CLAIMS

1. A computer implemented system for performing electromotive force analysis of a storage device comprising:

~~a solid state drive;~~

~~an AI co-processor chipset;~~

~~a thin~~ an inductance coil positioned in proximity to a ~~portion of the surface of the~~drive controller of the ~~solid state drive~~storage device for capturing data from electromotive force energy generated by the ~~solid state drive~~storage device;

a coprocessor chipset communicatively coupled to the drive controller, wherein the coprocessor chipset captures from the drive controller, data corresponding to operation of the storage device while capturing the data corresponding to electromotive force energy generated by the storage device;

at least one signal wire for communicating the captured data from the inductor coil to the coprocessor chipset;

wherein the coprocessor chipset is configured to digitally filter away unwanted signals from the captured data from the inductance coil, and to log time periods associated with the digitally filtered data; and

wherein the coprocessor chipset performs analysis based on the digitally filtered data, the logged time periods associated with the digitally filtered data and the data corresponding to operation of the storage device to detect any anomalies throughout the entire operation of the storage device, whereby a period of the analysis is determined based on the data corresponding to the operation of the storage device.

~~an analog-to-digital converter;~~

~~at least one probe for communicating the captured data to an analog-to-digital converter;~~

~~a solid state drive SoC controller; and~~

~~a circuit chipset in communication with the solid state drive SoC controller;~~

~~wherein the data is captured by the thin inductance coil and communicated to the analog-to-digital converter via the at least one probe;~~

~~wherein the analog-to-digital converter digitizes the voltage level of the captured data and communicates the results of the digitization and amplification to the Ai-Coprocessor;~~

~~wherein the Ai-Coprocessor chipset performs analysis of the data to detect any anomalies in the operation of the solid state drive and outputs a result for further processing;~~

~~wherein the solid state drive SoC controller monitors the hardware performance of the solid state drive by measuring electromotive force of the solid state drive and communicates the measured electromotive force data to the AI-Coprocessor;~~

~~wherein the Ai-Coprocessor chipset performs analysis to provide real time protection against any anomalies in the operation of the solid state drive; and~~

~~wherein the Ai-Coprocessor is interfaced with the solid state drive utilizing NVMe protocol or AHCI protocol.~~

2. The computer implemented system of claim 1, wherein the coprocessor chipset correlates the data corresponding to operation of the storage device with the captured data from the inductance coil, and wherein an anomaly is detected if the correlation exceeds a pre-determined threshold.

3. The computer implemented system of claim 2, wherein upon detection of the anomaly, the coprocessor chipset further derives a spectral image based on the data corresponding to operation of the storage device and the captured data from the inductance coil to identify the anomaly.

4. The computer implemented system of claim 3, wherein the coprocessor chipset identifies the anomaly by comparing the spectral image against a database of spectral image signatures.

5. The computer implemented system of claim 3, wherein the coprocessor chipset is an Artificial Intelligence (AI) coprocessor chipset configured to learn the operation of the storage device, and wherein the AI coprocessor chipset identifies the anomaly by comparing the spectral image against a database of spectral image signatures that is trained by the AI coprocessor chipset.

6. The computer implemented system of any one of the preceding claims, wherein the coprocessor chipset performs analysis in real time to detect any anomaly in the operation of the storage device.

7. The computer implemented system of any one of claims 1 to 6, wherein the coprocessor chipset communicates with the drive controller utilizing NVMe protocol.

8. The computer implemented system of any one of claims 1 to 6, wherein the coprocessor chipset communicates with the drive controller utilizing AHCI protocol.

9. The computer implemented system of any one of the preceding claims, wherein the anomalies are caused by malware.

10. The computer implemented system of any one of the preceding claims, wherein the coprocessor chipset interrupts the operation of the storage device when an anomaly is detected.

11. The computer implemented system of any one of the preceding claims integrated with the storage drive, wherein the storage drive is a solid-state drive.

12. The computer implemented system of claim 1, further comprising a power management integrated circuit (PMIC) for powering the coprocessor chipset separately from the drive controller.

13. The computer implemented system 11 or 12, furthering comprising a boundary guard trace, wherein the coprocessor chipset is positioned within the boundary guard trace to protect against unintentional signals, and wherein the inductance coil and the drive controller are positioned outside the boundary guard trace.

14. A computer implemented method for performing electromotive force analysis of a storage device comprising the steps of:

capturing data corresponding to electromotive force energy generated by the storage device by an inductance coil positioned in proximity to a drive controller of the storage device that controls the operation of the storage device;

communicating the captured data to a coprocessor chipset,

digitally filtering away, using the coprocessor shipset, unwanted signals from the captured data from the inductance coil, and logging time periods associated with the digitally filtered data;

capturing data corresponding to operation of the storage device from the drive controller while capturing the data corresponding to electromotive force energy generated by the storage device;

communicating the data corresponding to operation of the storage device to the coprocessor chipset;

analyzing the digitally filtered data, the logged time periods associated with the digitally filtered data and the data corresponding to operation of the storage device, using the coprocessor chipset to detect any anomalies throughout the entire operation of the storage device, whereby a period of the analysis is determined based on the data corresponding to the operation of the storage device.

15. The method of claim 14, further comprising:

correlating the captured data from the inductance coil with the data corresponding to operation of the storage device to detect an anomaly in the operation of the storage device.

16. The method of claim 15, further comprising:

deriving a spectral image based on the captured data from the inductance coil and the data corresponding to operation of the storage device, upon detection of an anomaly, and

comparing the spectral image against a database of spectral image signatures to identify the anomaly.

17. The method of claim 14, furthering comprising learning the operation of the storage device by Artificial Intelligence (AI) to obtain the database of spectral image signatures.

18. The method of any one of claims 14 to 17, wherein the storage device is a solid-state drive.

19. The method of claim 18, further comprising the step of:

interrupting the operation of the solid-state drive when an anomaly is detected by the coprocessor chipset.

~~2. The computer implemented system according to claim 1 wherein anomaly activities are caused by malware and wherein the further processing interrupts the operation of the solid state drive.~~

~~3. The computer implemented system according to claim 1 wherein the AI-CoProcessor applies artificial intelligence algorithms to detect ransomware activities.~~

~~4. The computer implemented system according to claim 3, wherein when the ransomware activities are detected, the operation of the solid state drive is interrupted.~~

~~5. A computer implemented method for performing electromotive force analysis of a storage device comprising the steps of:~~

~~capturing data from electromotive force energy generated by a solid state drive using a thin inductance coil positioned in proximity to a surface of the solid state drive;~~

~~communicating the captured data to an analog-to-digital-converter via at least one probe;~~

digitizing the voltage level of the captured data using the analog-to-digital converter;

communicating the voltage level to an Ai-Coprocessor;

analyzing the voltage level using the Ai-Coprocessor to detect any anomalies in the operation of the solid state drive;

outputting a result for further processing;

monitoring the hardware performance of the solid state drive by measuring electromotive force of the solid state drive with a solid state drive SoC controller and a circuit chipset in communication with the solid state drive SoC controller;

communicating the measured electromotive force data to the AI-Coprocessor;

using the Ai-Coprocessor to analyze the measured electromotive force data;

outputting the results of the analysis to provide real time protection against any anomalies in the operation of the solid state drive;

wherein the Ai-Coprocessor chipset performs analysis to provide real time protection against any anomalies in the operation of the solid state drive; and

wherein the Ai-Coprocessor is interfaced with the solid state drive utilizing NVMe protocol or AHCI protocol.

6. The computer implemented method according to claim 5 wherein anomaly activities are caused by malware and further comprising the step of:

interrupting the operation of the solid state drive when an anomaly caused by malware is detected.

7. The computer implemented method according to claim 6, wherein the Ai-Coprocessor utilizes artificial intelligence algorithms to detect ransomware activities.