

Formation « Analyse inforensique Windows »

Réf : FORENSIC1

Les raisons ne manquent pas de vouloir effectuer une analyse inforensique :

- Collaborateur indélicat ayant volé des documents interne de valeur
- Intrusion d'un poste suite à une erreur d'un utilisateur
- Compromission d'un serveur

Quelle que soit la raison, FORENSIC 1 vous apprendra à analyser les différents artefacts inforensiques et finalement créer une frise chronologique de l'incident.

Objectifs

- Gérer une investigation numérique sur un ordinateur Windows
- Avoir les bases de l'analyse numérique sur un serveur Web
- Acquérir les médias contenant l'information
- Trier les informations pertinentes et les analyser
- Utiliser les logiciels d'investigation numérique
- Maîtriser le processus de réponse à incident

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Personnes souhaitant apprendre à réaliser des investigations numériques
- Personnes souhaitant se lancer dans l'inforensique
- Administrateurs système Windows
- Experts de justice en informatique

Pré-requis

- Formation SECUCYBER
- (ou) Solides bases en sécurité des systèmes d'information

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

Supports

- En présentiel : Support de cours au format papier en français – En distanciel : support de cours au format numérique après signature du règlement intérieur
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Kit d'investigation numérique
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration
- Evaluation de pré-formation envoyé avant le début de la formation
- Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques
- Examen final à la fin de la formation (cf certification)

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC1 par HS2.

Programme

Jour 1

- Présentation de l'inforensique
- Périmètre de l'investigation
- Trousse à outil
- Méthodologie "First Responder"
- Analyse Post-mortem
- Disques durs
- Introduction aux systèmes de fichiers
- Horodatages des fichiers
- Acquisition des données : Persistante et volatile
- Gestion des supports chiffrés
- Recherche de données supprimées
- Sauvegardes et Volume Shadow Copies
- Aléas du stockage flash
- Registres Windows
- Les structures de registres Windows
 - Utilisateurs
 - Systèmes
- Événements / antivirus / autres logiciels

Jour 2 - Scénario d'investigation

- Téléchargement/Accès à des contenus confidentiels
- Exécution de programmes
- Traces de manipulation de fichiers et de dossiers
- Fichiers supprimés et espace non alloué
- Carving
- Géolocalisation
- Photographies (données Exifs)
- Points d'accès WiFi
- Exfiltration d'informations
- Périphérique USB

- Courriels
- Journaux SMTP
 - Analyse client messagerie
- Utilisateurs abusés par des logiciels malveillants

Jour 3 - Interaction sur Internet

- Utilisation des Navigateurs Internet
- IE/Edge / Firefox
- Traces sur les AD Windows
- Présentation des principaux artefacts
- Bases de l'analyse de la RAM
 - Conversion des hyperfiles.sys
 - Extraction des clés de chiffrement

Jour 4 - Inforensique Linux

- Les bases de l'inforensique sur un poste de travail Linux"
- Les bases de l'inforensique sur un serveur Linux
 - Journaux serveurs Web & Corrélations avec le système de gestion de fichiers
- Création et analyse d'une frise chronologique du système de fichier

Jour 5 - Vue d'ensemble

- Création et analyse d'une frise chronologique enrichie d'artefacts
- Exemple d'outil d'interrogation de gros volume de données
- Examen de certification HS2 (QCM sur ordinateur)