Scan of the Month

October 2002

Fox-IT is an IT security company specialized in three important areas: Forensic IT, IT security and Practical training. Fox-IT was founded 3 years ago and has grown to employ 20 professionals. Fox-IT is known for its personal approach to customers, confidential treatment of sensitive material, delivery of custom products, large expertise, realistic pricing and implementation of large and prestigious projects.

Fox-IT's customers are found in many and varying areas: the police, governmental departments, sports organisations, financial businesses such as banks and insurance companies, lawfirms and notaries. Other areas where security and confidentiality are paramount are continually being added to this list.

EXPERTS IN IT SECURITY

Table of Contents

Preface

This report has been written for the 'Scan of the Month' project (SotM), Scan 24, September 2002. To be found at the URL: http://www.honeynet.org/scans/scan24/.

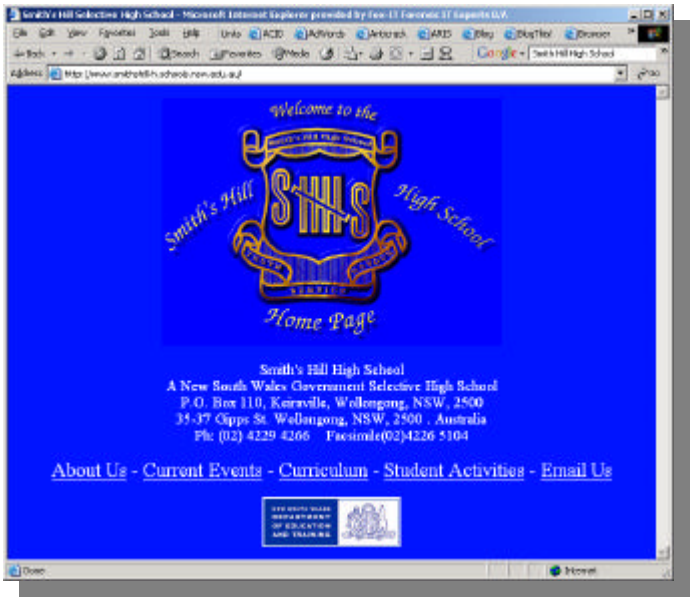
The scan is about a fictional situation, where our job is to analyze forensic evidence. This means analyzing a recovered floppy, read a police report and answer the questions asked.

A 'SotM' like this one is pretty similar to the real forensic IT investigations that we encounter. An investigation is never only technical, but also requires analytical skills as well.

At Fox-IT we've enjoyed solving this 'puzzle' and have put our effort towards finding the right answers and conclusions. We've even put this challenge into a small competition between our forensic IT investigators and the management.

May the best win,

Fox-IT Management Team



Challenge

The SotM Challenge 24, of September 2002, gave us the following information:

A. image.zip file, MD5 checksum b676147f63923e1f428131d59b1d6a72. contains a file: “image” (no extension). File size: 1474560, Creation Time: 2-10-2002 12:02, Last Access Time: 2-10-2002 12:05, Last Write Time: 18-9-2002 16:50, MD5 checksum: ac3f7b85816165957cd4867e62cf452b
B. Police report, see appendix A.
C. Questions

The image.zip file has been downloaded and the checksum successfully verified. The image.zip files contains a file named “image”. This file was investigated using proprietary forensic IT tools. In this report, the term ‘floppy disk’ refers to this file “image”.

Questions

In order to solve the SotM Challenge, the following questions have to be answered:

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Bonus Question:

6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

Answers

This section of the report describes the answers to the questions asked and the way we found them.

Question 1: Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

The floppy disk contains a Microsoft Word file with a letter from 'joe' to:

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

From the contents of the letter it appears that the name of Joe's supplier is "Jimmy Jungle" and the address mentioned above is his address.

The letter can be found in Appendix B.

Question 2: What crucial data is available within the coverpage.jpg file and why is this data crucial?

The floppy disk contains a JPG file with a JPEG image. This JPG file has a size of 15585 bytes (0x3ce1).

Within the slackspace of this file we found the reference 'pw=goodtimes'. 'goodtimes' turns out to be the password to open the password-protected zip file we found on the floppy disk. This password was not really crucial to open the zip file. This zipfile could also have been brute-forced because we know some known plain text, namely the fact that the zip file contains an Excel spreadheet with a known header.

Question 3: What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

We found an Excel spreadsheet on the floppy disk named 'Scheduled Visits.xls'. This Excel spreadsheet contains a reference to the some dates and High School names. This spreadsheet can be found in appendix C.

These are the names of High Schools that we've found besides Smith Hill High School:

- Key High School
- Leetch High School
- Birard High School
- Richter High School
- Hull High School

From the sole facts that these names of a number of high schools and several dates are stored in a spreadsheet and a reference to 'a schedule' in a Word document, both found on a floppy disk, can not be concluded that Joe Jacobs frequents other high schools. However, this information may be used in a further investigation.

The spreadsheet has been created by an author: 'CSTC' from company: 'AFRL'.

Question 4: For each file, what processes were taken by the suspect to mask them from others?

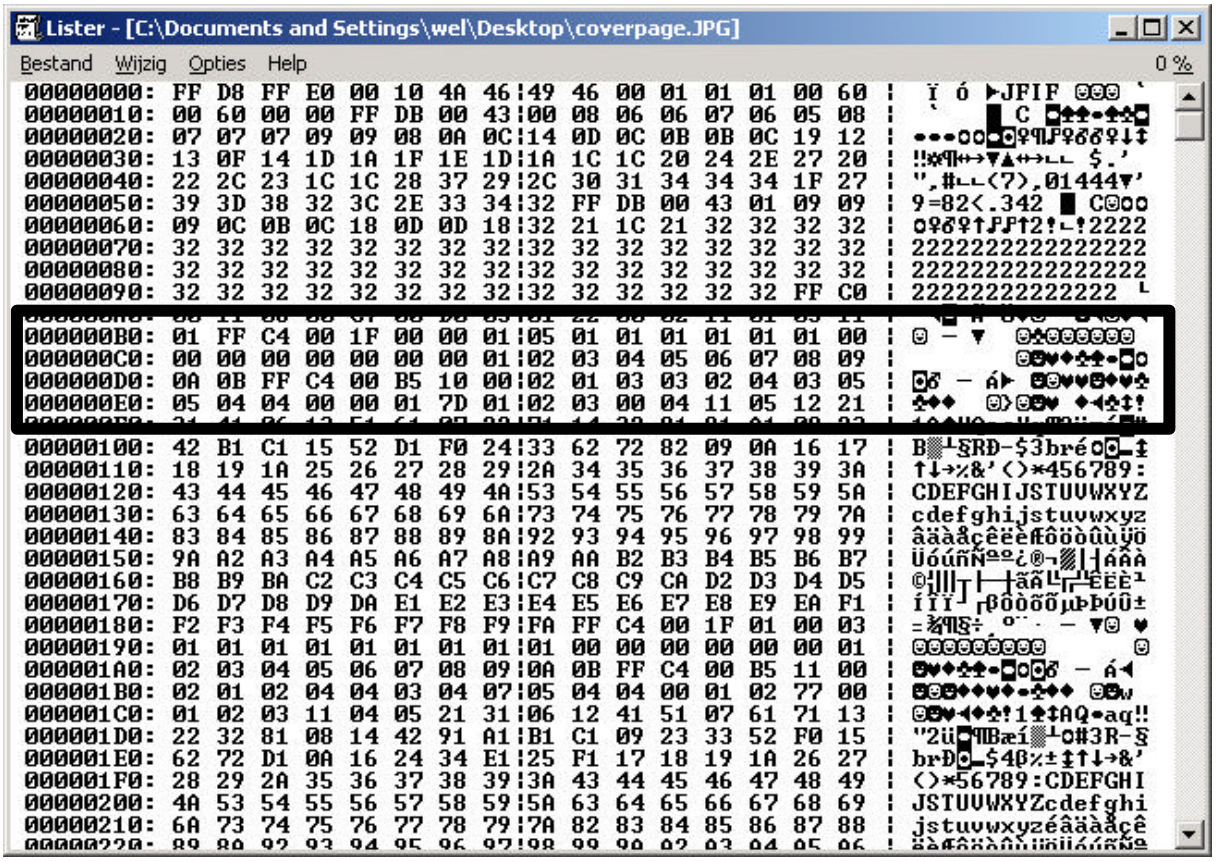
- Schedule.exe: Zip file was renamed as an executable (.exe). File length in the root directory was changed from 2420 to 1000 bytes.
- Cover page.jpg: file name was edited. Start cluster was changed from sector 42 to 420.
- Jimmy jungle.doc: File was deleted
- Scheduled Visits.xls: File was hidden in a password protected zip file.

Question 5: What processes did you (the investigator) use to successfully examine the entire contents of each file?

A. We've download the IMAGE.ZIP file from the SotM website.
B. We've verified the MD5 hash.
C. We've extracted the file 'IMAGE' from the downloaded file.
D. We transferred the file 'IMAGE' to a 3,5" floppy disk, using RAWRITE.EXE.
E. We've edited the floppy disk using DISKEDIT in the following order:
    a. After examining the floppy we concluded that the JPG file starts at cluster 42 and not 420 as stated in the directory entry.
    b. The zip file seems to be longer than 1000 bytes. The exact size has been determined by examining the zip file format structure and we concluded that this should be 2420 bytes.
    c. Both errors where edited in the directory entries after which we were able to copy the files.
    d. The word file was deleted. We recoverd this file by using the dos-UNDELETE tool.
F. We've opened the Word file in MS Word, reviewed the contents and file attributes.
G. We've opened the COVERPAGE.JPG in MS Photo Editor to examine the contents.
H. We've opened the COVERPAGE.JPG in UltraEdit to examine the headers of the file and the slackspace.
I. We've done some background research on JPG headers.
J. We've opened the ZIP file using the password found in the slackspace of the COVERPAGE.JPG file.
K. We've opened the Excel file in MS Excel, reviewed the contents and file attributes.

Question 6: What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

The program used was Microsoft Paint. The Huffman table used by this application seems to be unique and has not been found to be used by another application.



Extra information

We also found the following extra information on the floppy disk:

- The text “Hp deskjet 970c” was found. This could mean that a HP Deskjet 970c printer was connected to the PC/workstation that was used.

Appendix A: Police Report

The scenario is: Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students. A local police officer posed as a high school student was approached by Jacobs in the parking lot of Smith Hill High School. Jacobs asked the undercover cop if he would like to buy some marijuana. Before the undercover cop could answer, Jacobs pulled some out of his pocket and showed it to the officer. Jacobs said to the officer "Look at this stuff, Colombians couldn't grow it better! My supplier not only sells it direct to me, he grows it himself."

Jacobs has been seen on numerous occasions hanging out at various local high school parking lots around 2:30pm, the time school usually ends for the day. School officials from multiple high schools have called the police regarding Jacobs' presence at their school and noted an increase in drug use among students, since his arrival.

The police need your help. They want to try and determine if Joe Jacobs has been selling drugs to students at other schools besides Smith Hill. The problem is no students will come forward and help the police. Based on Joe's comment regarding the Colombians, the police are interested in finding Joe Jacob's supplier/producer of marijuana.

Jacobs has denied selling drugs at any other school besides Smith Hill and refuses to provide the police with the name of his drug supplier/producer. Jacobs also refuses to validate the statement that he made to the undercover officer right before his arrest. Upon issuing a search warrant and searching of the suspect's house the police were able to obtain a small amount of marijuana. The police also seized a single floppy disk, but no computer and/or other media was present in the house.

The police have imaged the suspect's floppy disk and have provided you with a copy. They would like you to examine the floppy disk and provide answers to the following questions. The police would like you to pay special attention to any information that might prove that Joe Jacobs was in fact selling drugs at other high schools besides Smith Hill. They would also like you to try and determine if possible who Joe Jacob's supplier is.

Jacob's posted bail set at $10,000.00. Afraid he may skip town, the police would like to get him locked up as soon as possible. To do so, the police have asked that you have the results fully completed and submitted by October 25, 2002. Please provide the police with a strong case consisting of your specific findings related to the questions, where the findings are located on the disk, processes and techniques used, and any actions that the suspect may have taken to intentionally delete, hide and/or alter data on the floppy disk. Good Luck!

Any names, locations, and situations presented are completely made up. Any resemblance to any name, locations and/or situation is purely coincidence.

Appendix B: Word Document

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

Document properties:

Title:	Jimmy Jungle
Author:	0000
Company:	OOOO
Template:	Normal.dot
Size:	35,5 kB (36.352 bytes)

Appendix C: Spreadheet

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)