



 FORMATION COURTE MICROCERTIFIANTE

# Investigation et analyse d'environnement macOS

## PUBLIC CONCERNÉ

Membres des corps de police et d'autres organismes étatiques liés à la sécurité (armée, services de renseignement, justice, douanes, gardes-frontière, services administratifs communaux, cantonaux et fédéraux)

Membres de services d'investigation, de sécurité informatique, antifraudes, d'audit et de conformité d'entreprises privées ou d'organisations internationales ou non gouvernementales

*Cette formation a été conçue pour des personnes déjà formées aux bases de l'investigation numérique. Si tel n'est pas votre cas, nous vous recommandons de suivre, au préalable, les formations "Investigation numérique : les fondamentaux" puis "Investigation de supports numériques".*

## ORGANISATION

Ecole des sciences criminelles (ESC),  
Faculté de droit, des sciences criminelles  
et d'administration publique (FDCA),  
Université de Lausanne

## ENJEUX

Les ordinateurs et appareils mobiles ont radicalement transformé nos modes de vie, révolutionnant la manière dont nous communiquons, accédons à l'information, nous déplaçons ou nous divertissons. Véritables témoins de nos activités physiques et numériques, ces supports conservent précieusement les traces de celles-ci. Dans ce contexte, les environnements Apple – ordinateurs, téléphones mobiles et tablettes – prennent une place croissante, aussi bien dans la sphère privée que professionnelle.

Cependant, de par ses spécificités techniques, son architecture et ses mécanismes de sécurité intégrés, macOS a un fonctionnement particulier, différent de Windows ou Linux. Cela exige de la part des professionnel-le-s de l'investigation numérique, des compétences spécialisées et la mise en œuvre de processus spécifiques pour collecter, préserver, analyser, évaluer et interpréter les traces numériques utiles aux investigations ou à la résolution de problèmes opérationnels.

## OBJECTIFS

- Acquérir des compétences avancées d'analyse et d'interprétation des données stockées dans les appareils macOS
- Comprendre les principales structures de données utilisées par le système d'exploitation macOS, et être capable d'extraire et analyser les données d'intérêt
- Développer une démarche adéquate de préservation de l'intégrité des données numériques issues d'environnement macOS
- Favoriser la mise en réseau des professionnel-le-s du domaine



La formation est composée de :

- 16 heures d'enseignement en ligne (soit 4 demi-journées) les 25 février, 4, 11 et 25 mars 2026
- 3 jours d'enseignement en présentiel sur le campus UNIL-EPFL (Lausanne) du 18 au 20 mars 2026
- Évaluation en ligne : 22 avril 2026



CHF 2'500.-



Microcertification de 4 crédits ECTS  
Formation reconnue dans le cadre du CAS INAD



Inscription en ligne

Admission sur dossier : voir les conditions d'admission sur la page web de la formation

Délaï d'inscription : 12 décembre 2025

Nombre de places limité

EN SAVOIR PLUS



## PROGRAMME

### Partie 1 : Prise en compte des supports et acquisition des données

Présentation du matériel / Prélèvement d'ordinateurs Apple / Acquisition de données informatiques

### Partie 2 : Examen du support

Systèmes de fichiers / Environnement d'un ordinateur sous macOS

### Partie 3 : Analyse du support

Analyse d'un système macOS / Structures de données (PLIST, SQLite, SEGB...) / Logs / Mécanismes de persistance / Systèmes de protection (SIP, XProtect, Gatekeeper, Quarantine...)

### Partie 4 : Cours en présentiel

Travaux pratiques "prélèvement" / Travaux pratiques "acquisition de données informatiques" / Travaux pratiques "analyse d'un système macOS"

### Partie 5 : Présentation des résultats

Timeline / Rapport et interprétation

### Évaluation finale

Rédaction d'un rapport et présentation orale d'un cas pratique d'analyse d'un ordinateur sous macOS

## OBTENIR UN CERTIFICATE OF ADVANCED STUDIES ?

L'ESC propose une offre étendue de formations microcertifiantes dans le domaine de l'investigation numérique et l'analyse de données (INAD). Le suivi de plusieurs de ces formations peut mener à l'obtention d'un *Certificate of Advanced Studies* (CAS) en **Investigation Numérique et Analyse de Données (INAD)**.

La formation "**Investigation numérique : les fondamentaux**" est recommandée avant de suivre les autres programmes délivrés dans le cadre du CAS INAD. Sa réussite est obligatoire pour l'obtention du CAS.

Plus d'infos : [www.formation-continue-unil-epfl.ch/formation/cas-inad/](http://www.formation-continue-unil-epfl.ch/formation/cas-inad/)

## RESPONSABLES DE LA FORMATION

- **Johann Polewczyk**, coordinateur du programme, ESC, FDCA, UNIL
- **Prof. Thomas Souvignet**, responsable académique, ESC, FDCA, UNIL

## COMITÉ DIRECTEUR

- **Prof. Thomas Souvignet**, responsable académique, ESC, FDCA, UNIL
- **Prof. Quentin Rossy**, responsable académique, ESC, FDCA, UNIL
- **Johann Polewczyk**, coordinateur du programme, ESC, FDCA, UNIL
- **Martina Reif**, ESC, FDCA, UNIL
- **Prof. Olivier Glassey**, pôle gouvernance numérique, FDCA, UNIL
- **Prof. Sylvain Pasini**, Institute for Information and Communication Technologies, HEIG-VD
- **Dr Julien Cartier**, Police cantonale vaudoise
- **Dr Simon Baechler**, Police neuchâteloise