

QUIZ FORENSIQUE

30 QCM - VERSION

Évaluation des connaissances - Forensique numérique, DFIR, SIEM et

Nom /	BOICHÉ Gauvain _____
Dat	07 / 08 / 2026
Durée conseillée	45 minutes
Barèm	30 points - 1 point par question

CONSIGNES

Pour chaque question, cochez une seule réponse. Aucune pénalité en cas de mauvaise réponse. Les questions portent sur la forensique disque et mémoire, la réponse à incident, les SIEM, les artefacts Windows et les outils DFIR utilisés dans les Labs 2026.

Bonne

1

MÉTHODOLOGIE

Quelle est la première étape d'une investigation forensique correctement préparée ?

- ☐ A. Analyse
- ☐ B. Collecte
- ☒ C. Préparation
- ☐ D. Présentation

2

MÉMOIRE

Quel outil est principalement utilisé pour l'analyse d'une image mémoire vive ?

- ☐ A. Autopsy
- ☐ B. The Sleuth Kit
- ☒ C. Volatility
- ☐ D. Wazuh

3

PREUVE

Qu'est-ce que la chaîne de conservation (chain of custody) ?

- ☐ A. Une méthode d'analyse des journaux
- ☐ B. Un mécanisme de compression des images
- ☒ C. Une traçabilité documentée des personnes, actions et transferts concernant une preuve
- ☐ D. Une base de données SIEM

4

INCIDENT

En 2026, quelle publication NIST constitue la référence actualisée pour les recommandations de réponse aux incidents ?

- ☐ A. NIST SP 800-53 Rev. 4
- ☒ B. NIST SP 800-61 Rev. 3 <https://csrc.nist.gov/pubs/sp/800/61/r3/final>
- ☐ C. NIST SP 800-171 Rev. 1
- ☐ D. NIST SP 800-30 Rev. 1

5

DISQUE

Quelle commande de The Sleuth Kit affiche typiquement la structure des partitions d'une image disque ?

- ☐ A. fls
- ☒ B. mmls
- ☐ C. icat
- ☐ D. fsstat

6

DISQUE

Que permet principalement Autopsy ?

- ☐ A. Uniquement l'analyse mémoire
- ☒ B. L'analyse forensique de supports et systèmes de fichiers via une interface graphique
- ☐ C. Le monitoring temps réel d'un SOC
- ☐ D. La capture de paquets réseau

7

SOC

Que signifie l'acronyme SIEM ?

- ☒ A. Security Information and Event Management
- ☐ B. Secure Internet Exchange Mechanism
- ☐ C. System Integrity Event Mapper
- ☐ D. Security Incident Encryption Module

8

INCIDENT

Avec NIST SP 800-61 Rev. 3, la réponse aux incidents est principalement intégrée à :

- ☐ A. Un cycle isolé en quatre phases uniquement
- ☒ B. NIST Cybersecurity Framework (CSF) 2.0
- ☐ C. ISO 9001
- ☐ D. PCI DSS uniquement

9

MÉMOIRE

Le plugin windows.pslist de Volatility 3 permet notamment :

- ☒ A. De lister les processus présents dans l'image mémoire
- ☐ B. De créer une image E01
- ☐ C. De parser une base SQLite Android
- ☐ D. De déployer un agent Wazuh

10

PREUVE

Un artefact forensique est :

- ☐ A. Un outil d'attaque
- ☒ B. Une trace numérique pouvant contribuer à une investigation
- ☐ C. Un malware obligatoirement actif
- ☐ D. Uniquement un fichier texte

11

NORMES

Quelle norme fournit des lignes directrices pour l'identification, la collecte, l'acquisition et la préservation des preuves numériques ?

- ☐ A. ISO/IEC 27001
- ☐ B. ISO/IEC 27017
- ☒ C. ISO/IEC 27037
- ☐ D. ISO 9001

12

PREUVE

À quoi sert principalement une empreinte SHA-256 dans une investigation ?

- ☐ A. À chiffrer un disque
- ☒ B. À vérifier l'intégrité d'un fichier ou d'une image
- ☐ C. À monter un volume
- ☐ D. À retrouver un mot de passe

13

MÉMOIRE

Dans Volatility, quelle vue aide à comprendre les relations parent/enfant entre processus ?

- ☒ A. pstree
- ☐ B. strings
- ☐ C. filescan
- ☐ D. hashdeep

14

SOC

Splunk est principalement utilisé pour :

- ☒ A. Indexer, rechercher et analyser des journaux et événements
- ☐ B. Chiffrer un poste Windows
- ☐ C. Créer des images E01
- ☐ D. Analyser uniquement la mémoire RAM

15

MÉTHODOLOGIE

Après la collecte et la préservation, quelle activité est centrale dans une investigation forensique ?

- ☒ A. L'analyse des données et artefacts
- ☐ B. La suppression des originaux
- ☐ C. La désactivation de la journalisation
- ☐ D. La modification des horodatages

16

TIMELINE

L'outil log2timeline.py fait partie de :

- ☐ A. Autopsy
- ☒ B. Plaso
- ☐ C. Wazuh
- ☐ D. Volatility

17

SOC

Dans Elastic Security, quelle interface est utilisée pour explorer et visualiser les événements ?

- ☒ A. Kibana
- ☐ B. Wireshark
- ☐ C. Autopsy
- ☐ D. FTK Imager

18

ACQUISITION

Le terme live acquisition désigne :

- ☒ A. Une collecte effectuée sur un système encore en fonctionnement
- ☐ B. Une analyse effectuée uniquement après extinction
- ☐ C. Le clonage d'un DVD
- ☐ D. La suppression de la mémoire volatile

19

WINDOWS

Quel outil d'Eric Zimmerman est spécialisé dans l'analyse des fichiers Prefetch Windows ?

- ☐ A. Timeline Explorer
- ☒ B. PECmd <https://ericzimmerman.github.io/#forensic-tools>
- ☐ C. MFTECmd
- ☐ D. Registry Explorer

20

INCIDENT

Une gestion d'incident mature doit notamment :

- ☐ A. Se limiter à la détection
- ☒ B. Intégrer préparation, détection, réponse, récupération et amélioration continue
- ☐ C. Éviter toute documentation
- ☐ D. Supprimer les journaux après analyse

21

WINDOWS

Le fichier pagefile.sys peut contenir :

- ☒ A. Des fragments de données précédemment présentes en mémoire
- ☐ B. Uniquement les mises à jour Windows
- ☐ C. Uniquement les clés de registre
- ☐ D. Aucune donnée utile en forensics

22

OUTILS

La commande strings sert principalement à :

<https://man7.org/linux/man-pages/man1/strings.1.html>

- ☒ A. Extraire des chaînes lisibles depuis des fichiers ou données binaires
- ☐ B. Monter une partition NTFS
- ☐ C. Calculer automatiquement une timeline
- ☐ D. Créer un hash uniquement

23

ACQUISITION

Quelle extension est couramment utilisée pour une image disque RAW produite avec dd ?

- ☒ A. .img
- ☐ B. .evtx
- ☐ C. .pcapng
- ☐ D. .vmdk uniquement

24

DÉTECTION

Un honeypot est principalement utilisé pour :

- ☒ A. Attirer et observer une activité hostile dans un environnement contrôlé
- ☐ B. Accélérer un antivirus
- ☐ C. Chiffrer un réseau
- ☐ D. Remplacer les sauvegardes

25

IOC

Que signifie IOC en cybersécurité ?

- ☒ A. Indicator of Compromise
- ☐ B. Input Output Channel
- ☐ C. Internal Operating Code
- ☐ D. Incident Output Certificate

26

PREUVE

Que fait hashdeep ?

- ☒ A. Calcule et compare des empreintes de fichiers, notamment à grande échelle
- ☐ B. Monte une image E01
- ☐ C. Parse des journaux EVT×
- ☐ D. Capture des paquets réseau

27

ACQUISITION

FTK Imager est notamment utilisé pour :

- ☒ A. Acquérir et visualiser des supports ou images forensiques
- ☐ B. Déployer Elasticsearch
- ☐ C. Déboguer un malware en mémoire
- ☐ D. Gérer un agent Wazuh

28

WINDOWS

Qu'est-ce qu'un fichier .evtx ?

- ☒ A. Un journal d'événements Windows
- ☐ B. Une image disque E01
- ☐ C. Une base SQLite Android
- ☐ D. Un fichier PCAP

29

SOC

Dans une architecture Wazuh actuelle, quel composant fournit l'interface web native de visualisation et d'investigation ?

- ☐ A. Kibana obligatoire
- ☒ B. Wazuh Dashboard
- ☐ C. FTK Imager
- ☐ D. Volatility Workbench

30

MÉTHODOLOGIE

La documentation forensique doit être :

- ☒ A. Maintenue tout au long de l'investigation
- ☐ B. Réalisée uniquement à la fin
- ☐ C. Optionnelle
- ☐ D. Réservée aux autorités judiciaires