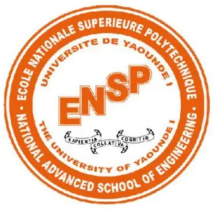

REPUBLIQUE DU CAMEROUN

Paix – Travail – Patrie

****

UNIVERSITE DE YAOUNDE I

****

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

****

DEPARTEMENT DE GENIE

REPUBLIC OF CAMEROON

Peace – Work – Fatherland

****

UNIVERSITY OF YAOUNDE I

****

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE

****

DEPARTMENT OF COMPUTER

Rapport professionnel d'expertise en investigation numérique judiciaire : AFFAIRE MARTINEZ ZOGO — Affaire d'homicide ciblé dans un contexte politico-sécuritaire

---

Expert judiciaire : TAPA LOIC

Tribunal compétent : Tribunal militaire de Yaoundé

Février 2024

Table des matières

Introduction générale

Au cœur des transformations de la criminalité contemporaine, la trace numérique constitue désormais une preuve centrale dans les affaires de grande complexité. Les homicides planifiés, souvent dissimulés derrière des logistiques sophistiquées, laissent aujourd'hui derrière eux un cortège de données électroniques : téléphones, messages, géolocalisations, vidéosurveillance, transactions, etc.

Dans le cadre d'une enquête ouverte à la suite de la découverte du corps sans vie d'un journaliste connu pour ses dénonciations publiques, la justice militaire a ordonné une expertise en investigation numérique judiciaire. L'objectif était d'éclairer les autorités sur :

— les moyens électroniques utilisés pour préparer, suivre et exécuter le crime,

— les réseaux de communication ayant servi à la coordination des acteurs,

— et les éléments probatoires exploitables pour établir la matérialité des faits.

L'expert judiciaire désigné a conduit un travail d'analyse rigoureux, basé sur la méthodologie forensique internationale, afin de produire un rapport complet destiné à appuyer la décision de renvoi devant la juridiction compétente.

Chapitre 1

Cadre juridique et institutionnel

1.1 Cadre légal de l'expertise numérique au Cameroun

L'intervention de l'expert judiciaire en matière d'investigation numérique s'appuie sur un ensemble de textes juridiques :

— **Code de procédure pénale** (articles 256 à 261) : autorise le juge d'instruction à recourir à des experts pour toute question nécessitant des compétences techniques.

— **Loi n°2010/012 du 21 décembre 2010** relative à la cybersécurité et à la cybercriminalité : confère à la preuve numérique la même valeur que la preuve écrite ou matérielle.

— **Loi n°2017/012 du 12 juillet 2017** portant Code de justice militaire : encadre les enquêtes impliquant des personnels militaires ou assimilés.

— **Code pénal camerounais** : articles 74 à 97 sur la complicité, et 276 à 277 sur l'homicide et la torture.

1.2 Mission de l'expert judiciaire

L'expert en investigation numérique a pour mandat :

— Identifier les supports numériques pertinents

— Procéder à leur extraction et analyse sans altération

— Garantir la chaîne de possession (*chain of custody*)

— Produire un rapport clair, traçable et exploitable par le juge

1.3 Contexte institutionnel et collaboration inter-agences

L'enquête, conduite sous l'autorité du juge d'instruction militaire, a mobilisé :

— La brigade de gendarmerie territoriale pour les opérations de terrain
— La division technique du renseignement pour la fourniture des métadonnées
— Un laboratoire de criminalistique numérique pour l'exploitation des supports saisis

Chapitre 2

Collecte et préservation des preuves numériques

2.1 Identification des sources numériques

Les premiers actes de l'enquête ont permis d'identifier plusieurs types de supports pertinents :

— Téléphones portables des suspects et de la victime

— Ordinateurs portables professionnels

— Terminaux GPS et appareils de communication radio

— Caméras de vidéosurveillance urbaines

— Enregistrements issus des opérateurs de téléphonie mobile

2.2 Méthodes de saisie et d'isolation

— Téléphones mis sous scellés et placés sous surveillance

— Ordinateurs clonés sur le terrain à l'aide de **write-blockers**

— Vidéos copiées à partir des DVR via interfaces forensiques

2.3 Outils et logiciels utilisés

— **Cellebrite UFED 4PC** : extraction des téléphones

— **FTK Imager, EnCase Forensic** : duplication bit à bit

— **Autopsy 4.21** : récupération de fichiers supprimés

— **DVR Examiner** : extraction vidéos de surveillance

— **Wireshark** : inspection de paquets réseau

2.4 Préservation et documentation (Chain of Custody)

Chaque support a été enregistré dans un registre de scellés numériques avec numéro unique, date, responsable et signature du greffier.

Chapitre 3

Analyse technique et corrélation des données

3.1 Exploitation des téléphones portables

— Messages indiquant surveillance préalable de la victime
— Communications coordonnées le jour des faits
— Fichiers multimédias : images du véhicule, croquis, plans

3.2 Données de géolocalisation

Analyse via **ArcGIS** et **Magnet AXIOM** :

— Trajets des véhicules avant et après le meurtre
— Présence simultanée de plusieurs terminaux sur le lieu d'enlèvement
— Corrélation avec les images vidéo

3.3 Vidéosurveillance et métadonnées

Images extraites et authentifiées par empreinte **SHA-256**, analyse image par image avec **Amped Five** :

— Reconnaissance du véhicule utilisé pour la filature
— Identification des horaires exacts
— Coordination temporelle avec téléphones localisés

3.4 Corrélation multi-sources

Données centralisées dans une base chronologique normalisée :

— Trame temporelle complète

— Groupes d'activité synchronisés

— Cartographie relationnelle entre utilisateurs

Chapitre 4

Exploitation judiciaire des preuves numériques

4.1 Analyse approfondie des communications

Identification des contacts, historique des appels et messages, éléments de coordination logistique. Techniques pour données cryptées.

4.2 Exploitation des données informatiques

Récupération de fichiers supprimés, identification de scripts et accès distants, analyse des logs, corrélation avec les activités de terrain.

4.3 Synthèse de l'exploitation judiciaire

Rapport précisant origine des preuves, corrélation multi-sources, conclusions pour le juge. Validation par experts indépendants.

Chapitre 5

Difficultés et limites techniques

5.1 Obstacles liés à l'environnement numérique

Cryptage des communications, suppression volontaire de fichiers, multiplicité des plateformes.

5.2 Contraintes légales et institutionnelles

Délais de réquisition, secret des correspondances, filtrage rigoureux.

5.3 Limites matérielles et humaines

Conservation limitée des vidéos, mobilisation de plusieurs experts spécialisés.

Chapitre 6

Aspects éthiques et déontologiques

6.1 Respect de la légalité et de la procédure

Mandats judiciaires respectés, chaîne de possession strictement suivie.

6.2 Confidentialité et protection des données

Anonymisation des tiers, stockage sécurisé des copies d'analyse.

6.3 Neutralité et objectivité de l'expertise

Indépendance, conclusions basées sur éléments vérifiables, journal d'analyse détaillé.

Chapitre 7

Recommandations et conclusion

7.1 Recommandations opérationnelles

Formation des forces et magistrats, infrastructure nationale sécurisée, coopération rapide avec opérateurs télécoms.

7.2 Recommandations législatives

Encadrement des communications cryptées, conservation des vidéos, standards uniformes d'expertise.

7.3 Conclusion finale

Démonstration de la planification du crime, fiabilité des données, admissibilité probatoire, contribution à la manifestation de la vérité judiciaire.