

1 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.

2 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 <i>voodoo science</i> . 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 <i>monde réel</i> . 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.