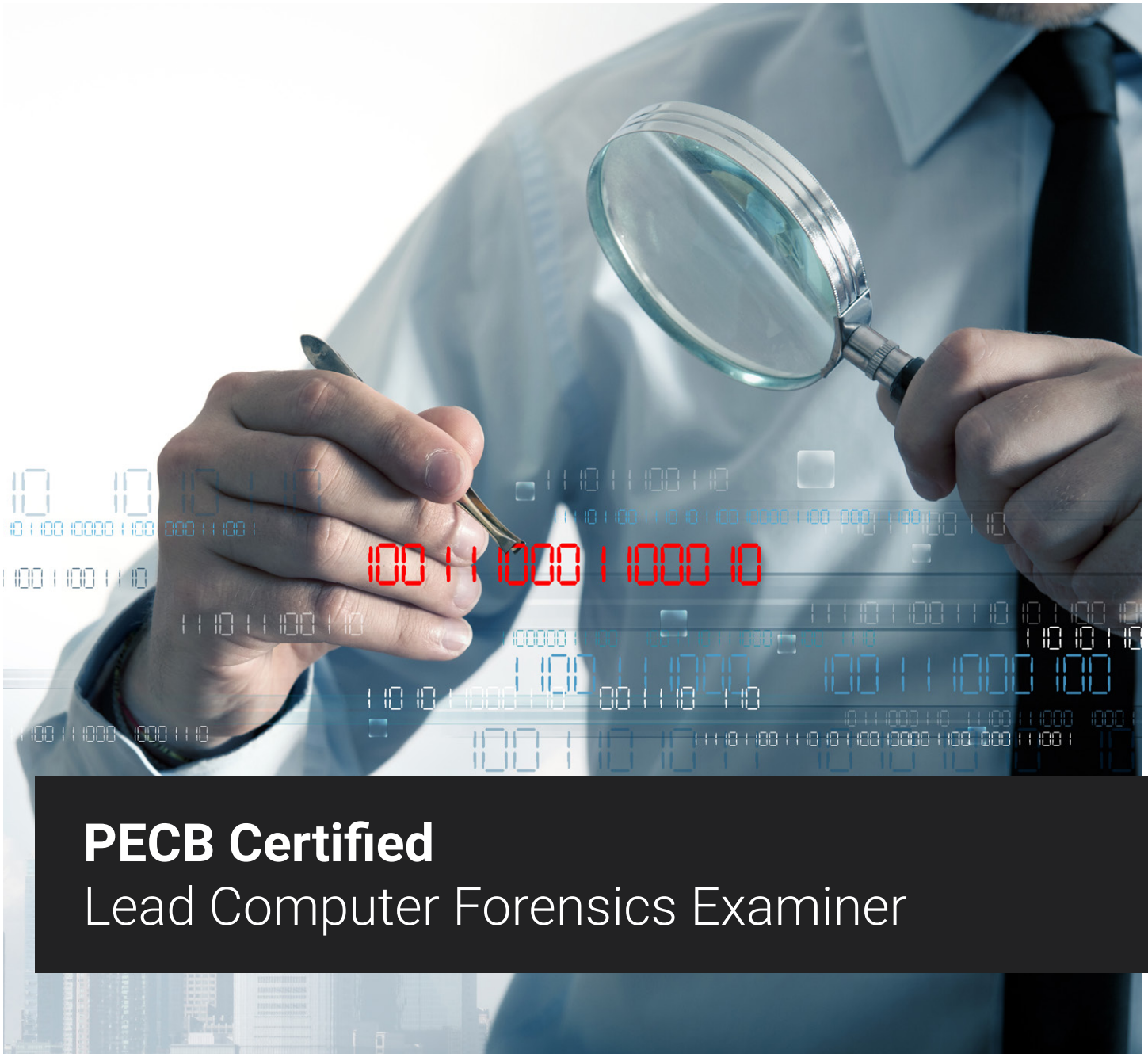
PECB BEYOND RECOGNITION



PECB Certified
Lead Computer Forensics Examiner

Maîtrisez les processus d'investigation judiciaire

Pourquoi devriez-vous y participer ?

La formation Lead Computer Forensics Examiner vous permettra d'acquérir l'expertise nécessaire pour exécuter les processus relatifs à l'investigation judicaire afin d'obtenir des preuves numériques complètes et fiables. Durant de cette formation, vous obtiendrez également une compréhension approfondie des fondamentaux de l'informatique légale, basée sur les bonnes pratiques utilisées pour mettre en œuvre le processus de récupération des preuves forensiques et des techniques analytiques. Cette formation se concentre sur les compétences de base nécessaires pour recueillir et analyser les données de Windows, Mac OS X, système informatique Linux ainsi que des appareils mobiles.

Après avoir maîtrisé l'ensemble des concepts relatifs aux processus d'investigation légale informatique, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified Lead Computer Forensics Examiner ». En étant titulaire d'une certification PECB Lead Computer Forensics Examiner, vous démontrerez que vous disposez de l'expertise nécessaire pour diriger des enquêtes judiciaires avancées et réaliser des analyses judiciaires, des rapports et l'acquisition des preuves.

À qui s'adresse la formation ?

- Spécialistes en informatique judiciaire
- Consultants en informatique judiciaire
- Professionnels de cybersécurité
- Analystes de Cyber intelligence
- Analystes de données électroniques
- Spécialistes en récupération des preuves informatiques
- Professionnels qui travaillent ou qui s'intéressent à l'application de la loi
- Professionnels souhaitant approfondir leurs connaissances en analyse des investigations informatiques
- Membres de l'équipe chargée de la sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Personnes responsables de l'examen des médias pour en extraire et divulguer des données
- Spécialistes des TI

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique

- Explorer l'ISO 27037
- Principes scientifiques et juridiques relatifs à l'informatique judicaire
- Principes fondamentaux de la réponse aux incidents et des opérations judiciaires informatiques
- Exploration des meilleures pratiques mentionnées dans diverses lignes directrices du DoJ et des lignes directrices NIST
- Exigences relatives au laboratoire d'investigation informatique

Jour 2 | Préparer et diriger une enquête informatique judiciaire

- Enquête sur la criminalité informatique et l'enquête numérique
- Systèmes d'exploitation et systèmes de fichiers communs
- Appareils mobiles
- Maintien de la chaîne des preuves
- Politiques et procédures pour maintenir la chaîne des preuves

Jour 3 | Analyse et gestion des artefacts numériques

- Introduction aux outils libres et aux outils commerciaux
- Identifier, acquérir, analyser et communiquer des artefacts numériques
- Utilisation d'outils d'investigation informatique et d'outils libres
- Simulation d'incident

Jour 4 | Présentation du cas et jeux de simulation

- Les menaces émergentes
- Présenter des résultats numériques judiciaires
- Présenter les preuves devant une cour de justice

Jour 5 | Examen de certification

Objectifs de la formation

- Comprendre les rôles et les responsabilités d'un Lead Computer Forensics Examiner au cours de l'enquête judiciaire informatique
- Comprendre le but de l'examen des médias électroniques et sa relation avec les normes et méthodologies communes
- Comprendre la séquence correcte des étapes d'une enquête sur un incident informatique et d'une opération d'investigation légale numérique
- Comprendre les outils communs et les outils libres qui peuvent être utilisés lors d'une enquête d'incident et d'une opération judiciaire numérique
- Acquérir les compétences nécessaires pour planifier et exécuter une opération informatique judiciaire, mettre en œuvre et maintenir un réseau de sécurité pour protéger les preuves

Examen

Durée : 3 heures

L'examen « PECB Certified Lead Computer Forensics Examiner » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

Domaine 1 | Principes et concepts fondamentaux de l'investigation informatique

Domaine 2 | Meilleures pratiques en investigation informatique

Domaine 3 | Exigences relatives au laboratoire légal numérique

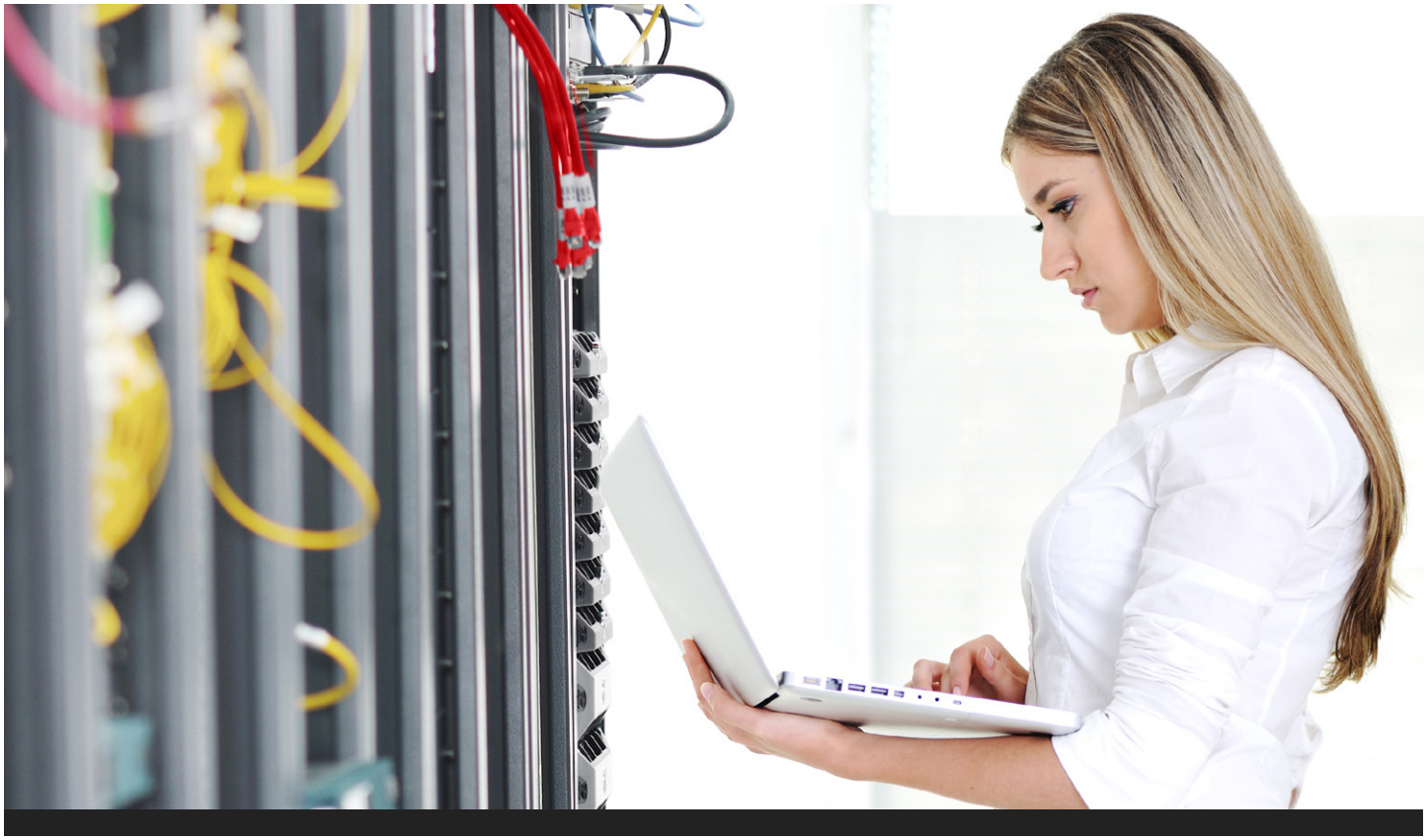
Domaine 4 | Système d'exploitation et structure de système de fichiers

Domaine 5 | Appareils mobiles

Domaine 6 | Enquête sur la criminalité informatique et examen forensique

Domaine 7 | Maintien de la chaîne des preuves

Pour de plus amples informations concernant l'examen, veuillez consulter Politiques et règlement relatifs à l'examen



Certification

Après avoir réussi l'examen, vous pouvez demander l'une des qualifications mentionnées sur le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la qualification sélectionnée.

Pour de plus amples informations concernant les certifications Computer Forensics et le processus de certification PECB, veuillez cliquer sur Politiques et règlement de certification

Qualification	Examen	Expérience professionnelle	Expérience relative à l'investigation légale informatique	Autres exigences
PECB Certified Provisional Computer Forensics Examiner	Examen PECB Certified Lead Computer Forensics ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified Computer Forensics Examiner	Examen PECB Certified Lead Computer Forensics ou équivalent	**Deux années :** Une année d'expérience dans le domaine de l'informatique judiciaire	Activités totalisant 200 heures	Signer le Code de déontologie de PECB
PECB Certified Computer Lead Forensics Examiner	Examen PECB Certified Lead Computer Forensics ou équivalent	**Cinq années :** Deux années d'expérience dans le domaine de l'informatique judiciaire	Activités totalisant 300 heures	Signer le Code de déontologie de PECB

Informations générales

- Les frais de certification sont inclus dans le prix de l'examen
- Un manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques est fourni
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires