NTFS/FAT Time Zone Comparison

On a FAT volume the time is stored based on the local machine's time. When processing a FAT volume FTK will prompt the user to select a time zone so that everything can then be converted from the local machine's time to Greenwich Mean Time (UTC). For the case, the time is actually being stored in the database as GMT/UTC and the calculation is based on the time zone the user selected at Pre-processing. FTK will then automatically calculate the time difference between GMT/UTC and the local examination machine's time. Everything will be displayed based on the local examination machine's time zone.

If you want to look at the times based on the evidence time zone you will need to either calculate the time difference between the local machine's time and the evidence time zone, or simply change the time zone on the examination machine to match the evidence time zone.

If you have FTK 1.61 or above you do not need to change the time zone of the examination machine, the time zone of the evidence can be changed within FTK by going to View->Time Zone Display.

On an NTFS volume FTK will NOT prompt the user for a time zone when the case is being processed because the times are already stored in Greenwich Mean Time (UTC). FTK will automatically convert the times from GMT/UTC to the local machine's time. Once the evidence has been added and the case has completed processing you will need to either calculate the time difference between the local machine's time and the evidence time zone, or simply change the time zone on the examination machine to match the evidence time zone. You can also change the time zone within FTK as described below.

Again, if you have FTK 1.61 or above you do not need to change the time zone of the examination machine, the time zone of the evidence can be changed within FTK by going to View->Time Zone Display.

JP 09-13-06