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

EPREUVE D'INVESTIGATION NUMERIQUE AVANCEE
SESSION NORMALE MAI 2025

Enseignant : **MINKA Thierry**
Durée : 3h
Présentation : 2 points.

PARTIE 1: Questions de compréhension des concepts et procédures (45 points)

1. Concepts de base de l'investigation numérique (10 pts)

Q1.1. Définissez les concepts suivants (1 pt chacun) :

- Preuve numérique
- Chaîne de possession (chain of custody)
- Image forensique
- Intégrité des données
- Volatilité des preuves

Q1.2. Expliquez les différences entre une analyse de logs, une recherche de fichiers supprimés, et une analyse de mémoire vive. (5 pts)

2. Procédure complète d'investigation numérique judiciaire (10 pts)

Q2.1. Citez et décrivez succinctement chacune des grandes étapes d'une procédure d'investigation numérique judiciaire, de la saisine à la déposition devant le tribunal. (6 pts)
Q2.2. Quelle est la place du rapport d'expertise dans ce processus ? Quelles sont ses principales composantes formelles et légales ? (4 pts)

3. Modalités d'accès à la fonction d'expert judiciaire et contraintes (10 pts)

Q3.1. Décrivez les conditions d'accès au statut d'expert judiciaire dans un pays de droit continental (comme le Cameroun ou la France). (4 pts)
Q3.2. Énumérez trois contraintes ou obligations légales spécifiques liées à ce rôle. (3 pts)
Q3.3. Donnez deux cas dans lesquels un expert pourrait voir sa responsabilité engagée. (3 pts)

4. Investigation judiciaire vs. investigation en entreprise (15 pts)

Q4.1. Présentez trois différences clés entre une mission d'investigation numérique commandée par un tribunal et celle menée dans un cadre purement organisationnel. (6 pts)
Q4.2. Dans le cas d'une entreprise, qui est le commanditaire ? Quels sont les risques de conflits d'intérêts ? (5 pts)
Q4.3. Que faire lorsqu'un élément de preuve identifié dans une mission interne pourrait intéresser la justice ? (4 pts)

PARTIE 2: Cas pratique : L'affaire des serveurs fantômes du Gondwana (55 points)

2.1 Contexte:

La République du **Gondwana**, récemment sortie d'une transition numérique controversée, a mis en place un programme baptisé **"Serveurs pour Tous"** visant à doter toutes les régions administratives de mini data centers.

En mars 2025, un audit de l'Autorité de Régulation révèle que plusieurs serveurs installés dans le cadre du projet sont **inaccessibles, introuvables physiquement, ou émettent des signaux suspects vers l'étranger**.

Le président de l'Autorité saisit le parquet numérique, qui ordonne une **expertise judiciaire** pour :

- Vérifier l'existence et l'usage effectif de ces serveurs ;
- Déterminer s'ils ont été manipulés, redirigés, ou utilisés à des fins non autorisées ;
- Documenter les preuves de toute infraction numérique.

Vous êtes **mandaté comme expert judiciaire** dans ce dossier.

2.2 Instructions :

2.2.1 Décrivez les premières mesures techniques et juridiques que vous prenez en tant qu'expert dès réception de l'ordonnance de mission. (10 pts)

2.2.2 Sur la base des données suivantes (fictives à compléter par l'enseignant : ex. adresse IP, logs d'accès, captures de paquets, noms d'hôtes), identifiez les incohérences ou anomalies. (15 pts)

2.2.3 Élaborez une **mini version du rapport d'expertise numérique** (1 page max) comprenant :

- Objet de la mission
- Méthodologie
- Résultats clés
- Recommandations
- Avis de l'expert (20 pts)

2.2.4 En tant qu'expert, que répondriez-vous si l'avocat de la défense vous demande :
a. Pourquoi vous avez travaillé sans assistant certifié ?
b. Sur quelle base vous affirmez que les paquets étaient illégitimes ?
(5 pts)

2.2.5 Quelles précautions devez-vous prendre si vous êtes appelé à la barre pour défendre votre rapport ? (5 pts)

2.3 Annexe au Cas pratique:

2.3.1 Table des serveurs déclarés dans le projet

Fichier : serveurs_officiels.xlsx

N°	ID Serveur	Nom machine	IP assignée	Région	Status Inventaire	Remarques
1	SRV-001	dc-nord.gdw	192.168.100.11	Nord	Présent	OK
2	SRV-002	dc-sud.gdw	192.168.100.12	Sud	Présent	OK
3	SRV-003	dc-est.gdw	192.168.100.21	Est	Présent	Objet de l'investigation
4	SRV-004	dc-ouest.gdw	192.168.100.13	Ouest	Introuvable	Ping KO
5	SRV-005	dc-centre.gdw	192.168.100.14	Centre	Présent	OK

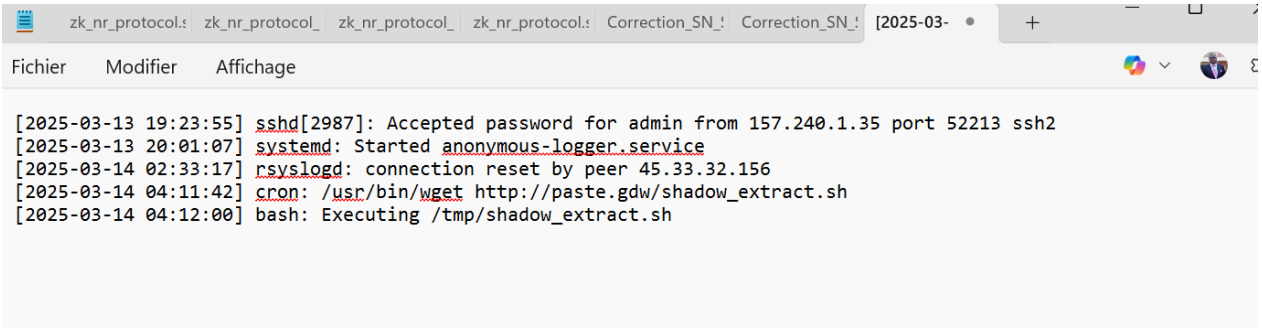
2.3.2 Données réseau (extrait de logs de pare-feu)

Fichier : fw_logs_gondwana.csv

Timestamp	Source IP	Destination IP	Port	Action	Protocol	Remarks
2025-03-14 11:05:33	192.168.100.21	10.10.45.5	22	ALLOW	TCP	SSH vers site régional Est
2025-03-14 11:06:02	192.168.100.21	157.240.1.35	443	ALLOW	TCP	Connexion vers IP extérieure (US)
2025-03-14 11:07:10	192.168.100.21	10.10.45.9	80	DENY	TCP	Refusé – port HTTP
2025-03-14 11:09:55	10.10.45.5	192.168.100.21	22	ALLOW	TCP	Retour SSH
2025-03-14 11:12:41	192.168.100.21	45.33.32.156	443	ALLOW	TCP	Connexion persistante 7h (VPN ?)

2.3.3 Fichier journal système du SRV-003

Fichier : syslog_srv003.log (extraits)



2.3.4 Capture mémoire vive (résumé)

Fichier : memdump_srv003.txt

« Vous n'êtes ni en retard, ni en avance, vous êtes où vous êtes aujourd'hui. La question est, où voulez-vous aller ? Décidez et agissez en conséquence.»

Architecte de l'Ombre