# *Smartphone Forensics*

*Cours Pratique de 4 jours - 28h*
*Réf : FOB - Prix 2024 : 2 790CHF HT*

Cette formation vous permettra d'acquérir les connaissances pour réaliser des analyses Forensics sur différents systèmes mobiles (iOS, Android).

### OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Apprendre à utiliser les outils et la méthodologie d'investigation forensic sur téléphone à un niveau basique

Analyser les attaques sur les systèmes mobiles.

Rédiger un rapport d'investigation forensic

### TRAVAUX PRATIQUES

Formation alternant théorie et pratique. Tout ce qui est appris sera expérimenté.

## LE PROGRAMME

dernière mise à jour : 05/2022

### 1) L'analyse forensic d'un système mobile

- Informatique judiciaire.
- Les types de crimes informatiques sur les systèmes mobiles.
- Rôle de l'enquêteur informatique.

### 2) La cybercriminalité moderne

- Types de criminalité.
- Cadre de gestion d'un incident de sécurité, CERT.
- Mise en place des labs : outils pour investigation iOS.
- Analyser et comprendre les attaques sur les systèmes mobiles.
- Outils de protection, législation française.

*Travaux pratiques : Analyse réseaux d'attaques DDOS, d'infection et de traffic BotNet.*

### 3) La preuve numérique

- Définition, rôle, types et règles de classement.
- Evaluer et sécuriser les éléments électroniques d'une scène de crime.
- Collecter et préserver l'intégrité des preuves.

*Travaux pratiques : Duplication bit à bit, intégrité, récupération de fichiers et analyse des données.*

### 4) Bases de forensic des systèmes mobiles.

- Comprendre l'architecture des systèmes mobiles et cartes SIM.
- Techniques de forensic mobiles.
- Processus forensic mobiles.

*Travaux pratiques : Analyse des applications et malwares sous mobile. Investigation forensic avec la distribution Santoku.*

### 5) Collecte et analyse de données des systèmes mobiles

- Collecte des données volatiles et non volatiles.
- Fonctionnement du système d'identification.
- Analyse des données.

### PARTICIPANTS

Personnes souhaitant se lancer dans l'inforensique mobile. Administrateurs système. Experts de justice en informatique.

### PRÉREQUIS

Avoir de solides bases en sécurité des systèmes d'information.

### COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

### MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

### MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

### MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

### ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Analyse du cache, cookie, historique navigation, événements.
- Acquisition, analyse et réponse.
- Processus de démarrage.

*Travaux pratiques : Collecter, analyser la mémoire vive. Vérifier l'intégrité des fichiers. Explorer les données du navigateur, du registre.*

### 6) Les bases de l'analyse forensic des systèmes Android

- Analyse et reverse engineering applicatifs.
- Etude des architectures : Kernel, Android Runtime, Librairies.
- Etude de la sécurité des systèmes.
- Bypasser les techniques de verrouillage.
- Obtention des droits root.

*Travaux pratiques : Investigation d'une image capturée d'un système Android : Bypass chiffrements, analyse des données images.*

### 7) Les bases de l'analyse forensic des systèmes iOS

- La structure matérielle des systèmes Apple.
- Système de fichiers.
- Architecture et sécurité.
- Collecte des données depuis une image et depuis un système iCloud.
- Exploitation d'outils tels que Elcomsoft iOS ou Oxygen Forensic Detective.

*Travaux pratiques : Mettre en oeuvre une investigation d'une image iOS.*

### 8) Rapports d'investigation forensic

- Comprendre l'importance des rapports.
- Méthodologies de rédaction et templates.

## LES DATES

CLASSE À DISTANCE
2024 : 24 sept.