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.

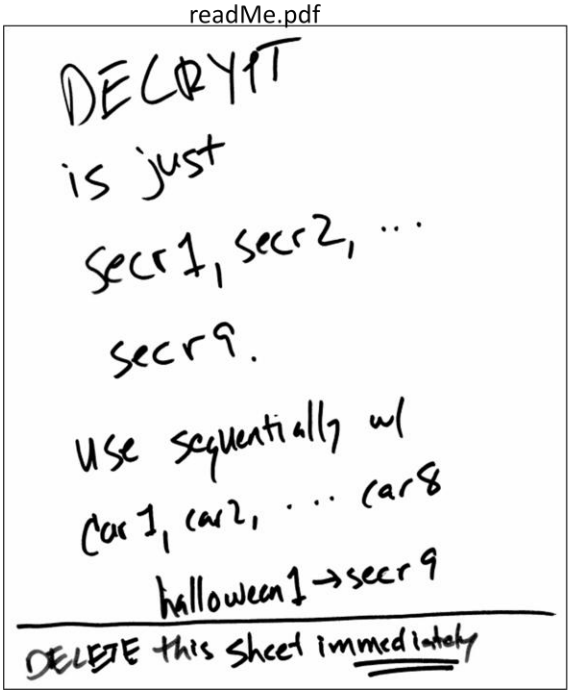
- Scenario: a thumb drive has been given to you by the DHS, and they want to know what is on it. So far it looks innocuous – just pics and videos. Find out if there is anything worthwhile on it.

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



readMe.txt

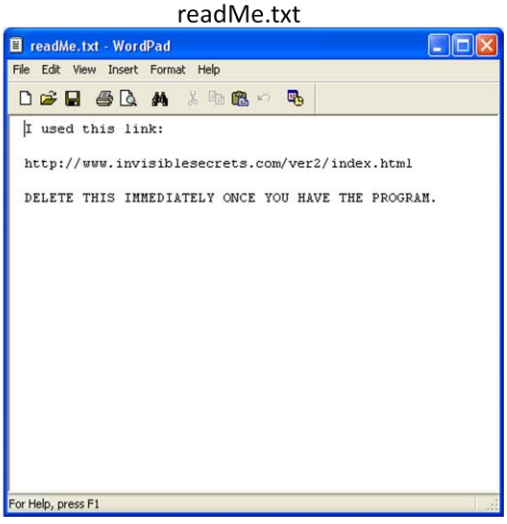


Image Format: dmg

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.