Travaux pratiques

Digital forensics

Exercice 3: Cold case (le pilote de la série)

Une machine Linux que vous administrez a subi un incident. Après examen des fichiers de log, il semble que tout soit arrivé après qu'Henri (un sinistre élève de SEOC) ait connecté une clef USB à la machine. Heureusement quelqu'un a pu faire une image `usb.dd` de cette clef USB. À vous de jouer !

Question 6 Que contient cette clef USB ?

Question 7 À votre avis quelles sont les commandes qu'a e□ectuer Henri ? Qu'est-il arrivé à la machine ?