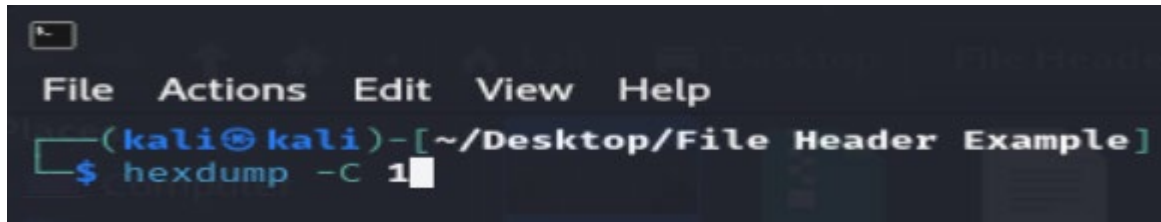


File Header Example

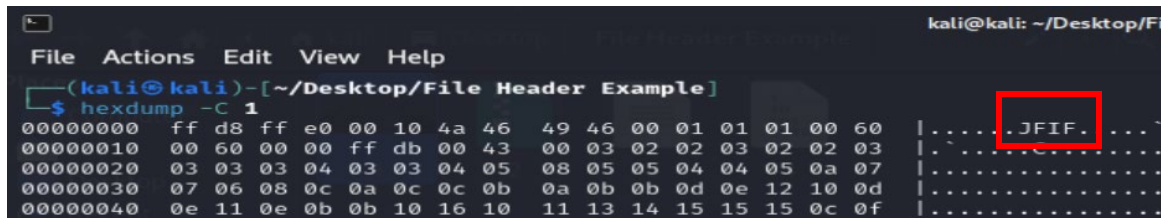
For this example, we will be using the Hexdump tool in Kali to view file headers. To use the tool, download the Wk3 In Class Demo from Google Drive, extract the contents onto your Kali Desktop, right click and select “Open Terminal Here”, and input the following command:

Hexdump (so Kali knows which tool to run) -C (Conical – displays output in hex and text) *filename* (which file do you want hexdump to output?).

Here is an example of the command:

A terminal window with a dark background. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~/Desktop/File Header Example]'. The command '\$ hexdump -C 1' has been entered and is highlighted with a blue cursor.

The file header will be the first few bytes of the file so you will need to scroll back up to the top to see it as in the example below:

A terminal window showing the output of the hexdump command. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~/Desktop/File Header Example]'. The command '\$ hexdump -C 1' has been entered. The output shows hex values and their corresponding ASCII characters. The first line of output is '00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 |.....JFIF.....'. The word 'JFIF' is highlighted with a red box.

Here is a cross reference of a few common file headers.

Header	Type
ÿØÿà or JFIF	Picture
PK	Document or Zip
AVI	Audio
ftypMSNV	Video

Once you know what type of file it is, answer the question in the poll, and repeat the steps for the next example.