Spy device: playback of sound in the room by HDD vibration

Maksym Buleshnyi
Applied Science Faculty
Ukrainian Catholic University
Lviv, Ukraine

Mykhailo Buleshnyi
Applied Science Faculty
Ukrainian Catholic University
Lviv, Ukraine

Artur Pelcharskyi
Applied Science Faculty
Ukrainian Catholic University
Lviv, Ukraine

Yuliia Moliashcha
Applied Science Faculty
Ukrainian Catholic University
Lviv, Ukraine

***Abstract*—eq In today's digital age, security has become a top priority for individuals and organizations alike. As technology continues to evolve, threats to data confidentiality and integrity are on the rise, ruiring robust security measures to protect sensitive information. However, safety can sometimes stem from unexpected sources — devices that were never originally intended for surveillance. In this paper, we will explore various methods by which hard disk drives (HDDs) can be repurposed as microphones.**

***Index Terms*—hdd, spy device, PES, smartctl**

I. Introduction

Hard Disk Drives (HDDs) have long been a popular method for storing information, making it essential to understand the potential problems and dangers associated with them. While it is a well-known fact that HDDs can be damaged by certain sound frequencies, an intriguing question arises: can use this property of disc to make a microphone?. There have been many researches that tried to answer on this question. In paper [2] authors are using PES (Position Error Signal) as analogy to membrane in microphone to extract sound. It was shown that Shazam was able to correctly identify the song recorded by HDD, even though it sounded like noise for human ear.

A. HDD structure

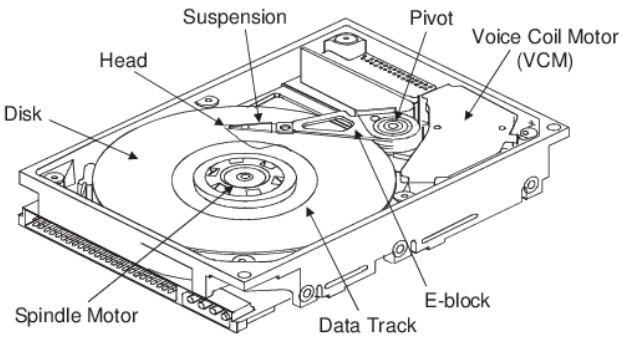

Fig. 1. HDD structure [1]

The main components of a disk drive are the platters and the head. A magnetic platter is a thin, circular metal plate used for data storage. During operation, the platter rotates with the help of a spindle motor. Typically, modern drives operate at speeds of 5400 RPM or 7200 RPM. The magnetic head reads or writes data to the platter and hovers a very short distance above its surface, maintained by an air gap created by the high rotational speed of the platter.

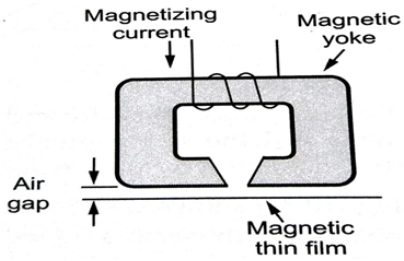

Fig. 2. Read/write head [1]

However, such a system has certain limitations. When the data that the head needs to read is not located on the same track, the trajectory of the head relative to the disk does not form a perfect circle. This increases the likelihood of the head reading incorrect data, as only a 7 nm margin of error is allowed. To address this issue, the disk generates a Position Error Signal (PES), which indicates how far the head has deviated from the intended track. The servo system's coordinate system is used to generate the PES and to facilitate movement between tracks. [4]

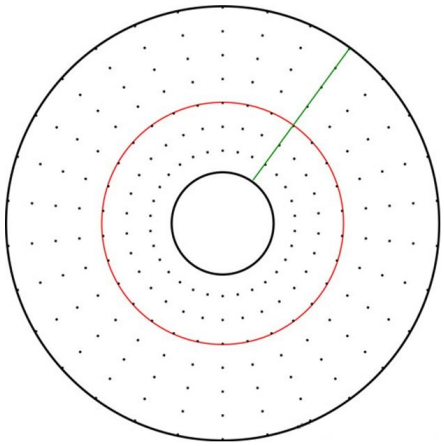

Fig. 3. Servo system [4]

The disk is divided into logical memory units called sectors, which are of a fixed size, typically 4 KB. In Fig. 3, black dots represent servo sectors, which are the points where reading or writing begins. The red circle illustrates a servo track. All paths contain the same number of servo sectors, usually between 200 and 300. Each servo sector is assigned a number within its path. The green line represents a straight line extending from the center to the edge of the disk, connecting all servo sectors with the same number; this line is referred to as a wedge.

B. HDD as microphone

In this section, we explore the parallel between traditional acoustic sensing devices, specifically microphones, and the inherent acoustic sensing capabilities of HDDs, focusing on the mechanical similarities and underlying principles that enable this phenomenon.

1) Microphone: A carbon microphone consists of four primary components: a power source, output mechanism, diaphragm, and carbon element. The recording process begins when acoustic waves create air pressure fluctuations. The diaphragm oscillates in response to these fluctuations, and the microphone generates a proportional voltage output. This analog value represents the acoustic wave's air pressure oscillations over time.

In essence, sound waves displace the diaphragm, and the output measures this displacement.

2) HDD: The read/write head represents the most sensitive component of an HDD, requiring extreme precision in track following with tolerance for error only in the order of nanometers. The sources of this error can be internal, such as HDD mechanics causing disk oscillations, or external factors, such as heat and vibrations.

Track following requires continuous monitoring of the head's deviation from the track center, this is done through PES measurement, followed by computing and applying the necessary adjustments. This process operates as a feedback control loop, as illustrated in Figure 4

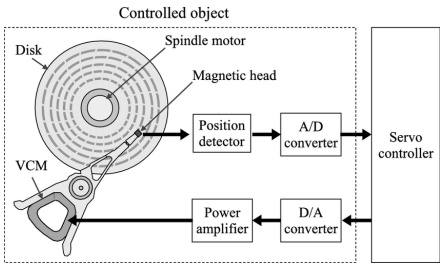

Fig. 4. HDD head-positioning control system [6]

As the head passes over the servo sector, it derives the PES from the servo burst pattern. This signal feeds into the controller, which then actuates the head to correct any positioning error.

We can state that in HDD mechanism external factors as vibrations displace r/w head and PES measures r/w head displacement.

Although HDDs were not designed to function as microphones, their internal mechanical components inherently respond to vibrations, specifically acoustic waves. The relationship between sound wave-induced head displacement and PES measurement suggests that PES can serve as an approximation of external vibrations.

The following section explores various approaches to reading the PES signal.

II. Approaches

A. SMART status

Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) is a monitoring system included in HDD that analyzes its health. It includes parameters that track the number of errors, which should increase in response to sound or vibration.

Smartmontools (S.M.A.R.T. Monitoring Tools) allows to monitor and manage the status of drives.

Each disk may have a different set of available parameters. However some parameters remain static, while others change but may not be useful for detecting sound. However, we have identified a parameter that is more common, frequently changing, and can be useful for detecting noise: the Spin Retry Count.

But for this parameter we observed that the value fluctuates unpredictably, and we were unable to detect any significant impact from sound or moderate vibration on the parameter increase. Additionally, the value naturally rises due to system operation, which complicates the task of distinguishing the effects of sound.

Additionally, to extend this approach to hearing sounds, not just vibration, we need a much higher sampling rate, which is not easily available for S.M.A.R.T. status. Also the Spin Retry Count parameter increases by approximately 20 every 0.1 seconds, and even increasing the sampling rate will not help to distinguish sound.

B. kscope

Kscope [3] is open-source tool to visualize small differences on syscall timing. Kscope uses POSIX function clock_gettime to retrieve the current time from system's real-time clock. Main idea is to measure difference between clock time before and after read operation. This difference can provide critical insights into the number of errors when reading from the HDD, as well as indicate the presence of noise or disturbances during the read process.

With this approach we were able to observed a clear pattern when a small vibrations were applied. However, we were unable to reproduce it with reasonable loudness of music.

C. PES

As mentioned in section I-B, PES is a valuable method for extracting sound. Unlike statistics such as the seek error rate or spin retry count, PES cannot be accessed using tools like smartctl or similar utilities, as it is not included in the attributes

monitored by S.M.A.R.T. Therefore, alternative methods must be used to obtain it.

The primary method for retrieving PES involves connecting to a specific pin on the HDD board responsible for transmitting PES data. AMUX is the pin we need.

However, to utilize this pin, real-time PES output must first be enabled. Without this, the pin may output unrelated data or remain inactive. To enable PES output, the F3 terminal [5] — a diagnostic and recovery interface for disk drives — is used. The F3 terminal [5] is available exclusively on Seagate drives and requires a connection to the drive's serial port via UART.

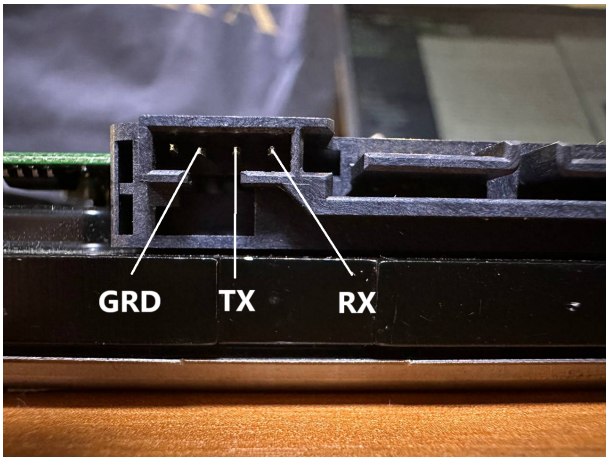

Fig. 5. Seagate 4-pin serial port

Figure 5 shows a write pin (**TX**) and a read pin (**RX**). These pins are cross-connected to the UART pins so that the UART read pin receives data from the drive's **TX** pin, while the UART write pin sends data to the drive via its **RX** pin.

Once connected to the F3 terminal, enabling PES output involves executing the `e 0` command at level 4. To disable PES output, the `e,1` command can be used.

Now that we can receive PES output in real time from the pin, we can begin locating the AMUX pin on the board. To identify the AMUX pin, we used two methods: pin analysis based on their properties and board component analysis based on their datasheets. Since PES is calculated for each servo sector, we can determine how many PES values the AMUX pin will return and, consequently, calculate its frequency.

To compute this frequency, two values are required: the disk's rotational speed (in revolutions per second) and the number of servo sectors per path. The rotational speed can typically be derived from the drive's name. For example, the drive we are working with, Seagate Barracuda 7200.9, indicates 7200 revolutions per minute (RPM), where "7200" represents the RPM and "9" denotes the drive's generation. Converting 7200 RPM to revolutions per second (RPS) gives us 120 RPS.

The number of servo sectors can be obtained from the disk's datasheet. If the datasheet is unavailable, it can be determined using the F3 terminal, specifically from the reference information (the first paragraph of the output) of the `f0` command at level 3.

For instance, with the number of servo sectors $n = 220$ and the RPS $f_{RPS} = 120$ Hz, the frequency of PES output can be calculated as follows:

$$f_{AMUX} = n \times f_{RPS} = 220 \times 120 \text{ Hz} = 26400 \text{ Hz}$$

After checking all the pins on the board with an oscilloscope, we identified 10 suitable candidates(Fig.6) that had a frequency of 26.4 kHz. With this narrowed set of candidates, we could then check the frequency at which these pins operate. By turning off the real-time PES output, for some drives, the corresponding pin would show a frequency of 0 Hz. However, this behavior depends on the specific hdd model. When PES output is disabled, the values on the AMUX pin might represent different data, causing the frequency to remain unchanged. Alternatively, in some cases, AMUX might not output anything at all [2], or it may output at a lower frequency. Unfortunately, we were not so lucky — the frequency for all pins remained the same despite toggling the PES output. As a result, we had to explore alternative methods to identify the correct pin.

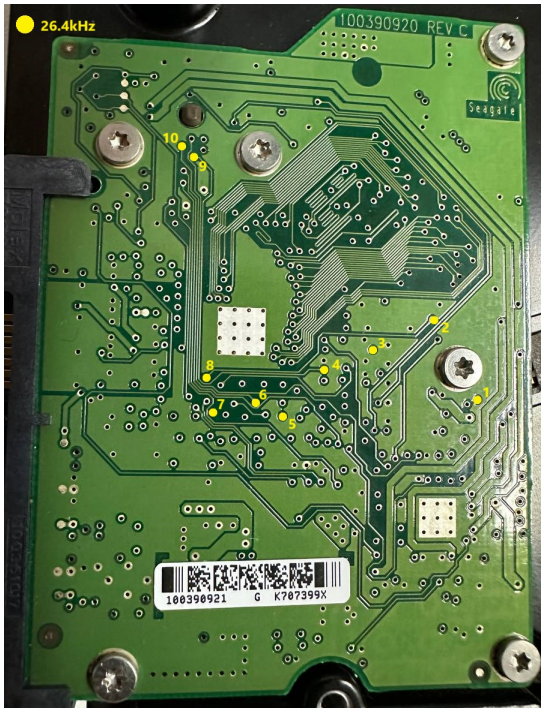

Fig. 6. AMUX candidates

Considering that the PES is generated by the Voice Coil Motor (VCM), it is important to check the connections of the pins on the internal side of the board. Fig.7 shows the components of the board that are most relevant to our investigation: Voice Coil Motor (VCM) Controller, MCU, and Ribbon Cable. Five out of the ten pins are connected to the internal components in internal side of board, resulting in the following connections:

- Pins 1, 2, and 8 are connected to the VCM Controller. Pin 8 is connected to Pin 2 on the front side.
- Pins 4, 6, 9, and 10 are connected to the Ribbon Cable. Pins 4 and 6 are connected to Pins 9 and 10, respectively, on the front side.
- Pin 3 is connected to the MCU.
- Pins 5 and 7 are not connected to any other pins and are located beneath the MCU, suggesting that they might be connected to it.

Fig. 7. Inner part of the hdd board

As a result, we narrowed the potential candidates even further, reducing the number from 10 to just 3 pins: 1, 2, and 8.

Next, we checked the values returned by these pins on the UART. It turned out that none of the pins returned any values, leading us to conclude that this method for identifying a pin is not very effective. Therefore, we moved to the second method of finding the AMUX pin: detecting it through board components.

We already knew that the PES is generated in the VCM controller, so we decided to look for the datasheet of this controller model based on its markings for our disk. Unable to find the specific chip, we found a datasheet for a chip that closely resembled ours. Assuming that the pin placements in these two chips were the same, we discovered that the pin outputting the PES data was not connected to anything. Consequently, for this disk model, we could not identify another way to read the PES data from the board, necessitating the search for alternative options.

D. PES-2. F3 commands

We identified two commands that output PES data, but in different formats.

The first command is `f0` at level 3. According to the F3 terminal documentation: "f0 collects PES (16-bit) data at the current track for the specified revolutions (or until the maximum data limit is reached)." The data is returned as a continuous stream of binary data. However another problem arose: the data is not transmitted in full. The F3 terminal for our hdd model supports a baud rate of 9600 Hz, while the PES data is transmitted at 26400 Hz. As a result, much of the data is lost during transmission.

The second command is `U100D` at level 4, which visualizes the PES values relative to the wedge, rather than individual servo sectors. As a result, we get three hexadecimal numbers for each wedge, represented as xxxx, which correspond to the minimum, average, and maximum PES values. The ideal value is considered to be 0000.

Let the minimum value be $xxxx$, the average $yyyy$, and the maximum $zzzz$. The deviation from the norm is calculated as follows:

- $FFFF - xxxx$
- $yyyy - 0000$
- $zzzz - 0000$

After removing the extra zeros, we are left with the following result:

- $FFFF - xxxx$
- $yyyy$
- $zzzz$

E. Impact of sound on PES

Using data from the `U100D`, we conducted several experiments to investigate whether sound affects the PES value. First, we collected PES data from a disk in a quiet room, ensuring no external vibrations affected the disk. The results of this experiment are shown in Fig. 8.

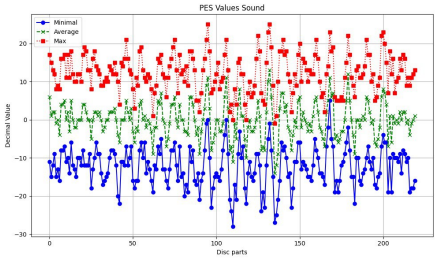

Fig. 8. PES in calm condition.

Next, we examined the effect of loud music on the disk. A speaker was placed near the disk without making direct contact. The speaker was positioned both on the same surface as the disk and suspended in the air to minimize the influence of vibrations transmitted through the surface. However, we observed no significant difference between these two setups. Figure 9 shows the PES results under the influence of music on the disk.

As seen in Fig. 8 and Fig. 9, sound has a noticeable effect on the PES value. Although the average value remains largely unchanged, the range between the maximum and minimum

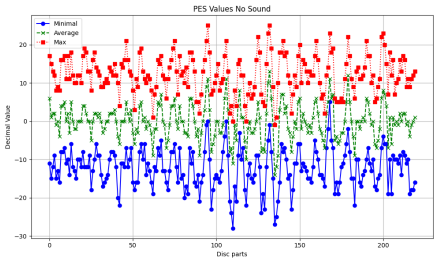

Fig. 9. PES under influence of sound

values has increased. This indicates that the head is deflecting more compared to the case without sound.

F. Nyquist–Shannon sampling theorem

The Shannon Sampling theorem states that the sample rate must be at least twice the bandwidth of the signal to avoid aliasing. Aliasing is the overlapping of frequency components resulting from a sample rate below the Nyquist rate.

The female voice covers the frequency range from 350 Hz to 17 kHz. The male voice covers the frequency range from 100 Hz to 8 kHz. In the case of our hard disk, which has a frequency of 26.4 KHz for pes, it is possible to recover human speech. But it depends on the disk, the frequency can be lower or higher. For example, an old laptop disk has a spindle speed of 90 Hz and 147 servo sectors, which gives 13.2 KHz, which may not be enough.

III. Future works

1) Read real time raw PES data from pin.
2) Try out more disks.
3) Detect recorded music using Shazam.

IV. Conclusion

There are number of methods for measuring the impact of sound, but many of them are either influenced by external factors or suffer from insufficient sampling rates, making them unsuitable for sound identification. The most effective metric to measure impact of sound on disk is PES (Position Error Signal). The best way to capture this data is by reading it directly from the diagnostic pin. However, as we investigated not all disk PCBs provide easy access to this information.

References

[1] Chirag Bhalodia. “Structure of Magnetic Disk — Structure of Hard Disk”. In: *bloger.com* (2021).

[2] Andrew Kwong, Wenyuan Xu, and Kevin Fu. “Hard drive of hearing: Disks that eavesdrop with a synthesized microphone”. In: *2019 IEEE symposium on security and privacy (SP)*. IEEE. 2019, pp. 905–919.

[3] Alfredo Ortega. *Turning hard disk drives into accidental microphones*. https://github.com/ortegaalfredo/kscope. 2017.

[4] Artem Rubtsov. “HDD inside: Tracks and Zones.” In: *hddscan.com* (2020).

[5] Seagate. *F3 Serial Port Diagnostics*. https://files.hddguru.com/download/Datasheets/Seagate/Seagate%20terminal%20commands/. 2009.

[6] Shota Yabui and Tsuyoshi Inoue. “Adaptive feedforward cancellation with damping control system in head positioning systems of HDDs”. In: *Microsystem Technologies* 25 (Dec. 2019). DOI: 10.1007/s00542-019-04465-5.