Acquiring and Analysing Digital Evidence - a Teaching and Learning Experience in Class

By: Aziz, NA (Aziz, Normaziah A.)[1]; Hanizam, AR (Hanizam, Ahmad Rasyad)[1]; Yusof, MSM (Yusof, Muhammad Saifulldin M.)[1]; Abd Rahman, LH (Abd Rahman, Lukman Hakim)[1]; Malik, MHB (Malik, Muhammad Helmi Bin Ab)[1]

PROCEEDINGS OF THE 2018 CYBER RESILIENCE CONFERENCE (CRC)
Edited by: Abidin, KAZ; Mohd, M; Shukur, Z
Published: 2018
Document Type: Proceedings Paper

Conference

Conference: Cyber Resilience Conference (CRC)
Location: Putrajaya, MALAYSIA
Date: NOV 13-15, 2018
Sponsor(s): Fac Informat Sci & Technol, Ctr Cyber Secur; Univ Kebangsaan Malaysia; CyberSecur Malaysia; Standard Chartered; Asean Univ Network; IEEE Comp Soc

Abstract

The advancement of Information and Communication Technology (ICT) offers positive and negative impacts in our daily life today. Criminals too leverage on sophisticated ICT in their modus operandi. Hence, digital evidences are abundant to be acquired and analysed as part of investigation, today. Two homegrown tools i.e. PenDua and Kloner are used for digital evidence acquisition tool while FTK and Autopsy are among tools applied for analysis of the evidences. Various artifacts are used as evidences of some made-up crime cases. The whole exercise is compiled as a learning package that can be a good exposure for beginners of Digital Evidence Forensics learners. We have tested the usage of this learning package with 120 students of a Digital Evidence Forensic class for 3 semesters. Majority of the students found that they enjoyed experiencing the hands-on to learn the proper procedure of acquiring and analyzing digital evidence, usage of several popular digital forensics tool and producing proper report. The made-up of real cases make the exercise interesting, appreciated by the students and enhance their understanding.

Keywords

Author Keywords: ISO/IEC 27037; digital evidence; acquisition tool; analysis tool; learning exercise

Author Information

Reprint Address: Aziz, NA (reprint author)

+ Int Islamic Univ Malaysia, Dept Comp Sci, Kuala Lumpur, Malaysia.

Addresses:

+ [1] Int Islamic Univ Malaysia, Dept Comp Sci, Kuala Lumpur, Malaysia

E-mail Addresses: naa@iium.edu.my; a.rasyad@gmail.com; saifulldin.yusof@gmail.com; lukman.har94@gmail.com; mshelmimalik@gmail.com

Publisher

IEEE, 345 E 47TH ST, NEW YORK, NY 10017 USA

Categories / Classification

Research Areas: Computer Science; Engineering
Web of Science Categories: Computer Science, Theory & Methods; Engineering, Electrical & Electronic

See more data fields

Cited References: 7

Showing 7 of 7 **View All in Cited References page** *(from Web of Science Core Collection)*

1. **Developing Computer Forensics Minor - Chanlenges and Opportunities** **Times Cited: 1**
   By: Adam, F.; Yanna, K.; Suk-Chung, Y.
   SIGCE 18 P 49 TECHN Pages: 1105 Published: 2018

2. **Guidelines for identification, collection, acquisition, and preservation of digital evidence** **Times Cited: 9**
   By: [Anonymous].
   ISO/IEC 27037:2012 Published: 2012
   Publisher: ISO Copyright office, Geneva

3. **Mobile device forensics: extracting and analysing data from an android-based smartphone** **Times Cited: 3**
   By: Aziz, N.A.; Mokhti, F.; Nozri, M.N.M.
   2015 Fourth International Conference on Cyber-Security, Cyber-Warfare and Digital Forensics (CyberSec). Proceedings Pages: 123-8 Published: 2015

4. **Experiences and methodologies teaching hands-on cyberforensics skills online** **Times Cited: 1**
   By: Kessler, G.C.
   P CFET 2007 1 INT C Published: 2007
   CD version

5. **Digital Forensics Curriculum in Security Education** **Times Cited: 1**
   By: Srinivasan, S.
   JOURNAL OF INFORMATION TECHNOLOGY EDUCATION-INNOVATIONS IN PRACTICE Volume: 12 Pages: 147-157 Published: 2013

6. Title: [not available] **Times Cited: 3**
   Group Author(s): Technical Working Group on Biological Evidence Preservation
   BIOL EV PRES HDB BES Published: 2013
   Publisher: U.S. Department of Commerce, National Institute of Standards and Technology

7. **Teaching Computer Forensics: Challenges and Opportunities** **Times Cited: 1**
   By: Yanna, K.
   Journal of Computing Sciences in Colleges Volume: 32 Pages: 208 Published: June 2017
   6

Showing 7 of 7 **View All in Cited References page**