Reconstruction et analyse sémantique de chronologies cybercriminelles

Yoan Chabot[*,**], Aurélie Bertaux[**], Tahar Kechadi[*], Christophe Nicolle[**]

[*]School of Computer Science and Informatics, University College Dublin, Ireland
yoan.chabot@ucdconnect.ie
[**]Equipe CheckSem, Laboratoire Le2i, UMR CNRS 6306,
Faculté des sciences Mirande, 21078 Dijon, France
http://checksem.u-bourgogne.fr

Résumé. La reconstruction de chronologies d'évènements cybercriminels (ou reconstruction d'évènements) est une étape primordiale dans une investigation numérique. Cette phase permet aux enquêteurs d'avoir une vue des évènements survenus durant un incident. La reconstruction d'évènements requiert l'étude d'importants volumes de données en raison de l'omniprésence des nouvelles technologies dans notre quotidien. De plus, les conclusions produites se doivent de respecter les critères fixés par la justice. Afin de répondre à ces challenges, nous proposons une nouvelle méthodologie basée sur une ontologie permettant d'assister les enquêteurs tout au long du processus d'enquête.

1 Introduction

En raison de l'évolution des nouvelles technologies, le domaine de la criminalistique informatique se heurte à des problèmes qui étaient encore anecdotiques il y a quelques années. Bien que des outils existent pour aider les enquêteurs, leur portée est limitée aux premières étapes du processus d'investigation défini par (Palmer, 2001). La collecte et l'étude des caractéristiques des pièces à conviction sont d'importantes phases du processus, toutefois il est également nécessaire de déduire de nouvelles connaissances telles que les raisons de l'état actuel des pièces à conviction (Carrier et Spafford, 2004) pour produire des conclusions utiles dans un procès. La reconstruction d'évènements peut être vue comme un processus utilisant un ensemble de pièces à conviction pour produire une chronologie décrivant les évènements composant un incident. Dans ce papier, nous présentons l'approche SADFC (Semantic Analysis of Digital Forensic Cases) qui permet de reconstruire et d'analyser des chronologies à partir de sources de données hétérogènes (traces laissées sur une scène de crime). La section suivante passe en revue les approches de reconstruction existantes. La section 3 présente ensuite notre approche et expose notamment les aspects relatifs à la gestion des connaissances et aux possibilités de raisonnements offertes. La section 4 introduit un prototype ayant permis la validation expérimentale de notre approche. Enfin, les travaux futurs sont présentés dans la section 5.