Creation Process:

Realistic Forensic Corpora for Undergraduate Education and Research

Using a MAC
Select Finder/Applications/Utilities/Disk Utilities

- Create New Image
- Called it "Gilbert"
- Custom size of 64 MB
- Placed on Desktop
- MSDOS-FAT format

Once Disk Image created, double click on the image, and zero out the free space (it's all free space at this point).

Once the image was created, I put 3 folders onto the image

Folder Contents initially on Image:
"Docs" Folder contains:

- Alice1.bmp – a bmp of page 1 of Alice in Wonderland
- Video0001.3g2 – a 30 second video of the lab taken with an LG cellphone

Pics Folder contains:

- car1.bmp, car2.bmp, car3.bmp, car4.bmp, car5.bmp, car6.bmp, car7.bmp, car8.bmp, halloween1.bmp, halloween2.bmp, halloween3.bmp, halloween4.bmp, halloween5.bmp, halloween6.bmp

"Copy of Pics" Folder contains:

- car1.bmp, car2.bmp, car3.bmp, car4.bmp, car5.bmp, car6.bmp, car7.bmp, car8.bmp, halloween1.bmp, halloween2.bmp, halloween3.bmp, halloween4.bmp, halloween5.bmp, halloween6.bmp, readMe.pdf, readMe.txt

Once the folders were on the image, the following steps were taken:

- opened every file in each folder (one at a time)
- opened each pic in "Pics" sequentially with its copy in "Copy of Pics"
    - so I had two files open with the same name, then closed them and moved onto the next one
- Deleted the readMe.pdf and readMe.txt in the "Copy of Pics" folder
- Made 5 copies of the video0001.3g2 in the "Docs" folder (to fill up space)
- Deleted the 5 copies of video0001.3g2

A copy of the image was saved and then exported to an external hard drive.

Image Name: Gilbert.dmg

Image Author: LT Henry T Gilbert, USN

Image Creation Date: 10/22/09

Instructor Documentation:

Realistic Forensic Corpora for Undergraduate Education and Research

Image Name: Gilbert.dmg

Image Author: LT Henry T. Gilbert, USN

Image Creation Date: 10/22/09

Objectives: The objective is to analyze a 64MB image (chose the size for a thumb drive but created the image on a MAC) and recover any sensitive data.

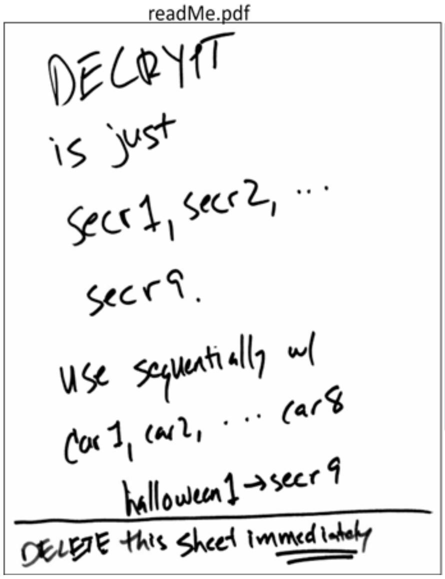
- Scenario: a thumb drive has been given to you by the DHS, and they want to know what is on it. So far it looks innocuous – just pics and videos. Find out if there is anything worthwhile on it.

Tools: Sleuthkit, Invisible Secrets 2.1

Resources/Websites:
http://www.sleuthkit.org
http://www.invisiblesecrets.com/ver2/index.html

Answer Key:
There are 9 steganography pictures inside the "Copy of Pics" folder. They are the same size as their counterparts in the "Pics" Folder. There are also readMe.pdf and a readMe.txt which have been deleted. They contain useful information:

readMe.pdf

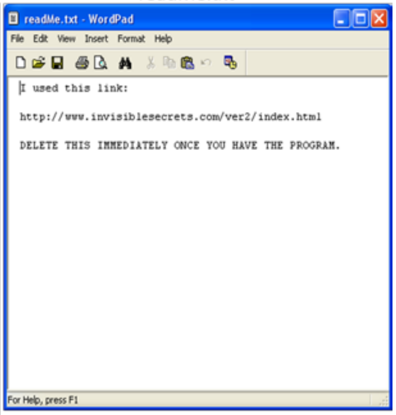


DECRYPT
is just
secr1, secr2, ...
secr9.

Use sequentially w/
car1, car2, ... car8
halloween1 → secr9

DELETE this sheet immediately

readMe.txt



I used this link:

http://www.invisiblesecrets.com/ver2/index.html

DELETE THIS IMMEDIATELY ONCE YOU HAVE THE PROGRAM.

Image Format: dmg

File Information

File Name	File Description	File Type	File Status	Useful Info	Tools needed
Docs Folder:					
Alice1	Alice in Wonderland page	Png	available		
video0001	Lab video	3g2	available		
Pics Folder:					
car1	car picture	Bmp	available		
car2	car picture	Bmp	available		
car3	car picture	Bmp	available		
car4	car picture	Bmp	available		
car5	car picture	Bmp	available		
car6	car picture	Bmp	available		
car7	car picture	Bmp	available		
car8	car picture	Bmp	available		
halloween1	halloween picture	Bmp	available		
halloween2	halloween picture	Bmp	available		
halloween3	halloween picture	Bmp	available		
halloween4	halloween picture	Bmp	available		
halloween5	halloween picture	Bmp	available		
halloween6	halloween picture	Bmp	available		
Copy of Pics Folder:					
car1	car picture	Bmp	available	steg - pw: secr1	Invisible Secrets
car2	car picture	Bmp	available	steg - pw: secr2	Invisible Secrets
car3	car picture	Bmp	available	steg - pw: secr3	Invisible Secrets
car4	car picture	Bmp	available	steg - pw: secr4	Invisible Secrets
car5	car picture	Bmp	available	steg - pw: secr5	Invisible Secrets
car6	car picture	Bmp	available	steg - pw: secr6	Invisible Secrets
car7	car picture	Bmp	available	steg - pw: secr7	Invisible Secrets
car8	car picture	Bmp	available	steg - pw: secr8	Invisible Secrets
halloween1	halloween picture	Bmp	available	steg - pw: secr9	Invisible Secrets
halloween2	halloween picture	Bmp	available		Invisible Secrets
halloween3	halloween picture	Bmp	available		Invisible Secrets
halloween4	halloween picture	Bmp	available		Invisible Secrets
halloween5	halloween picture	Bmp	available		Invisible Secrets
halloween6	halloween picture	Bmp	available		Invisible Secrets
readMe	text file	Txt	deleted/partial	need to recover	Sleuthkit
readMe	pdf scan	Pdf	deleted/partial	need to recover	Sleuthkit
Steg Files:					
secr1	secret message	Jpg		embedded in car1	Invisible Secrets
secr2	secret message	Doc		embedded in car2	Invisible Secrets
secr3	secret message	Xls		embedded in car3	Invisible Secrets
secr4	secret message	Ppt		embedded in car4	Invisible Secrets
secr5	secret message	Txt		embedded in car5	Invisible Secrets
secr6	secret message	Rtf		embedded in car6	Invisible Secrets
secr7	secret message	Mht		embedded in car7	Invisible Secrets

secr8	secret message	Bmp		embedded in car8	Invisible Secrets
secr9	secret message	Gif		embedded in halloween1	Invisible Secrets

If the two readMe files are not recovered, students may need to look at the hex code of the pics and determine if they have been altered. Then that can run a password cracker to recover the embedded files.

Student Instructions:

Realistic Forensic Corpora for Undergraduate Education and Research

Image Author: LT Henry T Gilbert, USN

Image Creation Date: 10/22/09

Image Name: Gilbert.dmg

Objectives:

- Analyze the disk image for any abnormalities or indications of sensitive data being transferred.
- There are 3 folders on the disk image: Docs, Pics and Copy of Pics
- Carefully look at the files to determine if there is something suspicious
- Try to recover any deleted files and analyze them for clues
- You may need to look at the hex dump of the files, but there are easier methods and clues on the image

Tools:

- Sleuthkit
- You may need other programs, but part of the process is figuring out what you'll need. Any software required will be widely available and freeware, so the process should not be too painful

Resources/Websites:
http://www.sleuthkit.org