VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Manteniendo la cadena de custodia en una investigación electronica en la Nube

Ing. Elkin Valenzuela M.A.,

¿Qué es cadena de custodia?

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

MINISTERIO PÚBLICO
Fiscalía del Distrito Nacional

CONTROL DE CADENA DE CUSTODIA

Referencia: _____
Hora: _____

Fecha de Embalaje: _____
Organismo Responsable: _____
Tipo de Diligencia: _____
Lugar de Recolección de la Evidencia: _____

Descripción de la Evidencia: _____

Imputado (s): _____

Víctima (s): _____

Calificación Jurídica Inicial: _____

REGISTRO DE LA CADENA DE CUSTODIA

(Verifique que la evidencia no tenga una alteración, que no se haya hecho constar en la descripción de la misma)

ENTREGA	RECIBE	FECHA	FIRMA

Para ser llenado en la Oficina de Control de Evidencias (OCE)

Fecha Entrada: _____ Hora: _____

Clave de Localización: _____ Código OCE: _____

¿ Cuáles son las investigaciones electrónicas ?

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Ley 53-07

Artículo 4.- Definiciones. Para los fines de esta ley, se entenderá por:

Delito de Alta Tecnología: Aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.

Escenario #1

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Escenarios #1 – Público

Si en un allanamiento (lugar del hecho), es encontrado un dispositivo electrónico y el técnico realiza un análisis forense digital en vivo y tiene acceso a todas las credenciales de las cuentas redes sociales, drive entro otros y puede descargar todas las informaciones, incluyendo una imagen (fotografía) donde es la evidencia de la investigación, esta fue descargada, calculado el valor de hash y almacenada.

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD

IFC 2023

Informática Forense & Ciberseguridad

26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Interrogante del escenario #1

Legales

Que articulo y de que ley,

- 1 - Me permite realizar un análisis forense digital a un equipo encendido en el lugar del hecho.
- 2 - Me permite realizar una extracción de la información
- 3 - Me permite realizar una extracción de información de informaciones almacenada en la nube (otros servidores posiblemente compañía en el extranjero y el centro de almacenamiento en otro país)
- 4 - Me permite y me dice como salvaguardar las informaciones extraidas
- 5 -Me dices como debo custodiar las informaciones que han sido extraidas en un lugar de un hecho.

Técnicas

Que herramienta y cuál es el procedimiento,

- 1 - Como realizar un análisis forense digital a un equipo encendido.
- 2 - Como realizar una extracción de la información
- 3 -Como realizar una extracción de información de informaciones almacenada en la nube
- 4 - Como salvaguardar las informaciones extraidas
- 5 -Como debo custodiar las informaciones que han sido extraidas en un lugar de un hecho

Escenario #2

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Escenario #2 – Privado

Si dentro de una empresa sucede un incidente en el cual es una acción antijuridica (penal o administrativa), entonces por el privilegio de un usuario (otro empleado) en ciberseguridad, pueden acceder remotamente a el ordenador del empleado (imputado o que está cometiendo el hecho) y extraer las informaciones que son relevante para acreditar la participación del mismo (las informaciones obtenidas serán utilizarla para un proceso penal)

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Interrogante del escenario #2

Legales

- Que articulo y de que ley,
- 1 - Me permite realizar Análisis Forense Digital de los equipos propiedad de la empresa sin necesidad de orden judicial o entrega voluntaria
- 2 - Me permite realizar adquisición (extracción) de forma remota
- 3 - Me dice como debo almacenar las informaciones extraidas remotamente a un ordenador de un empleado de la empresa, el cual las informaciones serán utilizada como evidencia digital de un proceso judicial..

Técnicas

- Que herramienta y cuál es el procedimiento,
- 1 - Como debo de realizar Análisis Forense Digital a los Ordenadores
- 2 – Como realizar adquisición (extracción) de forma remota
- 3 - Como debo almacenar las informaciones extraidas remotamente a un ordenador de un empleado de la empresa, el cual las informaciones serán utilizadas como evidencia digital de un proceso judicial..

Solución Legal

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Codigo Procesal Penal

Art. 189.- Procedimiento. Rige el procedimiento previsto para el registro. Los efectos secuestrados son individualizados, inventariados y depositados de forma que asegurare su custodia y buena conservación, bajo la responsabilidad del ministerio público si los objetos secuestrados corren el riesgo de alterarse, desaparecer, sean de difícil custodia o perecederos, o estén sujetos a destrucción, se ordenaron reproducciones, copias, pericias o certificaciones sobre su existencia y estado.

MINISTERIO PÚBLICO

Ley 53-07

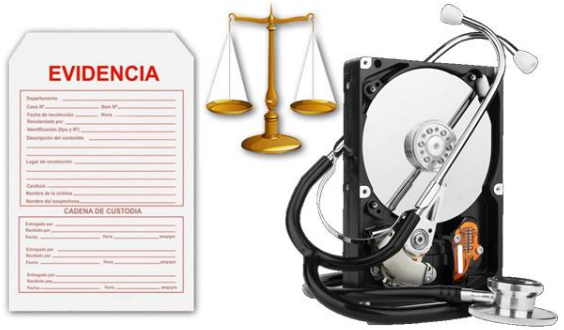
Artículo 55.- Mejores Prácticas de Recopilación de Evidencia. El Ministerio Público, el Departamento de Investigación de Delitos y Crímenes de Alta Tecnología (DICAT) de la Policía Nacional, la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones, y demás instituciones auxiliares, deberán procurar el uso de mejores prácticas y métodos eficientes durante los procesos de investigación para la obtención, recuperación y conservación de evidencia.

Ley 53-07

Artículo 58.- Responsabilidad del Custodio. A quien se le haya confiado la preservación del sistema de información o de cualquiera de sus componentes, así como de su contenido, conservará la confidencialidad e integridad de los mismos, impidiendo que terceros extraños, fuera de las autoridades competentes, tengan acceso y conocimiento de ellos. Asimismo, la persona encargada de la custodia no podrá hacer uso del objeto en custodia para fines distintos a los concernientes al proceso investigativo.

Artículo 59.- Confidencialidad del Proceso Investigativo. Quien colabore con el proceso de investigación, en la recolección, interceptación e intervención de datos de un sistema de información o de sus componentes, o cualquiera otra acción, incluyendo a los proveedores de servicios, mantendrá confidencial el hecho de la ejecución de los actos realizados por parte de la autoridad competente.

Párrafo.- La violación a los Artículos 51 y 52 será castigada con las penas establecidas para la revelación de secretos en el Código Penal de la República Dominicana.



Solución Tecnica

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

¿SE PUEDE PRESERVAR LA CADENA DE CUSTODIA SIN FIRMAS HASH?

Definitivamente NO. Es imprescindible obtener las firmas hash tanto del archivo digital estudiado como del soporte que la contiene.

=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

¿ Qué es el Valor hash?

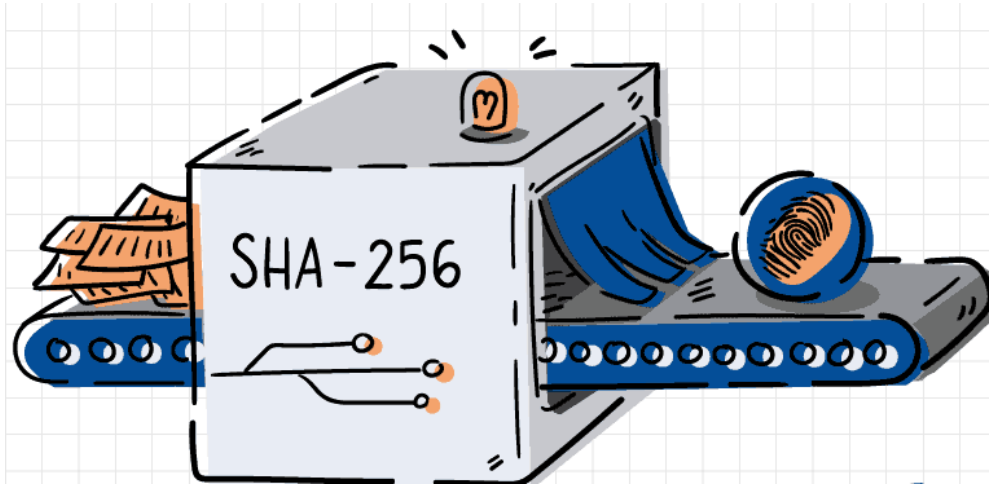
VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Firma Hash

Procedimiento matemático que mediante el empleo de un algoritmo permite identificar un archivo con valor único. Resulta claro que este valor se calcula sobre el contenido del archivo y no sobre el nombre del mismo, mediante el uso de una función específica MD5, SHA1 entre otros.

Es una suma de Verificación

Integridad!



Este es un mensaje

c0ac1bDt3jk4l5jmslw

Este es un mensaje!

Caracter diferente.

zt8jk4l5jmslwc0ac1k

Resultado diferente.

Retos

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

No Coinciden

ORIGEN

01001010011
11010101010
11101010101
11110001010
1010111110

DESTINO

01001010011
11010101010
11101010101
11110001001
1010111110

A34C42FF9AC14 = HASH ≠ 492C97F78ADD7

Coinciden

ORIGEN

01001010011
11010101010
11101010101
11110001010
1010111110

DESTINO

01001010011
11010101010
11101010101
11110001010
1010111110

A34C42FF9AC14 = HASH = A34C42FF9AC14

Que nos dice la NIST – En sus políticas sobre Hash

15 de marzo 2006

Las agencias federales **deben dejar de usar SHA-1** para firmas digitales, marcas de tiempo digitales y otras aplicaciones que requieren resistencia a colisiones tan pronto como sea posible, y deben usar la familia SHA-2 de funciones hash para estas aplicaciones después de 2010,

28 de septiembre 2012

SHA-1: Las agencias federales **deberían dejar de usar** SHA-1 para generar firmas digitales, generar marcas de tiempo y para otras aplicaciones que requieren resistencia a colisiones.

SHA-2: las agencias federales **pueden usar estas funciones hash** para todas las aplicaciones que emplean algoritmos hash seguros.

SHA-3: cuando el algoritmo hash SHA-3 esté disponible, también podrá

5 de agosto de 2015

SHA-1: las agencias federales **deberían dejar de usar** SHA-1 para generar firmas digitales, generar marcas de tiempo y para otras aplicaciones que requieren resistencia a colisiones.

SHA-2 las agencias federales **pueden usar estas funciones hash** para todas las aplicaciones que emplean algoritmos hash seguros.

SHA-3: las agencias federales **pueden utilizar** los cuatro algoritmos

15 de diciembre 2022

NIST está anunciando un cronograma para una transición para SHA-1. Después del 31/12/2030, cualquier módulo criptográfico validado FIPS 140 que tenga SHA-1 como algoritmo aprobado se moverá a la lista histórica.

El NIST recomienda que las agencias federales **abandonen SHA-1 para todas las aplicaciones lo antes posible**. Las agencias federales deberían utilizar SHA-2 o SHA-3 como alternativa a SHA-1

National Institute of Standards and Technology

Muchas Gracias

Ing. Elkin Valenzuela,
Analista Forense Digital

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom