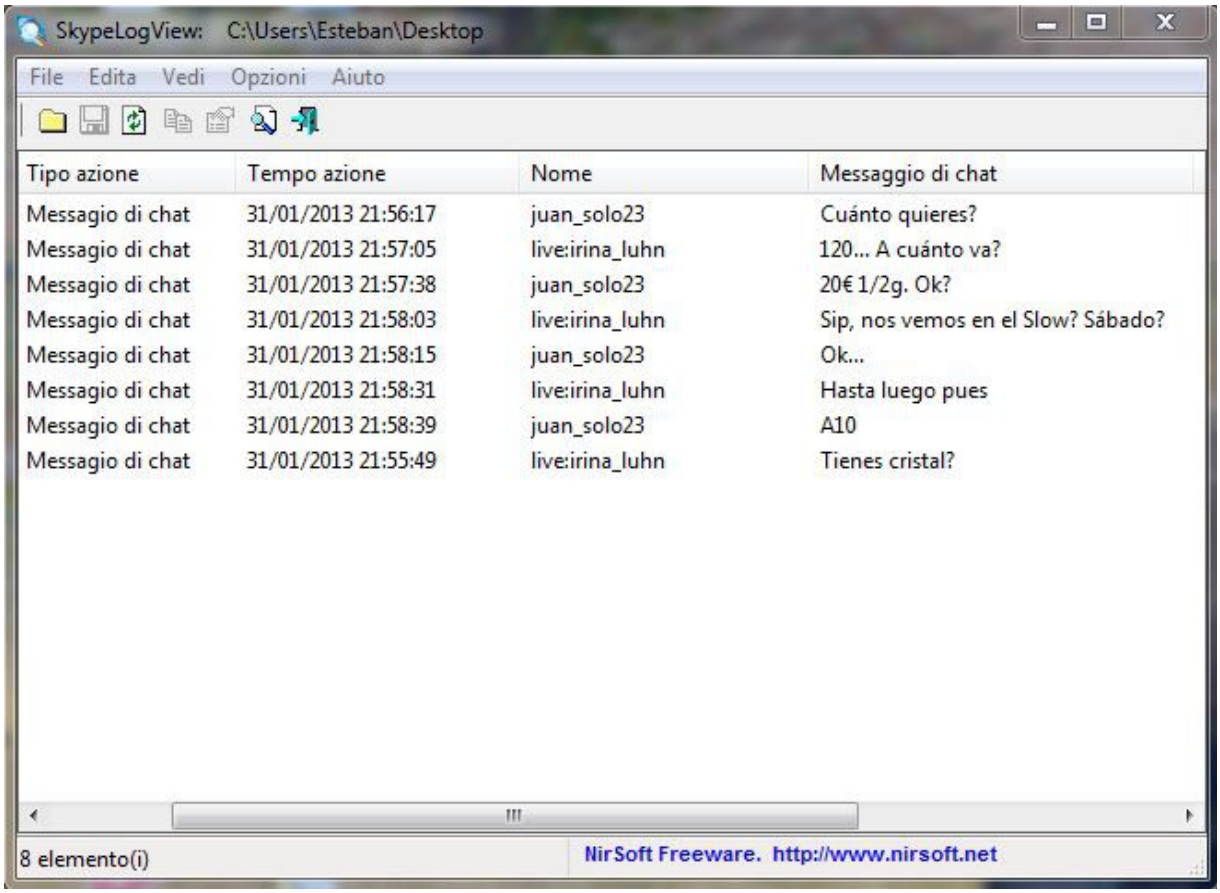
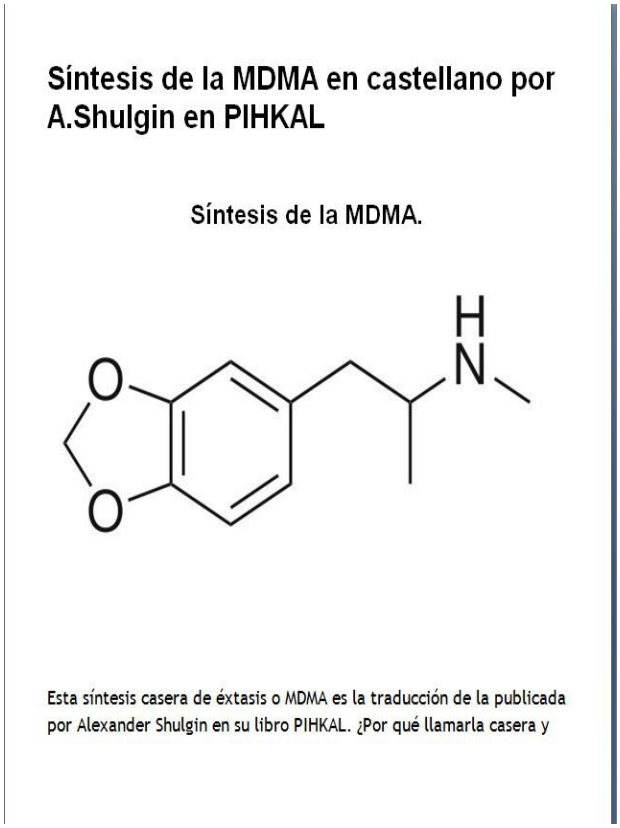


Figura 12. Detall de la conversa entre l'usuari Juan Solo i Irina Luhn

Donna Leon – Altas esferas.doc, Donna Leon – Justicia uniforme.doc, Donna Leon – Muerte en la Fenice.doc i Donna Leon – Veneno de cristal.doc. Aquest grup de quatre fitxers es troben a la carpeta *eBooks* de l'usuari **Juan Solo**. Crida molt l'atenció que siguin els únics que tenen extensió *.doc* en comptes de *.pdf*, com la resta de fitxers d'aquesta carpeta. Obrint els arxius es veu clarament que no corresponen a cap novel·la ni a cap obra literària, es tracta de documents o manuals, il·lustrats, que expliquen com crear drogues sintètiques tant en llengua castellana com en llengua anglesa.

Figura 13. Imatges de drogues sintètiques contingudes a l'arxiu Altas esferas.doc



Síntesis de la MDMA en castellano por A.Shulgin en PIHKAL

Síntesis de la MDMA.

Esta síntesis casera de éxtasis o MDMA es la traducción de la publicada por Alexander Shulgin en su libro PIHKAL. ¿Por qué llamarla casera y qué significa eso exactamente? Es casera porque tanto las cantidades como los tiempos están ajustados para producir pequeños lotes de la sustancia, y porque no requiere maquinaria industrial sino que basta con la que se puede tener en un pequeño laboratorio montado en un lugar adecuado, en una casa o en otro lugar.
Esta síntesis no está optimizada ni ajustada para producir grandes cantidades (industriales) de MDMA, sino para la síntesis del éxtasis por varias rutas pero siempre a pequeña escala (unos gramos).

¿Qué NO significa lo de casera?
No significa que con tener una casa, ya puedas realizar esta síntesis.
No significa que puedas sustituir el material de laboratorio por las cazuelas y vasos que tengas por casa.
No significa que por leer esta receta, vayas a poder comprar 3 productos a una farmacia, mezclarlos, calentarlos un rato y que por eso vayas a obtener nada parecido a la MDMA.
No significa que sin conocer y entender algunos conceptos y procedimientos básicos en química, estés capacitado para intentar sintetizar nada.

Además de los obvios peligros que enfrenta quien se pone a realizar síntesis con solventes volátiles e inflamables, productos corrosivos (ácidos y bases) y fuentes de calor, hay que recordar que la síntesis de algunos compuestos -entre otros la MDMA- es un delito en la mayoría de países si no has obtenido la autorización previa del organismo de

Figura 14. Detall del contingut del fitxer Justicia uniforme.doc

[www.rhodium.ws] [] [Chemistry Archive]

A Complete MDMA Synthesis for the First Time Chemist

Compilation and Editorial by Bright Star

HTML and Pictures by Rhodium

Introduction

Thanks to Strike, Rhodium, Ritter, Osmium, r2d3, Semtex Enigma, Spiceboy, ChemHack, Labrat, Eleusis, Ketone/LabGrrrl, and a personal hero, Dr. Shulgin. And to the object that made this possible - the Internet.
Disclaimer: *This is for theoretical argument only. IF someone chooses to follow this synthesis, note that the product has been 'Scheduled 1' by the United States Government, and offenders can be prosecuted. In no way do I condone this activity.*
This is a hypothetical synthesis for: 3,4-methylenedioxy-N-methylamphetamine. Or MDMA.HCl. Or Ecstasy. The synthesis as described **1.** does not put off nasty fumes, **2.** doesn't require suspicious chemicals, and therefore is **3.** perfect for the clandestine chemist. The synthesis itself can be performed in a series of weekends or in a straight shot. If one were to follow this exactly - with no shortcuts - buying everything they're told - doing exactly what is written - they and they're friends will have a lovely spring. For those who think they are better than the instructions as written - be prepared to screw it up at least 4 times before success (or you finally figure out I'm right). Be prepared to invest ~$800. Be prepared to read and learn. It's also a good idea when investing in chemicals to buy 5x what is needed for a synthesis - this way you can repeat it without buying it again. Read the whole thing before you start. There is some prep-work that can be done ahead of time, or while you're distilling. Good luck.

Overview:

Distillation: of Natural Oil to obtain pure Safrole
Rxn: Formaldehyde + Ammonium Chloride -> MethylAmine.HCl (MeAm.HCl)
Rxn: Safrole -(Wacker Oxidation(PdCl$_2$+Benzoquinone))-> MDP2P
Distillation: of Reaction contents to yield pure MDP2P
Rxn: MDP2P -(Al/Hg Amalgam (MeAm.HCl) -> MDMA oil
Crystallization: (MDMA oil + HCl in IPA/Xylene) (anhydrous conditions)

What you need:

This list is the basics. Do not even start this without **ALL** the Chemicals and Apparatus.

Apparatus and Glass:

'The Organic Chem Lab Survival Manual' *by James W. Zubrick.* (A must, throughout this text, pages from this book will be mentioned. ~32$) (and very handy pictures of glass set-ups)
Distillation Apparatus (1x500mL and 1x1000mL Round Bottom Flask, 1x250mL Round Bottom Flask, condenser, distillation adapter, vacuum adapter, thermometer adapter) (Get Ground Glass Joints. These are the best. 19/22 or 24/40 - my first set was 19/22 - and is still used to this day.)
Thermometer (0°C to ~300°C)
Stand (Home Depot - (2x10in., flange, 2 ft. of Vain pipe))
Clamp (Buy it. Trust me its worth it) (for holding the glassware to the stand - these support several hundred dollars in glass - buy a nice one!)
Hotplate/Stirrer combo (got to have it, its worth it) (www.labx.com - spend $200)
Magnetic stir bar (look on the Web) (teflon coated)
Water Aspirator (or a good vacuum source. But aspirators are cheap <$20)
Boiling Stones (for distillations. Small shards from a broken coffee mug)
Tubing (about 10ft. total (3 meters) - hardware store - vacuum tubing is better than dialysis tubing - but both will work)
Vaseline (not much - for coating of the ground glass joints)
Measuring Cups (Preferably pyrex, and in milliliters (mL))
10 various sized glass containers/bottles (250mL, 500mL, 1L, 2L etc)
Scale (a three beam analytical balance are great - and can be found for less than $100 - www.balances.com - they can weigh as much as a kilo and as little as 0.1g - perfect!)
pH paper (chemical supply) (just one roll will do - ~10$) (nothing specific, just need to tell the difference between an acid and a basic solution)

Chemicals:

Safrole (160g)(sassafras oil, yellow camphor oil) (Natural/Essential Oil distributor)
Dimethylformamide (DMF) (350mL) (Diethylformamide or Formamide will work)
p-Benzoquinone (Quinone, Benzoquinone) (120g) (Photo Shop, or Chem supply)
Palladium Chloride ($PdCl_2$) (2g) (Photo Shop, or chem supply)
Methylene Chloride (DiChloroMethane, DCM) (this can be distilled from automotive solvents (just go into Nationwise, PepBoys, Sears, AutoZone And read the labels) Or a Liter can be bought from a Chem supplier.)(Zip-Strip furniture polish remover)
Hg salt (1 gram of: $HgCl_2$, $Hg(NO_3)_2$, $Hg(OAc)_2$, HgCl, It can be anything, and 1g should last you a long time.)
Isopropyl Alcohol (IPA, Pharmacies 91% Isopropyl Alcohol will be available)(get +3L)(don't get the 70% stuff) (or you can get pure stuff from a chem supplier)
Epsom Salts (Magnesium Sulphate) ($MgSO_4$) (grocery store/pharmacy) (Spread out on a cookie sheet, and bake in the oven at 200°C for 3hr to dry them - pretty useless if you don't dry it)
Thick Al foil (heavy duty, or pie pans from the Grocery store)
Muriatic Acid (31.45% HCl)(Pool pH down, Driveway cleaner, ~3$/gallon)
Sodium Hydroxide (NaOH) (Drain Cleaner Crystals) (Read these labels. Get the stuff that is JUST NaOH.) (Red Devil Lye, Lye - Hardware Store)
Ammonium Chloride (NH_4Cl) (Photo Store or Chem Supplier)
Paraformaldehyde (Hardware store) (called Mildewcyde or DiGas - made by the same people who brought you Damp-Rid - hint-hint)
Peanut oil (this is a high boiling oil that we will use as an oil bath on the hotplate/stirring plate combo)
Acetone (for cleaning your glass and crystal work-up) (Paint Section of Hardware Stores)
Xylene (for crystallization) (paint section - thinner - get it specifically)

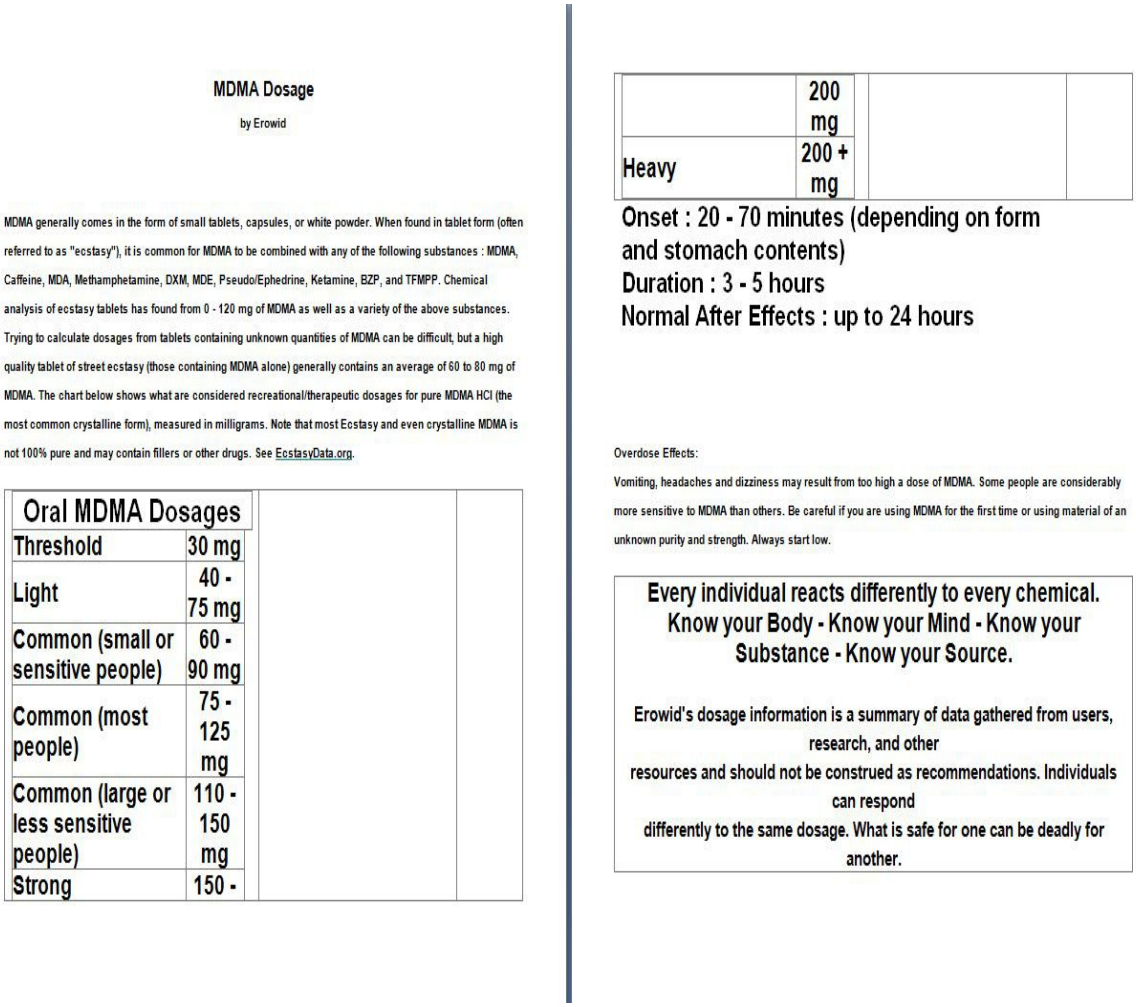
Step 1. (4 hours)

1. Distillation: of Natural Oil to obtain pure Safrole.

A Comprehensive Description of This Step by Chromic
Set up for a vacuum distillation like on page 53 of Zubrick. Always put a little Vaseline on the ground glass joints - this way they won't stick when you try to take them apart. Put as much Natural oil (Sassy, Camphor, ect) as you have, but not more than 300mL, into the 500mL Round Bottom Flask (RBF) with several Boiling Stones. Put one of your 250mL RB flasks as the receiving flask. Set up your Water Aspirator Vacuum, in the sink (this may require setting this up a day before - parts, trips to the plumbing store, etc.) and attach the vacuum hose to the aspirator and then to the vacuum adapter on the distillation set up. Start turning up the heat slowly! SLOWLY! The slower you do it, the better/purer your safrole will be. At normal pressure safrole boils at 232°C - but under your vacuum, it may boil at anywhere from 110-160°C. Whatever temp it starts to come over at - make a note of it. And if the temp is higher than 160°C - check your seals on the tubing and glassware - More than likely there is a little leak. Remember that Vaseline! At the end of the distillation, you should have a water white oil that really refracts light - And has a lovely smell - a little like potpourri.
Distillation set-up: *Set up the distillation set-up on your bed, before you try to put it together on the stand. You will get a good idea about how the pieces go together, and become familiar with the fragility of the whole thing. Read Zubrick for advise about where to place the clamp.*
The Peanut Oil: *A bowl with a flat bottom rests on the Hotplate. It is filled with Peanut Oil. The distillation flask sits in the bowl but not touching the bottom, so that the Hotplate heats the bowl, the bowl heats the Peanut Oil, the Peanut Oil heats the distillation flask. This is VERY effective. And will be perfect for all your distillation needs - especially if you do it under vacuum.*

Step 2. (2 hour work + 4 hours wait + 4 hours work)

Figura 15. Contingut del fitxer Muerte en la Fenice.doc, explicant la síntesi de la MDMA



MDMA Dosage

by Erowid

MDMA generally comes in the form of small tablets, capsules, or white powder. When found in tablet form (often referred to as "ecstasy"), it is common for MDMA to be combined with any of the following substances : MDMA, Caffeine, MDA, Methamphetamine, DXM, MDE, Pseudo/Ephedrine, Ketamine, BZP, and TFMPP. Chemical analysis of ecstasy tablets has found from 0 - 120 mg of MDMA as well as a variety of the above substances. Trying to calculate dosages from tablets containing unknown quantities of MDMA can be difficult, but a high quality tablet of street ecstasy (those containing MDMA alone) generally contains an average of 60 to 80 mg of MDMA. The chart below shows what are considered recreational/therapeutic dosages for pure MDMA HCl (the most common crystalline form), measured in milligrams. Note that most Ecstasy and even crystalline MDMA is not 100% pure and may contain fillers or other drugs. See EcstasyData.org.

Oral MDMA Dosages	
Threshold	30 mg
Light	40 - 75 mg
Common (small or sensitive people)	60 - 90 mg
Common (most people)	75 - 125 mg
Common (large or less sensitive people)	110 - 150 mg
Strong	150 - 200 mg
Heavy	200 + mg

Onset : 20 - 70 minutes (depending on form and stomach contents)
Duration : 3 - 5 hours
Normal After Effects : up to 24 hours

Overdose Effects:

Vomiting, headaches and dizziness may result from too high a dose of MDMA. Some people are considerably more sensitive to MDMA than others. Be careful if you are using MDMA for the first time or using material of an unknown purity and strength. Always start low.

Every individual reacts differently to every chemical. Know your Body - Know your Mind - Know your Substance - Know your Source.

Erowid's dosage information is a summary of data gathered from users, research, and other resources and should not be construed as recommendations. Individuals can respond differently to the same dosage. What is safe for one can be deadly for another.

Figura 16. Detall dels efectes la MDMA segons la dosi, contingut al fitxer Veneno de cristal.doc

10. Annex D. Informació d'imatges trobades al disc dur

El arxius de gràfics o fotografies trobats, i que mereixen una atenció especial, es descriuen a les següents taules:

Nom del fitxer	Localització	Mida (en Bytes)
ecstasylab1.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	151775
ecstasylab10.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	133328
ecstasylab2.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	121957
ecstasylab3.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	145884
ecstasylab4.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	132848
ecstasylab5.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	115761
ecstasylab6.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	132523
ecstasylab7.jpg	\Documents and Settings\Juan Solo\Mis documentos\Dropbox\Lab\	126662
DSCN2687.jpg	\Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	3234252
DSCN2688.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	3234440
DSCN3223.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	2323760
DSCN3273.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	3583890
DSCN3274.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	3584071
DSCN3336.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	2055235
DSCN3349.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	2421917
DSCN3353.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2011	2119042
Budapest Verano 2012 064.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4628195

Taula 6a. Detalls dels fitxers d'imatge analitzats

Nom del fitxer	Localització	Mida (en Bytes)
Budapest Verano 2012 087.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4855662
Budapest Verano 2012 091.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4730176
Budapest Verano 2012 152.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4222904
Budapest Verano 2012 179.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4852769
Budapest Verano 2012 181.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4685603
Budapest Verano 2012 221.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4638734
Budapest Verano 2012 225.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4150882
Budapest Verano 2012 318.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4654512
Budapest Verano 2012 356.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4227793
Budapest Verano 2012 424.bmp *	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	36000054
Budapest Verano 2012 424.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	4893422
DSCN3794.jpg	Documents and Settings\Nadine\Mis documentos\Mis imágines\Vacaciones 2012	1528037

Taula 6b. Detalls de la resta de fitxers d'imatge analitzats

Nom del fitxer	Hash MD5	Modificació	Últim accés	Creació
ecstasylab1.jpg	da1ef8691743e1be6e977eb5a1165fe1	27/01/2013 20:02:39	25/02/2013 19:49:29	03/02/2013 00:08:26
ecstasylab10.jpg	d41a4fb44714a1e82323357f53f786a6	27/01/2013 20:04:44	03/02/2013 00:08:27	03/02/2013 00:08:26
ecstasylab2.jpg	a5716c97275778109639558cbb41f437	27/01/2013 20:02:50	03/02/2013 00:08:27	03/02/2013 00:08:27
ecstasylab3.jpg	ca86a3c44a7bcabb87e2f9bd89c0cf73	27/01/2013 20:03:07	03/02/2013 00:08:27	03/02/2013 00:08:27
ecstasylab4.jpg	26990bdb75706ffd8b505b90022aa081	27/01/2013 20:03:23	03/02/2013 00:08:27	03/02/2013 00:08:27
ecstasylab5.jpg	43cb2792e7cbc7a414a2bce4820a71e9	27/01/2013 20:01:37	03/02/2013 00:08:27	03/02/2013 00:08:27
ecstasylab6.jpg	e376cbc38f40c6d311afd1d946de1f53	27/01/2013 20:02:25	03/02/2013 00:08:27	03/02/2013 00:08:27
ecstasylab7.jpg	6310cc89bc24729164a655cde095909d	27/01/2013 20:03:52	03/02/2013 00:08:27	03/02/2013 00:08:27
DSCN2687.jpg	9a53a2df1ed0d9c554f07152583cd370	29/08/2010 17:44:48	26/01/2013 21:02:46	26/01/2013 18:09:29
DSCN2688.jpg	ac7b1958bbb908dc7967ce1997c12845	18/07/2012 12:26:18	26/01/2013 21:02:48	26/01/2013 18:09:29
DSCN3223.jpg	9cd9290ec79646cd19515a5f1b629f8d	22/08/2011 12:15:00	26/01/2013 18:09:29	26/01/2013 18:09:29
DSCN3273.jpg	0b3f7b0533004c4512633feda5b6426c	24/08/2011 16:19:54	26/01/2013 18:09:30	26/01/2013 18:09:29
DSCN3274.jpg	c56f290d067907f8a7a29a7169489a1f	18/07/2012 12:28:06	26/01/2013 21:03:08	26/01/2013 18:09:30
DSCN3336.jpg	159bfcad5e5583af07d3353355d69f46	24/08/2011 16:21:12	26/01/2013 18:09:30	26/01/2013 18:09:30
DSCN3349.jpg	543a1362aaa6226271fafafe68ec7220	23/08/2011 11:05:28	26/01/2013 18:09:30	26/01/2013 18:09:30
DSCN3353.jpg	c25086b6a3f78daf9ac36943a0157549	23/08/2011 11:08:10	26/01/2013 18:09:30	26/01/2013 18:09:30
Budapest Verano 2012 064.jpg	45dcef513f9ec4d525a3f0ae159b79e8	20/08/2012 18:02:58	26/01/2013 19:58:35	26/01/2013 19:58:35
Budapest Verano 2012 087.jpg	1c14d0bfafe7bae88dd8c1f7d5f6d9b9	20/08/2012 18:03:18	26/01/2013 19:58:36	26/01/2013 19:58:35
Budapest Verano 2012 091.jpg	138f093158673f9df6fda3954faa0b61	20/08/2012 18:03:20	26/01/2013 19:58:36	26/01/2013 19:58:36
Budapest Verano 2012 152.jpg	6178c634c6cc0c70ef1cd8860c2bf2e7	20/08/2012 18:04:12	26/01/2013 19:58:36	26/01/2013 19:58:36
Budapest Verano 2012 179.jpg	d10ca852d6c1b8f6d71650686aadd76c	20/08/2012 18:04:32	26/01/2013 19:58:36	26/01/2013 19:58:36
Budapest Verano 2012 181.jpg	d99330b67f771bd6c49b8014e2ceed3d	20/08/2012 18:04:32	26/01/2013 19:58:37	26/01/2013 19:58:36

Taula 7a. Mactimes i Hashes dels arxius d'imatge que s'analitzen

Nom del fitxer	Hash MD5	Modificació	Últim accés	Creació
Budapest Verano 2012 221.jpg	b7a65098960ea96bf7eb77156af45ff1	20/08/2012 18:05:04	26/01/2013 19:58:37	26/01/2013 19:58:37
Budapest Verano 2012 225.jpg	a2e4a5c6712750c094c6a0751bd023a7	20/08/2012 18:05:08	26/01/2013 17:52:17	26/01/2013 19:58:37
Budapest Verano 2012 318.jpg	16a9740fe0e660d4abc264176e9998e7	20/08/2012 18:06:22	26/01/2013 19:58:35	26/01/2013 19:58:34
Budapest Verano 2012 356.jpg	dcf8c1792c591193f8602412666ba093	20/08/2012 18:06:52	26/01/2013 19:58:35	26/01/2013 19:58:35
Budapest Verano 2012 424.bmp *	412980739992d3b983d94a6f60c57780	26/01/2013 20:36:39	26/01/2013 12:09:22	26/01/2013 20:36:38
Budapest Verano 2012 424.jpg	28802bdf40c7f76de0c59da366b7865d	20/08/2012 18:07:50	26/01/2013 12:09:03	26/01/2013 19:58:35
DSCN3794.jpg	0ca169c734d7442beb77b9521ae0c19e	16/08/2012 11:44:40	26/01/2013 17:52:09	26/01/2013 19:58:35

Taula 7b. Continuació de les Mactimes i Hashes dels fitxers d'imatge analitzats

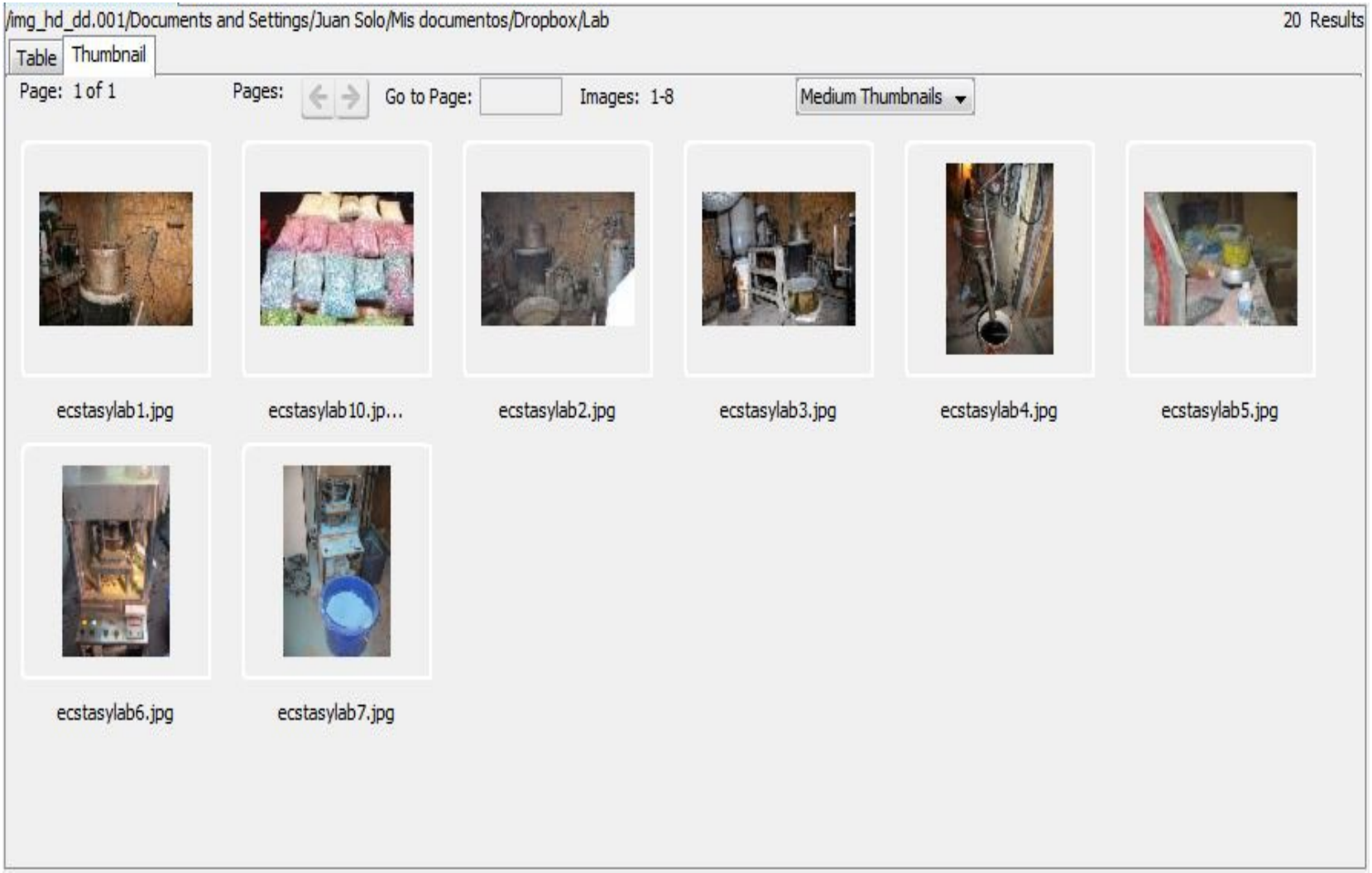


Figura 17. Imatges del que sembla un laboratori clandestí, emmagatzemades a la carpeta d'arxius de Dropbox

De tots els fitxers d'imatges analitzats, cal destacar l'arxiu **Budapest Verano 2012 424.bmp**, doncs ni la seva mida ni la seva extensió, o tipus d'arxiu, és coherent amb la resta d'imatges que es troben a la mateixa carpeta.

S'analitza aquesta imatge amb el programari *S-Tools* i es descobreix un arxiu de text ocult al seu interior, esteganografia. Aquest fitxer de text conté numeracions vàlides de targetes de crèdit, incloent el CCV.

Nom fitxer	Hash MD5
Numeraciones_tarjetas.txt	b468be09ea67d34e7e72e25294d9018d

Taula 8. Detalls del fitxer ocult dins d'una imatge

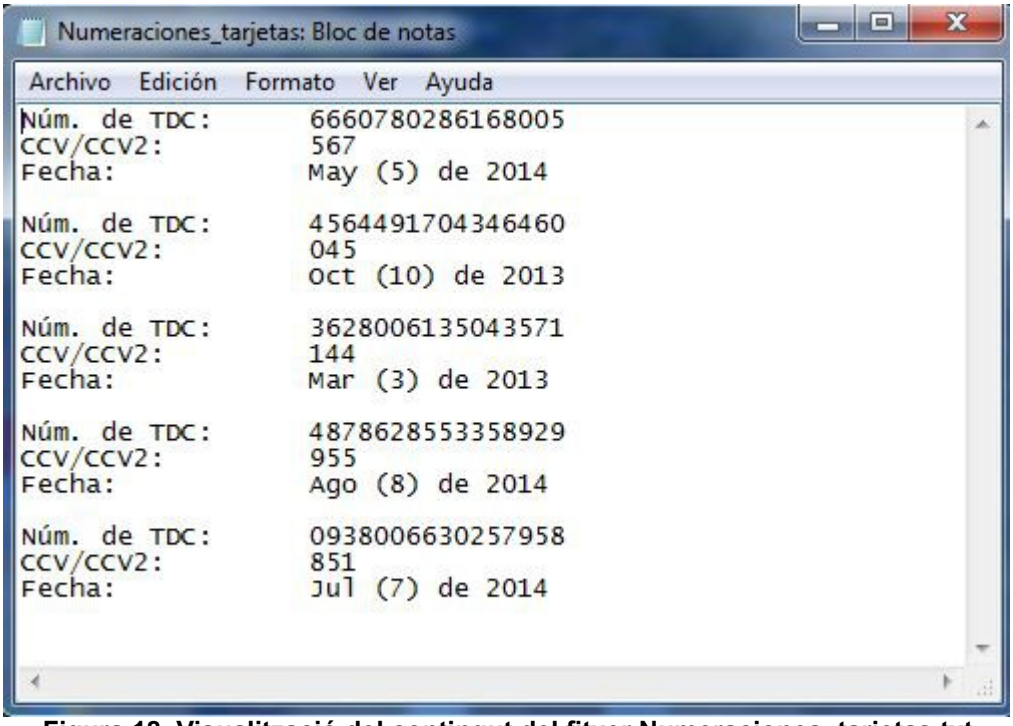


Figura 18. Visualització del contingut del fitxer Numeraciones_tarjetas.txt

11. Annex E. Recuperació de fitxers eliminats

Es realitza l'anàlisi de la imatge de disc dur proporcionada per les autoritats policials per cercar els elements, arxius o carpetes, que han estat eliminats per part dels usuaris investigats. Un cop detectades les dades eliminades, s'intentarà la seva recuperació.

S'utilitza l'eina *ProDiscover Basic* per cercar i extreure els fitxers eliminats. Aquest programari separa els fitxers eliminats en dos grups. D'una banda, mostra els fitxers que ja han estat esborrats i, d'altra banda, els arxius que han estat enviats a la *Paperera de reciclatge*, però encara no s'han eliminat definitivament.

Com es pot observar a les següents captures, la *Paperera de reciclatge* de l'usuari **Juan Solo** conté arxius que recentment s'han eliminat i que es poden recuperar,

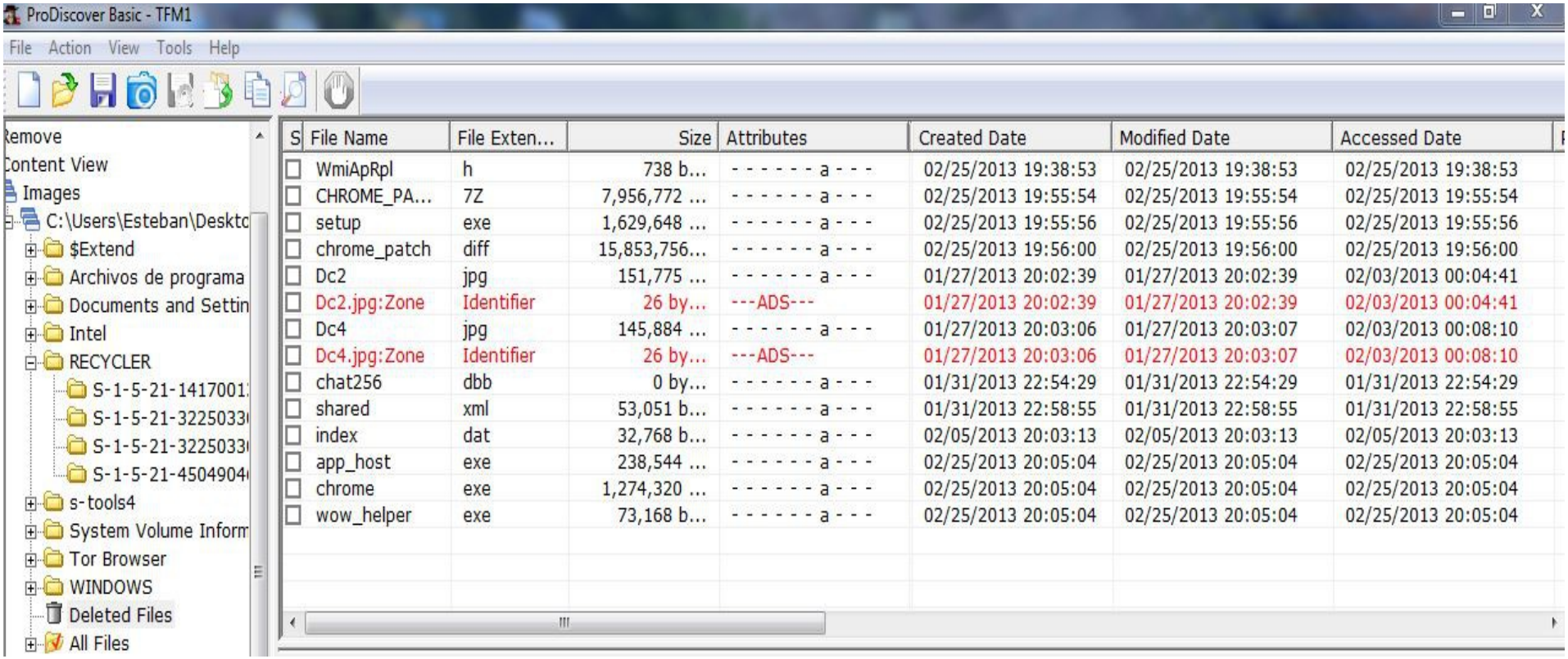


Figura 19. Fitxers que han estat eliminats del disc dur analitzat en dates recents

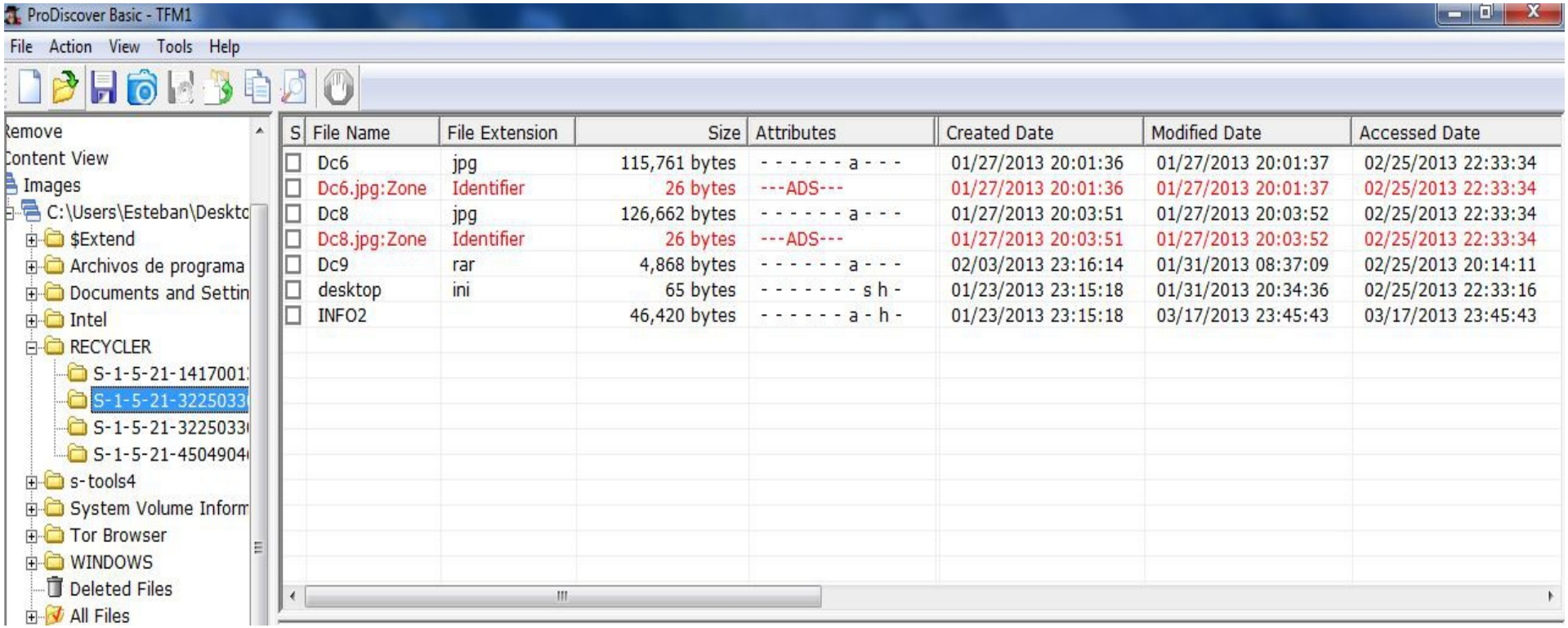


Figura 20. Arxius trobats a la Paperera de reciclatge de l'usuari Juan Solo

De tots els fitxers que han estat eliminats i que es poden recuperar, s'han trobat els següents que són rellevants per la investigació que es duu a terme:

Fitxer	Hash	Tipus
Dc2.jpg	da1ef8691743e1be6e977eb5a1165fe1	Imatge
Dc6.jpg	43cb2792e7cbc7a414a2bce4820a71e9	Imatge
Dc8.jpg	6310cc89bc24729164a655cde095909d	Imatge
Dc9.rar *	2b02818561a1bb85feba176cd34fde96	Fitxer comprimit

Taula 9. Arxius rellevants que s'han pogut recuperar

* El fitxer *Dc9.rar* és una copia de *Contactos.rar* (veure l'Annex C).

Figura 21. Contingut del fitxer Dc2.jpg, l'únic fitxer eliminat que s'ha pogut recuperar

Figura 22. Detall de l'arxiu Dc6.jpg, recuperat de la paperera de reciclatge

Figura 23. Visualització del contingut del fitxer Dc8.jpg

12. Annex F. Informació sobre programari específic

Analitzant la imatge del disc dur proporcionada, s'han trobat diversos programes que poden ser relacionats amb activitats il·lícites comeses pels usuaris de l'equip que ocupa aquesta investigació. De tots els programes instal·lats al disc dur cal destacar els que a continuació s'enumeren a la següent taula,

Programari	Propòsit
Tor Browser v.2.3.25-2	*Navegador web* que permet la navegació de manera totalment anònima per Internet. És imprescindible el seu ús per visitar la *Deep Web*, és a dir aquelles pàgines de contingut poc o gens legal.
S-Tools v 4.0	Programari utilitzat per ocultar, i recuperar, informació dins d'arxius gràfics (esteganografia).
Dropbox v 1.6.16	Programari que permet l'emmagatzematge *online* i ofereix la possibilitat de compartir d'arxius d'una manera molt senzilla.
Skype v 3.6.248	Programari que permet les comunicacions entre usuaris ja sigui via xat, missatges de text, o via *VoIP*.
TrueCrypt v 7.1.a	Aplicació que permet el xifrat dels arxius, fent ús d'una contrasenya, i crea una unitat de disc virtual amb la informació protegida que pot ser muntada.
WinRan v 4.20	Programari per comprimir i descomprimir carpetes i fitxers, permet protegir els arxius xifrats amb contrasenya.

Taula 10. Programari especialitzat detectat a la imatge del disc dur analitzat

13. Annex G. Historial dels navegadors d'Internet

A continuació s'inclouen les cerques més rellevants realitzades pels usuaris **Juan Solo** i **Nadine** mitjançant el buscador *Google*, des dels navegadors webs instal·lats a l'equip analitzat,

Paraules cercades	Navegador	Data de la cerca
download tor	Chrome	17/03/2011 17:16:06
monografía tarjeta magnetica	Chrome	17/03/2011 14:46:01
algoritmo de la clave de luhn	Chrome	17/03/2011 14:54:27
verificar tarjetas de credito on line	Chrome	17/03/2011 14:54:30
msr 206	Chrome	18/03/2011 08:04:36
impresora de tarjetas	Chrome	18/03/2011 08:04:54
uso de tor anonimizacion	Firefox	27/01/2013 17:58:30
uso de silk road	Firefox	27/01/2013 18:04:42
download asus web storage	Firefox	29/01/2013 23:45:58
download net framework version 2	Firefox	29/01/2013 23:51:51
download windows live messenger for windows xp	Firefox	30/01/2013 22:00:10
download dropbox	Firefox	30/01/2013 22:01:57
download winrar	Firefox	30/01/2013 23:09:01
crear cuenta hotmail	Firefox	26/01/2013 18:17:54
comprar joyas	Firefox	26/01/2013 18:23:10
comprar abrigo piel	Firefox	26/01/2013 18:27:10
tarjeta banda magnética	Firefox	26/01/2013 18:32:43
download chrome	Firefox	26/01/2013 18:35:26
hotmail	Firefox	26/01/2013 20:48:09
drop	Firefox	26/01/2013 21:13:21
minus	Firefox	26/01/2013 21:13:44
download firefox	Internet Explorer	23/01/2013 22:13:19

Taula 11. Llistat de les diferents cerques a Internet realitzades des de l'equip analitzat

També s'han analitzat els historials de navegació dels diferents *navegadors web*. A les següents taules s'inclouen les pàgines més visitades i més rellevants per la investigació que es duu a terme per a cadascun dels usuaris actius (**Nadine** i **Juan Solo**),

Historial de Google Chrome

Localitzat a l'arxiu **/Documents and Settings/Nadine/Configuración local/Datos de programa/Google/Chrome/User Data/Default/History**,

Modificació	Últim accés	Creació	Mida (en Bytes)
02/02/2013 23:50:04	02/02/2013 23:50:04	26/01/2013 18:37:54	106496

Taula 12. Metadades de l'historial de navegació web

Amb el *Hash*, calculat fent servir l'algoritme *MD5*: **6cff3720698a4f68e767bc4c23700758**

URL	Títol	Data d'accés
http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica.shtml	Introducción a la tarjeta con banda magnética - Monografias.com	17/03/2011 14:46:01
http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica2.sshtml	Introducción a la tarjeta con banda magnética(página 2) - Monografias.com	17/03/2011 14:46:03
http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica3.shtml	Introducción a la tarjeta con banda magnética(página 3) - Monografias.com	17/03/2011 14:46:01
http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica4.shtml	Introducción a la tarjeta con banda magnética(página 4) - Monografias.com	17/03/2011 14:46:06
http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica5.shtml	Introducción a la tarjeta con banda magnética(página 5) - Monografias.com	17/03/2011 14:46:15
http://www.ngeeks.com/2011/07/07/algoritmo-de-luhn-en-php/	Algoritmo de Luhn en PHP	17/03/2011 14:54:20
http://donkeysharp.blogspot.com/2011/07/algoritmo-luhn-para-validacion-de.html	Donkey Sharp: Algoritmo Luhn para validación de tarjetas de crédito	17/03/2011 14:54:24
http://donkeysharp.blogspot.com.es/2011/07/algoritmo-luhn-para-validacion-de.html	Donkey Sharp: Algoritmo Luhn para validación de tarjetas de crédito	17/03/2011 14:54:24

Taula 13a. Detall de les pàgines visitades per l'usuari Nadine

URL	Títol	Data d'accés
http://generadatosfalsos.com/valitar.php	Generador de Datos Falsos... Validador de Tarjetas de Credito	17/03/2011 14:54:30
http://generadatosfalsos.com/generador.php	Generador de Datos Falsos... Generador de Identidad	17/03/2011 14:54:32
http://generadatosfalsos.com/genebin.php	Generador de Datos Falsos... Generador de Tarjetas de Credito por medio de BIN	17/03/2011 14:55:30
http://www.a3m.eu/es/lectores-de-tarjetas/grabadores-de-pistas-magneticas/grabador-uniform-msr-206.html	Grabador Uniform MSR 206	18/03/2011 08:04:37
http://www.a3m.eu/es/lectores-de-tarjetas/lectores-y-grabadores-de-tarjetas-magneticas/grabador-uniform-msr-206	Grabador Uniform MSR 206	18/03/2011 08:04:38
http://www.a3m.eu/es/IMG/png/msr206_2_550.png	msr206_2_550.png (550x550)	18/03/2011 08:04:38
http://www.a3m.eu/es/tarjetas-plasticas/tarjetas-plasticas-blancas/tarjetas-magneticas.html	Tarjetas magnéticas	18/03/2011 08:04:39
http://www.a3m.eu/es/lectores-de-tarjetas/lectores-y-grabadores-de-tarjetas-magneticas/lector-grabador-loco-lowriter.html	Lector grabador LoCo LoWriter	18/03/2011 08:04:48
http://www.enaf.es/shop/category-Category-19-language-esp-Impresoras%20Tarjetas.htm	Impresoras Tarjetas - ENAF I Distribuidor de tpv I lectores de código de barras I impresoras de tickets I monitor táctil I cajón portamonedas tpv I visor banda magnética I lector de código de barras I balanzas registradoras I software tpv I AQSONIC I CITIZEN I ZEBEX	18/03/2011 08:04:55
http://www.enaf.es/shop/moreinfo-Product_ID-48-category-19-IMPRESORA_DE_TARJETAS_EVOLIS_TATTO2_COLOR.htm	Comprar IMPRESORA DE TARJETAS EVOLIS TATTO2 COLOR - ENAF I Distribuidor de tpv I lectores de código de barras I impresoras de tickets I monitor táctil I cajón portamonedas tpv I visor banda magnética I lector de código de barras I balanzas registradoras I software tpv I AQSONIC I CITIZEN I ZEBEX	18/03/2011 08:04:57

Taula 13b. Continuació del llistat de visites realitzades amb el navegador Chrome

L'historial del navegador *Google Chrome* és guarda a l'arxiu **/Documents and Settings/Juan Solo/Configuración local/Datos de programa/Google/Chrome/User Data/Default/History**,

Modificació	Últim accés	Creació	Mida (en Bytes)
27/01/2013 20:06:29	27/01/2013 20:06:29	26/01/2013 18:38:53	90112

Taula 14. Metadades del fitxer que emmagatzema l'historial de navegació web

Amb el *Hash MD5*: **4885c32b7d1de38ea00755115cfa2506**

URL	Títol	Data d'accés
https://torproject.org/download	Download Tor	17/03/2011 17:16:13
https://www.torproject.org/projects/torbrowser.html.en	Tor Browser Bundle	17/03/2011 17:16:27

Taula 15. Historial rellevant de navegació web de l'usuari Juan Solo

Historial de Microsoft Internet Explorer

L'historial del navegador *Microsoft Internet Explorer* és guarda a l'arxiu **/Documents and Settings/Nadine/Configuración local/Datos de programa/Historial/ History.IE5/index.dat**,

Modificació	Últim accés	Creació	Mida (en Bytes)
03/02/2013 00:03:43	26/01/2013 18:05:15	26/01/2013 18:05:15	32768

Taula 16. Metadades del fitxer que emmagatzema l'historial de navegació web

Amb el *Hash MD5*: **0608983e8900ccc2cdf6421fb0a09b71**

URL	Títol	Data d'accés
file/Documents and Settings/Nadine/Escritorio/Fotos_para_Irina.rar		26/01/2013 20:14:32
file/Documents and Settings/Nadine/Escritorio/Vacaciones.odt		27/01/2013 11:07:26
file/Documents and Settings/Nadine/Mis Documentos/Mis imágenes/Vacaciones 2012/Vacaciones_Budapest.jpg.odt		27/01/2013 16:52:19

Taula 17. Detall de les activitats més rellevants a l'historial del navegador de Microsoft

L'historial del navegador *Microsoft Internet Explorer* és guarda a l'arxiu **/Documents and Settings/Juan Solo/Configuración local/Datos de programa/Historial/ History.IE5/index.dat**,

Modificació	Últim accés	Creació	Mida (en Bytes)
25/02/2013 22:20:24	23/01/2013 22:01:10	23/01/2013 22:01:10	49152

Taula 18. Metadades del fitxer index.dat, que emmagatzema l'historial de navegació web

Amb el *Hash MD5*: **6b34a9eea2b6616281b94009daef316c**

No ha enregistrat cap activitat que sigui rellevant per la investigació.

Historial de Mozilla Firefox

L'historial del navegador *Mozilla Firefox* de l'usuari **Nadine** s'emmagatzema al fitxer **/Documents and Settings/Nadine/Datos de programa/Mozilla/Firefox/Profiles/fs3f2xpr.default/places.sqlite**,

Modificació	Últim accés	Creació	Mida (en Bytes)
26/01/2013 22:11:08	03/02/2013 00:03:58	26/01/2013 18:17:31	10485760

Taula 19. Detalls del fitxer que emmagatzema l'historial de navegació web de Firefox

El seu *Hash*, calculat amb l'algoritme *MD5* és: **cb87c4283db11e969ed2f83c8e76d971**

URL	Títol	Data d'accés
http://windowslive.es.msn.com/hotmail/	Hotmail.com » Iniciar sesion y crear una cuenta	26/01/2013 18:17:58
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1359220700&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.aspx&lc=3082&id=64855&mkt=es-es&cbcxt=mai&snsc=1	Iniciar sesión	26/01/2013 18:18:24
https://signup.live.com/signup.aspx?wa=wsignin1.0&rpsnv=11&ct=1359220700&rver=6.1.6206.0&wp=MBI&wreply=http%3a%2f%2fmail.live.com%2fdefault.aspx&id=64855&cbcxt=mai&snsc=1&bk=1359220702&uiflavor=web&mkt=ES-ES&lc=3082&lic=1	Registrarse cuenta Microsoft	26/01/2013 18:18:38
http://sn140w.snt140.mail.live.com/default.aspx	Página principal - Windows Live	26/01/2013 18:22:16
http://sn140w.snt140.mail.live.com/default.aspx#!/mail/InboxLight.aspx?n=1686341912	Hotmail - nadine_solo@hotmail.es	26/01/2013 18:22:23
http://www.joyeriavirtual.net/joyas/comprar-joyas.htm	Comprar Joyas - JoyeriaVirtual.net	26/01/2013 18:23:18
http://www.joyeriavirtual.net/ecommerce/web/default.php?cPath=25	Colgantes - Joyeria Virtual - Tienda joyas - regalo y ofertas compromiso, diamantes, pulseras, anillos, comprar gemas	26/01/2013 18:23:31

Taula20a. Detalls de l'historial de navegació de Firefox de l'usuari Nadine

URL	Títol	Data d'accés
http://www.joyeriavirtual.net/ecommerce/web/product_info.php?cPath=18&products_id=909	Collar oro. nº2268 - Collares - JoyeriaVirtual.Net	26/01/2013 18:24:06
http://www.joyeriavirtual.net/ecommerce/web/default.php?cPath=20	Pendientes - Joyeria Virtual - Tienda joyas - regalo y ofertas compromiso, diamantes, pulseras, anillos, comprar gemas	26/01/2013 18:24:22
http://www.joyeriavirtual.net/ecommerce/web/product_info.php?cPath=26&products_id=146	Pulsera oro. nº362 - Pulseras - JoyeriaVirtual.Net	26/01/2013 18:24:50
http://www.laredoute.es/search.aspx?keyword=abrigos&mkwid=s0626I2rd&pcrid=23862537910&kword=comprar%20abrigos&match=p&plid=&omniturecode=06006512857600008200013945ES	La Redoute, tu portal de moda | La Redoute	26/01/2013 18:27:21
http://www.milanoo.com/es/c1075	Comprar piel de la mujer y chaquetas de cuero, abrigos y chalecos de descuento - Milanoo.com	26/01/2013 18:27:49
http://www.milanoo.com/es/p209498.html	Chaqueta de piel de la mujer del Collar de piel de zorro de V-cuello de pelo de gracia gris Cony - Milanoo.com	26/01/2013 18:27:59
http://www.milanoo.com/es/p227012.html	Acogedor abrigo de visón negro largo mangas de la mujer - Milanoo.com	26/01/2013 18:29:59
http://www.milanoo.com/es/p227010.html	Gris abrigo de mangas largas mujer de visón - Milanoo.com	26/01/2013 18:31:00
http://www.milanoo.com/es/p227018.htm	Abrigo de piel de visón marrón largo mangas de la mujer - Milanoo.com	26/012013 18:31:18
https://www.google.com/intl/es/chrome/browser/?hl=es	Navegador Chrome	26/01/2013 18:35:32
https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7B9582700A-023A-CCD7-2076-88352B322ACC%7D%26lang%3Des%26browser%3D3%26usagestats%3D0%26appname%3DGoogle%2520Chrome%26needsadmin%3Dprefers/update2/installers/ChromeSetup.exe	ChromeSetup.exe	26/01/2013 18:35:48
http://www.winrar.es/descargas	WinRAR España - Descargas	26/01/2013 21:00:24
http://downloads.winrar.es/index.php?action=downloads&file=52	wrar420es.exe	26/01/2013 21:00:41

Taula20b. Detalls de l'historial de navegació de Firefox de l'usuari Nadine (continuació)

URL	Títol	Data d'accés
https://www.wetransfer.com/	WeTransfer	26/01/2013 21:05:25
https://droplr.com/hello	Droplr · Hello	26/01/2013 21:12:30
http://minus.com/	Minus - Share simply.	26/01/2013 21:13:48

Taula20c. Detalls de l'historial de navegació de Firefox de l'usuari Nadine (continuació)

L'historial del navegador web *Mozilla Firefox* de l'usuari **Juan Solo** s'emmagatzema a l'arxiu **/Documents and Settings/Juan Solo/Datos de programa/Mozilla/Firefox/Profiles/fs3f2xpr.default/places.sqlite**,

Modificació	Últim accés	Creació	Mida (en Bytes)
24/02/2013 13:24:50	24/02/2013 13:24:50	23/01/2013 23:15:28	10485760

Taula 21. Detalls del fitxer que emmagatzema l'historial de navegació web de Firefox

El seu *Hash*, calculat amb l'algoritme *MD5* és: **a52ef6e847ac04e703808c9c1ccf7152**

URL	Títol	Data d'accés
http://www.mozilla.org/es-ES/firefox/18.0.1/firstrun/	Bienvenido a Firefox	23/01/2013 23:15:38
http://gparted.sourceforge.net/download.php	GParted -- Download	26/01/2013 17:58:36
http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf		27/01/2013 17:59:16
https://www.mozilla.org/es-ES/plugincheck/	Navegador Firefox - Comprobación y actualizaciones de plugins	27/01/2013 17:59:25
http://www.sinfocol.org/2009/10/como-anonimizar-la-conexion-de-internet-seleccionando-un-pais-de-salida/	Cómo anonimizar la conexión de internet seleccionando un país de salida | Seguridad Informática Colombiana	27/01/2013 17:59:40
http://blogs.eset-la.com/laboratorio/2012/05/08/troyano-utiliza-tor-anonimizar-actividad-maliciosa/	ESET Latinoamérica - Laboratorio » Blog Archive » Troyano utiliza Tor para anonimizar su actividad maliciosa	27/01/2013 18:00:24
http://onsoftware.softonic.com/navegacion-anonima-la-red-sin-rostro	Navegación anónima: Tor, I2P y los proxy gratuitos | Onsoftware	27/01/2013 18:00:43

Taula 22a. Visites més rellevants a l'historial del Firefox de l'usuari Juan Solo

URL	Títol	Data d'accés
https://redescebolla.wordpress.com/tag/tor/	Tor « Redes Cebolla	27/01/2013 18:02:44
http://ha-games.com/foro/index.php?topic=21.0	Guia y Uso de Mbot crack en Silkroad Hispano	27/01/2013 18:04:55
http://es.wikipedia.org/wiki/Archivo:Trade_in_silkroad.jpg	Archivo:Trade in silkroad.jpg - Wikipedia, la enciclopedia libre	27/01/2013 18:09:13
http://silkroad.softonic.com/	SilkRoad - Descargar	27/01/2013 18:09:33
http://energycontrol.org/foro/Foro-sobre-drogas-y-gesti%C3%B3n-de-placeres-y-riesgos/22350-Silk-Road-el-tr%C3%A1fico-de-drogas-en-la-internet.html	Silk Road: el tráfico de drogas en la internet	27/01/2013 18:09:48
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1359311032&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.aspx&lc=3082&id=64855&mkt=es-es&cbcxt=mai&snsc=1	Iniciar sesión	27/01/2013 19:23:56
http://sn144w.snt144.mail.live.com/default.aspx	Página principal - Windows Live	27/01/2013 19:24:40
http://sn144w.snt144.mail.live.com/default.aspx#!/mail/InboxLight.aspx?n=568680985	Hotmail - juan_solo23@hotmail.es	27/01/2013 19:24:45
https://www.asuswebstorage.com/navigate/downloads/	Online backup, file sync, for pad, PC, Android and iPhone - ASUS WebStorage	29/01/2013 23:46:03
http://content.asuswebstorage.com/asuswebstorage/dlp/asp/wsync/WebStorageSyncAgent1.1.13.exe	WebStorageSyncAgent1.1.13.exe	29/01/2013 23:46:24
http://www.microsoft.com/es-es/download/details.aspx?id=6523	Download: .NET Framework, versión 2.0, Redistributable Package (x64) - Microsoft Download Center - Download Details	29/01/2013 23:51:55
http://www.microsoft.com/es-es/download/details.aspx?id=1639	Download: .NET Framework 2.0 Service Pack 2 - Microsoft Download Center - Download Details	29/01/2013 23:52:37
http://windows.microsoft.com/en-US/messenger/home	Messenger - Microsoft Windows	30/01/2013 22:00:15
http://windows.microsoft.com/en-US/windows/download-shop	Windows Download and Shop - Microsoft Windows	30/01/2013 22:00:44
https://www.dropbox.com/install	Dropbox - Descargar Dropbox - Simplifica tu vida	30/01/2013 22:02:27

Taula 22b. Visites més rellevants a l'historial del Firefox de l'usuari Juan Solo (continuació)

URL	Títol	Data d'accés
https://d1ilhw0800yew8.cloudfront.net/client/Z/Dropbox%201.6.16.exe	Dropbox 1.6.16.exe	30/01/2013 22:02:38
http://www.winrar.es/descargas	WinRAR España - Descargas	30/01/2013 23:09:04
http://downloads.winrar.es/index.php?action=downloads&file=52	wrar420es.exe	30/01/2013 23:09:09
https://mtgox.com/	Mt.Gox - Bitcoin Exchange	30/01/2013 23:11:54

Taula 22c. Visites més rellevants a l'historial del Firefox de l'usuari Juan Solo (continuació)

14. Annex H. Anàlisi de la memòria RAM

Es fa servir l'eina *Volatility* per extreure informació de la imatge de la memòria *RAM* de l'equip analitzat. Aquesta utilitat proporciona dades molt valuoses de cara a la investigació que es duu a terme.

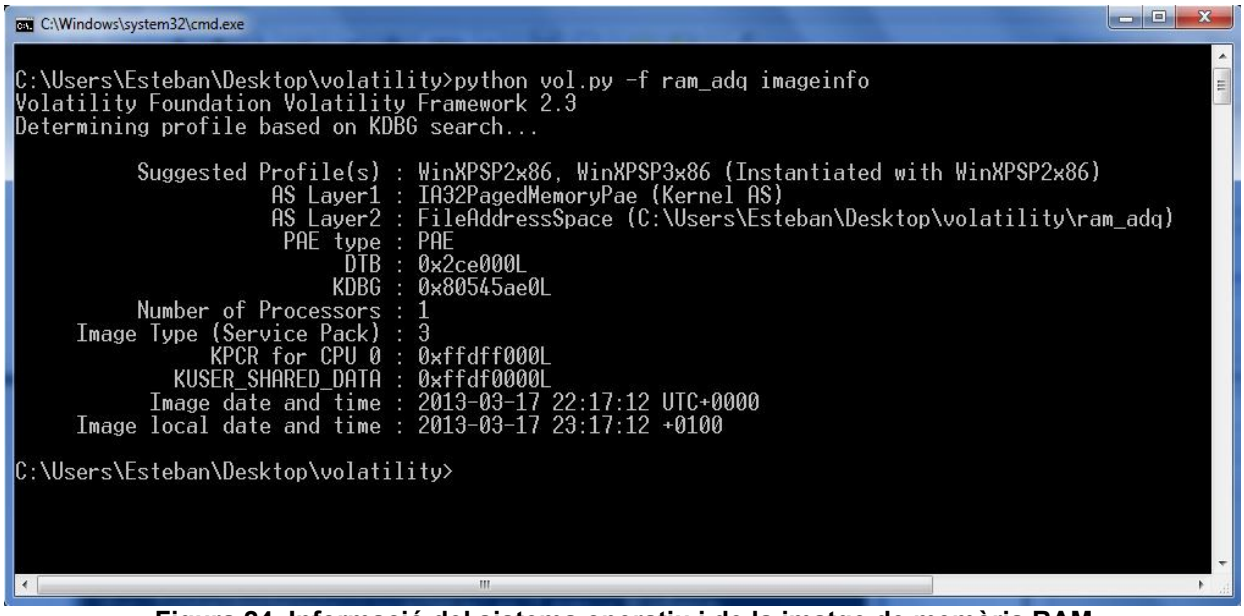


Figura 24. Informació del sistema operatiu i de la imatge de memòria RAM

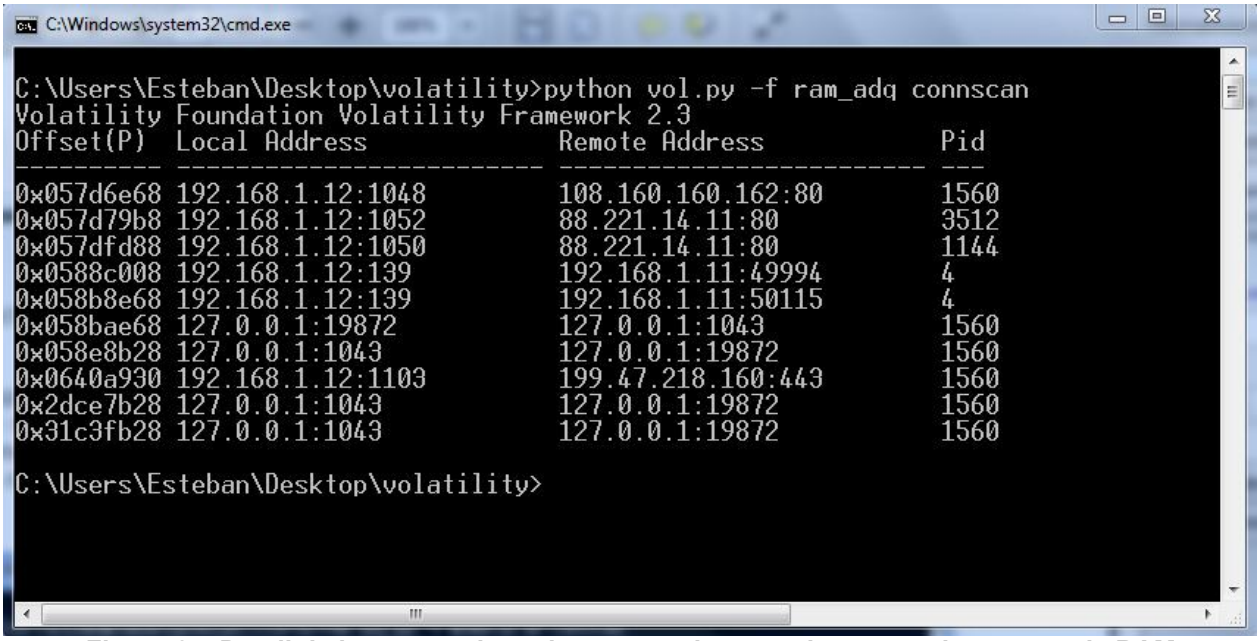


Figura 25. Detall de les connexions de xarxa actives en el moment de capturar la RAM

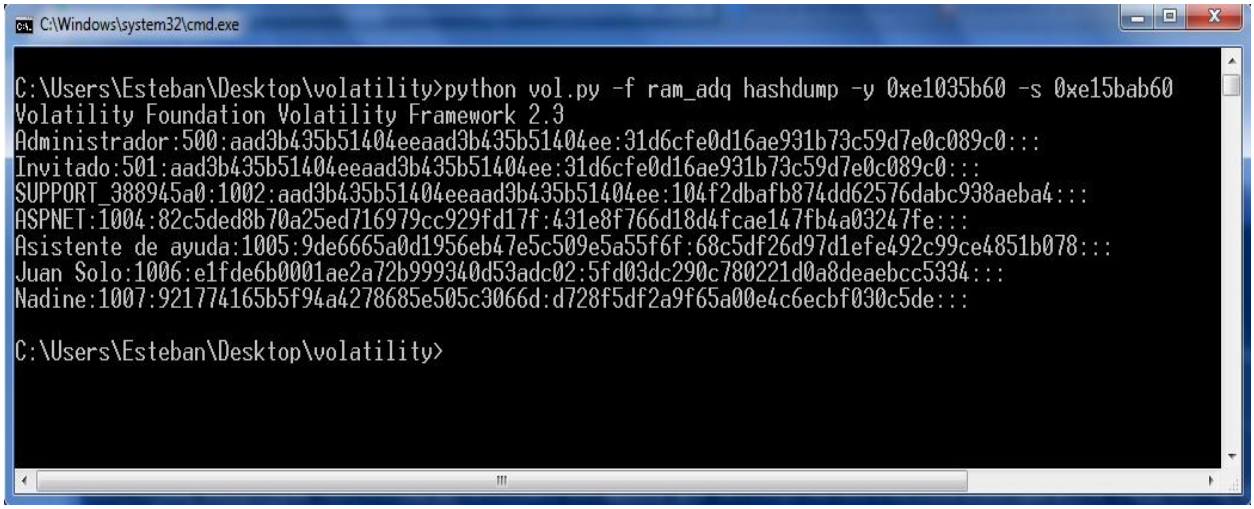


Figura 26. Llistat de tots els usuaris del sistema analitzat

A la següent taula es poden observar les credencials dels usuaris del sistema. S'ha fet servir el programari *John the ripper* per esbrinar les contrasenyes d'accés,

Usuari	Hash	Contrasenya
Administrador	aad3b435b51404eeaad3b435b51404ee	--- sense contrasenya ---
Invitado	aad3b435b51404eeaad3b435b51404ee	--- sense contrasenya ---
SUPPORT_388945a0	aad3b435b51404eeaad3b435b51404ee	--- sense contrasenya ---
ASPNET	82c5ded8b70a25ed716979cc929fd17f	.....=;KB3OJ
Asistente de ayuda	9de6665a0d1956eb47e5c509e5a55f6f	BZ=8MTSTPX25HC
Juan Solo	e1fde6b0001ae2a72b999340d53adc02	JUANS1978
Nadine	921774165b5f94a4278685e505c3066d	NADINE1980

Taula 23. Credencials dels usuaris de l'equip, destacant els usuaris actius

També s'han cercat les adreces de correu electrònic més utilitzades i rellevants per la investigació. Els resultats obtinguts es poden observar a la següent taula,

Adreces de correu electrònic
3@hotmail.es
-loginJuan_Solo23@hotmail.es
-loginNadine_Solo@hotmail.es
anselmo_rodriguez@hotmail.es
eandres_carlos4h@yopmail.com
enndeakin@sympatico.ca
frarho@gmail.com
happy_lab@hotmail.es
irina_luhn@hotmail.es
jsaucedal@gmail.com
juan_solo23@hotmail.es
miki.tebeka@gmail.com
nadine_solo@hotmail.es
ppy_lab@hotmail.es
saruman@unigsm.com
tacanin91@yahoo.com
vital76@gmail.com
y_lab@hotmail.es

Taula 24. Llistat de les adreces de correu electrònic trobades

15. Annex I. Altres

Aquest apartat es centra en altres informacions que, si bé no són l'objectiu principal d'aquest informe pericial, són igualment importants en la investigació que es duu a terme.

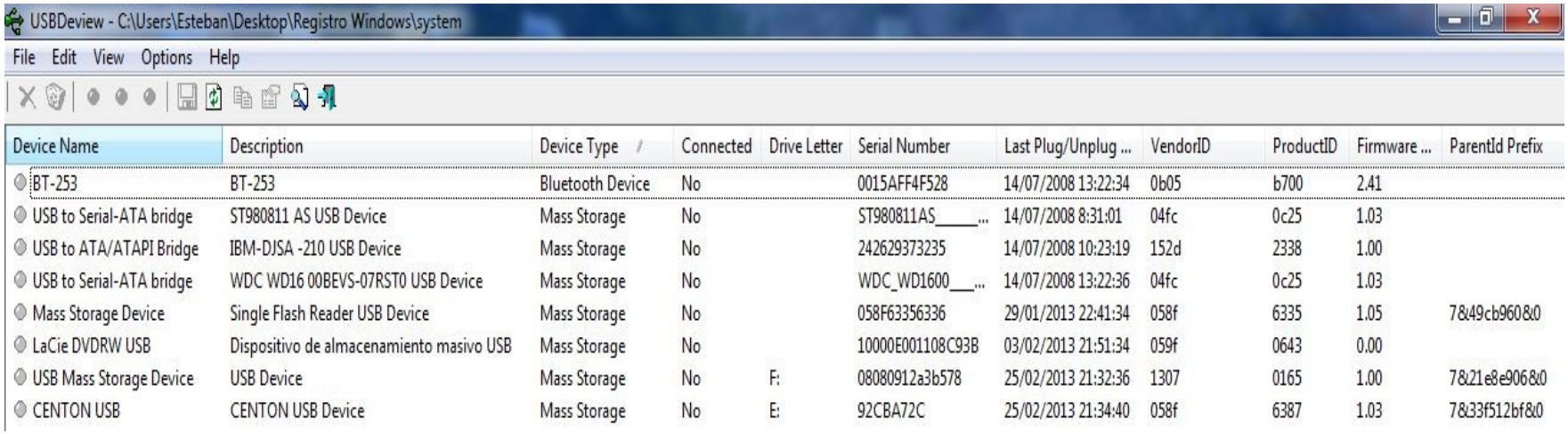
Dispositius connectats

A continuació es mostra la informació obtinguda dels dispositius d'emmagatzematge *USB* que han estat connectats a l'equip que s'està analitzant.

El fet de trobar una instal·lació del programari *TrueCrypt* al sistema analitzat, motiva que es faci aquesta anàlisi.

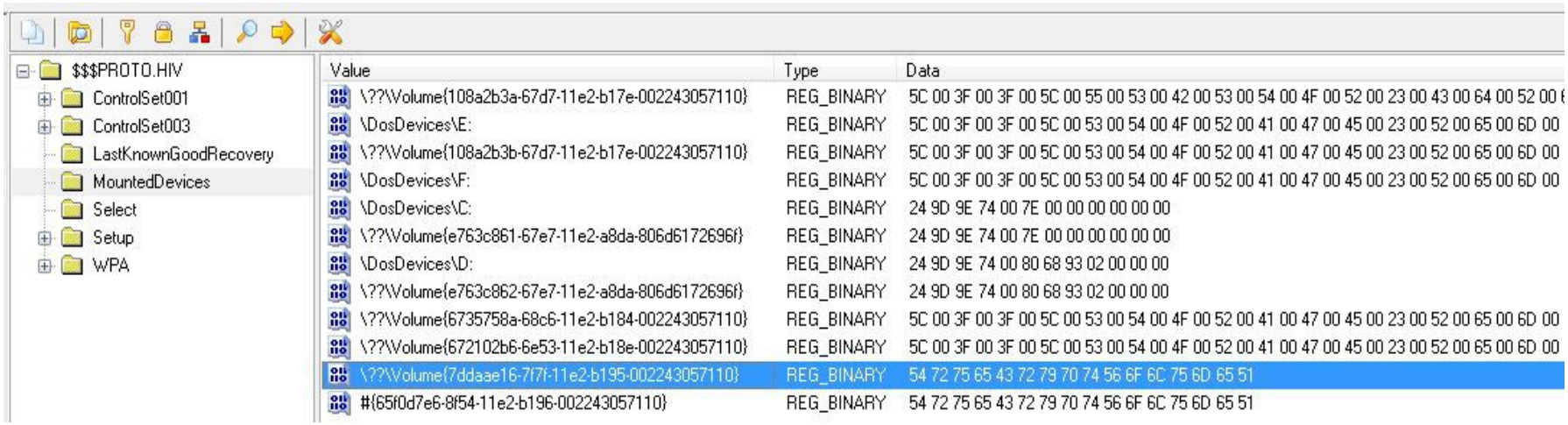
Es fa servir l'eina *USBDeview* per obtenir el llistat de tots els dispositius que s'han connectat als ports *USB.* Seguidament, s'inspecciona el Registre de *Windows* amb el programari *Windows Registry Recovery*.

El resultat d'aquestes operacions es poden veure a les captures de pantalla següents,



Device Name	Description	Device Type	Connected	Drive Letter	Serial Number	Last Plug/Unplug ...	VendorID	ProductID	Firmware ...	ParentId Prefix
BT-253	BT-253	Bluetooth Device	No		0015AFF4F528	14/07/2008 13:22:34	0b05	b700	2.41	
USB to Serial-ATA bridge	ST980811 AS USB Device	Mass Storage	No		ST980811AS_____...	14/07/2008 8:31:01	04fc	0c25	1.03	
USB to ATA/ATAPI Bridge	IBM-DJSA -210 USB Device	Mass Storage	No		242629373235	14/07/2008 10:23:19	152d	2338	1.00	
USB to Serial-ATA bridge	WDC WD16 00BEVS-07RST0 USB Device	Mass Storage	No		WDC_WD1600___...	14/07/2008 13:22:36	04fc	0c25	1.03	
Mass Storage Device	Single Flash Reader USB Device	Mass Storage	No		058F63356336	29/01/2013 22:41:34	058f	6335	1.05	7&49cb960&0
LaCie DVDRW USB	Dispositivo de almacenamiento masivo USB	Mass Storage	No		10000E001108C93B	03/02/2013 21:51:34	059f	0643	0.00	
USB Mass Storage Device	USB Device	Mass Storage	No	F:	08080912a3b578	25/02/2013 21:32:36	1307	0165	1.00	7&21e8e906&0
CENTON USB	CENTON USB Device	Mass Storage	No	E:	92CBA72C	25/02/2013 21:34:40	058f	6387	1.03	7&33f512bf&0

Figura 27. Llistat dels dispositius d'emmagatzematge que s'han connectat als ports USB de l'equip analitzat



Value	Type	Data
\??\Volume{108a2b3a-67d7-11e2-b17e-002243057110}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23 00 43 00 64 00 52 00
\DosDevices\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6D 00
\??\Volume{108a2b3b-67d7-11e2-b17e-002243057110}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6D 00
\DosDevices\F:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6D 00
\DosDevices\C:	REG_BINARY	24 9D 9E 74 00 7E 00 00 00 00 00 00
\??\Volume{e763c861-67e7-11e2-a8da-806d6172696f}	REG_BINARY	24 9D 9E 74 00 7E 00 00 00 00 00 00
\DosDevices\D:	REG_BINARY	24 9D 9E 74 00 80 68 93 02 00 00 00
\??\Volume{e763c862-67e7-11e2-a8da-806d6172696f}	REG_BINARY	24 9D 9E 74 00 80 68 93 02 00 00 00
\??\Volume{6735758a-68c6-11e2-b184-002243057110}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6D 00
\??\Volume{672102b6-6e53-11e2-b18e-002243057110}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00 4F 00 52 00 41 00 47 00 45 00 23 00 52 00 65 00 6D 00
\??\Volume{7ddaae16-7f7f-11e2-b195-002243057110}	REG_BINARY	54 72 75 65 43 72 79 70 74 56 6F 6C 75 6D 65 51
#{65f0d7e6-8f54-11e2-b196-002243057110}	REG_BINARY	54 72 75 65 43 72 79 70 74 56 6F 6C 75 6D 65 51

Figura 28. Detall de les claus del Registre de Windows que mostren els dispositius USB que s'han muntat al sistema

Com es pot observar a la figura 29, es veu que s'ha connectat un dispositiu *USB*, amb total probabilitat un *pendrive*, que s'ha utilitzat amb el programari *TrueCrypt* i el sistema l'ha assignat la lletra d'unitat **Q:**.

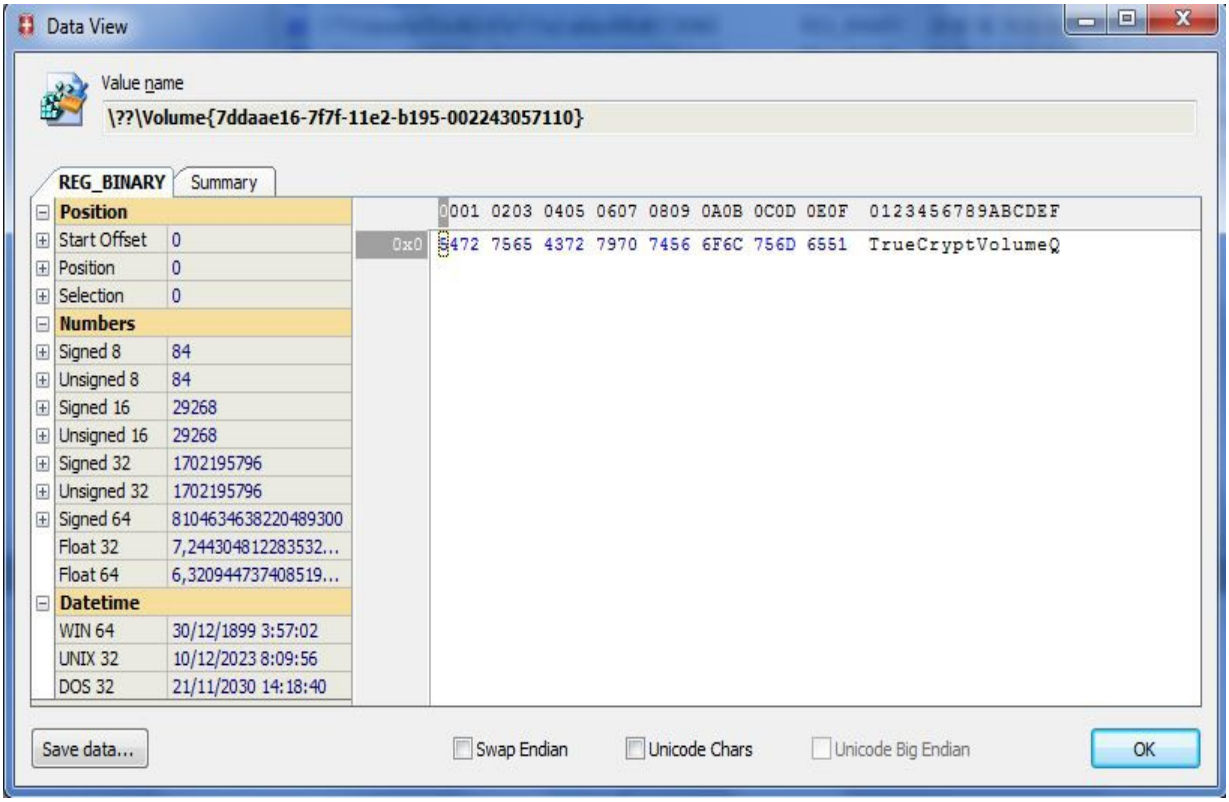


Figura 29. Informació del dispositiu: es tracta de la unitat Q, xifrada amb TrueCrypt

Cerca de paraules clau

Es realitza una cerca de les paraules més importants en aquest tipus d'investigació a la imatge del disc dur analitzat. S'utilitza tant el programari *Autopsy Framework*. Els resultats obtinguts són els següents:

Paraula cercada	Resultats
tarjetas	- Es localitza als historials del navegadors web de l'usuari **Nadine** (veure l'annex G).
Irina	- Es localitza a les bases de dades de converses del programari *Skype* (veure l'annex C). - Localitzada a l'historial de navegació web de l'usuari **Nadine** (veure l'annex G). - Es troba una referència al fitxer **Fotos_para_Irina.rar** però el fitxer no es troba al disc dur. Aquest fitxer torna a ser referenciat a l'historial de navegació de l'usuari **Nadine**.
sex	- Es localitza als fitxers de "caché" del *navegador web Firefox* de l'usuari **Juan Solo** (veure l'annex G).
compra	- Es localitza a diversos fitxers *PDF*, trobats a la carpeta de *Ebooks* de l'usuari **Juan Solo**. - Localitzada als fitxers de "caché" i a l'historial de navegació web de l'usuari **Nadine** (veure l'annex G).
drogas	- Localitzada a diversos fitxers *PDF*, trobats a la carpeta de *Ebooks* de l'usuari **Juan Solo**. - Localitzada als arxius de "caché" i a l'historial del navegador *Firefox* de l'usuari **Juan Solo (**veure l'annex G).
drugs	- Aquesta paraula es troba als arxius de "caché" del *navegador web Firefox* i a l'historial de navegació de l'usuari **Juan Solo** (veure l'annex G). - Es localitza a un dels fitxers relacionats amb la investigació (veure l'annex C).

Taula 25. Detall de la cerca de les paraules clau de la investigació

Informació sobre el Sistema Operatiu instal·lat i els usuaris del sistema

S'analitza la imatge del disc dur de l'ordinador investigat, principalment les claus del *Registre de Windows*, i s'ha arriba a les següents conclusions:

- L'ordinador analitzat és un *Netbook* de la marca *Asus* pertanyent a la sèrie *Eee PC*.

- L'ordinador fa servir la **versió 5.1.2600** del sistema operatiu *Microsoft Windows*. Aquesta versió es coneix amb el nom comercial de *Microsoft Windows XP Professional* amb el *Service Pack 3*, que és una actualització, de components i de seguretat, realitzada per la mateixa *Microsoft*.

- La instal·lació del sistema operatiu es va fer el dia **23 de Gener de l'any 2013** a les **20:58:58**, per l'usuari **Juan Solo**, que figura com a propietari del sistema (el seu compte d'usuari té privilegis d'*administrador*).

- El sistema operatiu és original o, al menys, té un nombre de sèrie vàlid.

- S'han definit set usuaris al sistema operatiu analitzat. No obstant això, només dos dels usuaris tenen un compte d'usuari personalitzat i han iniciat sessió al sistema. Aquest dos usuaris són: **Juan Solo** i **Nadine**. La resta d'usuaris són serveis del sistema operatiu i comptes que són creades per defecte durant el procés d'instal·lació de *Microsoft Windows*. Aquests cinc usuaris són: **Administrador**, I**nvitado**, **SUPPORT_388945a0**, **ASPNET** i **Asistente de ayuda**.

- L'usuari **Juan Solo** té una contrasenya definida al seu compte que va ser definida el **27 de Gener de 2013** a les **16:57:14**. Aquest compte d'usuari no caduca mai, té assignada una data incorrecta, el **30 de Desembre de 1899** a les **2:48:05**.

- L'usuari **Nadine** té assignada una contrasenya que va ser definida el **26 de Gener de 2013** a les **17:14:29**. Aquest compte d'usuari no caduca mai, té assignada una data incorrecta, el **30 de Desembre de 1899** a les **2:48:05**.

- L'usuari **Juan Solo** va iniciar sessió per última vegada el dia **17 de Març de 2013** a les **22:27:47**.

- L'usuari **Nadine** va iniciar sessió per última vegada el dia **2 de Febrer de 2013** a les **22:44:42**.

A continuació es mostra la informació, extreta amb el programari *MiTeC Windows Registry Recovery*, referent al sistema operatiu instal·lat i als usuaris actius de l'equip analitzat,

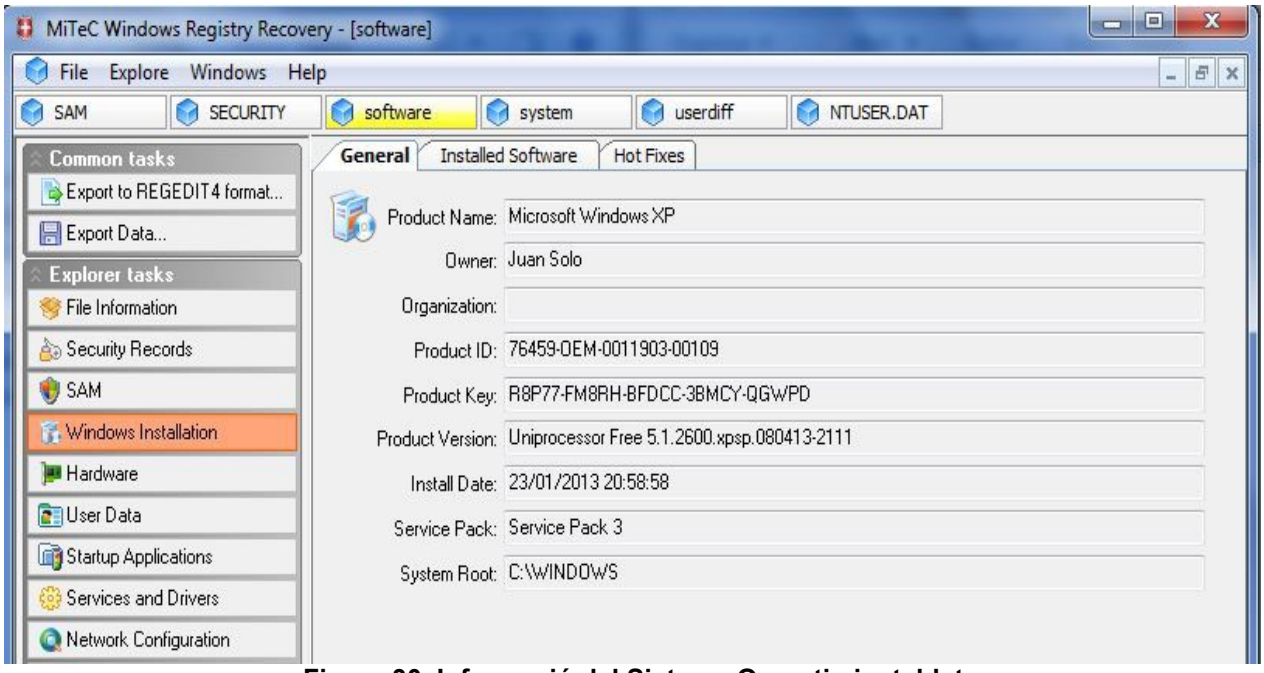


Figura 30. Informació del Sistema Operatiu instal·lat

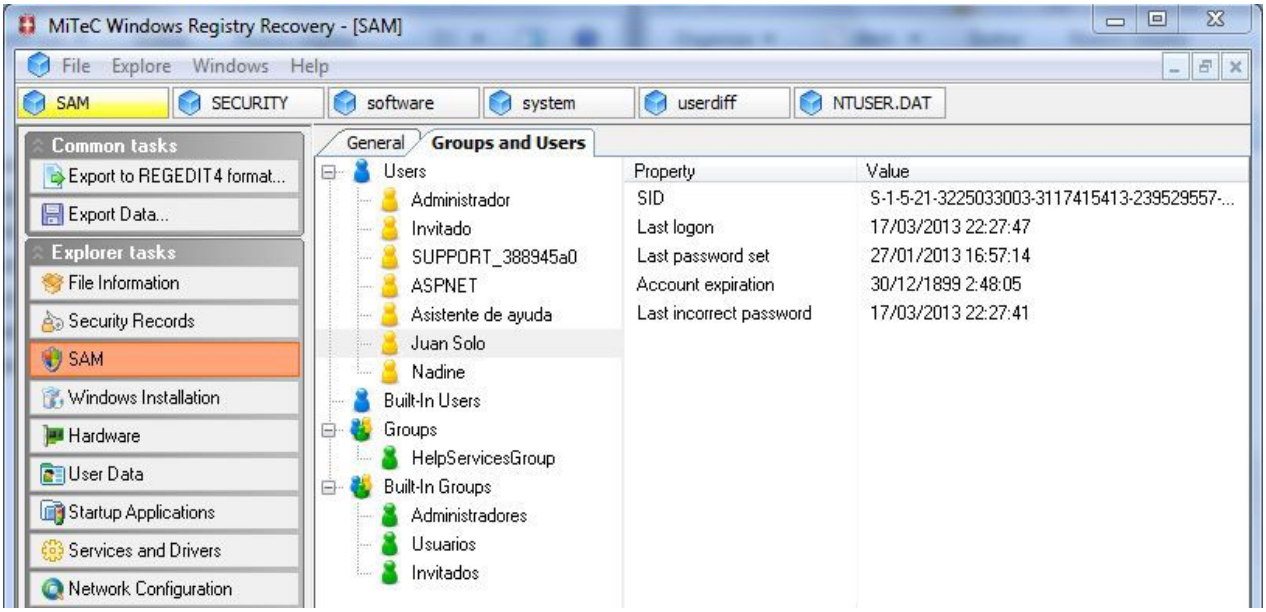


Figura 31. Detalls corresponents al compte d'usuari Juan Solo

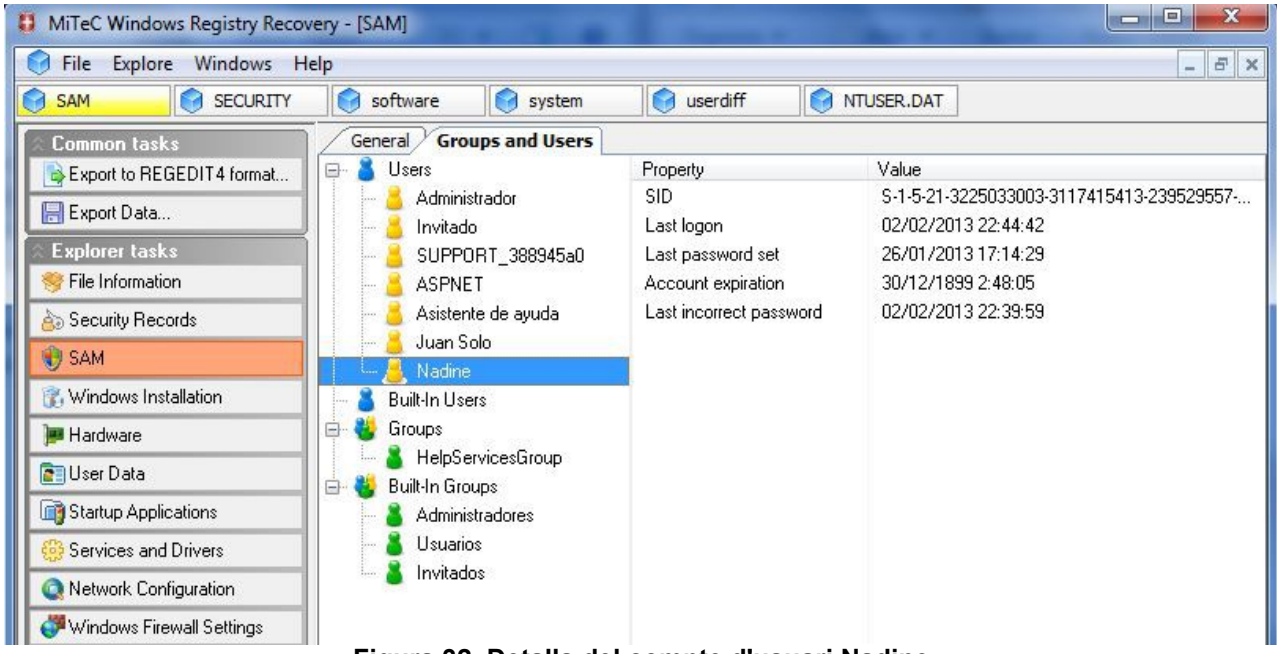


Figura 32. Detalls del compte d'usuari Nadine

Altres investigacions

Addicionalment, s'analitzen les converses contingudes al fitxer **whatsapp.db** que no guarden relació directa amb la investigació amb l'eina *Whatsapp Xtract*.

Chat session # 21531: 34999999621

PK	Chat	Msg date	From	Msg content	Msg status	Media Type	Media Size
21505	34999999621	2012-02-16 23:31:08	me	Hola Josep!	4	0	0
21506	34999999621	2012-02-16 23:31:11	me	no hem vaig recordar avisar-te... però hi ha una pràctica de la uoc per fer i és molt difícil!	4	0	0
21507	34999999621	2012-02-16 23:31:20	me	i s'ha de lliurar aquest cap de setmana X_D	5	0	0
21517	34999999621	2012-02-17 09:10:09	34999999621	hola carlos	0	0	0
21518	34999999621	2012-02-17 09:10:14	34999999621	ah! ja ho vaig fer tot i ja l'he entregada	0	0	0
21519	34999999621	2012-02-17 10:06:50	me	i ara m'ho dius!! ja et preguntaré el que no hem surti...	5	0	0
21520	34999999621	2012-02-17 10:06:55	me	¬¬	5	0	0

Figura 33. Detall d'una conversa entre dos estudiants sense relació amb la investigació

Chat session # 21527: 34999999118

PK	Chat	Msg date	From	Msg content	Msg status	Media Type	Media Size
21508	34999999118	2012-02-16 23:31:42	me	Laia :*	5	0	0
21509	34999999118	2012-02-16 23:31:45	me	Mña a k hora hay k ir al cole????	5	0	0
21510	34999999118	2012-02-16 23:32:03	34999999118	A las 8:15	0	0	0
21511	34999999118	2012-02-16 23:32:14	me	Clase normal?	5	0	0
21512	34999999118	2012-02-16 23:29:24	34999999118	Las 3 primeras horas si	0	0	0
21513	34999999118	2012-02-16 23:33:45	me	Justo las k tngo	5	0	0
21514	34999999118	2012-02-16 23:33:47	me	:/	5	0	0
21515	34999999118	2012-02-16 23:33:51	me	XD	5	0	0
21516	34999999118	2012-02-16 23:34:00	me	Bueno ps nos vemos.mña :)	5	0	0

Figura 34. Missatges intercanviats entre dos estudiants que assisteixen a classes presencials

16. Glossari

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.

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* (*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.

Netbook. Anglicisme, ultraportàtil. Aquest terme va ser introduït per *Intel* al febrer del 2008 per descriure a una categoria d'ordinadors de baix cost, i de rang inferior al *subnotebook,* creats per a ser usats especialment per navegar per *Internet*, però també per a realitzar tasques bàsiques com és l'edició de textos o l'execució de petits programes poc potents.

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.

Pendrive. Anglicisme, 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.

Registre de Windows. És una base de dades jeràrquica que emmagatzema els ajustos de configuració i opcions en els sistemes operatius *Microsoft Windows*. Conté la configuració dels components de baix nivell del sistema operatiu, així com de les aplicacions que hi ha funcionant en la plataforma: fan ús del registre el nucli (*kernel*, en anglès), els controladors de dispositius, els serveis, el *SAM*, la interfície d'usuari i les aplicacions de tercers. El registre també proporciona un mitjà d'accés als comptadors per generar un perfil del rendiment del sistema.

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.

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.