FINAL PROJECT

Jimmy Jungle

Team 1 – IST 454

Steven Bell, Alaric Bresler, Jonathan Mahoney, Patrick Rafter

Part 1

Data Forensic Workers: Steven Bell, Alaric Bresler, Jonathan Mahoney, Patrick Rafter
Data File Provided: Part 1.zip
Tools used: Autopsy / Foremost
Results:

The disk image file was provided in a zipped folder. Upon inspection of the zipped folder we found a file called "image" without an extension. We ran the image through Autopsy and found several files of interest:

cover page.jpgc
Jimmy Jungle.doc
Scheduled Visits.zip
Scheduled Visits.xls

The following are answers to questions of interest provided:

Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

Based on evidence in both the "cover page.jpgc" and the "Jimmy Jungle.doc" we conclude that Jimmy Jungle is the supplier of marijuana. The following address was listed at the top of the "Jimmy Jungle.doc":

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

What crucial data is available within the cover page.jpg file and why is this data crucial?

The file shows that Jimmy Jungle is both the grower and Joe Jacob's supplier.

What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

Provided in this report (attached at the end) is a list of scheduled visits found in the "Scheduled Visits.xls". These outline other schools scheduled to be visited. We conclude that Jimmy Jungle has probably visited most of these schools before.

For each file, what processes were taken by the suspect to mask them from others?

cover page.jpgc

- This file was readily available from importing the image file looking for carved space. We conclude that the "c" at the end of the jpg was added to throw off the file type.

Jimmy Jungle.doc

- This file was deleted and had to be recovered

Scheduled Visits.zip/xls

- "Scheduled Visits.xls" was found inside a zipped file "Scheduled Visits.zip". To open the zipped file required a password. We found the password using a keyword search for "pw". The password revealed was "goodtimes". Using the password we were able to open the zipped file and reveal the Scheduled Visits.xls inside.

What processes did you (the investigator) use to successfully examine the entire contents of each file?

cover page.jpg

- Found by mounting the "image" drive inside Autopsy. The "image" drive was also scanned using foremost. The .jpg was readily accessed by Windows 10 Photos.

Jimmy Jungle.doc

- Found by mounting the "image" drive inside Autopsy. The "image" drive was also scanned using foremost. The document was available in plaintext.

Scheduled Visits.zip

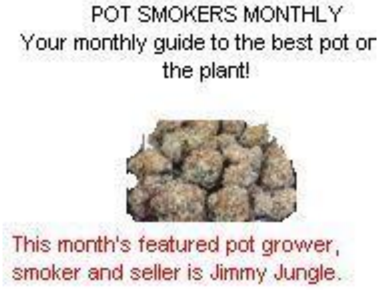
- We did a keyword search within autopsy using the criteria "pw" and came across the password, "goodtimes", used to open Scheduled Visits.zip.

What Microsoft program was used to create the Cover Page file. What is your proof?

The cover page.jpgc is most likely created in Microsoft Paint. We conclude this because in the cover page there is a bitmap which is created through Microsoft Paint. We also conclude that because after inspection of the image through Adobe Lightroom, we saw clear outlines of text boxes.

Provided Below is a visual of the files found including the chart of schools to be visited.

cover page.jpgc



POT SMOKERS MONTHLY
Your monthly guide to the best pot or the plant!

This month's featured pot grower, smoker and seller is Jimmy Jungle.

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

Scheduled Visits.xls

Chart1:

Month	**DAY**	**HIGH SCHOOLS**
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)
	Wednesday (3)	Birard High School (D)
	Thursday (4)	Richter High School (E)
	Friday (5)	Hull High School (F)
	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)

	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
June		
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)
	Wednesday (3)	Birard High School (D)
	Thursday (4)	Richter High School (E)
	Friday (5)	Hull High School (F)
	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)

Part 2:

Data Forensic Workers: Steven Bell, Alaric Bresler, Jonathan Mahoney, Patrick Rafter
Data File Provided: Part 2.zip
Tools used: Autopsy / XSteg / Invisible Secrets
Results:

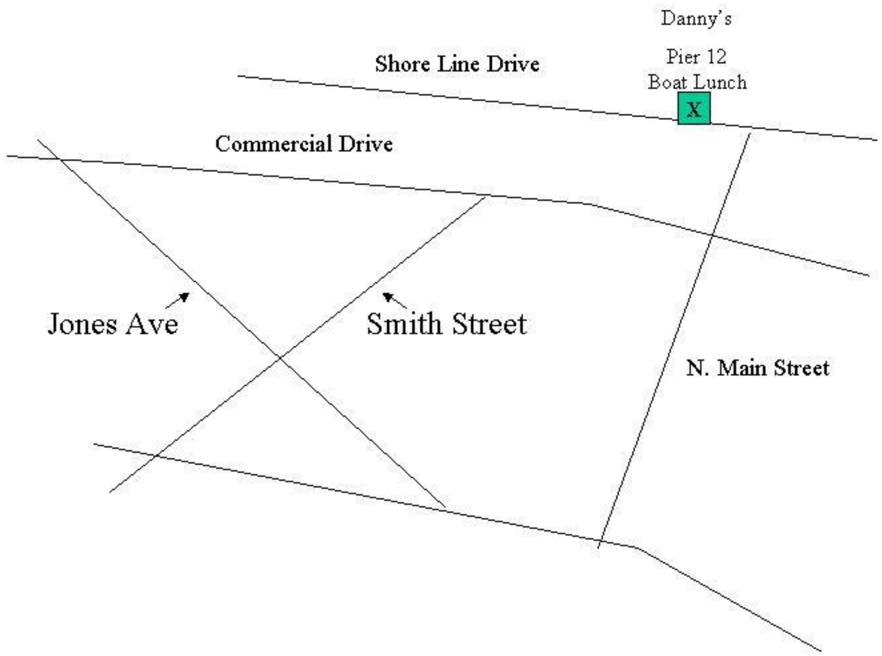
The disk image file was provided in a zipped folder. We ran the image through Autopsy and found several files of interest:

F00000000.jpg
F00000000.bmp
Unalloc_33_16896_1474560

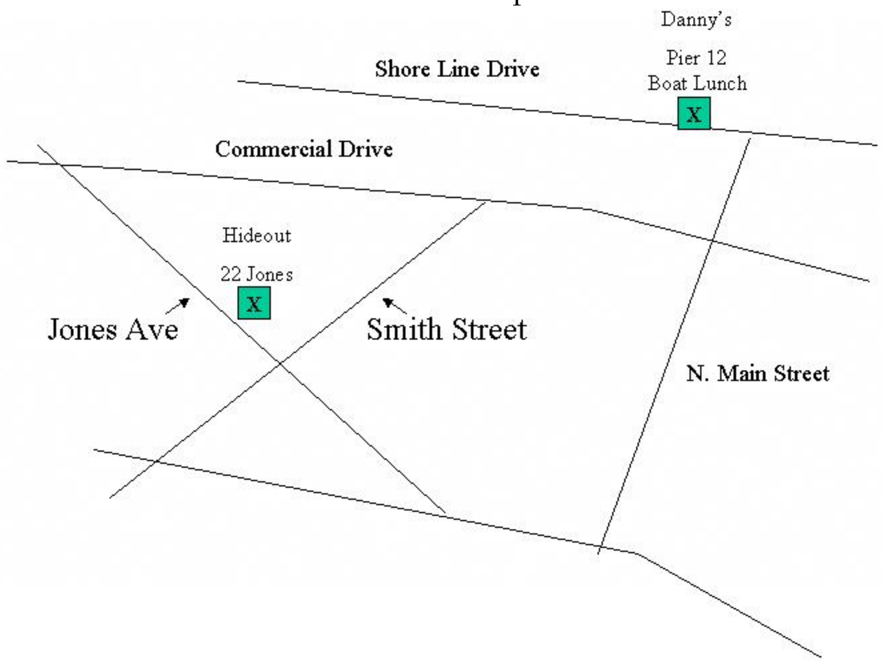
The following are answers to the problem provided:
Using autopsy, we found the following images along with an address, password, and website.
John Smith's Address: 1212 Main Street, Jones, FL 00001
pw: help
Dfrws.org

Along with the information listed above, we inspected the two images of maps and marked them as significant.

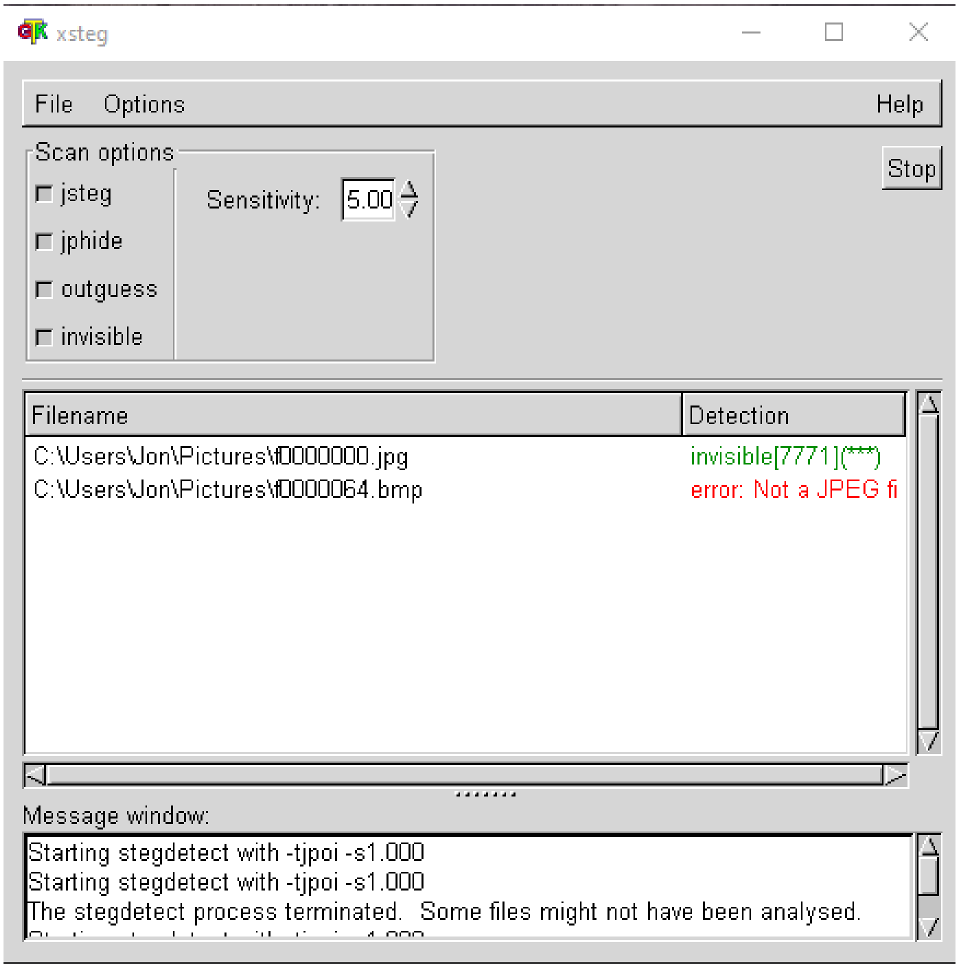
F00000000.jpg



F00000000.bmp



stegdetect Xsteg



Scan options

□ jsteg

□ jphide

□ outguess

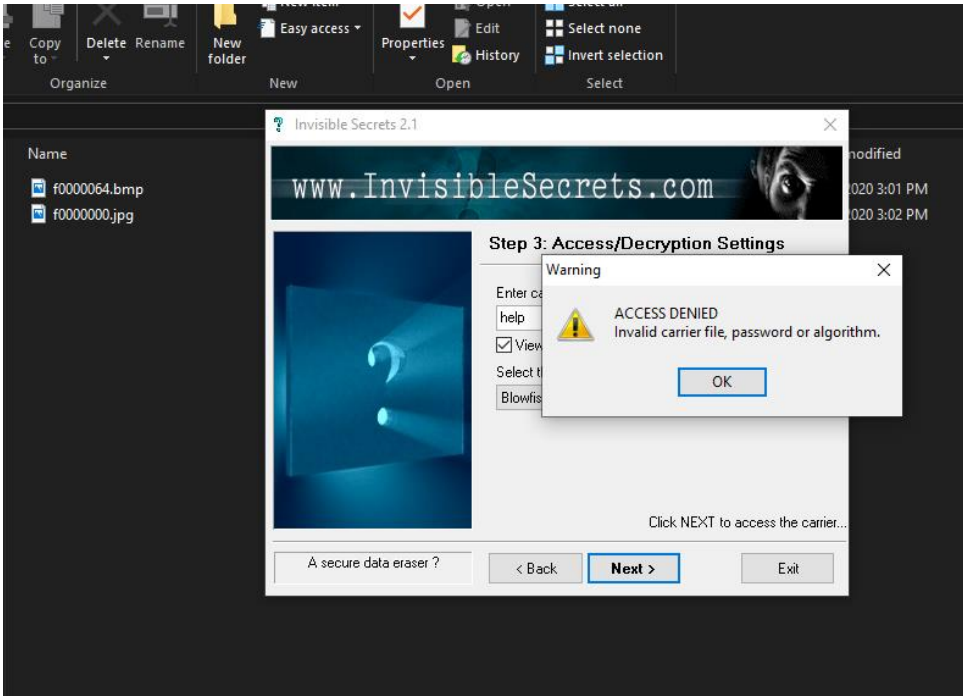
□ invisible

Sensitivity: 5.00

Filename	Detection
C:\Users\Jon\Pictures\f0000000.jpg	invisible[7771](***)
C:\Users\Jon\Pictures\f0000064.bmp	error: Not a JPEG fi

```
Starting stegdetect with -tjpoi -s1.000
Starting stegdetect with -tjpoi -s1.000
The stegdetect process terminated.  Some files might not have been analysed.
```

Using Xsteg, we confirmed that there was a file hidden using Invisible Secrets on the jpg.



Step 3: Access/Decryption Settings

help

Blowfis

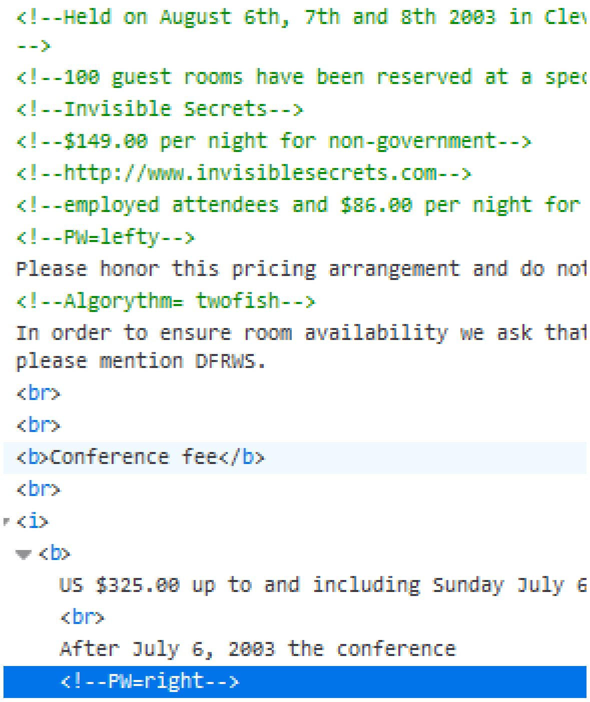
Click NEXT to access the carrier...

ACCESS DENIED
Invalid carrier file, password or algorithm.

After downloading Invisible Secrets, we pointed the program at the Bitmap and JPG with password from file “help” but neither worked.

We followed the website provided in the case and fond nothing of use one the home page, sub-pages, or source code. We then decided to use a wayback machine to inspect the website as it was Nov 30th 2002. We came to this decision due to the fact that the spreadsheet in part 1 was from 2002.

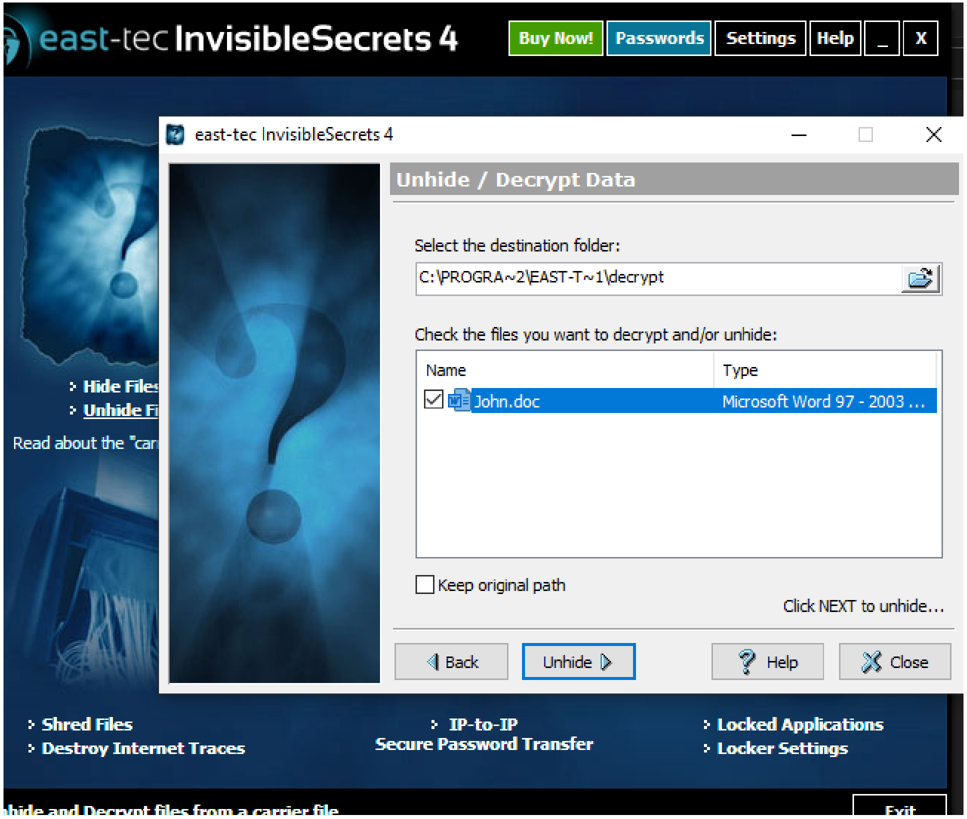
https://web.archive.org/web/20021002230915/http://www.dfrws.org/
In the source code we found the passwords “lefty” and “right” and the algorithm “twofish”



```
<!--Held on August 6th, 7th and 8th 2003 in Clev
-->
<!--100 guest rooms have been reserved at a spec
<!--Invisible Secrets-->
<!--$149.00 per night for non-government-->
<!--http://www.invisiblesecrets.com-->
<!--employed attendees and $86.00 per night for
<!--PW=lefty-->
Please honor this pricing arrangement and do not
<!--Algorythm= twofish-->
In order to ensure room availability we ask that
please mention DFRWS.
<br>
<br>
<b>Conference fee</b>
<br>
<i>
<b>
   US $325.00 up to and including Sunday July 6
   <br>
   After July 6, 2003 the conference
   <!--PW=right-->
```

The first version of Invisible Secrets we used was version 2.1, and did not have TwoFish encryption. We downloaded Invisible Secrets version 4.8 and were able to use the TwoFish encryption along with plenty of other algorithms.

Using the password “lefty” and TwoFish encryption, we found a hidden Word Document



east-tec InvisibleSecrets 4

Unhide / Decrypt Data

Select the destination folder: C:\PROGRA~2\EAST-T~1\decrypt

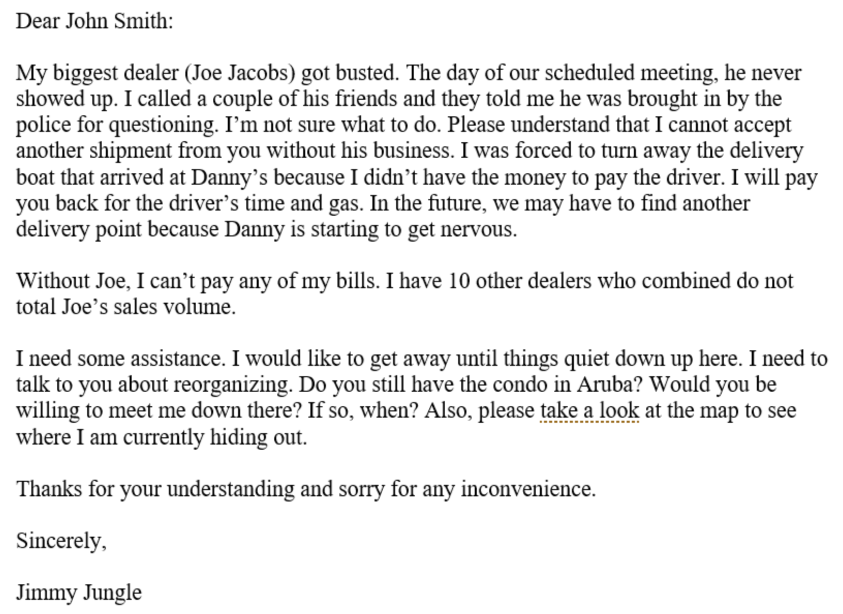
Check the files you want to decrypt and/or unhide:

Name	Type
☑ John.doc	Microsoft Word 97 - 2003 ...

□ Keep original path

Click NEXT to unhide...

Here are the contents of the Word Document



Dear John Smith:

My biggest dealer (Joe Jacobs) got busted. The day of our scheduled meeting, he never showed up. I called a couple of his friends and they told me he was brought in by the police for questioning. I'm not sure what to do. Please understand that I cannot accept another shipment from you without his business. I was forced to turn away the delivery boat that arrived at Danny's because I didn't have the money to pay the driver. I will pay you back for the driver's time and gas. In the future, we may have to find another delivery point because Danny is starting to get nervous.

Without Joe, I can't pay any of my bills. I have 10 other dealers who combined do not total Joe's sales volume.

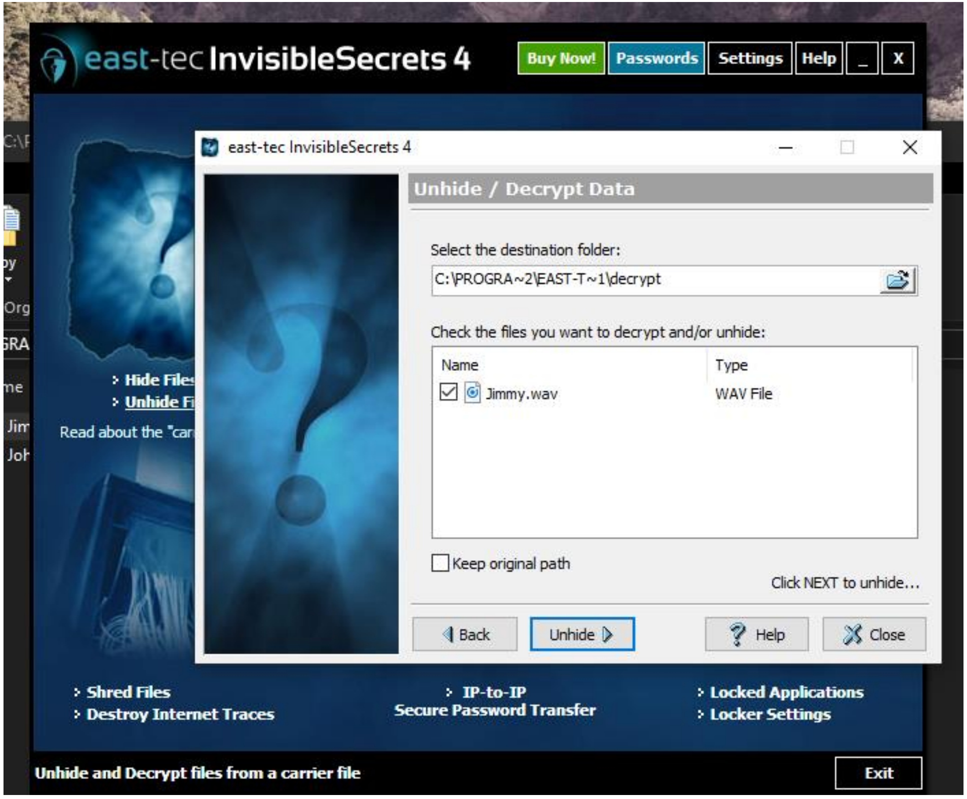
I need some assistance. I would like to get away until things quiet down up here. I need to talk to you about reorganizing. Do you still have the condo in Aruba? Would you be willing to meet me down there? If so, when? Also, please take a look at the map to see where I am currently hiding out.

Thanks for your understanding and sorry for any inconvenience.

Sincerely,

Jimmy Jungle

Using the other password, we found on the website, "right", we found a wav file. We again used the TwoFish encryption.



Unhide / Decrypt Data

Select the destination folder:

C:\PROGRA~2\EAST-T~1\decrypt

Check the files you want to decrypt and/or unhide:

Name	Type
☑ Jimmy.wav	WAV File

□ Keep original path

Click NEXT to unhide...

Unhide and Decrypt files from a carrier file

The Audio says,
"This is Jimmy. Meet me at the pier tomorrow. I drive a blue 1978 Mustang with Ontario License Plates."

Conclusions:

1. John Smith is the supplier to Jimmy Jungle and has a condo in Aruba
2. Jimmy Jungle is in a hideout at 22 Jones Ave
3. Jimmy drives a Blue 1978 Mustang with Ontario License Plates