Digital Forensics
Prof. Taras Holotyak — EPFL

Notes by Tanguy Cavagna

Computer Science Master — Semester 1
Autumn 2024

This document is based on the work on Joachim Favre, a friend who studied at EPFL and wrote all of his classes notes using this method. To view the original repository, please visit the link bellow :

`https://github.com/JoachimFavre/UniversityNotes`

I made this document for my own use, but I thought that typed notes might be of interest to others. There are mistakes, it is impossible not to make any. If you find some, please feel free to share them with me (grammatical and vocabulary errors are of course also welcome). You can contact me at the following e-mail address :

`tanguy.cavagna@etu.unige.ch`

If you did not get this document through my GitHub repository, then you may be interested by the fact that I have one on which I put those typed notes and their LaTeX code. Here is the link (make sure to read the README to understand how to download the files you're interested in) :

`https://github.com/ToguyC/Computer-Science-Master-Notes`

Please note that the content does not belong to me. I have made some structural changes, reworded some parts, and added some personal notes ; but the wording and explanations come mainly from the Professor, and from the book on which they based their course.

Since you are reading this, I will give you a little advice. Sleep is a much more powerful tool than you may imagine, so do not neglect a good night of sleep in favour of studying (especially the night before an exam). I wish you to have fun during your exams.

Version 2024–09–18

To Gilles Castel, whose work has
inspired me this note taking method.

Rest in peace, nobody
deserves to go so young.

Table des matières

Liste des cours

Chapitre 1

Summary by lecture

- Principes de base du digital forensics
- Introduction à la forensics multimédias
- Principes généraux de la forensics multimédias
- Exemples de forensics multimédias

Chapitre 2

Organisation

Moodle Tout les documents sont présent sur le Moodle du cours. À consulter régulièrement.

Évaluation Les cours comportent des contrôles continues (toutes les 6 séances) ainsi qu'un examen orale, total 40%. L'examen oral est facultatif si les contrôles continues (2 questions écrites par contrôles) se sont bien passé. Les labos comptent pour 30%, et le mini-projet pour 30%. Le mini projet est basé sur un papier de recherche choisi que l'on doit étendre et implémenté, accompagné d'un rapport et d'une petite présentation.

Chapitre 3

Principes de base du digital forensics

Qu'est-ce que le digital forensics Le digital forensics est une discipline émergente en sciences informatiques qui peut paraître un peu *voodoo science*. Cette discipline n'est pas encore complètement standardisée et encore beaucoup reste à faire en recherche. L'utilisation du digital forensics vient à la suite d'un incident afin de répondre aux questions : qui, quoi, quand, où, pourquoi, et comment. Pour chaque investigation, quatre étapes sont toujours nécessaires : acquisition, identification, évaluation, et présentation.

Acquisition L'acquisition consiste à gagner la possession des appareils numériques, réseaux, et autres outils de stockage. Cette acquisition est analogue aux scènes de crimes du *monde réel*. Les données ne doivent en aucun cas être altérée. Les investigateurs doivent documenter le plus possible l'ensemble des procédures faites lors de l'investigation dans un but de non-répudiation, et de créer des copies conformes de chaque preuve acquise.

Identification Cette étape consiste à évaluer quelles données peuvent être recouvrée et les récupérer en utilisant différents outils de digital forensics. Chaque action doit être faite sur des copies afin de ne pas altérer les originaux, et les données cachée, supprimée, chiffrée, etc, peuvent être difficile à récupérer, voir impossible.

Évaluation L'évaluation consiste à déterminer si les informations collectées peuvent être utilisées contre le suspect. Cette détermination est faite en utilisant différentes méthodologies dépendant des objectifs, et recréer la timeline des événements.

Présentation Une fois que toutes les données ont été récupérées et qu'elles sont utilisable contre le suspect, il faut les présenter afin que les personnes n'étant pas dans le monde technique puissent comprendre, comme des avocats, et pour que les informations puissent être utilisée comme preuve par les différentes instances judiciaires.

Toutes les étapes sont analogue à la criminologie réelle, et les mêmes genre de méthodologies doivent être appliquée afin que le monde réel et numérique puissent travail dans un même environnement.