Recueil et analyse de la preuve numérique

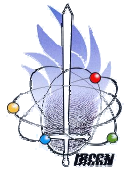
SSTIC 2008

Nicolas DUVINAGE

Chef du département informatique-électronique

Institut de recherche criminelle de la gendarmerie nationale

Accréditation Cofrac n°1-1916 – Portée disponible sur www.cofrac.fr



PLAN

- Introduction

- Définition et recueil de la preuve numérique
- Exploitation de la preuve numérique
- Interprétation de la preuve numérique

- Conclusion: (ébauche de) conduite à tenir pour les RSSI qui découvrent une infraction dans leur périmètre de responsabilité

INTRODUCTION

- L'image d'Epinal du « forensic numérique »…
  - *Exploit 0-day*, vulnérabilités routeurs Cisco IOS
  - Hackers communiquant par canaux cachés
  - Debian avec *kernel* recompilé « maison », disques durs chiffrés PGP, techniques d'*anti-forensics*
  - Compromission de serveurs de la NSA

INTRODUCTION

- La réalité…
  - (Très) peu d'affaires judiciaires relatives à des intrusions/compromissions…
    - …et utilisation de vulnérabilités bien connues!
  - Communication par email et clients de *chat* (MSN…)
  - Windows à 90%, (très) peu de chiffrement (MS Office, zip, rar protégés par mdp…)

INTRODUCTION

- Pourquoi une telle différence???
  - Crimes et délits les plus fréquents
    - Vols, escroqueries, abus de confiance, abus de biens sociaux, détournements de fonds, faux et usage de faux
    - Trafic de stupéfiants, trafic de véhicules volés, trafic d'armes, trafic d'antiquités volées
    - Violences, homicides, viols
  - Eléments de preuve
    - ADN, empreintes digitales…
    - …et la preuve numérique ?!

INTRODUCTION

- 3 grandes familles de crimes et délits
  - Crimes et délits où l'objet numérique est utilisé de façon « accessoire »
    - Stupéfiants (échange de SMS), détournement de fonds (fichiers de comptabilité), etc
  - Crimes et délits où l'objet numérique est utilisé de façon principale
    - Contenus illicites sur Internet (pédopornographie, diffamation, xénophobie…), etc
  - Crimes et délits où l'objet numérique est l'objet-même de l'infraction
    - Atteintes aux STAD, contrefaçon carte bancaire, etc

INTRODUCTION

- 3 grandes familles de crimes et délits
  - Dans les 3 cas l'objet numérique peut contenir des données intéressantes (voire vitales…) pour l'enquête
  - Dans les 2 premiers cas les connaissances technologiques requises sont nulles/faibles de la part du délinquant
  - Dans tous les cas le travail d'analyse de la preuve doit être scientifique et indiscutable

DEFINITION ET RECUEIL DE LA PREUVE NUMERIQUE

DEFINITION DE LA PREUVE NUMERIQUE

- Qu'est-ce que la preuve numérique?
  - Tout élément matériel ou immatériel…
    - Disque dur, téléphone GSM, etc
    - Fichier-utilisateur, logs, etc
  - …recueilli et analysé
    - dans le respect de la législation en vigueur
    - conformément à « l'état de l'art technique » du moment
  - …apportant un indice
    - disculpant
    - incriminant
    - autre (corroboratif, informatif…)

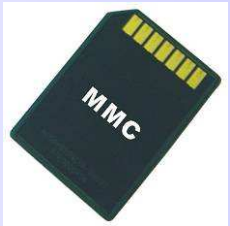
DEFINITION DE LA PREUVE NUMERIQUE

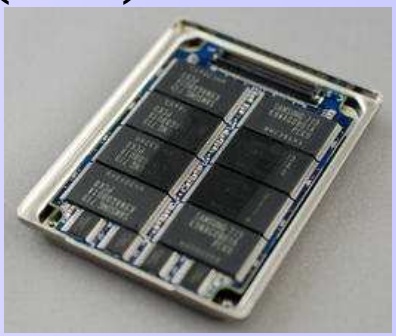
- En pratique: supports de stockage numérique de tous formats et de toutes interfaces (1/3)
  - Magnétique
    - disques durs (ESDI/IDE/SATA/SCSI/ZIF, 1’’-1.8’’-2.5’’-3.5’’…)
    - disquettes (3’’1/2-5’’1/4)
    - bandes et cartouches (DAT, ZIP, JAZ, Tandberg…)
    - cartes à piste magnétique (CB, cartes fidélité…)

MINISTÈRE DE LA DÉFENSE

DEFINITION DE LA PREUVE NUMERIQUE

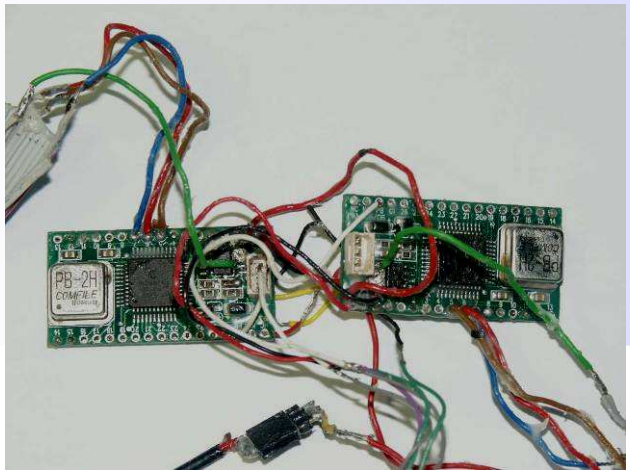
- En pratique: supports de stockage numérique de tous formats et de toutes interfaces (2/3)
  - Mémoire Flash
    - clés USB, disque dur SSD
    - cartes à mémoire (SD/MMC/CF…)
    - mémoire interne téléphone GSM/PDA/GPS
    - lecteurs MP3/iPOD, dictaphones





DEFINITION DE LA PREUVE NUMERIQUE

- En pratique: supports de stockage numérique de tous formats et de toutes interfaces (3/3)
  - Optique: CD/DVD, DVD-RAM, BluRay
  - Magnéto-optique (rare): HiMD
  - Microcontrôleurs: cartes à puce (CB, SIM, carte Vitale, etc), skimmers



MINISTÈRE DE LA DÉFENSE

DEFINITION DE LA PREUVE NUMERIQUE

- En pratique: fichiers pouvant être stockés chez des tiers qui n'ont aucune complicité avec le suspect
  - Logs des FAI (ex.: Alice) et des FSI (ex.: Yahoo!)
  - Logs des opérateurs de téléphonie fixe/mobile
  - Serveurs de la société qui emploie le suspect

RECUEIL DE LA PREUVE NUMERIQUE

- Modalités de recueil
  - « Collecte directe »
    - Déplacement physique des enquêteurs, perquisitions et saisies chez le suspect
  - « Collecte indirecte »
    - Envoi par les enquêteurs (courrier, fax, email) de réquisitions judiciaires à un tiers qui détient des éléments de preuve relatifs au suspect
    - C'est le tiers qui « apporte sur un plateau » les éléments de preuve aux enquêteurs, sans que ceux-ci n'aient rien à faire

RECUEIL DE LA PREUVE NUMERIQUE

- Défis et difficultés (1/2)
  - La preuve numérique intervient potentiellement dans toute enquête…
    - …mais les enquêteurs spécialisés ne peuvent pas se déplacer partout en même temps!
  - La preuve numérique peut être stockée sur un serveur distant

  - La preuve numérique peut revêtir une extrême variété de formes…
    - …encore faut-il les reconnaître et les trouver!

RECUEIL DE LA PREUVE NUMERIQUE

- Auriez-vous pensé à…?

RECUEIL DE LA PREUVE NUMERIQUE

- Défis et difficultés (2/2)
  - Ordinateur allumé: comment l'éteindre?
    - Extinction « propre » ou arrachage prise électrique?
    - Capture RAM avant extinction? (oui/non/dans quels cas?)
    - Le transporter sans l'éteindre?
  - Téléphone GSM et SIM en fonctionnement
    - Extinction avec risque de non accès ultérieur à la SIM (PIN/PUK)?
    - Non-extinction et risque de recevoir un flot d'appels/SMS écrasant la mémoire?
    - Transport dans une cage de Faraday?

EXPLOITATION DE LA PREUVE NUMERIQUE

EXPLOITATION DE LA PREUVE NUMERIQUE

- L'exploitation ne doit pas modifier l'élément de preuve
  - Afin de rendre indiscutables les résultats trouvés (pas de données ajoutées ou effacées par l'expert)
    - Ex.: polémique sur l'analyse des supports informatiques des guérilléros des FARC en Colombie
  - Une contre-expertise doit permettre de retrouver les mêmes résultats

EXPLOITATION DE LA PREUVE NUMERIQUE

- Mais…
  - Booter un OS suspect modifie de nombreux logs (ex.: journaux d'événements Windows)
    - Ces logs peuvent être directement utiles à l'enquête (ex.: date/heure de dernière extinction de la machine dans une affaire d'homicide)
    - Même s'ils sont inutiles: leur modification peut écraser des données utiles

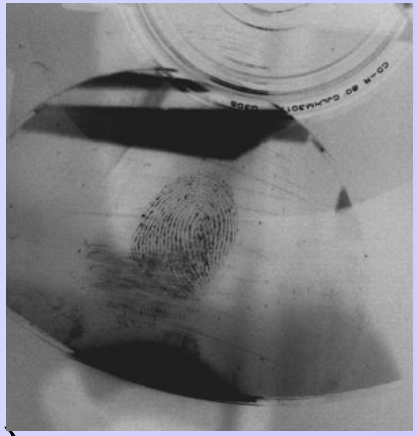
EXPLOITATION DE LA PREUVE NUMERIQUE

- Mais…
  - Accéder à un disque dur « monté en esclave » présente des risques (même sous Linux…)
    - Modification des dates d'accès aux fichiers
    - Prise de swap
    - Sous Windows: répartition automatique de la corbeille (\Recycler) et des points de restauration (\System Volume Information) sur tous les disques durs
    - Déplacement de disques en RAID vers une autre unité centrale
  - Sans compter les risques de pannes matérielles!

EXPLOITATION DE LA PREUVE NUMERIQUE

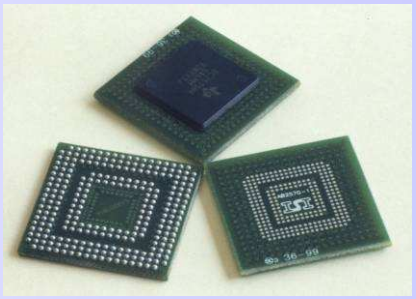
- Alors que faire? Travailler sur une copie bit à bit intégrale de l'original!
  - Copie réalisée à l'aide d'un bloqueur matériel en écriture (ex.: www.tableau.com)
  - Copie réalisée sous Linux (dd et variantes: dcfldd, rdd…) « avec les bonnes options de montage »
    - Mount –ro –noswap –noatime –noexec –nodev
    - …et sans confondre disque source et disque destination!
  - Désactivation des compteurs SMART et du G-List Remapper? (ex.: outil Deepspare Imager)

EXPLOITATION DE LA PREUVE NUMERIQUE



- Problèmes pouvant survenir lors de la copie
  - Ordre des examens scientifiques successifs (ex.: ADN, empreintes digitales…)?
  - Connectique/lecteur trop ancien, trop rare (ou trop récent!) (ex.: bandes magnétiques)

  - Connectique ou protocole ne supportant pas la copie bit à bit (ex.: port COM, source TWAIN, commandes AT, OBEX, ActiveSync)
  - Copie bit à bit nécessitant une modification de l'original (ex.: dessoudage d'une mémoire Flash BGA)
  - Secteurs défectueux
  - Supports physiquement endommagés ou en panne
  - Norme ATA: HPA, DCO, Security Mode
  - Reconstruction des configurations RAID



EXPLOITATION DE LA PREUVE NUMERIQUE

- Analyse de la copie
  - Il existe des outils d'analyse semi-automatique avec GUI des systèmes de fichiers les plus courants (FAT12/16/32, NTFS, HFS/HFS+, Ext2/Ext3, ISO9660, UDF…)
    - Reconnaissance/montage des partitions (y compris cachées ou effacées), listing/affichage des fichiers (y compris système, *hidden* et si ACL)
    - Recherche de fichiers effacés, analyse du *slack*
    - « Déconstruction » automatique des formats de fichiers les plus courants (décompression archives, traitement des emails type Outlook Express .dbx ou Outlook .pst…)

EXPLOITATION DE LA PREUVE NUMERIQUE

- Analyse de la copie
  - Problèmes techniques
    - Systèmes de fichiers « classiques » mais corrompus
    - Systèmes de fichiers liés à des OS rares (Novell Netware, SCO System V, QNX, Solaris…)
    - Formats de stockage/compression des données sur les bandes magnétiques
    - Systèmes de fichiers propriétaires des téléphones GSM (TFS4, GDFS, HAFSFAT, Calypso, KFAT…)
    - Absence de système de fichiers (ex.: disques durs de vidéosurveillance)

EXPLOITATION DE LA PREUVE NUMERIQUE

- Analyse de la copie
  - Problèmes non techniques
    - « Chercher toute donnée utile à l'enquête en cours » : vaste programme!
    - Mise à disposition des données/fichiers dans un format « ouvrable par double-clic » par un programme grand public
      - Extraits de bases de données « CIEL comptabilité » en PDF
    - Mise à disposition des données/fichiers sur un support physique lisible par les juges
      - Pas de lecteurs DVD dans certains tribunaux!
      - Certains juges exigent que l'expert imprime tous les fichiers (y compris les vidéos, sous forme de vignettes successives)…

EXPLOITATION DE LA PREUVE NUMERIQUE

- Analyse de la copie
  - Problèmes non techniques
    - Volumes de données croissants (disques durs d'1 To) *vs.* temps accordé pour l'analyse non croissant (de 24-48h à plusieurs semaines)
      - Problématique du tri des images/vidéos (pédopornographie)
      - Problématique des recherches indexées/par mot-clé

INTERPRETATION DE LA PREUVE NUMERIQUE

INTERPRETATION DE LA PREUVE NUMERIQUE

- Il ne suffit pas d'extraire des fichiers ou des données…(1/2)
  - Il faut les mettre en perspective, les relier les uns aux autres et au reste de l'enquête
    - Ex.: l'utilisation des mots-clés « hack phpbb » sur Google par le suspect est-elle compatible avec le fait qu'il déclare ne pas avoir de connaissances techniques en informatique?
    - Ex.: comment expliquer que la date de modification du fichier Word « test.doc » soit antérieure à sa date de création? Quelles conséquences cette observation a-t-elle?

INTERPRETATION DE LA PREUVE NUMERIQUE

- Il ne suffit pas d'extraire des fichiers ou des données…(2/2)
  - Il faut les expliquer et les rendre intelligibles pour un non-spécialiste (le juge, les jurés de la Cour d'Assises, etc)
    - ⇒ Tout les membres majeurs de votre famille sont-ils capables de comprendre les phrases suivantes et leurs conséquences?
    - Ex.: « la perquisition a mis en évidence la présence d'un Access Point WiFi sécurisé en WEP »
    - Ex.: « son client MSN était configuré pour logger par défaut tous les *chats* avec sa *buddy-list* »

INTERPRETATION DE LA PREUVE NUMERIQUE

- Il faut exprimer clairement les limites de fiabilité de son analyse (1/3)
  - Les dates/heures indiquées (M.A.C. times, logs…) permettent de reconstruire une séquence d'événements…
    - …mais quid si la date/heure système a été modifiée (éventuellement plusieurs fois de suite avant d'être remise à l'heure)?

INTERPRETATION DE LA PREUVE NUMERIQUE

- Il faut exprimer clairement les limites de fiabilité de son analyse (2/3)
  - Le fichier « je vais la tuer.doc » a été trouvé dans le répertoire « Mes documents » de l'utilisateur « Toto »
    - Peut-on assurer pour autant que Toto était derrière l'écran et le clavier ?
      (ex.: absence de mot de passe de session, session ouverte non verrouillée, mot de passe connu de toute la famille/de tous les collègues, etc)
    - S'il l'était, est-il pour autant l'auteur de ce document?
      (ex.: enregistrement en local d'une pièce jointe d'email reçu d'un tiers)

INTERPRETATION DE LA PREUVE NUMERIQUE

- Il faut exprimer clairement les limites de fiabilité de son analyse (3/3)
  - Les fichiers et traces trouvés sont-ils issus d'un comportement volontaire (=> infraction) ou involontaire (=> absence d'infraction)?
    - Ex.: « je viens porter plainte pour piratage car j'ai une facture de téléphone de 2.500 euros ce mois-ci »
      - *Dialer* sur le PC ou plaignant de mauvaise foi qui ne souhaite pas payer ses appels Audiotel surtaxés?
    - Ex.: images pédopornographiques dans le cache web
      - Consultation volontaire de sites illicites ou *pop-ups* lors de navigations pornographiques licites?

CONCLUSION: (ébauche de) conduite à tenir pour les RSSI qui découvrent une infraction dans leur périmètre de responsabilité

QUELQUES CONSEILS…

- « Les RSSI qui découvrent une infraction… »
  - Vous découvrez ce que vous pensez/supposez être une infraction…
  - …mais vous n'êtes pas magistrat!
    - …ce n'est pas forcément une infraction
    - …et même si c'en est une, le suspect n'est pas forcément celui que l'on croit (ex.: poste de travail partagé, *trojan*, etc)
    - …et même si c'est bien lui, il n'est pas forcément coupable (ex.: comportement involontaire)
    - …et même s'il l'est pour tout le monde, il ne sera pas forcément condamné (ex.: absence de preuves suffisantes, vice de procédure, etc)

QUELQUES CONSEILS…

- De fausses accusations (même énoncées de bonne foi et sans intention de nuire) peuvent avoir de lourdes conséquences
  - Il est plus facile de détruire une réputation en 5 minutes que de la reconstruire
    - …même s'il est prouvé que la personne est innocente
      - « Il n'y a pas de fumée sans feu »
      - Les accusations de pédophilie sont souvent indélébiles
  - Pour le suspect
    - Risque de mise à pied ou de licenciement
    - Risque de rupture conjugale, de suicide (pédophilie)
    - Méfiance de l'entourage, de la famille, des amis, des collègues

QUELQUES CONSEILS…

- Conseil n°1: PRUDENCE et DISCRETION
  - Ne pas alerter toute l'entreprise
    - Se contenter (par exemple et selon la taille de l'entreprise) du responsable juridique et du directeur du site
    - Attention aux éventuelles complicités internes
  - Laisser faire les spécialistes du droit
    - Signaler les faits à la gendarmerie/police
  - Ne pas porter de jugement hâtif sur l'intéressé (lui laisser le bénéfice du doute et la présomption d'innocence)

QUELQUES CONSEILS…

- Pour autant, il faut réagir!
  - Conseil n°2: tout en respectant le droit du travail et les libertés fondamentales de la personne
    - Pas d'analyse des fichiers personnels privés du PC du suspect
      (cf. « arrêt Nikon » de la Cour de Cassation)
    - Pas de « perquisition » dans son vestiaire, dans ses tiroirs en son absence

QUELQUES CONSEILS…

- Pour autant, il faut réagir!
  - Conseil n°3: préserver les éléments de preuve
    - Remplacer le PC suspect par un autre PC
      (ex.: en prétextant une maintenance, une mise à jour, un problème de sécurité)
      (ex.: au pire, en prétextant une infraction moins infamante que la pédophilie [piratage, escroquerie…])
    - Extraire/graver les fichiers issus de serveurs
      (ex.: logs gravés sur CD)

QUELQUES CONSEILS…

- Pour autant, il faut réagir!
  - Conseil n°3: préserver les éléments de preuve
    - Si vous avez impérativement besoin de faire des analyses: réaliser une copie bit à bit des supports mis de côté (cf. diapos 19 à 22) et n'analyser que ces copies
    - Conserver les supports mis de côté dans un endroit sûr (ex.: coffre-fort) en attendant de les donner à la gendarmerie/police

MERCI DE VOTRE ATTENTION!

nicolas.duvinage@gendarmerie.defense.gouv.fr

NOUS AUSSI NOUS AVONS BESOIN DE VOUS!

- Etudiants, profs, écoles d'ingénieurs, universités
- Stages de 2 à 6 mois à Rosny-sous-Bois
  - Non rémunérés ☹
  - Chez « Les experts » ☺
- Projets
  - Exemples
    - Projets scientifiques collectifs (PSC) de l'Ecole Polytechnique
    - Projets de fin d'études (PFE) de l'EPITA/EPITECH