

# COMPUTER HACKING FORENSIC INVESTIGATOR V10

La certification de l'investigation numérique - « Accredited Training Center » by EC-Council

Code : CHFIV10

Les nouvelles technologies sont en train de changer le monde professionnel. Les entreprises s'accommodant rapidement aux technologies numériques comme le cloud, le mobile, le big data ou encore l'IoT, rendent l'étude du forensique numérique dorénavant nécessaire.

Le cours CHFIV10 a été développé pour des professionnels en charge de la collecte de preuves numériques après un cyber crime. Il a été conçu par des experts sur le sujet et des professionnels du secteur, il présente les normes mondiales en matière de bonnes pratiques forensiques. En somme, il vise également à élever le niveau de connaissances, de compréhension et de compétences en cybersécurité des acteurs du forensique.

Le programme CHFIV10 offre une approche méthodologique détaillée du forensique et de l'analyse de preuves numériques. Il apporte les compétences nécessaires à l'identification de traces laissées par un intrus mais également à la collecte de preuves nécessaires à sa poursuite judiciaire. Les outils et savoirs majeurs utilisés par les professionnels du secteur sont couverts dans ce programme. La certification renforcera le niveau de connaissances de toutes les personnes concernées par l'intégrité d'un réseau et par l'investigation numérique.

## PROGRAMME

**Méthodes mobilisées :** Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

**Modalités d'évaluation :** Les objectifs sont régulièrement évalués tout au long de la formation (20% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur, ainsi que par le passage de la certification.

### Modules enseignés

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Understanding hard disks and file systems
4. Data acquisition and duplication
5. Defending anti-forensics techniques
6. Operating system forensics
7. Network forensics
8. Investigating web attacks
9. Database forensics
10. Cloud forensics
11. Malware forensics
12. Investigating email crimes
13. Mobile forensics
14. Forensic report writing and presentation

Pour passer l'examen à distance, vous devrez alors disposer d'un PC, d'une webcam et d'une bonne connexion à internet.

- **Titre de l'examen :** CHFI
  - **Format de l'examen :** QCM
  - **Nombre de questions :** 150
  - **Durée :** 4 heures
  - **Langue :** anglais
  - **Score requis :** il se situe entre 70% et 78%, selon la difficulté du set de questions proposées.
- En conséquence, si le stagiaire a des « questions faciles », il devra au minimum avoir 78% tandis que celui qui tombe sur les « questions difficiles » sera reçu avec un score de 70%.

### CERTIFICATION

#### Passage de l'examen

L'examen CHFIV10 (312-49) aura lieu à distance dans le lieu de votre choix.

### RÉSULTAT

Directement disponible en fin d'examen.

#### Maintien de la certification

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année.

Pour plus d'informations, vous pouvez consulter le site d'EC-Council.



**PROCHAINES DATES**

20 février, 2023,  
3 avril 2023,  
26 juin 2023,  
18 septembre 2023,  
16 octobre 2023,  
13 novembre 2023



**OBJECTIFS** .....

- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires
- Se préparer à l'examen CHF1



**INFORMATIONS GÉNÉRALES** .....

**Code :** CHF1v10

**Durée :** 5 jours

**Prix :** 4 050 € HT

**Horaires :** 9h30 - 17h30

**Lieu :** Levallois (92)

**Examen CHF1 :** inclus. Valable 12 mois pour un passage de l'examen à distance.



**PUBLIC VISÉ** .....

- Toutes les personnes intéressées par le cyber forensique, avocats, consultants juridiques, forces de l'ordre, officiers de police, agents fédéraux et gouvernementaux, personnes en charge de la défense, militaires, détectives et enquêteurs, membres des équipes de réponse après incident, managers IT, défenseurs réseaux, professionnels IT, ingénieurs système/ réseau, analystes/consultants/auditeurs sécurité...



**PRÉ-REQUIS** .....

- Avoir des connaissances basiques en cybersécurité forensique et gestion d'incident
- L'obtention préalable de la certification CEH est un plus



**RESSOURCES** .....

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement Windows de démonstration et de mise en pratique



**FORMATIONS ASSOCIÉES** .....

- RILM : Rétro-Ingénierie de Logiciels Malveillants
- MDIE : Malwares : Détection, Identification et Éradication v2