


## Lab 10 - Forensics

### Overview

Computer forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

### Exercises


You are a private investigator and you have 2h to solve 9 crimes. At the end of every crime you will find a flag that looks like **ISC{...}**. Are you up to the task?

 Here is your data.

All exercises can be solved on the local Linux machine.



#### 00. Capture 1

This is traffic capture of a suspect that we've been following for a long time. Can you find anything interesting like login credentials?

Hint1    
Hint2  

#### 01. Unknown File Type

We've found this file on a confiscated machine, but we can't figure what it is. Can you help us?



Hint1  

#### 02. Hidden Flag

There is something uncanny about this image. Is it trying to give us a hint?



#### 03. Corrupted File

During a transmission, one of our files got corrupted. Take a look and see if you can do something about it.

Hint1  



#### 04. Audio Visualization

We have intercepted an alien transmission, but there is no way to understand what is it saying. Maybe we should look at it.

Hint1  



#### 05. Hidden File

There is something wrong with the size of this image. Is there anything else there?

Hint1  

#### 06. Censored

We've found a letter in the trash can of a suspect, but some of the info is censored. Do some magic and find what is underneath the black box.



Hint1  

#### 07. Waiting for eternity

We stared at this gif for the last hour but nothing is happening. Would you like to join us and stare at it for the next hour?

#### 08. Capture 2

This is an USB capture of a device connected to a suspect's machine. Can you find what he's been typing?

Hint1  

### Resources

- Hex Editor
- Wireshark
- Binwalk
- Audacity
- Image extractor
- USB documentation

#### 11. [10p] Feedback

Please take a minute to fill in the  feedback form for this lab.

Search

#### Lectures

- [Lecture 01 - Introduction](#)
- [Lecture 02 - Cryptography](#)
- [Lecture 03 - Hardware Security](#)
- [Lecture 04 - Access Control](#)
- [Lecture 05 - Authentication and Key Establishment](#)
- [Lecture 06 - Application Security](#)
- [Lecture 07 - Operating System Security](#)
- [Lecture 08 - Network Security](#)
- [Lecture 09 - Web Security](#)
- [Lecture 10 - Privacy Preserving Technologies](#)
- [Lecture 11 - Forensics](#)

#### Labs

- **kernel**
- [Lab 01 - Introduction](#)
- [Lab 02 - Cryptography](#)
- [Lab 03 - Authentication and Key Establishment Lab](#)
- [Lab 03 - Hardware Security](#)
- [Lab 04 - Access control](#)
- [Lab 05 - Authentication in Linux](#)
- [Lab 06 - Application Security](#)
- [Lab 07 - Operating System Security](#)
- [Lab 08 - Network Security](#)
- [Lab 09 - Web Security](#)
- [Lab 10 - Forensics](#)
- [Lab 11 - Privacy Technologies](#)
- [Lab 12 - Security and Machine Learning](#)

#### Support

- [Useful resources](#)
- [Virtual Machine](#)

#### Table of Contents

- Lab 10 - Forensics
  - Overview
  - Exercises
    - 00. Capture 1
    - 01. Unknown File Type
    - 02. Hidden Flag
    - 03. Corrupted File
    - 04. Audio Visualization
    - 05. Hidden File
    - 06. Censored
    - 07. Waiting for eternity
    - 08. Capture 2
  - Resources
    - 11. [10p] Feedback