a) What is the difference between Internal Storage & External Storage?

Internal Storage :

When building an app that uses the internal storage, the Android OS creates a unique folder, which will only be accessible from the app, so no other app, or even the user, can see what's in the folder.

The internal storage should only be used for application data, (preferences files and settings, sound or image media for the app to work).

External Storage:

The external storage is more like a public storage, so for now, it's the sdcard, but could become any other type of storage (remote hard drive, or anything else).

If it is intended to download many mp3s, it is reccomended saving them to external storage, as the external storage is often bigger.

b) For how long the data resides in the cache?

The best cache size is application specific and depends on the size and frequency of the files being downloaded. Increasing the limit may improve the hit rate, but it may also just waste filesystem space!

For some applications it may be preferable to create the cache in the external storage directory. There are no access controls on the external storage directory so it should not be used for caches that could contain private data. Although it often has more free space, external storage is optional and—even if available—can disappear during use. Retrieve the external cache directory using getExternalCacheDir(). If this method returns null, your application should fall back to either not caching or caching on non-external storage. If the external storage is removed during use, the cache hit rate will drop to zero and ongoing cache reads will fail.

c) What are the critical Permissions and Normal Permissions? What are the

examples of each?

Normal Permission :

Many permissions are designated as PROTECTION\_NORMAL, which indicates that there's no great risk to the user's privacy or security in letting apps have those permissions. For example, users would reasonably want to know whether an app can read their contact information, so users have to grant this permission explicitly. By contrast, there's no great risk in allowing an app to vibrate the device, so that permission is designated as normal. , e.g., ->ACCESS\_LOCATION\_EXTRA\_COMMANDS

>ACCESS\_NETWORK\_STATE

Critical Permission :

When requesting for critical but unclear permissions, use of warm welcome screen is helpful to understand that a permission is requested. For critical permissions, such as a camera app that needs camera permission, ask up-front for it. Secondary features can be requested later in context, such as a geotagging app when asking for a location permission. For permissions that are secondary and unclear, you should include a rationale explanation if you really need them.