



FORENSICS / CRIMINALISTIQUE
Conférence CLUSIF
1^{er} décembre 2010

Synthèse et recommandations

Plan

- 1) Synthèses
- 2) Quelques supports!
- 3) Exemple concret
- 4) Recommandations générales



Synthèses

La perquisition:

- En tant que victime
 - Préservation de la preuve numérique.
 - Gèle des matériels informatiques.
 - Dépôt de plainte auprès des forces de l'ordre.
 - Tous éléments permettant d'aider l'enquête.
 - Immobilisation partielle de l'entreprise le jour de la perquisition.



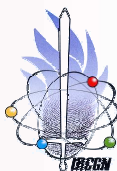
Synthèses

La perquisition:

- Les autres cas
 - Gèle de l'entreprise pour garantir la préservation de la preuve numérique.
 - Mise à disposition de personnes spécialisées (administrateur réseaux, etc..).
 - Mise sous scellés
 - Remise en fonction de l'entreprise



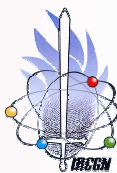
Auriez-vous pensé à...?



Exemple concret

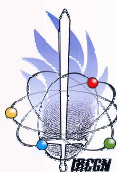
Vol d'un ordinateur dans un secrétariat d'un hôpital

- Gèle des lieux
- Identification du matériel volé
- Recherche des différents logs de connexions
- Constatations générales
- Conclusions.



Recommandations générales

- La préservation de la preuve numérique
- Les logs
- La gestion de l'administrateur du réseaux
- La gestion du parc informatique
- Les mises sous scellés judiciaires
- Conclusion



CONTACT

Chef d'Escadron Laurent LESOBRE

IRCGN/DCIN/INL - Gendarmerie Nationale

✉ laurent.lesobre@gendarmerie.interieur.gouv.fr

IRCGN

Département: Informatique Electronique

Tél: 01 58 66 50 30

Fax: 01 58 66 50 27

inl.ircgcn@gendarmerie.interieur.gouv.fr

