El primer pas ha estat muntar el fitxer "image.zip". Aquest fitxer conté un sistema de fitxers, per la qual cosa s'ha de muntar com a dispositiu en loop. D'aquesta manera es podrà veure com si es tractés d'un dispositiu connectat (USB, DVD, disquet ...):

```
$ sudo bash
$ unzip image.zip
$ mkdir /mnt/disk
$ mount -o loop image /mnt/disk
```

A continuació, he anat al directori /mnt/disk i he fet `ls -al` per veure què hi havia, i també veure les mides del fitxer. L'output és el següent:

```
:$ ls -al /mnt/disk
total 28
drwxr-xr-x 2 root root  7168 Dec 31  1969  .
drwxr-xr-x 3 root root  4096 Dec  5 06:08  ..
-rwxr-xr-x 1 root root 15585 Sep 11  2002 'cover page.jpgc           '
-rwxr-xr-x 1 root root  1000 May 24  2002  SCHEDU~1.EXE
```

Puc veure que hi ha una imatge (amb una extensió de fitxer equivocada) "cover page.jpgc" i un fitxer .exe, que el seu nom sembla "Schedule" i és un executable de Windows.

Ara obro l'**autopsy** i creo un cas nou amb la imatge (com diu el LabBooklet). Un cop fet vaig a "Anàlisi d'arxius" on hi ha un fitxer "*Jimmy Junge.docx*" que es va eliminar. També el fitxer "*cover image.jpgc*" es va editar a les 8.30, però va ser creat a les 8.50. Finalment un fitxer "Scheduled Visits.exe". Ara si fem un clic sobre aquest fitxer "cover image.jpgc" i després anem a l'informe ASCII, notem que el fitxer està marcat com a "PC formatted floppy with no filesystem".

Ara vaig al **ASCII report** del fitxer .docx suprimit. El fitxer es mostra com "Composite Document File V2 Document, Little Endian" i el seu nom de fitxer és "\ **_IMMYJ ~ 1.DOC2**". Això es deu a que quan un fitxer s'esborra en un sistema de fitxers FAT, el sistema posarà un caràcter (hex. E5) com a primera lletra del fitxer a l'entrada del directori d'arrel del fitxer per marcar-lo com que ja no s'utilitza i posarà els sectors que utilitza el fitxer de la taula FAT a 0. (Això ho he trobat a wiki forense) Això vol dir que en un sistema FAT els fitxers no s'eliminen definitivament, de manera que és possible recuperar aquest fitxer. Finalment a la secció "metadades" veiem clarament que comença a la secció 33 del disc. També podem veure que conté algun text interessant que pot ser útil:

```
Contents Of File: C:/Jimmy Jungle.doc

......Jimmy Jungle
  626 Jungle Ave Apt 2
  Jungle, NY 11111

``

  Jimmy:

``

  Dude, your pot must be the best  it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

``
```

```
   These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

``

  I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive.  Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

``

  Thanks,

``

  Joe

  .....????? ??;         ,     ??/ ??\ ??] ??? ??? ??? ??k?.....
```

Per últim, faig una ullada a l'informe ASCII de "Visites programades.exe" i ens podria sorprendre veure que no està marcat com a fitxer .exe. De fet, diu que és un "ERROR:[gzip: Exec `gzip' failed, No such file or directory] (Zip archive data, at least v2.0 to extract) ", de manera que podria ser que en Jacob hagi canviat el fitxer d'extensió per ocultar-ne el contingut.

Al sistema FAT, cada sector és de 512B, de manera que si dividim la mida del fitxer .docx per la mida del sector, obtindrem la quantitat de sectors d'aquest fitxer. 20480/512 = 40. Ara, potser podré extreure el fitxer complet de la imatge mitjançant la comanda `dd` (això ho he trobat buscant "Manually recover files from FAT system forensics" des d'aquest enllaç)

```
dd if=image bs=512 count=40 skip=33 of=jimmy.doc
```

El que fa aquesta comanda es:

> Del input file **image** que té els segments de bloc de **512B** agafa **40 segments** començant per el segment **33** i posa-ho en un output file anomenat **jimmy.doc**.

Ara intentarem fer el mateix amb l'arxiu "cover page.jpgc". En el ASCII report de l'**autopsy** hem vist que té una mida total de 15585 bytes i que comença en el sector 451. He fet la divisió per a obtenir els sectors que ocupa i m'he trobat que no dona un numero enter com a resultat, ens dona 30.4. Pel que puc pensar està ocupant 30 sectors i un 40% del sector que faria 31. Com que la comanda `dd` em deixa escollir la mida dels segments ara puc posar un **bs=1** i fer 451*512 i això ens donarà **quants** bytes de sectors hem de saltar per tal de començar on volem (seria el mateix que posar 451 amb bs=512). El que és interessant es posar el **count=15585** així obtindrem exactament la part que ocupa la imatge.

```
dd if=image bs=1 count=15585 skip=230912 of=coverimage.jpg
```

Després de fer això veig que no puc obrir la imatge encara i que encara està marcada com un "PC formatted floppy with no filesystem"... No sé molt bé què pot ser, he pensat que podria ser que la imatge estigués encriptada.

Fent recerca per internet i veient la pàgina de "Magic Numbers" m'he adonat que puc veure els strings que hi ha en un fitxer amb una comanda anomenada `strings`. A la pàgina dels Magic Numbers, buscant ".jpg" he trobat que pot apareixer com a un d'aquests codis:

FF D8 FF DB

FF D8 FF E0 00 10 4A 46 49 46 00 01

FF D8 FF EE

FF D8 FF E1 ?? ?? 45 78 69 66 00 00

yØÿÛ

ÿØÿà..JFIF..

ÿØÿî

ÿØÿá..Exif.

I d'aquest video he extret que concretament la paraula `JFIF` sol aparèixer al principi de tots els arxius jpg (és el seu "*Magic Number*"). Llavors he fet `strings image | grep JFIF` i he vist que realment apareix en algun lloc la paraula. Consultant el manual he vist que es pot fer sortir l'offset amb un flag i opcions. Finalment he obtingut el seguent:

strings -t d image | grep JFIF

37382 JFIF

Així que l'offset original es 37382, sé que ocupa 15585 bytes. Així que faré el mateix procediment que abans:

```
dd if=image bs=1 count=15585 skip=37376 of=coverpage.jpg
```

Ara si! He obtingut la imatge jpg que es un text negre amb una imatge estranya i un text vermell a sota on apareix el nom de Jimmy Jungle.

Per últim intentaré poder visualitzar l'arxiu **Scheduled Visits.exe** sabem que és un arxiu comprimit per el que hem vist en les metadades del **autopsy**. Però quan l'intento descomprimir dona un error. Així que el que he fet ha sigut anar a l'apartat de metadades de l'**autopsy** i allà he pogut veure els segments que ha detectat. He clicat a sobre el segment on comença (el 104) i m'ha portat a una pàgina on puc visualitzar el contingut dels segments. La visualització en ASCII no em deia res així que he anat provant i al final he vist que amb la visualitzacio HEX es com ho veia més ordenat.

El que estem buscant és el segment on acaba per tal de poder-lo extreure de la imatge correctament. Ja que després de provar-ho amb l'inici al segment 104 i el final amb la mida del fitxer ha fallat (llavors vol dir que es possible que m'estigui equivocant amb el final del fitxer).

Així doncs he anat clicant NEXT buscant algun punt on em dongués una pista de que allà acabaven les dades, i finalment he vist en el sector 108 que allà començaven uns HEX amb tots els seus valors a zero. He suposat que en aquest sector es on acaba l'arxiu.

Finalment tenim que l'arxiu comprimit camuflat en un .exe comença al sector 104 i acaba en el sector 108 (suposadament) i això sumen 4 sectors (Després de fer proves i només obtenir errors m'he adonat que realment són **5 sectors** ja que el sector 4 també compta). Executem la seguent comanda, seguint la mateixa tècnica:

```
dd if=image bs=512 count=5 skip=104 of=schedule.exe
```

Ara si que es un fitxer comprimit, si ho comprovo amb la comanda **file** diu el seu tipus "Zip archive data, at least v2.0 to extract". Al descomprimir-lo m'he adonat que necessito una contrassenya. Del document de text (la carta d'en Jacob a en Jimmy) sé que aquesta contrassenya l'havien dit el mateix missatge on va ser adjuntat l'arxiu "cover page.jpgc". Finalment després d'una estona sense trobar res, he fet un **strings** de la imatge, i per allà dins he trobat una cadena de text que m'ha cridat l'atenció que deia **pw=goodtimes** així que he suposat que seria la contrassenya. No entenc ben bé d'on prové ja que es troba en el byte 53024 i no hem trobat res per aquella zona (el més proper és la imatge).

En l'arxiu que conté el comprimit (scheduled visits.xls) veiem les escoles que ha freqüentat en Jacob durant Abril, Maig i Juny.