

COMPLI 73R

FOR 3N5105

- ANALYSE
- INVESTIGATION
- EXPERTISE
- INTERPRÉTATION

M&O

COMPU7ER F0R3N51C5

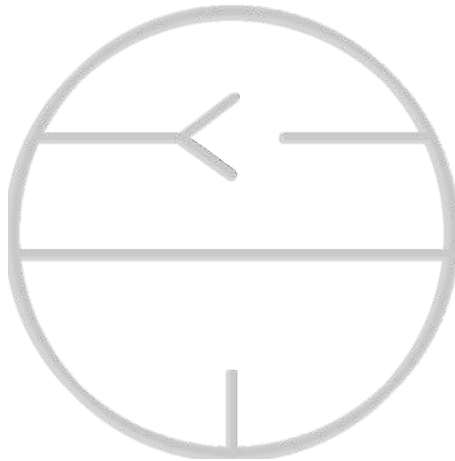
Note technique - Procédure et Méthodologie de l'Inforensics.

Cette documentation n'a pas pour vocation de donner un cours sur l'investigation numérique, mais se considère plus comme une approche sur les différentes étapes qui jalonnent l'expertise judiciaire en informatique.

Pas d'exhaustivité, pour la simple et bonne raison que les techniques d'analyse évoluent constamment, les outils se développent régulièrement et que je ne voudrais pas paraître chauvin sur telle ou telles applications.

De ce fait, la méthodologie ainsi que les outils de base d'un expert seront survolés dans les différents chapitres de cette note technique.

Technicien d'Investigation Numérique
Mikaël BONTEMPS



COMPUTER FOR3N51C5

SOMMAIRE

1. LES MANDANTS

- 1.1 Réquisition Judiciaire 6
- 1.2 Ordonnance de commission d'Experts 7

2. DECRIRE L'ETAT DES SCELLES

- 2.1 Photo scellé fermé 8
- 2.2 Ouverture de scellé et description visuelle 8
- 2.3 Tableau inventaire 9

3. COPIE PHYSIQUE ET/OU IMAGE DU OU DES SUPPORTS

- 3.1 Extraction du ou des supports disques durs 10
- 3.2 Clone avec le copieur IM SOLO 4 FORENSIC IMAGER 10
- 3.3 Copie sous Linux 12
- 3.4 Copie sous un système Microsoft Windows 14
- 3.5 Montage d'une image 19
- 3.6 Virtualisation d'une image 22
- 3.7 Travail en urgence 24

4. INVESTIGATION ORDINATEUR

- 4.1 Extraction binaire ENCASE V3 31
- 4.2 Analyse Logs et Datation 32
 - 4.2.1 Journaux événements système (Log Parser ; Evtvpt.pl ; RtCA) 32
 - 4.2.2 Identification matériel et système 33
 - 4.2.3 Commande Linux 37
- 4.3 Analyse des données 38
 - 4.3.1 Logique (résident) 38
 - 4.3.2 Analyse de la base de registres 39
 - 4.3.3 Physique (effacé) Carving 41
- 4.4 Recherche par mot clé 43
 - 4.4.1 Sous Encase 43
 - 4.4.2 Sous Microsoft Windows 45
- 4.5 Traces Internet 48
 - 4.5.1 Navigateur Internet PC 48
 - 4.5.2 Navigateur Safari MAC 53

COMPUTER FORNSICS

4.6	Images	54
4.6.1	Recherche par extension et/ou signature numérique	54
4.6.2	Analyse photo et des métadonnées	55
4.7	Vidéos	64
4.8	Audio	70
4.9	Messagerie	71
4.9.1	Recherche par extension	71
4.9.2	Reconstruction de Mails	73
4.10	Extraction des comptes utilisateurs et autres mots de passe	74
4.10.1	Cain & Abel	74
4.10.2	Casser du mot de passe	76
4.10.3	OSForensics	83
4.10.4	Recherche fichiers verrouillés	85
4.10.5	Récupération d'autre mot de passe	86
4.10.6	Backup téléphone (Iphone ; Samsung ; Sony)	87
5.	INVESTIGATION TELEPHONE	
5.1.	Mode Avion	93
5.2.	Copie physique de la carte mémoire SD	94
5.3.	Clone de la carte SIM et export des données	96
5.4.	Extraction des données d'un Smartphone avec XRY	98
5.5.	Analyse des données XRY avec SPOTLIGHT	100
5.6.	Vérif. des bases de données SQL XML PLIST...	102
5.7.	Dessoudage de composants (CHIP-OFF)	104
6.	LISTE DES OUTILS (LIBRE ; PAYANT ; LIVE)	
6.1.	Liste non exhaustive des outils que l'expert peut être amené à utiliser	105
6.2.	Live CD-ROM (pour les plus connus)	108