RÉPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
*****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
*****
DÉPARTEMENT DE GÉNIE INFORMATIQUE
*****

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
*****
MINISTRY OF HIGHER EDUCATION
*****
UNIVERSITY OF YAOUNDE I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
COMPUTER ENGINEERING DEPARTMENT
*****

RAPPORT D'INVESTIGATION NUMÉRIQUE JUDICIAIRE

RECONSTITUTION DES ELEMENTS TECHNIQUES DE L'ORDONNANCE DE REVOI N°015/ORD/J.NZIE/TMY DU 29 FEVRIER 2024

Rédigé par
NZOUCK TOUMPE ERIC - OLIVIER
Matricule : ***22P060***

Sous la supervision de
Thierry MINKA, Eng

Année académique 2025/2026

Contents

Introduction

L'investigation numérique judiciaire est aujourd'hui un pilier incontournable de la procédure pénale moderne, particulièrement dans les affaires sensibles impliquant des acteurs étatiques, militaires ou de renseignement. L'ordonnance de renvoi **n°015/ORD/J.NZIE/TMY du 29 février 2024**, signée par le **Colonel-Magistrat NZIE Pierrot Narcisse**, s'inscrit dans ce contexte.

Elle conclut une longue instruction relative à une série de faits graves — enlèvements, séquestrations, actes de torture et atteintes à la liberté individuelle — attribués à des membres présumés des services de renseignement camerounais, dont le *Commissaire Divisionnaire EKO EKO Maxime Léopold*, Directeur général de la DGRE au moment des faits.

Pour qu'une telle ordonnance soit rendue, le magistrat a dû s'appuyer sur un faisceau d'éléments matériels, humains et numériques rigoureusement collectés et authentifiés. Le présent rapport vise à reconstituer, dans une perspective d'ingénierie judiciaire, l'ensemble des analyses, extractions, corrélations et expertises numériques qui ont nécessairement soutenu la décision du juge d'instruction militaire.

L'étude est organisée en quatre grandes parties :

- la première présente le cadre juridique et méthodologique de l'investigation numérique judiciaire ;
- la deuxième identifie les sources et éléments numériques potentiels figurant explicitement ou implicitement dans l'ordonnance ;
- la troisième analyse les mécanismes d'exploitation, de corrélation et de contextualisation des données par l'expert judiciaire ;
- la quatrième propose une évaluation critique et des recommandations techniques pour le renforcement de la chaîne probatoire numérique.

Chapter 1

Cadre juridique et procédural de l'investigation numérique judiciaire

1.1 Fondements légaux de la preuve numérique au Cameroun

Le traitement d'une affaire telle que celle jugée par le **Tribunal Militaire de Yaoundé** repose sur une articulation entre le **Code de Procédure Pénale camerounais**, la **Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité**, et la **Loi n°2010/013 régissant les communications électroniques**.

Ces textes autorisent la saisie, l'analyse, la conservation et la présentation de preuves issues de supports électroniques, à condition que leur intégrité soit garantie et leur traçabilité documentée. L'article 65 du CPP prévoit que toute preuve peut être admise, pourvu qu'elle soit obtenue de manière licite.

Dans un dossier d'une telle portée, impliquant des agents d'État, la preuve numérique devient essentielle pour corroborer ou contredire les témoignages, et pour objectiver la chronologie des faits à travers des artefacts techniques : *logs, métadonnées, géolocalisation, etc.*

1.2 Rôle et mission de l'expert judiciaire numérique

L'expert judiciaire agit comme interface technique entre la donnée et le droit. Son rôle consiste à :

- identifier les sources de données pertinentes ;
- assurer la chaîne de custodie (préservation intégrale et authentifiée des preuves) ;
- effectuer des copies forensiques certifiées conformes (bit à bit) ;
- analyser les supports saisis et établir un rapport technique clair et vérifiable pour le magistrat instructeur.

L'expert doit s'appuyer sur des standards internationaux tels que la norme **ISO/IEC 27037** (identification et préservation des preuves numériques) et la norme **ISO/IEC 27041** (évaluation des processus d'investigation).

1.3 Spécificités procédurales devant le Tribunal Militaire

La compétence du Tribunal Militaire découle du statut des inculpés, tous agents relevant des forces de sécurité. L'enquête a probablement impliqué la coordination entre le magistrat instructeur, la

gendarmerie, la DGRE elle-même, et les opérateurs de télécommunication (MTN, Orange, Camtel), sous mandat judiciaire. Ces institutions ont dû fournir les réquisitions techniques nécessaires à la reconstruction des communications et à la localisation des protagonistes.

Chapter 2

Identification et reconstitution des éléments numériques

2.1 Les communications électroniques des protagonistes

L'ordonnance évoque la coordination d'une opération de filature et de détention illégale menée par plusieurs agents. Pour établir la matérialité de cette coordination, l'expert a dû produire :

- des relevés téléphoniques détaillés (Call Detail Records – CDR) ;
- des analyses de bornage GSM ;
- des traces d'échanges via WhatsApp, Signal ou Telegram, extraites des téléphones saisis.

Ces données ont permis de cartographier les interactions et de reconstituer le réseau de communication entre les inculpés avant, pendant et après les faits.

2.2 Données de géolocalisation et mobilité

L'ordonnance mentionne les lieux de détention et les déplacements suspects. Ces éléments reposent sur :

- les données GPS contenues dans les smartphones ou véhicules de service ;
- les métadonnées EXIF de photos ;
- les données de localisation opérateur (cell ID).

Ces corrélations ont permis d'établir la présence effective de certains inculpés sur les lieux des faits.

2.3 Supports numériques saisis

Les supports saisis incluent téléphones, ordinateurs, clés USB et disques durs externes. La copie forensique de ces supports a été effectuée avec des outils certifiés (*FTK Imager, EnCase, Autopsy*). Chaque image disque a été accompagnée d'un **hash cryptographique (MD5/SHA-256)** garantissant son intégrité probatoire.

2.4 Exploitation des systèmes institutionnels

Des recherches dans les systèmes informatiques de la DGRE ont visé :

- les journaux d'accès ;
- les connexions suspectes ;
- les échanges de courriels internes.

Ces investigations ont permis d'établir si les ordres litigieux venaient de la hiérarchie ou d'initiatives individuelles.

2.5 Analyse OSINT et sources ouvertes

Les informations médiatiques et sur les réseaux sociaux ont été examinées via des techniques **OSINT (Open Source Intelligence)**. L'expert a vérifié l'authenticité, la provenance et la chronologie des contenus, contribuant à renforcer la crédibilité des témoignages.

Chapter 3

Analyse et corrélation des preuves numériques

3.1 Méthodologie d'exploitation

L'expert a suivi une approche structurée :

1. Collecte légale des supports sous mandat judiciaire ;
2. Préservation et duplication sous scellés ;
3. Extraction ciblée des artefacts pertinents ;
4. Corrélation des données ;
5. Rédaction d'un rapport final.

3.2 Corrélations temporelles et spatiales

La reconstitution de la **timeline numérique** a permis d'associer :

- l'heure de capture de la victime ;
- la durée de détention ;
- les communications internes entre agents ;
- la réception et exécution des ordres.

3.3 Détection de falsifications et dissimulations

Les outils forensiques ont permis de détecter :

- des effacements volontaires de messages ;
- des altérations d'horodatage ;
- des suppressions de fichiers.

3.4 Exploitation des métadonnées et documents internes

L'analyse des métadonnées (*date, auteur, terminal utilisé*) a révélé les circuits décisionnels réels. Ces éléments ont aidé le magistrat à distinguer les ordres officiels des initiatives personnelles.

3.5 Synthèse des résultats

Le rapport de l'expert comprenait :

- un inventaire des supports ;
- des visualisations (graphiques, timelines, cartes) ;
- des analyses d'attribution et de corrélation.

Chapter 4

Évaluation critique et recommandations techniques

4.1 Robustesse de la chaîne de custodie

Le succès probatoire repose sur la **traçabilité continue** des preuves numériques. Toute rupture dans cette chaîne peut invalider la validité d'une preuve judiciaire.

4.2 Limites et défis

Les difficultés majeures incluent :

- le manque de laboratoires forensiques agréés ;
- la faible standardisation des procédures ;
- la formation limitée des acteurs judiciaires ;
- l'accès restreint aux données télécoms.

4.3 Recommandations

1. Créer un pôle national de criminalistique numérique ;
2. Former les magistrats et officiers d'enquête à la preuve électronique ;
3. Renforcer la collaboration avec l'ANTIC ;
4. Créer une base de données probatoire protégée par *blockchain* ;
5. Certifier les laboratoires judiciaires selon la norme ISO 27037.

Conclusion

L'ordonnance de renvoi du 29 février 2024 représente l'aboutissement d'un processus d'investigation hybride, mêlant analyse humaine, reconstitution judiciaire et science numérique. L'expert judiciaire, en reconstituant les communications, déplacements et interactions numériques des acteurs, a permis au magistrat de transformer des suspicions en certitudes probatoires.

En définitive, l'affaire **EKO EKO** démontre que la vérité judiciaire du XXI^{e} siècle ne se limite plus à la parole humaine : elle s'écrit désormais dans les logs, les métadonnées et les empreintes numériques laissées par ceux qui croyaient pouvoir les effacer.