PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE INGENIERÍA
INF239 SISTEMAS OPERATIVOS

LABORATORIO 5

TEMA: SISTEMA DE ARCHIVOS FAT

Material Proporcionado:

1) *Carrier – File System Forensic Analysis – Chapter 9 FAT Concepts and Analysis.pdf*
2) Carrier – File System Forensic Analysis – Chapter 10 FAT Data Structures.pdf
3) *Material para el laboratorio 5 de Sistemas Operativos.pdf* (este archivo)
4) *visorFAT.py.zip* (conteniendo el programa escrito en Python)
5) Imagen – Carpeta conteniendo la imagen de un sistema de archivos con FAT16 (el archivo comprimido está dividido en tres parte, lea el *Readme.txt* para obtener el *zip*)

A) Preparar imagen de sistema de archivos FAT16

El siguiente procedimiento permitirá obtener un archivo con la imagen de un sistema de archivo FAT16 y a continuación montarlo sobre */media/$USER/<ID>*

Se necesita tener instalado el paquete *udisks2*, en las computadoras de los laboratorios ya se encuentra instalado.

A continuación preparamos un archivo con sistema de archivo FAT16, desde una terminal escriba:

```
dd if=/dev/zero of=./FAT16D1.img bs=1024 count=32768

mkfs.vfat FAT16D1.img
```

Ahora procedemos a montarlo, debe conocer la ruta absoluta del archivo imagen. Asumamos que se encuentra en */home/alulab/Documentos*, entonces

```
udisksctl loop-setup -f /home/alulab/Documentos/FAT16D1.img
```

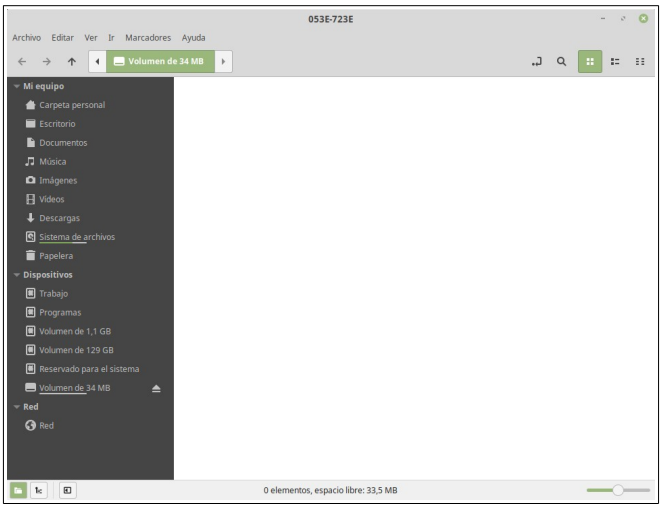
Como respuesta deberá aparecer en la terminal los siguiente:

```
Mapped file /home/alulab/Documentos/FAT16D1.img as /dev/loop0.
```

El sistema crea un directorio con nombre igual a algo como 053E-723E (el nombre puede variar) en */media/alulab/* (asumiendo que el usuario es *alulab*) y monta sobre este directorio la imagen del disco. El directorio creado tiene como propietario al que ejecutó el comando (*alulab* en este caso), de forma que puede copiar y borrar archivos en esta imagen. Puede ver su contenido de forma acostumbrada:

```
ls -l /media/alulab/053E-723E
```

También se abrirá (en Linux Mint 19) una ventana del navegador de archivos (Nemo) mostrando el directorio donde se ha montado la imagen.



En adelante cuando ingrese a este directorio, estará accediendo a este disco virtual. Cuando ya no se desee acceder más a esta imagen se debe desmontarlo para que los cambios tomen efecto.

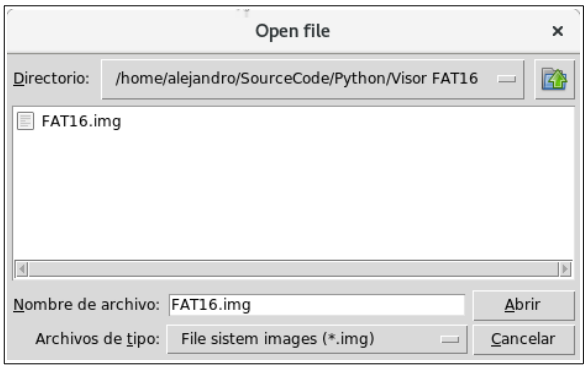
```
udisksctl unmount -b /dev/loop0
```

La idea de enseñarle este procedimiento, es que usted pueda crear y modificar su propia imagen, muy aparte de la que se le proporciona como modelo. De esta forma podrá experimentar con diferentes formatos de FAT. Inclusive, durante el laboratorio, esta parte no se necesitará.

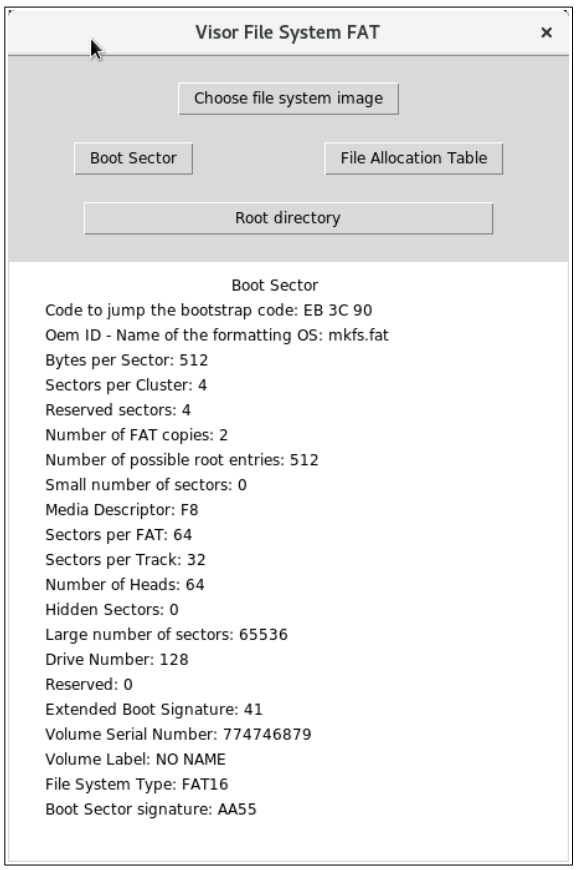
B) El programa

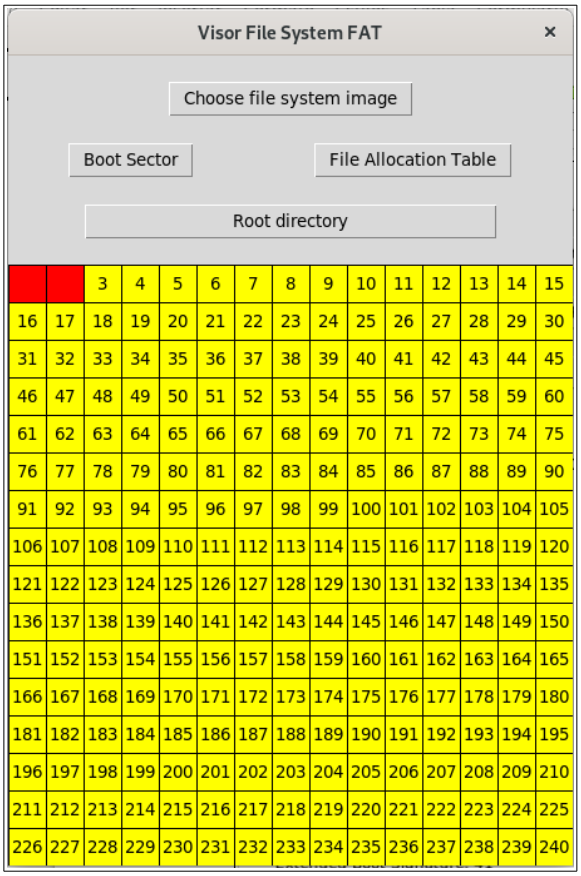
El programa *visorFAT.py* es una pequeña aplicación cuyo objetivo es mostrar, de forma gráfica e interpretada, el contenido de la estructura de un sistema de archivo FAT.

El primer paso será elegir el archivo que contiene la imagen de un sistema de archivo con FAT16.



A partir de ahí, la aplicación podrá mostrar la información del *Boot Sector* o de la FAT.





		3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160	161	162	163	164	165
166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195
196	197	198	199	200	201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
226	227	228	229	230	231	232	233	234	235	236	237	238	239	240

Hay varias cosas que están inconclusas o mejoras que se pueden agregar. Su tarea será completar según las indicaciones que se dan abajo:

TAREA

1) Modifique el programa para que cuando se elija el archivo se verifique que realmente contenga un sistema de archivos FAT (12,16 o 32). En caso contrario enviar un mensaje y proceder como si no se hubiera elegido archivo alguno.

2) En el módulo que muestra la información correspondiente a la FAT el puntero se ha desplazado 2048 bytes. Esto funciona solo para la imagen proporcionada como ejemplo. Modifíquelo para que funcione para cualquier imagen que contenga FAT.

3) Complete el módulo que muestra la FAT, en principio este lee 240 entradas. Modifíquelo para que lea todas las entradas de la FAT. Investigue en Tkinter como crear *scrollbar* para mostrar todas las entradas de la FAT, a medida que se va arrastrando la barra vertical.

4) Complete el módulo que muestra el directorio raíz. Presente los datos más relevantes de cada entrada: nombre, tamaño de archivo y primer *cluster*.

5) Al módulo que muestra el directorio raíz agregue la siguiente funcionalidad: cuando se haga clic sobre el primer *cluster*, se debe mostrar la FAT pintando con otro color la cadena de *clusters* que corresponden al archivo sobre el que se ha hecho clic.

Nota: Para verificar que su programa esté haciendo lo correcto deberá conocer bien las estructuras del sistema de archivos FAT. De igual forma se le recomienda variar las opciones de formato del sistema de archivo (parte A) cambiando, por ejemplo, el tamaño del *cluster* (`man mkfs.vfat`). Luego con uso de algún editor hexadecimal puede verificar directamente si la información, presentada en el visor por su modificaciones, es la correcta.

Importante: Una vez creado el sistema de archivos, modifique su contenido copiando y borrando archivos sobre la imagen. Para luego ver en el visor los cambios llevados a cabo por el *virtual file system* de Linux. Recuerde que antes de usar el visor debe desmontar la imagen del sistema de archivos de esta forma los cambios se podrán notar en el visor.

Prof. Alejandro T. Bello Ruiz