ENSEIRB-MATMECA

Investigation numérique et Enquête judiciaire cyber

École / Prépa
ENSEIRB-MATMECA

Niveau d'étude
Bac + 5

Présentation

Code interne : EIN9-SECU1

Description

Ce module s'intéresse à l'investigation numérique et l'enquête judiciaire cyber. Il couvre le cycle de vie complet d'une procédure d'investigation, depuis la préservation des logs à l'enquête judiciaire.

Objectifs

- Comprendre les enjeux et les contraintes d'une analyse forensic.
- Comprendre l'importance de l'aspect légal et des procédures de forensic.
- Découvrir des techniques de base d'analyse forensic sur la collecte de données puis l'analyse. (Exemple récupération de log d'un
- serveur PHP et suivre les traces d'une attaque simple)
- Comprendre les contraintes liés à l'investigation numérique
- Manipulation des outils et type d'acquisition de données
- Exploitation des formats de fichiers
- Manipulation des outils pour analyser la mémoire RAM
- comprendre les concepts sous-jacents et outils pour l'analyse de systèmes d'exploitation Linux et Windows
- Mise en place d'approche d'une analyse à grande échelle
- comprendre l'état actualisé de la menace cybercriminelle
- présentation institutionnelle des différents services d'enquête français et de l'organisation de la Justice
- présentation des principales infractions pénales en lien avec la cybercriminalité
- présentation des principes de la coopération policière et judiciaire internationale
- présentation des principales typologies d'enquête et des besoins en matière de préservation des preuves numériques

Heures d'enseignement

CI	Cours Intégrés	32h

Pré-requis obligatoires

L'apprenant sera capable de respecter une procédure de forensic déj à établie et de restitue ses actions dans un format compréhensible par une gouvernance d'entreprise.

Syllabus

Introduction au forensic
Aspect légal du forensic (quand agit-on dans une démarche judiciaire, quand agit-on dans une démarche privée, quand l'analyse simple devient une analyse judiciaire, problématique de la destruction de preuve)
Carnet de bord de l'analyse forensic, (Log de connexion, IOC, Chronographe)
Exemple d'une procédure de forensic (Collecte, Analyse, Restitution)

Informations complémentaires

Investigations numériquesEnquête judiciaire cyber
Définition
L'Investigation numérique ou le forensic est une investigation qui permet de rechercher des traces numériques de compromission d'un système d'information. Cela consiste en la collecte d'un ensemble de données brutes qui vont être analysées pour retrouver des traces d'un attaquant informatique.

Modalités de contrôle des connaissances

Évaluation initiale / Session principale

Type d'évaluation	Nature de l'évaluation	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'évaluation	Note éliminatoire de l'évaluation	Remarques
Contrôle Continu Intégral	Contrôle Continu			1		