Ecole Nationale Supérieure Polytechnique
Département de Génie Informatique
Humanité Numérique Niveau 4

EPREUVE D'INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUE

Enseignant : Thierry MINKA, Sr-Eng., GRC Expert.
Durée : 3h

Le sujet est constitué de 2 grandes parties. A : des questions ouvertes couvrant l'essentiel du programme de cours et B : une discussion scientifique au choix sur les grands enjeux de l'investigation numérique.

A. Questions ouvertes (80 points)

NB : Chaque question vaut 10 points, gardez ça à l'esprit lorsque vous penserez avoir fourni une réponse complète.

1. Define the term *chain of custody* in the context of digital evidence. Why is it critical in computer forensics?
2. What are the key challenges of network forensics in identifying and tracking cybercriminals? Suggest two solutions for overcoming these challenges.
3. Describe three types of evidence collected during a forensic investigation and their importance.
4. During live evidence acquisition, what are the key volatile data components that must be captured first? Provide an example for each.
5. A company suspects an employee of sending sensitive data via email. Outline the steps for conducting an email investigation, including key tools used.
6. Expliquez l'importance du journal des activités (*log*) dans une enquête numérique. Comment ces journaux peuvent-ils être manipulés par des attaquants, et comment s'en prémunir ?
7. Dans une enquête sur un crime numérique, décrivez comment utiliser un logiciel d'imagerie bit-à-bit pour préserver l'état d'un disque dur suspect.
8. Un fichier supprimé a été récupéré sur un système suspect. Expliquez comment vous valideriez son authenticité en utilisant des outils standards de forensique.

B. Discussion (20 points)

Choisir et traiter, en 600 mots maximum, un des 3 sujets suivants sous forme de discussion scientifique, telle que vue en classe.

Sujet 1 : Impact de l'intelligence artificielle et des deepfakes sur l'investigation numérique : défis et solutions ;
Sujet 2 : Technologies quantiques : opportunités et menaces pour le chiffrement et l'investigation numérique ;
Sujet 3 : Investigation numérique en Afrique et au Cameroun : défis liés aux infrastructures et au cadre juridique.

« *Like a conscientious and methodical craftsman, every day, refine your practice. Only in this way will you be and remain an Expert.* »

Thierry MINKA.