

# ÍNDICE GENERAL

## INTRODUCCIÓN

### ***CAPÍTULO I***

<b><i>INFORMÁTICA FORENSE</i></b>	<b><i>1</i></b>
1.1. ¿QUÉ ES LA INFORMÁTICA FORENSE?	2
1.1.1. Orígenes	4
1.1.2. Situación actual de la Informática Forense	5
1.2. IMPORTANCIA DE LA INFORMÁTICA FORENSE	6
1.3. OBJETIVOS DE LA INFORMÁTICA FORENSE	7
1.4. EL PROCESO FORENSE	8
1.4.1. RFC3227	8
1.4.2. Guía De La IOCE	8
1.4.2.1. Fase 1. Recolección de la Evidencia	10
1.4.2.2. Fase 2: Autenticación de la Evidencia	12
1.4.2.3. Fase 3: Análisis	12
1.4.2.4. Fase 4: Reporte Final	14
1.4.3. Investigación en la Escena del Crimen Electrónico	15
1.4.4. Examen Forense de Evidencia Digital	16
1.4.5. Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong)	16
1.4.6. Guía de buenas prácticas para Evidencia basada en Computadores (Guía Reino Unido)	17
1.4.7. Guía para el Manejo de Evidencia en IT (Guía Australia)	17
1.5. DELITOS INFORMÁTICOS	18
1.6. TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS	21
1.6.1. Legislación Ecuatoriana	27
1.7. BIBLIOGRAFÍA	29

### ***CAPÍTULO II***

<b><i>EVIDENCIA DIGITAL</i></b>	<b><i>31</i></b>
2.1. IMPORTANCIA DE LA EVIDENCIA DIGITAL	32
2.2. CLASIFICACIÓN DE LA EVIDENCIA DIGITAL	35
2.3. PROCEDIMIENTO DE RECOLECCIÓN DE EVIDENCIA DIGITAL	37
2.3.1. Herramientas para Informática Forense	38
2.3.2. Cómo obtener la Evidencia Digital?	39

2.3.3. ¿Apagar o no apagar? _____	43
2.3.4. Preservación de la Evidencia _____	43
<b>2.4. CRITERIOS DE ADMISIBILIDAD Y VALOR PROBATORIO _____</b>	<b>46</b>
2.4.1. Autenticidad _____	46
2.4.2. Confiabilidad _____	47
2.4.4. Conformidad con las Leyes y las Regulaciones de la Administración de Justicia _____	48
<b>2.5. TIPOS DE EVIDENCIA DIGITAL _____</b>	<b>49</b>
<b>2.6. BIBLIOGRAFÍA _____</b>	<b>50</b>

## ***CAPÍTULO III***

### ***HERRAMIENTAS DE INVESTIGACIÓN FORENSE***

<b>3.1. HERRAMIENTAS DE INFORMÁTICA FORENSE _____</b>	<b>54</b>
<b>3.2. HERRAMIENTAS PARA LA RECOLECCIÓN DE EVIDENCIA DIGITAL _____</b>	<b>55</b>
3.2.1. EnCase _____	59
3.2.2. The Coroner's Toolkit _____	62
3.2.3. ByteBack - TechAssist, Inc _____	64
3.2.4. The Access Data Forensic Toolkit (FTK) _____	64
3.2.5. Data Recovery Kit - LCTechnogy _____	65
3.2.6. COFEE _____	66
3.2.7. Safe Back - New Technologies Inc _____	66
3.2.8. The Forensic Tool Kit _____	66
3.2.9. The Sleuth Kit and Autopsy _____	67
3.2.10. Helix CD _____	69
3.2.11. F.I.R.E (Forensics and Incident Response Bootable CD) _____	70
<b>3.3. HERRAMIENTAS PARA EL MONITOREO Y/O CONTROL DE COMPUTADORES _____</b>	<b>71</b>
3.3.1. Keylogger _____	71
3.3.1.1 Revealer Keylooger _____	72
<b>3.4. HERRAMIENTAS DE MARCADO DE DOCUMENTOS _____</b>	<b>73</b>
3.4.1. WatermarkIt _____	75
3.4.2. Sandmark _____	76
<b>3.5. HERRAMIENTAS DE HARDWARE _____</b>	<b>77</b>
3.5.1. Portable Evidence Recovery Unit (DIBS) _____	77
3.5.2. MASSter Forensic Soft Case _____	78
3.5.3. Conclusiones y características de Hardware forense _____	79
<b>3.6. BIBLIOGRAFÍA _____</b>	<b>82</b>

## **CAPÍTULO IV**

### **INFORMÁTICA FORENSE, INSERCIÓN JURÍDICA**

<b>4.1. INFORMÁTICA FORENSE Y SU REALIDAD PROCESAL EN EL ECUADOR</b>	<b>86</b>
4.1.1. Unidad de Delitos Informáticos del Ministerio Público (UDIMP)	88
4.1.2. Departamento de Investigación y Análisis Forense	93
4.1.2.1.- Misión	94
4.1.2.2.- Funciones del Departamento de Análisis Forense	95
4.1.2.3.- Funciones del Jefe del Departamento de Análisis Forense	96
4.1.2.4.- Sección Técnica y Forense	97
<b>4.2. INFORMÁTICA FORENSE, LEYES INTERNACIONALES</b>	<b>98</b>
4.2.1. Legislación Informática de España	100
4.2.2. Legislación Informática de Venezuela	102
4.2.3. Legislación Informática dictada por las Naciones Unidas	103
4.2.4. Legislación Informática en México	104
4.2.5. Legislación Informática en Argentina	107
4.2.6. Legislación Informática en Estados Unidos	108
4.2.7. Legislación Informática en Gran Bretaña.	109
4.2.8. Legislación Informática en Holanda.	109
4.2.9. Legislación Informática en Francia.	110
4.2.10. Legislación Informática en Chile.	111
4.2.11. Delitos informáticos: Aplicación Colombia	112
<b>4.3. LEYES ECUATORIANAS E INTERNACIONALES</b>	<b>115</b>
<b>4.4. OTRAS CONSIDERACIONES</b>	<b>117</b>
<b>4.5. BIBLIOGRAFÍA</b>	<b>119</b>

## **CAPÍTULO V**

### **METODOLOGÍA DE TRABAJO PARA INVESTIGACIÓN**

<b>5.1. METODOLOGÍA DE TRABAJO PARA INVESTIGACIÓN EN INFORMÁTICA FORENSE</b>	<b>124</b>
<b>5.2. FASE DE IDENTIFICACIÓN</b>	<b>125</b>
5.2.1. Solicitud Forense	126
5.2.2. Asegurar la escena	127
5.2.3. Identificar las evidencias	127
5.2.3.1. Prioridades del administrador	128
5.2.3.2. Tipo de dispositivo	130
5.2.3.3. Modo de almacenamiento	130
<b>5.3. FASE DE PRESERVACIÓN</b>	<b>131</b>
5.3.1. Copias de la evidencia	132
5.3.2. Cadena de custodia	132
<b>5.4. FASE DE ANÁLISIS</b>	<b>133</b>

5.4.1. Preparación para el análisis _____	134
5.4.2. Reconstrucción de la secuencia temporal del ataque _____	135
5.4.3. Determinación de cómo se realizó el ataque _____	138
5.4.4. Identificación del atacante _____	139
5.4.5. Perfil del atacante _____	141
5.4.6. Evaluación del impacto causado al sistema _____	142
<b>5.5. FASE DE DOCUMENTACIÓN Y PRESENTACIÓN DE LAS PRUEBAS</b> _____	<b>142</b>
5.5.1. Utilización de formularios de registro del incidente _____	143
5.5.1.1. Informe Técnico _____	143
5.5.1.2. Informe Ejecutivo _____	144
<b>5.6. BIBLIOGRAFÍA</b> _____	<b>145</b>

## ***CAPÍTULO VI***

<b><i>CONCLUSIONES Y RECOMENDACIONES</i></b> _____	<b>147</b>
6.1. CONCLUSIONES _____	148
6.2. RECOMENDACIONES _____	150

## **ANEXOS**