PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS (PUCESE)

PROGRAMA DE MAESTRÍA EN:
TECNOLOGÍAS DE LA INFORMACIÓN

LÍNEA DE INVESTIGACIÓN:
L3: ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE REDES DE DATOS.

TÍTULO:

EVALUACIÓN DE HERRAMIENTAS PARA EL PROCESO DE GENERACIÓN DE INFORMES EN EL ÁMBITO DE LA INFORMÁTICA LEGAL BASADO EN LA NORMA ISO 27037:2012

PREVIO AL GRADO ACADÉMICO DE MAGÍSTER EN
TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:
Ing. Cinthya Castillo Montes

ASESOR:
Mgt. Juan Casierra Cavada

Esmeraldas, 22 de marzo del 2022

Evaluación de herramientas para el proceso de generación de informes en el ámbito de la informática legal basado en la norma ISO 27037:2012

Evaluation of tools for the report generation process in the field of legal informatics based on ISO 27037:2012.

Cinthya Castillo Montes. [1]

Juan Casierra Cavada. [2]

Resumen

Objetivo: Esta investigación tuvo como propósito evaluar herramientas para el proceso de generación de informes en el ámbito de la informática legal basada en la norma ISO 27037:2012, la cual garantiza la integridad de la evidencia digital a través de métodos y técnicas razonables para avalar su aceptación en los procedimientos legales.

Metodología: Este estudio se desarrolló basándose en el método de ponderación por criterios. Se utilizó muestreo no probabilístico para la selección de las herramientas de software utilizadas en la recopilación de evidencia digital, el criterio empleado fue el nivel de relevancia, confiabilidad y suficiencia, escogiéndose diez de ellas.

Resultados: De las investigaciones previas analizadas se considera ENCASE y Forensic Toolkit (FTK) como herramientas legalmente defendibles por disponer una serie de aplicaciones internas que ofrecen suficiencia y confiabilidad en la recolección de evidencia digital. Las herramientas evaluadas proporcionan un marco de informes flexible que permiten personalizar los informes de casos para satisfacer sus necesidades específicas.

Conclusiones: Las herramientas poseen características de alta tecnología de análisis forense digital, empezando por el bloqueo de escritura del dispositivo, tomando en consideración que todo en la recopilación de evidencia digital son FTK y Encase Forensic. El estándar ISO 27037:2012 desarrolla lineamientos para la identificación,

[1]Ingeniera en Sistemas Informáticos, Pontificia Universidad Católica del Ecuador Sede Esmeraldas, 0000-0002-9671-6980, cinthya.castillo@pucese.edu.ec

[2] Magister en Redes de Comunicaciones, Pontificia Universidad Católica del Ecuador Sede Esmeraldas, 0000-0002-0552-7720, juan.casierrac@pucese.edu.ec

recolección, adquisición y preservación de evidencia digital, por lo que se puede usar este documento como un modelo de buenas prácticas en informática forense.

Palabras claves: herramientas forenses, evidencia digital, informática legal, informática forense.

Abstract

Objective: The purpose of this research is to evaluate tools for the process of generating reports in the field of legal informatics based on ISO 27037:2012, which guarantees the integrity of digital evidence through reasonable methods and techniques to ensure its acceptance in legal proceedings.

Methodology: This study was developed based on the criteria weighting method. Non-probabilistic sampling was used for the selection of software tools used in the collection of digital evidence, the criteria used was the level of relevance, reliability and sufficiency, choosing ten of them.

Results: From the previous research analyzed, ENCASE and FTK are considered as legally defensible tools because they have a series of internal applications that offer sufficiency and reliability in the collection of digital evidence. The tools evaluated provide a flexible reporting framework that allow customization of case reports to meet their specific needs.

Conclusions: The tools possess high-tech digital forensic analysis features, starting with device write blocking, taking into consideration that everything in digital evidence collection are Forensic Toolkit (FTK) and Encase Forensic. The ISO 27037:2012 standard develops guidelines for the identification, collection, acquisition and preservation of digital evidence, so this document can be used as a model of good practices in computer forensics.

Keywords: forensic tools, digital evidence, legal computing, forensic computing.

AUTOR DE CORRESPONDENCIA:

- **Nombre de la revista científica:**
  Investigación e Innovación en Ingenierías
- **Enlace (URL) de la revista:**
  http://revistas.unisimon.edu.co/index.php/innovacioning/index
- **ISSN de la revista:** ISSN 2344-8652
- **Medio(s) de indexación:**
  - Dialnet
  - REDIB
  - MIAR
  - DRJI
  - Gold Rush
  - Infobaseindex
  - Google Académico
  - Latindex
  - Publindex
  - EBSCOhost
  - J-Gate

- **Nombre del contacto principal de la revista:** Doctora en Ingenierías Paola Sanchez Sanchez
- **Correo electrónico del editor de la revista:** revingenieria@unisimonbolivar.edu.co
- **Fecha de envío del artículo a la revista:** 19/03/2022

- Enlace del artículo en repositorio privado de la PUCESE (se almacena solo como evidencia hasta que el artículo se publique. Bajo ningún concepto el repositorio será público). Dentro del directorio "año/programa-maestría" se debe crear un directorio que siga el siguiente patrón: "Apellido1Apellido2Nombre-TitulodelEstudio"

Evidencias de envío a medio científico.

- Certificado de Aprobación por el asesor

Pontificia Universidad Católica del Ecuador
Sede Esmeraldas
Maestría en Tecnologías de la Información

PUCE

Esmeraldas 3 de marzo de 2022

CERTIFICADO DE PROCESO DE TFM

Mediante el presente certifico que la Maestrante Cinthya Elaine Castillo Montes presentó su documento final de investigación con el tema: Evaluación de herramientas para el proceso de generación de informes en el ámbito de la informática legal basado en la norma ISO 27037:2012, en modalidad artículo científico para la calificación requeridas del proceso.

Adicional adjunto el reporte de la herramienta Turnitin en un 5%.

Atentamente.

Mgt. Juan Casierra Cavada
Docente Asesor TFM
Maestría en Tecnología de la Información.

Dir: Calle Espejo y subida a Santa Cruz
Telf: (593) 2721 983 - 2721 595
Esmeraldas-Ecuador www.pucese.edu.ec

Turnitin Informe de Originalidad

Procesado el: 03-mar.-2022 15:33 -05
Identificador: 1775814850
Número de palabras: 5381
Entregado: 1

TFM Castillo Cinthya Por Cinthya Castillo

Índice de similitud	Similitud según fuente	
5%	Internet Sources:	3%
	Publicaciones:	1%
	Trabajos del estudiante:	1%

1% match (Internet desde 18-ene.-2022)
http://repositorio.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1750/Calidad%20pericial_%20JAIIO%20SID%202020%20v2.docx.pdf?sequence=1

1% match (Internet desde 13-jun.-2021)
https://dialnet.unirioja.es/descarga/articulo/7047153.pdf

1% match (Internet desde 29-oct.-2016)
https://prezi.com/iyzqvwhb6bel/admisibilidad-de-la-evidencia-digital-algunos-elementos-de-revision-y-analisis/

1% match (publicaciones)
Saurabh Agrawal, Abhishek Sahu, Girish Kumar. "A conceptual framework for the implementation of Industry 4.0 in legal informatics", Sustainable Computing: Informatics and Systems, 2022

1% match (publicaciones)
"Applied Technologies", Springer Science and Business Media LLC, 2020

1% match (trabajos de los estudiantes desde 23-feb.-2021)
Submitted to Universidad Internacional de la Rioja on 2021-02-23

1% match (Internet desde 03-ago.-2018)
http://repositorio.umsa.bo/bitstream/handle/123456789/8318/T.2866.pdf?sequence=1

- Carta al editor por medio del asesor

Pontificia Universidad
Católica del Ecuador
Sede Esmeraldas
Maestría en Tecnologías de la Información

Esmeraldas 19 de marzo de 2022

CARTA AL EDITOR

Mediante el presente extiendo un cordial saludo y a la vez envío la aceptación para publicar los resultados del proceso de investigación en el cual desempeñe el rol de asesor y coautor de la investigación la cual es el resultado del proceso de TFM del programa de Maestría en Tecnologías de la información y como coautor doy la autorización requerida para que el autor principal Ing. Cinthya Castillo Montes presente el envío a la revista seleccionada y aprobada por la academia.

Atentamente.

Atentamente.

Mgt. Juan Casierra Cavada
Docente Asesor TFM
Maestría en Tecnología de la Información.

- Capturas del envío