



# Analyse forensique



Niveau d'étude  
BAC +5



Composante  
Polytech Dijon  
(Ex-ESIREM)

## Présentation

### Description

- Introduction à l'analyse forensique
  - Investigation numérique et rôle de l'enquêteur informatique
  - Méthodologie et règles d'une bonne investigation
- Collecte des informations
  - Notion d'événement de sécurité
  - Hétérogénéité des sources et préservation de l'intégrité des indices
  - Journaux système des équipements (firewalls, routeurs, serveurs).
  - Récupération des données latentes et dans la mémoire vive
- Analyse de logs
  - Syslog
  - Outils d'analyse de logs : Splunk, AWK
  - Visualiser, trier, chercher dans les traces.
  - Splunk pour comprendre les attaques.
- Preuves numériques et édition de rapport
  - Confirmation / infirmation de scénarios
  - Rédaction d'un rapport d'analyse

### Objectifs

A définir

### Heures d'enseignement

CM	Cours Magistral	12,5h
TD	Travaux Dirigés	10,5h
TP	Travaux Pratiques	16h



## Pré-requis obligatoires

- Systèmes d'exploitation
- Réseaux informatiques / Services réseaux
- Introduction à la sécurité

## Modalités de contrôle des connaissances

### Évaluation initiale / Session principale - Épreuves

Type d'évaluation	Nature de l'épreuve	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'épreuve	Note éliminatoire de l'épreuve	Remarques
CC (contrôle continu)	CC : Ecrit et/ou Oral					
CC (contrôle continu)	Evaluation des pratiques techniques					

### Seconde chance / Session de rattrapage - Épreuves

Type d'évaluation	Nature de l'épreuve	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'épreuve	Note éliminatoire de l'épreuve	Remarques
CC (contrôle continu) 2nde chance	Ecrit sur table					
CC (contrôle continu) 2nde chance	Evaluation des pratiques techniques					