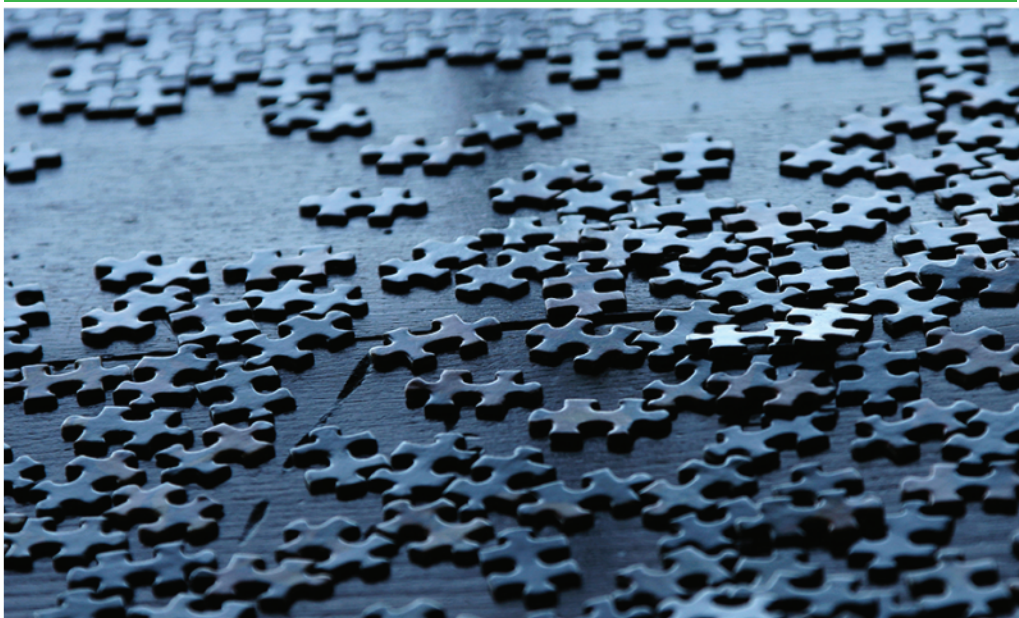




## Enquêtes informatiques et réponse aux incidents

La volatilité de la preuve électronique requiert le plus haut niveau de rigueur pour toute activité de collecte, de manipulation et d'analyse des données.

En raison du risque d'une altération involontaire de la preuve et afin d'assurer son admissibilité devant les tribunaux, les enquêtes informatiques doivent être réalisées par des experts en informatique judiciaire possédant l'expérience, les certifications et les outils spécialisés.



Depuis plus de 30 ans, OKIOK appuie son excellence sur la force de ses experts dans le domaine de la sécurité de l'information.

L'implication d'OKIOK en informatique judiciaire correspond à une progression naturelle des services spécialisés qu'elle offre à ses clients.

Soucieux d'un service personnalisé, nous proposons une approche pragmatique et sur mesure pour chaque mandat, en tenant compte de la confidentialité, de la réputation, des délais propres à chaque dossier et des différentes approches pouvant mener à la résolution d'un litige.

Depuis que les systèmes informatiques et Internet sont devenus des éléments indissociables de nos vies, les litiges impliquant des technologies de l'information sont en croissance constante.

Pour ces raisons, l'informatique judiciaire est devenue un domaine spécialisé de la sécurité de l'information en demande grandissante depuis ces dernières années.

Notre équipe d'experts en cyberenquêtes intervient rapidement et au meilleur tarif dans une large gamme de domaines, tels que:

- Actes criminels : fraudes, méfaits de données, falsification de documents, etc.
- Ordonnances Anton Piller
- Faute déontologique
- Audits internes
- Propriété intellectuelle
- Espionnage industriel
- Piratage informatique
- Cyberintimidation et diffamation
- Atteinte à la vie privée
- Incidents de sécurité



## Formations et outils spécialisés

Dans le cadre de procédures judiciaires ou d'enquêtes corporatives, certains systèmes informatiques doivent faire l'objet d'analyses approfondies pour déterminer s'ils ont été utilisés pour des activités illégales, non autorisées ou pour prouver un fait allégué. La complexité de la preuve électronique et le besoin d'en assurer le plus haut niveau d'intégrité requiert que seuls des experts en informatique judiciaire puissent procéder à l'identification de la meilleure preuve et remplir les objectifs de ces enquêtes.

Afin d'assurer la valeur probante de la preuve électronique recueillie et de faire face à toute prétention à l'effet que celle-ci n'a pas été obtenue conformément aux règles de l'art, OKIOK dispose de tout le matériel spécialisé, tel que :

- Duplicateurs de média (ex. : Tableau, TD2)
- Outils spécialisés d'analyse en informatique judiciaire (ex. : Encase, Guidance Software)
- Outils d'analyse cryptographique (ex. : Extreme GPU Bruteforcer, Hashcat, Proactive System Password Recovery, Elcomsoft)
- Outils spécialisés au domaine technologique ciblé (ex. : vidéo, audio, etc.)
- Outils de capture en temps réel de données (Live Forensics)

Par ailleurs, les clients d'OKIOK peuvent compter sur une équipe d'experts qui possèdent les formations et les certifications suivantes :

- Encase Certified Examiner (EnCE)
- Certified Information Systems Security Professional (CISSP)
- Maîtrise en sécurité des réseaux informatiques
- Baccalauréat en droit (LL.B.)
- Maîtrise en droit des technologies de l'information (LL.M.)
- Baccalauréat et maîtrise en génie informatique
- Network Penetration tester (GPEN)

## Services offerts

1. Expertise technique lors de perquisitions informatiques
2. Identification et corrélation de traces
3. Analyse de l'intégrité de données (fichiers, vidéo, audio, image, etc.)

4. Analyse de preuve présentée au soutien de procédures judiciaires

- Intégrité, fiabilité et authenticité de la preuve
- Failles/limites
- Meilleure preuve

5. Prise de copies sécurisées

- Disques durs
- Fichiers individuels
- Médias mobiles

6. Déchiffrement de clés

7. Analyse d'appareils mobiles

8. Anti-forensics

9. Analyse de courriels litigieux

- Identification de la source réelle
- Modification du contenu (métadonnées, corps du texte)

10. Détection de logiciels malveillants

- Logiciels espions
- Fonctionnalités dérobées

## Préservation de la preuve et expertise

La preuve identifiée par nos spécialistes est traitée selon une méthodologie précise de manière à assurer sa confidentialité, son intégrité et sa fiabilité tout au long des étapes de son traitement jusqu'à la présentation des résultats.

Outre ces procédures strictes, la preuve est analysée et conservée dans nos laboratoires d'expertises isolés et protégés par des contrôlés d'accès, des coffres-forts et des équipements de transports hautement sécurisés. Ainsi, toute preuve obtenue par nos experts respecte les exigences de recevabilité de la preuve prescrites notamment à la Loi concernant le cadre juridique des technologies de l'information.

Nos professionnels sont reconnus à titre de témoins-experts devant les tribunaux et peuvent présenter leurs conclusions sous forme de rapports écrits, de présentations et de témoignages devant les instances civiles, pénales et criminelles, le cas échéant.

Les marques de commerce appartiennent à leurs propriétaires respectifs.

**OKIOK est un chef de file en matière de sécurité informatique.** Depuis 1973, OKIOK se démarque par l'excellence de ses produits et la qualité de ses services. OKIOK offre une vaste gamme de solutions intégrées conçues pour répondre aux besoins des entreprises de toutes tailles.

