Philosophie et Fondements de l'Investigation Numérique

Matière : Théories et Pratiques de l'Investigation Numérique

Enseignant :M. MINKA Thierry

Année académique : 2025–2026

Par l'étudiante : ZE MVONDO Océanne M.

Filière : 4e année CIN

Exposé 1 : Présentation détaillée du protocole ZK-NR : RL et positionnement dans l'investigation numérique moderne

Le protocole ZK-NR :RL, pour Zero-Knowledge Non-Repudiation : Reliable Logging, représente une avancée majeure dans la manière dont les preuves numériques peuvent être collectées, vérifiées et opposées dans le cadre d'enquêtes informatiques. L'idée centrale repose sur la non-répudiation : il s'agit de garantir qu'une personne ou un système ne puisse contester une action qu'il a réellement accomplie. Mais là où le ZK-NR :RL se distingue, c'est dans sa capacité à concilier cette exigence de traçabilité avec la préservation de la confidentialité. Grâce aux preuves dites "à divulgation nulle de connaissance", il devient possible de prouver qu'une information est vraie sans en révéler le contenu, un principe essentiel pour protéger les données sensibles tout en assurant la fiabilité des investigations.

Ce protocole s'inscrit dans un vaste paysage de recherches en cryptographie moderne, où se côtoient les approches basées sur les STARKs, la cryptographie post-quantique et la sécurité formelle. Les chercheurs qui y travaillent cherchent à rendre les preuves numériques à la fois plus légères, plus rapides et résistantes aux menaces futures, notamment celles que feront peser les ordinateurs quantiques. Le ZK-NR :RL se positionne comme un équilibre entre rigueur théorique et application concrète, en permettant d'assurer une vérification solide des actions numériques sans compromettre l'intégrité du système global.

Derrière ce protocole, on trouve une communauté active composée de laboratoires universitaires, d'entreprises spécialisées et d'acteurs institutionnels. Chacun apporte sa pierre à l'édifice : certains se concentrent sur les aspects mathématiques et algorithmiques, d'autres sur les usages concrets dans l'investigation numérique ou sur les questions d'opposabilité juridique des preuves. Cette diversité d'approches favorise l'émergence d'un écosystème cohérent où la science, la technique et le droit travaillent ensemble pour construire des outils fiables et acceptables en justice.

Dans la pratique, le protocole ZK-NR :RL répond à un besoin très concret des enquêteurs numériques : pouvoir prouver qu'une action a eu lieu, dans un ordre précis, sans que les données associées puissent être falsifiées ni consultées par des tiers non autorisés. Cela ouvre la voie à des applications nombreuses, qu'il s'agisse d'auditer des systèmes sensibles, de retracer des opérations suspectes ou de garantir la valeur légale d'une preuve numérique. Couplé à des outils comme le CLO (Confidential Logging Operator), il permet d'assurer un enregistrement sûr et vérifiable de toutes les opérations critiques, dans le respect de la confidentialité.

En définitive, le protocole ZK-NR :RL illustre parfaitement la manière dont la cryptographie moderne se met au service de la justice numérique. En apportant à la fois sécurité, fiabilité et respect de la vie privée, il contribue à renforcer la confiance dans les processus d'enquête et à faire évoluer les standards de l'investigation numérique vers plus de transparence et d'intégrité.

Exposé 2 : Points sur les algorithmes de reconnaissance faciale

La reconnaissance faciale s'impose aujourd'hui comme l'une des technologies biométriques les plus utilisées, mais aussi les plus débattues. L'exposé s'attache à en présenter les grands principes et à offrir une lecture critique de son fonctionnement technique, de ses usages et de ses implications. Un système de reconnaissance faciale repose sur un processus en plusieurs étapes : détection du visage, extraction des caractéristiques distinctives (comme la forme du nez, des yeux, ou les distances entre certains points du visage), puis comparaison avec une base de données d'images connues. Cette architecture, combinant capteurs, logiciels d'analyse et algorithmes d'apprentissage, permet de transformer un visage en une signature numérique unique.

Les méthodes utilisées pour reconnaître un individu ont considérablement évolué. Aux approches classiques fondées sur la géométrie du visage ou les textures, se sont ajoutés les détecteurs et descripteurs de points d'intérêt, qui extraient des détails toujours plus précis. Aujourd'hui, les réseaux de neurones convolutifs et l'intelligence artificielle permettent d'atteindre des niveaux de fiabilité inédits, tout en réduisant les marges d'erreur.

Mais cette sophistication technologique s'accompagne d'importants enjeux. Sur le plan technique, les systèmes restent vulnérables aux biais des jeux de données, aux attaques par usurpation d'identité ou aux falsifications numériques (deepfakes). Les questions de sécurité, d'éthique et de respect de la vie privée deviennent alors centrales. La reconnaissance faciale soulève de vives inquiétudes quant à la surveillance de masse, la discrimination algorithmique et la gestion des données biométriques sensibles. Sur le plan juridique, elle interroge les principes de consentement, de proportionnalité et de conformité au RGPD. Elle bouleverse aussi l'organisation des institutions publiques et privées, qui doivent adapter leurs pratiques de gestion et de contrôle.

L'exposé se conclut sur une série de recommandations visant à encadrer l'usage de la reconnaissance faciale. Il met en avant la nécessité d'un développement responsable : choix rigoureux des bases de données, transparence des algorithmes, évaluation éthique avant déploiement, et limitation stricte des contextes d'utilisation. L'objectif est de trouver un équilibre entre efficacité technologique et respect des droits fondamentaux, afin que la reconnaissance faciale demeure un outil au service de la société et non un instrument de surveillance généralisée.

Exposé 3 : Conception et analyse d'un faux profil TikTok : choix d'une niche dans le cadre d'une investigation numérique

Cet exposé propose une étude concrète autour de la création et de l'analyse d'un faux profil sur TikTok, dans le but de comprendre les dynamiques de l'influence numérique et les comportements en ligne. L'expérience consiste à concevoir un profil fictif centré sur une

niche spécifique — un thème ou un univers ciblé — afin d'observer comment l'algorithme, les utilisateurs et les communautés réagissent à différents types de contenus. La démarche repose sur une méthodologie rigoureuse : élaboration du profil (photo, description, style), définition d'une stratégie de publication, choix des hashtags et des heures de diffusion, puis observation des interactions générées.

Le choix de la niche n'est pas anodin : il permet d'explorer un milieu particulier du réseau social, qu'il s'agisse de tendances de consommation, de communautés d'opinions ou de contenus à risque. Le travail montre que la viralité dépend souvent de facteurs subtils, comme la constance de la ligne éditoriale ou la manière dont le contenu s'aligne sur les tendances de la plateforme. Les outils de suivi et d'analyse — statistiques, engagement, partages, commentaires — servent à mesurer la portée du profil et la réaction des utilisateurs.

L'analyse révèle que la stratégie adoptée influence fortement la perception du profil : un ton trop neutre ou artificiel réduit la crédibilité, tandis qu'une personnalité bien définie attire plus d'interactions. Elle met également en lumière le rôle déterminant de l'algorithme de TikTok, capable de propulser ou d'ignorer un contenu en fonction d'indices comportementaux parfois opaques. Ce travail d'observation permet aussi de mieux comprendre comment des campagnes de désinformation, de manipulation d'opinion ou de marketing dissimulé peuvent se développer sur la plateforme.

Enfin, l'exposé débouche sur des recommandations pour les enquêteurs numériques : savoir concevoir des profils crédibles, maîtriser les codes de communication propres à chaque niche, et surtout interpréter avec prudence les données collectées. L'étude illustre de façon concrète la puissance et les dérives potentielles des réseaux sociaux dans la construction de l'opinion et dans les enquêtes en ligne.

Exposé 4 : L'utilité de l'investigation numérique dans la police judiciaire

L'investigation numérique est devenue un outil essentiel pour la police judiciaire moderne, profondément transformée par la généralisation des technologies et la dématérialisation des traces criminelles. Là où, autrefois, les preuves reposaient uniquement sur des objets matériels, des témoignages ou des observations directes, les enquêtes s'appuient désormais sur une multitude d'indices invisibles : fichiers, métadonnées, messages, historiques de navigation ou données de géolocalisation. Ces traces numériques permettent de remonter le fil des événements, d'identifier les auteurs et d'établir des preuves recevables devant les tribunaux.

Dans le contexte actuel, la police judiciaire tire un grand avantage de ces outils pour lutter contre la cybercriminalité et la criminalité organisée. Les enquêtes numériques permettent non seulement d'identifier et de tracer les auteurs d'actes malveillants en ligne, mais aussi de reconstituer avec précision la chronologie des faits. Elles soutiennent également les enquêtes traditionnelles : par exemple, un téléphone portable, un ordinateur ou une caméra de surveillance peuvent désormais fournir des éléments déterminants pour résoudre

une affaire de meurtre, de fraude ou d'enlèvement.

L'exposé souligne que les domaines d'application sont extrêmement variés : lutte contre la cybercriminalité, contre la criminalité financière et économique, contre le terrorisme, mais aussi protection de l'enfance et démantèlement de réseaux pédopornographiques. L'investigation numérique joue un rôle clé dans la coopération internationale, en permettant aux forces de l'ordre de collaborer au-delà des frontières grâce au partage de données et à des standards d'analyse communs.

Cependant, ces avancées s'accompagnent de nombreux défis. Les enquêteurs doivent maîtriser une grande diversité d'outils — logiciels d'analyse, techniques de récupération de données, surveillance réseau — tout en restant dans le cadre strict de la loi. Au Cameroun, l'exposé met en lumière des difficultés spécifiques : explosion du volume de données, manque de moyens matériels, dépendance à l'expertise technique étrangère, mais aussi question du respect des droits fondamentaux et de la vie privée. La formation des agents et l'adaptation des cadres juridiques apparaissent comme des enjeux majeurs.

En définitive, l'investigation numérique n'est plus un domaine accessoire mais un pilier de la police judiciaire moderne. Elle permet de révéler l'invisible, de donner un poids juridique à des traces électroniques et de renforcer l'efficacité des enquêtes. Sa réussite dépend toutefois de l'équilibre entre puissance technique, cadre légal rigoureux et éthique professionnelle.

Exposé 5 : Deepfake vocal

Le phénomène du deepfake vocal représente l'un des défis les plus récents et les plus préoccupants de l'ère numérique. Cette technologie, fondée sur l'intelligence artificielle et les réseaux de neurones, permet de reproduire la voix d'une personne de manière extrêmement réaliste à partir de simples échantillons audio. L'exposé explore son évolution, ses usages, ses risques, mais aussi ses implications pour l'investigation numérique et la sécurité.

À l'origine, les deepfakes vocaux ont été développés dans un cadre expérimental ou artistique, mais leur accessibilité croissante a ouvert la voie à des dérives : usurpation d'identité, escroqueries téléphoniques, manipulation de preuves ou diffusion de fausses informations. Les systèmes comme MINIMAX audio, étudié dans l'exposé, illustrent la puissance de ces outils capables de synthétiser des voix crédibles en quelques secondes. Dans un cas pratique, il est montré comment un tel logiciel peut être utilisé pour simuler la voix d'un dirigeant d'entreprise, amenant des employés à transférer des fonds sur de faux comptes — une escroquerie rendue possible par la perfection trompeuse du signal audio.

Au-delà des risques financiers, les deepfakes vocaux soulèvent d'importants enjeux éthiques et juridiques. Ils fragilisent la notion de confiance dans la parole humaine, menacent la réputation des individus et compliquent considérablement le travail des enquêteurs. Pour l'investigation numérique, ils représentent à la fois un objet d'étude et un nouveau type de menace à détecter. Les outils de vérification audio doivent désormais être capables d'analyser la structure du signal, les fréquences et les microvariations qui trahissent la

synthèse artificielle.

L'exposé évoque également les contre-mesures : développement d'algorithmes de détection, création de bases de données de référence, sensibilisation des professionnels de la justice et des médias. Il insiste sur la nécessité d'une régulation juridique claire, afin de définir les responsabilités et de prévenir les usages malveillants. Le deepfake vocal apparaît ainsi comme un double visage du progrès technologique : fascinant par ses capacités créatives, mais dangereux par son potentiel de manipulation. Pour les enquêteurs, il devient urgent de comprendre et de maîtriser cet outil, afin que la voix longtemps symbole de vérité ne devienne pas une arme de désinformation.

Exposé 6 : Simulation d'une série de messages sur WhatsApp

Cet exposé aborde la question sensible de la falsification de conversations numériques à travers une simulation de messages WhatsApp entre un homme et sa maîtresse. L'objectif est d'analyser la manière dont certains outils permettent de créer de fausses preuves numériques, tout en évaluant les implications que cela peut avoir sur les enquêtes et la justice. La mise en situation présente des échanges fictifs soigneusement reconstitués à partir d'éléments remis pour l'analyse, illustrant comment une discussion apparemment authentique peut être fabriquée de toutes pièces.

La méthodologie décrite s'appuie principalement sur l'utilisation de deux outils : Chatsmock, une application en ligne qui permet de simuler des conversations sur différentes plateformes de messagerie, et Adobe Photoshop, utilisé pour retoucher et perfectionner l'apparence des captures d'écran. Grâce à ces outils, il devient possible de modifier les noms, les horaires, les bulles de messages et même les images de profil, de sorte que le résultat soit indiscernable d'un vrai échange WhatsApp. Des pièces jointes au rapport illustrent le réalisme de la simulation et montrent jusqu'où la falsification peut aller.

L'exposé met cependant en lumière les limites de Chatsmock : si l'outil est accessible et simple d'usage, il reste détectable dans certains cas, notamment grâce à des incohérences dans les métadonnées ou les polices d'écriture. D'autres outils plus sophistiqués, parfois payants, offrent des possibilités encore plus réalistes, ce qui complique le travail des experts en investigation numérique.

Cette capacité à créer de fausses conversations a un impact majeur sur les enquêtes judiciaires et les expertises numériques. Les enquêteurs doivent désormais redoubler de vigilance, car une capture d'écran ne constitue plus une preuve suffisante sans vérification approfondie des fichiers sources, des horodatages et des métadonnées. L'exposé se conclut par des recommandations fortes : renforcer les outils de détection de falsifications, développer la formation des enquêteurs à la lecture critique des preuves numériques, et encourager la sensibilisation du public aux risques liés à la manipulation de contenus. Cette étude rappelle que, dans un monde où l'image et le texte peuvent être aisément falsifiés, la vérité numérique nécessite une rigueur technique et éthique sans faille.

Exposé 7 :À l'aide d'une IA, réaliser une vidéo dans laquelle le chef de groupe dispense le premier chapitre du cours : Deepfake

Cet exposé illustre de manière concrète la puissance des intelligences artificielles génératives à travers la création d'une vidéo de type deepfake, dans laquelle le chef de groupe apparaît en train de dispenser le premier chapitre du cours. L'expérience vise à explorer les possibilités offertes par les outils modernes d'IA pour la synthèse vocale et la génération d'images animées, tout en questionnant les enjeux éthiques et pédagogiques de ces technologies.

Le travail s'appuie sur deux outils principaux : HeyGen AI et GPT. HeyGen permet de générer des avatars réalistes à partir d'une photo et d'un texte, en synchronisant parfaitement les mouvements des lèvres et les expressions du visage avec la voix artificielle. GPT, quant à lui, a été utilisé pour la rédaction du script et la structuration du contenu du chapitre. En combinant ces deux technologies, les étudiants ont pu produire une vidéo cohérente où le "faux" chef de groupe semble véritablement donner cours, avec une diction fluide et des gestes crédibles.

Au-delà de la démonstration technique, cette expérience met en lumière la frontière de plus en plus floue entre le réel et le virtuel. Si ces outils ouvrent des perspectives fascinantes pour l'éducation — comme la création de supports interactifs, de cours automatisés ou de contenus multilingues — ils soulèvent également des questions éthiques : à qui appartient l'image utilisée ? Comment éviter les détournements malveillants ? Et comment préserver la confiance du public face à des contenus générés artificiellement ?

L'exposé conclut que les deepfakes, lorsqu'ils sont utilisés de manière encadrée et transparente, peuvent devenir des outils puissants d'apprentissage et de communication. Mais il rappelle aussi que leur banalisation impose une vigilance accrue. L'intelligence artificielle n'est ni bonne ni mauvaise en soi : tout dépend de la manière dont on choisit de s'en servir. Cette simulation vidéo devient ainsi un exemple à la fois fascinant et avertisseur des défis à venir dans la société numérique.

Exposé 8 :Les trois meilleurs logiciels de rédaction de mémoire

Cet exposé propose une analyse claire et argumentée des trois principaux outils utilisés dans la rédaction académique moderne : Overleaf, Microsoft Word et Zotero. L'objectif est de comprendre les forces, les limites et les combinaisons optimales de ces logiciels dans le cadre de la réalisation d'un mémoire universitaire ou professionnel.

Overleaf : l'excellence académique par LaTeX

La première partie est consacrée à Overleaf, une plateforme en ligne basée sur le langage LaTeX, largement utilisée dans les milieux scientifiques et techniques. L'exposé retrace

brièvement son historique, né du besoin de simplifier l'accès à LaTeX sans nécessiter d'installation locale. Overleaf incarne une philosophie de travail axée sur la précision, la structure et la collaboration en temps réel.

Ses atouts majeurs résident dans la qualité professionnelle des documents produits, la gestion parfaite des équations et symboles scientifiques, ainsi que dans la possibilité de travailler à plusieurs auteurs simultanément. La synchronisation automatique, les modèles intégrés et l'exportation fluide vers le PDF final en font une référence dans le monde académique. Cependant, la courbe d'apprentissage de LaTeX reste un frein pour les débutants. Certains étudiants préfèrent ainsi des alternatives plus accessibles comme Word ou Google Docs, notamment dans les disciplines littéraires ou sociales.

Microsoft Word : le pilier du traitement de texte universel

La deuxième partie s'intéresse à Microsoft Word, le logiciel le plus populaire dans le monde de la rédaction. Word se distingue par sa polyvalence et sa familiarité : il est présent dans tous les environnements éducatifs et professionnels. L'exposé souligne ses points forts académiques, tels que l'insertion automatique des tables des matières, la numérotation des figures, les styles prédéfinis et surtout la compatibilité avec des outils comme Zotero pour la gestion des références.

Word brille par sa simplicité d'utilisation, sa compatibilité multiplateforme et ses fonctions de correction grammaticale. Toutefois, certaines faiblesses sont relevées : une gestion parfois complexe des longs documents, une mise en page perfectible pour les travaux scientifiques, et une dépendance à la suite Microsoft. Ses concurrents (LibreOffice, Google Docs, WPS Office) peinent encore à égaler sa stabilité et sa richesse fonctionnelle.

Zotero : le spécialiste de la bibliographie

Le troisième volet met en lumière Zotero, un gestionnaire de références open-source indispensable pour toute rédaction universitaire. Ce logiciel permet de collecter, organiser et citer automatiquement les sources bibliographiques selon différents styles (APA, MLA, Chicago, etc.). Grâce à son intégration directe avec Word ou Overleaf, il automatise la création des bibliographies et fait gagner un temps considérable.

Zotero se distingue aussi par ses fonctionnalités collaboratives — comme les Zotero Groups — et son écosystème complet (extensions de navigateur, synchronisation cloud, export vers BibTeX). L'exposé mentionne également ses alternatives, telles que Mendeley ou EndNote, tout en rappelant que Zotero reste la solution la plus accessible et la plus éthique, puisqu'elle est totalement gratuite et respectueuse des données utilisateurs.

Combinaisons gagnantes et workflows optimisés

Une partie essentielle du rapport est dédiée aux synergies logicielles. Trois configurations principales sont décrites :

Word + Zotero, la solution la plus accessible, idéale pour les étudiants de toutes disciplines ;

Overleaf + Zotero + ZoteroBib, un trio d'excellence pour les mémoires scientifiques né-

cessitant une grande rigueur de présentation ;

Overleaf + Zotero Groups, un workflow collaboratif pour les équipes de recherche ou les co-auteurs.

Ces combinaisons permettent d'optimiser la gestion du temps, d'assurer la cohérence des citations et d'améliorer la qualité générale du rendu final. L'exposé aborde également les intégrations techniques entre les logiciels et fournit des recommandations selon le profil de l'utilisateur (débutant, chercheur, étudiant en sciences humaines, etc.).

Tableau comparatif et conclusion

La dernière section synthétise les fonctionnalités clés des trois logiciels sous forme de tableau comparatif : ergonomie, collaboration, compatibilité, automatisation bibliographique, et coût. L'analyse montre qu'aucun outil n'est parfait isolément, mais que leur complémentarité constitue la véritable force.

En conclusion, le texte rappelle que la réussite d'un mémoire ne dépend pas seulement de la maîtrise intellectuelle du sujet, mais aussi de la capacité à exploiter les bons outils numériques. Overleaf incarne la rigueur scientifique, Word la polyvalence et l'accessibilité, et Zotero la fiabilité bibliographique. Ensemble, ils forment un écosystème complet au service de la production académique moderne — où efficacité technique et excellence intellectuelle se rejoignent.

Exposé 9 :Les 10 cas africains les plus importants d'hacking

Cet exposé examine la cybersécurité sur le continent africain à travers une série de cas emblématiques, illustrant à la fois la vulnérabilité des infrastructures numériques et l'évolution des menaces en matière de hacking. Le texte commence par dresser un contexte général : l'Afrique connaît une adoption rapide des technologies numériques, mais cette croissance s'accompagne de défis majeurs en termes de protection des systèmes d'information, de formation des acteurs et de régulation juridique. Les infrastructures critiques — banques, télécommunications, santé, transports — deviennent des cibles privilégiées pour les cybercriminels, souvent motivés par le gain financier, l'espionnage industriel ou des objectifs politiques.

L'exposé décrit ensuite la méthodologie d'investigation employée pour analyser ces incidents, basée sur l'étude des rapports publics, des communiqués officiels et des analyses d'experts. Les critères retenus incluent la gravité de l'attaque, son impact économique et social, la sophistication technique et la portée régionale ou internationale.

Une partie centrale de l'exposé présente dix cas africains marquants. Parmi eux, le ransomware qui a frappé Transnet en Afrique du Sud en 2021 illustre les risques pour les infrastructures logistiques et le commerce international. Le piratage de la CNSS au Maroc en 2025 et l'attaque sur Eneo au Cameroun en 2024 montrent la vulnérabilité des institutions publiques et des services essentiels. D'autres cas, comme GhostLocker 2.0 en

Égypte, le scandale Pegasus au Maroc ou le piratage des banques ivoiriennes, soulignent la diversité des méthodes utilisées : logiciels malveillants sophistiqués, espionnage téléphonique et cyberattaques ciblées sur le secteur financier. Les systèmes de santé tunisiens, Ethiopian Airlines, et les incidents liés à Mobile Money ou à la Banque centrale du Nigeria révèlent quant à eux l'impact concret sur la vie quotidienne des citoyens et sur l'économie nationale, montrant que la cybersécurité est désormais un enjeu stratégique au plus haut niveau.

Enfin, l'exposé propose des recommandations pour renforcer la cybersécurité sur le continent africain. Il insiste sur la nécessité de mettre en place des cadres légaux adaptés, de former les professionnels aux menaces émergentes, de développer des infrastructures résilientes et de favoriser la coopération régionale et internationale. La conclusion souligne que la croissance numérique de l'Afrique ne sera durable que si elle s'accompagne d'une protection efficace contre les cyberattaques, combinant vigilance technique, prévention et réglementation adaptée.