DFIR ORC est un logiciel de collecte de données Forensiques (DFIR) éprouvé

Pour faire face à des incidents d'un genre nouveau,
les « Advanced Persistent Threats » (APTs), apparus il y a près de 10 ans,
l'ANSSI a dû adapter sa méthodologie de traitement ainsi que son outillage.

DFIR ORC est directement issu de cette démarche et n'a cessé de se développer depuis pour s'adapter aux besoins en matière d'investigation et de réponse à incident.

Créé et utilisé de longue date par les équipes de l'ANSSI, le logiciel de collecte DFIR ORC regroupe un ensemble d'outils qui permettent la recherche, l'extraction et la mise à disposition des données forensiques.

Il a été entièrement conçu afin de fonctionner dans l'écosystème Microsoft Windows de façon décentralisée et à grande échelle.

« Après 8 ans d'usage, DFIR ORC a été utilisé sur plus de 150 000 postes dans le cadre de nos activités opérationnelles en matière de réponse à incident. » François Deruty, sous-directeur Opérations de l'ANSSI.

En s'engageant dans une démarche d'ouverture avec la communauté de la sécurité numérique, l'ANSSI souhaite aujourd'hui partager cet outil mature qu'elle utilise au quotidien depuis plusieurs années*.

Source