# Pratiques de l'Investigation Numérique

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

**Département de Génie Informatique**

Cybersécurité et Investigation Numérique

**4ème année**

**LABS d'Investigation Numérique**

**Thierry MINKA**, Sr-Eng, Sr-Lead Auditor, GRC Expert, Legal Expert in Cybercrime

# Table des matières

Chers étudiants,

Bienvenue dans ce Lab de Référence, conçu pour être **le fil conducteur de notre cours durant ce second semestre**. Plus qu'un simple exercice, ce Lab sera une base pratique et structurée qui vous accompagnera dans la compréhension et la maîtrise des compétences clés de l'expertise judiciaire numérique.

Le cas que nous étudierons n'a pas été choisi au hasard. Il aborde des problématiques actuelles et concrètes, comme l'utilisation abusive des réseaux sociaux, les atteintes à la réputation, et les défis liés à la collecte et à l'analyse de preuves numériques dans des environnements complexes. Ces enjeux sont représentatifs des défis que rencontrent aujourd'hui les experts en investigation numérique.

Au cours de ce Lab, vous apprendrez à :

- **Analyser des preuves numériques issues d'un groupe WhatsApp,**
- **Appliquer des méthodologies forensiques rigoureuses pour garantir l'intégrité des données,**
- **Produire des rapports d'expertise détaillés et les défendre dans un cadre judiciaire.**

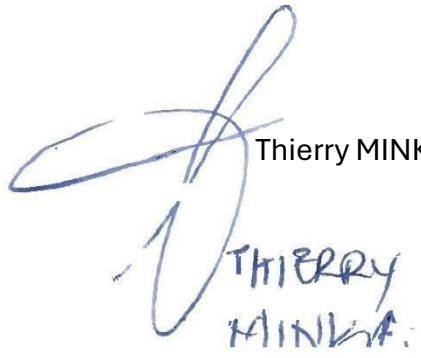
Ce Lab a été conçu pour vous offrir une expérience progressive et structurée, vous permettant d'explorer toutes les facettes du processus judiciaire numérique, depuis le dépôt de la plainte jusqu'à la défense du rapport devant un tribunal simulé. Vous serez confrontés à des situations réalistes où votre rigueur, votre méthode et votre capacité à argumenter seront déterminantes.

Ce travail n'est pas uniquement académique. Il vise à vous préparer aux réalités d'un métier exigeant où la précision, l'éthique et la maîtrise technique sont essentielles. Je vous encourage à aborder chaque étape avec sérieux et engagement. Ce Lab est une opportunité de développer des compétences pratiques qui vous seront précieuses dans votre future carrière.

Je vous souhaite beaucoup de succès dans ce défi, et n'oubliez pas : votre implication aujourd'hui forge votre expertise de demain.

**COURAGE !**

Thierry MINKA.



## A. CONTEXTE GENERAL :

Dans un contexte fictif, le pays du Gondwana est confronté à une augmentation des cyberincidents liés à l'utilisation abusive des réseaux sociaux. À l'université de Gondwana, un groupe WhatsApp officiel de la classe est utilisé par des étudiants pour diffuser des rumeurs malveillantes, des injures et des calomnies visant un enseignant. Ces messages, sous forme de captures d'écran et d'extraits, sont ensuite partagés dans d'autres groupes WhatsApp et Telegram, publics et privés.

Estimant que son honneur a été bafoué, l'enseignant porte plainte auprès du procureur de la République pour diffamation, injures publiques, et calomnies au moyen des TIC. Le procureur mandate un expert judiciaire numérique pour enquêter sur l'affaire, identifier les responsables, et établir un rapport détaillé. Ce rapport sera défendu devant le tribunal, où les étudiants joueront les rôles d'enquêteurs, de procureur, de témoins et de tribunal.

## B. OBJECTIFS PEDAGOGIQUES :

Les objectifs de ce Lab visent à fournir une compréhension approfondie et une application pratique des concepts d'expertise judiciaire numérique, en alignant vos apprentissages sur des situations concrètes et actuelles, afin de développer vos compétences techniques, juridiques et professionnelles dans un cadre structuré et réaliste.

### B.1 Objectifs juridiques :

1. Appliquer les lois en matière de cybercriminalité, diffamation, et gestion des preuves numériques.
2. Maîtriser la rédaction des documents juridiques : plainte, mandat d'expertise, acte de mise en accusation.

### B.2 Objectifs techniques :

1. Simuler un environnement complet d'investigation numérique avec un groupe WhatsApp.
2. Collecter, analyser et documenter des preuves numériques.
3. Conduire des interrogatoires et rédiger un rapport d'expertise.

### B.3 Objectifs professionnels :

1. Défendre un rapport technique devant le procureur et un tribunal fictif.
2. Développer des compétences en analyse critique, argumentation, et prise de décision.

## C. ENVIRONNEMENT VIRTUEL :

L'ensemble du Lab se déroulera dans un environnement virtuel immersif, où chaque étudiant disposera d'une machine virtuelle (VM) dédiée. Le groupe WhatsApp officiel sera simulé dans cet environnement, avec les rôles suivants :

1. Machine enquêteur (Kali Linux) : Utilisée par les experts judiciaires.
2. Machines utilisateurs (Windows 10) : Simulent les étudiants impliqués dans l'affaire.
3. Machine plaignant (Windows 10) : Représente l'enseignant plaignant.
4. Serveur central (Windows Server 2019) : Gère les échanges, les journaux réseau, et les preuves centralisées.
5. Machine tribunal/procureur (Windows Server 2019) : Utilisée pour centraliser les livrables et gérer la simulation du procès.

### C.1 Description technique des machines virtuelles

#### *C.1.1 Serveur Gondwana-DC (Serveur central)*

- Rôle :
    - Gérer les utilisateurs et centraliser les preuves numériques (captures d'écran, conversations exportées, logs réseau).
    - Héberger les dossiers partagés pour l'accès des enquêteurs.
    - Simuler une infrastructure réseau d'université.
- Caractéristiques techniques :
    - Système d'exploitation : Windows Server 2019.
    - Configuration matérielle :
        - CPU : 4 cœurs virtuels.
        - RAM : 8 Go.
        - Disque : 120 Go SSD.
    - Services activés :
        - Contrôleur de domaine pour la gestion des utilisateurs.
        - Serveur SMB pour le partage sécurisé des fichiers.
        - Enregistreur des logs réseau simulant les connexions WhatsApp et Telegram.
    - Logiciels installés :

        - Wireshark (surveillance réseau).
        - Gestionnaire de fichiers partagés.
- Configuration effectuée à quelle étape :
    - Avant le début du Lab : Configuré par l'enseignant ou l'administrateur pour stocker et partager les preuves numériques.
    - Les étudiants y accèdent dès la Phase 2 (analyse des preuves).

### *C.1.2. Machines utilisateurs (VM des mis en cause)*

- Rôle :
    - Simuler les étudiants qui ont participé à la diffusion des rumeurs dans le groupe WhatsApp.
    - Contenir des données à analyser par les enquêteurs (historique de conversations WhatsApp et Telegram, fichiers supprimés, captures d'écran).
- Caractéristiques techniques :
    - Système d'exploitation : Windows 10 Pro.
    - Configuration matérielle :
        - CPU : 2 cœurs virtuels.
        - RAM : 4 Go.
        - Disque : 60 Go SSD.
    - Logiciels installés :
        - WhatsApp Desktop ou accès à WhatsApp Web via navigateur.
        - Telegram Desktop.
        - Navigateur Chrome ou Firefox.
        - Applications fictives simulant des activités normales (ex. : Microsoft Office).
    - Données préchargées :
        - Historique de conversations incriminées.
        - Fichiers supprimés pouvant être récupérés.
        - Captures d'écran de messages WhatsApp ou Telegram.
- Configuration effectuée à quelle étape :

- Avant la Phase 1 : Les données initiales (historique WhatsApp, captures d'écran) sont préconfigurées par l'administrateur.
- Les étudiants enquêteurs y accèdent lors de la Phase 4 pour l'extraction des preuves.

### *C.1.3. Machine enquêteur (VM Kali Linux)*

- Rôle :
  - Réaliser l'extraction, l'analyse et la validation des preuves numériques.
- Caractéristiques techniques :
  - Système d'exploitation : Kali Linux (dernière version stable).
  - Configuration matérielle :
    - CPU : 4 cœurs virtuels.
    - RAM : 8 Go.
    - Disque : 80 Go SSD.
  - Logiciels et outils installés :
    - FTK Imager : Acquisition d'images forensiques.
    - Autopsy : Analyse des disques durs et récupération des fichiers supprimés.
    - Cellebrite UFED (ou alternative open source) : Extraction des données mobiles (WhatsApp, Telegram).
    - ExifTool : Analyse des métadonnées des fichiers.
    - Wireshark : Analyse des journaux réseau pour détecter les connexions suspectes.
    - HashCalc / sha256sum : Génération et vérification des empreintes hachées.
    - Python avec scripts personnalisés : Analyse des fichiers exportés de WhatsApp.
- Configuration effectuée à quelle étape :
  - Avant la Phase 4 : Les outils forensiques sont préinstallés sur cette machine.
  - Utilisée dès le début de la Phase 4 par les étudiants jouant le rôle d'expert judiciaire.

### *C.1.4. Machine du plaignant (Windows 10)*

- Rôle :
    - Fournir les preuves initiales issues des interactions sur WhatsApp et Telegram.
    - Représenter l'enseignant victime des rumeurs.
- Caractéristiques techniques :
    - Système d'exploitation : Windows 10 Pro.
    - Configuration matérielle :
        - CPU : 2 cœurs virtuels.
        - RAM : 4 Go.
        - Disque : 50 Go SSD.
    - Données préchargées :
        - Captures d'écran des messages incriminés.
        - Fichier .txt exporté depuis WhatsApp, contenant l'historique du groupe.
        - Copies des conversations Telegram montrant les partages de captures.
- Configuration effectuée à quelle étape :
    - Avant la Phase 2 : Les fichiers sont préparés par l'administrateur et fournis au moment du dépôt de la plainte.

### *C.1.5. Machine tribunal/procureur (Windows Server 2019)*

- Rôle :
    - Simuler la salle d'audience et gérer les livrables du Lab (rapports d'expertise, actes juridiques).
    - Centraliser les présentations orales des étudiants.
- Caractéristiques techniques :
    - Système d'exploitation : Windows Server 2019.
    - Configuration matérielle :
        - CPU : 4 cœurs virtuels.
        - RAM : 6 Go.
        - Disque : 100 Go SSD.
    - Logiciels installés :

        - Microsoft Word : Rédaction des rapports et actes juridiques.
        - Microsoft PowerPoint : Présentations orales.
        - Partage réseau DFS pour collecter les livrables des étudiants.
- Configuration effectuée à quelle étape :
    - Avant la Phase 5 : Configurée pour recevoir les rapports et les actes à défendre.
    - Utilisée lors des Phases 5 et 6 (simulation du procès).

## D. DEROULEMENT DU LAB :

***Phase 1 : Création du groupe WhatsApp (Semaine 1)***

***Action :***

- Un groupe WhatsApp officiel est créé dans l'environnement virtuel.
- Chaque étudiant configure WhatsApp Desktop ou Web sur sa machine virtuelle avec un numéro fictif.
- Les étudiants mis en cause échangent des messages dans le groupe : rumeurs, insultes, captures d'écran.
- Les conversations incluent des messages explicites incriminant l'enseignant.

***Livrables :***

- Captures d'écran des messages (générées par les étudiants).
- Historique des conversations exporté depuis WhatsApp (fichiers .txt).

***Outils :***

- WhatsApp Desktop/Web (préinstallé sur les VM).

**Phase 2 : Dépôt de la plainte (Semaine 2)**

***Action :***

- L'étudiant jouant le rôle du plaignant rédige une plainte formelle détaillant les faits et demandant l'ouverture d'une enquête judiciaire.

***Livrables :***

- Une plainte complète, incluant :
  - Les faits (conversations WhatsApp incriminées).
  - Les articles de loi applicables.
  - La demande de nomination d'un expert judiciaire.

**Phase 3 : Mandat de l'expert judiciaire (Semaine 3)**

***Action :***

- Le procureur rédige un mandat d'expertise confié à l'étudiant ou au groupe jouant le rôle d'expert judiciaire.

***Contenu du mandat :***

- Objectifs : Analyse des messages WhatsApp et identification des auteurs.
- Délai : 10 jours.

- Résultats attendus : Rapport détaillé incluant les preuves, les responsabilités, et les conclusions.

***Livrables :***

- Mandat formel signé par le procureur.

**Phase 4 : Exécution de l'expertise judiciaire (Semaine 4 à 6)**

***Collecte des preuves :***

- Extraction des messages WhatsApp et Telegram depuis les machines utilisateurs à l'aide de Cellebrite UFED ou d'autres outils.
- Analyse des captures d'écran fournies par le plaignant.

***Analyse des preuves :***

- Authentification des captures d'écran : Vérification des métadonnées avec ExifTool.
- Analyse des conversations exportées :
  - Recherche de mots-clés incriminants.
  - Validation de l'intégrité des fichiers (empreintes hachées).
- Détection des manipulations : Analyse des journaux réseau pour détecter les suppressions de messages.

***Documentation des étapes :***

- Tenir un journal d'actions détaillé pour garantir la traçabilité.

***Livrables :***

- Rapport d'expertise complet (voir structure ci-dessous).
- Journal des actions.

**Phase 5 : Conduite des interrogatoires (Semaine 7 à 8)**

***Conception des questionnaires :***

- Préparer un ensemble de questions ouvertes pour interroger les témoins et suspects :
  - *Avez-vous partagé des captures d'écran sur d'autres groupes ?*
  - *Pourquoi avez-vous écrit ce message ?*

***Simulation des interrogatoires :***

- Les étudiants jouent les rôles de témoins et d'enquêteurs.

- Les interrogatoires sont conduits en respectant les règles de neutralité et d'impartialité.

***Livrables :***

- Questionnaire d'interrogatoire.
- Synthèse des entretiens.

**Phase 6 : Défense du rapport et simulation du procès (Semaine 9 à 10)**

***Présentation du rapport :***

- L'expert présente son rapport devant le procureur et un tribunal fictif.
- Le rapport doit inclure :
  - Introduction, méthodologie, résultats, conclusions, annexes.

***Simulation du procès :***

- Le procureur utilise le rapport pour argumenter.
- Les mis en cause (étudiants) se défendent, avec des avocats fictifs.

***Livrables :***

- Rapport final défendu oralement.
- Acte de mise en accusation.

## E. STRUCTURE DU RAPPORT D'EXPERTISE :

Cette section présente la structure attendue pour le rapport d'expertise, afin de garantir une documentation claire, complète et professionnelle des analyses effectuées, des résultats obtenus, et des conclusions tirées au cours du Lab.

**Introduction :**

- Mandat reçu et objectifs de l'expertise.

**Méthodologie :**

- Description des outils et étapes suivies.

**Résultats :**

- Authenticité des captures confirmée ou réfutée.
- Identification des auteurs et des messages suspects.

**Conclusions :**

- Synthèse des responsabilités.
- Avis sur les faits incriminés.

**Annexes :**

- Copies des preuves numériques (captures d'écran, logs).

**Modèle de Rapport d'Expertise Judiciaire**

République du Gondwana
Tribunal de Première Instance

Rapport N° : 001
Date : 07.02.2025

***Introduction***

**Rappel du mandat reçu :**

En date du 25.01.2025, le Procureur de la République du Gondwana m'a mandaté, en ma qualité d'expert judiciaire en investigation numérique, par l'acte N° xxxxxxx pour :

1. Analyser l'authenticité des captures d'écran et messages incriminés transmis par M. X, enseignante à Polytechnique Gondwana-City, qui allègue des faits de diffamation, calomnies et injures publiques perpétrés via les TIC.
2. Identifier les auteurs des propos incriminés et déterminer la chaîne de diffusion des messages dans les groupes WhatsApp et Telegram.
3. Rechercher des preuves d'effacement ou de manipulation des données relatives à cette affaire.

**Objectifs de l'expertise :**

L'expertise vise à fournir un rapport détaillé permettant au tribunal de statuer sur la matérialité des faits, les responsabilités des mis en cause, et la pertinence des poursuites judiciaires.

**Méthodologie**

1. Collecte des preuves
   - Réception des éléments fournis par M. X :
     - Captures d'écran des messages WhatsApp/Telegram incriminés.
     - Description des faits allégués, accompagnée des dates et circonstances.
   - Saisie des appareils numériques des mis en cause et témoins :
     - Téléphones et ordinateurs de Mlle. A, Mlle. J et M. E, et des administrateurs des groupes concernés ont été saisis en présence de témoins.
     - Chaque appareil a été sécurisé avec un bloqueur d'écriture et documenté dans un registre de saisie.
   - Préservation des preuves numériques :
     - Création d'images forensiques des appareils avec FTK Imager et génération d'empreintes hachées (MD5/SHA256) pour garantir leur intégrité.

2. Analyse des données
   - Extraction des messages WhatsApp et Telegram :
     - Utilisation de Cellebrite UFED pour analyser les bases SQLite (msgstore.db pour WhatsApp et tdlib.db pour Telegram).
     - Décryptage des données chiffrées via les sauvegardes disponibles.
   - Recherche d'anomalies :
     - Analyse des journaux système et caches pour détecter des preuves d'effacement.
     - Vérification de la cohérence des métadonnées (dates, expéditeurs).
   - Identification des auteurs et chaîne de diffusion :
     - Analyse des transferts de messages pour comprendre leur propagation.

3. Documentation et traçabilité
   - Un journal de collecte a été tenu pour chaque étape de l'analyse.
   - Les preuves ont été classées et annexées au rapport sous forme de copies horodatées.

**Résultats**

4. Authenticité des captures d'écran :
   - Les captures fournies par M. X sont authentiques. Les métadonnées EXIF confirment qu'elles ont été prises entre 17 et 24 janvier 2025, avec un appareil compatible.
   - Aucun signe de falsification n'a été détecté (ex. : retouches numériques, incohérences dans les données).
5. Identification des auteurs :
   - Les messages diffamatoires et injurieux ont été envoyés par :
     - Mlle. B: Auteur principal de plusieurs messages diffamatoires.
     - Mlle. A : Auteur principal de plusieurs messages calomnieux et a contribué à la propagation des messages en les transférant dans d'autres groupes WhatsApp ;
     - M. E : A contribué à la propagation des messages en les transférant dans d'autres groupes Telegram publics.
   - Chaîne de diffusion des messages :

    - Les messages ont initialement été publiés dans l'un des groupes WhatsApp officiel de la classe.
    - Ils ont ensuite été transférés vers au moins trois autres groupes Telegram et 2 groupe WhatsApp.
- Anomalies détectées :
    - Des tentatives d'effacement ont été identifiées sur le téléphone de Mlle. A et de M. E.
        - Analyse des blocs libres : des fragments de messages supprimés ont été retrouvés, confirmant l'intention de dissimuler des preuves.

**Conclusions**

- Synthèse des responsabilités :
    - Mlle. J est responsable de la rédaction et de la publication des messages diffamatoires.
    - Mlle. A est responsable de la rédaction et de la publication des messages diffamatoires.
    - M. E a facilité la diffusion de ces messages, aggravant leur impact.
    - Les messages ont causé un préjudice significatif à M X, atteignant sa dignité et sa réputation professionnelle.
- Avis sur la matérialité des faits :
    - Les faits de diffamation, calomnies et injures publiques via les TIC sont avérés.
    - Les preuves collectées corroborent les allégations de M. X.

**Annexes**

- Captures d'écran authentifiées :
    - Copies horodatées des messages WhatsApp et Telegram incriminés.
- Logs d'analyse :
    - Résultats des métadonnées (dates, expéditeurs, transferts).
- Journal de collecte :
    - Liste détaillée des éléments saisis, avec numéros de série et empreintes hachées.
- Fragments de messages supprimés :
    - Copies récupérées des messages effacés sur le téléphone de M. E et Mlle. A.

**Fait à : Gondwana City**
**Le : 7.02.2025**

**Par :** ETUDIANT

**Signature :**

**Cachet Officiel :**

## F. OUTILS, CONFIGURATION DES OUTILS ET LOGICIELS PAR PHASE

Cette section détaille la configuration spécifique des outils et logiciels nécessaires à chaque phase du Lab, en précisant leur rôle, leur installation, et leur utilisation pour garantir une exécution fluide et méthodique des différentes étapes de l'enquête numérique.

### F.1 Configuration par phase

| Phase | Configuration requise |
|---|---|
| Phase 1 (WhatsApp) | Configuration du groupe WhatsApp sur les machines des utilisateurs et du plaignant. |
| Phase 2 (Plainte) | Préparation des fichiers de preuves sur la machine du plaignant. |
| Phase 3 (Mandat) | Aucun outil supplémentaire nécessaire ; rédaction sur Word depuis la machine du procureur. |
| Phase 4 (Analyse) | Activation des outils sur Kali Linux : FTK Imager, Autopsy, Cellebrite, ExifTool. |
| Phase 5 (Rapport) | Préparation des livrables sur les machines enquêteur et tribunal. |
| Phase 6 (Procès) | Collecte et défense des rapports devant le tribunal à partir du serveur central. |

### F.2 Ressources nécessaires pour les étudiants

#### *F.2.1 Accès à une plateforme de virtualisation :*

- VMware Workstation, VirtualBox, ou un serveur cloud (Proxmox).

#### *F.2.2 Matériel étudiant :*

- Ordinateur portable avec au moins 16 Go de RAM (idéal pour gérer plusieurs VM).
- Connexion réseau stable pour accéder aux machines virtuelles.

#### *F.2.3 Formation préalable :*

- Introduction à l'utilisation de Kali Linux et des outils forensiques (FTK Imager, Autopsy).
- Sensibilisation aux concepts juridiques applicables (diffamation, injures publiques, cybercriminalité).

## G. ÉVALUATION :

La section a pour but de mesurer votre capacité à appliquer les compétences et connaissances acquises tout au long du Lab, en prenant en compte la qualité de vos analyses, la rigueur de vos méthodologies, et votre aptitude à défendre vos conclusions dans un cadre professionnel et judiciaire simulé.

Chaque phase est notée, avec un total de 100 points :

1. Création du groupe WhatsApp et collecte des preuves : 20 points.
2. Rédaction de la plainte : 10 points.
3. Mandat de l'expert judiciaire : 10 points.
4. Rapport d'expertise : 40 points.
5. Interrogatoires : 10 points.
6. Simulation du procès : 10 points.

## H. CONCLUSION :

Vous voici arrivés au terme de ce Lab, un parcours qui vous aura permis de plonger au cœur des défis techniques, juridiques et pratiques de l'expertise judiciaire numérique. Chaque étape, du dépôt de la plainte jusqu'à la défense devant un tribunal simulé, a été l'occasion d'appliquer vos connaissances, de renforcer vos compétences et de démontrer votre capacité à mener une enquête avec rigueur et méthode.

Vous avez eu l'opportunité de confronter théorie et pratique, de travailler en équipe, et d'affronter des problématiques actuelles exigeant précision et réflexion critique. Ce travail n'a pas simplement testé vos connaissances, il a mis en lumière votre engagement et votre professionnalisme face à des situations complexes.

En tant qu'enseignant, j'ai joué mon rôle en vous guidant, en vous fournissant le cadre et les outils nécessaires. À présent, tout ce qui découlera de ce travail est entre vos mains. La balle est désormais dans votre camp.

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

***Thierry MINKA***