



# INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

## FORENSICS CYBER-SECURITY

MEIC, METI

### Lab Assignment I

**STORM AREA 51 – Stage I**

2019/2020

nuno.m.santos@tecnico.ulisboa.pt

## Introduction

You will be conducting the investigation of a case entitled “Storm Area 51”. This investigation will be guided along three progressive stages performed respectively at each lab assignment. This first guide provides an overall introduction of the case and describes the first assignment, which will help you gain hands-on experience on file forensics and steganalysis. This exercise requires the examination of a small number of files which can be downloaded from the course website (`csf-lab1-artifacts.zip`). To analyze these artifacts, you may use the Kali Linux distribution on a forensically sound virtual machine.

## Scenario presentation

On September 20, 2019, an American Facebook event took place at Area 51, a highly classified United States Air Force (USAF) facility in Nevada. It was created by the initiative of Matty Roberts, a 21-year-old college student, to raid the site in a search for extraterrestrial life. Matty quickly fell under the suspicion of the military forces responsible for patrolling the site. As always in these cases, a contingent of the USAF was tasked to conduct an investigation with the purpose of determining whether Matty may have had access to classified information and discover how it leaked from Area 51. Hired as a member of this team, your role is to lead the forensic operations in search for relevant digital evidence.

In addition to Matty, several potential stakeholders were identified by the USAF team:

- **Joe Bartels:** News reporter that gained worldwide attention by covering this story for KTNV.
- **Justin Roberts:** Matty’s older brother, a high-ranked USAF military working in Area 51 facilities.
- **Tim Frasik:** Matty’s close friend; they know each other for years, and share the same dorm room.

The following files were extracted from a pen drive that was found in Matty’s dorm room:

File	MD5 Value
masashi_kishimoto.txt	990eea6aae1cda8dba7f9e2b291b8163
naruto_run.gif	d28309dde3a82dddd524eb28d0cccd641
naruto_wikipedia.txt	d441c7d49cab2adf84d2c95302a04d36
villains.zip	12e20730cccdadfcfe72908be84ea27f1
akamaru.bmp	2954d9fc50198672430f053a455be783
attack	0fae36d3e066288d255df5a00fed1d13
naruto_scream.wav	3a50e65840707bd28f26219d6b7c9401
naruto_opening.wav	ddb4e1171739df0f1d8bdc5f2f705d4

Your task is to analyze these files and search for evidence about any leaked information. Write a forensic report that describes your findings. The deadline for this work is October 25<sup>th</sup>. Until then, you must upload to Fenix a compressed zip file containing three deliverables:

- **Digital Forensic Report:** A document in which you present your main findings. You must identify all recovered evidence artifacts, if any, and explain how you obtained them. We recommend you to use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.
- **Auxiliary Items:** Programs, scripts, and additional documents that you have produced during the investigation which are important to justify your results must also be included.

**TIPS:** There are in total 6 hidden secrets in the provided artifacts. The secrets were hidden using some of the techniques that were introduced in the theory classes about file forensics and steganography.

Good luck!