Analyse des compromissions de documents PDF

Daniel Mouly – Expert près la Cour d'Appel de Bordeaux
CNEJITA – Groupe Pénal
JFC 25 septembre 2018

Sommaire

- Réputation des documents PDF
- Conjoncture favorable à la fraude
- Exemples concrets de fraudes
- Outils pour l'investigateur numérique

Réputation des documents PDF

- Perception du public
  - Documents sûrs
  - Documents inaltérables
  - Confiance généralisée
- Réalité
  - Faciles à forger
  - Potentiellement porteurs de charge virale
  - Pas vraiment dignes de confiance sauf si signés numériquement par certificat vérifiable

Conjoncture favorable à la fraude

- Vers un monde numérique
  - Relations avec les administrations
  - Factures électroniques
  - Banque électronique
- Naïveté des interlocuteurs
  - Cf. réputation du format PDF
  - Méconnaissance des principes d'une vraie signature numérique
- Disponibilité des outils
  - Éditeurs de PDF
  - Photoshop

Exemples concrets de fraudes

- Documents à destination du Greffe du TC
  - Fausses signatures d'associés
- Documents douaniers
  - Construction complexe
  - Récupération d'extraits de documents légitimes
  - Montage Photoshop
  - Génération du PDF par Word

Outils pour l'investigateur numérique

- Connaissance du format interne des PDF
  - Mélange texte et binaire, tags, objets : COS (Carousel Object Structure)
  - https://en.wikipedia.org/wiki/PDF
  - http://www.planetpdf.com/developer/article.asp?ContentID=navigating_the_internal_struct&page=0
- Outils Python
  - pdfid
  - pdfparser
  - peepdf
- Qpdf
- Xpdf-tools
- exiftool
- Et aussi
  - Acrobat avec le plugin CanOpener
  - Un œil attentif