CipherShed - Feature #93

support "quick" encrypt for new media (especially flash/SSD)

01/25/2015 09:59 PM - Jason Pyeron

Status:	New	**Start date:**	01/25/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

This mode simply applies the header and metadata, but since the container is empty, no encipherment is performed. The container is esentailly pre-filled with gibberish.

Once the OS starts to write (with a format first) it put the known data and the driver encypts only the writes and decrypts the future reads.

There is a single security risk with this approach, as the drive leaks the information about which portions have not had data written to it since the encryption was applied. This could be a risk for some usecases, but can be mitigated at any time by wiping the "free" space.

This would also require drivers to be written for OS installation.