

Prácticas de Laboratorio

Informática Forense y Auditoría

Hugo Fonseca Díaz

UO258318

uo258318@uniovi.es

Convocatoria Junio-Julio 2021.



Universidad de Oviedo

Universidá d'Uviéu

University of Oviedo

Escuela de Ingeniería Informática

Universidad de Oviedo

España

28 de junio de 2021

Índice

| | |
|-----------------------------|-----------|
| 1. Introducción | 2 |
| 2. Práctica 02 | 3 |
| 2.1. Ejercicio 27 | 3 |
| 2.2. Ejercicio 31 | 5 |
| 3. Práctica 03 | 12 |
| 4. Práctica 04 | 12 |
| 5. Práctica 05 | 12 |

1. Introducción

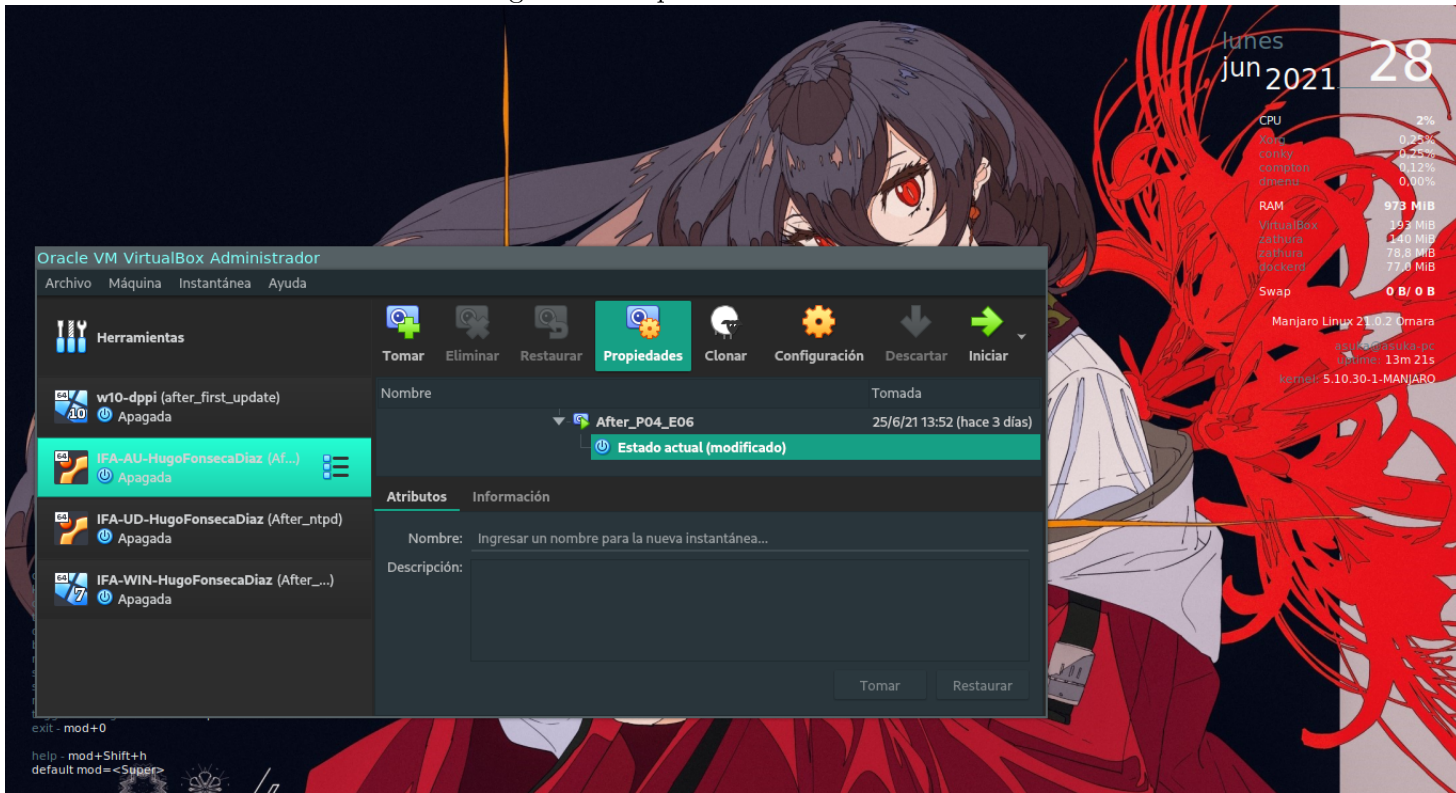
Los ejercicios de este documento se han realizado en una máquina cuyas características se muestran en la siguiente captura.

Figura 1: Sistema del alumno Hugo Fonseca Díaz.



Las máquinas virtuales utilizadas pueden verse en la siguiente imagen.

Figura 2: Máquinas virtuales.

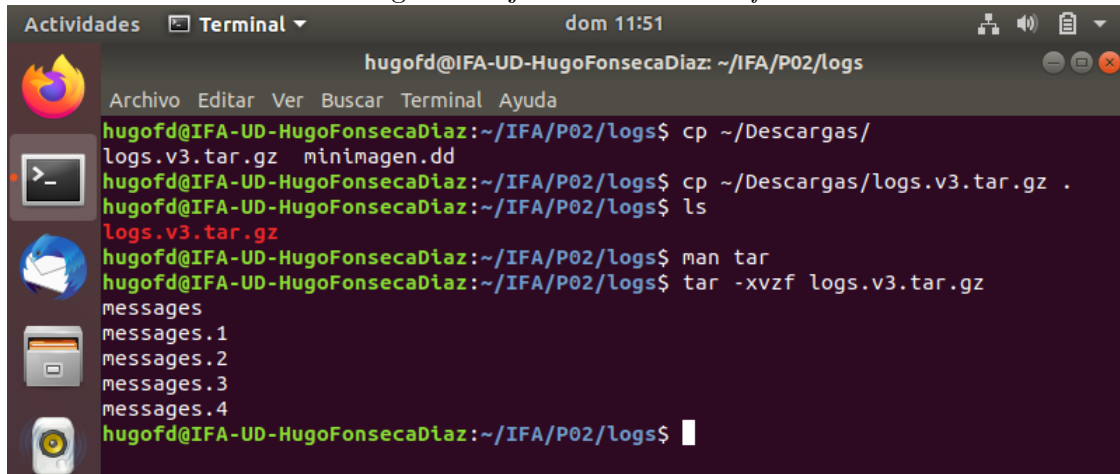


2. Práctica 02

2.1. Ejercicio 27

Se descomprime el archivo con el comando `tar` y las flags `xvzf`, siendo x una indicación de que se quiere extraer los contenidos del archivo comprimido, v para que lo haga de manera verbosa, z para indicarle al comando que el archivo es un zip y f para pasarle el fichero que se desea extraer al comando.

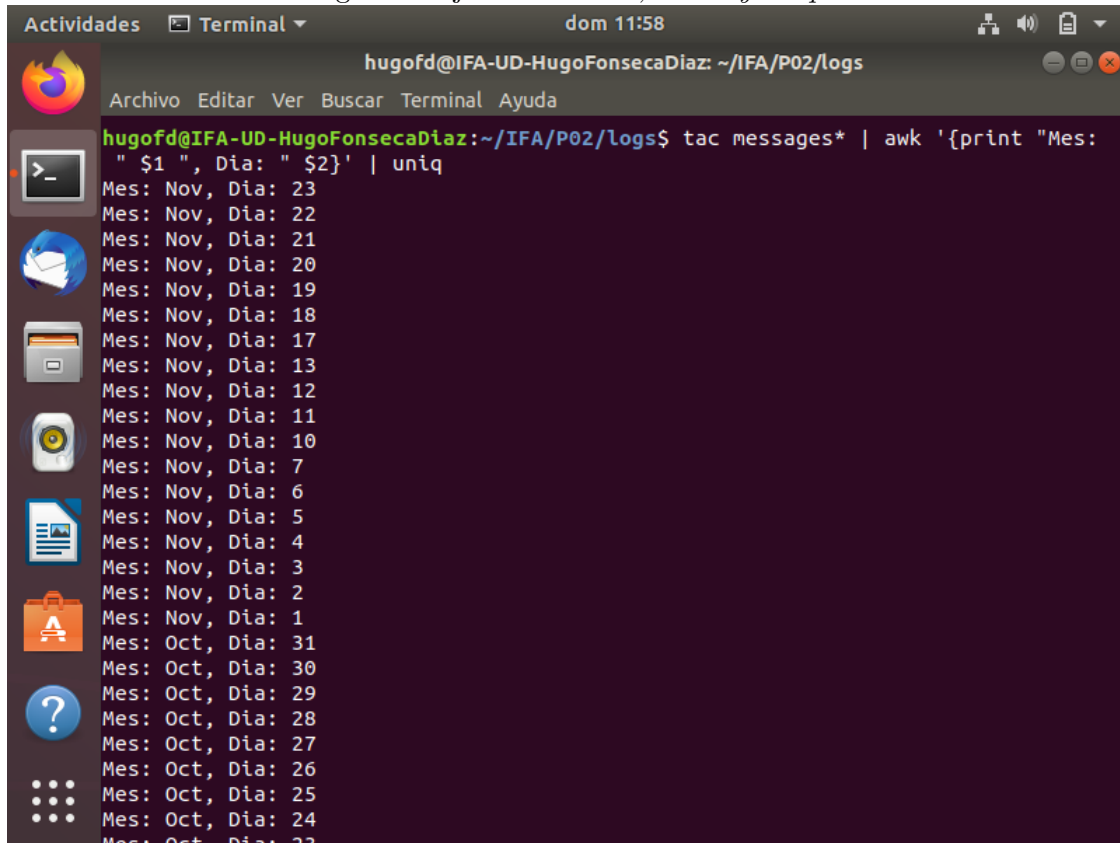
Figura 3: Ejercicio 27: *tar -xvzf*.



```
hugofd@IFA-UD-HugoFonsecaDiaz: ~/IFA/P02/logs
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ cp ~/Descargas/
logs.v3.tar.gz minimagen.dd
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ cp ~/Descargas/logs.v3.tar.gz .
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ ls
logs.v3.tar.gz
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ man tar
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ tar -xvzf logs.v3.tar.gz
messages
messages.1
messages.2
messages.3
messages.4
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$
```

Una vez descomprimidos los ficheros de texto, se procede a utilizar tres nuevas herramientas. Se usa `tac` para concatenar ficheros de forma inversa (es el comando `cat` invertido), el lenguaje de programación AWK para procesar texto y el comando `uniq` para omitir líneas repetidas.

Figura 4: Ejercicio 27: *tac*, *AWK* y *uniq*.



The screenshot shows a terminal window titled "hugofd@IFA-UD-HugoFonsecaDiaz: ~/IFA/P02/logs". The command executed is `tac messages* | awk '{print "Mes: " $1 " ", Dia: " $2}' | uniq`. The output lists dates from November 23 down to October 23, with each line formatted as "Mes: Nov, Dia: 23".

```
hugofd@IFA-UD-HugoFonsecaDiaz: ~/IFA/P02/logs
hugofd@IFA-UD-HugoFonsecaDiaz:~/IFA/P02/logs$ tac messages* | awk '{print "Mes:
" $1 " ", Dia: " $2}' | uniq
Mes: Nov, Dia: 23
Mes: Nov, Dia: 22
Mes: Nov, Dia: 21
Mes: Nov, Dia: 20
Mes: Nov, Dia: 19
Mes: Nov, Dia: 18
Mes: Nov, Dia: 17
Mes: Nov, Dia: 13
Mes: Nov, Dia: 12
Mes: Nov, Dia: 11
Mes: Nov, Dia: 10
Mes: Nov, Dia: 7
Mes: Nov, Dia: 6
Mes: Nov, Dia: 5
Mes: Nov, Dia: 4
Mes: Nov, Dia: 3
Mes: Nov, Dia: 2
Mes: Nov, Dia: 1
Mes: Oct, Dia: 31
Mes: Oct, Dia: 30
Mes: Oct, Dia: 29
Mes: Oct, Dia: 28
Mes: Oct, Dia: 27
Mes: Oct, Dia: 26
Mes: Oct, Dia: 25
Mes: Oct, Dia: 24
Mes: Oct, Dia: 23
```

2.2. Ejercicio 31

Se crea el caso en Autopsy con los datos solicitados.

Figura 5: Ejercicio 31: Creación del caso

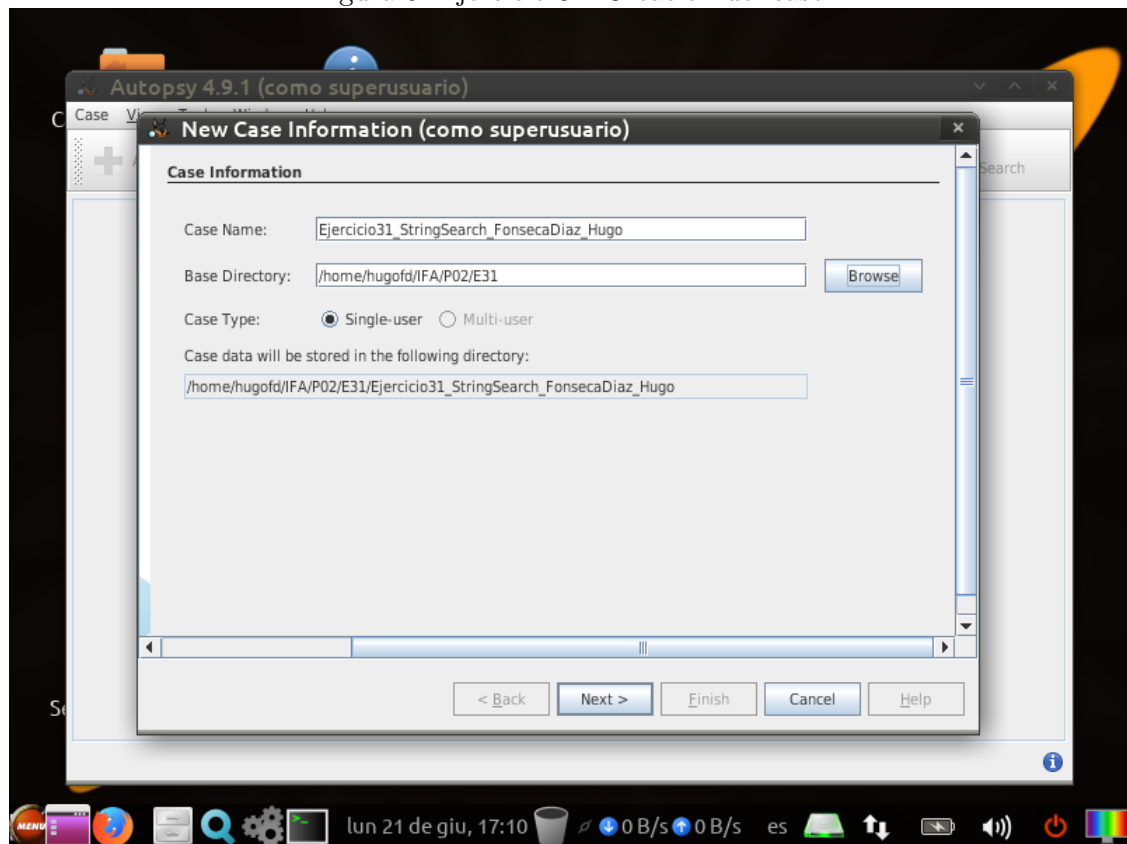
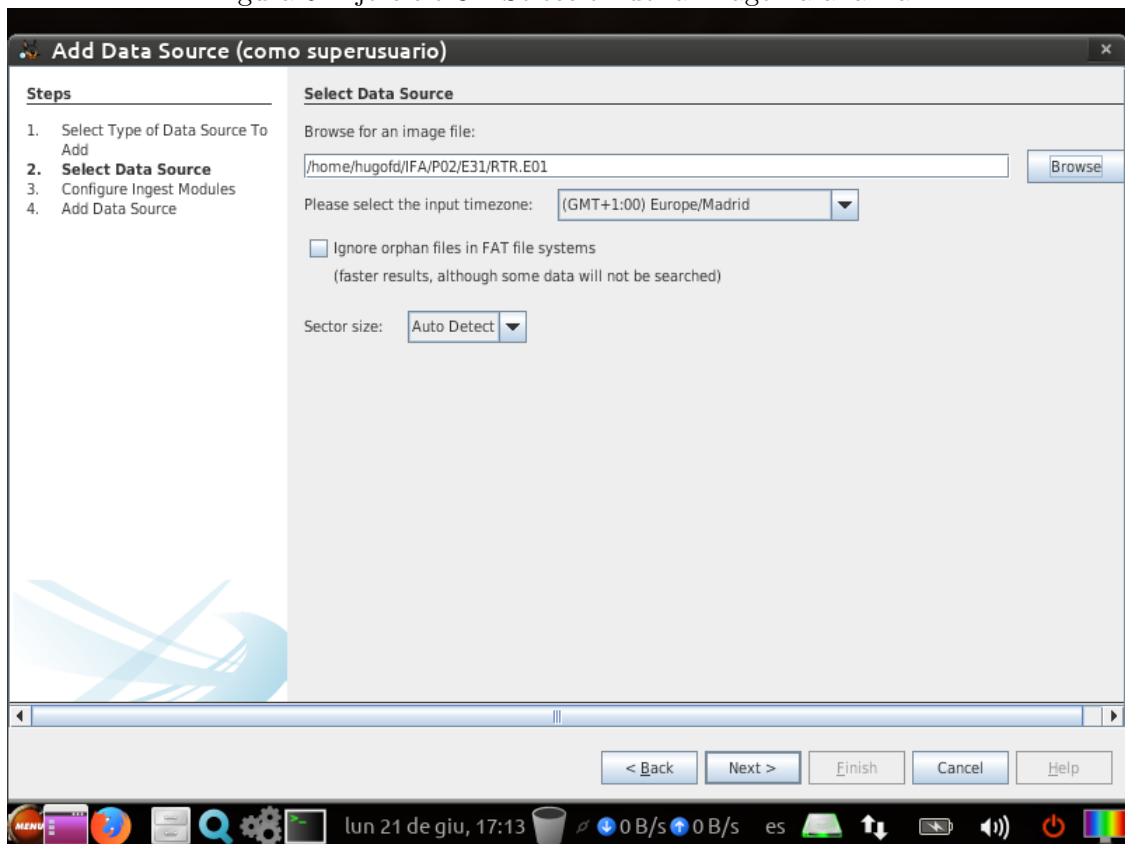


Figura 6: Ejercicio 31: Selección de la imagen a analizar



Se seleccionan los módulos y se configura el módulo de búsqueda de palabras clave.

Figura 7: Ejercicio 31: Palabras clave

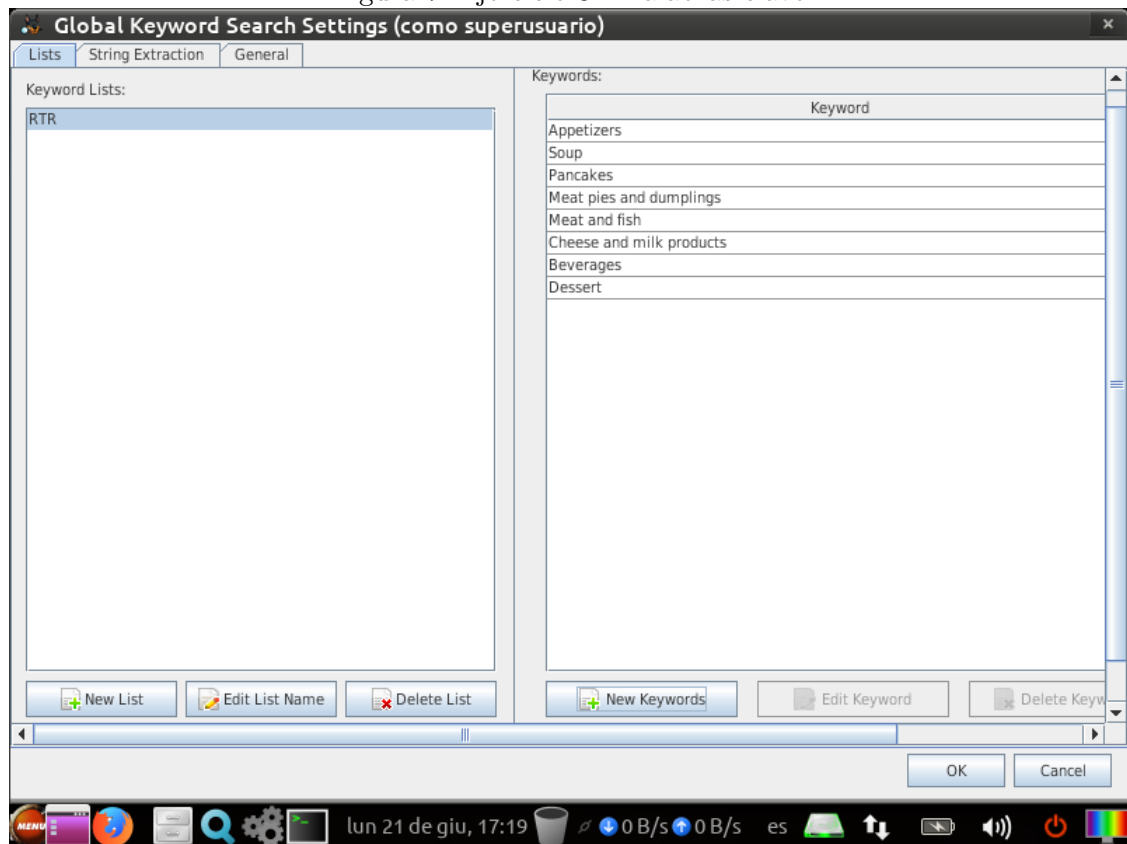


Figura 8: Ejercicio 31: Módulos seleccionados

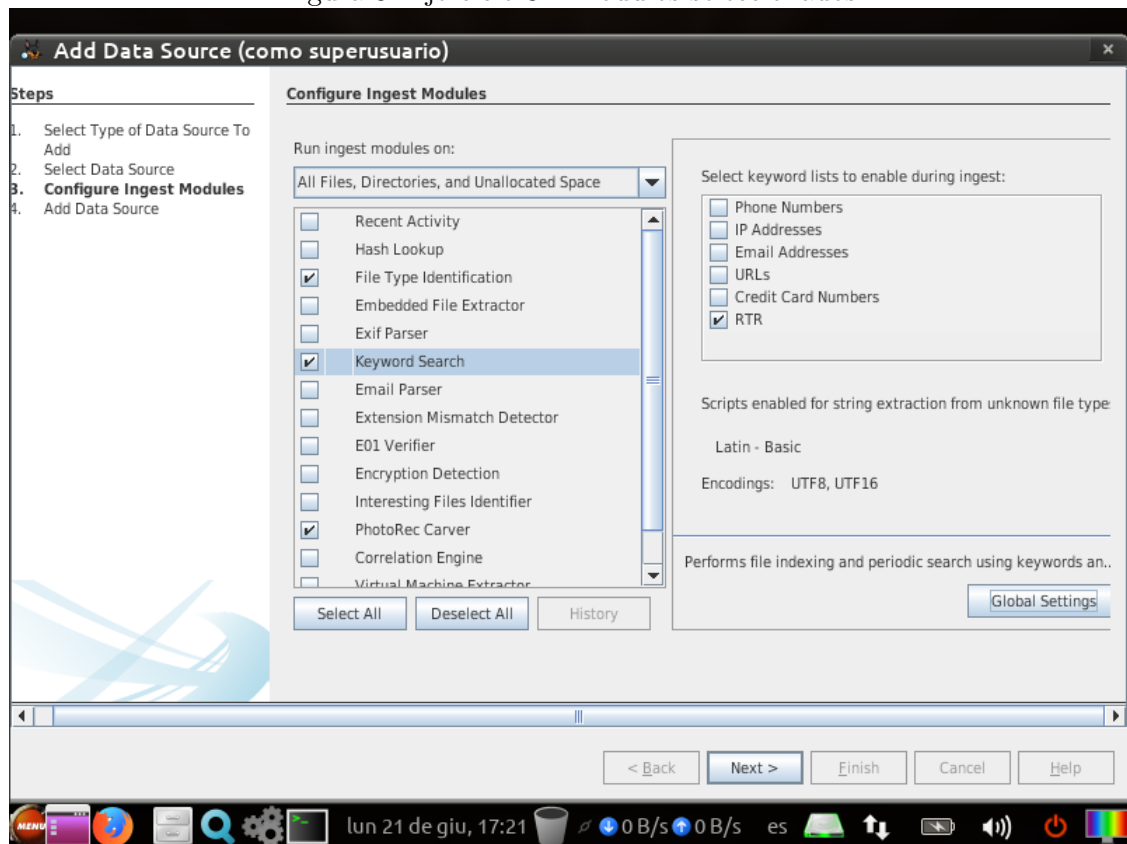
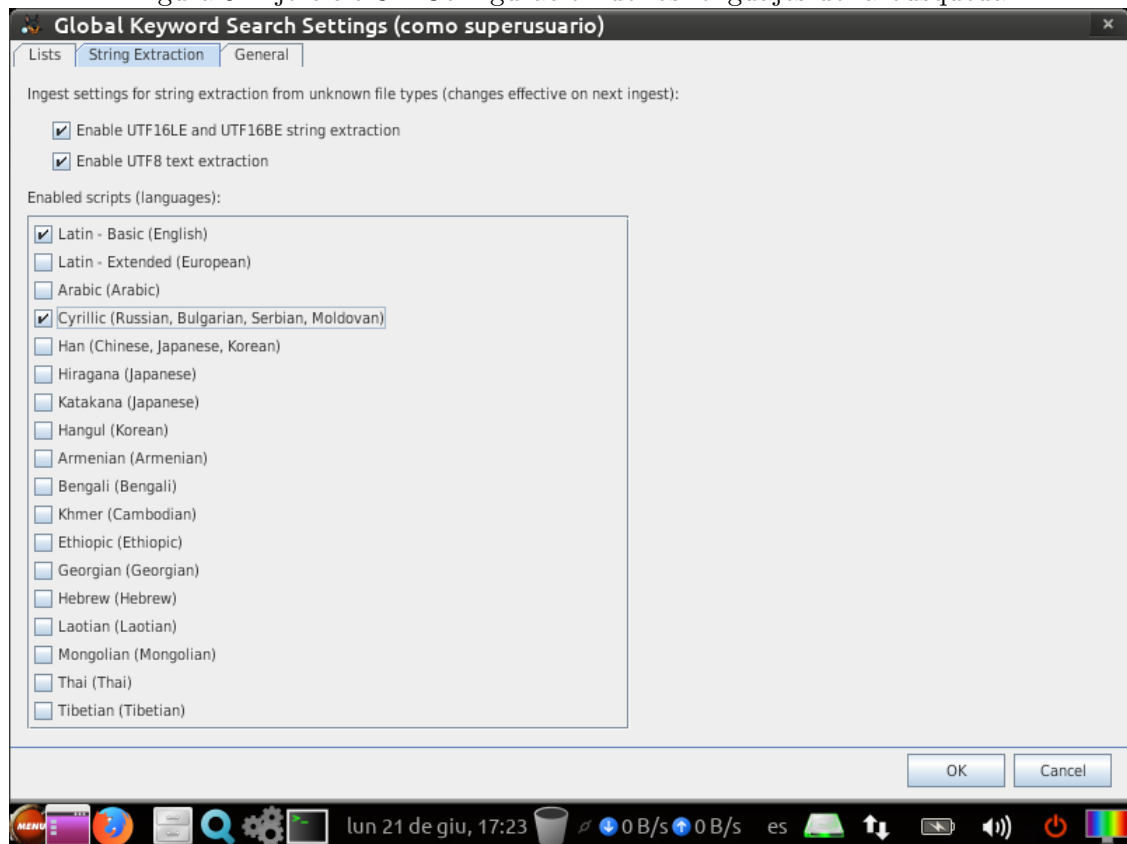
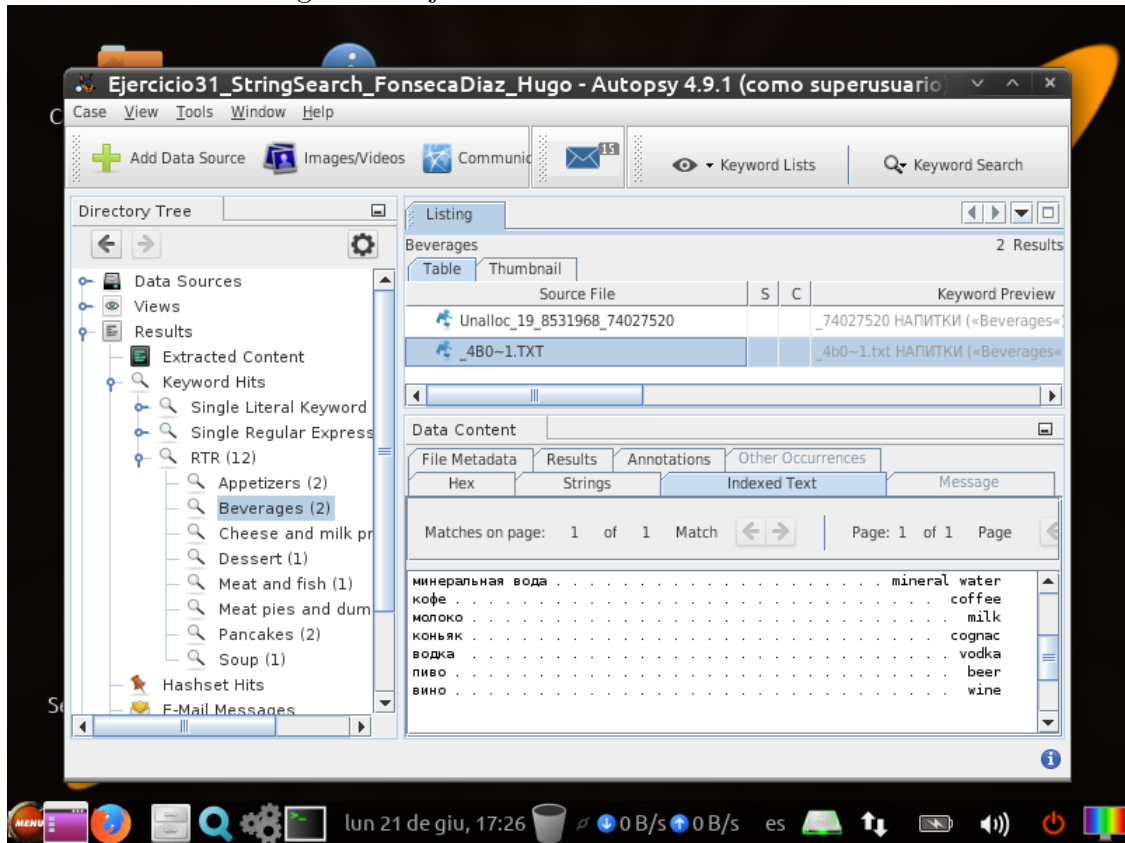


Figura 9: Ejercicio 31: Configuración de los lenguajes de la búsqueda



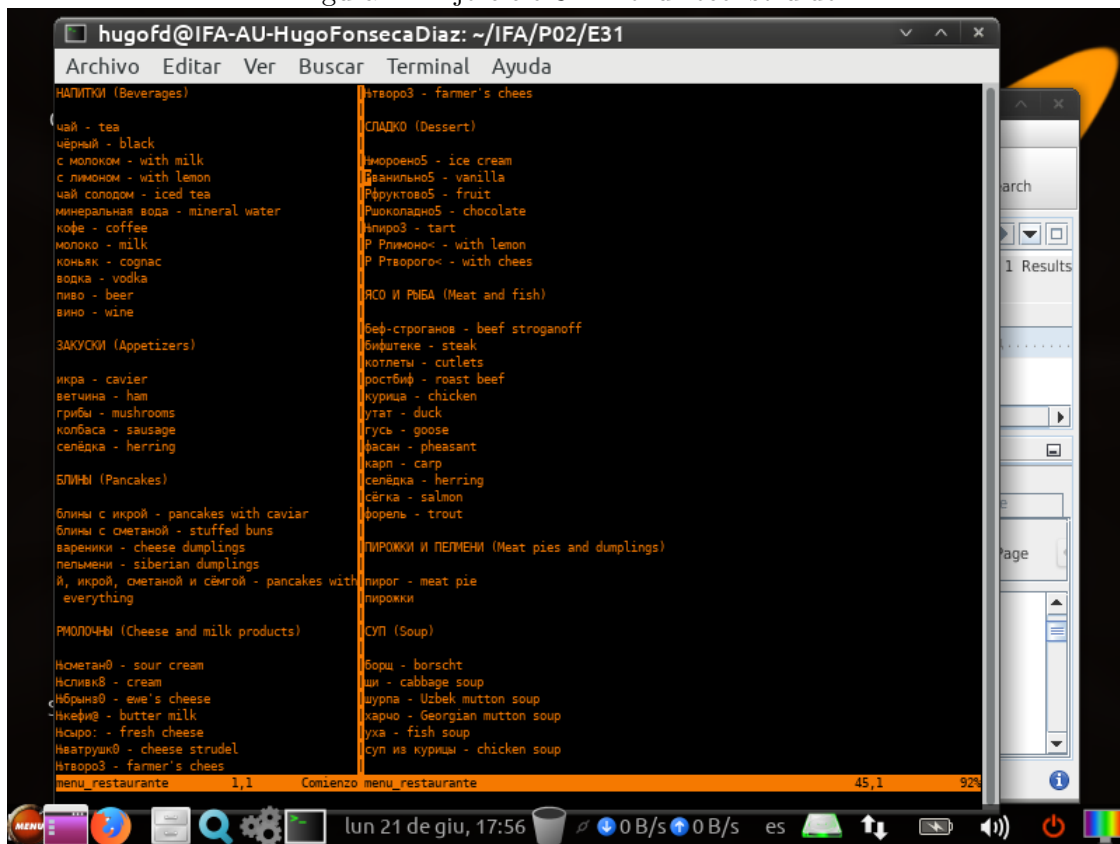
Una vez finalizado el análisis, se pueden observar los ficheros encontrados.

Figura 10: Ejercicio 31: Resultados del análisis



Se reconstruye el menú del restaurante, creado inicialmente el 3 de noviembre de 2004.

Figura 11: Ejercicio 31: Menú reconstruido



3. Práctica 03

4. Práctica 04

5. Práctica 05