

# Informe de los ejercicios entregables

Convocatoria diciembre 2024

*Informática Forense y Auditoría*



## Control de versiones

**Versión actual:** 2024.ES.003

**Fecha:** 21/12/2024

Versión	Fecha	Comentarios de versión
2024.ES.001	20/12/2024	Creación del documento y su plantilla.
2024.ES.002	21/12/2024	Realización de los ejercicios indicados.
2024.ES.003	21/12/2024	Corrección de errores en ejercicios y “beautify” del documento.

## Índice

Control de versiones	1
Índice	2
Índice de Ilustraciones	13
Índice de tablas	16
Consideraciones previas	17
Objeto del peritaje	18
Resolución	19
Práctica 2 – Ejercicio 21	19
Enunciado	19
Toma de pruebas	20
Resultados obtenidos	23
Conclusiones	26
Práctica 2 – Ejercicio 35	26
Enunciado	26
Toma de pruebas	26
Análisis de las pruebas	26
Resultados obtenidos	27
Conclusiones	28
Práctica 2 – Ejercicio 36	28
Enunciado	28
Toma de pruebas	28
Análisis de las pruebas	28
Resultados obtenidos	28
Conclusiones	29
Práctica 2 – Ejercicio 37	29
Enunciado	29
Toma de pruebas	29
Análisis de las pruebas	29
Resultados obtenidos	29
Conclusiones	30
Práctica 3 – Ejercicio 1	30
Enunciado	30
Toma de pruebas	31

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 2 de 109

Análisis de las pruebas	31
Resultados obtenidos	31
Conclusiones preliminares	33
Conclusiones	33
Práctica 3 – Ejercicio 10	33
Enunciado	33
Toma de pruebas	33
Análisis de las pruebas	33
Resultados obtenidos	35
Conclusiones preliminares	36
Conclusiones	36
Práctica 3 – Ejercicio 14	36
Enunciado	36
Toma de pruebas	36
Análisis de las pruebas	36
Resultados obtenidos	37
Conclusiones preliminares	37
Conclusiones	38
Práctica 3 – Ejercicio 14 – Apartado a	38
Enunciado	38
Resultados obtenidos	38
Conclusiones preliminares	39
Conclusiones	39
Práctica 3 – Ejercicio 14 – Apartado b	39
Enunciado	39
Resultados obtenidos	39
Conclusiones	39
Práctica 3 – Ejercicio 14 – Apartado c	40
Enunciado	40
Resultados obtenidos	40
Conclusiones	40
Práctica 4 – Ejercicio 8	40
Enunciado	40
Toma de pruebas	41

Análisis de las pruebas	41
Práctica 4 – Ejercicio 8 – Apartado bb	41
Enunciado	41
Resultados obtenidos	42
Conclusiones preliminares	43
Conclusiones	43
Práctica 4 – Ejercicio 8 – Apartado vv	43
Enunciado	43
Resultados obtenidos	43
Conclusiones preliminares	43
Conclusiones	43
Práctica 4 – Ejercicio 8 – Apartado xx	44
Enunciado	44
Resultados obtenidos	44
Conclusiones	44
Práctica 4 – Ejercicio 8 – Apartado ccc	44
Enunciado	44
Resultados obtenidos	44
Conclusiones	45
Práctica 4 – Ejercicio 8 – Apartado fff	46
Enunciado	46
Resultados obtenidos	46
Conclusiones	47
Práctica 4 – Ejercicio 8 – Apartado iii	47
Enunciado	47
Resultados obtenidos	47
Conclusiones	49
Práctica 4 – Ejercicio 8 – Apartado mmm	49
Enunciado	49
Resultados obtenidos	50
Conclusiones	51
Práctica 4 – Ejercicio 8 – Apartado nnn	51
Enunciado	51
Resultados obtenidos	51

Conclusiones _____	51
Práctica 4 – Ejercicio 8 – Apartado ppp _____	51
Enunciado _____	51
Resultados obtenidos _____	51
Conclusiones _____	52
Práctica 4 – Ejercicio 8 – Apartado rrr _____	52
Enunciado _____	52
Resultados obtenidos _____	53
Conclusiones _____	53
Práctica 4 – Ejercicio 8 – Apartado sss _____	53
Enunciado _____	53
Resultados obtenidos _____	53
Conclusiones _____	53
Práctica 4 – Ejercicio 9 _____	53
Enunciado _____	53
Toma de pruebas _____	54
Análisis de las pruebas _____	54
Práctica 4 – Ejercicio 9 – Apartado aa _____	54
Enunciado _____	54
Resultados obtenidos _____	54
Conclusiones _____	54
Práctica 4 – Ejercicio 9 – Apartado bb _____	54
Enunciado _____	54
Resultados obtenidos _____	55
Conclusiones _____	55
Práctica 4 – Ejercicio 9 – Apartado cc _____	55
Enunciado _____	55
Resultados obtenidos _____	56
Conclusiones _____	56
Práctica 4 – Ejercicio 9 – Apartado dd _____	56
Enunciado _____	56
Resultados obtenidos _____	56
Conclusiones _____	56
Práctica 4 – Ejercicio 9 – Apartado ee _____	56

Enunciado	56
Resultados obtenidos	57
Conclusiones	57
Práctica 4 – Ejercicio 9 – Apartado ff	57
Enunciado	57
Resultados obtenidos	57
Conclusiones	57
Práctica 4 – Ejercicio 9 – Apartado gg	57
Enunciado	57
Resultados obtenidos	58
Conclusiones	58
Práctica 4 – Ejercicio 9 – Apartado hh	58
Enunciado	58
Resultados obtenidos	59
Conclusiones	59
Práctica 4 – Ejercicio 9 – Apartado ii	59
Enunciado	59
Resultados obtenidos	60
Conclusiones	60
Práctica 4 – Ejercicio 9 – Apartado jj	60
Enunciado	60
Resultados obtenidos	60
Conclusiones	60
Práctica 5a – Ejercicio 28	60
Enunciado	60
Toma de pruebas	61
Análisis de las pruebas	61
Práctica 5a – Ejercicio 28 – Apartado i	61
Enunciado	61
Resultados obtenidos	61
Conclusiones	62
Práctica 5a – Ejercicio 28 – Apartado j	62
Enunciado	62
Resultados obtenidos	62

Conclusiones	63
Práctica 5a – Ejercicio 28 – Apartado k	63
Enunciado	63
Resultados obtenidos	63
Conclusiones	64
Práctica 5a – Ejercicio 28 – Apartado l	64
Enunciado	64
Resultados obtenidos	64
Conclusiones	64
Práctica 5a – Ejercicio 28 – Apartado m	64
Enunciado	64
Resultados obtenidos	65
Conclusiones	65
Práctica 5a – Ejercicio 28 – Apartado n	65
Enunciado	65
Resultados obtenidos	65
Conclusiones	66
Práctica 5a – Ejercicio 28 – Apartado o	66
Enunciado	66
Resultados obtenidos	66
Conclusiones	67
Práctica 5a – Ejercicio 28 – Apartado p	67
Enunciado	67
Resultados obtenidos	67
Conclusiones	67
Práctica 5a – Ejercicio 28 – Apartado q	68
Enunciado	68
Resultados obtenidos	68
Conclusiones	68
Práctica 5a – Ejercicio 34	68
Enunciado	68
Toma de pruebas	69
Análisis de las pruebas	69
Práctica 5a – Ejercicio 34 – Imagen 2	69

Resultados obtenidos	69
Conclusiones	71
Práctica 5a – Ejercicio 34 – Imagen 4	71
Resultados obtenidos	71
Conclusiones	73
Práctica 5a – Ejercicio 34 – Imagen 15	73
Resultados obtenidos	73
Conclusiones	75
Práctica 5a – Ejercicio 35	75
Enunciado	75
Toma de pruebas	76
Análisis de las pruebas	76
Práctica 5a – Ejercicio 35 – Fichero 3	76
Resultados obtenidos	76
Conclusiones	77
Práctica 5a – Ejercicio 35 – Fichero 6	77
Resultados obtenidos	77
Conclusiones	78
Práctica 5a – Ejercicio 35 – Fichero 9	78
Resultados obtenidos	78
Conclusiones	79
Práctica 5a – Ejercicio 42	79
Enunciado	79
Toma de pruebas	79
Análisis de las pruebas	79
Práctica 5a – Ejercicio 42 – Apartado a	80
Enunciado	80
Resultados obtenidos	80
Conclusiones	80
Práctica 5a – Ejercicio 42 – Apartado b	80
Enunciado	80
Resultados obtenidos	81
Conclusiones	81
Práctica 5a – Ejercicio 42 – Apartado c	81

Enunciado	81
Resultados obtenidos	82
Conclusiones	82
Práctica 5a – Ejercicio 42 – Apartado d	82
Enunciado	82
Resultados obtenidos	83
Conclusiones	83
Práctica 5a – Ejercicio 42 – Apartado e	83
Enunciado	83
Resultados obtenidos	84
Conclusiones	84
Práctica 5a – Ejercicio 42 – Apartado f	84
Enunciado	84
Resultados obtenidos	84
Conclusiones	85
Práctica 5a – Ejercicio 42 – Apartado g	85
Enunciado	85
Resultados obtenidos	85
Conclusiones	85
Práctica 5a – Ejercicio 42 – Apartado h	86
Enunciado	86
Resultados obtenidos	86
Conclusiones	86
Práctica 5a – Ejercicio 42 – Apartado i	86
Enunciado	86
Resultados obtenidos	87
Conclusiones	87
Práctica 5a – Ejercicio 45	87
Enunciado	87
Toma de pruebas	88
Práctica 5a – Ejercicio 45 – Apartado a	88
Enunciado	88
Resultados obtenidos	88
Conclusiones	88

Práctica 5a – Ejercicio 45 – Apartado b	88
Enunciado	88
Resultados obtenidos	89
Conclusiones	89
Práctica 5a – Ejercicio 45 – Apartado c	89
Enunciado	89
Resultados obtenidos	89
Conclusiones	91
Práctica 5a – Ejercicio 45 – Apartado d	91
Enunciado	91
Resultados obtenidos	91
Conclusiones	91
Práctica 5a – Ejercicio 45 – Apartado e	92
Enunciado	92
Resultados obtenidos	92
Conclusiones	92
Práctica 5a – Ejercicio 45 – Apartado f	92
Enunciado	92
Resultados obtenidos	92
Conclusiones	92
Práctica 5a – Ejercicio 45 – Apartado g	92
Enunciado	92
Resultados obtenidos	92
Práctica 5b – Ejercicio 3	93
Enunciado	93
Toma de pruebas	93
Práctica 5b – Ejercicio 3 – Apartado a	94
Enunciado	94
Resultados obtenidos	94
Conclusiones	94
Práctica 5b – Ejercicio 3 – Apartado b	94
Enunciado	94
Resultados obtenidos	95
Conclusiones	95

Práctica 5b – Ejercicio 3 – Apartado c	95
Enunciado	95
Resultados obtenidos	96
Conclusiones	96
Práctica 5b – Ejercicio 3 – Apartado d	96
Enunciado	96
Resultados obtenidos	97
Conclusiones	97
Práctica 5b – Ejercicio 3 – Apartado e	97
Enunciado	97
Resultados obtenidos	98
Conclusiones	98
Práctica 5b – Ejercicio 3 – Apartado f	98
Enunciado	98
Resultados obtenidos	99
Conclusiones	99
Práctica 5b – Ejercicio 3 – Apartado g	99
Enunciado	99
Resultados obtenidos	100
Conclusiones	100
Práctica 5b – Ejercicio 3 – Apartado h	100
Enunciado	100
Resultados obtenidos	101
Conclusiones	101
Práctica 5b – Ejercicio 3 – Apartado i	101
Enunciado	101
Resultados obtenidos	101
Conclusiones	101
Práctica 5b – Ejercicio 3 – Apartado j	101
Enunciado	101
Resultados obtenidos	102
Conclusiones	102
Práctica 5b – Ejercicio 3 – Apartado k	102
Enunciado	102

Resultados obtenidos	104
Conclusiones	104
Práctica 5b – Ejercicio 3 – Apartado l	104
Enunciado	104
Resultados obtenidos	105
Conclusiones	105
Práctica 5b – Ejercicio 3 – Apartado m	105
Enunciado	105
Resultados obtenidos	105
Conclusiones	106
Práctica 5b – Ejercicio 3 – Apartado n	106
Enunciado	106
Resultados obtenidos	106
Conclusiones	106
Práctica 5b – Ejercicio 3 – Apartado o	106
Enunciado	106
Resultados obtenidos	106
Conclusiones	106
Práctica 5b – Ejercicio 3 – Apartado p	107
Enunciado	107
Resultados obtenidos	107
Conclusiones	107
Práctica 5b – Ejercicio 3 – Apartado q	107
Enunciado	107
Resultados obtenidos	108
Conclusiones	108
Práctica 5b – Ejercicio 3 – Apartado r	108
Enunciado	108
Resultados obtenidos	109
Conclusiones	109

## Índice de Ilustraciones

Ilustración 1. Diagrama Sujeto y Recolector de Evidencias	19
Ilustración 2. Dispositivo en uso Práctica 2 - Ejercicio 21	20
Ilustración 3. Configuración Bridge Caine 13	20
Ilustración 4. Configuración Bridge Ubuntu Desktop	21
Ilustración 5. Filtro para la unidad USB	21
Ilustración 6. Ip de Caine 13	22
Ilustración 7. Ip de Ubuntu Desktop	22
Ilustración 8. Comunicación ping de Caine 13 a Ubuntu Desktop	22
Ilustración 9. Comunicación ping de Ubuntu Desktop a Caine 13	23
Ilustración 10. Comprobación montaje USB	23
Ilustración 11. Resolución Práctica 2 - Ej 21 - Parte 1	24
Ilustración 12. Resolución Práctica 2 - Ej 21 - Parte 2	24
Ilustración 13. Resolución Práctica 2 - Ej 21 - Parte 3	24
Ilustración 14. Resolución Práctica 2 - Ej 21 - Parte 4	25
Ilustración 15. Resolución Práctica 2 - Ej 21 - Parte 5	25
Ilustración 16. Resolución Práctica 2 - Ej 21 - Parte 6	25
Ilustración 17. Resolución Práctica 2 - Ej 21 - Parte 7	26
Ilustración 18. Descarga recursos del ejercicio	26
Ilustración 19. Resolución Práctica 2 - Ej 35 - Parte 1	27
Ilustración 20. Resolución Práctica 2 - Ej 35 - Parte 2	27
Ilustración 21. Resolución Práctica 2 - Ej 36	28
Ilustración 22. Resolución Práctica 2 - Ej 37	30
Ilustración 23. Resolución Práctica 3 - Ej 1 - Parte 1	31
Ilustración 24. Resolución Práctica 3 - Ej 1 - Parte 2	31
Ilustración 25. Resolución Práctica 3 - Ej 1 - Parte 3	32
Ilustración 26. Resolución Práctica 3 - Ej 1 - Parte 4	33
Ilustración 27. Ejemplo propiedades Windows	34
Ilustración 28. Resolución Práctica 3 - Ej 10	35
Ilustración 29. Archivos de audio encontrados	36
Ilustración 30. Resolución Práctica 3 - Ej 14	37
Ilustración 31. Volúmenes encontrados	38
Ilustración 32. Resolución Práctica 3 - Ej 14 - Apartado a	39
Ilustración 33. Resolución Práctica 3 - Ej 14 - Apartado c	40
Ilustración 34. Resolución Práctica 4 - Ej 8 - Apartado bb – Parte 1	42
Ilustración 35. Resolución Práctica 4 - Ej 8 - Apartado bb – Parte 2	42
Ilustración 36. Resolución Práctica 4 - Ej 8 - Apartado vv	43
Ilustración 37. Resolución Práctica 4 - Ej 8 - Apartado xx	44
Ilustración 38. Resolución Práctica 4 - Ej 8 - Apartado ccc - Parte 1	45
Ilustración 39. Resolución Práctica 4 - Ej 8 - Apartado ccc - Parte 2	45
Ilustración 40. Resolución Práctica 4 - Ej 8 - Apartado fff - Parte 1	46
Ilustración 41. Resolución Práctica 4 - Ej 8 - Apartado fff - Parte 2	46
Ilustración 42. Localización de Facebook 1	47
Ilustración 43. Localización de Facebook 2	47
Ilustración 44. Localización de Instagram	48

Ilustración 45. Localización de Pinterest	48
Ilustración 46. Localización de Twitter	49
Ilustración 47. Resolución Práctica 4 - Ej 8 - Apartado mmm - Parte 1	50
Ilustración 48. Resolución Práctica 4 - Ej 8 - Apartado mmm - Parte 2	50
Ilustración 49. Resolución Práctica 4 - Ej 8 - Apartado ppp – Parte 1	51
Ilustración 50. Resolución Práctica 4 - Ej 8 - Apartado ppp – Parte 2	52
Ilustración 51. Resolución Práctica 4 - Ej 8 - Apartado rrr	53
Ilustración 52. Resolución Práctica 4 - Ej 9 - Apartado aa	54
Ilustración 53. Resolución Práctica 4 - Ej 9 - Apartado bb	55
Ilustración 54. Resolución Práctica 4 - Ej 9 - Apartado cc	56
Ilustración 55. Resolución Práctica 4 - Ej 9 - Apartado ee	57
Ilustración 56. Resolución Práctica 4 - Ej 9 - Apartado gg	58
Ilustración 57. Resolución Práctica 4 - Ej 9 - Apartado hh	59
Ilustración 58. Resolución Práctica 4 - Ej 9 - Apartado ii	60
Ilustración 59. Resolución Práctica 5a - Ej 28 - Apartado i - Parte 1	61
Ilustración 60. Resolución Práctica 5a - Ej 28 - Apartado i - Parte 2	62
Ilustración 61. Resolución Práctica 5a - Ej 28 - Apartado k - Parte 1	63
Ilustración 62. Resolución Práctica 5a - Ej 28 - Apartado k - Parte 2	63
Ilustración 63. Resolución Práctica 5a - Ej 28 - Apartado l	64
Ilustración 64. Resolución Práctica 5a - Ej 28 - Apartado n	66
Ilustración 65. Resolución Práctica 5a - Ej 28 - Apartado o	67
Ilustración 66. Resolución Práctica 5a - Ej 28 - Apartado q	68
Ilustración 67. Resolución Práctica 5a - Ej 34 - Imagen 2 - Parte 1	69
Ilustración 68. Resolución Práctica 5a - Ej 34 - Imagen 2 - Parte 2	70
Ilustración 69. Resolución Práctica 5a - Ej 34 - Imagen 2 - Parte 3	71
Ilustración 70. Resolución Práctica 5a - Ej 34 - Imagen 4 - Parte 1	72
Ilustración 71. Resolución Práctica 5a - Ej 34 - Imagen 4 - Parte 2	72
Ilustración 72. Resolución Práctica 5a - Ej 34 - Imagen 4 - Parte 3	73
Ilustración 73. Resolución Práctica 5a - Ej 34 - Imagen 15 - Parte 1	74
Ilustración 74. Resolución Práctica 5a - Ej 34 - Imagen 15 - Parte 2	74
Ilustración 75. Resolución Práctica 5a - Ej 34 - Imagen 15 - Parte 3	75
Ilustración 76. Resolución Práctica 5a - Ej 35 - Fichero 3	77
Ilustración 77. Resolución Práctica 5a - Ej 35 - Fichero 6	78
Ilustración 78. Resolución Práctica 5a - Ej 35 - Fichero 9	79
Ilustración 79. Resolución Práctica 5a - Ej 42 - Apartado a	80
Ilustración 80. Resolución Práctica 5a - Ej 42 - Apartado b	81
Ilustración 81. Resolución Práctica 5a - Ej 42 - Apartado c	82
Ilustración 82. Resolución Práctica 5a - Ej 42 - Apartado d	83
Ilustración 83. Resolución Práctica 5a - Ej 42 - Apartado e	84
Ilustración 84. Resolución Práctica 5a - Ej 42 - Apartado f	85
Ilustración 85. Resolución Práctica 5a - Ej 42 - Apartado g	85
Ilustración 86. Resolución Práctica 5a - Ej 42 - Apartado h	86
Ilustración 87. Resolución Práctica 5a - Ej 42 - Apartado i	87
Ilustración 88. Toma de pruebas Práctica 5a - Ej 45	88
Ilustración 89. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 1	89
Ilustración 90. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 2	90

Ilustración 91. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 3	90
Ilustración 92. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 4	91
Ilustración 93. Resolución Práctica 5b - Ej 3 - Apartado a - Parte 2	94
Ilustración 94. Resolución Práctica 5b - Ej 3 - Apartado b	95
Ilustración 95. Resolución Práctica 5b - Ej 3 - Apartado c	96
Ilustración 96. Resolución Práctica 5b - Ej 3 - Apartado d	97
Ilustración 97. Resolución Práctica 5b - Ej 3 - Apartado e	98
Ilustración 98. Resolución Práctica 5b - Ej 3 - Apartado f	99
Ilustración 99. Resolución Práctica 5b - Ej 3 - Apartado g	100
Ilustración 100. Resolución Práctica 5b - Ej 3 - Apartado h	101
Ilustración 101. Resolución Práctica 5b - Ej 3 - Apartado j - Parte 2	102
Ilustración 102. Resolución Práctica 5b - Ej 3 - Apartado j - Parte 3	102
Ilustración 103. Enunciado Práctica 5b - Ej 3 - Apartado k - Parte 1	103
Ilustración 104. Enunciado Práctica 5b - Ej 3 - Apartado k - Parte 2	103
Ilustración 105. Enunciado Práctica 5b - Ej 3 - Apartado k - Parte 3	103
Ilustración 106. Resolución Práctica 5b - Ej 3 - Apartado k	104
Ilustración 107. Resolución Práctica 5b - Ej 3 - Apartado l	105
Ilustración 108. Resolución Práctica 5b - Ej 3 - Apartado m - Parte 2	106
Ilustración 109. Resolución Práctica 5b - Ej 3 - Apartado p	107
Ilustración 110. Enunciado Práctica 5b - Ej 3 - Apartado q	108
Ilustración 111. Resolución Práctica 5b - Ej 3 - Apartado r	109

## Índice de tablas

Tabla 1. Resolución Practica 3 - Ej 10	35
Tabla 2. Resolución Practica 3 - Ej 14	37
Tabla 3. Resolución Práctica 3 - Ej 14 - Apartado b	39
Tabla 4. Resolución Práctica 5b - Ej 3 - Apartado a - Parte 1	94
Tabla 5. Resolución Práctica 5b - Ej 3 - Apartado j - Parte 1	102
Tabla 6. Resolución Práctica 5b - Ej 3 - Apartado m - Parte 1	105

## Consideraciones previas

- El Sistema Operativo utilizado en mi equipo personal es un Debian puro, por lo que todos los ejercicios en los que salgan capturas en el Sistema Operativo *Windows* serán en una máquina virtual, es decir, los ejercicios donde la máquina host es *Windows* en mi caso es una máquina virtual.
- Los comandos cortos se indican con el siguiente formato: comandoX > resultadoY, es decir, con fondo gris.
- Los comandos largos (varios comandos seguidos) se indican con el siguiente formato:
  - 1. # Previamente habiendo hecho un: Comando0
  - 2. Comando1 | grep “cadena”
  - 3. Comando2 | awk 3
- Si en una tabla aparece únicamente en una celda el siguiente carácter “-”, implica que no se ha encontrado nada referente a esa celda concreta.
- En algunos ejercicios donde las pruebas se usan en todos o varios subapartados, se indicará la toma de pruebas y el análisis de las mismas en el apartado correspondiente al ejercicio (ej: Práctica4-Ejercicio8) y cada subapartado compartirá las mismas pruebas salvo que se indique lo contrario (no habrá subapartados Toma de pruebas y Análisis de pruebas en cada dapartado del tipo PrácticaX-EjercicioY-ApartadoZ). De esta forma evitamos la repetición innecesaria de información.
- En la máquina de Caine 13 me identifico con el prompt de la terminal, mientras que en la máquina de Windows me identifico con un .txt que indica mi nombre, apellidos y UO en cada captura.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 17 de 109

## Objeto del peritaje

El siguiente peritaje, realizado por el alumno Eduardo Blanco Bielsa de la *Universidad de Oviedo* para la asignatura *Informática Forense y Auditoría*, tiene como objetivo responder a las siguientes preguntas y sus correspondientes subapartados, con el fin de esclarecer los hechos y proporcionar un análisis detallado sobre las evidencias digitales encontradas:

- **Práctica 2**
  - **Ejercicio 21.** Adquisición de evidencia en red incluyendo integridad hash con Bash.
  - **Ejercicio 35.** Análisis de evidencia textual con Bash.
  - **Ejercicio 36.** Análisis de evidencia textual con Bash.
  - **Ejercicio 37.** Análisis de evidencia textual con Bash.
- **Práctica 3**
  - **Ejercicio 1.** Carving de imagen JPG con Bash.
  - **Ejercicio 10.** Carving de archivos de audio con Autopsy.
  - **Ejercicio 14.** Recuperación de evidencias borradas mediante metadatos con Autopsy.
- **Práctica 4**
  - **Ejercicio 8.** (apartados: (bb, vv, xx, ccc, fff, iii, mmm, nnn, ppp, rrr, sss)). Análisis de imagen física de smartphone con Autopsy.
  - **Ejercicio 9.** (apartados: aa, bb, cc, dd, ee, ff, gg, hh, ii, jj). Análisis de imagen lógica de smartphone con Aleapp.
- **Práctica 5<sup>a</sup>**
  - **Ejercicio 28.** (apartados: i, j, k, l, m, n, o, p, q). Análisis de volcado de memoria principal con Volatility.
  - **Ejercicio 34.** (imágenes: 2, 4 y 15). Análisis de metadatos EXIF.
  - **Ejercicio 35.** (ficheros: 3, 6 y 9). Análisis de metadatos de ficheros.
  - **Ejercicio 42.** (apartados: a, b, c, d, e, f, g, h, i). Análisis de cabeceras de correo electrónico incluyendo recursos OSINT.
  - **Ejercicio 45.** (apartados: a, b, c, d, e, f, g). Análisis de registros de servicio móvil.
- **Práctica 5b**
  - **Ejercicio 3.** (todos los apartados). Análisis de resolución DNS mediante sondeo de interfaz de red en cliente web con Wireshark.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 18 de 109

# Resolución

## Práctica 2 – Ejercicio 21

### Enunciado

En algunas ocasiones es necesario adquirir las evidencias de un sistema utilizando un disco de arranque y una conexión de red a la cual está conectada la plataforma de recolección de evidencias. El ordenador del cual crearemos la imagen lo llamaremos ordenador “objetivo” y en el que almacenaremos la imagen lo llamaremos ordenador “recolector de evidencias”. Para poder realizar la imagen a través de la red necesitaremos en primer lugar hacer que el “recolector de evidencias” escuche el flujo de datos proveniente del ordenador “objetivo”. Esto puede hacerse mediante el comando netcat (nc).

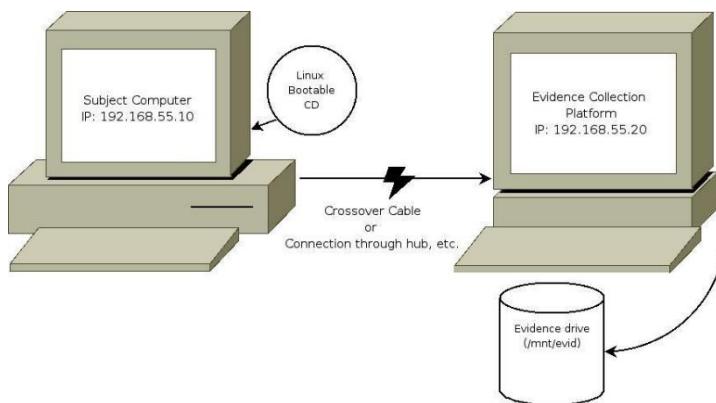


Ilustración 1. Diagrama Sujeto y Recolector de Evidencias

El primer paso será abrir una conexión de escucha en el “recolector de evidencias” y redirigir todos los datos recibidos en dicha conexión al comando dd. En la computadora objetivo debemos ejecutar el comando dd tomando como fichero de entrada el fichero que representa el disco (o la partición) del cual queremos hacer la imagen y en lugar de suministrar un fichero de salida canalizaremos la salida al comando nc en la dirección IP y puerto en la que está esperando el comando homónimo en la máquina “recolector de evidencias”. Para probar esta técnica, vamos a hacer una imagen de un dispositivo conectado a su máquina virtual IFA-UD-XX en su máquina virtual IFA-AU-XX. Para ello modifique los interfaces de red de ambas máquinas y colóquelos en modo “adaptador puente”. En segundo lugar añada un filtro para el lápiz USB que va a conectar a la máquina IFA-UD-XX. Si ya tenía un filtro creado para dicho dispositivo en la máquina IFA-AU-XX, elimínelo primero. Una vez añadido el filtro, conecte dicho dispositivo a la máquina IFA-UD-XX y compruebe que ha sido detectado por el Sistema Operativo de dicha máquina. Haga un hash del dispositivo del cual va a crear la imagen antes de realizarla. Luego haga la imagen utilizando el procedimiento descrito anteriormente para lo cual tendrá que averiguar la IP de la máquina que asume el rol de “recolector de evidencias”. Una vez concluido el proceso de realización de la imagen, haga un hash en destino del fichero de imagen y compruebe si coincide con el hash del dispositivo del cual ha realizado la imagen en origen.

## Toma de pruebas

El dispositivo que se usará será el siguiente USB 2.0 genérico de 2GB:



Ilustración 2. Dispositivo en uso Práctica 2 - Ejercicio 21

Tenemos que configurar previamente las máquinas de Caine y Ubuntu con el adaptador de red en puente (Bridge):

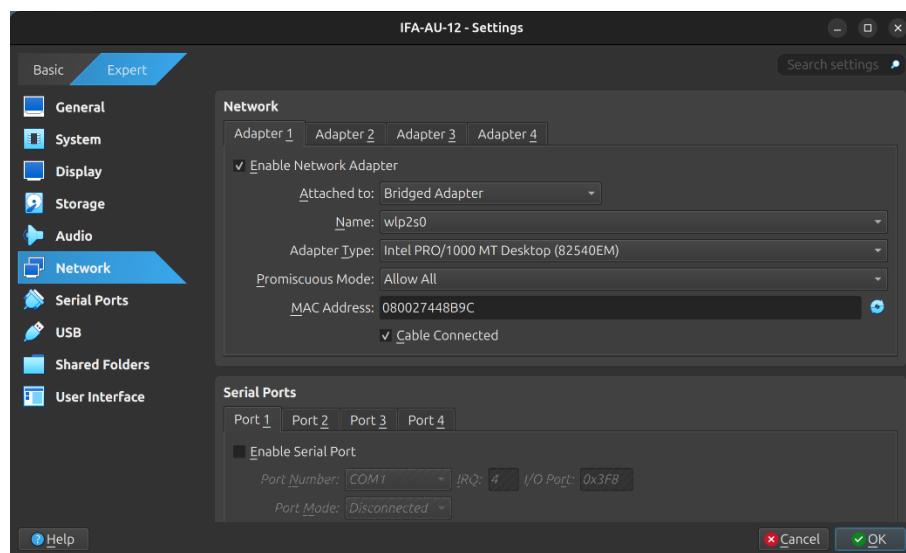


Ilustración 3. Configuración Bridge Caine 13

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 20 de 109

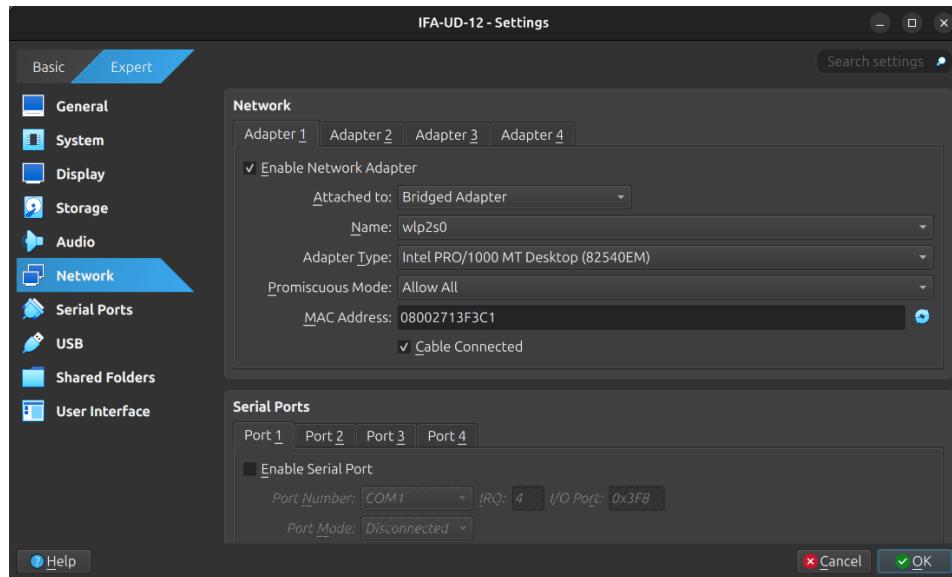


Ilustración 4. Configuración Bridge Ubuntu Desktop

Ahora añadiremos un filtro para la unidad USB en la máquina de Ubuntu Desktop:

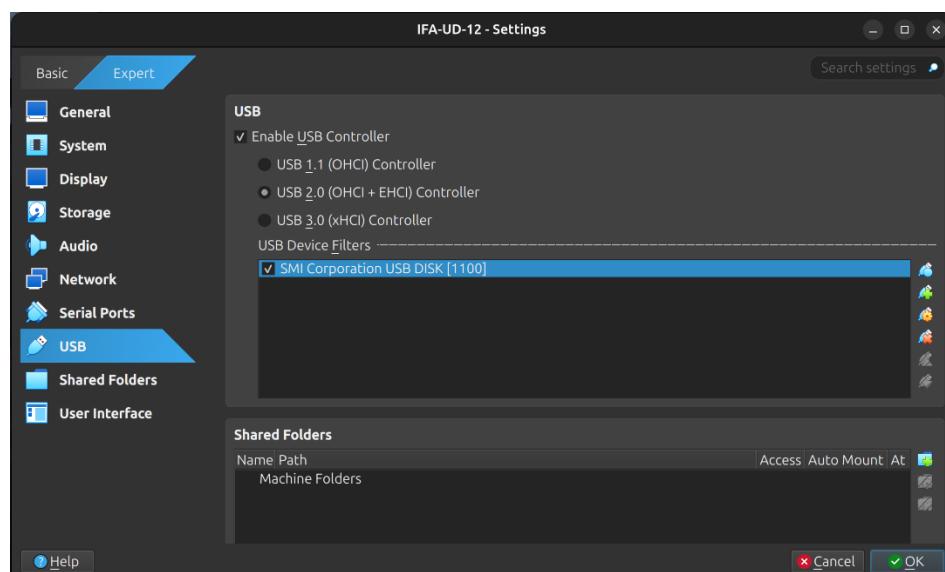
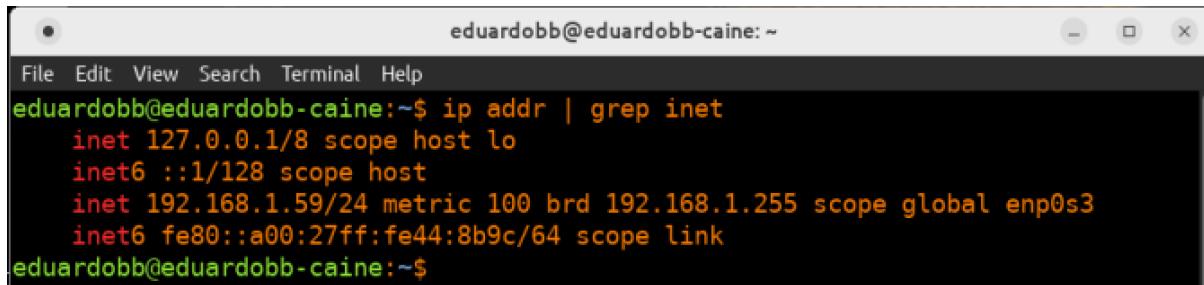


Ilustración 5. Filtro para la unidad USB

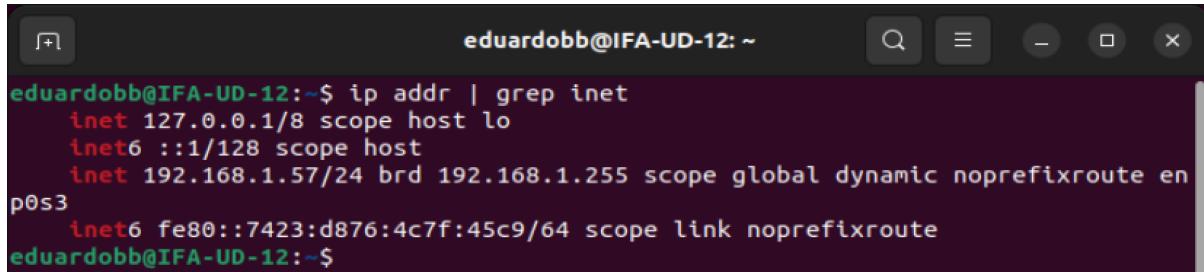
- Ahora arrancaremos las dos máquinas y comprobaremos que se pueden comunicar mediante peticiones ping:
  - Comprobaremos las ips de ambos equipos con el comando `ip addr | grep inet`

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 21 de 109



```
eduardobb@eduardobb-caine:~$ ip addr | grep inet
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            inet 192.168.1.59/24 metric 100 brd 192.168.1.255 scope global enp0s3
                inet6 fe80::a00:27ff:fe44:8b9c/64 scope link
eduardobb@eduardobb-caine:~$
```

Ilustración 6. Ip de Caine 13



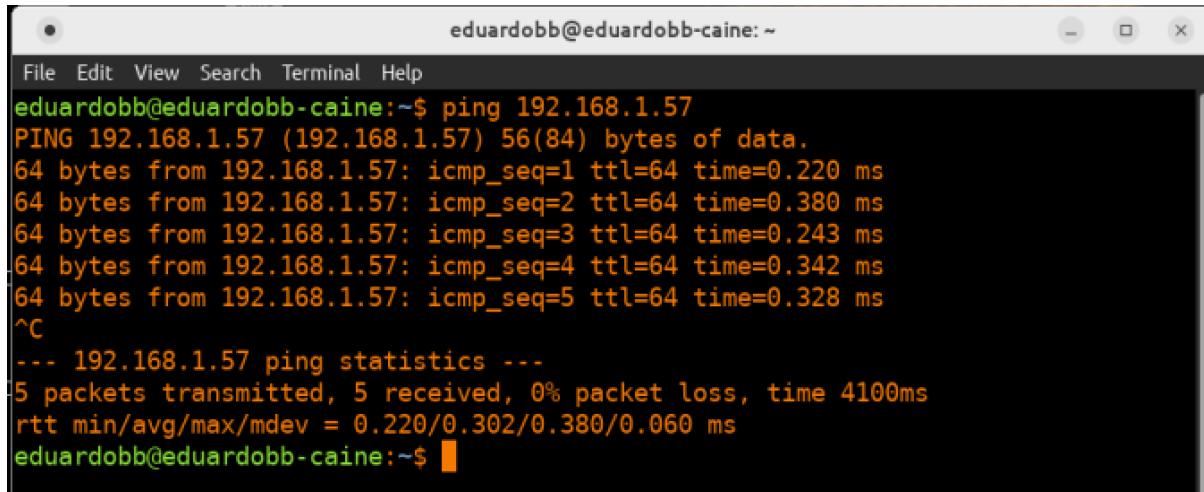
```
eduardobb@IFA-UD-12:~$ ip addr | grep inet
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            inet 192.168.1.57/24 brd 192.168.1.255 scope global dynamic noprefixroute en
p0s3
                inet6 fe80::7423:d876:4c7f:45c9/64 scope link noprefixroute
eduardobb@IFA-UD-12:~$
```

Ilustración 7. Ip de Ubuntu Desktop

Vemos las siguientes direcciones de red:

- **Caine 13:** 192.168.1.59
- **Ubuntu Desktop:** 192.168.1.57

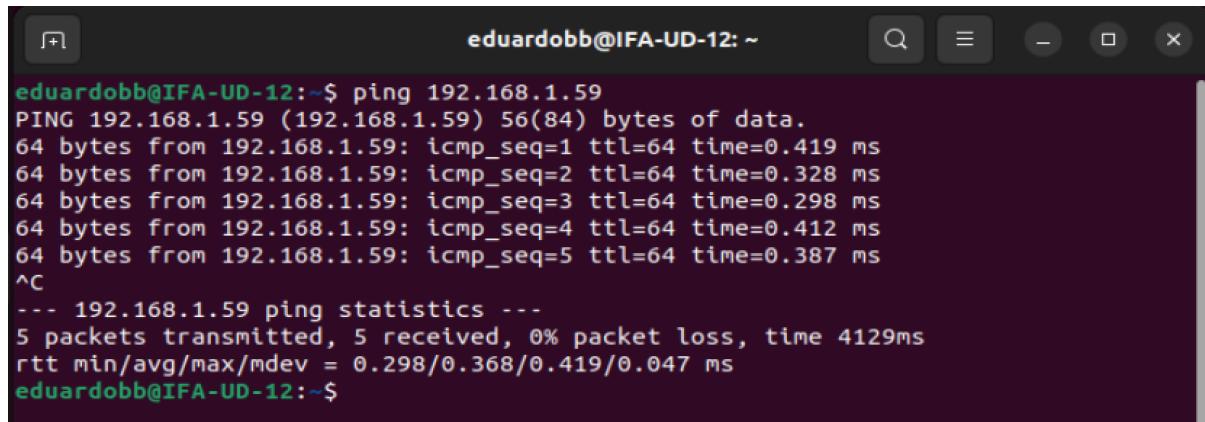
Procedemos a comprobar la comunicación bidireccional:



```
eduardobb@eduardobb-caine:~$ ping 192.168.1.57
PING 192.168.1.57 (192.168.1.57) 56(84) bytes of data.
64 bytes from 192.168.1.57: icmp_seq=1 ttl=64 time=0.220 ms
64 bytes from 192.168.1.57: icmp_seq=2 ttl=64 time=0.380 ms
64 bytes from 192.168.1.57: icmp_seq=3 ttl=64 time=0.243 ms
64 bytes from 192.168.1.57: icmp_seq=4 ttl=64 time=0.342 ms
64 bytes from 192.168.1.57: icmp_seq=5 ttl=64 time=0.328 ms
^C
--- 192.168.1.57 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4100ms
rtt min/avg/max/mdev = 0.220/0.302/0.380/0.060 ms
eduardobb@eduardobb-caine:~$
```

Ilustración 8. Comunicación ping de Caine 13 a Ubuntu Desktop

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 22 de 109

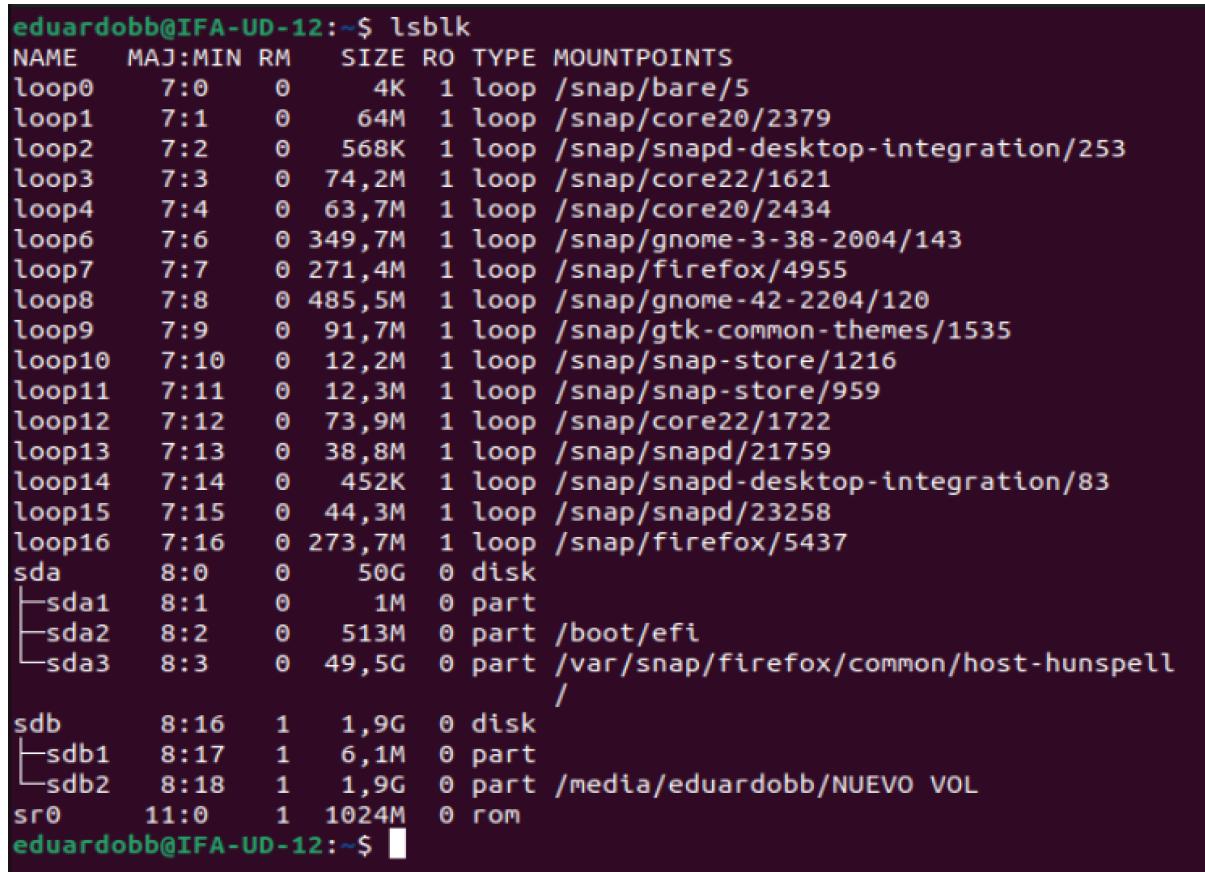


```
eduardobb@IFA-UD-12:~$ ping 192.168.1.59
PING 192.168.1.59 (192.168.1.59) 56(84) bytes of data.
64 bytes from 192.168.1.59: icmp_seq=1 ttl=64 time=0.419 ms
64 bytes from 192.168.1.59: icmp_seq=2 ttl=64 time=0.328 ms
64 bytes from 192.168.1.59: icmp_seq=3 ttl=64 time=0.298 ms
64 bytes from 192.168.1.59: icmp_seq=4 ttl=64 time=0.412 ms
64 bytes from 192.168.1.59: icmp_seq=5 ttl=64 time=0.387 ms
^C
--- 192.168.1.59 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4129ms
rtt min/avg/max/mdev = 0.298/0.368/0.419/0.047 ms
eduardobb@IFA-UD-12:~$
```

Ilustración 9. Comunicación ping de Ubuntu Desktop a Caine 13

Por tanto, queda confirmado que ambos equipos **pueden comunicarse**.

- Comprobamos que el USB se haya montado correctamente con lsblk:



```
eduardobb@IFA-UD-12:~$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0    7:0     0    4K  1 loop /snap/bare/5
loop1    7:1     0   64M  1 loop /snap/core20/2379
loop2    7:2     0  568K  1 loop /snap/snapd-desktop-integration/253
loop3    7:3     0 74,2M  1 loop /snap/core22/1621
loop4    7:4     0 63,7M  1 loop /snap/core20/2434
loop6    7:6     0 349,7M  1 loop /snap/gnome-3-38-2004/143
loop7    7:7     0 271,4M  1 loop /snap/firefox/4955
loop8    7:8     0 485,5M  1 loop /snap/gnome-42-2204/120
loop9    7:9     0 91,7M  1 loop /snap/gtk-common-themes/1535
loop10   7:10    0 12,2M  1 loop /snap/snap-store/1216
loop11   7:11    0 12,3M  1 loop /snap/snap-store/959
loop12   7:12    0 73,9M  1 loop /snap/core22/1722
loop13   7:13    0 38,8M  1 loop /snap/snapd/21759
loop14   7:14    0 452K  1 loop /snap/snapd-desktop-integration/83
loop15   7:15    0 44,3M  1 loop /snap/snapd/23258
loop16   7:16    0 273,7M  1 loop /snap/firefox/5437
sda      8:0     0   50G  0 disk
└─sda1   8:1     0    1M  0 part
└─sda2   8:2     0  513M  0 part /boot/efi
└─sda3   8:3     0 49,5G  0 part /var/snap/firefox/common/host-hunspell
/
sdb      8:16    1  1,9G  0 disk
└─sdb1   8:17    1  6,1M  0 part
└─sdb2   8:18    1  1,9G  0 part /media/eduardobb/NUEVO VOL
sr0     11:0    1 1024M 0 rom
eduardobb@IFA-UD-12:~$
```

Ilustración 10. Comprobación montaje USB

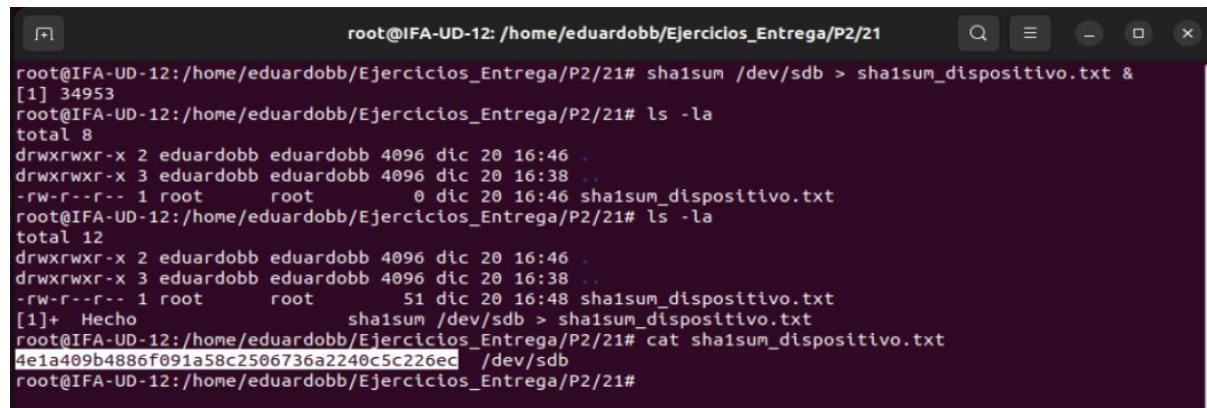
Aparece como *sdb* y tiene dos particiones.

## Resultados obtenidos

Ahora como **root**, primero realizaremos un hash del dispositivo del cuál haremos la imagen (usaremos SHA1):

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 23 de 109

```
1. # Previamente habiendo hecho un: sudo su  
2. sha1sum /dev/sdb > sha1sum_dispositivo.txt &
```

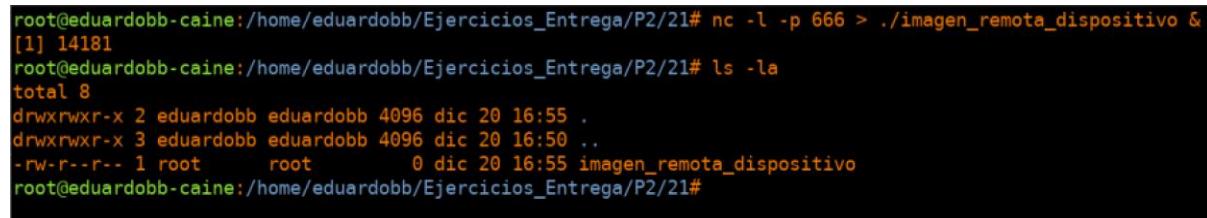


```
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21# sha1sum /dev/sdb > sha1sum_dispositivo.txt &  
[1] 34953  
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la  
total 8  
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 16:46 .  
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:38 ..  
-rw-r--r-- 1 root root 0 dic 20 16:46 sha1sum_dispositivo.txt  
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la  
total 12  
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 16:46 .  
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:38 ..  
-rw-r--r-- 1 root root 51 dic 20 16:48 sha1sum_dispositivo.txt  
[1]+ Hecho sha1sum /dev/sdb > sha1sum_dispositivo.txt  
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21# cat sha1sum_dispositivo.txt  
4e1a409b4886f091a58c2506736a2240c5c226ec /dev/sdb  
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21#
```

Ilustración 11. Resolución Práctica 2 - Ej 21 - Parte 1

Ahora, en nuestra máquina Caine ejecutaremos este otro comando (como **root**):

```
1. nc -l -p 666 > ./imagen_remota_dispositivo &
```

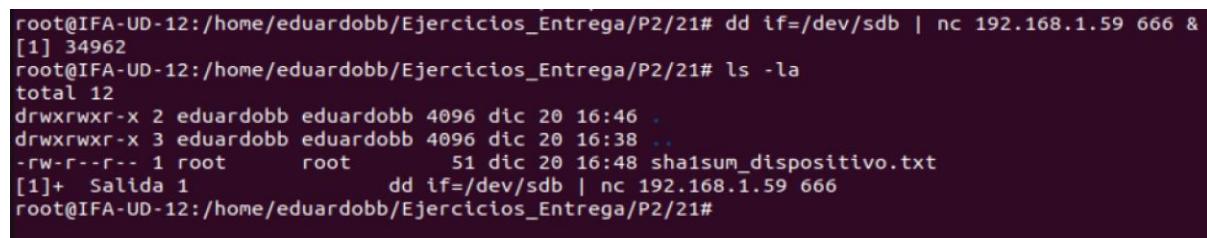


```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# nc -l -p 666 > ./imagen_remota_dispositivo &  
[1] 14181  
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la  
total 8  
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 16:55 .  
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:50 ..  
-rw-r--r-- 1 root root 0 dic 20 16:55 imagen_remota_dispositivo  
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21#
```

Ilustración 12. Resolución Práctica 2 - Ej 21 - Parte 2

Entonces, en nuestra máquina Ubuntu ejecutaremos el siguiente comando (como **root**):

```
1. dd if=/dev/sdb | nc 192.158.1.59 666 &
```



```
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21# dd if=/dev/sdb | nc 192.158.1.59 666 &  
[1] 34962  
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la  
total 12  
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 16:46 .  
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:38 ..  
-rw-r--r-- 1 root root 51 dic 20 16:48 sha1sum_dispositivo.txt  
[1]+ Salida 1 dd if=/dev/sdb | nc 192.158.1.59 666  
root@IFA-UD-12:/home/eduardobb/Ejercicios_Entrega/P2/21#
```

Ilustración 13. Resolución Práctica 2 - Ej 21 - Parte 3

Vemos que se creará la imagen del dispositivo de Ubuntu Desktop en nuestra máquina Caine:

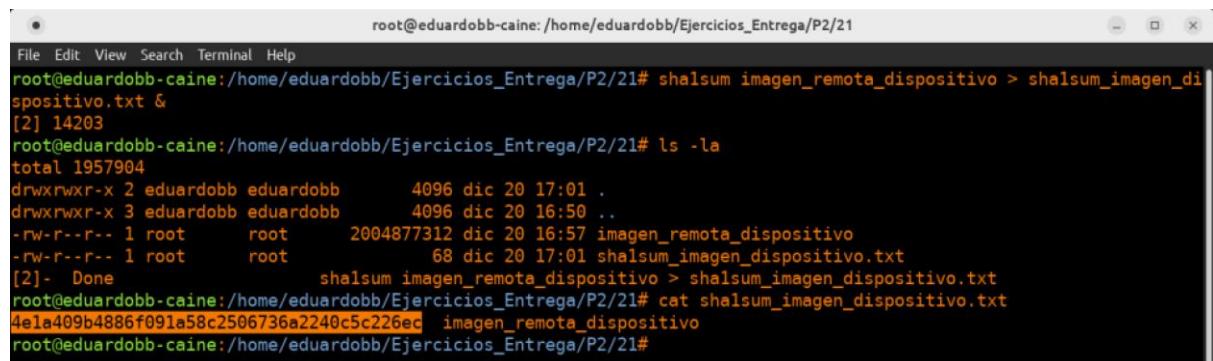
Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 24 de 109

```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la
total 1957900
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 16:55 .
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:50 ..
-rw-r--r-- 1 root root 2004877312 dic 20 16:57 imagen_remota_dispositivo

[1]+ Stopped nc -l -p 666 > ./imagen_remota_dispositivo
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la
total 1957900
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 16:55 .
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:50 ..
-rw-r--r-- 1 root root 2004877312 dic 20 16:57 imagen_remota_dispositivo
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21#
```

Ilustración 14. Resolución Práctica 2 - Ej 21 - Parte 4

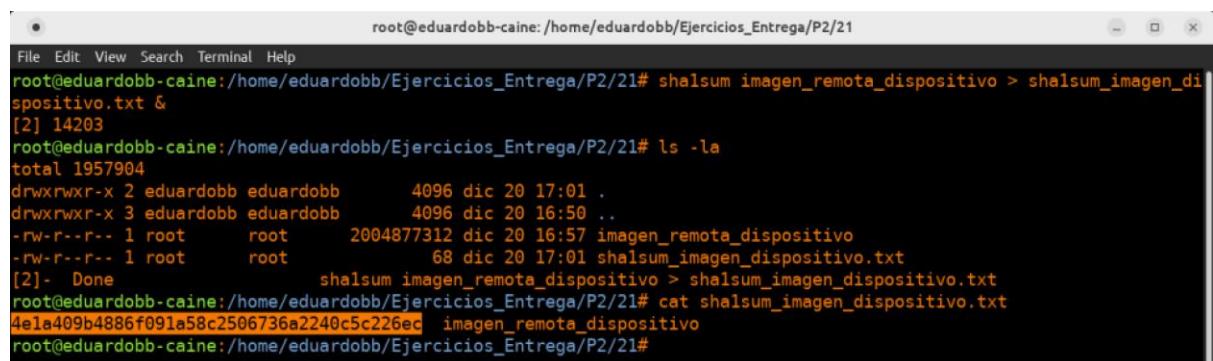
Por último, realizaremos un hash (utilizando SHA1) de la imagen en Caine para comprobar que coincide con el hash del dispositivo realizado en Ubuntu Desktop (también como **root**):



```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# shasum imagen_remota_dispositivo > shasum_imagen_dispositivo.txt &
[2] 14203
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la
total 1957904
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 17:01 .
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:50 ..
-rw-r--r-- 1 root root 2004877312 dic 20 16:57 imagen_remota_dispositivo
-rw-r--r-- 1 root root 68 dic 20 17:01 shasum_imagen_dispositivo.txt
[2]- Done shasum imagen_remota_dispositivo > shasum_imagen_dispositivo.txt
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# cat shasum_imagen_dispositivo.txt
4e1a409b4886f091a58c2506736a2240c5c226ec imagen_remota_dispositivo
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21#
```

Ilustración 15. Resolución Práctica 2 - Ej 21 - Parte 5

#### 1. shasum imagen\_remota\_dispositivo > shasum\_imagen\_dispositivo.txt &



```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# shasum imagen_remota_dispositivo > shasum_imagen_dispositivo.txt &
[2] 14203
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# ls -la
total 1957904
drwxrwxr-x 2 eduardobb eduardobb 4096 dic 20 17:01 .
drwxrwxr-x 3 eduardobb eduardobb 4096 dic 20 16:50 ..
-rw-r--r-- 1 root root 2004877312 dic 20 16:57 imagen_remota_dispositivo
-rw-r--r-- 1 root root 68 dic 20 17:01 shasum_imagen_dispositivo.txt
[2]- Done shasum imagen_remota_dispositivo > shasum_imagen_dispositivo.txt
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21# cat shasum_imagen_dispositivo.txt
4e1a409b4886f091a58c2506736a2240c5c226ec imagen_remota_dispositivo
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/21#
```

Ilustración 16. Resolución Práctica 2 - Ej 21 - Parte 6

Podemos contrastar ambos hashes y comprobar que son idénticos:

- En **Caine**: 4e1a409b4886f091a58c2506736a2240c5c226ec
- En **Ubuntu**: 4e1a409b4886f091a58c2506736a2240c5c226ec

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 25 de 109

Utilizando una herramienta como [Text Compare](#):

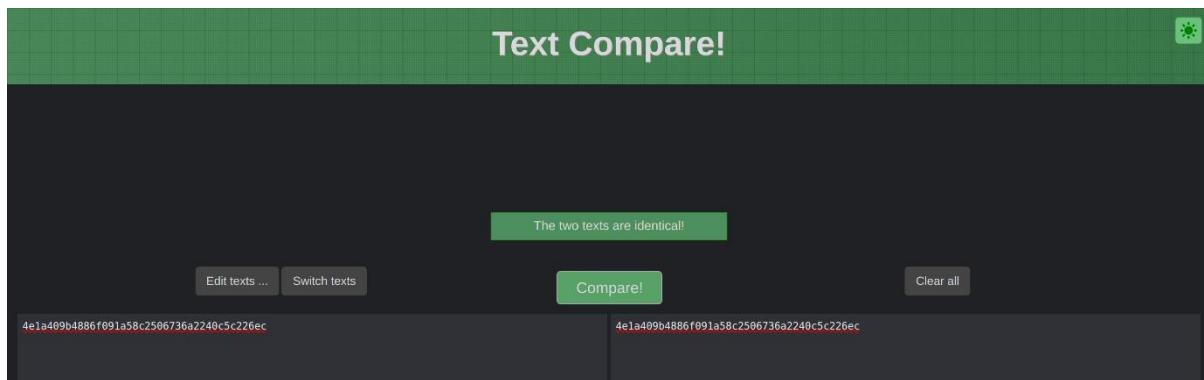


Ilustración 17. Resolución Práctica 2 - Ej 21 - Parte 7

## Conclusiones

Por tanto, que coincidan los hashes nos asegura que no se ha roto la cadena de custodia y por tanto dicha imagen pertenece a dicho dispositivo, y no ha sufrido ningún cambio.

## Práctica 2 – Ejercicio 35

### Enunciado

Busca, en los ficheros de log anteriores, todas las entradas correspondientes al 13 de noviembre.

### Toma de pruebas

Primero descargamos el fichero "Recursos de Prácticas-> Práctica 2-> logs.v3.tar.gz" tal y como indica el enunciado y lo descomprimimos con el comando tar -xvzf logs.v3.tar.gz:

```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35
File Edit View Search Terminal Help
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35# ls
logs.v3.tar.gz
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35# tar -xvzf logs.v3.tar.gz
messages
messages.1
messages.2
messages.3
messages.4
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35# ls
logs.v3.tar.gz messages messages.1 messages.2 messages.3 messages.4
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35#
```

A terminal window showing a root shell on the 'eduardobb-caine' host. The user runs 'ls' to show the file 'logs.v3.tar.gz'. Then they run 'tar -xvzf logs.v3.tar.gz' to extract the contents. After extraction, they run 'ls' again to show five files: 'logs.v3.tar.gz', 'messages', 'messages.1', 'messages.2', 'messages.3', and 'messages.4'. The terminal has a dark theme with white text and a light gray background.

Ilustración 18. Descarga recursos del ejercicio

### Análisis de las pruebas

Las pruebas se han sometido a un proceso de filtrado manual.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 26 de 109

## Resultados obtenidos

Para buscar todas las entradas correspondientes al 13 de noviembre usaremos el siguiente comando:

```
1. cat messages* | grep ^"Nov[ ]*13"
2. # Otra alternativa sería usar: cat messages* | grep ^"Nov 13"
```

```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35# cat messages* | grep ^"Nov[ ]*13"
Nov 13 04:05:46 hostname123 su[pm_unix][10635]: session opened for user news by (uid=0)
Nov 13 04:05:46 hostname123 su[pm_unix][10635]: session closed for user news
Nov 13 20:08:33 hostname123 login[pm_unix][1069]: bad username []
Nov 13 20:08:33 hostname123 login[pm_unix][1069]: FAILED LOGIN 1 FROM (null) FOR , Authentication failure
Nov 13 20:08:33 hostname123 login[pm_unix][1069]: bad username []
Nov 13 20:08:33 hostname123 login[pm_unix][1069]: FAILED LOGIN 2 FROM (null) FOR , Authentication failure
Nov 13 20:08:39 hostname123 login[pm_unix][1069]: authentication failure; logname=LOGIN uid=0 euid=0 tty=ttyl ruser= rhost= user=root
Nov 13 20:08:41 hostname123 login[pm_unix][1069]: FAILED LOGIN 3 FROM (null) FOR root, Authentication failure
Nov 13 20:08:49 hostname123 login[pm_unix][1069]: session opened for user root by LOGIN(uid=0)
Nov 13 20:08:49 hostname123 .. root[1069]: ROOT LOGIN ON ttyl
Nov 13 20:14:14 hostname123 shutdown: shutting down for system halt
Nov 13 20:14:15 hostname123 init: Switching to runlevel: 0
Nov 13 20:14:15 hostname123 login[pm_unix][1069]: session closed for user root
Nov 13 20:14:17 hostname123 atd: atd shutdown succeeded
Nov 13 20:14:17 hostname123 Font Server[976]: terminating
Nov 13 20:14:18 hostname123 xfs: xfs shutdown succeeded
Nov 13 20:14:19 hostname123 gpm: gpm shutdown succeeded
Nov 13 20:14:19 hostname123 squid: Stopping squid
Nov 13 20:14:21 hostname123 squid:
Nov 13 20:14:50 hostname123 last message repeated 14 times
Nov 13 20:14:51 hostname123 squid[1045]: Squid Parent: child process 1047 exited with status 0
Nov 13 20:14:52 hostname123 squid:
Nov 13 20:14:52 hostname123 sshd: sshd -TERM succeeded
Nov 13 20:14:53 hostname123 sshd[853]: Received signal 15: terminating.
Nov 13 20:14:53 hostname123 xinetd[886]: Exiting...
Nov 13 20:14:53 hostname123 crond: crond shutdown succeeded
Nov 13 20:14:54 hostname123 dd: 1+0 records in
Nov 13 20:14:54 hostname123 dd: 1+0 records out
Nov 13 20:14:54 hostname123 random: Saving random seed: succeeded
Nov 13 20:14:54 hostname123 kernel: Kernel logging (proc) stopped.
Nov 13 20:14:54 hostname123 kernel: Kernel log daemon terminating.
Nov 13 20:14:55 hostname123 syslog: klogd shutdown succeeded
Nov 13 20:14:55 hostname123 exiting on signal 15
Nov 13 20:17:02 hostname123 syslogd 1.4.1: restart.
Nov 13 20:17:03 hostname123 syslog: syslogd startup succeeded
Nov 13 20:17:03 hostname123 syslog: klogd startup succeeded
Nov 13 20:17:03 hostname123 kernel: klogd 1.4.1, log source = /proc/kmsg started.
Nov 13 20:17:03 hostname123 kernel: Linux version 2.4.18-3 (bhcompile@daffy.perf.redhat.com) (gcc version 2.96 20000731 (Red Hat Linux 7.3 2.96-110)) #1 Thu Apr 18 07:37:53
```

Ilustración 19. Resolución Práctica 2 - Ej 35 - Parte 1

```
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35
File Edit View Search Terminal Help
Nov 13 20:17:03 hostname123 kernel: Mount-cache hash table entries: 4096 (order: 3, 32768 bytes)
Nov 13 20:17:03 hostname123 kernel: Buffer cache hash table entries: 16384 (order: 4, 65536 bytes)
Nov 13 20:17:03 hostname123 kernel: Page-cache hash table entries: 65536 (order: 6, 262144 bytes)
Nov 13 20:17:03 hostname123 kernel: CPU: L1 I cache: 16K, L1 D cache: 16K
Nov 13 20:17:03 hostname123 kernel: CPU: L2 cache: 512K
Nov 13 20:17:03 hostname123 kernel: Intel machine check architecture supported.
Nov 13 20:17:03 hostname123 keytable: Loading keymap: succeeded
Nov 13 20:17:03 hostname123 kernel: Intel machine check reporting enabled on CPU#0.
Nov 13 20:17:03 hostname123 kernel: CPU: Intel Pentium II (Klamath) stepping 04
Nov 13 20:17:03 hostname123 kernel: Checking 'ht' instruction... OK.
Nov 13 20:17:03 hostname123 kernel: POSIX conformance testing by UNIFIX
Nov 13 20:17:03 hostname123 kernel: mtrr: v1.49 (20010327) Richard Gooch (rgooch@atnf.csiro.au)
Nov 13 20:17:03 hostname123 kernel: mtrr: detected mtrr type: Intel
Nov 13 20:17:03 hostname123 kernel: PCI: PCI BIOS revision 2.10 entry at 0xfd9b3, last bus=1
Nov 13 20:17:03 hostname123 kernel: PCI: Using configuration type 1
Nov 13 20:17:03 hostname123 kernel: PCI: Probing PCI hardware
Nov 13 20:17:03 hostname123 kernel: Unknown Bridge resource 0: assuming transparent
Nov 13 20:17:03 hostname123 kernel: Unknown bridge resource 1: assuming transparent
Nov 13 20:17:03 hostname123 kernel: Unknown bridge resource 2: assuming transparent
Nov 13 20:17:03 hostname123 kernel: PCI: Using IRQ router PIIX [8086/7110] at 00:07.0
Nov 13 20:17:03 hostname123 kernel: Limiting direct PCI/PCI transfers.
Nov 13 20:17:03 hostname123 kernel: isapnp: Scanning for PnP cards...
Nov 13 20:17:03 hostname123 kernel: isapnp: No Plug & Play device found
Nov 13 20:17:03 hostname123 kernel: Linux NET4.0 for Linux 2.4
Nov 13 20:17:03 hostname123 keytable: Loading system font: succeeded
Nov 13 20:17:03 hostname123 kernel: Based upon Swansea University Computer Society NET3.039
Nov 13 20:17:03 hostname123 kernel: Initializing RT netlink socket
Nov 13 20:17:03 hostname123 kernel: apm: BIOS version 1.2 Flags 0x03 (Driver version 1.16)
Nov 13 20:17:03 hostname123 kernel: Starting kswapd
Nov 13 20:17:03 hostname123 kernel: VFS: Diskquotas version dquot_6.5.0 initialized
Nov 13 20:17:03 hostname123 kernel: Detected PS/2 Mouse Port.
Nov 13 20:17:03 hostname123 kernel: pty: 2048 Unix98 ptys configured
Nov 13 20:17:03 hostname123 kernel: Serial driver version 5.05c (2001-07-08) with MANY_PORTS MULTIPORT SHARE_IRQ SERIAL_PCI ISAPNP enabled
Nov 13 20:17:03 hostname123 kernel: tty500 at 0x03f8 (irq = 4) is a 16550A
Nov 13 20:17:04 hostname123 kernel: Real Time Clock Driver V1.10e
Nov 13 20:17:04 hostname123 kernel: block: 496 slots per queue, batch=124
Nov 13 20:17:04 hostname123 kernel: Uniform Multi-Platform E-IDE driver Revision: 6.31
Nov 13 20:17:04 hostname123 kernel: ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
Nov 13 20:17:04 hostname123 kernel: PIIX4: IDE controller on PCI bus 00 dev 39
Nov 13 20:17:04 hostname123 kernel: PIIX4: chipset revision 1
Nov 13 20:17:04 hostname123 random: Init
root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35#
```

Ilustración 20. Resolución Práctica 2 - Ej 35 - Parte 2

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 27 de 109

## Conclusiones

Se encontraron múltiples entradas correspondientes al 13 de noviembre en los logs de mensajes.

## Práctica 2 – Ejercicio 36

### Enunciado

Busca, en los ficheros de log anteriores, todas las entradas en las que aparezca "Did not receive identification string from" y mostrar para cada una de ellas el mes, día, hora e IP.

### Toma de pruebas

Ya se cuenta con los ficheros correspondientes del ejercicio previo.

### Análisis de las pruebas

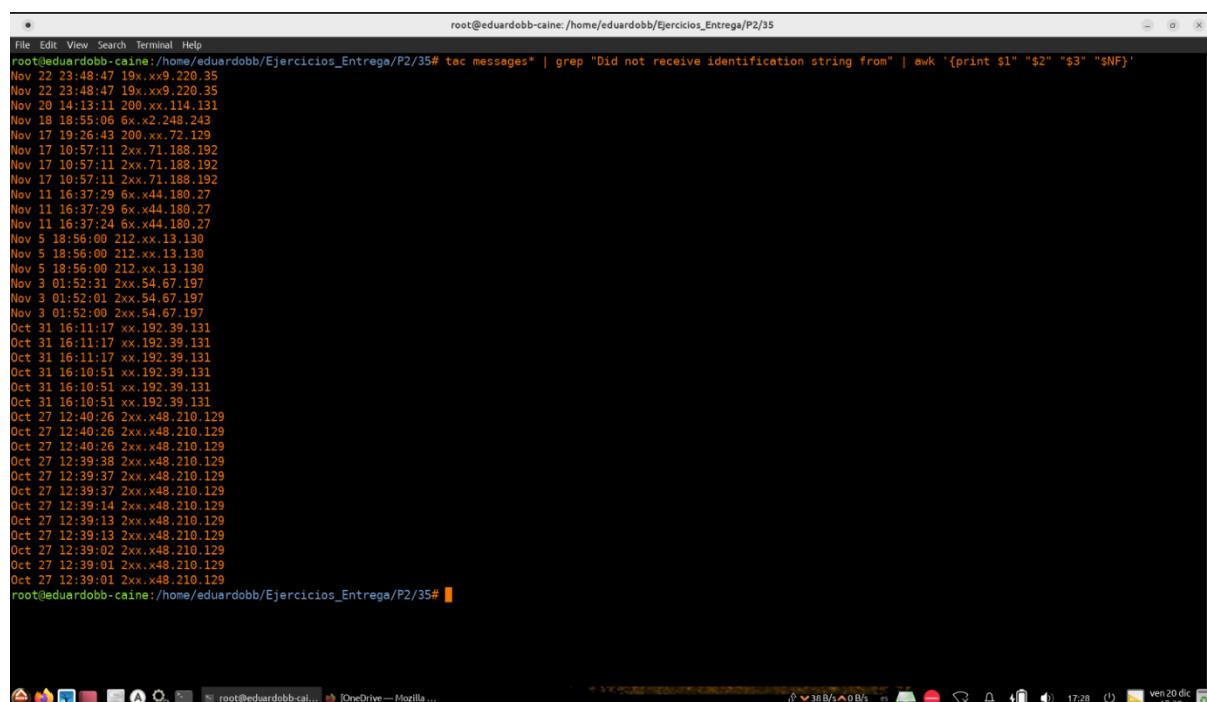
Las pruebas se han sometido a un proceso de filtrado manual.

### Resultados obtenidos

Para buscar todas las entradas en las que aparezca "Did not receive identification string from" y mostrar para cada una de ellas el mes, día, hora e IP, ejecutaremos el siguiente comando:

- *El \$NF es para sacar el elemento de la última columna*

```
1. tac messages* | grep "Did not receive identification string from" | awk '{print $1" "$2" "$3" "$NF}'
```



The terminal window shows the command being run and its output. The command is: `tac messages* | grep "Did not receive identification string from" | awk '{print $1" "$2" "$3" "$NF}'`. The output lists numerous entries, each consisting of a date and time followed by an IP address. For example, Nov 22 23:48:47 19.x.x.220.35, Nov 20 14:13:11 200.xx.114.131, Nov 18 18:55:06 6x.x2.248.243, etc. The terminal prompt at the bottom is `root@eduardobb-caine:/home/eduardobb/Ejercicios_Entrega/P2/35#`.

Ilustración 21. Resolución Práctica 2 - Ej 36

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 28 de 109

## Conclusiones

Se encontraron múltiples entradas correspondientes con la cadena requerida y se ha aprendido a realizar un filtrado con awk y el uso del operador `$NF` para indicar la última columna.

## Práctica 2 – Ejercicio 37

### Enunciado

Descargue del Campus Virtual una imagen denominada Recursos de Prácticas- >Práctica 2->minimagen.dd. Suponga que dicha imagen es la de un dispositivo que pertenece a un empleado de una multinacional que amenaza a la misma con desatar un virus si no se le paga un rescate de 50000\$. Para resolver este ejercicio utilizaremos en primer lugar herramientas de línea de comandos. Busque en el contenido de la imagen (en el espacio no asignado y en el espacio de fragmentación interna de los archivos que se puedan encontrar) palabras clave como “\$50,000”, “virus” o “ransom” (rescate) o variaciones de las mismas, tanto en mayúsculas como e minúsculas. Investigue para ello las posibilidades que le ofrece el comando grep y sus diferentes opciones. Almacene los Resultados obtenidos en un fichero de salida para luego analizar lo encontrado.

### Toma de pruebas

Descargaremos la imagen que nos indica el ejercicio en "Recursos de Prácticas-> Práctica 2->minimagen.dd".

### Análisis de las pruebas

Las pruebas se han sometido a un proceso de filtrado manual.

### Resultados obtenidos

Creamos la wordlist busqueda.txt:

- 1. 50,000
- 2. virus
- 3. VIRUS
- 4. Virus
- 5. ransom
- 6. RANSOM
- 7. Ransom

Ahora ejecutaremos el siguiente comando para buscar coincidencias dentro de la imagen:

```
1. tr '[:cntrl:]' '\n' < minimagen.dd | grep -abif busqueda.txt > resultado.txt
```

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 29 de 109

```
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P2/37$ ls
minimagen.dd
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P2/37$ vim busqueda.txt
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P2/37$ cat busqueda.txt
50,000
virus
VIRUS
Virus
ransom
RANSOM
Ransom
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P2/37$ tr '[:cntrl:]' '\n' < minimagen.dd | grep -abif busqueda.txt > resultado.txt
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P2/37$ cat resultado.txt
7449: http://www.umich.edu/~doug/virus-faq.html
75441: you and your entire business ransom.
75500: I have had enough of your mindless corporate piracy and will no longer stand for it. You will receive another letter next week. It will have a single bank account number and bank name. I want you to deposit $50,000 in the account the day you receive the letter.
75767: Don't try anything, and don't contact the cops. If you do, I will unleash a virus that will bring down your whole network and destroy your consumer's confidence.
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P2/37$
```

Ilustración 22. Resolución Práctica 2 - Ej 37

Como podemos apreciar, hay tres coincidencias:

- La primera hace referencia a lo que podría ser un enlace sobre información del virus que se ha ejecutado o quizás esté relacionada con el rescate
- La segunda y la tercera son amenazas e instrucciones por parte de un supuesto ciberdelicuente o grupo cibercriminal.

## Conclusiones

Este ejercicio es una simulación del módulo de Autopsy **KeywordSearch**.

Dadas las evidencias obtenidas podemos suponer que un ciberdelicuente o un grupo cibercriminal está extorsionando a una persona concreta.

## Práctica 3 – Ejercicio 1

### Enunciado

Realice este ejercicio en la máquina virtual donde ha instalado CAINE (IFA-AU-XX). En este caso vamos a realizar una práctica de carving de forma artesanal. Descarga del campus virtual (Recursos Prácticas-Práctica 3), el fichero L0\_Graphic.dd.bz2 y descomprímelo (bunzip2 -f L0\_Graphic.dd.bz2). Una vez descomprimido, tendrá un fichero denominado nombre\_fichero.dd. Vamos a utilizar el comando dd como unas “tijeras” para perfilar una imagen JPG contenida en el fichero anterior. Para usar el comando dd deberemos saber dónde comienza la imagen y donde debemos parar de “cortar”. Lo primero que debemos hacer es buscar el comienzo de la imagen. Una forma de buscar el inicio de la imagen dentro del fichero es buscar el patrón ffdb. En la misma línea que aparezca ese patrón debe aparecer la cadena “JFIF”. Si no fuese así, siga buscando la siguiente ocurrencia del patrón. Apunte el offset mostrado al principio de la línea por xxd ya que en esa línea se encuentra el

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 30 de 109

inicio del fichero JPG. Pase dicho offset a decimal. Ese será el comienzo real de la imagen en el conjunto de bytes anterior. Una vez tenemos localizado el comienzo de la imagen buscaremos a partir de ese punto el final de la misma; el patrón en este caso que debemos buscar es ffd9. Anotaremos el offset del comienzo de la línea donde aparece dicho patrón. Convertiremos dicho offset a decimal. Debemos de tener en cuenta que el offset es el del comienzo de la línea donde aparece el patrón y por tanto deberemos añadir tantos bytes a dicho offset como 2xnumero\_grupos\_hexadecimales anteriores al patrón ffd9. Calcularemos la diferencia entre el offset final e inicial y tendremos el tamaño del fichero de imagen que queremos extraer. Ya solo nos resta extraer la imagen utilizando el comando dd con las opciones skip (para posicionarnos en el offset de inicio del fichero dentro de la imagen), bs=1 (tamaño de bloque igual a 1 byte) y count (número de bloques de tamaño bs a cortar).

## Toma de pruebas

Descargaremos el fichero "L0\_Graphic.dd.bz2" y lo descomprimiremos con el comando bunzip2 –f L0\_Graphic.dd.bz2

## Análisis de las pruebas

Se han sometido las pruebas a un proceso de recuperación de datos borrados mediante técnicas de carving manuales.

## Resultados obtenidos

Buscaremos utilizando **xxd** los ficheros JFIF (imágenes) dentro de la imagen:

```
1. xxd L0_Graphic.dd | grep JFIF
```

```
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P3/1$ bunzip2 -f L0_Graphic.dd.bz2
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P3/1$ ls
L0_Graphic.dd
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P3/1$ xxd L0_Graphic.dd | grep JFIF
01bc8c00: ffdb ffdb 0010 4a46 4946 0001 0201 0096 .....JFIF.....
0230fd90: 4f50 524d 4c4d 4a46 4946 424d 4f49 464b OPRMLMJFIFBMOIFK
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P3/1$
```

Ilustración 23. Resolución Práctica 3 - Ej 1 - Parte 1

Anotamos el offset del comienzo de la línea donde aparece dicho patrón (0x01bc8c00) ejecutando el siguiente comando:

```
1. echo $((0x01bc8c00))
2. 29133824
```

```
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P3/1$ echo $((0x01bc8c00))
29133824
eduardobb@eduardobb-caine:~/Ejercicios_Entrega/P3/1$
```

Ilustración 24. Resolución Práctica 3 - Ej 1 - Parte 2

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 31 de 109

Ahora, una vez tenemos localizado el comienzo de la imagen, buscaremos a partir de ese el punto final de la misma (patrón **ffd9** -> magic number correspondiente a imágenes). Para ello, ejecutaremos el siguiente comando:

```
1. xxd -s $(echo $((0x01bc8c00))) L0_Graphic.dd | grep ffd9 | more
```

Ilustración 25. Resolución Práctica 3 - Ej 1 - Parte 3

Tenemos esta línea: 01bd7920: f7ce 7185 fd6a ac88 d7a1 ffd9 0000 0000 ..q..j..... Podemos calcular el offset de forma que cada dos números es un byte. Por tanto, su offset será **0x1bd7930**

Ejecutaremos el siguiente comando para recuperar la imagen:

```
1. dd if=L0_Graphic.dd of=imagen_extraida.jpg bs=1 skip=$((0x01bc8c00)) count=$((0x01bd7920 - 0x01bc8c00 + 1))
```

Autor: Eduardo Blanco Bielsa © 2024  
Escuela de Ingeniería Informática Universidad de Oviedo Versión: 2024.ES.003  
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre) Hoja 32 de 109

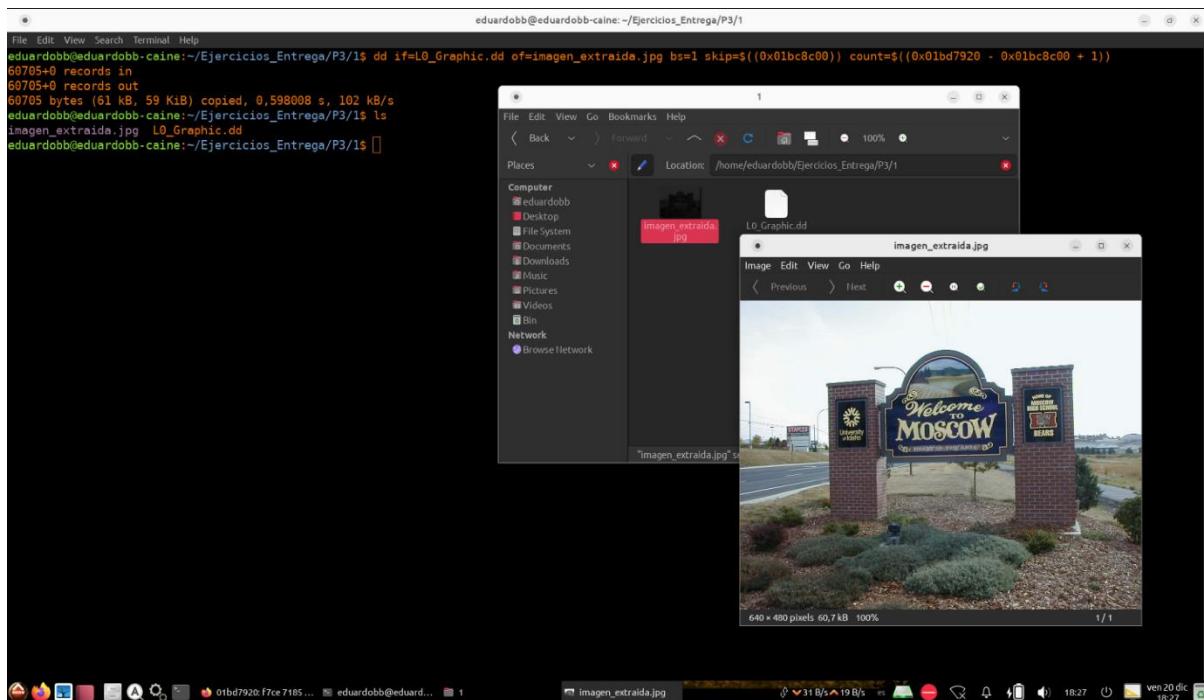


Ilustración 26. Resolución Práctica 3 - Ej 1 - Parte 4

## Conclusiones preliminares

Se encontró una imagen borrada de tipo jpg.

## Conclusiones

En este ejercicio se pretende realizar un Carving de forma manual (en lugar de usar un módulo de Autopsy). Se puede apreciar como claramente se ha conseguido recuperar una imagen mediante carving manual. Además, este ejercicio ha servido para tener en cuenta que elementos borrados de forma común no se borran realmente y aún son recuperables.

## Práctica 3 – Ejercicio 10

### Enunciado

En este ejercicio aplicaremos técnicas de carving sobre ficheros de formatos de audio (MP3, WAV, etc.). Descarga del campus virtual (Recursos Prácticas- Práctica 3), el fichero L2\_Audio.dd.bz2. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada además al caso los módulos de ingestión que ha utilizado en el ejercicio anterior. Realice el proceso de ingestión y una vez haya finalizado, compruebe los Resultados obtenidos para rellenar la siguiente tabla.

### Toma de pruebas

Descargaremos el fichero "Recursos Prácticas -> Práctica3 -> L2\_Audio.dd.bz2".

### Análisis de las pruebas

Se han llevado a cabo técnicas de carving para la recuperación de ficheros borrados mediante tres módulos de Autopsy, que se detallan a continuación.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 33 de 109

Algunos de los metadatos se han obtenido mediante las propiedades ofrecidas por el propio Windows:

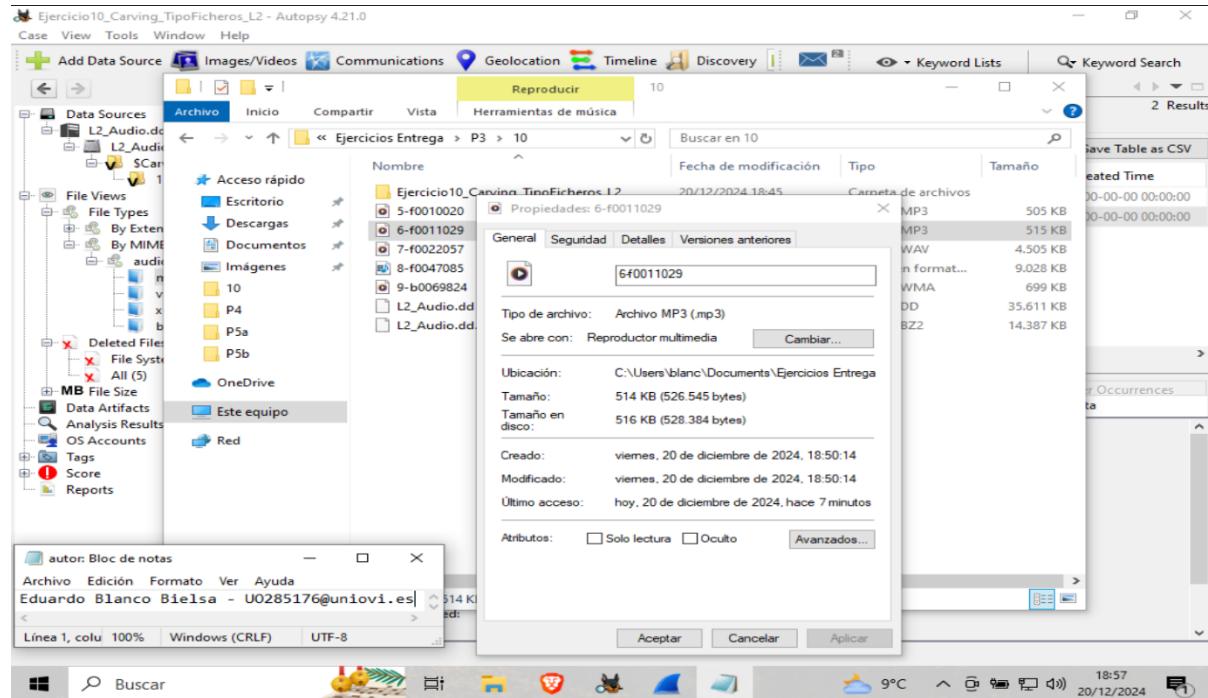


Ilustración 27. Ejemplo propiedades Windows

La tasa de muestreo se ha obtenido con **Exiftool**.

## Resultados obtenidos

Se creará un nuevo caso en **Autopsy** (con Data Source de tipo Disk Image or VM File) con los siguientes módulos de ingestión:

- **File Type Identification, Exif parser** (con la opción *Keep corrupted files* activada -> Ahora se llama **Picture Analyzer**) y **PhotorecCarver**

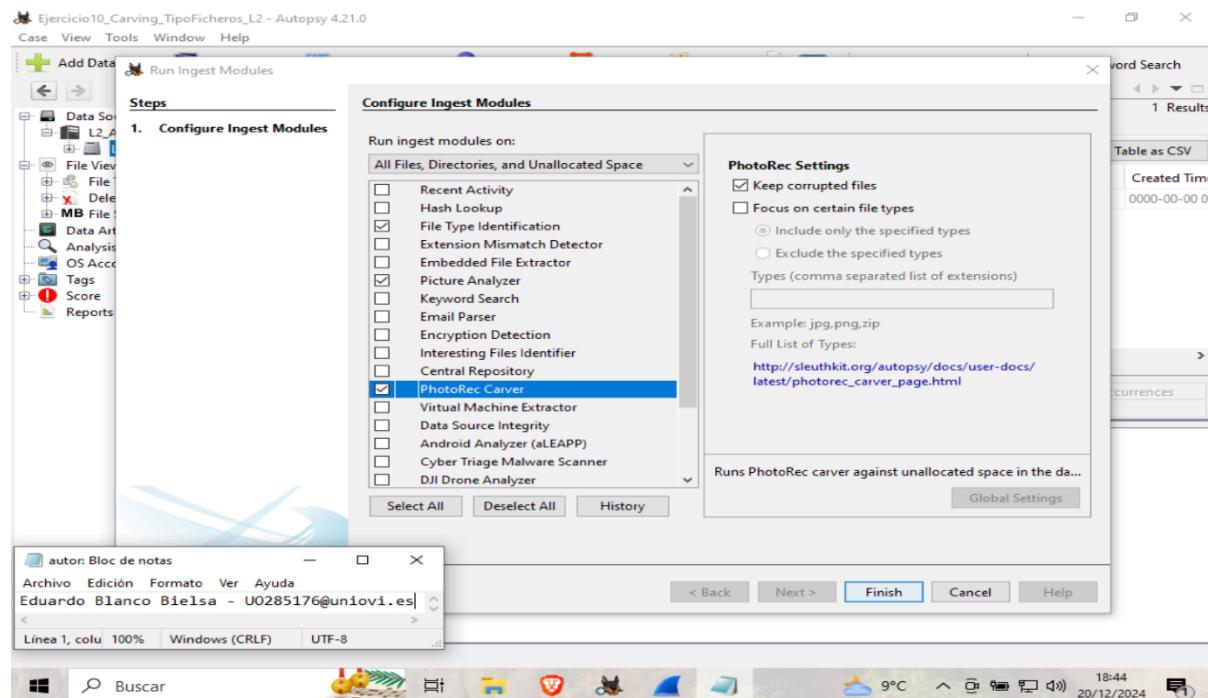


Ilustración 28. Resolución Práctica 3 - Ej 10

Nombre	Tamaño del fichero (Bytes)	Tipo MIME	Autor	Género	Duración (HH:MM:SS)	Tasa Muestreo
f0010020.mp3	51698	audio/mpeg	-	-	00:00:16	44,1 kHz
f0010029.mp3	526545	audio/mpeg	Kevin McLeod	Electronica	00:00:16	44,1 kHz
f0022057.wav	4612660	audio/vnd.wave	-	-	00:00:26	44,1 kHz
b0069824.wma	715776	audio/x-ms-wma	-	-	00:01:05	-
f0047085.au	9243672	audio/basic	-	-	00:00:52	44,1 kHz

Tabla 1. Resolución Práctica 3 - Ej 10

## Conclusiones preliminares

Se han encontrado un total de 5 archivos con MIME Type audio:

The screenshot shows the Autopsy 4.21.0 interface. In the left sidebar, under 'File Views', 'File Types' is expanded, showing 'By Extension' and 'By MIME Type'. Under 'By MIME Type', 'audio' is selected, displaying four subtypes: mpeg (2), vnd.wave (1), x-ms-wma (1), and basic (1). The main pane shows a table with 4 results. A preview window at the bottom displays a text file named 'autor: Bloc de notas' with the content 'Eduardo Blanco Bielsa - U0285176@uniovi.es'. The status bar at the bottom right shows the date and time as '18:46 20/12/2024'.

Ilustración 29. Archivos de audio encontrados

## Conclusiones

Se han encontrado varios archivos de audio y se han analizado sus respectivos metadatos para reflejarlos en el informe.

## Práctica 3 – Ejercicio 14

### Enunciado

Descarga del campus virtual (Recursos Prácticas- Práctica 3), el fichero dfr-03- mugt.dd.bz2. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada como módulos de ingestión de evidencia asociados al proyecto los módulos siguientes: File Type Identification, PhotorecCarver. Responda a las siguientes cuestiones.

### Toma de pruebas

Descargaremos el recurso "Recursos Prácticas -> Práctica 3 -> dfr-03- mugt.dd.bz2".

### Análisis de las pruebas

Se han llevado a cabo técnicas de carving para la recuperación de ficheros borrados mediante tres módulos de Autopsy, que se detallan a continuación.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 36 de 109

## Resultados obtenidos

Se creará un nuevo caso en **Autopsy** (con Data Source de tipo Disk Image or VM File) con los siguientes módulos de ingestión:

- **File Type Identification y PhotorecCarver**

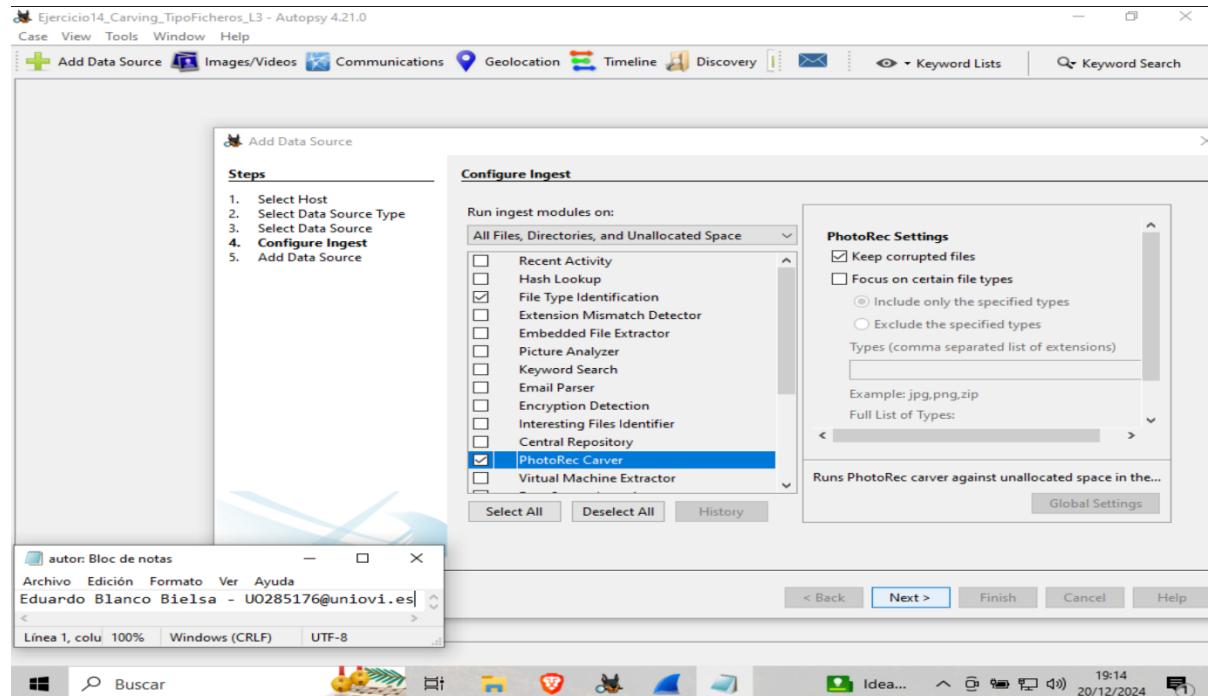


Ilustración 30. Resolución Práctica 3 - Ej 14

Se cumplimenta la tabla solicitada:

Número de partición	Sector de Comienzo	Sector de Finalización	Tipo Sistema de Ficheros
vol1	0	127	Unallocated
vol2	128	2091135	NTFS/exFAT
vol3	2091136	2097152	Unallocated

Tabla 2. Resolución Práctica 3 - Ej 14

## Conclusiones preliminares

Se han encontrados tres volúmenes dentro de la imagen.

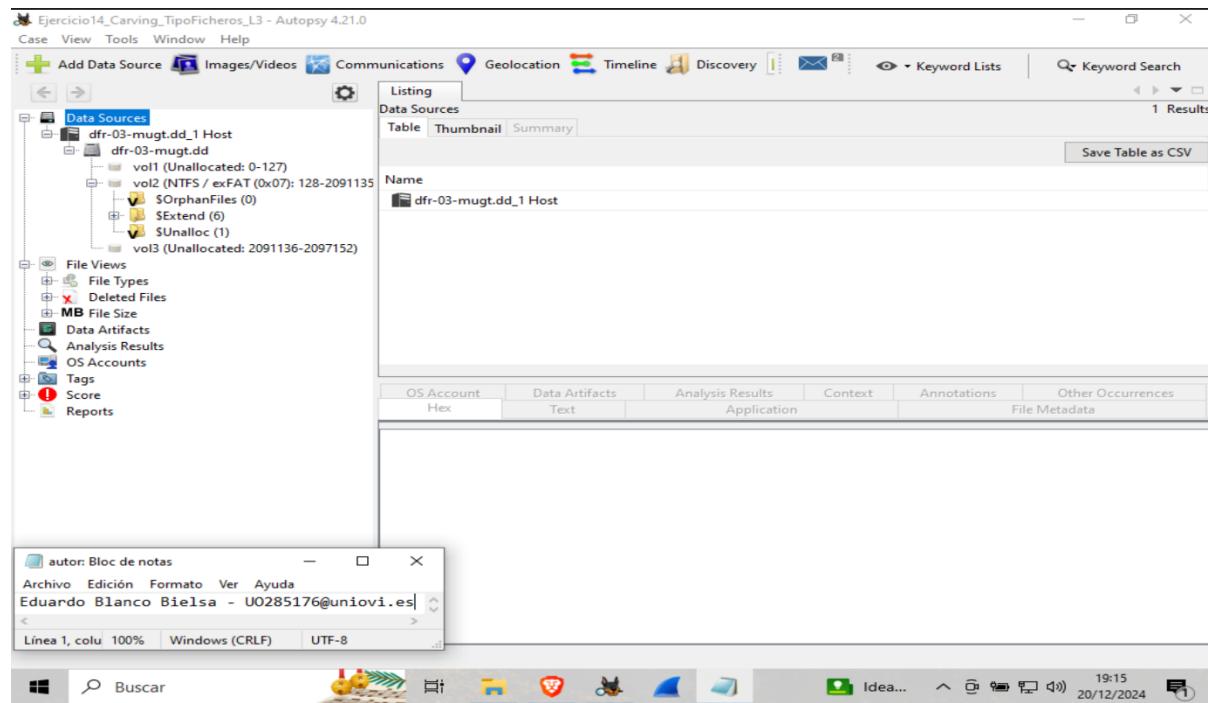


Ilustración 31. Volúmenes encontrados

## Conclusiones

Se han encontrado volúmenes y se han analizado sus respectivos metadatos para reflejarlos en el informe.

## Práctica 3 – Ejercicio 14 – Apartado a

### Enunciado

¿Cuantos ficheros de tipo mime text/plain borrados se encuentran en las particiones detectadas en la imagen?

### Resultados obtenidos

Borrado solamente se encuentra 1 (Bunda.txt), aunque hay 5 que comparten dicho tipo MIME:

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 38 de 109

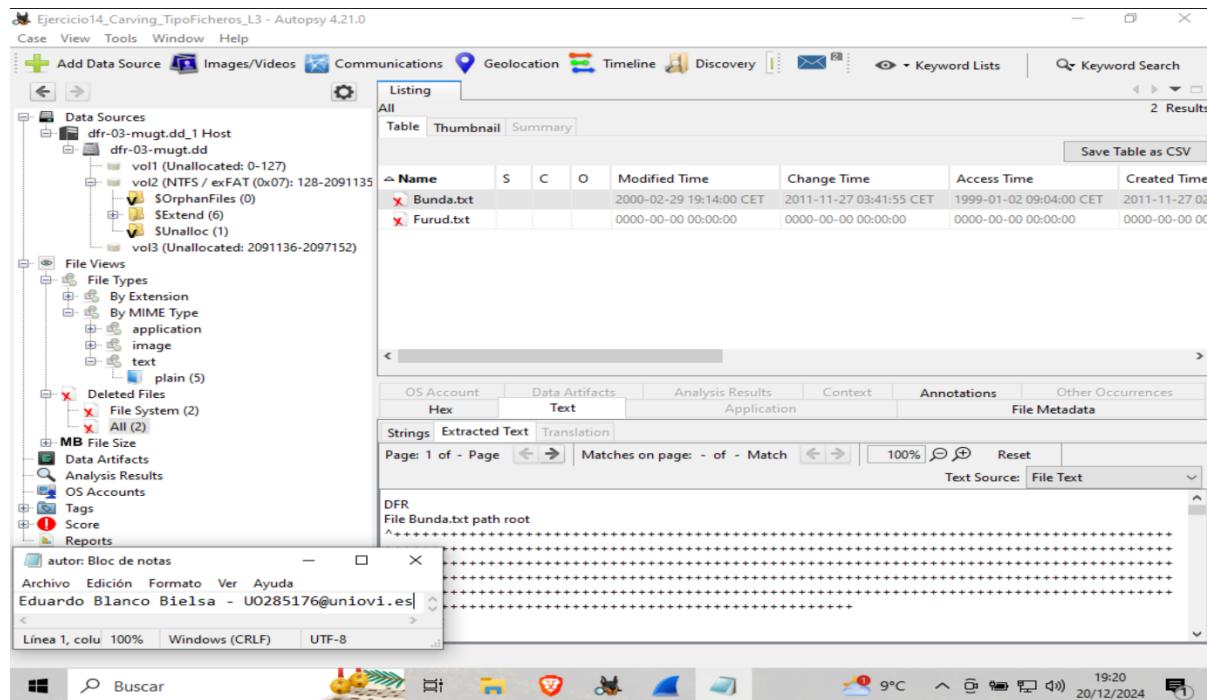


Ilustración 32. Resolución Práctica 3 - Ej 14 - Apartado a

## Conclusiones preliminares

Se ha encontrado un único archivo (Bunda.txt).

## Conclusiones

Se han examinado los distintos volúmenes, se ha encontrado un archivo y se han analizado sus respectivos metadatos para reflejarlos en el informe.

## Práctica 3 – Ejercicio 14 – Apartado b

### Enunciado

Por cada fichero anterior indique la siguiente información.

### Resultados obtenidos

MAC times por cada fichero borrado (GMT)						
Nombre	Tamaño (Bytes)	Partición	Acceso	Modificación	Cambio	Creación
Bunda.txt	2107392	Unallocated	1999-01-02 08:04:00	2000-02-29 18:14:00	2011-11-27 01:34:58	2011-11-27 02:41:55

Tabla 3. Resolución Práctica 3 - Ej 14 - Apartado b

## Conclusiones

Se ha analizado el fichero correspondiente y se han analizado sus metadatos para reflejarlos en el informe. Es importante tener en cuenta que las horas en Autopsy están como CET, así que hay que restar 1 hora a las que aparecen.

## Práctica 3 – Ejercicio 14 – Apartado c

### Enunciado

Por cada fichero de texto plano borrado muestre su línea temporal.

### Resultados obtenidos

Hacemos clic en el Timeline del archivo *Bunda.txt*:

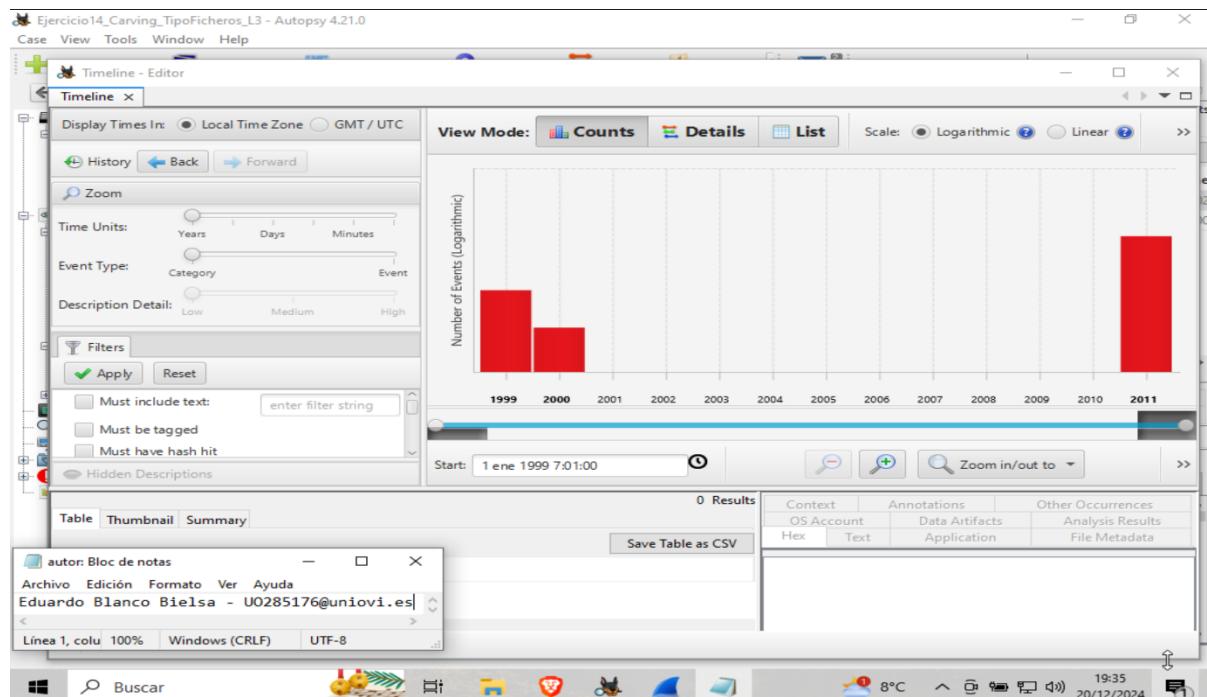


Ilustración 33. Resolución Práctica 3 - Ej 14 - Apartado c

### Conclusiones

Inspeccionando el Timeline podemos apreciar las MAC Times reflejadas en el apartado anterior, es decir, su momento de Modificación, Acceso y Creación de forma gráfica.

## Práctica 4 – Ejercicio 8

### Enunciado

Descarga del campus virtual (Recursos Prácticas->Práctica 4), el fichero JTAGSamsungS4.bin. Este fichero se corresponde con una imagen física de un teléfono móvil Samsung S4. Almacénalo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada, como módulos de ingestión de evidencia asociados al proyecto, los módulos siguientes: Recent Activity, File Type Identification, Picture Analyzer, Keyword Search (seleccione la búsqueda de números de teléfono, direcciones IP, emails, URLs y números de tarjeta de crédito), Email Parser, Extension Mismatch Detector, PhotorecCarver y Android Analyzer. Con todos esos módulos de ingestión activados, el proceso de búsqueda de artefactos por parte de Autopsy puede demorarse un buen rato. Responda a las siguientes cuestiones.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 40 de 109

## Toma de pruebas

Descargaremos el recurso "*Recursos Prácticas -> Práctica 4 -> JTAGSamsungS4.bin*".

## Análisis de las pruebas

Se realizo el siguiente perfil de ingestión con Autopsy, común a todos los apartados de este ejercicio (para no tener que indicar la misma información en cada apartado):

### Perfil de ingestión JTAG Samsung:

- Incremental, por etapas
- Data Source Type: Disk Image or VM File
- Ingest Profile (etapas):
  - File Type Identification, Extension Mismatch Detection (solamente marcar check all the types), PhotoRec Carver marcar keep corrupted files (2-5mins).
  - Picture Analyzer, Keyword Search (numbers, ip addresses, email addresses, url, credit cards), Email Parser (45 mins).
  - Recent Activity, Android Analyzer (seggs).

**Importante:** La ingestión se realizó al completo pero uno de los módulos duplicó algún contenido, por lo que en caso de afectar se indica en el apartado correspondiente.

## Práctica 4 – Ejercicio 8 – Apartado bb

### Enunciado

Abra el archivo de mensajes con un visor de SQLite y compruebe si la tabla sms del fichero mmssms.db tiene los mismos registros que los mostrados por Autopsy.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 41 de 109

## Resultados obtenidos

Para ver el contenido de la base de datos se usará el visor SQL web [sqliteviewer](#):

_id	thread_id	address	person	date
1	1	+12407555289	NULL	154224180461
2	2	+12407555289	NULL	154224187270
3	3	+12407555289	NULL	154224190598
4	4	+12407555289	NULL	154224203661
5	5	+12407555289	NULL	154224204757
6	6	+12407555289	NULL	154224223368
7	7	2407555289	NULL	154224248128
8	8	2407555289	NULL	154224271817
9	9	2407555289	NULL	154224284458
10	10	2407555289	NULL	154224321065
11	11	+12407555289	NULL	154224384902
12	12	+12407555289	NULL	154224390958
13	13	+12407555289	NULL	154224396585
14	16	NULL	NULL	154224431345

Ilustración 34. Resolución Práctica 4 - Ej 8 - Apartado bb – Parte 1

Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone
mmssms.db	0			Android Message	2018-11-15 02:05:09 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 02:06:05 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 01:30:04 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 01:31:12 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 01:31:45 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 01:33:56 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 01:34:07 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 02:04:09 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 02:05:09 CET	1	Incoming	+12407555289
mmssms.db	0			Android Message	2018-11-15 02:06:05 CET	1	Incoming	+12407555289
mmssms.db				Android Message	2018-11-15 01:41:21 CET	1	Outgoing	e17841fd-56
mmssms.db				Android Message	2018-11-15 01:47:24 CET	1	Outgoing	e17841fd-56
mmssms.db				Android Message	2018-11-15 02:13:34 CET	1	Outgoing	e17841fd-56
mmssms.db				Android Message	2018-11-15 01:41:21 CET	1	Outgoing	e17841fd-56
mmssms.db				Android Message	2018-11-15 01:47:24 CET	1	Outgoing	e17841fd-56
mmssms.db				Android Message	2018-11-15 02:13:34 CET	1	Outgoing	e17841fd-56

Ilustración 35. Resolución Práctica 4 - Ej 8 - Apartado bb – Parte 2

Sí muestran los mismos registros (dado que la ingestión duplicó algunos registros).

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 42 de 109

## Conclusiones preliminares

Ambos comparten 14 registros.

## Conclusiones

Se ha comprobado que tanto la tabla del visor como la de Autopsy tienen los mismos mensajes (hay que tener en cuenta que la ingestión duplicó ciertos Data Artifacts y no se están teniendo en cuenta las repeticiones generadas por Autopsy).

## Práctica 4 – Ejercicio 8 – Apartado vv

### Enunciado

¿Cuántos ficheros de vídeo de tipo mp4 fueron localizados por la herramienta?

### Resultados obtenidos

Un total de 10 ficheros con MIME Type mp4:

Name	S	C	O	Modified Time	Change Time
custom_sticker_onboarding_10_6.mp4				2018-11-16 01:20:25 CET	2018-11-16 01:20:25 CET
FB_VIDEO_FOR_UPLOAD_1542245053243.mp4				2018-11-15 02:24:16 CET	2018-11-15 02:24:16 CET
PART_1542244092760_20181114_200004_001_001.mp4				2018-11-15 02:08:13 CET	2018-11-15 02:08:13 CET
20181114_163729.mp4				2018-11-14 22:37:44 CET	2018-11-14 22:37:44 CET
bubbly.mp4				2018-11-14 22:14:41 CET	2018-11-14 22:14:41 CET
20181114_160934.mp4				2018-11-14 22:09:49 CET	2018-11-14 22:09:49 CET
video_help.mp4				2008-08-01 14:00:00 CEST	2016-10-09 02:52:16 CEST
camera.mp4				1970-05-05 10:54:24 CET	2016-10-09 02:52:16 CEST
group_play.mp4				2013-04-26 10:49:41 CEST	2016-10-09 02:52:16 CEST
motion.mp4				2013-04-26 10:49:41 CEST	2016-10-09 02:52:16 CEST

Ilustración 36. Resolución Práctica 4 - Ej 8 - Apartado vv

## Conclusiones preliminares

Se encontraron 10 ficheros de vídeo cuyo MIME Type es mp4.

## Conclusiones

Se han observado los diferentes archivos de vídeo encontrados por Autopsy y se han reflejado en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 43 de 109

## Práctica 4 – Ejercicio 8 – Apartado xx

### Enunciado

¿De qué marca es el ordenador portátil que aparece en el vídeo 20181114\_163729.mp4?

### Resultados obtenidos

El equipo es de la marca DELL:

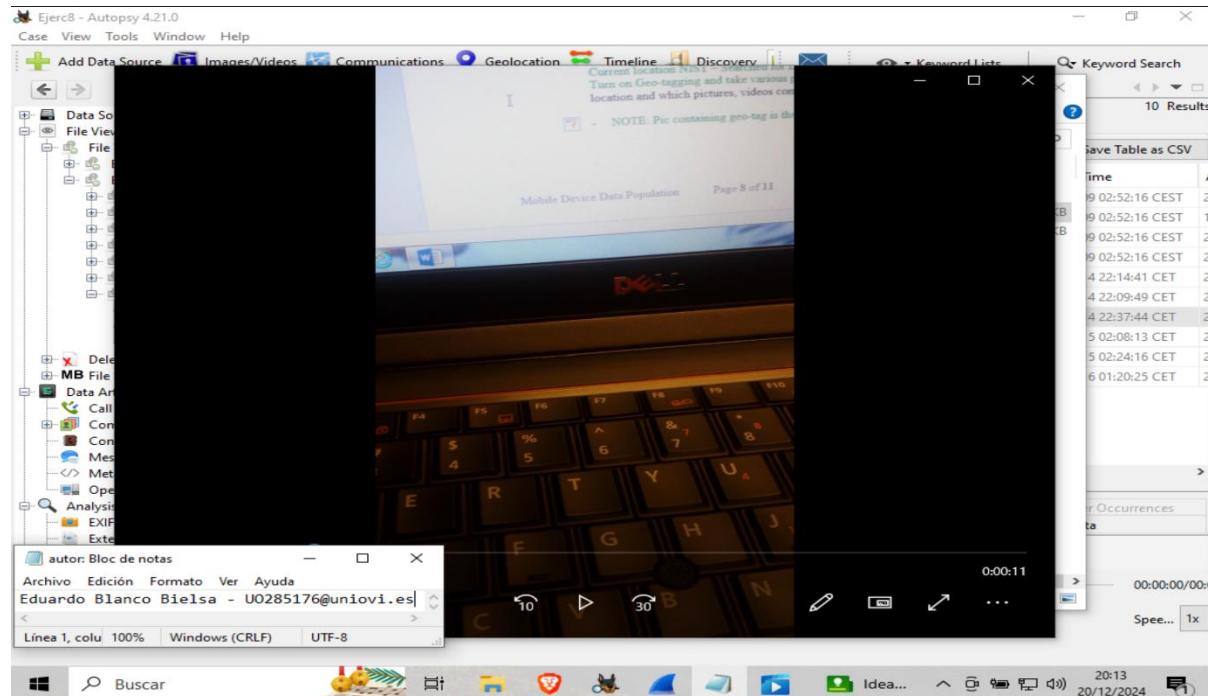


Ilustración 37. Resolución Práctica 4 - Ej 8 - Apartado xx

### Conclusiones

Se ha averiguado la marca del portátil y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 8 – Apartado ccc

### Enunciado

¿Cuántos ficheros de tipo jpeg fueron creados, accedidos o modificados en el teléfono entre el 1 de noviembre de 2018 y el 30 de noviembre de 2018 inclusive?

### Resultados obtenidos

Si nos fijamos en el timeline de los objetos cuyo MIME Type es jpeg y configuramos las fechas adecuadamente:

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 44 de 109

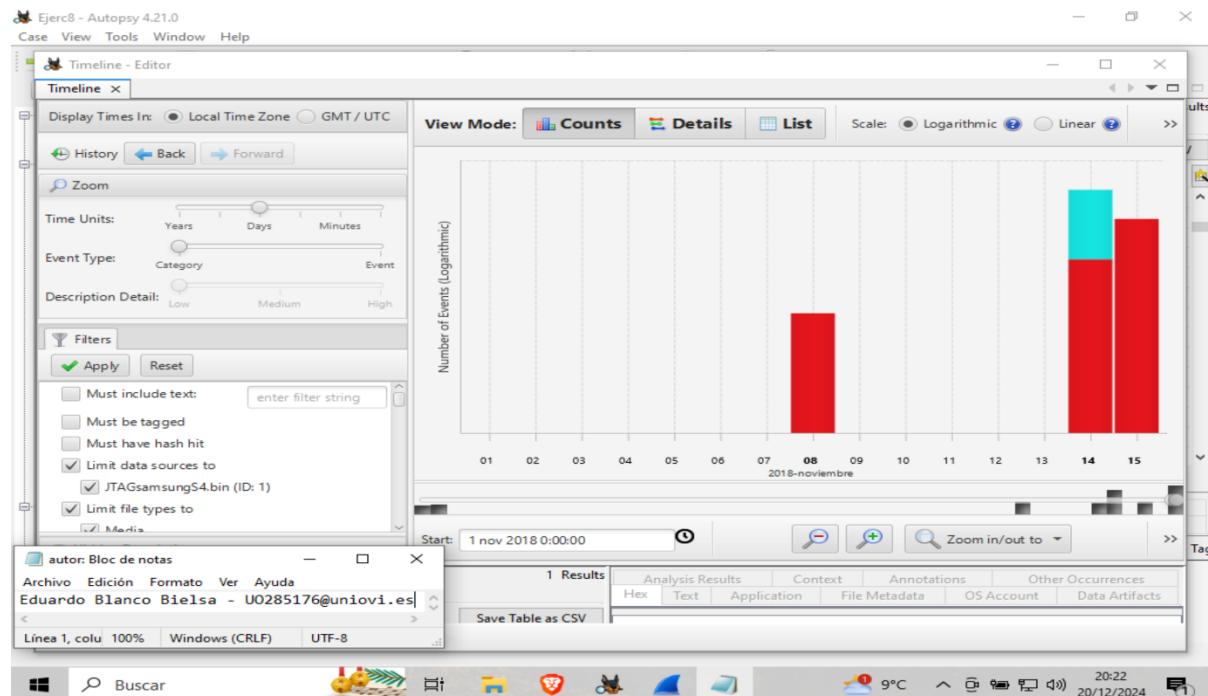


Ilustración 38. Resolución Práctica 4 - Ej 8 - Apartado ccc - Parte 1

Hay un total de 602 elementos que fueron creados, accedidos o modificados en el teléfono entre el 1 de noviembre de 2018 y el 30 de noviembre de 2018 en ese período temporal:

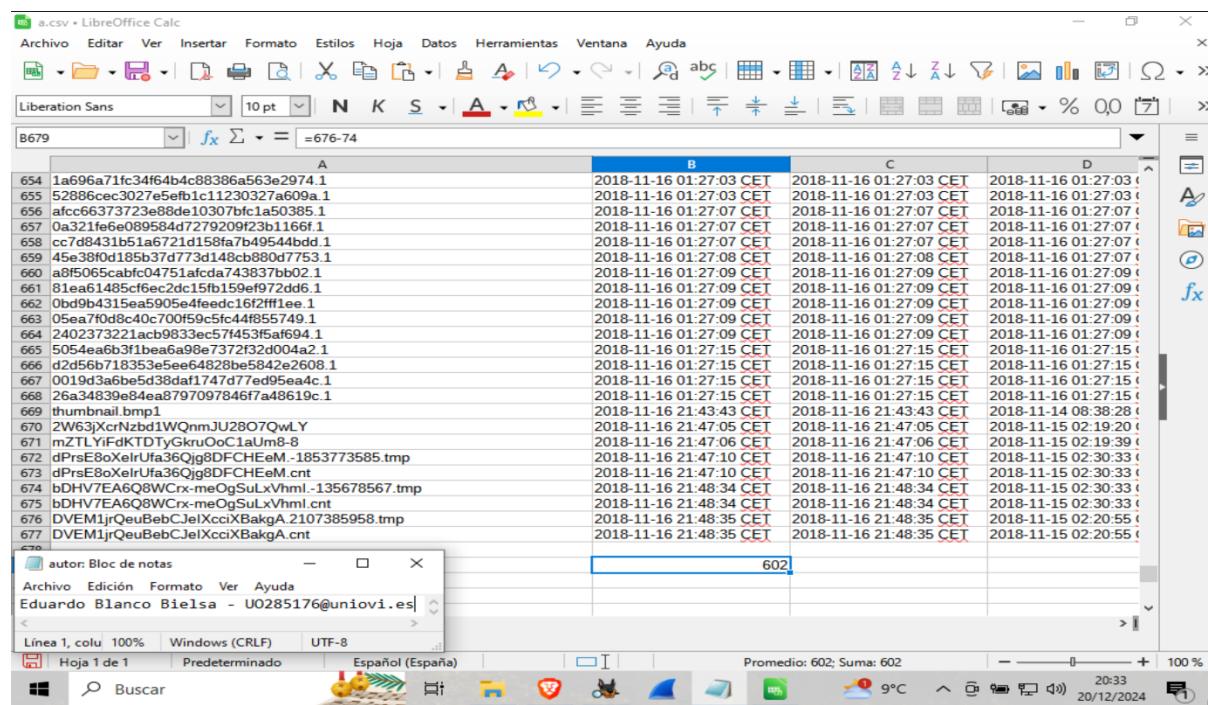


Ilustración 39. Resolución Práctica 4 - Ej 8 - Apartado ccc - Parte 2

## Conclusiones

Se anotaron el número de ficheros y se reflejaron en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 45 de 109

## Práctica 4 – Ejercicio 8 – Apartado fff

### Enunciado

Compruebe si hay algún fichero .jpg en la carpeta de Descargas (userdata/Media/0/Download), y en caso de haber alguno, extráigalo a la carpeta de Export del proyecto.

### Resultados obtenidos

Sí que hay uno llamado emma-girl.jpg:

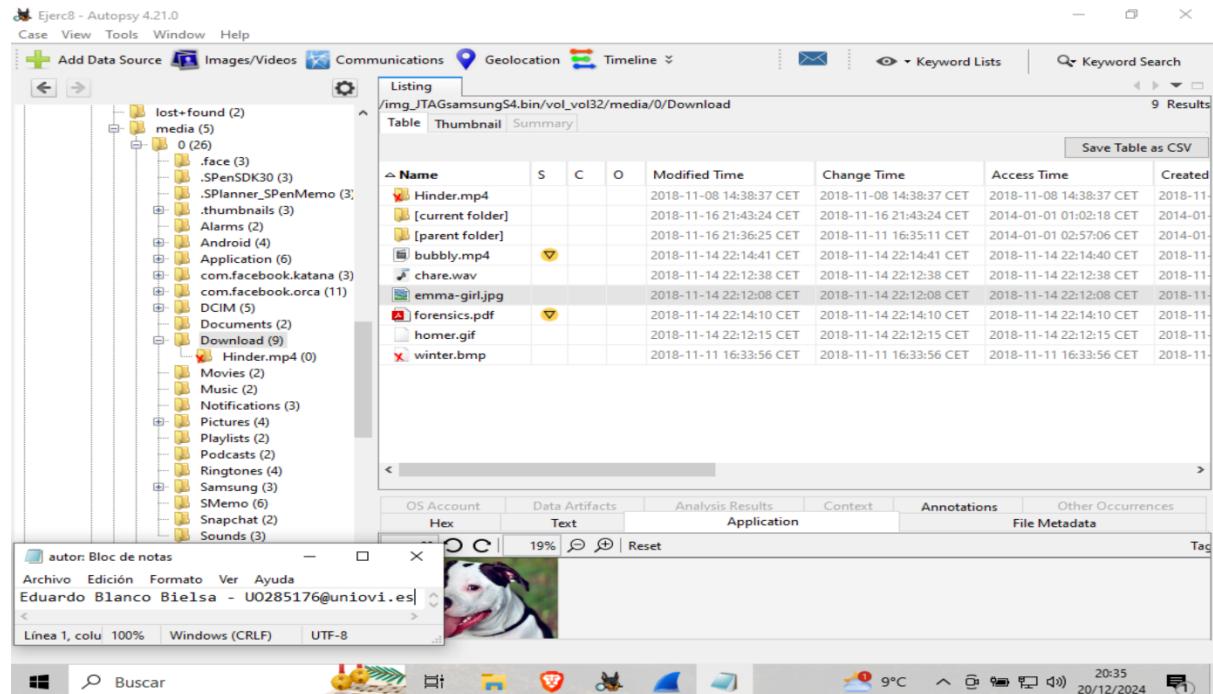


Ilustración 40. Resolución Práctica 4 - Ej 8 - Apartado fff - Parte 1

Si lo extraemos al explorador de archivos:

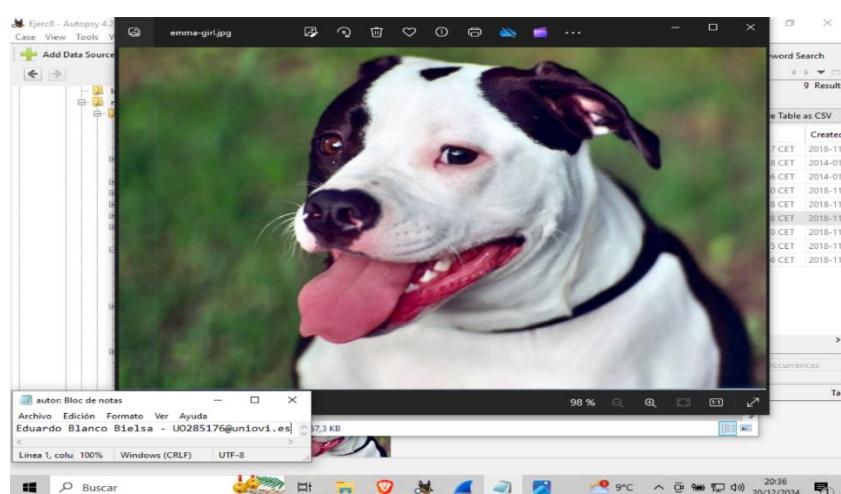


Ilustración 41. Resolución Práctica 4 - Ej 8 - Apartado fff - Parte 2

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 46 de 109

## Conclusiones

Se encontró una imagen y se reflejó en el informe.

## Práctica 4 – Ejercicio 8 – Apartado iii

### Enunciado

Enumere las redes sociales con que trabajaba el usuario.

### Resultados obtenidos

La carpeta típica donde se suelen almacenar las redes sociales es en "userdata/data/", por lo que se buscarán ahí las redes sociales. Se ha encontrado facebook, Instagram, Pinterest y Twitter:

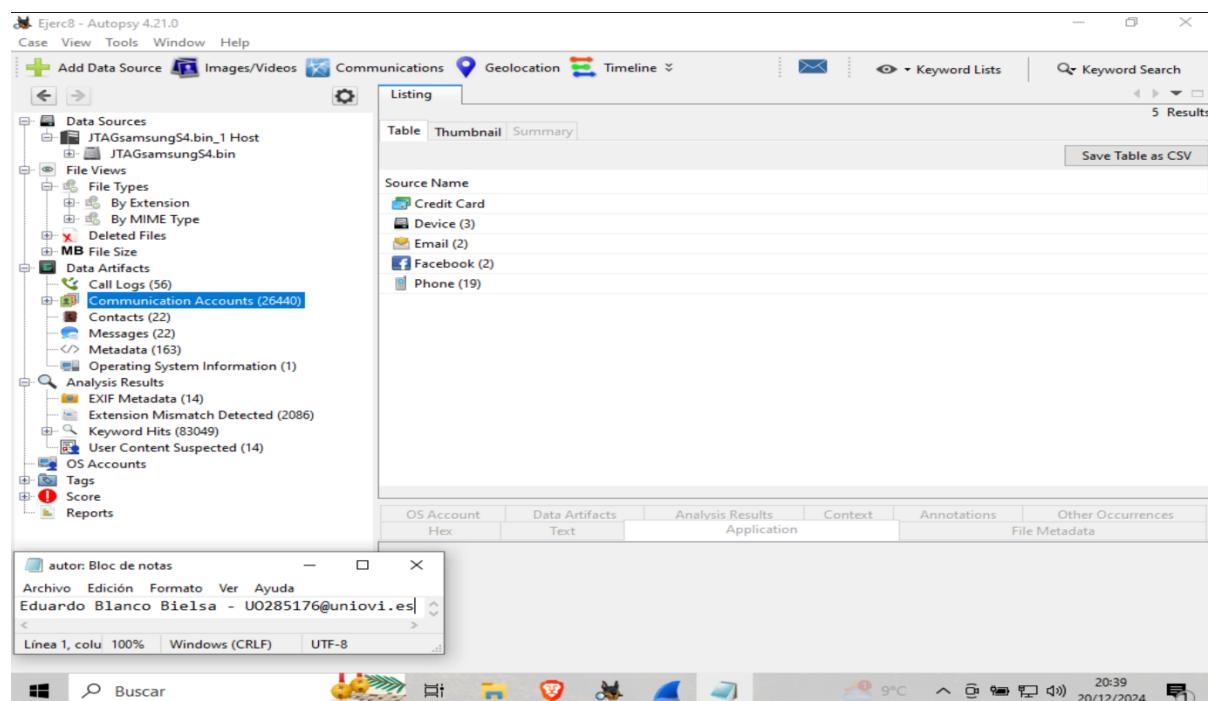


Ilustración 42. Localización de Facebook 1

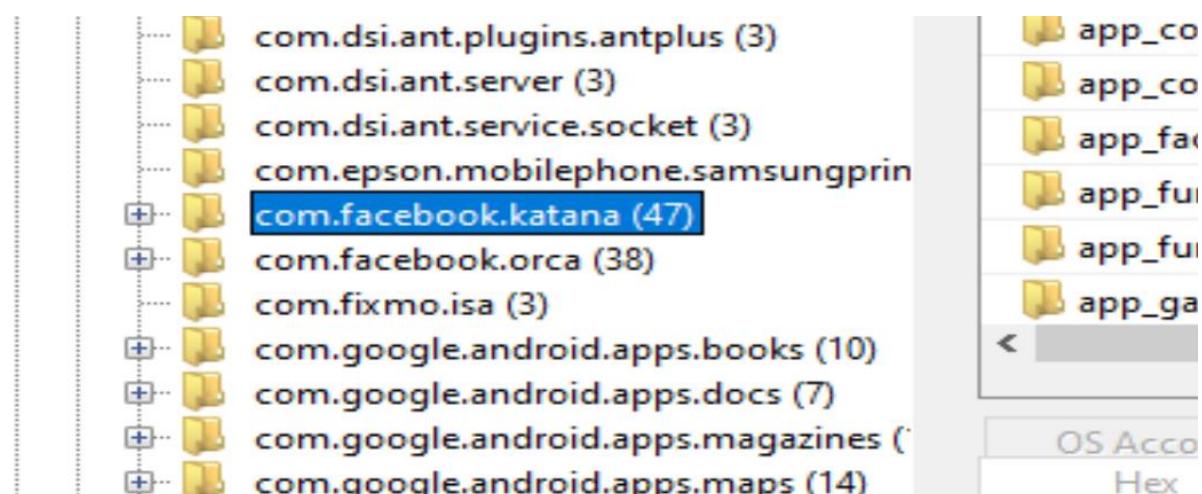


Ilustración 43. Localización de Facebook 2

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 47 de 109

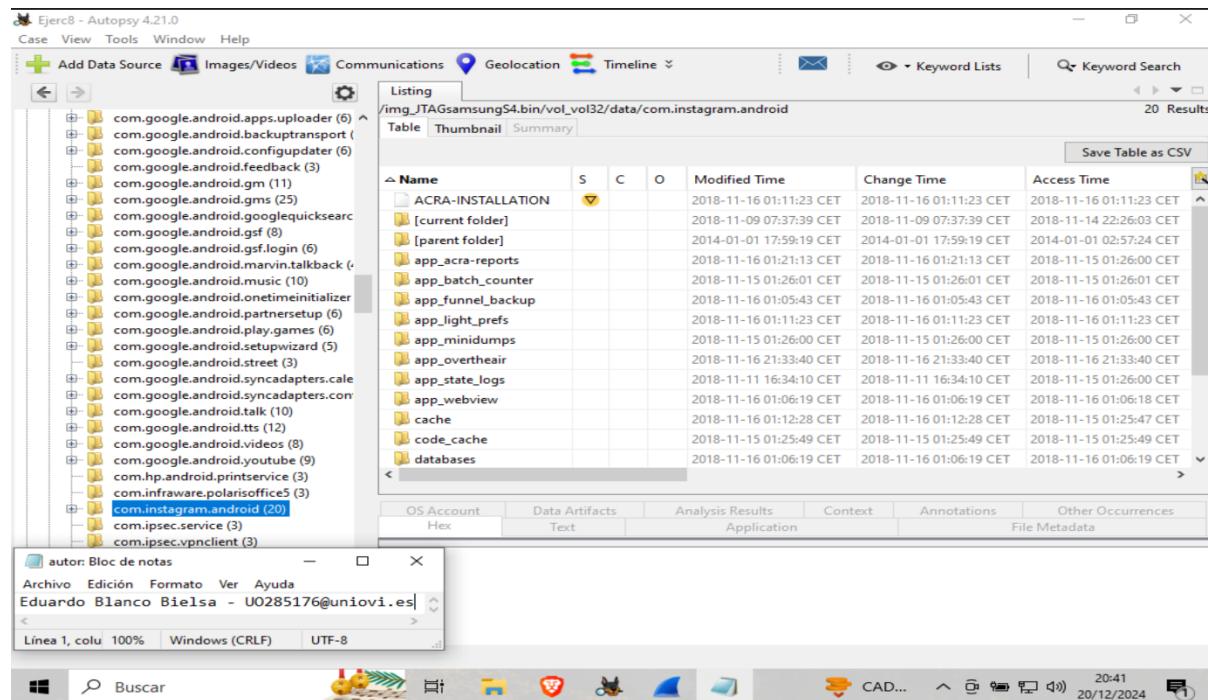


Ilustración 44. Localización de Instagram

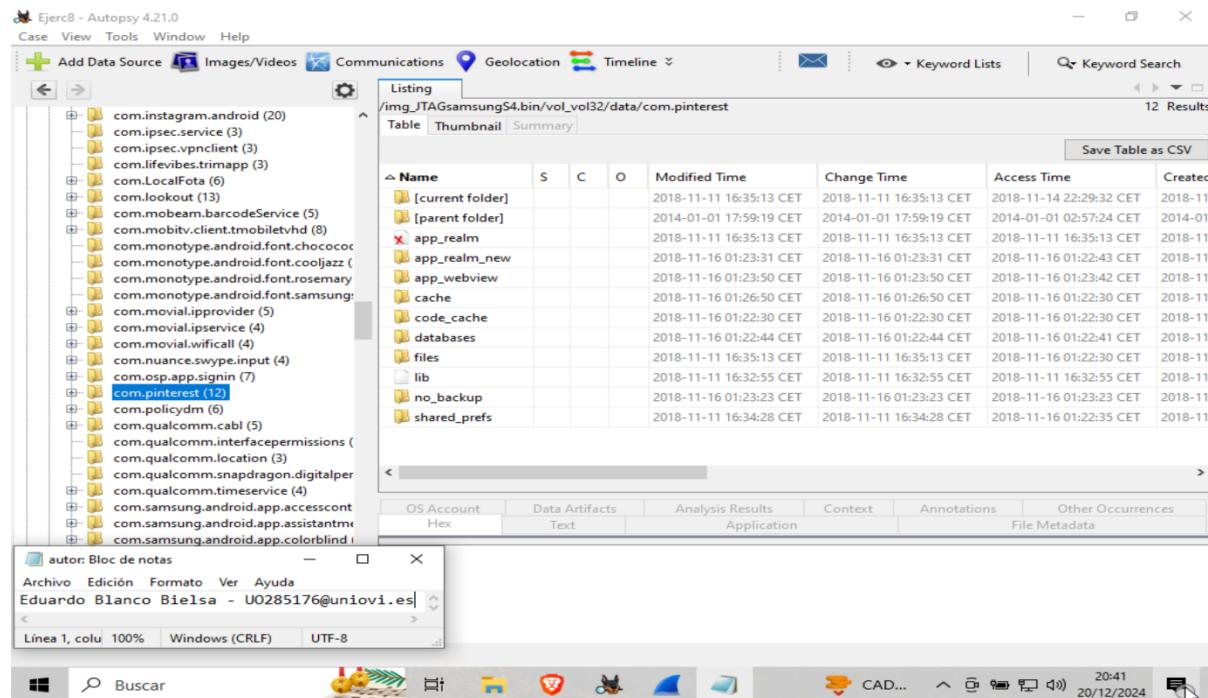


Ilustración 45. Localización de Pinterest

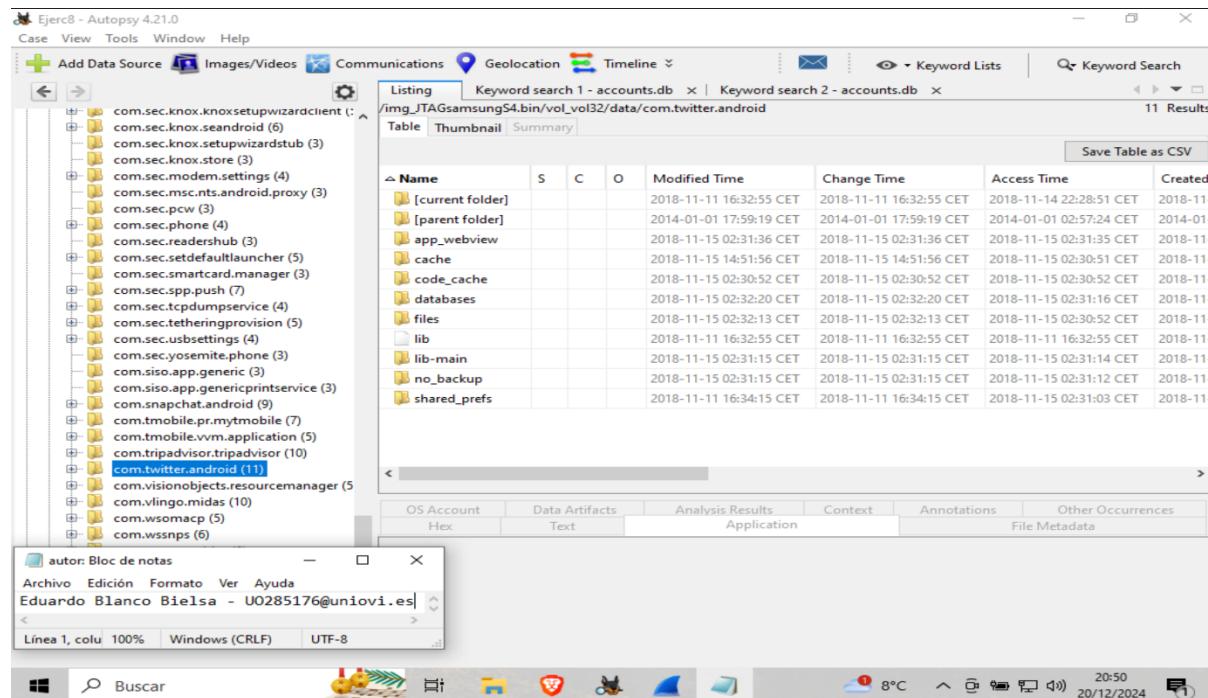


Ilustración 46. Localización de Twitter

## Conclusiones

Para este apartado no se ha tenido en cuenta únicamente que se encontrasen cuentas (como la de Facebook), sino también que tuviese rastros de las aplicaciones correspondientes a una red social (Instagram, Pinterest y Twitter).

## Práctica 4 – Ejercicio 8 – Apartado mmm

### Enunciado

Localice el fichero accounts.db. Indique en qué carpeta se encuentra. Almacene dicho fichero en la carpeta Export. Abra dicho fichero con DB Browser for SQLite. ¿Cuántas cuentas hay asociadas con el dispositivo?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 49 de 109

## Resultados obtenidos

La base de datos se encuentra dentro de `/img_JTAGsamsungS4.bin/vol_vol32/system/users/0/accounts.db`:

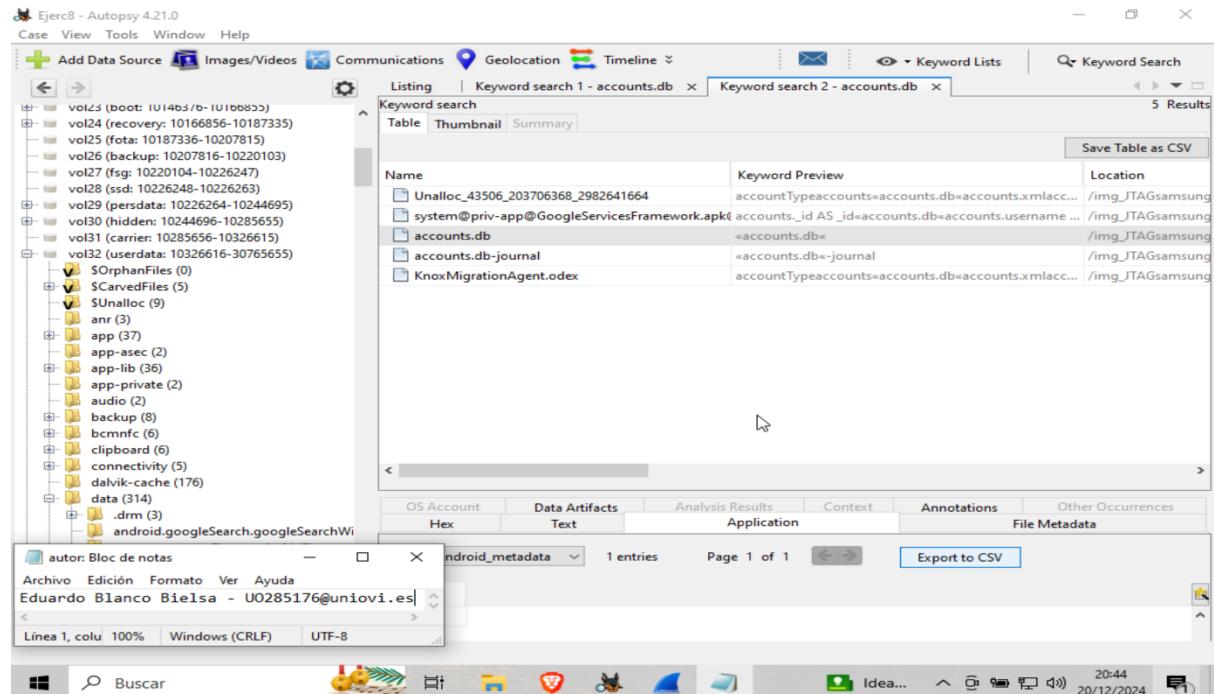


Ilustración 47. Resolución Práctica 4 - Ej 8 - Apartado mmm - Parte 1

Se va a utilizar otro visor de SQLite (**sqliteviewer**) porque el indicado me hacía crashear la máquina virtual. Hay 4 cuentas asociadas:

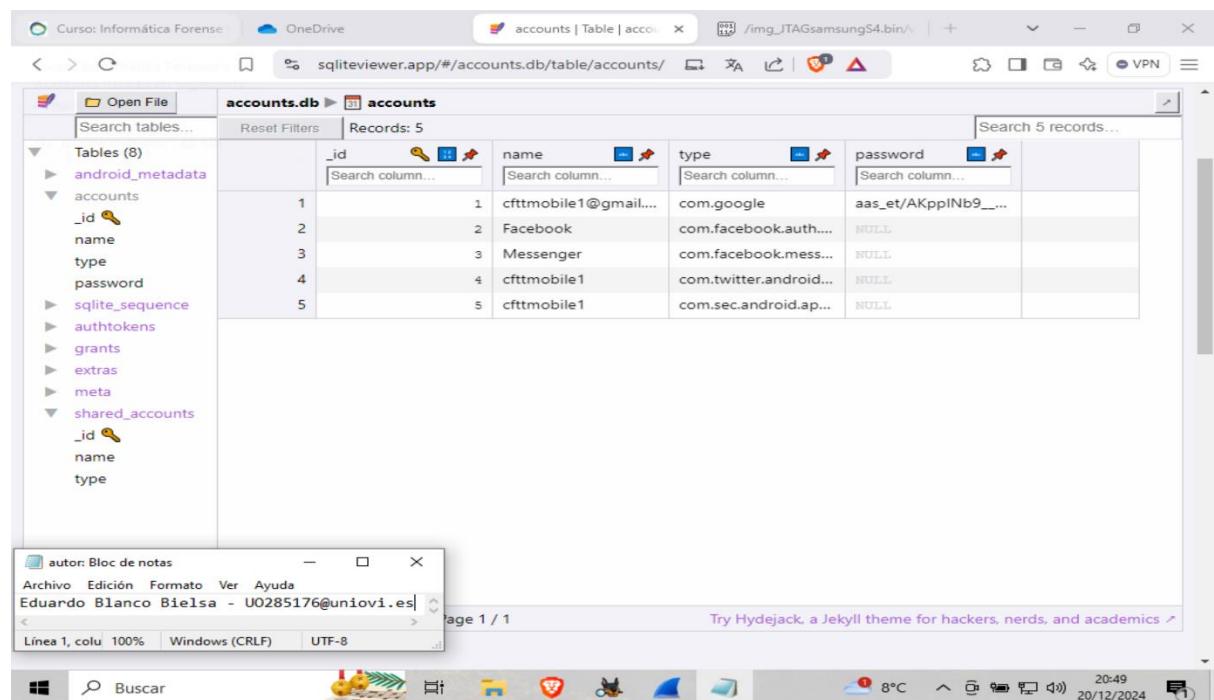


Ilustración 48. Resolución Práctica 4 - Ej 8 - Apartado mmm - Parte 2

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 50 de 109

## Conclusiones

Se han encontrado varias cuentas y se han reflejado en el informe.

## Práctica 4 – Ejercicio 8 – Apartado nnn

### Enunciado

Según la información obtenida en el apartado mmm), ¿cuál es la cuenta de Google?

### Resultados obtenidos

La cuenta usada es [cftmobile1@gmail.com](mailto:cftmobile1@gmail.com) (ver la imagen del apartado anterior).

## Conclusiones

Se ha encontrado la cuenta requerida y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 8 – Apartado ppp

### Enunciado

Obtenga información sobre los contactos de Facebook almacenados por dicha aplicación. ¿Cuántos contactos hay? ¿Cuáles son sus nombres?

### Resultados obtenidos

Nos dirigiremos a la

carpeta `/img_JTAGSamsungS4.bin/vol_vo32/data/com.facebook.katana/databases` y encontraremos **contacts\_db2**:

The screenshot shows the Autopsy 4.21.0 interface. The left pane displays a file system tree under the path `/img_JTAGSamsungS4.bin/vol_vo32/data/com.facebook.katana/databases`. The right pane shows a table titled "Listing" with the following data:

Name	S	C	O	Modified Time	Change Time
compost_draft_db-uid				2018-11-15 02:25:46 CET	2018-11-15 02:25:46 CET
contact_ranking_db				2018-11-15 02:19:57 CET	2018-11-15 02:19:57 CET
contact_ranking_db-journal				2018-11-15 02:19:57 CET	2018-11-15 02:19:57 CET
contact_ranking_db-uid				2018-11-15 02:19:57 CET	2018-11-15 02:19:57 CET
contacts_db2				2018-11-15 02:26:53 CET	2018-11-16 21:47:17 CET
contacts_db2-journal				2018-11-15 02:26:53 CET	2018-11-16 21:48:07 CET
contacts_db2-uid				2018-11-15 02:19:52 CET	2018-11-15 02:19:52 CET
graph_cursors				2018-11-16 21:47:14 CET	2018-11-16 21:47:14 CET
graph_cursors-journal				2018-11-16 21:47:14 CET	2018-11-16 21:47:14 CET
graph_cursors-uid				2018-11-15 02:19:16 CET	2018-11-15 02:19:16 CET
graphql_cache				2018-11-16 21:47:14 CET	2018-11-16 21:47:14 CET
graphql_cache-journal				2018-11-16 21:47:14 CET	2018-11-16 21:48:34 CET
local_media_db				2018-11-16 21:47:18 CET	2018-11-16 21:47:18 CET
local_media_db-journal				2018-11-16 21:47:18 CET	2018-11-16 21:47:18 CET

Below the table, there is a small window showing a text editor with the content:

```
autor: Bloc de notas
Archivo Edición Formato Ver Ayuda
Eduardo Blanco Bielsa - U0285176@uniovi.es
Línea 1, col 100% Windows (CRLF) UTF-8
```

Ilustración 49. Resolución Práctica 4 - Ej 8 - Apartado ppp – Parte 1

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 51 de 109

Nos descargaremos la base de datos y la abriremos de nuevo en **sqliteviewer**:

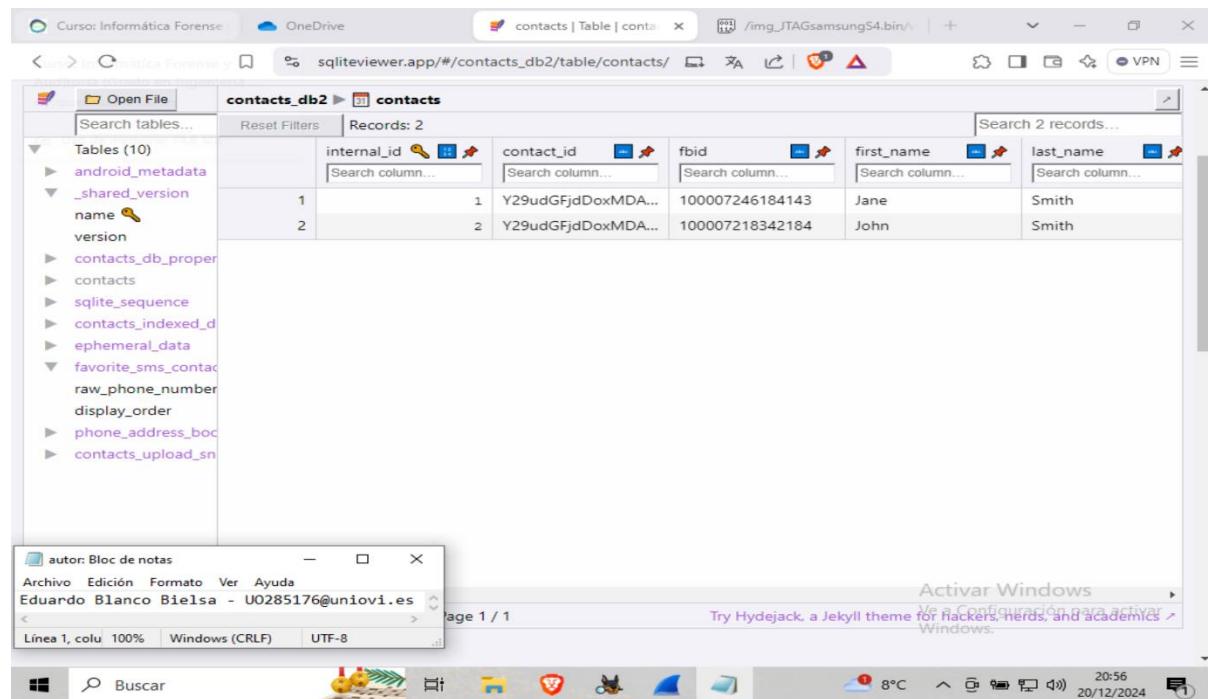


Ilustración 50. Resolución Práctica 4 - Ej 8 - Apartado ppp – Parte 2

Vemos que hay dos contactos: Jane Smith y John Smith.

## Conclusiones

Se han anotado los contactos correspondientes y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 8 – Apartado rrr

### Enunciado

Averigüe el mes y el día de nacimiento del primero de los contactos de Facebook almacenados en el móvil intervenido.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 52 de 109

## Resultados obtenidos

Nació el 23 de abril:

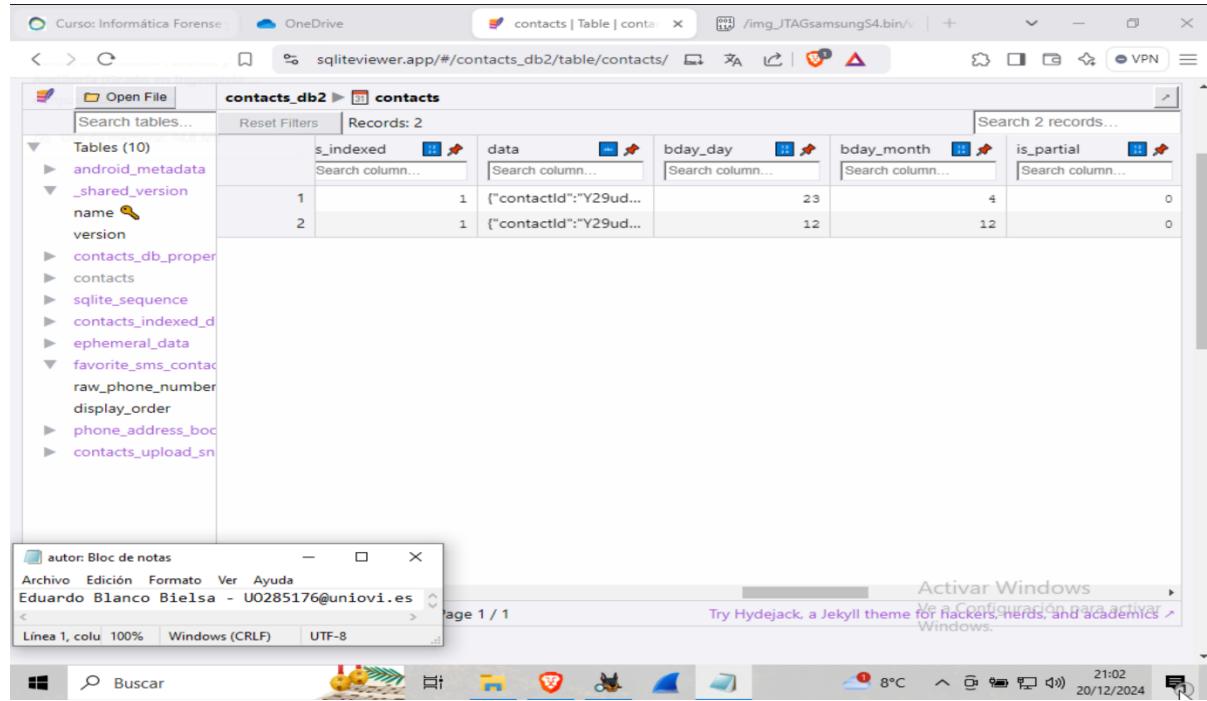


Ilustración 51. Resolución Práctica 4 - Ej 8 - Apartado rrr

## Conclusiones

Se ha anotado la fecha de nacimiento requerida y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 8 – Apartado sss

### Enunciado

Averigüe el mes y el día de nacimiento del último de los contactos de Facebook almacenados en el móvil intervenido.

## Resultados obtenidos

Nació el 12 de diciembre (ver la imagen del apartado anterior).

## Conclusiones

Se ha anotado la fecha de nacimiento requerida y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 9

### Enunciado

Descarga del campus virtual (Recursos Prácticas->Práctica 4), el fichero Pixel3- Data.tar. Este fichero se corresponde con un tar de la carpeta data de un móvil modelo Google Pixel 3. Utiliza ALEAPP GUI para hacer un triaje rápido de dicho fichero y responde a las siguientes cuestiones.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 53 de 109

## Toma de pruebas

Descargaremos el recurso "*Recursos Prácticas -> Práctica 4 -> Pixel3-Data.tar*".

## Análisis de las pruebas

Se descomprimió la imagen y se hizo un análisis con **ALEAPP GUI**. Todos los apartados siguientes serán respondidos usando los resultados generados por esta herramienta.

### Práctica 4 – Ejercicio 9 – Apartado aa

#### Enunciado

¿Cuántos marcadores (bookmarks) tiene registrados Chrome?

#### Resultados obtenidos

Solamente tiene uno: <https://www.cfreds.nist.gov>

The screenshot displays the ALEAPP 3.1.8 interface with the title "Chrome - Bookmarks report". The report summary states "Total number of entries: 1" and "Chrome - Bookmarks located at: C:\Users\blanc\Documents\IFA\P4\Ej9\ALEAPP\_Reports\_2024-11-15\_Friday\_114423\temp\data\user\0\com.android.chrome\app\_chrome\Default\Bookmarks". The main table lists the single bookmark entry:

Added Date	URL	Name	Parent	Type
2018-12-04 13:49:23.188162	<a href="https://www.cfreds.nist.gov/">https://www.cfreds.nist.gov/</a>	The CFReDS Project	Mobile bookmarks	url

Below the report, a Windows taskbar is visible with a Notepad window open. The Notepad window shows the same bookmark details: "The CFReDS Project" and the URL "https://www.cfreds.nist.gov/". The taskbar also shows icons for the Start button, Search, Task View, File Explorer, Edge browser, Taskbar settings, and system status (language, battery, date/time).

Ilustración 52. Resolución Práctica 4 - Ej 9 - Apartado aa

#### Conclusiones

Se ha encontrado el marcador requerido y se ha reflejado en el informe.

### Práctica 4 – Ejercicio 9 – Apartado bb

#### Enunciado

¿A qué página/s corresponden?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 54 de 109

## Resultados obtenidos

Se corresponde con la página del NIST concretamente: *Computer Forensic Reference DataSet Portal*:

The screenshot shows the homepage of the CFReDS portal. At the top, there's a search bar with placeholder text "Quick search using title, author, date or tag..." and a magnifying glass icon. To the left of the search bar is the portal's logo, "CFREDS". Below the search bar is a green header bar with the text "What is CFReDS?". The main content area has a dark background with several sections: "Welcome to the new and improved Computer Forensic Reference DataSet Portal.", "This portal is your gateway to documented digital forensic image datasets. These datasets can assist in a variety of tasks including tool testing, developing familiarity with tool behavior for given tasks, general practitioner training and other unforeseen uses that the user of the datasets can devise. Most datasets have a description of the type and locations of significant artifacts present in the dataset. There are descriptions and finding aides to help you locate datasets by the year produced, by author, or by attributes of the dataset.", "All of the datasets produced by NIST to support the Computer Forensic Tool Testing and Federated Testing projects are included here as well as many other collections. See the icon on the left sidebar for a list of the major collections.", "Browse Data-Sets" button with a folder icon, and "Contribute" button with an upward arrow icon. On the left sidebar, there are icons for Home, Search, Collection, and Help. Below the sidebar are two cards: "Newest Data-Sets" featuring "DFRWS 2023 Challenge" (marked as NEW) and "Popular Data-Sets" featuring "Hacking Case".

Ilustración 53. Resolución Práctica 4 - Ej 9 - Apartado bb

## Conclusiones

Se ha encontrado la página correspondiente y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado cc

### Enunciado

¿Qué expresiones o cadenas de búsqueda se han empleado en la app de Chrome?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 55 de 109

## Resultados obtenidos

Se ha empleado únicamente "Cult of Mac":

The screenshot shows the ALEAPP 3.1.8 application interface. In the main pane, it displays a table of search terms located at `C:\Users\blanc\Documents\IFA\P4\Ej9\ALEAPP_Reports_2024-11-15_Friday_114423\temp\data\user\0\com.android.chrome\app_chrome\Default\History`. The table has columns for Last Visit Time, Search Term, URL, and Title. One entry is visible:

Last Visit Time	Search Term	URL	Title
2020-10-04 14:06:33	Cult of Mac	<a href="https://www.google.com/search?q=Cult+of+Mac&amp;oq=Cult+of+Mac&amp;aqs=chrome..69i57j0l4.3764j1j4&amp;client=ms-android-google&amp;sourceid=chrome-mobile&amp;ie=UTF-8">https://www.google.com/search?q=Cult+of+Mac&amp;oq=Cult+of+Mac&amp;aqs=chrome..69i57j0l4.3764j1j4&amp;client=ms-android-google&amp;sourceid=chrome-mobile&amp;ie=UTF-8</a>	Cult of Mac - Google Search

A context menu is open over this entry, showing options like 'Borrar' (Delete), 'Copiar' (Copy), 'Cortar' (Cut), and 'Nuevo'. The status bar at the bottom right shows 'Activar Windows' (Activate Windows) and the date '20/12/2024'.

Ilustración 54. Resolución Práctica 4 - Ej 9 - Apartado cc

## Conclusiones

Se ha observado la expresión y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado dd

### Enunciado

¿Cuántas veces se ha buscado la expresión "Cult of Mac"?

## Resultados obtenidos

Solamente una vez, como se aprecia en la captura de ejercicio anterior.

## Conclusiones

Se ha buscado el número de veces y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado ee

### Enunciado

¿Cuántas entradas tiene la lista de sitios más visitados desde la aplicación de Chrome?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 56 de 109

## Resultados obtenidos

Tiene dos entradas:

ALEAPP 3.1.8

### Chrome - Top Sites report

Total number of entries: 2

Chrome - Top Sites located at:  
C:\Users\blanc\Documents\IFA\P4\Ej9\ALEAPP\_Reports\_2024-11-15\_Friday\_114423\temp\data\user\0\com.android.chrome\app\_chrome\Default\Top Sites

URL	Rank	Title	Redirects
http://www.espn.com/	1	Like it or not, the SEC will again be the center of the college football world in 2020	
https://www.starwars.com/	0	StarWars.com   The Official Star Wars Website	

autor: Bloc de notas  
Archivo Edición Formato Ver Ayuda  
Eduardo Blanco Bielsa - U0285176@uniovi.es  
Línea 1, col. 100% Windows (CRLF) UTF-8

Activar Windows  
Ve a Configuración 1  
Windows.

Buscar 9°C 21:36 20/12/2024

Ilustración 55. Resolución Práctica 4 - Ej 9 - Apartado ee

## Conclusiones

Se han encontrado las entradas y se han reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado ff

### Enunciado

¿Cuáles fueron los sitios más visitados?

## Resultados obtenidos

Los sitios más visitados fueron: <https://www.espn.com/> y <https://www.starwars.com/> (como se puede ver en la captura del apartado anterior).

## Conclusiones

Se han observado los sitios y se han reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado gg

### Enunciado

¿Cuántas entradas tiene el historial de sitios visitados en la aplicación de Chrome?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 57 de 109

## Resultados obtenidos

Tiene un total de 30 entradas:

ALEAPP 3.1.8

### Chrome - Web History report

Total number of entries: 30

Chrome - Web History located at:  
C:\Users\blanc\Documents\IFA\P4\Ej9\ALEAPP\_Reports\_2024-11-15\_Friday\_114423\temp\data\user\0\com.android.chrome\app\_chrome\Default\History

Show 15 entries Search:

Last Visit Time	URL
2020-07-18 12:15:02	http://sans.org/

autor: Bloc de notas  
Archivo Edición Formato Ver Ayuda  
Eduardo Blanco Bielsa - U0285176@uniovi.es  
Línea 1, col. 100% Windows (CRLF) UTF-8  
Buscar Activar Windows  
Ve a Configuración para activar Windows.

Ilustración 56. Resolución Práctica 4 - Ej 9 - Apartado gg

## Conclusiones

Se han encontrado las entradas del historial y se han reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado hh

### Enunciado

¿Cuál es la URL más reciente visitada desde la aplicación de Chrome?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 58 de 109

## Resultados obtenidos

La más reciente, si las filtramos por orden descendente es [https://en.m.wikipedia.org/wiki/The\\_Mandalorian](https://en.m.wikipedia.org/wiki/The_Mandalorian) :

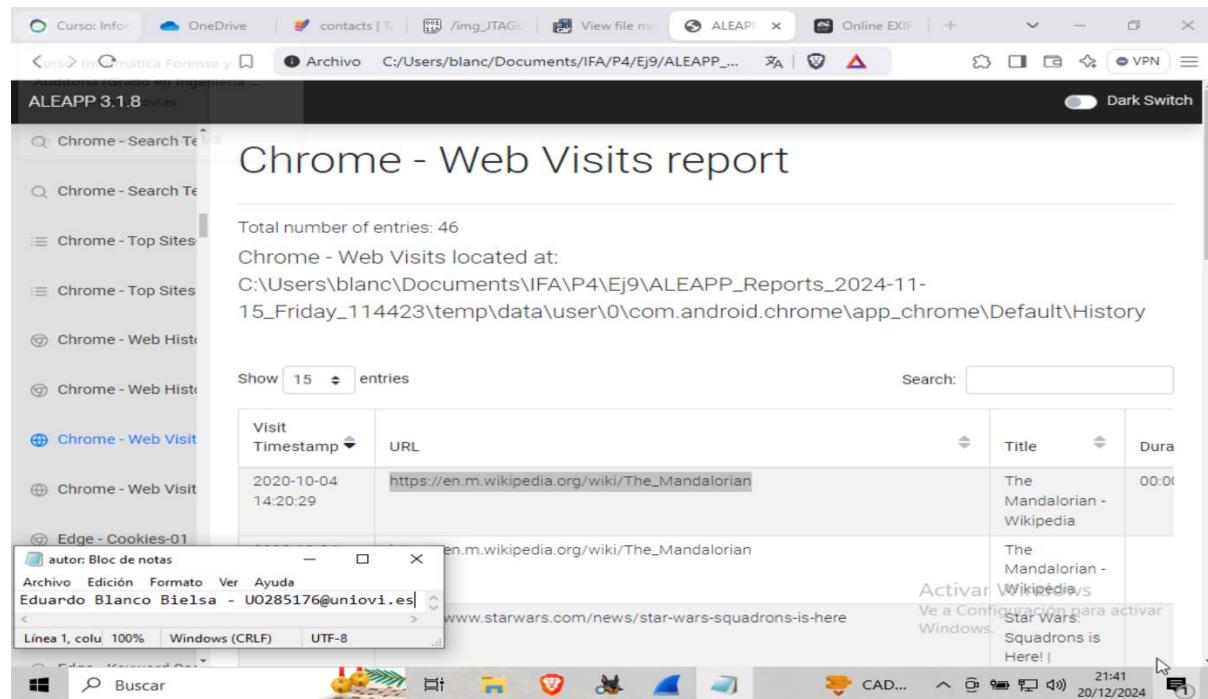


Ilustración 57. Resolución Práctica 4 - Ej 9 - Apartado hh

## Conclusiones

Se ha encontrado la URL requerida y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado ii

### Enunciado

¿Qué URL fue la más visitada desde la aplicación de Chrome?

## Resultados obtenidos

La web más visitada fue: <https://www.cultofmac.com/>:

The screenshot shows the ALEAPP 3.1.8 interface with the 'entries' tab selected. It displays a table of browser history entries:

URL	Title	Duration
https://www.cultofmac.com/	Cult of Mac   Tech and culture through an Apple lens	00:01:29.162
https://connect.garmin.com/oauthConfirm?oauth_token=e008dd3e-d1ea-4e7e-b8b7-66c7c3da723c	Garmin Connect	00:01:02.512
https://www.starwars.com/	StarWars.com   The Official Star Wars Website	00:00:34.211
https://www.autoevolution.com/news/after-android-auto-carplay-also-struggling-with-phone-calls-due-to-new-update-148905.html	After Android Auto, CarPlay Also Struggling With Phone Calls Due to New Update -	00:00:04.432

Below the table, there is a window titled 'autor: Bloc de notas' containing a single line of text: 'Eduardo Blanco Bielsa - U0285176@uniovi.es'. The status bar at the bottom right shows the date and time: '21:44 20/12/2024'.

Ilustración 58. Resolución Práctica 4 - Ej 9 - Apartado ii

## Conclusiones

Se ha anotado la URL requerida y se ha reflejado en el informe.

## Práctica 4 – Ejercicio 9 – Apartado jj

### Enunciado

En qué fecha/hora se realizó la última visita a la URL <https://www.starwars.com/> desde la app de Chrome.

### Resultados obtenidos

Al subdirectorio `/news/star-wars-squadron-is-here` se accedió en 2020-10-04 14:14:15 mientras que a la web como tal <https://www.starwars.com/> se accedió en 2020-10-04 14:13:41.

## Conclusiones

Se han reflejado dos posibilidades, ya que lo he percibido de forma difusa (pues ambos son la misma página realmente), así que hago esa pequeña distinción y lo reflejo en el informe.

## Práctica 5a – Ejercicio 28

### Enunciado

Descargue del campus virtual (Recursos Prácticas->Práctica 5) el fichero denominado windowsram.zip. Se trata de una captura de la memoria RAM de una máquina Windows.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 60 de 109

Descomprima dicho archivo. Vamos a intentar buscar en la captura de memoria trazas de malware. Utilice la herramienta Volatility y realice los siguientes apartados sobre dicha imagen.

## Toma de pruebas

Descargaremos el recurso "*Recursos Prácticas -> Práctica 5a -> windowsram.zip*".

## Análisis de las pruebas

Todos los apartados siguientes se realizarán con la herramienta **Volatility**.

## Práctica 5a – Ejercicio 28 – Apartado i

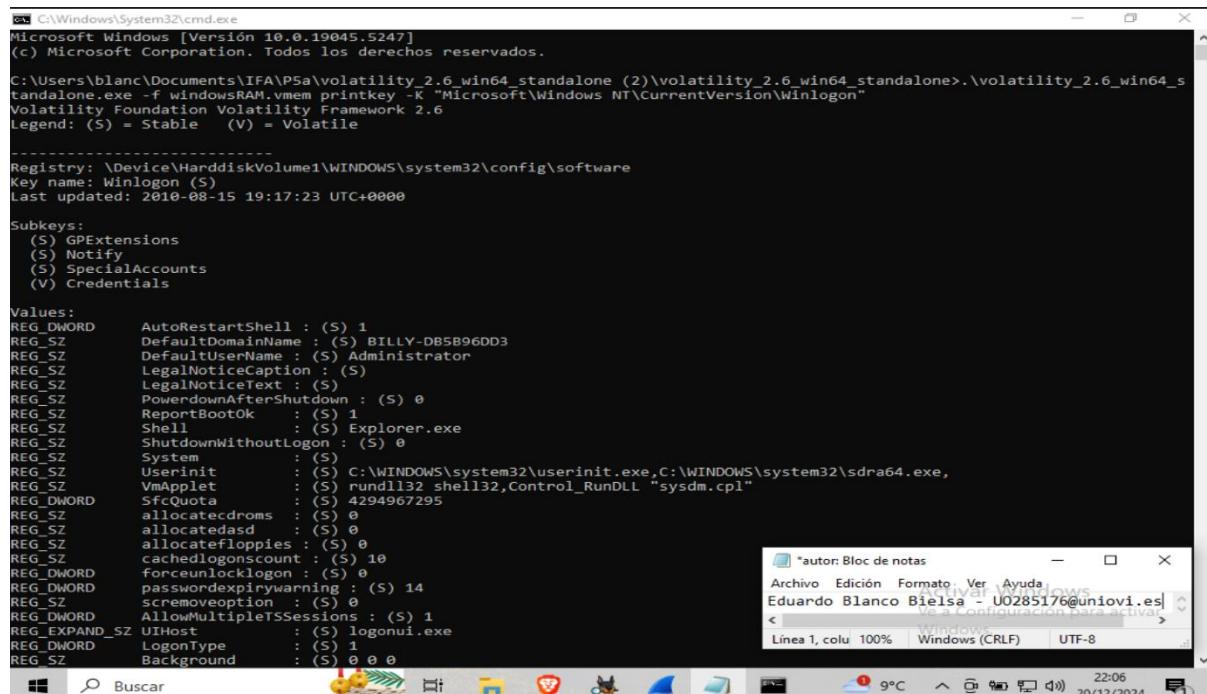
### Enunciado

Suponga que alguna de las IPs detectadas en el apartado d) se encuentra en una blacklist. Si el equipo está infectado por un Troyano, es normal que éste haya añadido una clave al registro de Windows para asegurarse de que se ejecutará en cada reinicio del sistema. Busque información sobre el comando printkey y aplíquelo para buscar información sobre la clave del registro "Microsoft\Windows NT\CurrentVersion\Winlogon".

### Resultados obtenidos

Se usará el siguiente comando:

```
1. .\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 printkeys -K "Microsoft\Windows NT\CurrentVersion\Winlogon"
```



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19045.5247]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\blanc\Documents\IFA\P5a\volatility_2.6.win64_standalone (2)\volatility_2.6.win64_standalone>.\volatility_2.6.win64_standalone.exe -f windowsRAM.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
(S) GPExtensions
(S) Notify
(S) SpecialAccounts
(V) Credentials

Values:
REG_DWORD  AutoRestartShell : (S) 1
REG_SZ    DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ    DefaultUserName : (S) Administrator
REG_SZ    LegalNoticeCaption : (S)
REG_SZ    LegalNoticeText : (S)
REG_SZ    PowerdownAfterShutdown : (S) 0
REG_SZ    ReportBootOk : (S) 1
REG_SZ    Shell : (S) Explorer.exe
REG_SZ    ShutdownWithoutLogon : (S) 0
REG_SZ    System : (S)
REG_SZ    Userinit : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ    VmApplet : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD  SfcQuota : (S) 4294967295
REG_SZ    allocatedcdroms : (S) 0
REG_SZ    allocateddasd : (S) 0
REG_SZ    allocatefloppies : (S) 0
REG_SZ    cachedlogonscount : (S) 10
REG_DWORD  forceunlocklogon : (S) 0
REG_DWORD  passwordexpirywarning : (S) 14
REG_SZ    scremoveoption : (S) 0
REG_DWORD  AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ UIHost : (S) logonui.exe
REG_DWORD  LogonType : (S) 1
REG_SZ    Background : (S) 0 0 0

*autor: Bloc de notas
Archivo Edición Formato Ver Ayuda
Eduardo Blanco Bielsa U0285176@uniovi.es
< Windows (CRLF) | UTF-8
Linea 1, colu 100% 22:06 20/12/2024
```

Ilustración 59. Resolución Práctica 5a - Ej 28 - Apartado i - Parte 1

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 61 de 109

```

C:\ Seleccionar C:\Windows\System32\cmd.exe
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
(S) GPExtensions
(S) Notify
(S) SpecialAccounts
(V) Credentials

Values:
REG_DWORD AutoRestartShell : (S) 1
REG_SZ DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ DefaultUserName : (S) Administrator
REG_SZ LegalNoticeCaption : (S)
REG_SZ LegalNoticeText : (S)
REG_SZ PowerdownAfterShutdown : (S) 0
REG_SZ ReportBootOk : (S) 1
REG_SZ Shell : (S) Explorer.exe
REG_SZ ShutdownWithoutLogon : (S) 0
REG_SZ System : (S)
REG_SZ Userinit : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ VmApplet : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD SfcQuota : (S) 4294967295
REG_SZ allocatedcdroms : (S) 0
REG_SZ allocateddasd : (S) 0
REG_SZ allocatefloppies : (S) 0
REG_SZ cachedlogonscount : (S) 10
REG_DWORD forceunlocklogon : (S) 10
REG_DWORD passwordexpirywarning : (S) 14
REG_SZ scremoveoption : (S) 0
REG_DWORD AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ UIHost : (S) logonui.exe
REG_DWORD LogonType : (S) 1
REG_SZ Background : (S) 0 0 0
REG_SZ AutoAdminLogon : (S) 0
REG_SZ DebugServerCommand : (S) no
REG_DWORD SFCDisable : (S) 0
REG_SZ WinStationsDisabled : (S) 0
REG_DWORD HibernationPreviouslyEnabled : (S) 1
REG_DWORD ShowLogonOptions : (S) 0
REG_SZ AltDefaultUserName : (S) Administrator
REG_SZ AltDefaultDomainName : (S) BILLY-DB5B96DD3

```

Ilustración 60. Resolución Práctica 5a - Ej 28 - Apartado i - Parte 2

Podemos apreciar los programas userinit.exe y sdra64.exe.

## Conclusiones

Se ha buscado información sobre el comando requerido y se han encontrado dos programas en la propiedad asociada al inicio. Toda la información ha sido reflejada en el informe.

## Práctica 5a – Ejercicio 28 – Apartado j

### Enunciado

Si ha realizado con éxito el apartado anterior, fíjese en el segundo valor de la subclave UserInit. Busque en internet información sobre ese ejecutable.

### Resultados obtenidos

El archivo sdra64.exe es un componente del software de *desconocido* propiedad de *desconocido*.

**sdra64** son las siglas de Trojan.Zbot

La mayoría de los programas antivirus identifican sdra64.exe como malware, como Microsoft lo identifica como un *VirTool:Win32/VBInject.gen!FU*, y Kaspersky lo identifica como un *Trojan.Win32.Scar.dowx*.

Más información en [file.net](#).

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 62 de 109

## Conclusiones

Se ha realizado investigación operativa para encontrar información sobre el troyano, que se ha reflejado en el informe.

## Práctica 5a – Ejercicio 28 – Apartado k

### Enunciado

Haga un volcado de los procesos que detectó en el apartado f) que no se correspondan con navegadores web. Utilice para ello el comando de volatility que permite extraer no solo el contenido de la memoria sino cualquier contenido en disco asociado a dicho proceso.

### Resultados obtenidos

Podemos sacar los procesos ejecutando el siguiente comando:

```
1. .\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 connscan
```

```
C:\Users\blanc\Documents\IFA\P5a\volatility_2.6_win64_standalone (2)\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address           Remote Address         Pid
-----
0x02214988 172.16.176.143:1054   193.104.41.75:80      856
0x06015ab0 0.0.0.0:1056          193.104.41.75:80      856
```

Ilustración 61. Resolución Práctica 5a - Ej 28 - Apartado k - Parte 1

Vemos que hay dos procesos. Ejecutaremos el siguiente comando para extraer contenido de memoria y disco asociado a dicho proceso:

```
1. .\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 procdump -p 856 -D .\dumped_files
```

```
C:\Users\blanc\Documents\IFA\P5a\volatility_2.6_win64_standalone (2)\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 procdump -p 856 -D .\dumped_files
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name           Result
-----
0x80ff88d8 0x01000000 svchost.exe    OK: executable.856.exe

C:\Users\blanc\Documents\IFA\P5a\volatility_2.6_win64_standalone (2)\volatility_2.6_win64_standalone>
```

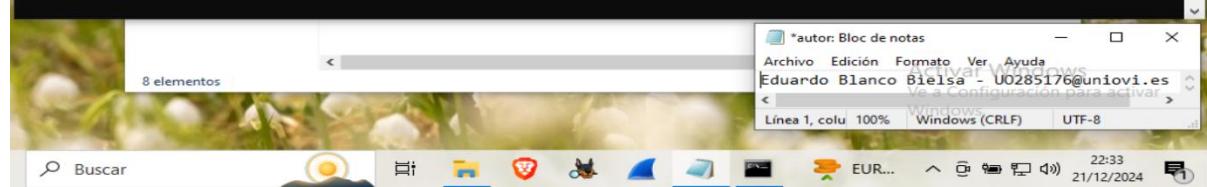


Ilustración 62. Resolución Práctica 5a - Ej 28 - Apartado k - Parte 2

Vemos que se ha creado un fichero executable.856.exe como resultado.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 63 de 109

## Conclusiones

Se ha conseguido extraer el ejecutable del proceso y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 28 – Apartado l

### Enunciado

Obtenga la firma hash de el/los fichero/s donde ha almacenado el volcado de/los proceso/s. Utilice para ello HashMyFiles que puede encontrar en la subcarpeta Nirsoft del CD de Caine.

### Resultados obtenidos

Filename	MD5	SHA1	CRC32	SHA-256	S
executable.856.exe	51d9e15ce372609889bdb07f43a4f096	b8646458f4333bb5bd0fd7306c454edac3601...	a793c49c	6c2e410fb752b62a1db31bf285f8188d4a0124...	9

Ilustración 63. Resolución Práctica 5a - Ej 28 - Apartado l

## Conclusiones

Se han obtenido las firmas hash correspondientes al ejecutable y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 28 – Apartado m

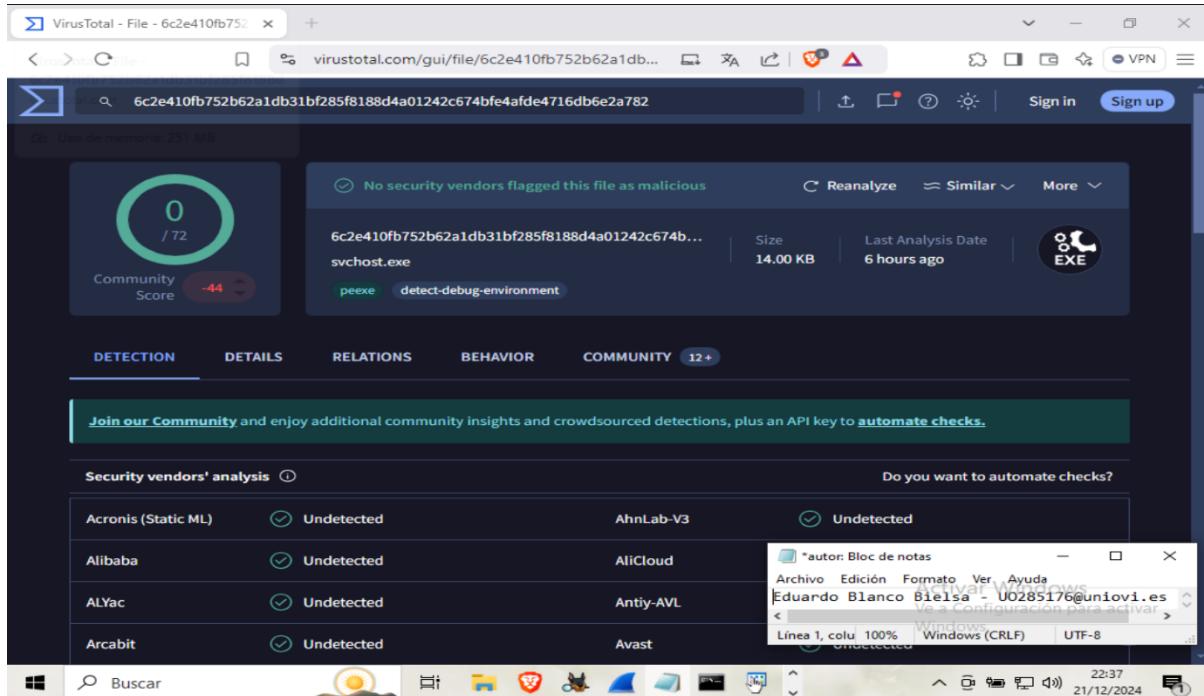
### Enunciado

Compruebe en la página Web de VirusTotal (<https://www.virustotal.com/gui/home/search>) si se reconoce la firma hash del/los fichero/s volcados como software malicioso.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 64 de 109

## Resultados obtenidos

No se ha detectado ninguna amenaza maliciosa en el ejecutable:



## Conclusiones

No se ha detectado software malicioso en el ejecutable mediante la búsqueda del hash en la base de datos de VirusTotal, por lo que no podemos garantizar que sea malicioso. Pese a que VirusTotal nos indique que no contiene un virus, no podemos garantizar que no lo tenga, pues puede ser un nuevo virus que aún no hayan almacenado en sus bases de datos.

## Práctica 5a – Ejercicio 28 – Apartado n

### Enunciado

Los mutex son variables de exclusión mútua que se utilizan para serializar el acceso a una sección crítica en programación concurrente. Hay software malicioso que crea mutex con nombre para asegurarse que una sola instancia del programa malicioso se está ejecutando en el sistema. Utilice el comando mutant de Volatility para obtener todos los objetos KMUTANT pertenecientes a mutex con nombre.

### Resultados obtenidos

Ejecutaremos el siguiente comando:

```
1. .\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 mutantscan
```

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 65 de 109

```
C:\Windows\System32\cmd.exe
DataSectionObject 0xff368130 856 \Device\HarddiskVolume1\WINDOWS\system32\shell32.dll
C:\Users\blanc\Documents\IFA\P5a\volatility_2.6.win64_standalone (2)\volatility_2.6.win64_standalone>.\volatility_2.6.win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 mutantscan
Volatility Foundation Volatility Framework 2.6
Offset(P) #Ptr #Hnd Signal Thread CID Name
0x000000000000962c0 1 1 1 0x0000000000000000
0x0000000000007c9840 1 1 1 0x0000000000000000
0x0000000000009d86e0 1 1 1 0x0000000000000000
0x0000000000009d9688 1 1 1 0x0000000000000000
0x000000000000da878 1 1 1 0x0000000000000000
0x000000000000da88 1 1 1 0x0000000000000000
0x000000000000105a278 1 1 1 0x0000000000000000
0x000000000000105a28 1 1 1 0x0000000000000000
0x000000000000105aa38 7 6 1 0x0000000000000000 _!MSFTHISTORY!
0x000000000000105ac10 2 1 0 0xffff3ba880 888:912 wsctnfy_mtx
0x000000000000105e900 1 1 1 0x0000000000000000
0x0000000000001061fe0 2 1 1 0x0000000000000000
0x00000000000010633b8 2 1 1 0x0000000000000000
0x0000000000001066480 2 1 1 0x0000000000000000
0x00000000000010669d0 2 1 1 0x0000000000000000
0x0000000000001066bd0 2 1 1 0x0000000000000000
0x00000000000010676d8 2 1 1 0x0000000000000000
0x0000000000001067d60 1 1 1 0x0000000000000000
0x0000000000001069fa8 2 1 1 0x0000000000000000
0x000000000000106fb60 3 2 1 0x0000000000000000
0x0000000000001070380 2 1 1 0x0000000000000000
0x00000000000010719b0 2 1 1 0x0000000000000000
0x0000000000001071e40 1 1 1 0x0000000000000000
0x000000000000107a2b0 2 1 1 0x0000000000000000
0x000000000000107b290 2 1 1 0x0000000000000000
0x000000000000107c200 1 1 1 0x0000000000000000
0x000000000000108af50 1 1 1 0x0000000000000000
0x0000000000001093568 1 1 1 0x0000000000000000
0x0000000000001093c10 1 1 1 0x0000000000000000
0x0000000000001093c90 4 3 1 0x0000000000000000
0x00000000000010aef80 1 1 1 0x0000000000000000
0x00000000000010b7f68 1 1 1 0x0000000000000000
0x00000000000010bb748 1 1 1 0x0000000000000000
0x00000000000010bb7b8 1 1 1 0x0000000000000000
0x00000000000010bf10 2 1 1 0x0000000000000000
0x00000000000010bc140 2 1 1 0x0000000000000000
0x00000000000010bc550 2 1 1 0x0000000000000000
ZonesLockedCache *autor: Bloc de notas
  Archivo Edición Formato Ver Ayuda
  Eduardo Blanco Bielsa UO285176@uniovi.es| < Línea 1, colu 100% Windows (CRLF) | UTF-8
  Tcpip_Perf_Library Lock PID 684
  MSDTC_Perf_Library Lock PID 684
  PerfDisk_Perf_Library Lock PID 684
  22:39 20/12/2024
```

Ilustración 64. Resolución Práctica 5a - Ej 28 - Apartado n

Se han encontrado los siguientes mutex: 2018 y 2019.

## Conclusiones

Se han documentado los mutex hallados en el informe.

## Práctica 5a – Ejercicio 28 – Apartado o

### Enunciado

Observe la lista de mutex con nombre que aparecen en la salida del comando de la opción anterior. Muestre solamente las líneas en las que aparece la palabra AVIRA.

### Resultados obtenidos

Se ejecutará el siguiente comando:

```
1. .\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 mutantscan |
findstr /i "AVIRA"
```

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 66 de 109

```

C:\Windows\System32\cmd.exe
0x0000000000644e898 3 2 1 0x0000000000000000 c:\documents and settings\localservice\local settings\histo
y\history_ie51 5 4 1 0x0000000000000000 WindowsUpdateTracingMutex
0x00000000006453bc8 1 1 1 0x0000000000000000
0x00000000006453c38 1 1 1 0x0000000000000000
0x00000000006453e48 1 1 1 0x0000000000000000
0x000000000064951d0 3 2 1 0x0000000000000000 WininetStartupMutex
0x00000000006495c0 1 1 1 0x0000000000000000
0x0000000000651a720 1 1 1 0x0000000000000000
0x00000000006560db0 1 1 1 0x0000000000000000
0x00000000006560e20 1 1 1 0x0000000000000000
0x000000000065c05a8 1 1 1 0x0000000000000000
0x000000000065e810 1 1 1 0x0000000000000000
0x000000000066290f8 1 1 1 0x0000000000000000
0x000000000066c678 1 1 1 0x0000000000000000
0x000000000066ad98 1 1 1 0x0000000000000000
0x000000000066ad28 1 1 1 0x0000000000000000
0x000000000066f68b0 5 4 1 0x0000000000000000 RasPbFile
0x000000000066f6cd0 1 1 1 0x0000000000000000
0x000000000067358a8 2 1 1 0x0000000000000000 RSVP_Perf_Library_Lock_PID_684
0x00000000006735dc0 2 1 1 0x0000000000000000 _AVIRA_2109
0x000000000067790f8 1 1 1 0x0000000000000000
0x00000000006779d48 1 1 1 0x0000000000000000
0x0000000000687f0f8 1 1 1 0x0000000000000000
0x00000000006961288 1 1 1 0x0000000000000000
0x00000000006944ba0 1 1 1 0x0000000000000000
0x00000000006945830 1 1 1 0x0000000000000000
0x00000000006945a30 1 1 1 0x0000000000000000
0x0000000000694678 1 1 1 0x0000000000000000
0x00000000006b1a460 2 1 1 0x0000000000000000
0x00000000006b40ff8 1 1 1 0x0000000000000000
C:\Users\blanc\Documents\IFA\P5a\volatility_2.6.win64_standalone (2)\volatility_2.6.win64_standalone> f windowsRAM.vmem --profile=WinXPSP2x86 mutantscan | grep -i "AVIR
tandalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 mutantscan | grep -i "AVIR
"grep" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\blanc\Documents\IFA\P5a\volatility_2.6.win64_standalone (2)\volatility_2.6.win64_standalone> .\volatility_2.6.win64_standalone> f windowsRAM.vmem --profile=WinXPSP2x86 mutantscan | findstr /i "AVIR
Volatility Foundation Volatility Framework 2.6
0x00000000005ca1e8 2 1 1 0x0000000000000000 _AVIRA_2108
0x00000000006735dc0 2 1 1 0x0000000000000000 _AVIRA_2109
Activar Windows
Ve a Configuración para activar
Windows.

C:\Users\blanc\Documents\IFA\P5a\volatility_2.6.win64_standalone (2)\volatility_2.6.win64_standalone>

```

Ilustración 65. Resolución Práctica 5a - Ej 28 - Apartado o

## Conclusiones

Se ha detallado en el informe los dos resultados obtenidos.

## Práctica 5a – Ejercicio 28 – Apartado p

### Enunciado

Busque en internet información sobre aquellas cadenas en las que figure AVIRA como subcadenas.  
¿De qué tipo de software malicioso se trata?

### Resultados obtenidos

Información extraída de [avira.com](http://avira.com)

Los **mutex** (objetos de sincronización en sistemas operativos) son utilizados por diversos tipos de software malicioso para garantizar que solo una instancia del malware se ejecute en el sistema. Algunos de estos mutex contienen la subcadena "AVIRA". Sin embargo, la presencia de "AVIRA" en el nombre del mutex no implica necesariamente una relación directa con el software de seguridad Avira.

Por ejemplo, el ransomware **Money Message** crea un mutex único al iniciarse para evitar que otras instancias del malware se ejecuten simultáneamente. Este comportamiento es común en muchos tipos de malware, incluyendo troyanos de acceso remoto (RATs) como **XWorm**, que se propaga a través de correos electrónicos de spam y puede infectar sistemas con ransomware u otras amenazas.

## Conclusiones

Se ha realizado investigación operativa acerca de subcadenas AVIRA y se ha reflejado la información obtenida en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 67 de 109

## Práctica 5a – Ejercicio 28 – Apartado q

### Enunciado

Compruebe si el FireWall está deshabilitado ya que o bien lo tenía deshabilitado el usuario o bien fue deshabilitado por un software malicioso. Para ello compruebe el valor de la clave de registro "ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile". ¿Estaba el FireWall de Windows deshabilitado?

### Resultados obtenidos

Ejecutaremos el siguiente comando:

```
1. .\volatility_2.6_win64_standalone.exe -f windowsRAM.vmem --profile=WinXPSP2x86 printkeys -K "ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile"
```

The screenshot shows a Windows desktop environment. In the foreground, a command prompt window displays the output of the volatility command. The output shows the registry key 'StandardProfile' under 'ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy'. A value named 'EnableFirewall' is listed with a REG\_DWORD type and a value of 0, indicating that the firewall is disabled. In the background, there is a 'Bloc de notas' (Note) window open, showing a single line of text: 'Eduardo Blanco Bielsa - UO285176@uniovi.es'. The desktop taskbar at the bottom shows various pinned icons and the date/time as 20/12/2024 22:52.

Ilustración 66. Resolución Práctica 5a - Ej 28 - Apartado q

Como hay un 0, el Firewall estaba deshabilitado.

### Conclusiones

Se ha concluido que el firewall estaba deshabilitado y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 34

### Enunciado

En este ejercicio vamos a tratar de obtener los metadatos de las fotografías existentes en los ficheros imagenXX.jpg resultado de descomprimir el fichero imágenesP5.zip (Recursos Prácticas->Práctica 5). Para cada una de dichas imágenes trate de obtener la siguiente información:

- Fecha en la que fue tomada la imagen.
- Ubicación. En caso de que dicha información no esté presente en los metadatos, trate de averiguarla a través de la búsqueda inversa de imágenes.
- Marca de la cámara.
- Modelo de la cámara.
- Modelo del teléfono en caso de haberse realizado con un Smartphone.
- Año de lanzamiento del teléfono.
- Características de la imagen:

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 68 de 109

- o Dimensión (ancho x alto) de la imagen en pixels.
- o Resolución.
- o Bits de color por píxel.
- Tamaño del archivo.

Para obtener los metadatos EXIF de dichas imágenes puede utilizar bien la herramienta EXIFToolGUI o bien desde la página <http://metapicz.com/>.

## Toma de pruebas

Descargaremos el fichero *imagenesP5.zip* del Campus Virtual.

## Análisis de las pruebas

Se han utilizado herramientas online para la extracción de metadatos (**Exiftool Online** y **Metadata2Go**). Además, para la búsqueda de imágenes se ha usado Google Lens y Google Maps y para obtener modelos de teléfono se ha realizado investigación operativa (OSINT).

## Práctica 5a – Ejercicio 34 – Imagen 2

### Resultados obtenidos

- **Fecha en la que fue tomada la imagen:** 2024:07:30 09:19:20 +02:00
- **Ubicación. En caso de que dicha información no esté presente en los metadatos, trate de averiguarla a través de la búsqueda inversa de imágenes:** las coordenadas no están disponibles, por lo que se usará la extensión de google Reverse Image Search para buscar en distintos navegadores como Yandex o Google Lens. Se corresponde con el Palacio Ducal de Venecia, geolocalizado en 45.43383, 12.34039:

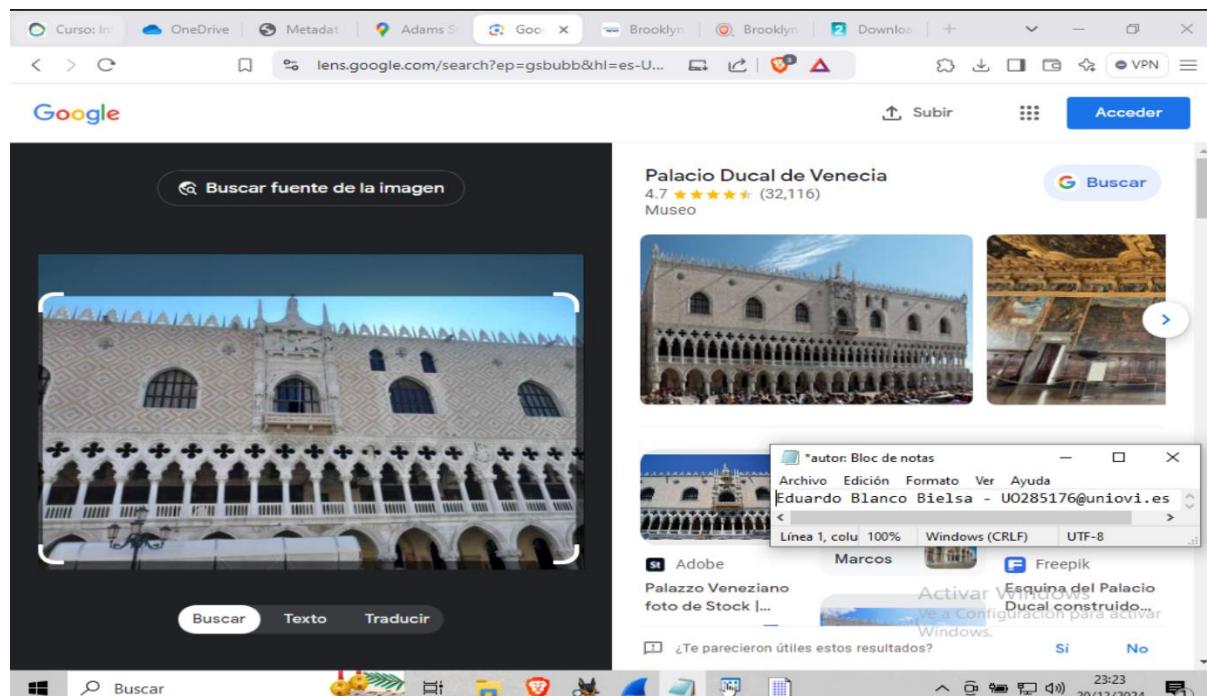


Ilustración 67. Resolución Práctica 5a - Ej 34 - Imagen 2 - Parte 1

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 69 de 109

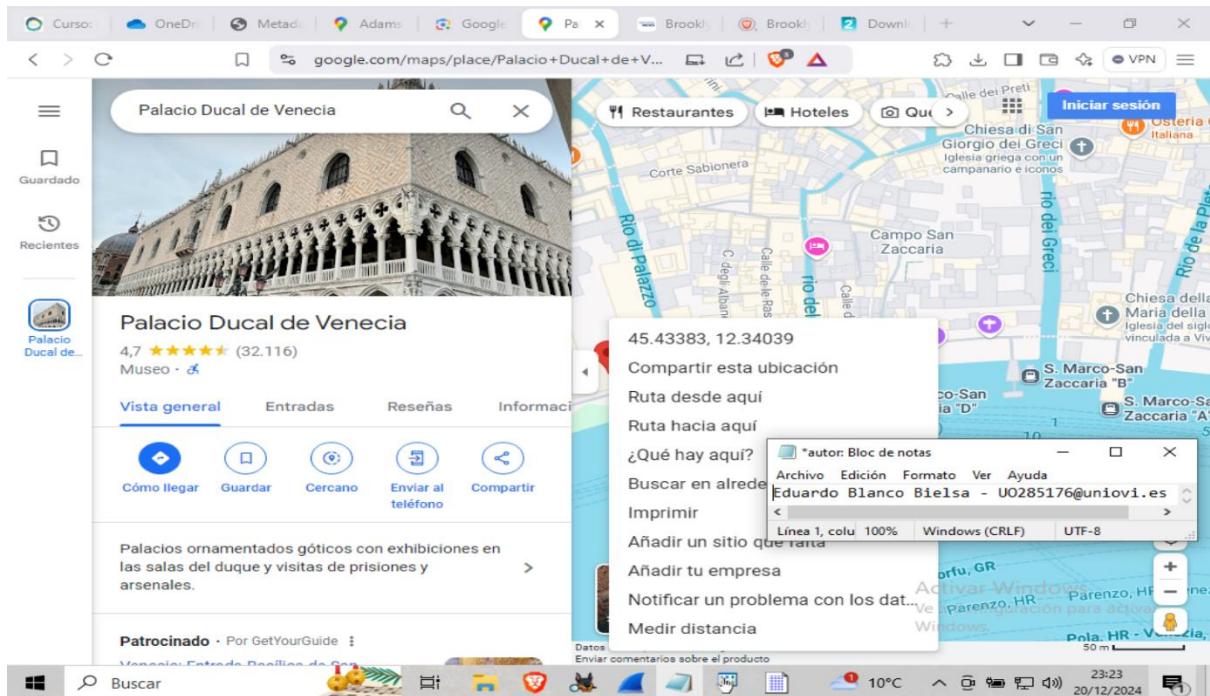


Ilustración 68. Resolución Práctica 5a - Ej 34 - Imagen 2 - Parte 2

- **Marca de la cámara:** Samsung
- **Modelo de la cámara:** SM-M135F
- **Modelo del teléfono en caso de haberse realizado con un Smartphone:** No se indica, pero si en Google Buscamos el teléfono asociado a dicha cámara se corresponde con el Samsung Galaxy A13
  - [Fuente](#)
- **Año de lanzamiento del teléfono:** 2022
- **Características de la imagen:**
  - **Dimensión (ancho x alto) de la imagen en pixels:** 4080x3060
  - **Resolución:** 72 píxeles por pulgada tanto en X como en Y
  - **Bits de color por píxel:** 8x3=24
- **Tamaño del archivo:** 3 MiB

The screenshot shows the Metadata2Go website interface. On the left, a list of file metadata is displayed:

- file\_name: imagen2.jpg
- file\_size: 3.0 MB
- file\_type: JPEG
- file\_type\_extension: jpg
- mime\_type: image/jpeg
- exif\_byte\_order: Little-endian (Intel, II)
- make: Canon

On the right, there are download and sharing options:

- Download
- Export As
- Share
- Delete

A preview window shows a portion of the image file content.

Ilustración 69. Resolución Práctica 5a - Ej 34 - Imagen 2 - Parte 3

## Conclusiones

Realizando diversas técnicas de OSINT se han conseguido datos tales como las coordenadas y el dispositivo usado para la realización de la fotografía. Además, se han analizado metadatos exif. Todos los datos han sido reflejados en el informe junto con todos los pasos del procedimiento.

## Práctica 5a – Ejercicio 34 – Imagen 4

### Resultados obtenidos

- Fecha en la que fue tomada la imagen:** 2024:08:02 12:36:20 +02:00
- Ubicación. En caso de que dicha información no esté presente en los metadatos, trate de averiguarla a través de la búsqueda inversa de imágenes:** las coordenadas no están disponibles, por lo que se usará la extensión de google Reverse Image Search para buscar en distintos navegadores como Yandex o Google Lens. Resulta ser el Palazzo della Ragione, en Verona, concretamente 45.44323, 10.99776:

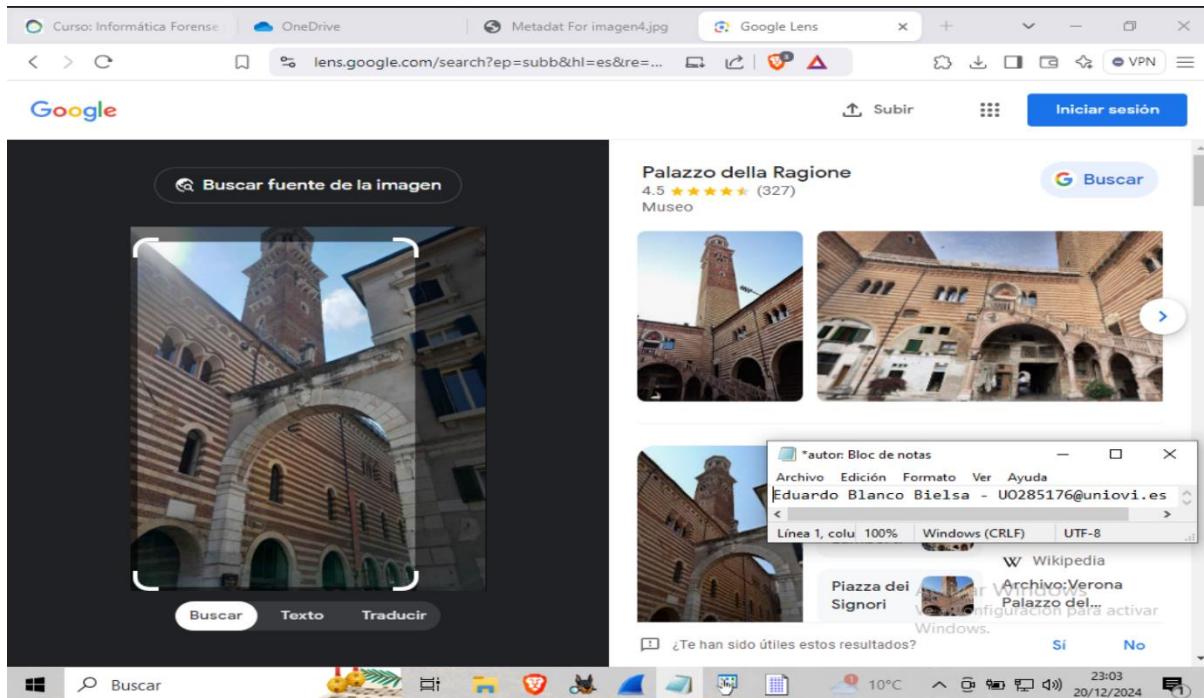


Ilustración 70. Resolución Práctica 5a - Ej 34 - Imagen 4 - Parte 1

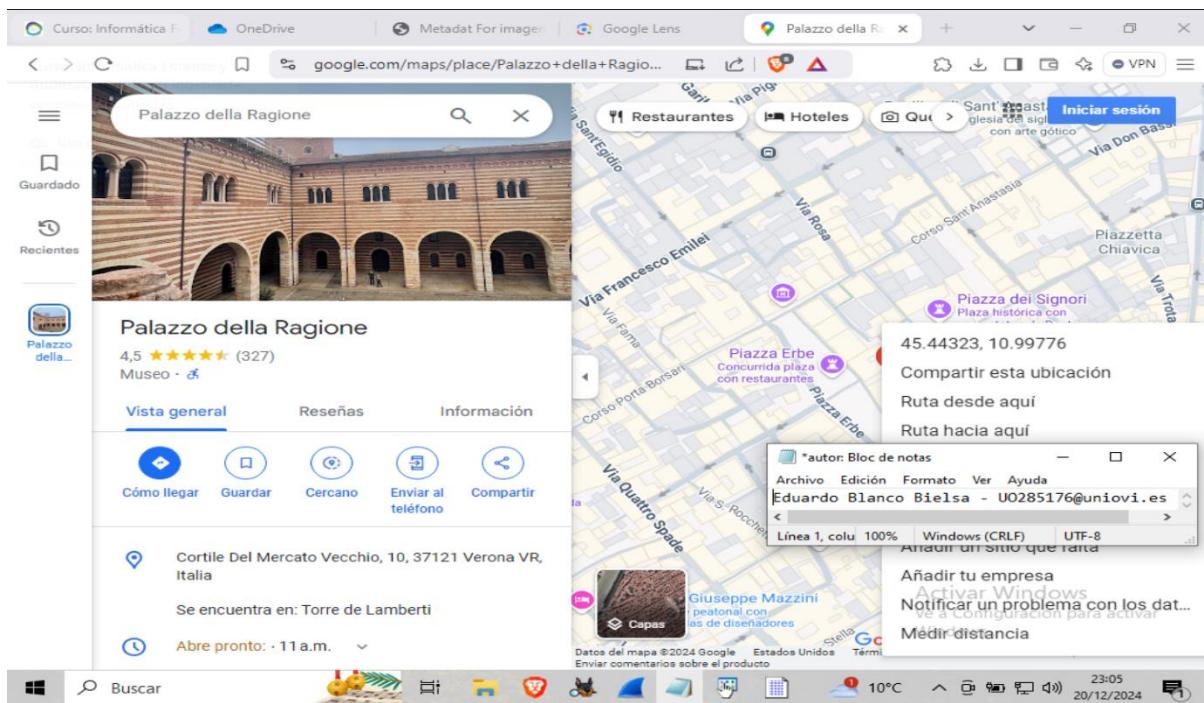


Ilustración 71. Resolución Práctica 5a - Ej 34 - Imagen 4 - Parte 2

- Marca de la cámara:** Samsung
- Modelo de la cámara:** SM-M135F
- Modelo del teléfono en caso de haberse realizado con un Smartphone:** No se indica, pero si en Google Buscamos el teléfono asociado a dicha cámara se corresponde con el Samsung Galaxy A13

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 72 de 109

- [Fuente](#)
- **Año de lanzamiento del teléfono:** 2022
- **Características de la imagen:**
  - **Dimensión (ancho x alto) de la imagen en pixels:** 4080 x 3060
  - **Resolución:** 72 píxeles por pulgada tanto en X como en Y
  - **Bits de color por píxel:** 8x3=24 bits
- **Tamaño del archivo:** 3MiB

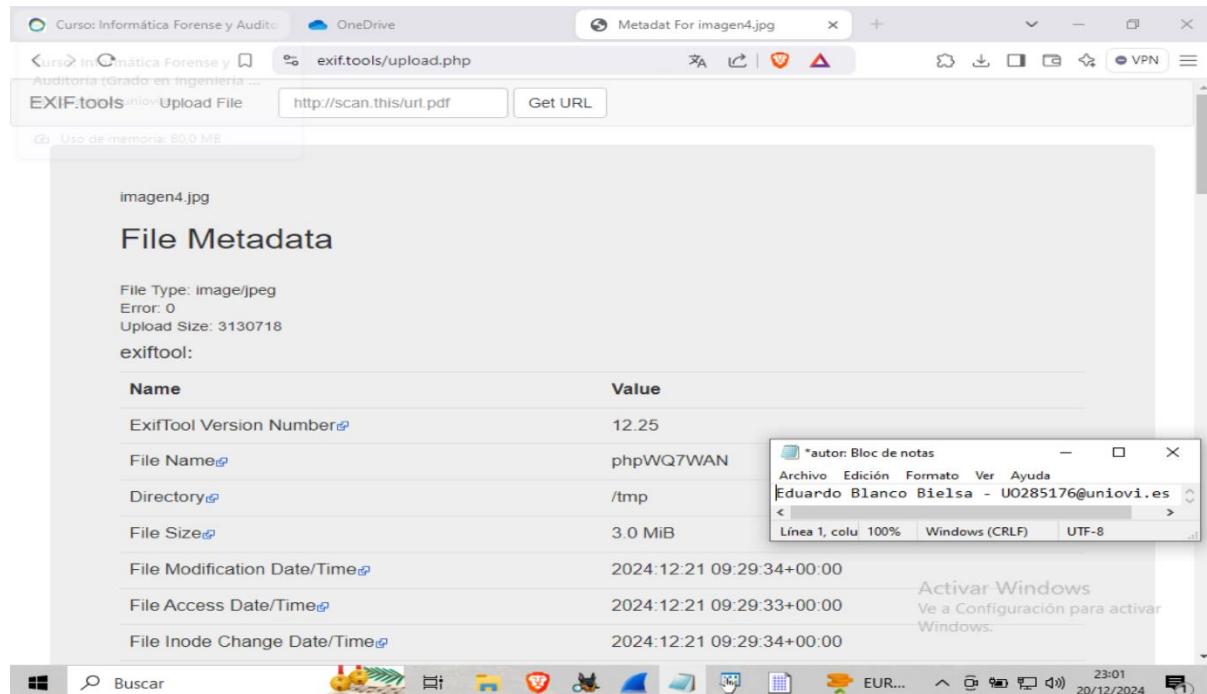


Ilustración 72. Resolución Práctica 5a - Ej 34 - Imagen 4 - Parte 3

## Conclusiones

Realizando diversas técnicas de OSINT se han conseguido datos tales como las coordenadas y el dispositivo usado para la realización de la fotografía. Además se han analizado metadatos exif. Todos los datos han sido reflejados en el informe junto con todos los pasos del procedimiento.

## Práctica 5a – Ejercicio 34 – Imagen 15

### Resultados obtenidos

- **Fecha en la que fue tomada la imagen:** no aparece la fecha de creación sólo las MAC Times, por lo que vamos a tomar como su fecha de creación la MAC de modificación (la más fiable) 2024:12:21 09:40:49 +00:00

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 73 de 109

- Ubicación.** En caso de que dicha información no esté presente en los metadatos, trate de averiguarla a través de la búsqueda inversa de imágenes: De nuevo tampoco aparece la ubicación, por lo que usaremos navegadores como Google Lens o Yandex para averiguar su geolocalización. Se corresponde con la Librería pública de Brooklyn (Adams Street Library), situada en 40.70449, -73.98828:

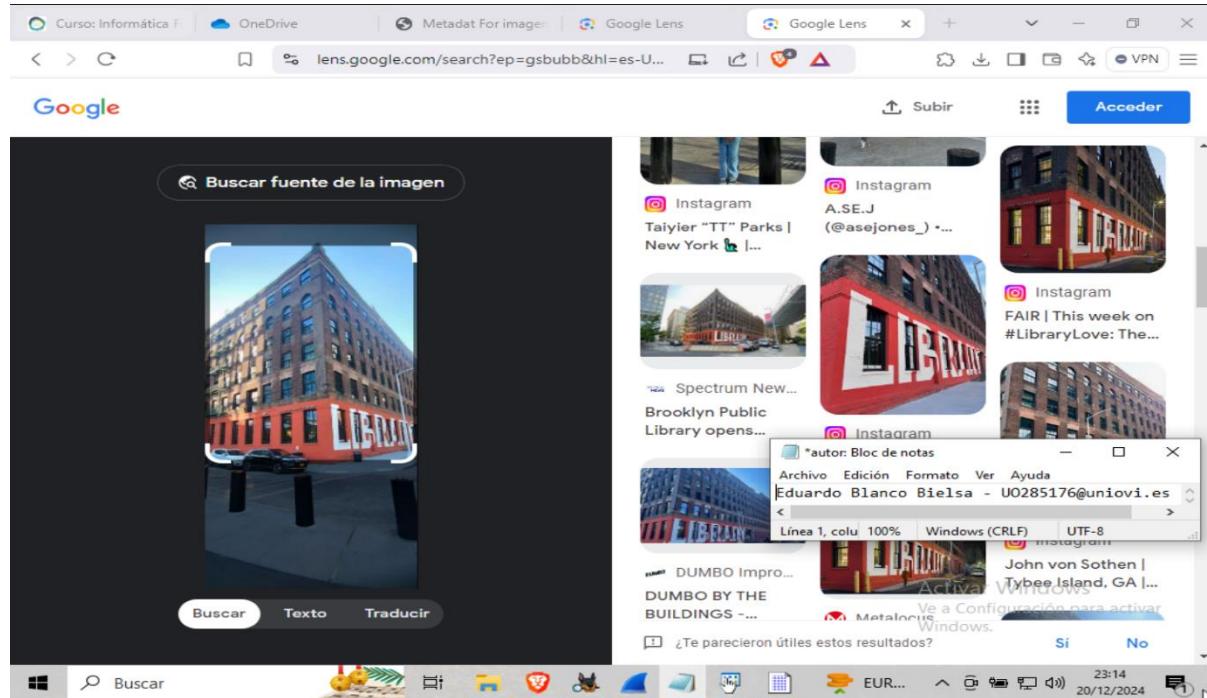


Ilustración 73. Resolución Práctica 5a - Ej 34 - Imagen 15 - Parte 1

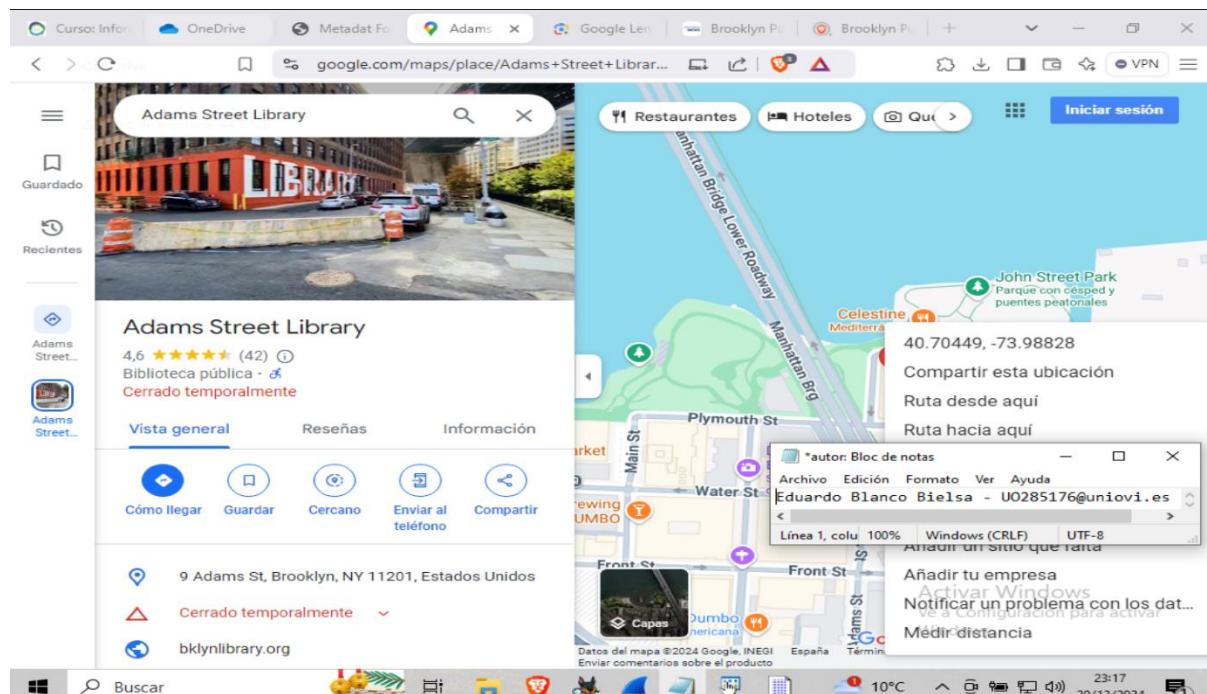


Ilustración 74. Resolución Práctica 5a - Ej 34 - Imagen 15 - Parte 2

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 74 de 109

- Marca de la cámara: -
- Modelo de la cámara: -
- Modelo del teléfono en caso de haberse realizado con un Smartphone: -
- Año de lanzamiento del teléfono: -
- Características de la imagen:
  - Dimensión (ancho x alto) de la imagen en pixels: 719x1600
  - Resolución: 1 píxel por pulgada tanto en X como en Y
  - Bits de color por píxel: 8x3=24
- Tamaño del archivo: 162 KiB

The screenshot shows a web browser window with the URL <http://exif.tools/upload.php>. The page displays file metadata for 'imagen15.jpg'. The 'File Metadata' section includes the following details:

Name	Value
ExifTool Version Number	12.25
File Name	phpC1s1m
Directory	/tmp
File Size	162 KiB
File Modification Date/Time	2024:12:21 09:40:49+00:00
File Access Date/Time	2024:12:21 09:40:49+00:00
File Inode Change Date/Time	2024:12:21 09:40:49+00:00

A small window titled 'autor: Bloc de notas' is overlaid on the browser, showing the text 'Eduardo Blanco Bielsa - U0285176@uniovi.es'. The browser's status bar at the bottom right shows 'Activar Windows' and 'Windows (CRLF)'. The taskbar at the bottom of the screen shows various pinned icons.

Ilustración 75. Resolución Práctica 5a - Ej 34 - Imagen 15 - Parte 3

## Conclusiones

En esta investigación no se han encontrado datos tales como el teléfono o el modelo de la cámara, pero se ha podido localizar dónde se hizo la foto. Todos los datos han sido reflejados en el informe junto con todos los pasos del procedimiento.

## Práctica 5a – Ejercicio 35

### Enunciado

En este ejercicio vamos a tratar de obtener los metadatos existentes en los ficheros resultado de descomprimir el archivo `ficherosP5.zip` (Recursos Prácticas->Práctica 5). Para obtener dichos metadatos utilice la página información que le proporcionará la página Web

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 75 de 109

<https://www.metadata2go.com/>. Para cada uno de los ficheros indicados, trate de obtener la siguiente información:

- Aplicación con la que se creó el archivo.
- Versión de la aplicación con la que se creó el fichero.
- Autor.
- Empresa/organización donde se crea el documento.
- Fecha/hora de creación.
- Fecha/hora modificación.
- Fecha/hora modificación metadatos.
- Número de páginas.
- Tamaño del archivo.

## Toma de pruebas

Descargaremos el fichero *ficherosP5.zip* del Campus Virtual.

## Análisis de las pruebas

Se ha utilizado la herramienta online **Metadata2Go** para la extracción de metadatos.

## Práctica 5a – Ejercicio 35 – Fichero 3

### Resultados obtenidos

- **Aplicación con la que se creó el archivo:** Microsoft Word para Microsoft 365
- **Versión de la aplicación con la que se creó el fichero:** 3.1-701
- **Autor:** Rosa Fernández Tiesta
- **Empresa/organización donde se crea el documento:** -
- **Fecha/hora de creación:** 2024:01:31 09:55:56 +01:00
- **Fecha/hora modificación:** 2024:01:31 09:55:56 +01:00
- **Fecha/hora modificación metadatos:** 2024:01:31 09:55:56 CET
- **Número de páginas:** 2
- **Tamaño del archivo:** 183 kB

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 76 de 109

The screenshot shows a web browser window for 'METADATA2GO'. The URL is 'metadata2go.com/result#j=b28f0262-411c-41d6-beee-af4956878465'. The main content area displays the following file metadata for 'fichero3.json':

- file\_name: fichero3.pdf
- file\_size: 183 kB
- file\_type: PDF
- file\_type\_extension: pdf
- mime\_type: application/pdf
- pdf\_version: 1.7
- linearized: No

On the right side, there are buttons for 'Download', 'Export As', 'Share', and 'Delete'. A green box labeled 'Done' encourages users to get a subscription. Below the metadata, a preview of the PDF document is shown, which contains the text 'autor: Bloc de notas', 'Eduardo Blanco Bielsa - U0285176@uniovi.es', and '10°C 23:36 20/12/2024'. The taskbar at the bottom shows various icons and the date/time.

Ilustración 76. Resolución Práctica 5a - Ej 35 - Fichero 3

## Conclusiones

Se han analizado los metadatos del fichero correspondiente y se han reflejado en el informe.

## Práctica 5a – Ejercicio 35 – Fichero 6

### Resultados obtenidos

- Aplicación con la que se creó el archivo:** Microsoft Office PowerPoint
- Versión de la aplicación con la que se creó el fichero:** 16
- Autor:** Usuario
- Empresa/organización donde se crea el documento:** -
- Fecha/hora de creación:** 2013:07:03 17:11:32Z
- Fecha/hora modificación:** 2018:10:05 14:11:15Z
- Fecha/hora modificación metadatos:** 2018:10:05 14:11:15Z
- Número de páginas:** 7
- Tamaño del archivo:** 126 kB

The screenshot shows a web browser window with the URL [metadata2go.com/result#j=2af8dceb-1e6f-4f55-8143-21091b0325cf](https://metadata2go.com/result#j=2af8dceb-1e6f-4f55-8143-21091b0325cf). The page displays metadata for a file named 'fichero6.json'. The left panel lists the following metadata items:

- file\_name: fichero6.pptx
- file\_size: 126 kB
- file\_type: PPTX
- file\_type\_extension: pptx
- mime\_type: application/vnd.openxmlformats-officedocument.presentationml.presentation
- zip\_required\_version: 20
- zip\_bit\_flag: 0

The right panel includes options to "Download", "Export As", "Share", and "Delete". A green box indicates the task is "Done". Below the main interface, a small window titled "Bloc de notas" shows the content of the file, which is a Microsoft Word document with the author listed as "Eduardo Blanco Bielsa - UO285176@uniovi.es". The system tray at the bottom right shows the date as 20/12/2024 and the time as 23:40.

Ilustración 77. Resolución Práctica 5a - Ej 35 - Fichero 6

## Conclusiones

Se han analizado los metadatos del fichero correspondiente y se han reflejado en el informe.

## Práctica 5a – Ejercicio 35 – Fichero 9

### Resultados obtenidos

- Aplicación con la que se creó el archivo:** Microsoft Office Word
- Versión de la aplicación con la que se creó el fichero:** 16
- Autor:** BELEN DIEZ GONZALEZ
- Empresa/organización donde se crea el documento:** -
- Fecha/hora de creación:** 2020:07:06 11:42:00Z
- Fecha/hora modificación:** 2024:10:11 08:18:00Z
- Fecha/hora modificación metadatos:** 2024:10:11 08:18:00Z
- Número de páginas:** 11
- Tamaño del archivo:** 13 MB

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 78 de 109

Illustración 78. Resolución Práctica 5a - Ej 35 - Fichero 9

## Conclusiones

Se han analizado los metadatos del fichero correspondiente y se han reflejado en el informe.

## Práctica 5a – Ejercicio 42

### Enunciado

Analice las cabeceras de correo que se encuentran en el fichero CabecerasMensajeSospechoso-2.txt el cual puedes descargar desde Recursos Prácticas->Práctica 5. Para analizar las cabeceras puedes utilizar la página tanto la página web <https://mha.azurewebsites.net/> como <https://mxtoolbox.com/public/tools/emailheaders.aspx>. Averiguar las IPs (<https://centralops.net/co/>, <https://viewdns.info/>, <https://research.domaintools.com/>) de los servidores de correo que aparecen en las cabeceras por los cuales ha pasado el mensaje y comprueba si se trata de IPs de sitios calificados como maliciosos (<https://www.abuseipdb.com>). Para averiguar si la dirección del remitente del mensaje ha sido comprometida utilice el siguiente URL <https://haveibeenpwned.com>. En base a su investigación, responda a las siguientes preguntas.

### Toma de pruebas

Descargaremos el fichero *ficherosP5.zip* del Campus Virtual.

### Análisis de las pruebas

Se han usado las siguientes herramientas para los distintos apartados:

- <https://mha.azurewebsites.net/> y [mxtoolbox](https://mxtoolbox.com/) para analizar cabeceras de correo
- [viewdns](https://viewdns.info/) para averiguar las ips
- [abuseipdb](https://www.abuseipdb.com) para saber si se trata de un sitio web calificado como malicioso

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 79 de 109

- [haveibeenpwned](#) para comprobar si una dirección ha sido comprometida

## Práctica 5a – Ejercicio 42 – Apartado a

### Enunciado

¿Desde qué dirección IP se envió el mensaje?

### Resultados obtenidos

Desde la 156.35.11.135:

#	Header	Value
1	Authentication-Results	spf=none (sender IP is 156.35.11.135) smtp.mailfrom=dslr.ch; unionoviedo.d=none;unionoviedo.mail.onmicrosoft.com; dmarc=none action=none header.from=dslr.ch;
2	Received-SPF	None (protection.outlook.com: dslr.ch does not designate permitted sender hosts)
3	X-Puc-N2	TRUE
4	IronPort-PHdr	9a23:fCQwphRJsgoQ315uNAXH8qvCKtpsv+yvbD5Q0Ylujvd0So/mwa6yHhON2/xhgRfzUJnB7Loc0qyK6/CmATRlyK3CmUhKSIZLWR4Bh/detCobK+nBN3fGKu3ZTx8sVlWQvt1Xi6NU9IBJS2PAWkBTW94jEIBxrwXkd+KPJrFY7OlcS30P2594HObwISizefbB/IA+qqQnN

Ilustración 79. Resolución Práctica 5a - Ej 42 - Apartado a

### Conclusiones

Se ha obtenido la ip y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado b

### Enunciado

¿Qué ISP gestiona el rango de IPs en el que está incluida dicha IP?

## Resultados obtenidos

Lo gestiona RedIris.es:

ViewDNS.info

Tools API Research Data

ViewDNS.info > Tools > Domain / IP Whois

Displays owner/contact information for a domain name or IP address. Can also be used to determine if a domain name is registered or not.

Need to lookup a large number of domains? Enquire about our [bulk whois](#) service by emailing us with your requirements.

Domain / IP Address:  GO

WHOIS Information for 156.35.11.135

This is the RIPE Database query service.  
The objects are in RPSL format.  
The RIPE Database is subject to Terms and Conditions.  
See <https://docs.db.ripe.net/terms-conditions.html>

Information related to '156.35.0.0 - 156.35.255.255'  
Abuse contact for '156.35.0.0 - 156.35.255.255' is 'iris@certsi.es'

inetnum: 156.35.0.0 - 156.35.255.255  
netname: UNIOVI  
descr: Universidad de Oviedo  
descr: Asturias  
country: ES  
admin-c: Rd1U1-RIPE  
tech-c: JAH78-RIPE  
abuse-c: RIAC2-RIPE  
status: LEGACY  
mnt-ixt: IRT-IRIS  
remarks: mail spam reports: iris@certsi.es

\*autor: Bloc de notas

Eduardo Blanco Bielsa - UO285176@uniovi.es

Línea 1, col 100% Windows (CRLF) UTF-8

Activar Windows

Ve a Configuración para activar Windows.

Ilustración 80. Resolución Práctica 5a - Ej 42 - Apartado b

## Conclusiones

Se ha obtenido el ISP concreto y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado c

### Enunciado

Averigüe a qué IPs estuvo vinculado el dominio desde el que se envió originalmente el correo.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 81 de 109

## Resultados obtenidos

Analizaremos **dsr.ch**, y vemos que estuvo vinculado a la ip 212.40.14.9 en Suiza:

The screenshot shows a screenshot of a Windows desktop. At the top, there's a browser window titled "ViewDNS.info > Tools > IP History". The main content area displays a table with the following data:

IP Address	Location	IP Address Owner	Last seen on this IP
212.40.14.9	Switzerland	VTX Services SA	2024-12-21

Below the table, there's a note: "Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address." At the bottom of the browser window, it says "IP history results for dsr.ch." To the right of the browser, a small "Bloc de notas" window is open, showing the text "Eduardo Blanco Bielsa - UO285176@uniovi.es". The Windows taskbar at the bottom includes icons for Start, Search, Task View, File Explorer, Edge, File Explorer, Task Manager, and Control Panel.

Ilustración 81. Resolución Práctica 5a - Ej 42 - Apartado c

## Conclusiones

Se ha averiguado la ip a la que estuvo asociada dicho dominio y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado d

### Enunciado

¿Cuántos dominios figuran vinculados a dicha IP en el momento actual? ¿Figura el dominio desde el cual se envió el correo entre ellos?

## Resultados obtenidos

El correo se envió en 2019, por lo que si filtramos en viewdnsinfo nos sale un total de 5 dominios vinculados:

Domain	Last Update
cagan.cn	2019-
capitals.ch	2024-12-14
cartes-a-gratter.ch	2024-05-29
charriolarchive.com	2024-12-14
citadin.ch	2024-12-14
cloverleaf.ch	2024-12-21
cogidoc.ch	2024-12-14
coindasie.ch	2020-03-29
cpdp-coach.ch	2024-12-14
cordonbleu-lausanne.ch	2024-12-14
cotyinstitute.ch	2022-03-27
coursdedessin.ch	2024-12-14
craniosacral-winterthur.ch	2024-12-14
creativsport.org	2019-07-12
cristian.ch	2024-12-14
decolletage-schweiz.ch	2020-02-23
decolletage-swiss.ch	2020-02-23
der-analytiker.ch	2024-12-14
deranalytiker.ch	2024-12-14
dogzone.ch	2024-12-14
dsr-restaurant.ch	2021-12-19
dsr.ch	2024-12-21
dtp-madarasi.ch	2024-12-14
dueco.ch	2024-12-14
eaglecoaching.ch	2023-11-05
eco-tuning.ch	2024-12-14
ecole-steiner.ch	2017-10-22

Ilustración 82. Resolución Práctica 5a - Ej 42 - Apartado d

## Conclusiones

Se ha averiguado el número de dominios y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado e

### Enunciado

¿A qué organización está asociada la IP que hace de hosting del dominio investigado?

## Resultados obtenidos

Está asociada a ORG-VA3-RIPE (212.40.14.9):

The screenshot shows a Windows desktop environment. A browser window in the foreground displays the WHOIS information for the domain 212.40.14.9. The results show the domain is managed by ORG-VA3-RIPE (VDC-RIPE) and is located in Switzerland (CH). A Notepad window titled 'autor: Bloc de notas' is open, containing the email address 'Eduardo Blanco Bielsa - UO285176@uniovi.es'. The taskbar at the bottom shows various icons and the system tray, which includes a message about activating Windows.

Ilustración 83. Resolución Práctica 5a - Ej 42 - Apartado e

## Conclusiones

Se ha averiguado la organización y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado f

### Enunciado

¿Dónde está radicada el ISP correspondiente a la red anterior?

## Resultados obtenidos

Está en St. Alban-Anlage 44, Basilea (Suiza), correspondiente al ISP VTX Datacom AG:

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 84 de 109

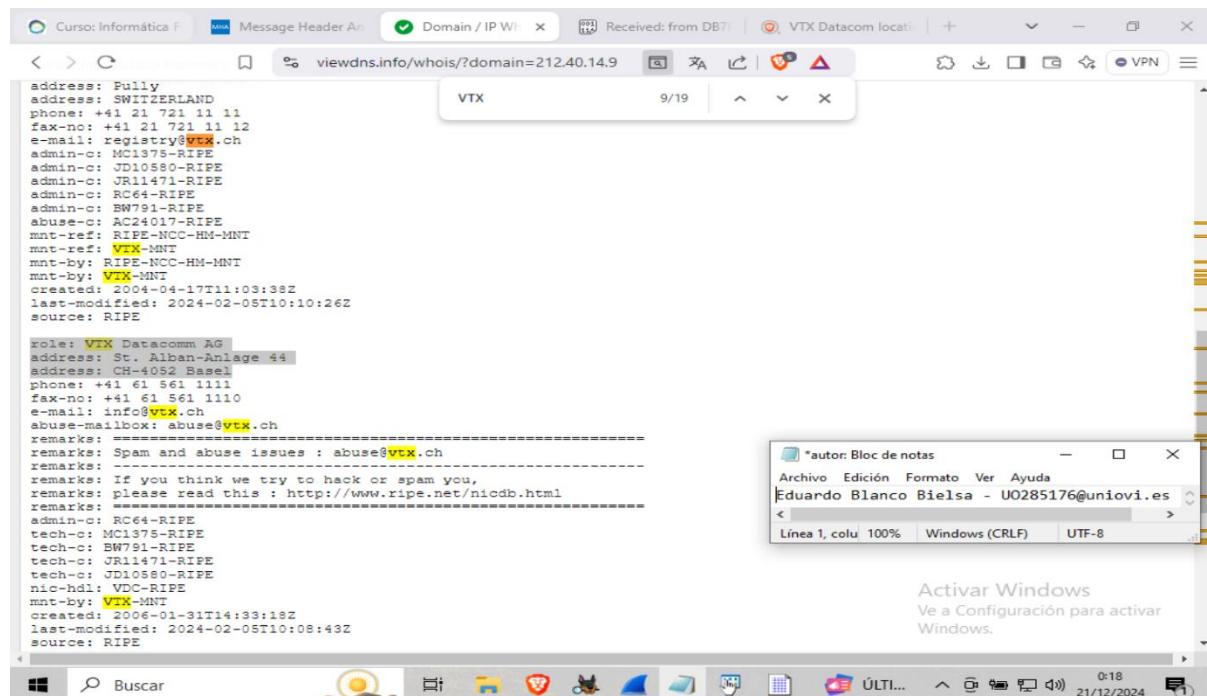


Ilustración 84. Resolución Práctica 5a - Ej 42 - Apartado f

## Conclusiones

Se ha averiguado la ubicación y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado g

### Enunciado

¿Quién aparentemente es el remitente del correo?

### Resultados obtenidos

Se corresponde con [admin@dsrlab.ch](mailto:admin@dsrlab.ch):

Ilustración 85. Resolución Práctica 5a - Ej 42 - Apartado g

## Conclusiones

Se ha averiguado el remitente del correo y se ha reflejado en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 85 de 109

## Práctica 5a – Ejercicio 42 – Apartado h

### Enunciado

¿Puede haber sido comprometida la dirección de correo que figura como remitente del mensaje?

### Resultados obtenidos

No podemos asegurar que haya sido comprometida, pues pese a que herramientas como **Haveibeenpwned** nos digan lo contrario, puede haber sido vulnerada igualmente:

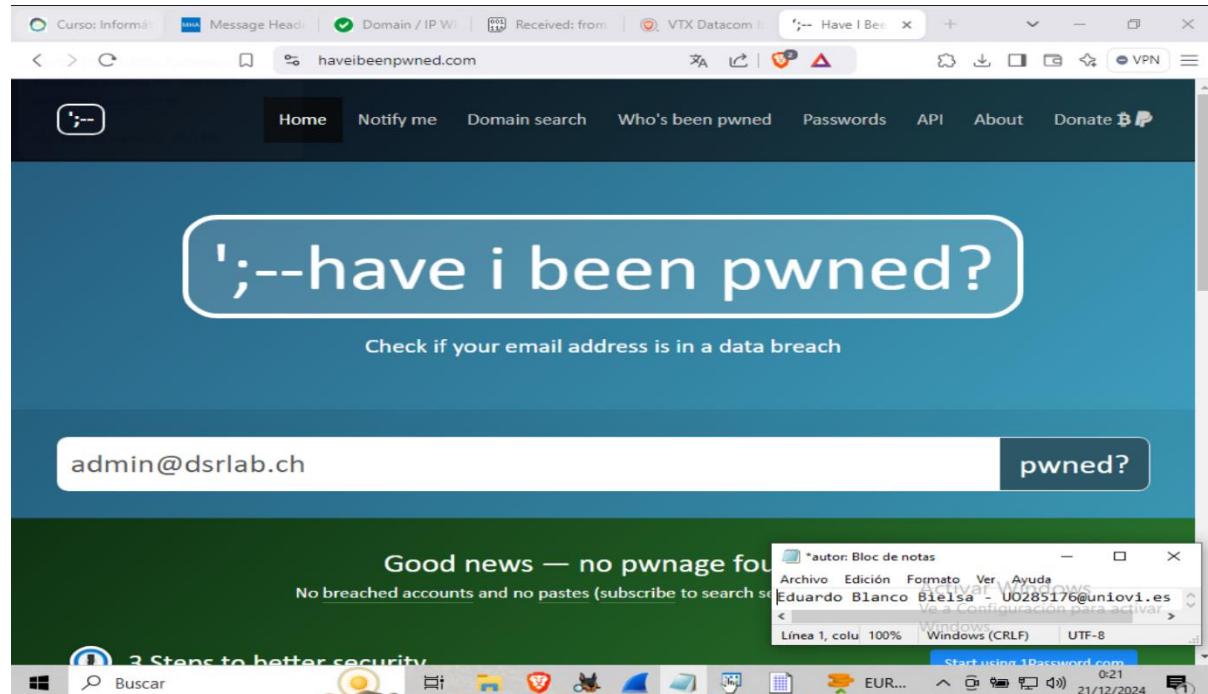


Ilustración 86. Resolución Práctica 5a - Ej 42 - Apartado h

### Conclusiones

No parece ser que la cuenta haya sido comprometida, pero de todos modos puede estarlo. El hecho de que ninguna herramienta diga que no ha sido vulnerada no quiere decir que sea ciertamente así. Dicha información se ha reflejado en el informe.

## Práctica 5a – Ejercicio 42 – Apartado i

### Enunciado

Comprueba si existe la dirección de correo del remitente del mensaje.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 86 de 109

## Resultados obtenidos

Se utilizará la herramienta [email-checker](#):

The screenshot shows a browser window with the URL [email-checker.net/check](https://email-checker.net/check). The main content area is titled "Email Checker" with the subtitle "A simple tool to check whether an email address exists." A form has an "Email Address" input field containing "admin@dsrlab.ch" and a "Check" button. To the right, the result is displayed as "Result : BAD" with the message "dsrlab.ch does not exist". Below this, a note says "Heads up! To verify emails in bulk, use our bulk email checker. You may use Our API via RapidAPI." At the bottom, there's a "How do we verify an email ?" section with a bulleted list and a "Windows" taskbar at the bottom.

Ilustración 87. Resolución Práctica 5a - Ej 42 - Apartado i

## Conclusiones

La cuenta de correo no existe, ya que herramientas para su verificación indican lo contrario.

## Práctica 5a – Ejercicio 45

### Enunciado

Este ejercicio trata de la trazabilidad de un dispositivo móvil, en términos de su actividad y posicionamiento en determinadas fechas, lo cual puede resultar de gran utilidad en ciertas investigaciones, auditorías y actividades de soporte técnico. No obstante, la información disponible o accesible puede ser sólo parcial debido a las circunstancias de los datos en los repositorios del proveedor de servicio o a cuestiones legales que amparen su obtención. El fichero p5\_tr\_cell.csv incluye varias líneas con datos relativos a los registros posicionales y de comunicaciones de un dispositivo móvil. Es habitual que, a instancias judiciales, estos datos se soliciten a los proveedores de servicio para dar curso a las correspondientes diligencias (atestados, peritaciones de parte, etc.) o, directamente, se realicen intervenciones de la línea desde los medios con los que cuente una administración competente. Analizar el fichero indicado, importándolo con separación de punto y coma y convirtiendo a texto las columnas A, B, H e I. A continuación, responder a las siguientes preguntas.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 87 de 109

## Toma de pruebas

Descargaremos el fichero *p5\_tr\_cell.csv* del Campus Virtual y lo importaremos en LibreOffice Calc:

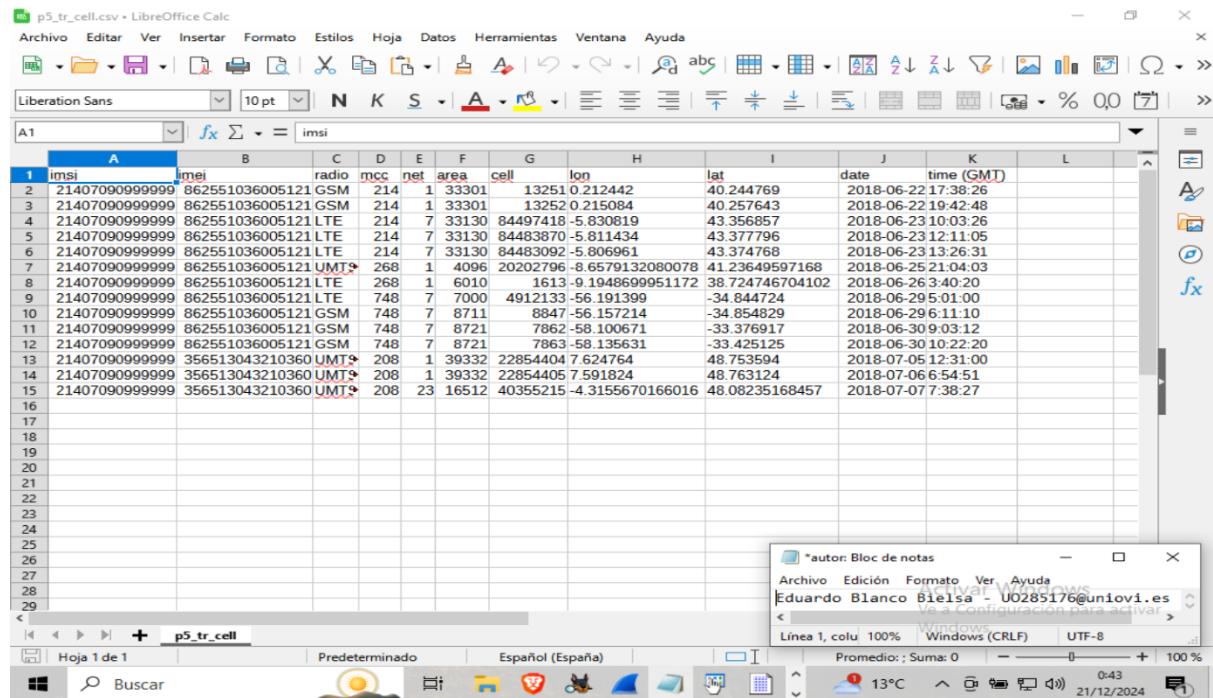


Ilustración 88. Toma de pruebas Práctica 5a - Ej 45

Esta captura sirve para resolver todos los apartados siguientes del ejercicio.

## Práctica 5a – Ejercicio 45 – Apartado a

### Enunciado

Identificación única internacional de la línea móvil (país y proveedor del servicio de origen y número de línea).

### Resultados obtenidos

Todos comparten el mismo **IMSI** -> 214 identifica como país a España, 07 indica como proveedor de servicio a movistar y 0999999999 indica el el número de teléfono (**MSIN**).

### Conclusiones

Se ha razonado la respuesta con la terminología dada en clase y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 45 – Apartado b

### Enunciado

¿Cuántos terminales móviles distintos aparecen registrados?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 88 de 109

## Resultados obtenidos

Hay dos **IMEI** distintos: 862551036005121 y 862551036005121, por lo que hay dos terminales móviles diferentes.

## Conclusiones

Se ha razonado la respuesta con la terminología dada en clase y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 45 – Apartado c

### Enunciado

Identificación única internacional del terminal o terminales móviles utilizados (modelo, fabricante y si está incluido en la Blacklist de España).

### Resultados obtenidos

Para realizar este apartado, se usará la web [imeicheck](#).

Vemos que el IMEI 862551036005121 se corresponde a un Huawei P8 Lite 2017:

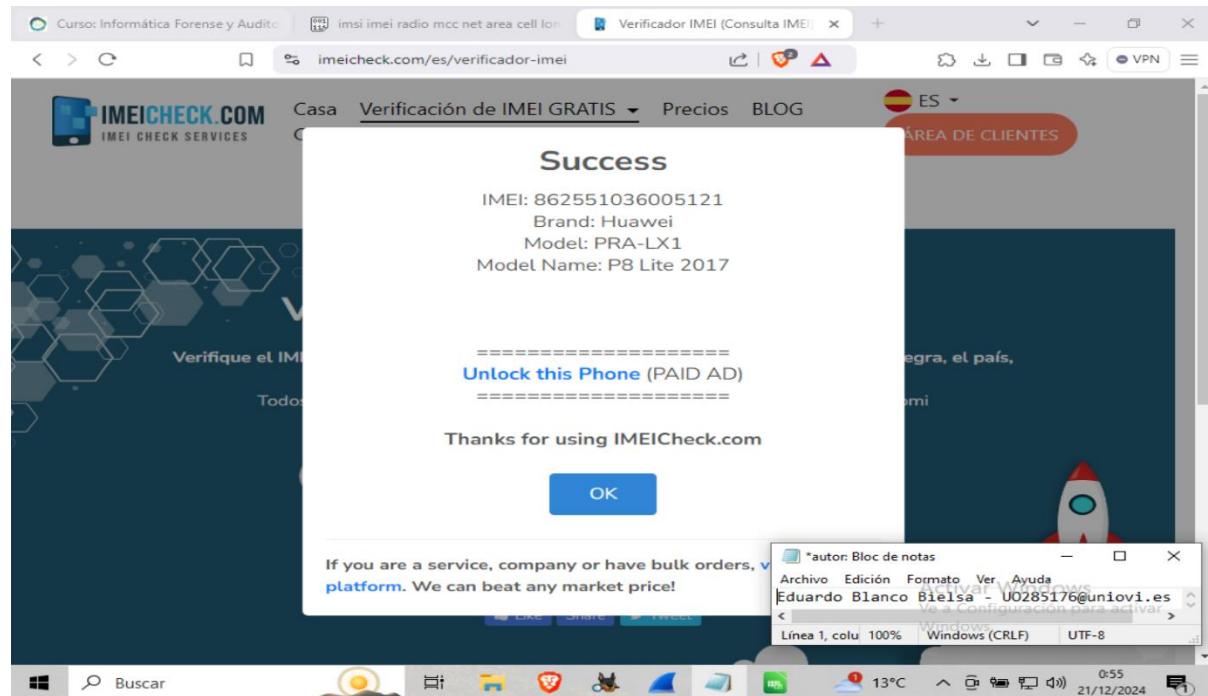


Ilustración 89. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 1

Comprobamos que no está en una BlackList:

The screenshot shows a browser window with the URL [imeicheck.com/imei-blacklist-check](https://imeicheck.com/imei-blacklist-check). The main content area displays the following information:

**Success**

IMEI: 862551036005121  
Brand: Huawei  
Model: PRA-LX1  
Model Name: P8 Lite 2017

Blacklist Status: Clean

=====

[Unlock this Phone \(PAID AD\)](#)

=====

Thanks for using IMEICheck.com

At the bottom, there is a blue "OK" button and a note for service companies about bulk orders.

Ilustración 90. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 2

Vemos que el IMEI 862551036005121 se corresponde a un Motorola Defy:

The screenshot shows a browser window with the URL [imeicheck.com/es/verificador-imei](https://imeicheck.com/es/verificador-imei). The main content area displays the following information:

**Success**

IMEI: 356513043210360  
Brand: Motorola  
Model: DE12310445, MVQ7-334411D11, MB526  
Model Name: Defy

Use [this link](#) to check Blacklist status for FREE

=====

[Unlock this Phone \(PAID AD\)](#)

=====

Thanks for using IMEICheck.com

At the bottom, there is a blue "OK" button and a note for service companies about bulk orders.

Ilustración 91. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 3

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 90 de 109

Comprobamos que no está en una BlackList:

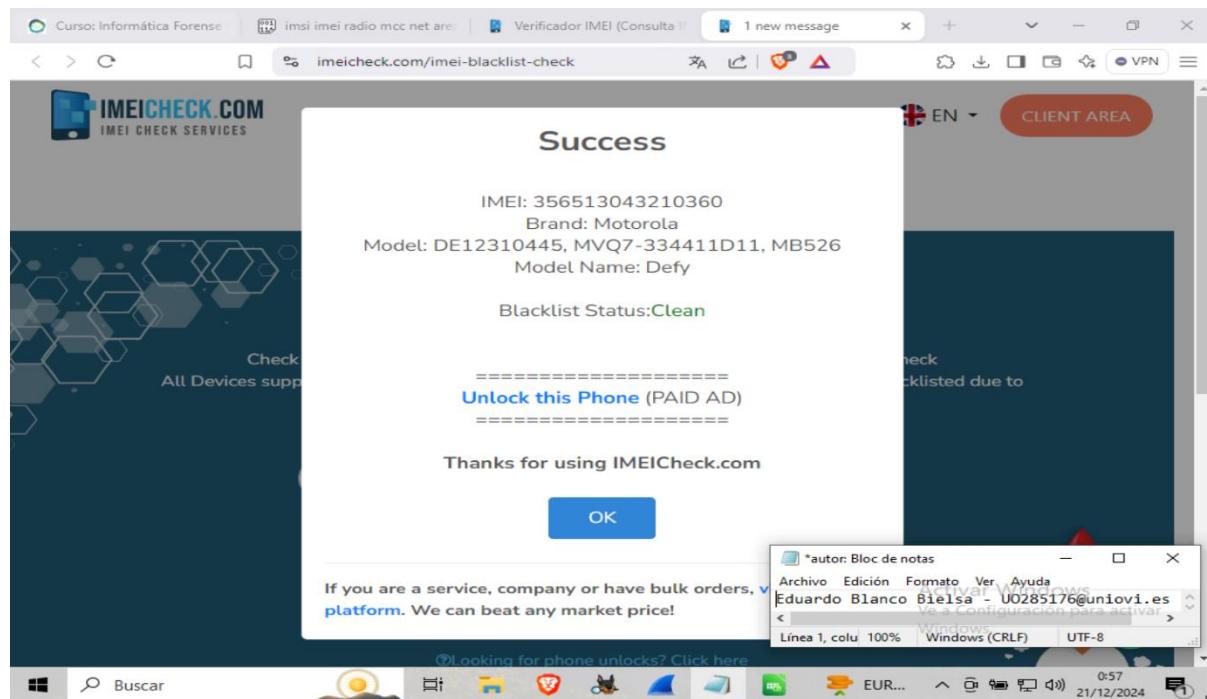


Ilustración 92. Resolución Práctica 5a - Ej 45 - Apartado c - Parte 4

## Conclusiones

Se ha comprobado la autenticidad de los IMEIs, así como de su pertenencia a una Blacklist, dando negativo en ambos casos. Dichos hallazgos se han reflejado en el informe.

## Práctica 5a – Ejercicio 45 – Apartado d

### Enunciado

Indicar el soporte, especificado por el fabricante, en términos de tecnologías de acceso móvil 2G, 3G, 4G y 5G, para el terminal o terminales móviles implicados.

### Resultados obtenidos

La información relativa al Huawei se obtuvo en [Xataka](#):

- Soporta **2G** (GSM 850/900/1800/1900 MHz), **3G** (HSPA 850/900/1900/2100 MHz) y **4G** (LTE 1/3/7/8/20).

La información relativa al Motorola se obtuvo en [Xataka](#):

- Soporta **2G** (GSM 850/900/1800/1900 MHz), **3G** (UMTS/HSPA 850/900/1900/2100 MHz) y **4G** (LTE 1/3/5/7/8/20/28/38/40/41).

### Conclusiones

Se realizó investigación operativa para contestar a este apartado y los datos obtenidos se han reflejado en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 91 de 109

## Práctica 5a – Ejercicio 45 – Apartado e

### Enunciado

Enumerar los países en los que se ha registrado la línea móvil junto con los proveedores de servicio implicados en cada uno de ellos.

### Resultados obtenidos

Hay 4 **MCC**: 214 (España) con proveedor (columna Net) 1 que corresponde a Movistar y proveedor 7 que corresponde a Orange, 268 (Portugal) con proveedor 1 que corresponde a Vodafone, 748 (Chile) con proveedor 7 que corresponde a Entel Chile y 208 (Francia) con proveedor 1 que corresponde a Orange francia y proveedor 23 que corresponde a SFR (Société Française du Radiotéléphone).

### Conclusiones

Se ha realizado investigación operativa para contestar este apartado y los hallazgos se han reflejado en el informe.

## Práctica 5a – Ejercicio 45 – Apartado f

### Enunciado

Indicar si se ha producido roaming, nacional o internacional, y los países implicados.

### Resultados obtenidos

Sí se ha producido roaming internacional porque ha cambiado varias veces el CARRIER (MCC y NET) con los mencionados en el apartado anterior.

### Conclusiones

Para contestar este apartado se ha hecho uso de terminología enseñada en clase y se ha reflejado en el informe.

## Práctica 5a – Ejercicio 45 – Apartado g

### Enunciado

Indicar el recorrido posicional, en sentido temporal creciente e identificando con la máxima precisión posible dicha localización, que se ha registrado para la línea móvil entre el 23 de junio y el 29 de junio, ambos inclusive y correspondientes al año 2018.

### Resultados obtenidos

El recorrido posicional en las fechas indicadas es el siguiente:

- **Coordenada 1:**  
**Latitud:** 43.356857, **Longitud:** -5.830819  
**Ubicación:** se sitúa en el norte de España, cerca de la ciudad de Oviedo, en la región de Asturias.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 92 de 109

- **Coordenada 2:**  
**Latitud:** 43.377796, **Longitud:** -5.811434  
**Ubicación:** Muy cerca de la anterior, en la misma región de Asturias.
- **Coordenada 3:**  
**Latitud:** 43.374768, **Longitud:** -5.806961  
**Ubicación:** Sigue en la región de Asturias, desplazándose ligeramente dentro de la misma área.
- **Coordenada 4:**  
**Latitud:** 41.236495, **Longitud:** -8.657913  
**Ubicación:** Se desplaza hacia el suroeste, cerca de Oporto, en Portugal.
- **Coordenada 5:**  
**Latitud:** 38.724746, **Longitud:** -9.194870  
**Ubicación:** Al sur de Lisboa, en Portugal.
- **Coordenada 6:**  
**Latitud:** -34.844724, **Longitud:** -56.191399  
**Ubicación:** Ahora en el hemisferio sur, en Uruguay, cerca de la ciudad de Paysandú.
- **Coordenada 7:**  
**Latitud:** -34.854829, **Longitud:** -56.157214  
**Ubicación:** Muy cerca de la anterior, en la misma región de Uruguay.

Como se puede apreciar en el recorrido, el usuario ha estado en Asturias, después se fue a Oporto, luego al sur de Lisboa y desde ahí a Uruguay, cerca de Paysandú. Dicho recorrido se ha reflejado detalladamente en el informe.

## Práctica 5b – Ejercicio 3

### Enunciado

Cuando utilizas Internet, estás utilizando el Sistema de Nombres de Dominio (DNS). DNS es una red distribuida de servidores que traduce nombres de dominio descriptivos como www.google.com a una dirección IP. Cuando se escribe la URL de un sitio web en el navegador, la PC realiza una consulta de DNS a la dirección IP del servidor DNS. La consulta del servidor DNS de su PC y la respuesta del servidor DNS hacen uso del Protocolo de Datagramas de Usuario (UDP) como protocolo de capa de transporte. A diferencia de TCP, UDP funciona sin conexión y no requiere una configuración de sesión. Las consultas y respuestas de DNS son muy pequeñas y no requieren la sobrecarga de TCP.

Objetivos de la práctica:

- En esta práctica de laboratorio, establecerá comunicación con un servidor DNS enviando una consulta de DNS mediante el protocolo de transporte UDP. Utilizará Wireshark para examinar los intercambios de consulta y respuesta de DNS con el mismo servidor

### Toma de pruebas

Al contrario de lo que indica el guión de prácticas, este ejercicio se va a realizar en Windows, tal y como se nos indicó por nuestro profesor en clase, en lugar de usar Caine.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 93 de 109

## Práctica 5b – Ejercicio 3 – Apartado a

### Enunciado

En su máquina virtual de CAINE utilice los comandos necesarios para encontrar y registrar las direcciones IPv4 y MAC de las tarjetas de interfaz de red (NIC) virtuales de sus VM, la dirección IPv4 del gateway. Registre esta información en la tabla proporcionada.

### Resultados obtenidos

Se ha consultado el comando `ipconfig /all` de Windows:

Descripción	Configuración
Dirección IPv4	10.0.2.15/16
Dirección MAC	08-00-27-4A-FF-73
Dirección IPv4 de la pasarela	10.0.2.2
Dirección IPv4 del servidor DNS	10.0.2.3

Tabla 4. Resolución Práctica 5b - Ej 3 - Apartado a - Parte 1

```
Microsoft Windows [Versión 10.0.19045.5247]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\blanc>ipconfig /all

Configuración IP de Windows

Nombre de host . . . . . : DESKTOP-923E9NK
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no
Lista de búsqueda de sufijos DNS: .

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . . . .
    Descripción física. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Dirección física. . . . . : 08-00-27-4A-FF-73
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . . . : sí
    Dirección IPv6 . . . . . : fd00:c75a:cb1951:f987(Preferido)
    Dirección IPv6 temporal. . . . . : fd00:b957:f0d0:1068:b81b(Preferido)
    Vínculo: dirección IPv6 local. . . . . : fe80:331c:f194:71d0:b89f%13(Preferido)
    Dirección IPv4. . . . . : 10.0.2.15(Preferido)
    Máscara de subred. . . . . : 255.255.255.0
    Concesión obtenida. . . . . : viernes, 20 de diciembre de 2024 17:40:23
    La concesión expira . . . . . : sábado, 21 de diciembre de 2024 22:54:02
    Puerta de enlace predeterminada . . . . . : fe80::2%13
    10.0.2.2
    Servidor DHCP . . . . . : 10.0.2.2
    IAID DHCPv6 . . . . . : 101187623
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-2E-98-5F-18-08-00-27-4A-FF-73
    Servidores DNS. . . . . : 10.0.2.3
    NetBIOS sobre TCP/IP. . . . . : habilitado

C:\Users\blanc>
```

Ilustración 93. Resolución Práctica 5b - Ej 3 - Apartado a - Parte 2

### Conclusiones

Se han consultado los datos requeridos y se han reflejado en el informe.

## Práctica 5b – Ejercicio 3 – Apartado b

### Enunciado

En una ventana de terminal introduce `wireshark &` para iniciar Wireshark. Haga clic en Aceptar para continuar.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 94 de 109

## Resultados obtenidos

Se va a abrir directamente en Windows:

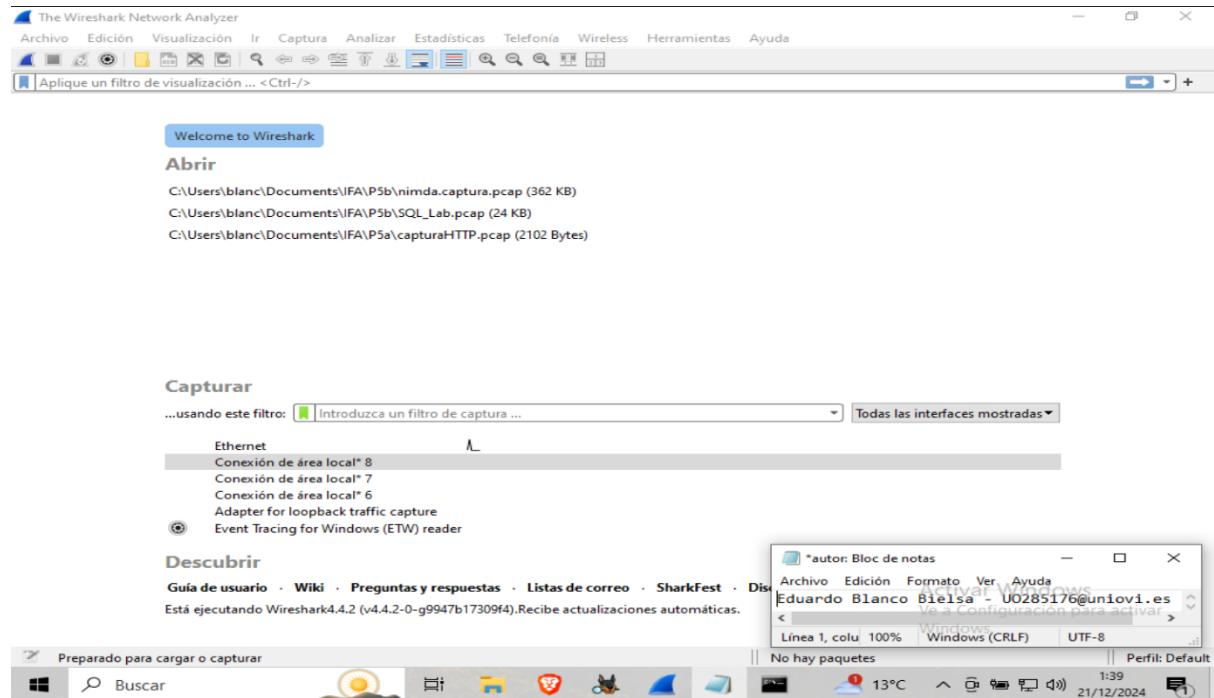


Ilustración 94. Resolución Práctica 5b - Ej 3 - Apartado b

## Conclusiones

Se ha reflejado cómo abrir Wireshark en el informe.

## Práctica 5b – Ejercicio 3 – Apartado c

### Enunciado

En la ventana de Wireshark selecciona con doble clic, en el apartado Captura, el interfaz desde el cual va a capturar los paquetes.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 95 de 109

## Resultados obtenidos

Capturaremos la interfaz Ethernet:

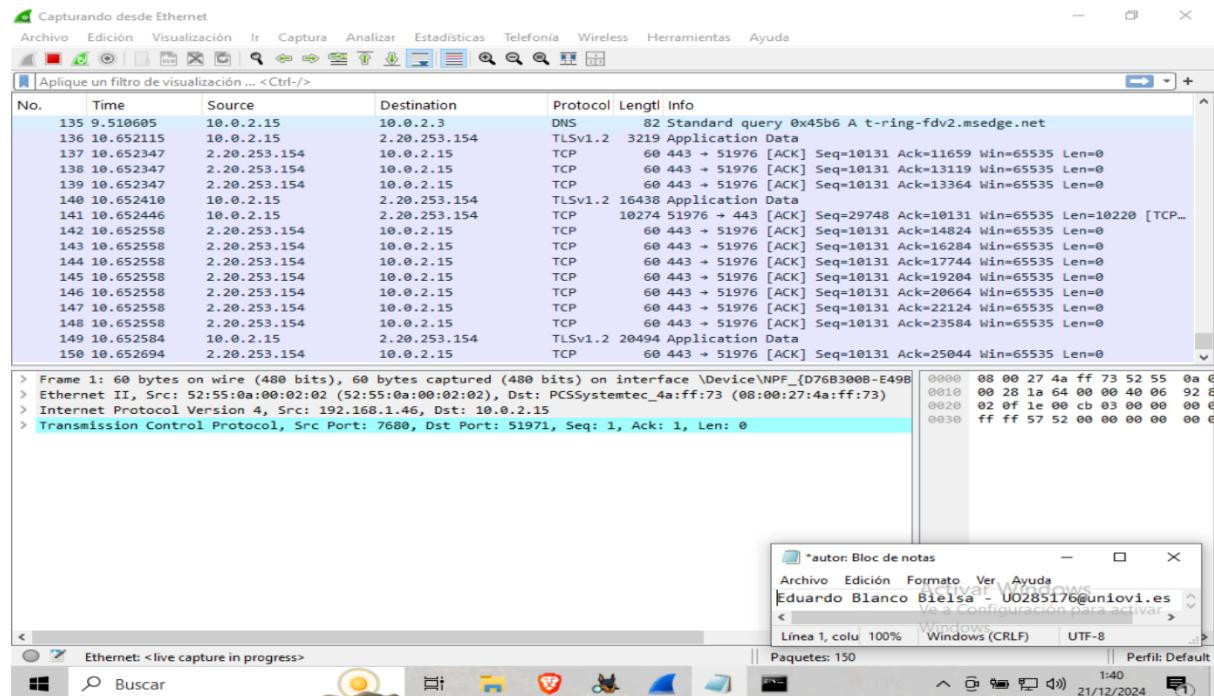


Ilustración 95. Resolución Práctica 5b - Ej 3 - Apartado c

## Conclusiones

Se ha reflejado en el informe cómo capturar una interfaz en Wireshark.

## Práctica 5b – Ejercicio 3 – Apartado d

### Enunciado

Abre el navegador web y dirígete a [www.google.com](http://www.google.com).

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 96 de 109

## Resultados obtenidos

Se ha abierto google en el navegador:

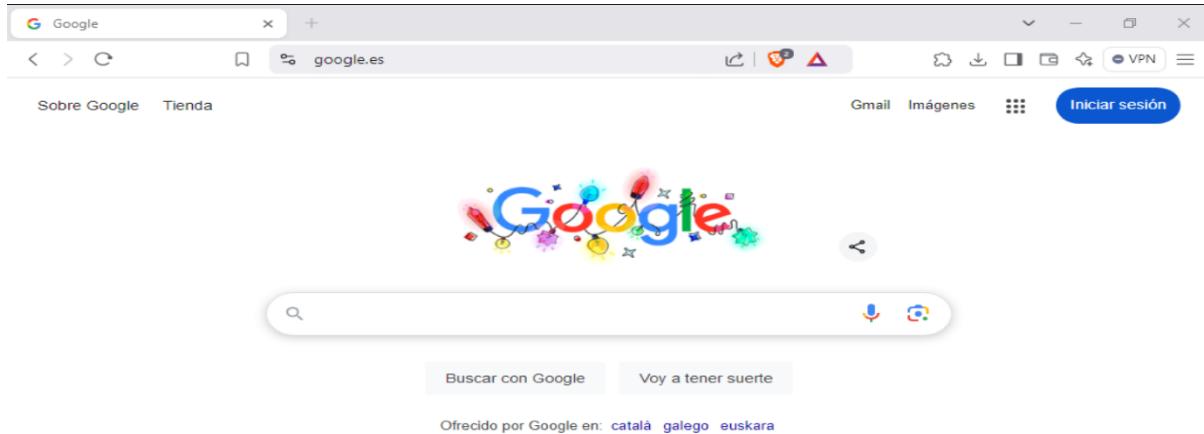


Ilustración 96. Resolución Práctica 5b - Ej 3 - Apartado d

## Conclusiones

Se ha reflejado cómo abrir Google en el informe.

## Práctica 5b – Ejercicio 3 – Apartado e

### Enunciado

Haga clic en Stop (Detener) para detener la captura de Wireshark cuando vea la página de inicio de Google.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 97 de 109

## Resultados obtenidos

Se ha realizado una captura de la petición a google del apartado anterior:

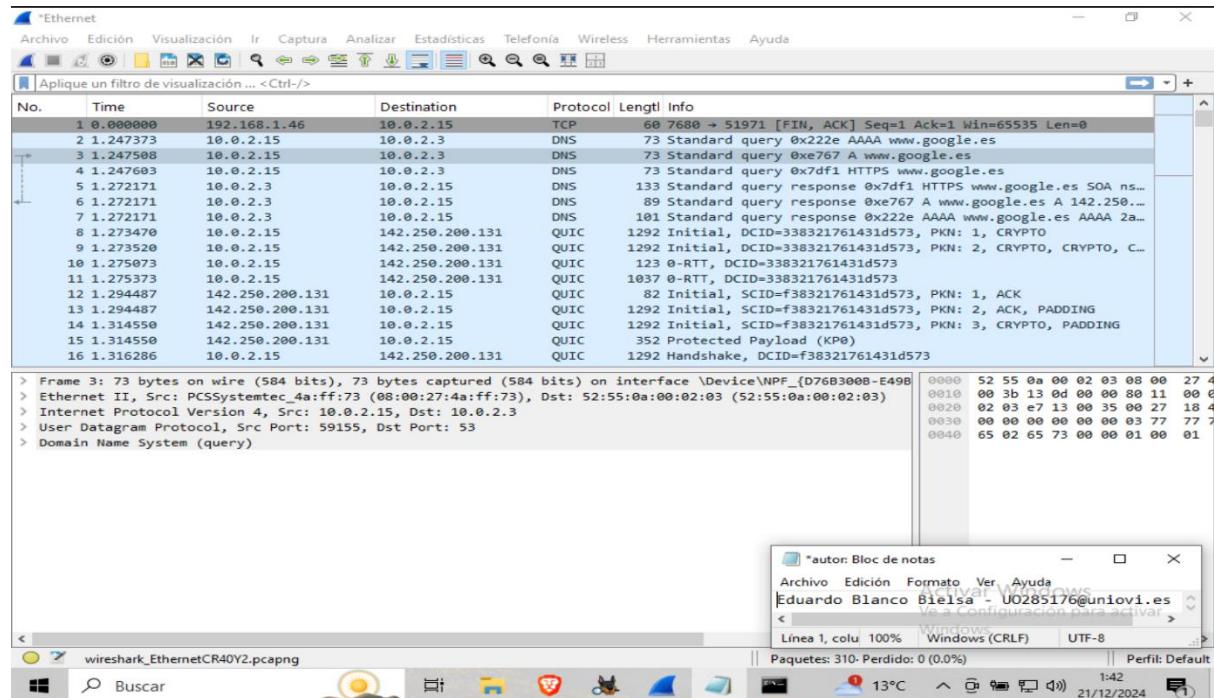


Ilustración 97. Resolución Práctica 5b - Ej 3 - Apartado e

## Conclusiones

Se ha reflejado cómo parar una captura de Wireshark en el informe.

## Práctica 5b – Ejercicio 3 – Apartado f

### Enunciado

En la ventana principal de Wireshark, escriba dns en el campo Filter (Filtro). Haga clic en Apply (Aplicar).

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 98 de 109

## Resultados obtenidos

Se ha aplicado el filtro de protocolo dns:

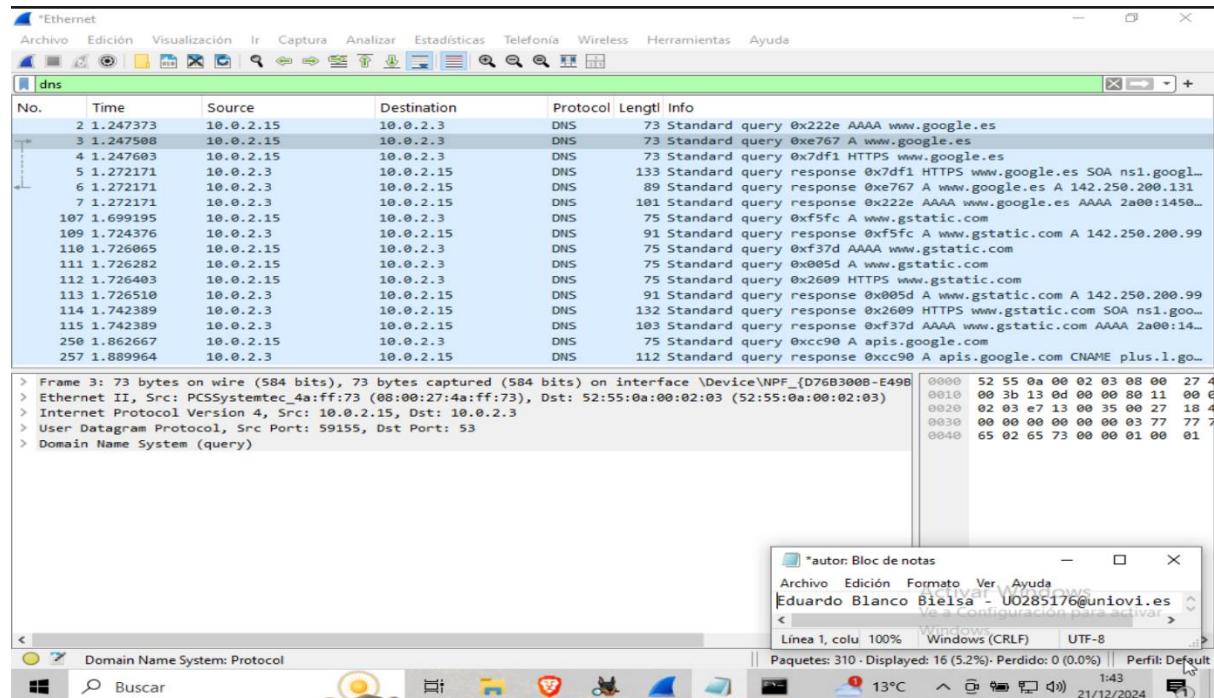


Ilustración 98. Resolución Práctica 5b - Ej 3 - Apartado f

## Conclusiones

Se ha reflejado como aplicar un filtro de protocolo en Wireshark en el informe.

## Práctica 5b – Ejercicio 3 – Apartado g

### Enunciado

En el panel de lista de paquetes (sección superior) de la ventana principal, localice el paquete que incluye Standard query (Consulta estándar) y A [www.google.com](http://www.google.com). Observe la trama 19 anterior como ejemplo.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 99 de 109

## Resultados obtenidos

Se ha marcado el paquete en contreo (el 3):

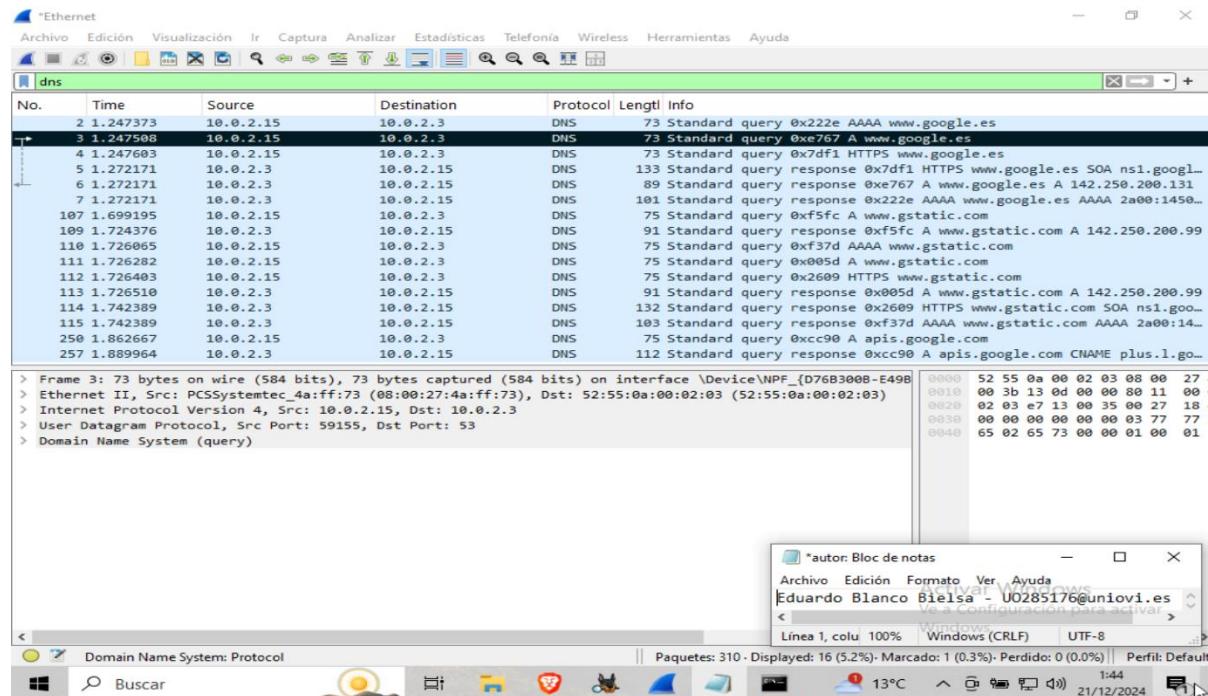


Ilustración 99. Resolución Práctica 5b - Ej 3 - Apartado g

## Conclusiones

Se ha reflejado cómo localizar el paquete que incluye Standard query en el informe.

## Práctica 5b – Ejercicio 3 – Apartado h

### Enunciado

Los campos del paquete, resaltados en color gris, se muestran en el panel de detalles del paquete (sección media) de la ventana principal. En la primera línea del panel de detalles del paquete, la trama 19 tiene 85 bytes de datos transmitidos (on wire). Esta es la cantidad de bytes que se necesitó para enviar una consulta DNS a un servidor con nombre que está solicitando las direcciones IP de [www.google.com](http://www.google.com). Si utilizaste otra dirección web, la cantidad de bytes podría ser diferente.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 100 de 109

## Resultados obtenidos

En mi caso tiene 73 bytes de datos transmitidos (on wire):

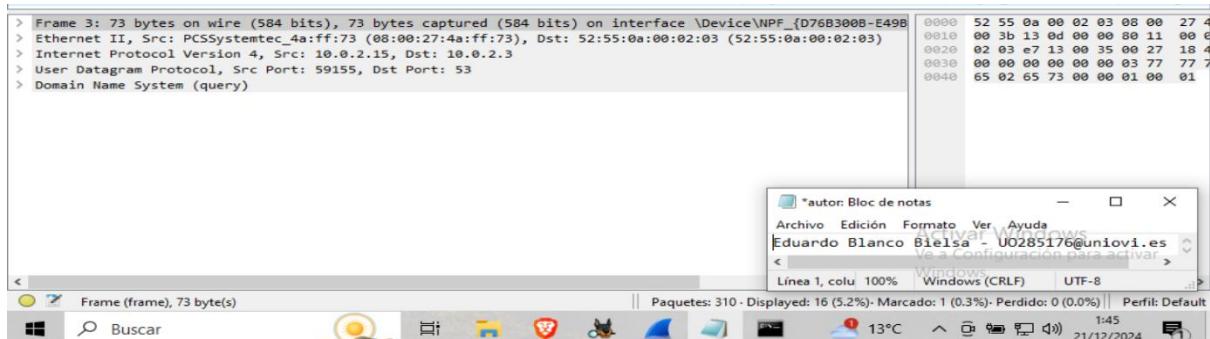


Ilustración 100. Resolución Práctica 5b - Ej 3 - Apartado h

## Conclusiones

Se ha constatado los campos del paquete en el informe.

## Práctica 5b – Ejercicio 3 – Apartado i

### Enunciado

La línea Ethernet II muestra las direcciones MAC de origen y destino. La dirección MAC de origen proviene de su máquina virtual porque su máquina virtual fue la que originó la consulta DNS. La dirección MAC de destino proviene del gateway predeterminado porque esta es la última parada antes de que esta consulta salga de la red local. ¿Es la dirección MAC de origen la misma que la registrada en la Parte 1 para la VM?

## Resultados obtenidos

En Wireshark la MAC se corresponde con 08:00:27:4a:ff:73 idéntica a la del apartado 1 (ver la captura del apartado anterior para contrastar).

### Conclusiones

Se ha comprobado que efectivamente ambas MAC coinciden y se ha reflejado en el informe.

## Práctica 5b – Ejercicio 3 – Apartado j

### Enunciado

En la línea del Protocolo de Internet Versión 4 (IPv4), la captura del paquete IP Wireshark indica que la dirección IP de origen de esta consulta de DNS es 192.168.22.25 (en este ejemplo) y la dirección IP de destino es 192.168.22.1 (en este ejemplo). ¿Puede identificar la dirección IP y dirección MAC de origen y destino de este paquete?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 101 de 109

## Resultados obtenidos

Dispositivo	Dirección IP	Dirección MAC
Máquina virtual cliente	10.0.2.15	08:00:27:4a:ff:73
Destino servidor DNS/Gateway predeterminado	10.0.2.3	52:55:0a:00:02:03

Tabla 5. Resolución Práctica 5b - Ej 3 - Apartado j - Parte 1

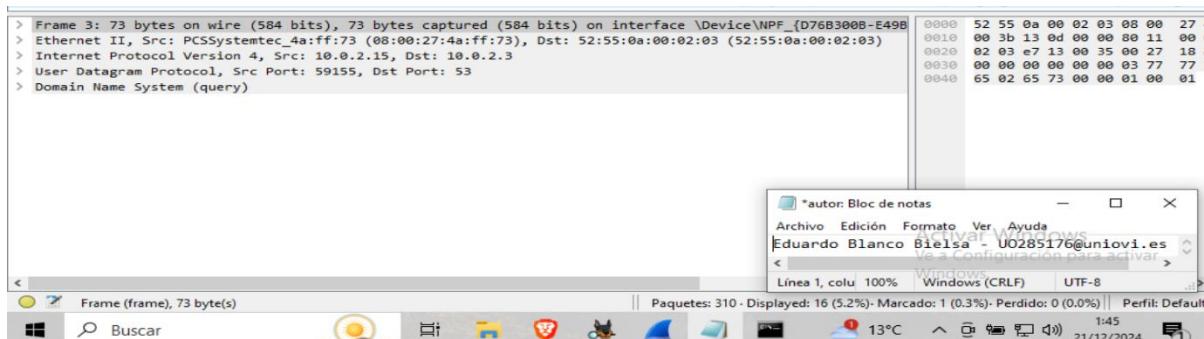


Ilustración 101. Resolución Práctica 5b - Ej 3 - Apartado j - Parte 2

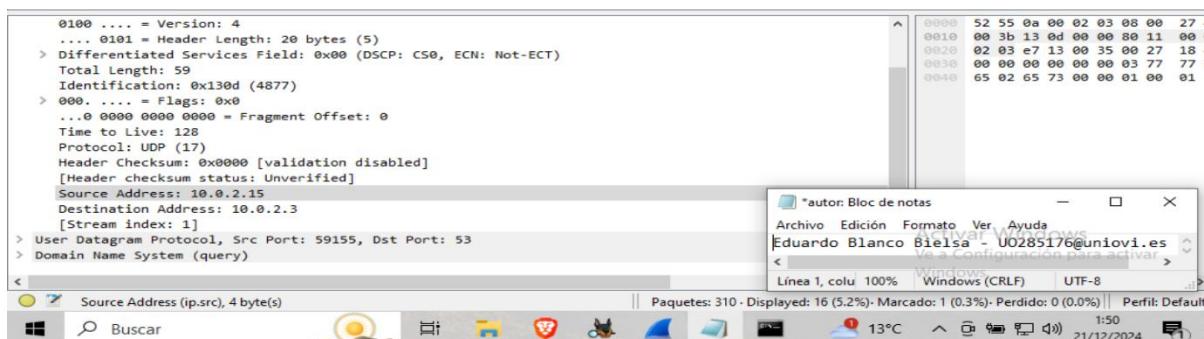


Ilustración 102. Resolución Práctica 5b - Ej 3 - Apartado j - Parte 3

## Conclusiones

Se han identificado ambas direcciones en Internet Protocol Version y se han reflejado en el informe.

## Práctica 5b – Ejercicio 3 – Apartado k

### Enunciado

El paquete IP y el encabezado encapsulan el segmento de UDP. El segmento de UDP contiene la consulta de DNS como datos. Haga clic en la flecha contigua a User Datagram Protocol para ver los detalles. Observa que solo hay cuatro campos. El número del puerto de origen en este ejemplo es 39303. La MV generó de manera aleatoria el puerto de origen utilizando números de puerto que no están reservados. El puerto de destino es 53. El puerto 53 es un puerto conocido reservado para el uso con DNS. Los servidores DNS esperan en el puerto 53 las consultas de DNS de los clientes.

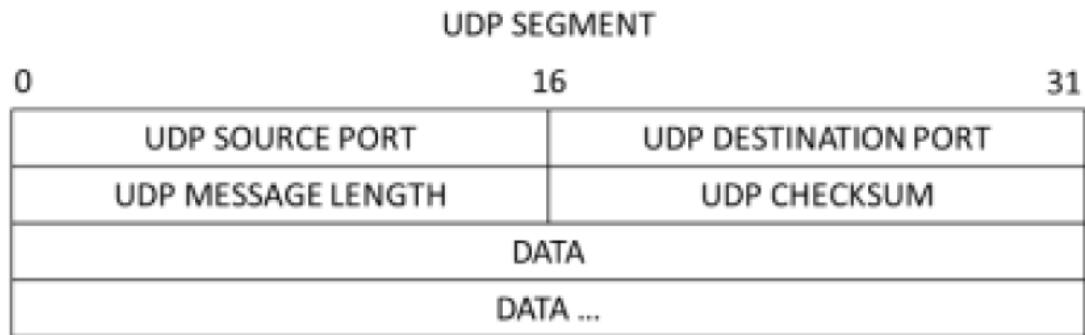


Ilustración 103. Enunciado Práctica 5b - Ej 3 - Apartado k - Parte 1

```

▶ Frame 19: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_a2:5f:ea (08:00:27:a2:5f:ea), Dst: Sercomm_bc:e0:2a (e0:60:66:bc:e0:2a)
▶ Internet Protocol Version 4, Src: 192.168.22.25, Dst: 192.168.22.1
▼ User Datagram Protocol, Src Port: 39303, Dst Port: 53
  Source Port: 39303
  Destination Port: 53
  Length: 51
  Checksum: 0xadaf [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
▶ Domain Name System (query)

```

Ilustración 104. Enunciado Práctica 5b - Ej 3 - Apartado k - Parte 2

En este ejemplo, la longitud del segmento de UDP es de 51 bytes. La longitud del segmento UDP de su ejemplo puede ser diferente. De los 51 bytes, 8 bytes se utilizan como encabezado. Los datos de la consulta de DNS utilizan los otros 43 bytes. Los 43 bytes de los datos de consulta DNS están el panel de bytes del paquete (sección inferior) de la ventana principal de Wireshark.

```

▶ User Datagram Protocol, Src Port: 39303, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x8e27
  Flags: 0x0100 Standard query
    0... .... .... = Response: Message is a query
    .000 0... .... = Opcode: Standard query (0)
    .... 0. .... .... = Truncated: Message is not truncated
    .... .1 .... .... = Recursion desired: Do query recursively
    .... .... 0... .... = Z: reserved (0)
    .... .... .... 0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  ▶ Queries
  ▶ Additional records
  [Response In: 20]

```

Ilustración 105. Enunciado Práctica 5b - Ej 3 - Apartado k - Parte 3

En este ejemplo, la dirección de destino es la del servidor DNS.

## Resultados obtenidos

En mi caso se corresponde con lo siguiente:

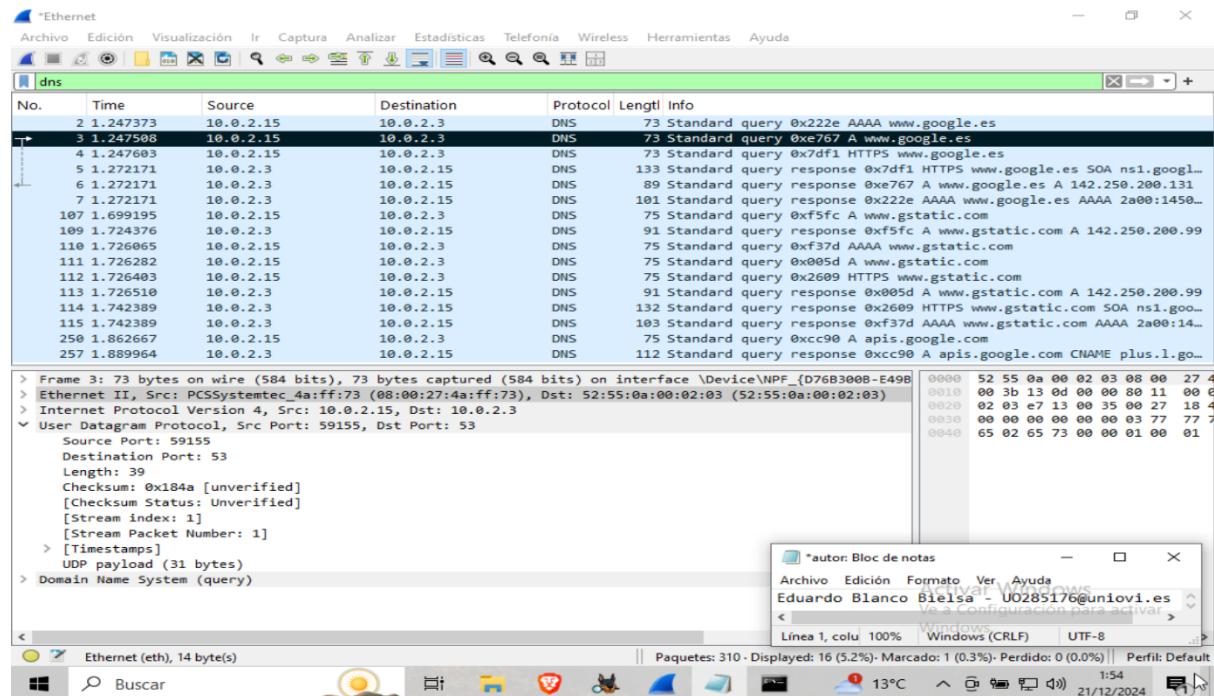


Ilustración 106. Resolución Práctica 5b - Ej 3 - Apartado k

## Conclusiones

Se ha visto el User Datagram Protocol y se ha reflejado en el informe.

## Práctica 5b – Ejercicio 3 – Apartado l

### Enunciado

Haz clic en la flecha que se encuentra a la izquierda de los Flags. Un valor de 1 significa que el flag está definido. Localice el flag que está definido en este paquete.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 104 de 109

## Resultados obtenidos

Está definido el flag de "Recursion desired":

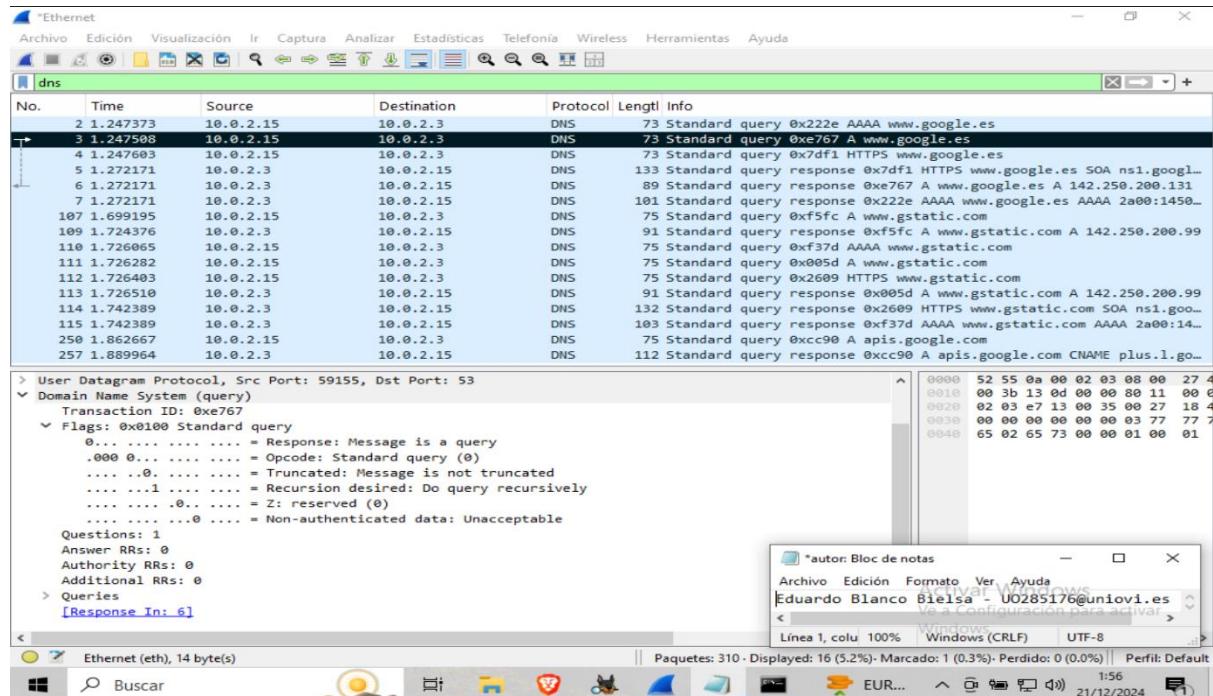


Ilustración 107. Resolución Práctica 5b - Ej 3 - Apartado l

## Conclusiones

Se ha reflejado el flag que está definido en el informe.

## Práctica 5b – Ejercicio 3 – Apartado m

### Enunciado

El checksum es usado para determinar la integridad del encabezado de UDP después de haber atravesado Internet. El encabezado de UDP tiene poca sobrecarga porque UDP no tiene campos que estén asociados con el protocolo de enlace de tres vías en TCP. Cualquier problema de confiabilidad de la transferencia de datos que ocurra debe ser manejado por la capa de aplicación. Expanda lo necesario para ver los detalles. Registre sus resultados de Wireshark en la tabla siguiente.

## Resultados obtenidos

Descripción	Resultado Wireshark
Tamaño de la trama	39
MAC origen	08:00:27:4a:ff:73
MAC destino	52:55:0a:00:02:03
IP origen	10.0.2.15
IP destino	10.0.2.3
Puerto origen	59155
Puerto destino	53

Tabla 6. Resolución Práctica 5b - Ej 3 - Apartado m - Parte 1

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 105 de 109

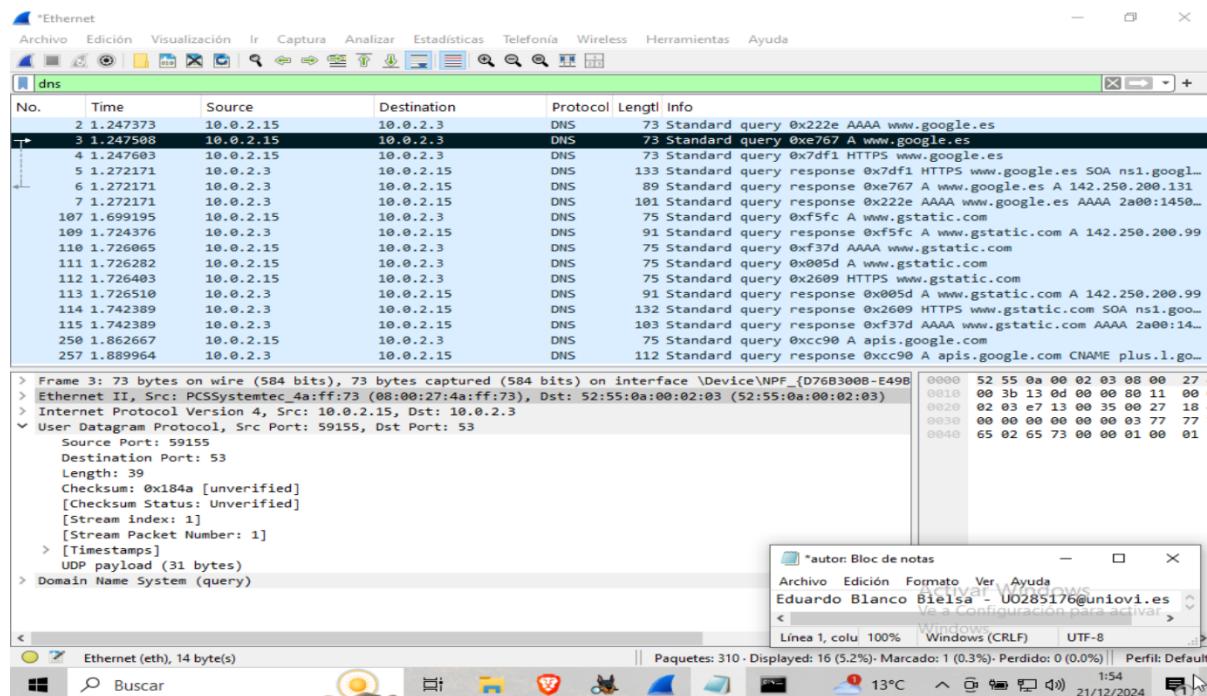


Ilustración 108. Resolución Práctica 5b - Ejercicio 3 - Apartado m - Parte 2

## Conclusiones

Se han llenado los datos requeridos en el informe.

## Práctica 5b – Ejercicio 3 – Apartado n

### Enunciado

¿Es la dirección IP de origen la misma que la dirección IP de la MV que registró en la parte 1?

### Resultados obtenidos

Sí, ambas direcciones son la 10.0.2.15 (mirar captura del apartado anterior para contrastar).

### Conclusiones

Se ha determinado que son la misma ip y se ha reflejado en el informe.

## Práctica 5b – Ejercicio 3 – Apartado o

### Enunciado

¿Es la dirección IP de destino la misma que la puerta de enlace predeterminada (gateway) que observó en la parte 1?

### Resultados obtenidos

Sí, ambas direcciones son la 10.0.2.3 (mirar captura del apartado m para contrastar).

### Conclusiones

Se ha determinado que son la misma ip y se ha reflejado en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 106 de 109

## Práctica 5b – Ejercicio 3 – Apartado p

### Enunciado

En la trama Ethernet II para la respuesta de DNS, ¿qué dispositivo es la dirección MAC de origen y qué dispositivo es la dirección MAC de destino?

### Resultados obtenidos

En mi caso, la MAC de origen es **52:55:0a:00:02:03** (de la puerta de enlace) y la MAC destino es **08:00:27:4a:ff:73** (de mi máquina Windows).

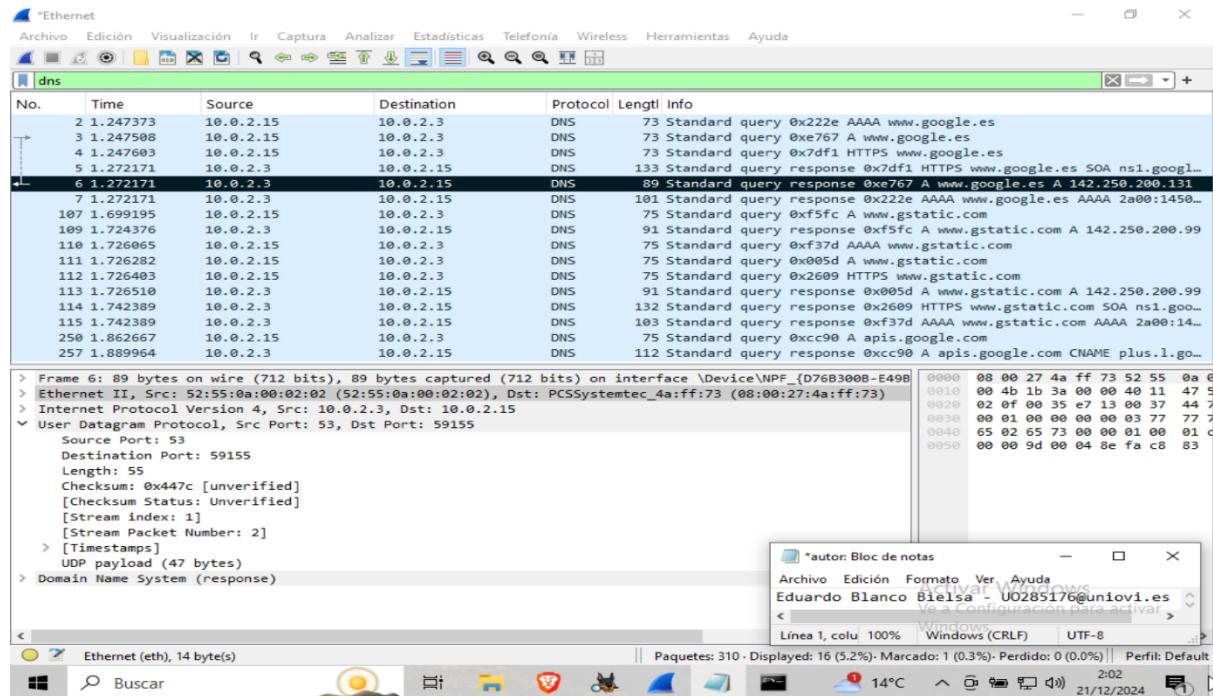


Ilustración 109. Resolución Práctica 5b - Ej 3 - Apartado p

### Conclusiones

Se han reflejado ambas direcciones en el informe.

## Práctica 5b – Ejercicio 3 – Apartado q

### Enunciado

Observe las direcciones IP de origen y destino en este paquete IP. ¿Cuál es la dirección IP de destino? ¿Cuál es la dirección IP de origen? ¿Qué sucedió con los roles de origen y destino correspondientes a la VM y al gateway predeterminado?

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 107 de 109

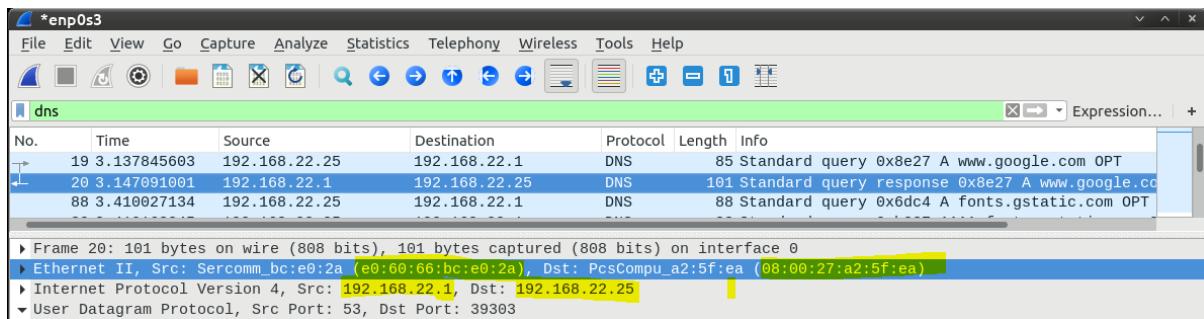


Ilustración 110. Enunciado Práctica 5b - Ej 3 - Apartado q

## Resultados obtenidos

En ese paquete, la dirección IP de destino es la 192.168.22.25 y la dirección IP de origen es la 192.168.22.1. En resumen, la dirección IP de origen (192.168.22.1) parece corresponder al **gateway predeterminado**, mientras que la dirección IP de destino (192.168.22.25) parece corresponder a un dispositivo (probablemente una **VM**) dentro de la misma red. Esto indica que el paquete está siendo enviado desde el gateway hacia la VM o dispositivo de destino.

## Conclusiones

Se han reflejado las respuestas a ambas preguntas en el informe.

## Práctica 5b – Ejercicio 3 – Apartado r

### Enunciado

En el segmento UDP, el rol de los números de puerto también se invirtió. El número del puerto de destino es 39303. El número de puerto 39303 es el mismo puerto que generó la MV cuando se envió la consulta DNS al servidor DNS. La MV espera una respuesta DNS en este puerto. El número del puerto de origen es 53. El servidor DNS espera una consulta de DNS en el puerto 53 y luego envía una respuesta de DNS con un número de puerto de origen 53 al originador de la consulta de DNS. Al expandirse la respuesta de DNS, observa las direcciones IP resueltas para [www.google.com](http://www.google.com) en la sección Answers (Respuestas) y captura la pantalla resaltando dicha información.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 108 de 109

## Resultados obtenidos

Vemos que hay una respuesta de 142.250.200.131:

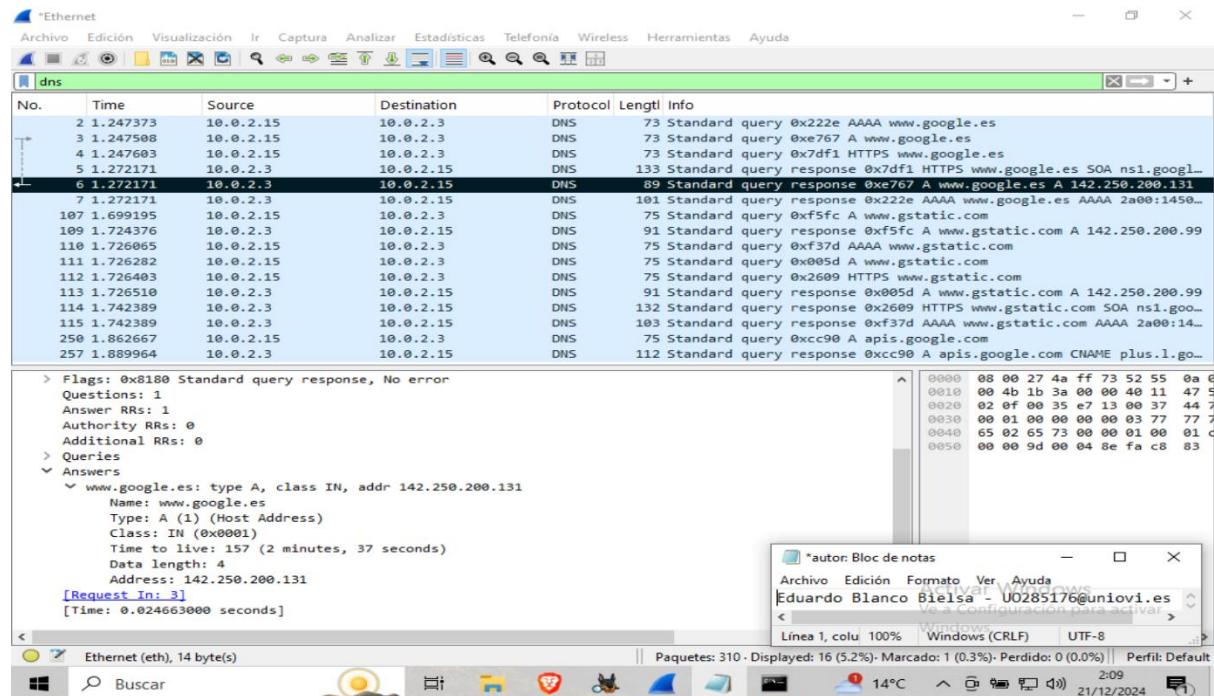


Ilustración 111. Resolución Práctica 5b - Ej 3 - Apartado r

## Conclusiones

Se ha reflejado la dirección del servidor de google en el informe.

Autor:	Eduardo Blanco Bielsa	© 2024
Escuela de Ingeniería Informática	Universidad de Oviedo	Versión: 2024.ES.003
Informática Forense y Auditoría, Laboratorio 4, Convocatoria Ordinaria (diciembre)		Hoja 109 de 109