

Introduction

Introduction

Pourquoi avoir besoin et qu'est ce le forensique / cadre légal / Explique comment nous collectons des preuves (on peut reprendre pdf du prof) -> utilisation de certains outils ect ..

Explication de pq garder les preuves

Commencer les dump / prendre l'heure checksum afin de montrer pour le screen / archive non compressé

> Analyse des preuves / disques & retrouver les informations et pq c interessant de les récup
On peut faire du file carving -> récup d'info meme si pas sur le fdisk

Analyse avec volatility montrer le début & l'image dcu truc montrer toute les analyses / version de windows par exemple on peut récup la version complète il ny a pas que les clefs de registre

A la fin de l'analyse on vérifie si les hash sont toujours bon et on le montre une fois analyse fait -> conclusion & conclu general en forensique du pc

Revision #1

Created 4 February 2025 13:25:10 by Admin

Updated 27 February 2025 07:34:44 by Admin