

Plan de cours 2018-2019

Module Options d'école – Prélèvement de Traces Numériques

Cours 644-17 / 645-27

David Billard, Flávio Barrero Lindo

Semestre printemps 2019

Objectifs du cours

Sensibiliser les étudiants à l'informatique légale (*digital forensics*) et aux techniques de prélèvement et recueil de traces numériques. Il s'agit d'une première approche permettant d'appréhender la notion de preuve numérique, dans un environnement litigieux ou criminel. À la fin du cours, l'étudiant sera capable de discerner les éléments à sauvegarder afin de constituer une preuve devant une juridiction civile ou pénale et produire un rapport d'investigation technique.

Objectifs disciplinaires – Compétences professionnelles

- Déterminer les éléments numériques à rechercher
- Extraire et sauvegarder de façon inforensique les éléments de preuve
- Rédiger un rapport d'analyse technique

Objectifs méthodologiques – Compétences méthodologiques

- Avoir une vision globale de l'informatique légale
- Avoir une vision précise du prélèvement de traces numériques

Objectifs liés au savoir intégré

- Confronter sa pratique de l'informatique aux impératifs légaux

Plan de cours (Contenu détaillé du cours)

1. Prélèvement par copie image de disques ou clés USB
2. Carving et analyse d'emails
3. Carving et analyse de documents de toutes sortes
4. Rédaction de rapports d'investigation technique

Méthodes pédagogiques

Théorie 30%, pratique 70%.

Le cours est fortement axé sur le travail sur cas pratiques.

L'étudiant est mis en situation pour appliquer immédiatement les concepts exposés, afin de les intégrer de manière durable.

L'étudiant sera formé pour utiliser des outils professionnels fonctionnant sur des systèmes Linux et Windows. La révision du cours précédent est nécessaire avant chaque nouvelle session.

Mode d'évaluation

Résolution de trois cas pratiques et production d'un rapport d'investigation technique. Chaque cas est noté pour 1/3 de la note finale.