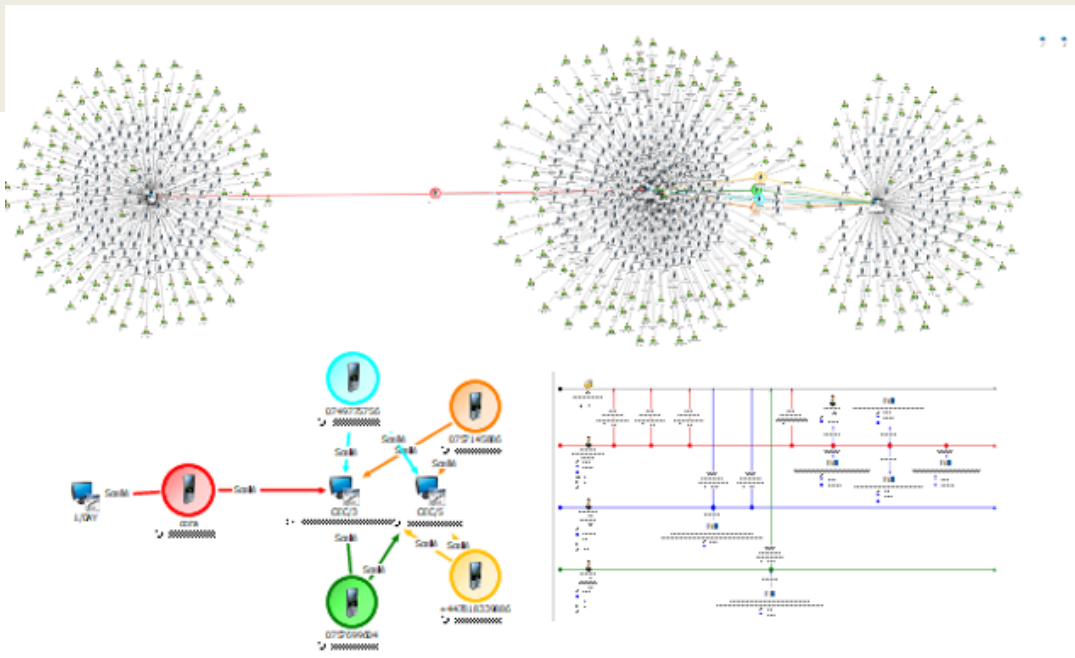
ARTICLE

DE L'ANALYSE CRIMINELLE A L'ANALYSE RELATIONNELLE VISUELLE AU PROFIT DES ENTREPRISES

Principe de rapprochements dans l'enquête



Croisement de données multi-sources pour matérialiser des réseaux de connexion et des chronologies.

L'information, une ressource stratégique

FREDERIC LENFANT – 20/01/2021

Dans le cadre d'une enquête judiciaire, l'objectif est d'identifier et appréhender les auteurs d'infraction(s) à la loi pénale, comprendre, expliquer les faits et recueillir les preuves, selon différentes techniques d'investigations. Pour se faire il est essentiel d'exploiter une masse importante d'informations, qui est collectée au fur et à mesure de l'enquête.
La gestion et l'analyse de l'information est donc au cœur de toute démarche de vérification et d'étude des faits. Ainsi, la formulation d'hypothèses, au vu des constatations, des témoignages, des réquisitions, des surveillances et d'actes techniques conduit, finalement, à produire une conclusion susceptible d'aider à rendre une décision de justice. De fait, on peut donc établir que l'information est une ressource stratégique qu'il est important de traiter selon les fondamentaux du cycle du renseignement :
1. l'expression du besoin et l'orientation des recherches,
2. La collecte de l'information,
3. Le traitement et l'analyse de l'information,
4. La diffusion de l'information analysée qui devient ainsi du renseignement.
Cette démarche itérative essentielle intervient dans de nombreux domaines d'application, y compris dans le secteur privé. L'analyse criminelle y apporte ainsi une vraie plus-value dans les phases 3 et 4.

Agréger des données pour révéler des éléments

L'analyse criminelle

Dans sa définition nominale, l'**Ana**lyse **Crim**inelle est une technique qui consiste en la recherche et la mise en évidence **méthodique** des **relations** entre des données criminelles ou contextuelles à des fins de pratique judiciaire. Communément appelé « AnaCrim », souvent annoncé comme un logiciel boule de cristal ou de schématisation, la réalité est entre les deux et répond plus simplement à un besoin de mise en perspective et d'analyse visuelle des données, pour l'aide à la décision dans les enquêtes. Cette spécialité, qui repose sur la théorie des graphes, est pratiquée depuis 1994 en Gendarmerie, bien avant le buzzword de l'**I**ntelligence **A**rtificielle. Issue de la méthode « anacapa sciences », pour faire face à l'explosion de la criminalité aux Etats Unis dans les années 1970, cette technique de traitement et d'analyse de l'information pour les investigations, s'appuie sur deux types de raisonnement : la méthode déductive qui part d'une hypothèse pour la vérifier et argumenter au regard des éléments déjà recueillis. Et la méthode inductive qui part d'une observation pour induire de nouveaux éléments qui peuvent alors révéler de nouveaux angles de vue. Et c'est bien dans ce dernier cas que l'analyse criminelle prend tout son sens.
Caractérisée par graphes visuels des relations entre les données, cette technique se retrouve implicitement dans le processus de fouille de données dit KDD (Knowledge Discovery in DataBases), notamment dans la phase d'identification de patterns pour produire de la connaissance utile à la prise de décision.

La démarche même d'une enquête repose sur le besoin récurrent de réaliser des recoupements (ou rapprochements) afin de révéler des axes de compréhension, d'isoler les éléments pertinents, qui serviront soit de preuves, soit de points pivots pour orienter de nouvelles recherches. Ceci-dit, cette approche de recoupement n'est pas chose aisée à réaliser dans la masse d'information textuelle qui reste pourtant la principale source de données dans les investigations. C'est pourquoi par son approche visuelle et analytique, l'Analyse Criminelle apporte une aide évidente à l'investigation.

En effet, c'est bien la visualisation relationnelle qui permet de révéler des informations, difficiles à percevoir en mode de représentation textuelle ou tabulaire. C'est souvent dans la relation et l'induction que l'on trouve la solution.

Ainsi, on peut dire que l'Analyse Criminelle permet de révéler du contexte, de faire du lien, de matérialiser des relations évidentes et d'autres induites, jusqu'à mettre en évidence des éléments de preuves dans une démarche forensique. C'est-à-dire qui s'applique à une action légale, judiciaire et méthodique, en respectant un protocole scientifique d'analyse.

Mais comme nous allons le voir, cette technique d'analyse de renseignement (intelligence analysis) est très facilement transposable aux besoins croissants d'investigations dans les entreprises : l'Analyse Relationnelle Visuelle pour le secteur privé.

MOT-CLÉ

La structure de l'information

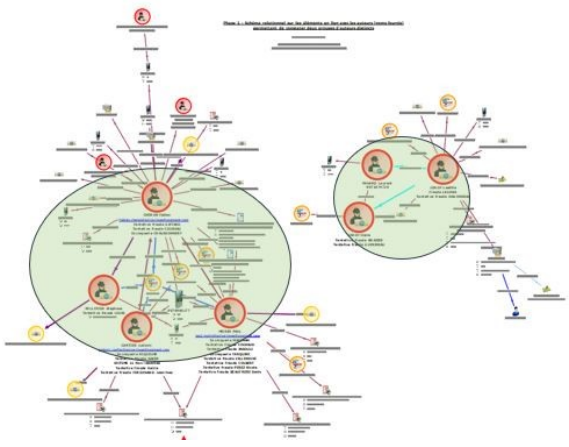
Entité – Relation - Entité

AU DELA DE LA SIMPLE REPRESENTATION

Beaucoup de logiciels ne font que représenter visuellement des données mais ne prennent pas en compte l'essence même de l'analyse criminelle : la décomposition de l'information en mettant l'action sur la relation entre les entités.
Ainsi, cette structure de l'information en « entité source » → « lien » → « entité destination », complétée par des d'attributs (ou propriétés) offre une capacité analytique supérieure au format tableau. Ceci permet de garder un maximum d'informations contextuelles, ce qui est particulièrement pertinent dans les investigations, par rapport à des graphiques quantitatifs.

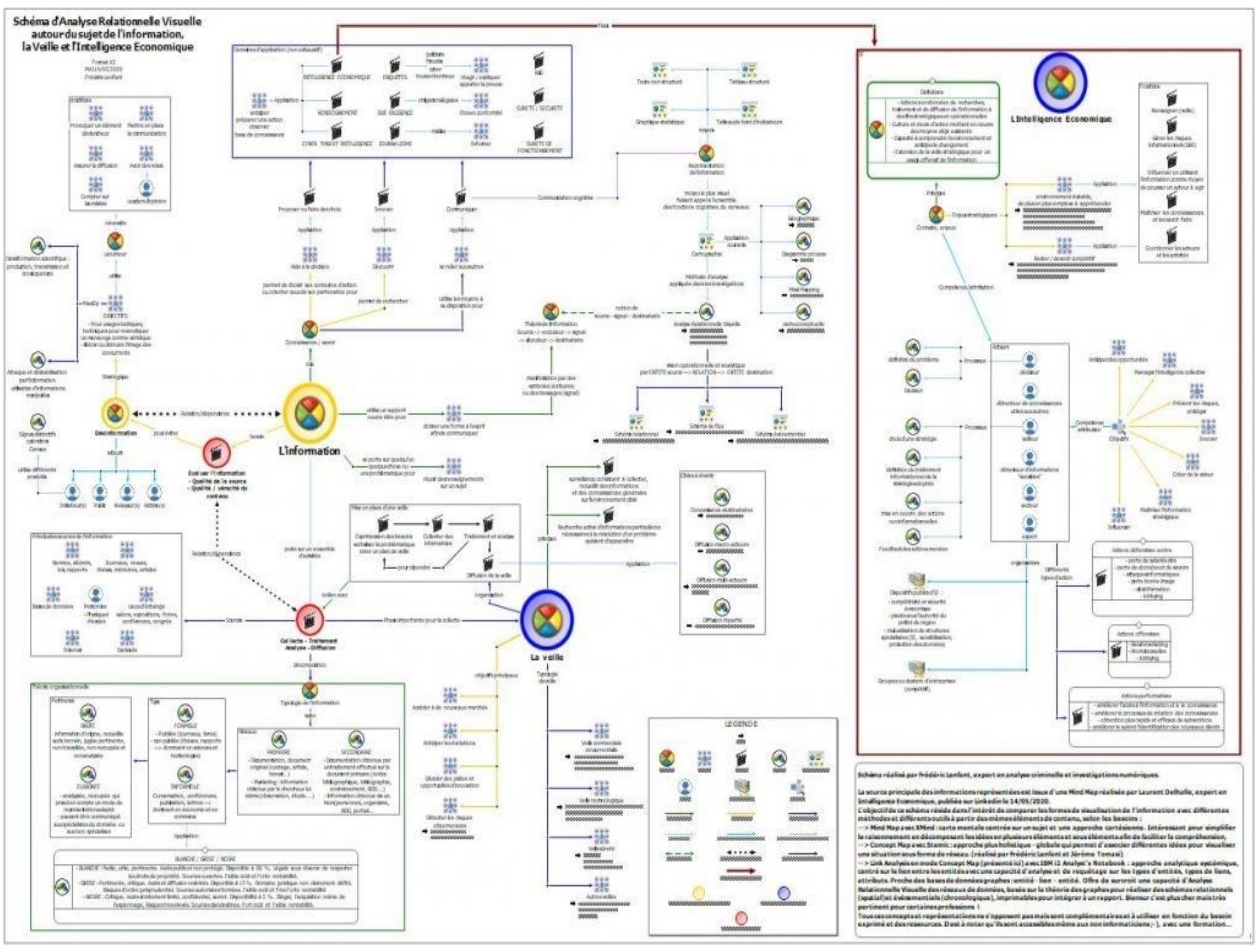
Ces corrélations que le cerveau humain fait naturellement, nécessitent une organisation méthodique de l'information, sous une forme permettant de favoriser l'analyse de données dans le cadre des situations complexes, telles que les enquêtes.

Apprendre le bon « réseau »nnement :
Cette approche est en effet fondée sur les principes mêmes de l'analyse systémique, dont l'origine repose sur la modélisation du complexe.
En effet, notre culture cartésienne a formaté notre mode de pensée pour ranger les informations dans des boîtes (table), ce qui a pour effet un cloisonnement qui simplifie sa réflexion. Mais toute la grandeur de l'analyse systémique est de sortir de cette linéarité pour réfléchir en réseau, ce qui a pour effet de prendre en compte les relations entre les boîtes. D'où l'adage : ***« le tout est PLUS que la somme des parties »*** ; le « plus » induisant la logique relationnelle qui favorise l'interaction, le contexte et la vision globale.



Dans la phase analyse, identification de clusters par les relations et compréhension des réseaux

L'analyste doit percevoir les éléments reliés pour y voir plus clair dans ses données



Réflexion sur le thème de l'information. Intérêt dans la phase « diffusion », d'une capacité de représentation visuelle et synthétique des données pour offrir une vue globale des éléments. Cette approche permet de modéliser des situations complexes et améliorer la compréhension pour l'aide à la décision.

MOT-CLÉ

Le logiciel historique

IBM I2 ANALYST'S NOTEBOOK

Afin d'outiller cette technique de raisonnement, l'Analyse Criminelle est historiquement portée par le logiciel i2 Analyst's Notebook (et sa suite i2), racheté par IBM en 2011. Ce logiciel couvre les fonctions d'importation, de corrélation, d'analyse et de visualisation de données. Il permet l'utilisation des algorithmes de la théorie des graphes, pour identifier facilement et visuellement des clusters (communautés) et de modéliser les données sous formes de graphes.
Il est ainsi possible de réaliser des graphes tant relationnels que de flux et des schémas dit événementiels afin de matérialiser une succession d'évènements à analyser selon une échelle de temps. L'intérêt principal de ce logiciel est sa capacité à changer de perspective de visualisation, de la vue spatiale des données à la vue chronologique temporelle pour révéler des indices ou mettre en évidence des éléments de preuve. En effet, la capacité d'importer différents ensembles de données dans un même graphe met en perspective des informations que l'on n'aurait pas perçues si on les avait analysées séparément. Et c'est bien là où se situe les atouts de l'analyse criminelle, pour y voir plus clair dans ses données. Pour ses fonctions « couteau suisse » comparable à un « excel pour graphe », ce logiciel, pouvant traiter les données en local, est utilisé depuis des années dans nombre de services d'enquête et de renseignement dans le monde entier pour aider les analystes métiers, sans être informaticiens.
De nombreux outils d'analyse de réseaux existent mais très peu permettent d'afficher autant d'informations sur chaque entité et lien, afin de reproduire simplement une base de données graphe. Il offre en plus des capacités de mise en page et d'impression pour intégrer les graphes à des rapports écrits. Il s'intègre parfaitement dans le cycle du renseignement, **mais tout outil n'est rien sans méthodologie.** Les produits i2 sont rachetés en 2022 par la société Harris Computer. *MAJ 2022*

MOT-CLÉ

Protection des données

LES EXIGENCES (RGPD & CONFORMITE)

Il est important d'encadrer juridiquement les activités d'investigation pour rester en conformité avec le **R**èglement **G**énéral sur la **P**rotection des **D**onnées. Au même titre que la Business Intelligence, la Data Security Intelligence, répond à des contraintes d'analyse de données pour assurer sa mission.
Une **A**nalyse d'**I**mpact relative à la **P**rotection des **D**onnées (**P**rivacy **I**mpact **A**ssessment) est alors recommandée pour les missions d'investigation.
En effet, plusieurs domaines d'application nécessitent la professionnalisation de ce domaine pour lequel il sera nécessaire de bien identifier la finalité claire et la base légale. Ceci aura une influence sur l'information et l'exercice des droits, la durée de rétention des données, les mesures de sécurité et la minimisation des données traitées (d'où l'intérêt de faire des analyses uniquement avec les extractions ponctuelles des données juste nécessaires). Ces métiers d'investigateurs analystes devraient compléter les services d' « ethic & compliance » pour mutualiser les compétences entre analyse juridique, analyse informatique et analyse forensique.

MOT-CLÉ

Evolution vers les notions de « data intelligence »

LA RECHERCHE D'AUTOMATISATION

Depuis quelques années, la masse d'information à traiter est telle que de nombreux éditeurs spécialistes de l'analytique se sont penchés sur ces questions de renseignement et d'enquêtes.
Linkurio.us a notamment été utilisé par le consortium ICIJ des journalistes d'investigations pour l'affaire des « Panama papers » et montre encore une fois l'intérêt de l'analyse relationnelle visuelle.
Aleph Networks, spécialisé sur la phase de collecte et d'analyse, notamment dans des sources difficilement accessibles comme le Dark Web, offre également des capacités analytiques par graphes relationnels pour identifier des clusters. Aleph Networks est notamment associé avec Stemic, logiciel français de carte conceptuelle dans le cadre d'un projet de recherches lié à l'analyse visuelle.
QlikView ou Tableau Software sont aussi des outils pertinents pour la fouille et la visualisation de données.
De nouvelles solutions complètes et voulant couvrir tout le spectre du cycle du renseignement, arrivent également sur le marché et méritent d'être considérées.
SAS Visual Investigator, DataWalk, ChapsVision promettent de belles avancées, notamment dans la reconnaissance automatique d'entités nommées et dans les capacités d'analyse sur de gros volumes de données, multi formats. Ces plateformes complètes regroupent notamment tous les outils de visualisation : textuel, relationnel, cartographique, tout en gardant la relation entre les données.
Faisant partie d'une équipe d'experts dans le cadre d'un partenariat avec l'Ecole Supérieure de Sûreté des Entreprises (ESSE) à Paris, j'ai la chance de tester des solutions et d'échanger sur ces problématiques de « Data Intelligence ».
De plus, l'OSINT (**O**pen**S**ource**Int**elligence), sujet en plein essor, participe à développer les concepts de renseignement et d'investigation au profit du secteur privé dans différents domaines.
Beaucoup d'outils sont en phase de R&D mais peu sont assez souples encore pour répondre aux besoins dynamiques et adaptatifs pour l'investigation.
Passionné par l'évolution des outils de « data intelligence », très pertinente pour la phase de détection et de collecte, je reste pour autant prudent sur le résultat produit pour la phase d'investigations et la souplesse dans l'analyse de l'information pour l'enquête. En effet, les outils et les algorithmes d'apprentissage sont une aide incontestable pour traiter le volume d'informations que l'humain n'est plus en capacité d'appréhender. Mais la place de l'humain reste primordiale, dans le dernier niveau d'analyse, pour assurer la logique de l'investigation opérationnelle. L'efficacité passera de fait par la formation à ce raisonnement analytique pour l'investigation et avec l'usage d'outils adaptés.
Un outil sans analyste ne sert à rien et un analyste sans outil efficient sera moins opérationnel.

Le besoin d'investigations de plus en plus présent dans le secteur privé

MOT-CLÉ

Les domaines d'application

Dans le secteur privé

POUR L'ANALYSE RELATIONNELLE VISUELLE

De plus en plus d'obligations légales, réglementaires, contractuelles sécuritaires ou de conformité, font appel à des démarches d'investigations, de corrélation d'informations et de compréhension de phénomènes complexes. De l'analyse de données à la mise en évidence des éléments (de preuve) pour accompagner les rapports textuels, les domaines d'application sont multiples : ***lutte contre les fraudes, LCB-FT, cyber investigations, OSINT, Cyber Threat Intelligence, enquêtes internes, gestion d'incidents, déclaration de soupçons, Intelligence économique et renseignements stratégiques…***

MOT-CLÉ

Formation MARVADRISK® par l'OSINT

LA METHODE AVANT LES OUTILS

Peu importe le type d'information traité c'est le « réseau-nement » qui compte, afin que les outils informatiques répondent à votre besoin…
L'objectif de cette formation est de :

- Comprendre et développer les techniques de l'investigation et de l'analyse relationnelle visuelle, pour améliorer la compréhension de situations complexes.
- Voir au-delà des données et révéler des éléments induits par les relations.
- Acquérir une approche factuelle pour la gestion de l'information dans l'enquête.
- Savoir développer un raisonnement aussi bien inductif que déductif par une approche globale.
- Savoir mettre en évidence les éléments essentiels par les relations contextuelles entre des entités, afin de convertir du texte non structuré en schéma analytique visuel.
- Répondre au besoin de communication synthétique de l'information
- Prendre en compte l'éthique et la protection des données dans le traitement des investigations

L'OSINT (**O**pen**S**ource**Int**elligence) ou ROSO (**R**enseignement d'**O**rigine **S**ources **O**uvertes) apparait particulièrement intéressant pour mettre en application ces techniques d'Analyse Relationnelle Visuelle. En effet, on retrouve cette logique de renseignement et d'investigation basée sur la collecte et l'exploitation de l'information librement accessible. Ces informations peuvent provenir de sources multiples, principalement issues d'internet, des réseaux sociaux (SocMInt), des bases de données OpenData, journaux… Dans un sens très large, la phase de collecte de l'OSINT commence par la maîtrise du langage de requêtage de Google et la connaissance des sources qu'il est possible d'interroger selon le thème recherché.
Cette approche est désormais de plus en plus utilisée par les entreprises pour des objectifs stratégiques, économiques et de sûreté. Elle présente aussi un réel intérêt dans les démarches de Due Diligence sur les clients et fournisseurs et bien évidemment dans toutes démarches d'investigation numérique sur les cyber fraudes & cyber incidents.
L'OSINT n'est pas un simple outil ou un script que l'on construit mais répond à une véritable logique d'investigation.
Et quid de la mise en évidence des éléments clés ?

Méthode d'**A**nalyse **R**elationnelle **V**isuelle pour l'**A**ide à la **D**écision et les **R**ecoupements dans les **I**nvestigations et **S**ituations **'K'**omplexes

Une formation à l'investigation et l'analyse sur les fondamentaux de la méthodologie MARVADRISK ® est en cours de préparation auprès de l'Ecole Supérieure de la Sûreté des Entreprises (ESSE) à Paris. Une formation plus courte sur une journée est également réalisée au profit de l'Agence de Lutte contre la Fraude à l'Assurance (ALFA). MAJ 2022

MOT-CLÉ

Présentation de l'auteur

FREDERIC LENFANT – INTELFE ®

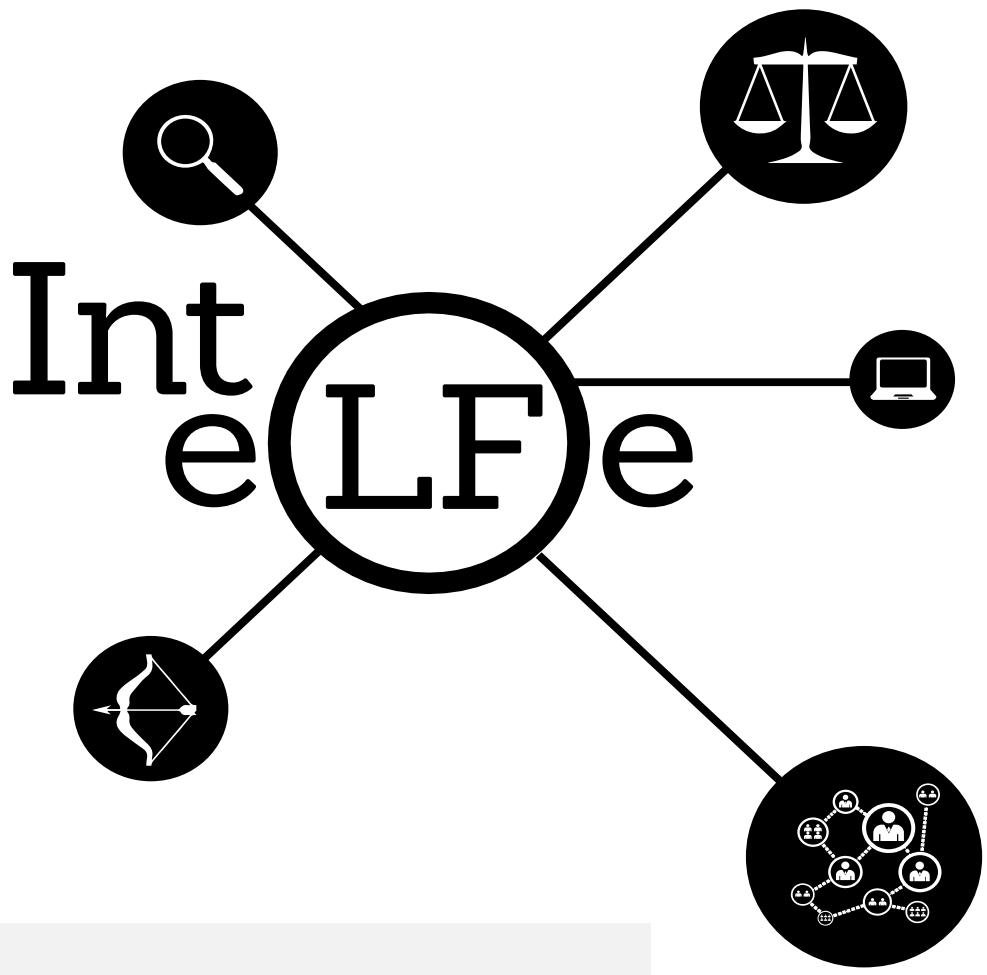
Major de Gendarmerie à la retraite, Frédéric Lenfant a eu une première carrière de 24 ans en Gendarmerie, principalement dans les services d'enquêtes judiciaires (Brigade et Section de Recherches). Après des fonctions d'enquêteurs et directeur d'enquête, il s'est spécialisé dans l'Analyse Criminelle Opérationnelle pour apporter une technicité dans l'appui aux enquêtes complexes (homicides, trafic de stupéfiants, criminalité organisée, mafia géorgienne, délinquance financière et pour la cybercriminalité). Passionné par le domaine des nouvelles technologies et la gestion de l'information dans l'enquête, il a développé certains outils et méthodes pour automatiser des tâches récurrentes dans les investigations et favoriser l'analyse de l'information, particulièrement pour l'analyse de la téléphonie.

En 2015, il entame une seconde carrière dans le secteur privé, d'abord dans un CERT (Computer Emergency Response Team) afin de travailler sur les processus de réponse à incidents et les notions montantes de la Threat Intelligence. Puis chez un industriel pour la mise en œuvre de sensibilisations de cybermenaces, dans la gouvernance cybersécurité et s'implique dans la conformité au RGPD.
Il assurait en parallèle une activité d'expertise judiciaire et de formateur dans différents établissements supérieurs.

Depuis Janvier 2021, afin de revenir dans son cœur de métier de l'investigation, Frédéric Lenfant partage son temps entre une activité dans un laboratoire de récupération de données et d'investigations numériques (Data-Labcenter) pour des missions d'expertise judiciaire et sa propre activité (InteLFe) de manière à développer des formations et s'investir dans des projets en lien avec la « data intelligence » dans un contexte d'investigations.

Eternel apprenant, il est titulaire de nombreuses formations dont le cursus de certification de management du risque de fraude et de corruption de l'ESSE à Paris. Son ambition : faire du lien et des passerelles entre les domaines professionnels par cette approche d'analyse relationnelle visuelle avec les aspects liés à l'expertise inforensique, les investigations sur les fraudes, l'OSINT, la conformité LCB-FT, les cybermenaces, la cybersécurité, et le RGPD… → approche systémique.
Dans cet objectif, Frédéric fait partie du comité de rédaction de la revue Cyber & Compliance.

INTELLIGENCE ENQUETE
LENFANT FREDERIC EXPERTISE



MOT-CLÉ

Formation MARVADRISK ®

Méthode d'**A**nalyse **R**elationnelle **V**isuelle pour l'**A**ide à la **D**écision et les **R**ecoupements dans les **I**nvestigations et **S**ituations **'K'**omplexes

Frédéric Lenfant
https://www.intelfe.com
contact@intelfe.com