CCF Lab Assignment: Hiding and Filesystems*

Arno Bakker Mick Pouw
Arno.Bakker@os3.nl

Feedback deadline:
February 22, 2018 10:00 CET

Abstract

This lab will introduce you to filesystem analysis and steganography. You should work mostly alone to achieve this.

1 Steganography

1. Look for 3 different tools that can hide files in images.
   (a) How do the tools hide the files?
   (b) Using very exotic tools usually leads to better results. Explain why this is.
   (c) Are there any detection tools that can detect the tools you name?
2. Pick your favorite tool and use this to send over a file to another student. Be creative in the way of transportation.
3. Install a detection package and use it to detect whether your secret is exposed. Write down the steps you take.
4. Decode a file from one of your colleagues. Explain the steps that you used.
5. Download Dave's usbkey.hdd from `https://software.os3.nl/CCF/`. Make sure you check the files.
6. How would you approach the detection of steganography in a large set of files? Use this method on Dave's USB key
7. Dave confessed that he used the steghide tool. Try to find out what file Dave hid.
8. Write a small paragraph of maximum 400 words about your approach and findings.

2 Filesystem

9. Read up on EXT4. Write a small paragraph of maximum 400 words answering the following questions:

*Version February 15, 2018.

(a) What is ext4's on-disk layout?

(b) How does ext4 use of a log affect your work as a forensic investigator?

10. Detect whether there is an encrypted container on the USB key. This can be done by calculating the entropy. *Hint:* `binwalk`

11. Using a hex editor, can you detect that something is off?

12. Try to find out what happened to the filesystem.

13. Write a small paragraph of maximum 200 words about your findings.