



Forensics / criminalistique :
avant l'analyse... la « perquiz »

Paris, 1^{er} décembre 2010

Evénement organisé en partenariat avec :

Orange Business Services

TelecityGroup





Le CLUSIF : *agir pour la sécurité de l'information*

Association **sans but lucratif** (création au début des années 80)

> 600 membres (pour 50% fournisseurs et prestataires de produits et/ou services, pour 50% RSSI, DSI, FSSI, managers...)

Partage de l'information

Echanges homologues-experts, savoir-faire collectif, fonds documentaire

Valoriser son positionnement

Retours d'expérience, visibilité créée,
Annuaire (Formations, Membres Offreurs)



*Logo pour vos actions commerciales,
votre site web*

Anticiper les tendances

Le « réseau », faire connaître ses attentes auprès des offreurs

Promouvoir la sécurité

Adhérer...

Groupes de travail en progression

Les groupes actifs en 2010

- Annuaire des Formations SI
- DDoS
- Documentation de MEHARI™
- Fiches de sécurité pour la micro-informatique
- Gestion des incidents
- Guide d'audit de sécurité physique
- Infogérance
- Menaces Informatiques et Pratiques de Sécurité en France (Edition 2010)
- Panorama de la cybercriminalité
- PCI-DSS
- Principes, mécanismes et bases de connaissances de Méhari
- Sécurité des Applications Web - Suite
- Série 27000 / Métriques
- Virtualisation et Sécurité

... et des Espaces dédiés

Espaces de travail actifs en 2010

- Espace Méthodes
- Espace Menaces
- Espace RSSI

Deux autres GT en annonce prochaine...

*« Democracy means that
if the doorbell rings in the early hours,
it is likely to be the milkman »*

W. Churchill

Nous allons voir un cas de figure où ce
n'est pas le laitier, tout en restant dans
les règles de la démocratie

Forensics et cybermondanités

Tout Geek qui « triture un peu l'octet » se présente aujourd'hui comme *forensics*, peut-être en omettant la partie « protocole d'expertise »

- 👉 Des affaires mémorables (aux E-U) où les pièces deviennent irrecevables par modification des dates d'enregistrement...
- 👉 Analyse post-mortem du disque dur

La recherche de la « preuve numérique »... une sorte de Saint Graal de l'Expert informatique ?..

Forensics/Criminalistique : cadre d'emploi (entre autres)

Pas une finalité en soi !.. mais :

- ☞ Historiser
- ☞ Environner
- ☞ Orienter ou exclure une option de recherche

Avec une montée en puissance :

- ✓ Indice
- ✓ Faisceau d'indices à valeur probante
- ✓ Preuve
- ✓ Intime conviction

Les prémisses...

Vous sollicitez une intervention

Vous êtes sollicité de façon impromptue...

- ✓ Cybercriminalité
- ✓ Plus largement, terrorisme, homicide...
 - ☞ Recherche de vidéos
 - ☞ de correspondances électroniques

Avant toute analyse

- ✓ Recueillir
- ✓ Geler et préserver les éléments

Pour cela, la perquisition éventuellement suivie d'une saisie...

Intervenants

☞ Cadre légal, télé-perquisition

Capitaine Olivier NAEL

✉ Section Technique – OCLCTIC
olivier.nael@interieur.gouv.fr

☞ Rôle de l'avocat

Me Garance MATHIAS

✉ Avocat au Barreau de Paris
garance@gmathias.ath.cx

☞ Témoignage...

M. Eric GROspeILLER

✉ FSSI – Ministère de l'Emploi, du Travail et de la Santé
eric.grospeiller@sante.gouv.fr

☞ Les recommandations !

Chef d'Escadron Laurent LESOBRE

✉ IRCGN/DCIN/INL - Gendarmerie Nationale
laurent.lesobre@gendarmerie.interieur.gouv.fr