Digital investigation for maritime systems : a global approach

Type de contenu : Texte

Titre(s) : Digital investigation for maritime systems : a global approach / Yunan Dutertre / Gabriel Flotté ; Tuteur de projet : David Brosset ; Organisme d'accueil : Ecole Navale

Editeur, producteur : Ecole Navale (PDS), 2023

Adresse bibliographique : : Ecole Navale (PDS), 2023

Description matérielle : 46 p. ; 29,7 cm

Résumé ou extrait : Les données numériques jouent un rôle crucial dans les enquêtes maritimes, en particulier parce que les navires modernes sont équipés de systèmes électroniques avancés et de protocoles de communication tels que NMEA et Siemens S7, permettent l'échange et le contrôle des données en temps réel. Les Voyages Data Recorder (VDR) sont des outils inestimables dans les enquêtes sur les accidents,enregistrant une multitudes de données. Ils sont comparables aux "boîtes noires" des avions, enregistrant des données provenant de divers capteurs à bord d'un navire. La préservation rapide des données du VDR après un incident maritime est d'une importance capitale, car elles sont d'une valeur immense pour les enquêtes. Une fois entre les mains des experts en criminalistique numérique, une gamme de logiciels est à leur disposition pour l'analyse des médias numériques, chacun étant adapté à des branches spécifiques de la criminalistique. Deux outils notables sur lesquels nous nous concentrerons sont Autopsy et Wireshark. Autopsy, une solution open-source, est conçue pour la récupération de fichiers, la recherche de fichiers, l'analyse chronologique, l'examen du registre et la génération de rapports. D'autre part, Wireshark, également open-source, est un analyseur de protocole réseau capable de capturer et de disséquer des paquets de données au sein des réseaux informatiques. Il est important de noter que, dans leurs configurations par défaut, ces applications logicielles ne sont pas en mesure de traiter les données NMEA maritimes. Alors qu'un disséqueur NMEA pour Wireshark est déjà disponible sur GitHub, nous avons dû développer un module pour Autopsy afin de lui permettre de détecter les fichiers contenant des données NMEA. Une fois ces fichiers NMEA acquis, les enquêteurs peuvent utiliser le plugin VDR sur OpenCPN pour rejouer et visualiser les données de navigation sur une carte. Afin de garantir aux enquêteurs une plateforme de criminalistique numérique prête à l'emploi, nous avons pris l'initiative de créer une machine virtuelle basée sur Debian 12 équipée d'Autopsy, Wireshark et OpenCPN, avec les plugins maritimes nécessaires déjà installés.