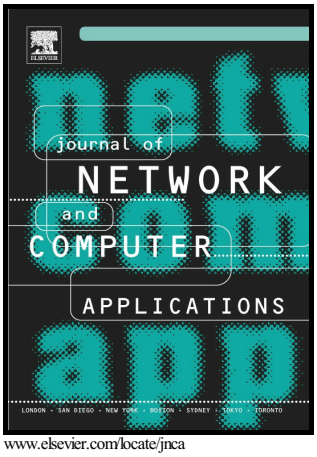
Author's Accepted Manuscript



www.elsevier.com/locate/jnca

Pervasive Social Networking Forensics: Intelligence and Evidence from Mobile Device Extracts

Darren Quick, Kim-Kwang Raymond Choo

PII: S1084-8045(16)30284-3
DOI: http://dx.doi.org/10.1016/j.jnca.2016.11.018
Reference: YJNCA1770

To appear in: *Journal of Network and Computer Applications*

Received date: 4 May 2016
Revised date: 13 November 2016
Accepted date: 16 November 2016

Cite this article as: Darren Quick and Kim-Kwang Raymond Choo, Pervasiv Social Networking Forensics: Intelligence and Evidence from Mobile Devic Extracts, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2016.11.018

This is a PDF file of an unedited manuscript that has been accepted fo publication. As a service to our customers we are providing this early version o the manuscript. The manuscript will undergo copyediting, typesetting, an review of the resulting galley proof before it is published in its final citable form Please note that during the production process errors may be discovered whic could affect the content, and all legal disclaimers that apply to the journal pertain

ACCEPTED MANUSCRIPT

Pervasive Social Networking Forensics: Intelligence and Evidence from Mobile Device Extracts

Darren Quick[1], Kim-Kwang Raymond Choo[2,1]*
[1]School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, SA 5095, Australia
[2]Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

darren.quick@mymail.unisa.edu.au
raymond.choo@fulbrightmail.org

*Corresponding Author. +1 210 458 7876

Accepted manuscript

Abstract

In pervasive social networking forensics, mobile devices (e.g. mobile phones) are a typical source of evidence. For example, figures from an Australian law enforcement agency show the number of mobile phones submitted for analysis increasing at an average of 60% per annum since 2006, and data from FBI regional computer forensics laboratory showing an increase of 67% per annum for mobile phone examinations. When coupled with the growth in capacity of memory card and device storage, which doubles approximately every 15 months, there is an ongoing and increasing growth in the volume of data available for evidence and intelligence analysis. There is a potential for information relevant to a range of crimes within the extracted data, such as terrorism and organised crime investigations, with potential cross-device and cross-case linkages. In this paper, we propose the Digital Forensic Intelligence Analysis Cycle (DFIAC). Using mobile device extracts from an Australian law enforcement agency, we demonstrate the utility of DFIAC in locating information across an increasing volume of forensically extracted data from mobile devices, and a greater understanding of the developing trends in relation to mobile device forensic analysis.

Keywords

Digital forensic intelligence analysis cycle, Forensic intelligence analysis, Mobile device forensic extracts, Pervasive social networking forensics, Social communication forensics, Social networking app forensics, big forensic data

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات