Introduction to Digital Forensics

Institute of Distributed Systems | Semester
Supervisor
Lecturer

Exercise X: Anti-Forensics

Overview

This exercise will emulate a forensic examination focusing on practicality and anti-forensics. The task is wrapped in a story and aims in putting the student in the role of a forensic examiner trying to solve a case.

As usual, you are free to use resources on the Internet. However, in each task, make sure you explain all steps taken. That means you need to **explain your answers**.

Submission

Please follow the submission guidelines given at the end of the assignments and in *Exercise Sheet 1*.

Task 1: Working Environment Setup (X)

To be able to solve this task, let us start with the preparation of our working environment. First of all, start with preparing a virtual machine. For this sheet, a Kali Linux distribution is recommended. You can find suitable Kali Linux virtual machines under `https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/`. Other Linux distros, and even Windows, are also suitable, but the effort of installing all needed packages is not worth it.

Submission:

- No need to submit anything for this task, just get your working environment up and running.

Task 2: Panda Steganography (X)

You are given a text file *panda.txt* about pandas. Take a look at it and figure out what hidden data is lying beneath. Think out of the box, try out different tactics and tools, the environment that you setup before could be helpful. Dont forget that you are a computer scientest, programming is also part of your job description.

Submission:

- *a1/* (the directory name)
  - *a1.txt*: add all documentation/explanations/answers/sources/etc. to this file

Task 3: BND Forensic Examination (X)

A Chinese spy has been arrested by the BND. The laptop of said spy was confiscated. It is known that Chinese spy especially like to communicate using information hidden within graphics.

You, as a world class forensic examiner at the BND, now have the task to uncover the secret information. It is extremely important to uncover the information, it is a matter of life and death. Simultaneously the agent is being questioned to extract further information out of him.

Whenever a new information is gathered, you will get a hint for your further examination. Let us start with two basic tips:

- banana
- dump.zip

Submission:

- *a2/* (the directory name)
  - *a2.txt*: add all documentation/explanations/answers/sources/etc. to this file