|  |
| --- |
|  |

**Helpful Task Tips & Hints!**

* Please note that the relevant traffic is all in http.
* When investigating packet capture files, you can filter the traffic using search terms to isolate certain types of traffic, for example using “http” in the search box, will only display http traffic.
* Once downloaded items have been identified, you will need to investigate them, and rebuild them forensically using a hex viewer.
* In order to rebuild the file you will need to carve out just that file’s hex data, and delete any other hex data surrounding it.

An essential part of solving some of these tasks is identifying what sort of file was downloaded by identifying its *file signature.* A file signature is some data at the start of a file that identifies what sort of file it is. These are usually viewed in hex form.

For example you can identify a jpeg image by its file signature. A jpeg will always start with the hex data “FFD8” and normally ends with the hex data “FFD9”.

Other files can be identified in the same way, with their own unique file signatures.

*Please note that some of the downloads made by the user contain more than just the files mentioned in the task template.*