1.0 Análisis Forense. 7
1.1 Introducción. 7
1.2 La Línea De Tiempo. 7
1.3 Etapas. 7
1.4 Cadena De Custodia Como Prueba Judicial. 8
1.5 Auto Evaluación. 8
2.0 Soporte De Datos. 10
2.1 Introducción. 10
2.2 Composición De Los Soportes De Datos. 10
2.2.1 Sistema De Archivos NTFS. 10
2.2.1.1 MFT Concepto. 11
2.2.2 Sistema De Archivos FAT. 12
2.2.2.1 FAT Estructura. 12
2.2.2.2 FAT12. 13
2.2.2.3 FAT16. 15
2.2.2.4 FAT32. 15
2.2.2.5 FAT Y Metadatos. 15
2.2.3 Sistema De Archivos, ext2, ext3, ext4. 16
2.2.3.1 ext2. 16
2.2.3.2 ext3. 16
2.2.3.3 ext4. 17
2.2.4 Modelo De Capas. 18
2.2.4.1 Nivel 1: dispositivos físicos. 18
2.2.4.2 Nivel 2: volúmenes y particiones. 18
2.2.4.3 Nivel 3: sistemas de archivos. 19
2.2.4.4 Nivel 4: bloques de datos. 19
2.2.4.5 Nivel 5: metadatos. 19
2.2.4.6 Nivel 6: nombre de archivo. 19
2.2.4.7 Nivel 7: journaling. 19
2.3 Introducción a OsForensic. 20
2.3.1 Creación De Una Imagen De Disco. 20
2.3.2 Analizando Imágenes De Disco. 22
2.3.2.1 Imágenes completas del dispositivo. 22

2.3.2.2 Imágenes parciales, donde se guardan los ficheros como $MFT, $UsnJrnl$J, $LogFile. 25
2.3.2.3 ¿Qué buscar?. 26
2.3.2.4 Examen Teórico. 27
2.3.2.5 Taller Analizar HD. 27
2.3.2.6 Taller Analizar USB. 27
3.0 Análisis En Equipos Activos Windows. 28
3.1 Introducción. 28
3.2 Recopilando Información Volátil. 28
3.2.1 Fecha Y Hora Del Sistema. 29
3.2.2 Información Del Sistema. 29
3.2.3 Conexiones de red abiertas. 31
3.2.4 Puertos TCP Y UDP Abiertos. 32
3.2.5 Ejecutables Conectados A Puertos TCP y UDP. 33
3.2.6 Usuarios Conectados Al Sistema. 33
3.2.7 Tablas De Enrutamiento Interna. 34
3.2.8 Procesos En Ejecución. 35
3.2.9 Archivos Abiertos. 36
3.3 Análisis Forense De La RAM. 37
3.3.1 Herramienta FTK Imager. 38
3.3.2 Herramienta DumpIT. 38
3.3.3 Análisis De La RAM Mediante Volatility Framework. 39
3.3.3.1 Imageinfo. 39
3.3.3.2 pslist. 39
3.3.3.3 Procdump. 40
3.3.3.4 Printkey. 40
3.3.3.5 cmdscan. 41
3.3.3.6 envars. 41
3.3.3.7 volshell. 41
3.3.3.8 connections. 42
3.3.3.9 connscan. 42
3.3.3.10 sockets. 42
3.3.3.11 sockscan. 43
3.3.3.12 netscan. 43

3.3.4 Taller Analizar Imagen De Memoria. 44
4.0 Redes Internas Y Externas. 45
4.1 Introducción. 45
4.2 Redes. 45
4.2.1 Red Corporativa/Internet. 45
4.2.2 Protocolos. 47
4.2.2.1 Modelo OSI. 48
4.2.3 Enrutamiento. 50
4.2.4 Protocolos De Nivel Superior: HTTP y SMB. 50
4.2.5 Wireshark Analizando Trafico De Red. 51
4.2.5.1 ¿Desde Donde Ejecutar Wireshark? 51
4.2.5.2 Introducción A Wireshark. 51
4.2.5.3 Filtros En Wireshark. 55
4.3 Buscando hash en paquetes SMB. 57
4.3.1 Autenticación NTLMv2. 60
4.3.1 Taller Analizar Red 1. 66
4.4 Buscando en paquetes HTTP Y TCP. 67
4.4.1 Viendo La Información De Un Paquete. 68
4.4.1.1 Viendo Paquetes Imágenes De Tipo Byte. 71
4.4.2 Taller Analizar Red 2. 74
4.5 Detectando Ataques A Redes. 75
4.5.1 Ataques ARP. 75
4.5.1.1 Protocolo ARP. 75
4.5.1.2 En Que Consiste El Ataque ARP. 76
4.5.1.3 Como Detectarlo Con WiresHark. 76
4.5.2 IP Protocol Scan. 78
4.5.3 ICMP Barrido De Ping. 78
4.5.4 TCP Barrido De Ping. 79
4.5.5 UDP Barrido De Ping. 79
4.5.6 Resumen Tabla Detección De Descubrimiento De Host. 79
4.5.7 TCP SYN / Stealth Scan (Buscando Equipos Modo Silencioso). 80
4.5.8 TCP Connect() Scan (Buscando Puertos). 80
4.5.9 TCP Null Scan (Firewall). 81
4.5.10 TCP FIN Scan (Firewall). 81

4.5.11 Xmass Scan (Firewall). 82
4.5.12 UDP Port Scan. 82
4.5.13 Resumen Tabla Scaneos Detección De Puertos. 83
4.5.13 Ataque Vlan Hoping. 84
4.5.14 Unexplained Packet Loss. 84
4.5.15 Resumen Tabla De Ataques A Redes 84
4.5.16 Exfiltracion De Datos. 85
4.5.16.1 Exfiltracion Por HTTP. 85
4.5.16.2 Exfiltracion Por SMTP. 85
4.5.16.3 Exfiltracion Por DNS. 85
4.5.16.4 Exfiltracion Por ICMP 86
4.5.16.5 Exfiltracion Por IPV6. 86
4.5.17 Ataque A Redes Wireless. 88
4.5.17.1 Deautenticacion De Cliente. 88
4.5.17.2 Disociación De Cliente. 89
4.5.17.3 Fake AP Beacom Flood. 90
4.5.17.4 Autenticación Denegación De Servicio. 91
4.5.18 Resumen Tablas De Ataque A Redes Wireless. 92
4.5.19 Taller Analizar Red 3 92
5.0 Análisis De Cabeceras Email. 93
5.1 Protocolos de autenticación SPF, DKIM y DMARK. 93
5.2 Trazas De Un Email. 93
5.3 Cabecera De Un Email. 94
5.4 Herramientas para análisis de email. 94
5.5 Análisis de una cabecera. 94
5.5.1 Return-Path (Primero parte superior del email). 97
5.5.2 Authentication-Results. 97
5.5.3 Received Uno. 97
5.5.3.1 Received Dos. 98
5.1.4 Whois sobre IP Origen del email. 98
5.1.5 Analizar Black List. 99
5.1.5.1 Analizamos Cabecera Del Email Enviado Por El Proveedor CompañiaX A Excavaciones CompañiaY, con fecha 12 de Mayo de 2022. 99
5.2 Análisis De Fichero Adjunto, PDF, Factura De Pago. 109

5.3 Resumen De Análisis. 111