Issues in Information Systems
Volume 26, Issue 3, pp. 457- 471, 2025

DOI: https://doi.org/10.48009/3_iis_2025_137

Suspicious cheering with bits

Emil Eminov, *University of Tulsa, eae5331@utulsa.edu*
Stephen Flowerday, *University of Tulsa, svflowerday@gmail.com*
Andrew Morin, *University of Tulsa, andrew-morin@utulsa.edu*

Abstract

This research analyzed irregularities in payment through monthly tips from users on a well-known live streaming platform by analyzing a public dataset containing over one million entries from January 2022 to October 2024. The platform records revenue through its Bits virtual tipping system while providing channel-level reporting about monthly earnings together with average Bits per message and cumulative revenue. The research method included first cleaning the data across months, then using Z-score thresholding and rolling average analysis as statistical detection tools to identify channels with abnormal revenue rises. A process of manual verification examined flagged anomalies by matching them to external metrics, including subscriber counts, streaming activity, viewership trends, and event timelines for the purpose of detecting legitimate spikes from potentially suspicious irregularities. Most flagged revenue spikes corresponded to actual popularity increases due to audience growth or occurred during special events. However, a distinct subset of these spikes lacked any external explanation, raising suspicion. These research findings contribute to the development of fraud detection capabilities for digital content platforms such as Twitch, YouTube Live, and Facebook Gaming, and help to create platforms that are more transparent regarding revenue and maintain higher integrity.

Keywords: anomaly detection, Bits revenue, revenue fraud, live streaming platforms, financial integrity

Introduction

A digital era transformation has converted live streaming into a primary online content medium, which allows content creators to obtain money from their viewers through virtual payments in the form of "Bits" (Wildwood, 2024). The core elements of this digital environment are virtual currencies and money gifts, which are purchased with real currency to show support for streamers during live streams (J. Cao, Zhang et al., 2022). Virtual gifting operates as a method that enables the monetization of live content by leveraging streamer fan emotions and viewer commitment (J. Cao, Zhang et al., 2022). The interactive monetization models used by streaming platforms through Bits, as well as by other services through their stickers and Super Chat features, have emerged as primary revenue sources for live content creators. As a result, platforms often gamify these transactions (Siutila, 2018).

Live-streaming monetization faces growing threats from cybercrime because of recent events, which have revealed the urgent requirement for anomaly detection systems (Abbasova, 2024). The analysis of revenue data anomalies has demonstrated their significance as indicators of fraudulent activities that range from suspicious actions to view-botting donations and various other types of financial fraud.

A prominent example of live-streaming financial fraud was detected on Twitch in late 2021 and became one of the biggest fraud cases in the platform's recorded history (Chalk, 2021). Approximately 2400 Twitch

streamers from Turkey worked with hackers to launder between $9.8 and $9.9 million in funds through fake Bits donations (Chalk, 2021). The fraudsters purchased large amounts of Bits using stolen credit card information before distributing them to Twitch streamers who returned most of the funds to the fraudsters after taking a fee for their participation (Carriço, 2023; Chalk, 2021). Platform hosts received a small commission to facilitate the processing of these illicit funds through the same payment system used for genuine Bit donations.

After Turkish news outlets identified the Bits-for-money laundering operation in late 2021, Twitch and gaming industry executives activated their response plans. By September 2021, Twitch reported that it had disciplined or permanently banned more than 150 streamers located in Turkey, owing to their improper use of monetization tools (Chalk, 2021). In addition, at least 40 suspects were arrested by Turkish law enforcement for participating in the scheme, and a number of e-sports players and content creators faced sanctions due to their participation (Weiss, 2022). The aftermath of the Twitch case underscored the seriousness of the situation and highlights how the artificial inflation of streamer earnings can lead to streamers becoming involved in criminal behavior, ultimately defrauding payment providers and Twitch itself. Traditional anti-fraud mechanisms proved ineffective in detecting the fraud, pointing to the necessity to expose such abuse.

This incident highlights how the artificial inflation of streamer earnings can lead to streamers becoming involved in criminal behavior, ultimately defrauding payment providers and Twitch itself. Traditional anti-fraud mechanisms proved ineffective in detecting the fraud, pointing to the necessity to expose such abuse.

Live-streaming revenue stream irregularities remain difficult to detect as the conditions are constantly changing. For example, benign events, such as when a creator experiences a massive donor response from viral content or charity campaigns, may resemble potentially criminal behavior due to sudden and abnormal revenue growth. Anomaly detection systems should be able to distinguish between truly suspicious events and sudden yet innocuous revenue fluctuations, thus avoiding unnecessary alerts. The streaming data also shows concept drift behavior, which leads to changes in underlying patterns over time (Y. Cao, Ma et al., 2025). The monetization patterns of viewers can vary based on seasonal factors and platform policy transitions. Therefore, anomaly detection systems in this area must be robust against shifting data distributions while being able to dynamically update normal revenue baselines. The detection algorithms must continually update their models to maintain accuracy in line with observations in streaming data environments (Y. Cao, Ma et al., 2025). The target domain requires the detection of unusual monetization behavior inside fluctuating revenue streams, while minimizing both false alarms, which label valid growth spikes as fraud, and false negatives, which fail to detect actual fraudulent behavior.

The current literature on cybercrime and anomaly detection offers fundamental knowledge, yet shows inadequate application potential for live-streaming revenue analysis. Standard financial detection systems adopt statistical outlier methods, together with threshold-based methods and Z-score algorithms, to find transactions that fall outside normal data ranges (Yaro et al., 2023). Single threshold-based detection methods demonstrate difficulty when applied to streamer income patterns that have intense skewness and burstiness. Financial anomaly detection requires domain experts to review alerts in order to resolve problems that algorithms cannot solve independently (Ding et al., 2023). Researchers have overlooked the deployment of human analyst observation together with algorithmic detection as a means to improve reliability systems for live-streaming revenues.

Our research introduces a detection method that combines statistical analysis techniques with human verification for the detection of revenue anomalies on live-streaming platforms. The statistical detection system relies on rolling averages to predict normal earnings, while Z-score outlier thresholds detect

significant deviations that act as the first stage of detection. Our method detects both trend patterns and seasonal structures in streaming revenue through the time-based measurement of standard deviation and moving average, before identifying income points that show substantial deviations from running trends. It marks revenue points as potential anomalies whenever their Z-scores reach a threshold level that exceeds the defined threshold. Our approach uses human inspection together with algorithm analysis, recognizing that full dependence on either method alone would not be sufficient. An automatic scanning procedure identifies irregular cases, which are verified by checking manually whether the observed spike matches known legitimate events or stands as a potential sign of fraud. The combined workflow optimizes robustness because the statistical model detects most of the possible anomalies initially, before manual verification tests eliminate potential false alarms. The integration of human expertise into systems helps resolve situations where algorithms present an excessive number of false alerts or fail to interpret situations that humans would understand. Our research sought to show that unifying this dual anomaly detection system creates better fraud prevention solutions for live-streaming monetization systems while maintaining accurate automation control.

Background and Literature Review

Over the last decade, digital streaming platforms have established themselves as a major new media system that gives content makers the power to deliver real-time broadcasts to global audiences while simultaneously generating financial profit. The COVID-19 pandemic accelerated live-streaming adoption rates because it provided people with digital alternatives to personal experiences, as well as with technological enhancements and cultural changes that promoted its widespread acceptance (Narassiguin & Garnès, 2020). Through platforms such as Twitch, YouTube Live, and Facebook Gaming, creators gain several sources of revenue by accepting advertisements while allowing subscriptions and sponsorships and receiving donations from viewers. Monetization works through digital tips that come from viewers in the specific virtual currencies of the platform. For example, viewers can buy Bits as virtual currency within the streaming platform to send cheer donations to streamers during live chat sessions. The fixed monetary value attributed to each Bit (about $0.01) allows viewers to donate small amounts that generate significant earnings for popular streamers (O'Donoghue, 2024). The live donation process supports creators financially, as it shows viewer participation through real-time alerts using leaderboards and notification systems, among other gamified donation features. The integration of digital tipping functions has established digital tipping as a fundamental economic foundation of the creator economy within live streaming platforms, fostering direct interaction between audiences and content creators (Nguyen, 2021).

The use of virtual currencies for instant donations creates financial integrity issues within the system. System features designed to facilitate seamless support operations can be exploited by fraudulent actors to achieve their goals. Streaming platforms have documented instances of irregular donation activities, such as unusually large contributions from individual donors and donation spikes occurring when streamers are offline (Carriço, 2023). Traditional financial transactions cannot match the volume and speed of virtual tipping systems, making it challenging to monitor them manually. The platform remains accessible to all viewers, who can use their credit cards to purchase Bits and send them to streamers, thereby increasing the risk of fraudulent activity. Content creators with smaller audiences sometimes receive unexpectedly large donations that exceed their regular income, raising doubts about the authenticity of such donations. Ensuring genuine audience contributions and maintaining trust in creator revenues has become a central operational challenge for platform management.

User-generated revenue from streaming platforms has experienced extensive growth, which has led to the development of advanced fraudulent tactics. Because of the way virtual tipping works, criminal operators have been able to devise methods to commit unlawful acts and increase viewer counts artificially to deceive

streaming platforms. This fraud typically involves criminals obtaining stolen payment methods, such as hacked credit cards, to purchase platform virtual currency by making fake donations before having the money returned via off-platform channels. The streamer, in turn, refunds the stolen money to the schemers using methods outside the payment system, allowing the stolen credit to be "cashed out" while avoiding payment processor alerts.

Identifying and monitoring anomalies is essential when analyzing financial revenue information, as irregularities or outliers often indicate significant problems. Early detection of such anomalies is a fundamental priority for fraud prevention because abnormal patterns can indicate suspicious activities that require immediate identification to minimize damage (Fraud.com International, 2024). By detecting rapid changes in revenue streams, organizations can prevent minor problems from escalating into major financial losses (Fraud.com International, 2024).

Z-score thresholding serves as an easy statistical method for anomaly detection. It identifies the distance of a specific data point from the mean by standard deviation. The Z-score threshold technique enables analysts in financial and transaction monitoring to identify major deviations from typical values in monitored data. This method enables researchers to quickly identify transactions that deviate either above or below typical revenue levels (Wang, 2024). When applying a Z-score cut-off threshold of 2.5, all revenue points exceeding this value are flagged for further analysis (Veasey & Dodson, 2014). The implementation and interpretation of this method is straightforward, as a high absolute Z-score value automatically indicates an outlier within historical data.

Financial institutions commonly use Z-score analysis as their basic operational method to detect anomalies. This technique is beneficial for discovering extreme data points together with unusual numerical distributions in datasets (Changalva, 2024). While valuable, the method has certain limitations. The application of thresholding creates two issues: it may flag normal outliers as fraud and fail to detect complex schemes that lack single-point extreme deviations (Changalva, 2024). In practice, Z-score analysis is implemented using rolling windows or robust statistics to detect changing trends and minimize false alerts. Financial monitoring systems flag Z-score anomalies based on established literature, as these flags indicate data points that deviate from typical activity levels (Wang, 2024). This approach offers a quick way of locating potential irregularities in revenue patterns.

Rolling averages serve as a standard anomaly detection method for time-series data, such as streaming platform revenue over time. The benefit of using a rolling average is that it smooths out short-lived volatility while maintaining the long-term trends. The smoothing process generates a standard pattern that serves as the reference point for examining actual data points relative to their local movement. Moving averages allow analysts and researchers to reveal metric trends so they can better identify observations that differ substantially from previous patterns (Yaro et al., 2023). The rolling average establishes an evolving predictive measurement that identifies irregularities when actual revenue surpasses the rolling mean value by an abnormal margin.

Rolling averages form the basis of most anomaly detection systems. The exponentially weighted moving average (EWMA) control chart operates as a statistical tool by running average data monitoring until it detects deviations beyond specific boundaries (Hunter, 1986). Anomaly detection research uses EWMA and moving average models, which automatically update the expected value while detecting points that exceed the range developed from rolling context data (Zhang et al., 2020). Researchers have used this method to detect financial time-series and other types of anomalies in various domains with success. The definition of normal behavior through rolling windows with mean or median calculation enables these methods to detect both rapid revenue spikes and consistent revenue drifts. Moving average methods,

together with thresholds or statistical tests, have been validated by research to effectively smooth data noise while revealing significant deviations that could represent both fraud and errors (Yaro et al., 2023; Zhang et al., 2020).

While automated anomaly detection provides excellent results, it requires supplementation through external verification and contextual interpretation by human analysts to obtain comprehensive fraud analytics. Financial institutions that apply anomaly detection systems still require human analysts to confirm suspicious patterns identified by their algorithms for additional verification purposes (Ding et al., 2023). Fully autonomous anomaly detection exists mainly in low-stakes domains rather than high-stakes domains such as finance. The process of automated modeling detection requires human oversight to verify and fix detected anomalies, as indicated by research findings (Ding et al., 2023). Following the identification of outliers, investigators or fraud analysts verify the transaction by examining relevant information like customer history or current events to determine whether the incident constitutes fraud.

Methodology

The following methodology outlines our process for detecting and visualizing anomalous streamer earnings. The implementation of this approach is divided into several steps, including data collection and preprocessing, detailed in the following section.

Dataset Collection and Cleaning

Analysis requires initial steps to gather public streamer revenue information and perform comprehensive data-cleaning procedures. The dataset collected provided 1,048,576 monthly records for numerous streaming platform channels, spanning 34 months from January 2022 to October 2024. The dataset contains records with channel names and monthly information, and metrics that show Bit-based revenue distribution. The use of public data sources for digital platform research remains common in academic studies, as access to proprietary data is limited. Nevertheless, valid results emerge from appropriate cleaning procedures (Le et al., 2021). Data cleaning operations, such as normalizing channel name spellings and currency formats, play an essential role in accuracy by removing errors (Rahm & Do, 2000). When integrating multiple data sources, normalization is necessary for removing duplicates and normalizing different representations to prevent statistical misinterpretations. Rahm and Do (2000) explain that raw data, which includes redundant and inconsistent formats, results in poor quality, famously described as “garbage in, garbage out” (Rahm & Do, 2000). Therefore, the initial stage of public data cleaning is essential for maintaining data quality and is fundamental for delivering reliable analysis.

Anomaly Detection Techniques

The next phase of the research involved detecting unusual earning pattern variations. To detect suspicious earning patterns, two effective methods were applied: rolling average windows and Z-score thresholds. The application of a three-month moving average window acted as a local revenue model for each streaming service. The analysis method uses a rolling mean to smooth data noise while it traverses statistical information through time-based data series. Through its application as a low-pass filter, the rolling average function reveals longer-term trends, which makes sudden spikes stand out better in comparison to the local statistical pattern (Erdmann, 2020). To address limitations in global anomaly detection, researchers have proposed the use of moving windows to detect smaller, abrupt changes that average-based analysis fails to capture (Erdmann, 2020). A standard Z-score calculation for mean deviation is performed after calculating the rolling mean. The “kσ rule,” a fundamental principle in outlier detection, is used in Shewhart’s control charts for quality control, identifying points that deviate more than a specified number of standard

deviations from the mean (Dahari et al., 2025; Ekle & Eberle, 2024). Applying the Z-score requires a predefined threshold value. In financial and behavioral data analysis, thresholds within the 2–3σ range are commonly used to detect statistically meaningful outliers. The current research applied Z-score anomaly detection with a threshold of 2.5 standard deviations to identify anomalous data that exceeded this value above the rolling three-month average. The use of this threshold is standard practice in research on anomaly detection. This matches the threshold of "an outlier being 2.5 standard deviations from the rolling mean" applied by Vasey and Dodson (2014).

Filtering Criteria (Low-activity Streamers)

Our data analysis methodology for anomalies removes streamers who generate less than 1000 Bits per month from the analysis process. The filtering process has been implemented to avoid noise and false positive results. Transactions performed by low-activity users show up as larger relative spikes in the total amount of income simply because their combined contributions remain small. Setting minimum activity thresholds in fraud detection contexts allows systems to disregard unimportant fluctuations that cannot represent relevant anomalies (Grill et al., 2017). Such a transaction on a small channel does not provide significant meaning if it results in a high Z-score, even though it could trigger a one-time large donation for a streamer who earns less than 1000 Bits. Studies of anomaly detection demonstrate how sensitivity and specificity should be balanced by eliminating low-volume cases because this helps reduce false alarms (Lee, 2025). A pre-filtering step that excludes streamers who earn less than 1000 Bits is consistent with recommended practices, owing to its ability to eliminate insignificant anomalies in the data set of consistent earners.

Manual Verification with External Data

Our research incorporated anomaly detection involving manual verification, using data from external public sources about streamer metrics or streaming events that would explain the flagged behaviors. The academic literature emphasizes that unusual data points require contextual analysis to ascertain whether they represent actual irregularities or measurable occurrences (Musa & Bouras, 2021). According to Chandola et al. (2009), "contextual anomalies" are data points that become anomalous only under specific conditions, and their detection demands in-depth knowledge of their contextual environment. In our case, for example, a spike in streamer revenue might result from a streamer conducting a special event, representing an explainable contextual anomaly. Such anomalies can be verified as legitimate by comparing them with data available publicly, such as the streamer's viewer engagement statistics or the release of popular games the streamer is playing at the time of the spike. This approach aligns with fraud detection methods that cross-check alerts against streamer data from profiles and prior incidents to distinguish true from false alerts. Therefore, additional data resources help determine whether specific outliers represent genuine information or measurement errors (Lee, 2025). Overall, the use of external verification is considered the most effective way to improve the reliability of anomaly analysis (Musa & Bouras, 2021). This step in the assessment process aims to create results that identify actual suspicious activities.

Visualization of Results

The evaluation consists of visualization techniques, including bar charts, time-series plots, and histograms, to identify differences between anomalous user earning patterns and those of normal users. Visualization serves as a strong method for anomaly identification as well as anomaly presentation. Scientists have created special visual analysis tools that identify abnormal patterns within normal datasets (Davidson, 2007). The visualization developed by Davidson displays anomalies in red against normal data points, which "graphically convey which observations are anomalous and why" (Davidson, 2007). Our

methodology uses bar plots to display streamer earnings data to identify outliers, while time-series line charts with marking features allow analysts to identify spikes successfully in timestamped earnings patterns. Distribution plots and histograms enable researchers to view the location of abnormal monthly earnings when compared to typical values for individual streamers. The literature supports the use of visual analytics for outlier validation because, through visual examination, analysts can confirm whether identified points deviate significantly from the pattern or follow typical trends. Visual analytics provides valid support as it uses human pattern recognition together with algorithmic detection to enable easy anomaly verification (Davidson, 2007). Our visualization methods display anomalous user data through distinct color or style coding, which follows industry standards for making anomaly detection results easier to understand.

Results

Data on the revenues from streaming services was collected month-by-month from January 2022 to October 2024. The individual monthly records were combined into one consolidated Microsoft Excel file for extensive examination purposes. A Python script performed calculations for rolling averages and Z-scores. The metrics for analysis consist of estimated Bits revenue, total Bits income accumulation, and Bit usage averages per message and per user, together with quarterly and semi-annual moving averages. The anomaly detection system records two indicators, which include Z-score calculation for monthly Bits income versus historical mean and binary flags that highlight anomalies by means of rolling averages and Z-score thresholds. The complete framework allowed us to investigate periodical trends in Bit revenue between both big streamers and small channels, which facilitated the detection of time-based outlier patterns.

The anomaly detection method identified 71 channel-month observations as statistical outliers across the dataset, which contained over one million observations. The 71 anomalies involved 48 different channels, demonstrating that several channels had more than one outlier occurrence. The identified anomalies mostly represent significant spikes in Bits monthly income that exceeded the normal earning patterns of individual channels. Few downward revenue anomalies occurred, with such cases mainly involving temporary channel service interruptions. The flagged spikes were significantly bigger than typical channel operating ranges. These extraordinary and prominent data points stood out from typical month-to-month changes because the rolling average combined with the Z-score technique identified these points using the standard k-sigma outlier criterion (Veasey & Dodson, 2014).

Of the 71 detected anomalies, only a single month's activity affected most of them, while the remaining anomalies stayed within normal boundaries. The streamer received a single large Bits donation, which quickly raised their financial income before their earnings returned to normal. Bit donations exhibit stable behavior because these extreme events occur very seldom between regular contributions. The unusual donation patterns occur during specific time periods with limited clustering behavior. The number of outlying cases in Bits donations during mid-2022 and late-2023 demonstrates that certain periods, such as holidays and special events, likely triggered increased irregular donation behavior on various channels. Most of the detected anomalies originated from smaller and medium-sized donation channels because such channels experienced major proportional changes in their Bit donations. The algorithm did not identify anomalies in the extremely large donation channels because their peak donation volumes remained within the established range boundaries of their already elevated donation levels.

Normal Streamers

The monthly revenue from Bits earned by top streamers shows stable fluctuations over 2022–2024 without any unusual patterns. As seen in Figures 1 and 2, the revenue from Bits in high-profile streamers, including Streamer 1 and Streamer 2, demonstrates regular trend patterns without showing any major deviant data points. Time-series data from the streamers displays regular content-related changes together with small spikes that occur during the main streaming events. However, all variations remain within standard ranges. The lack of flag indicators for leading streamers suggests their donation patterns stay consistent or their peaks exist within expected realms, since their audience size is substantial and their events are legitimate (e.g., a highly promoted stream). The increase in Streamer 1's Bit income in late 2023 followed a popular content period and then dropped afterward without triggering any abnormality alerts due to steady income changes. The monthly Bit incomes received by Streamer 2 showed typical patterns over time, because no individual month differed significantly from his established income range. Prominent streamers maintain stable and foreseeable Bit income patterns, which result from their stable follower interaction patterns. Such changes in their income are usually related to specific events or scheduled breaks, which do not align with the criteria of the anomaly detection system. The observed patterns in larger channels demonstrate consistent patterns, rather than the irregular behaviors that occur in smaller channels.

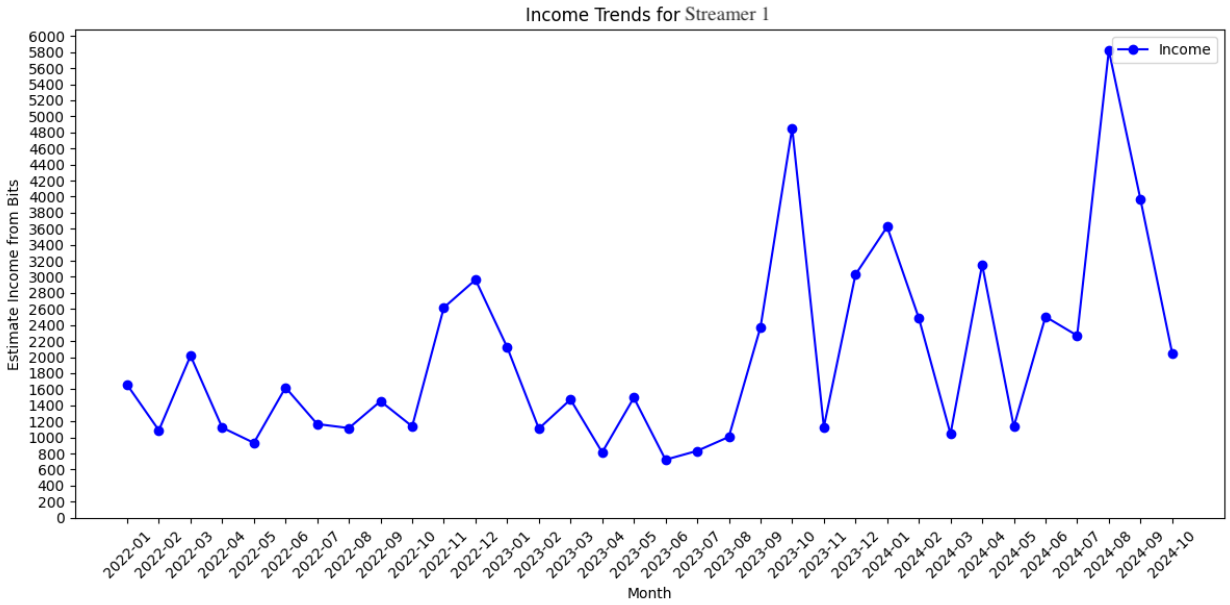

Figure 1: Monthly Income in Bits For The High-Profile Streamer 1.

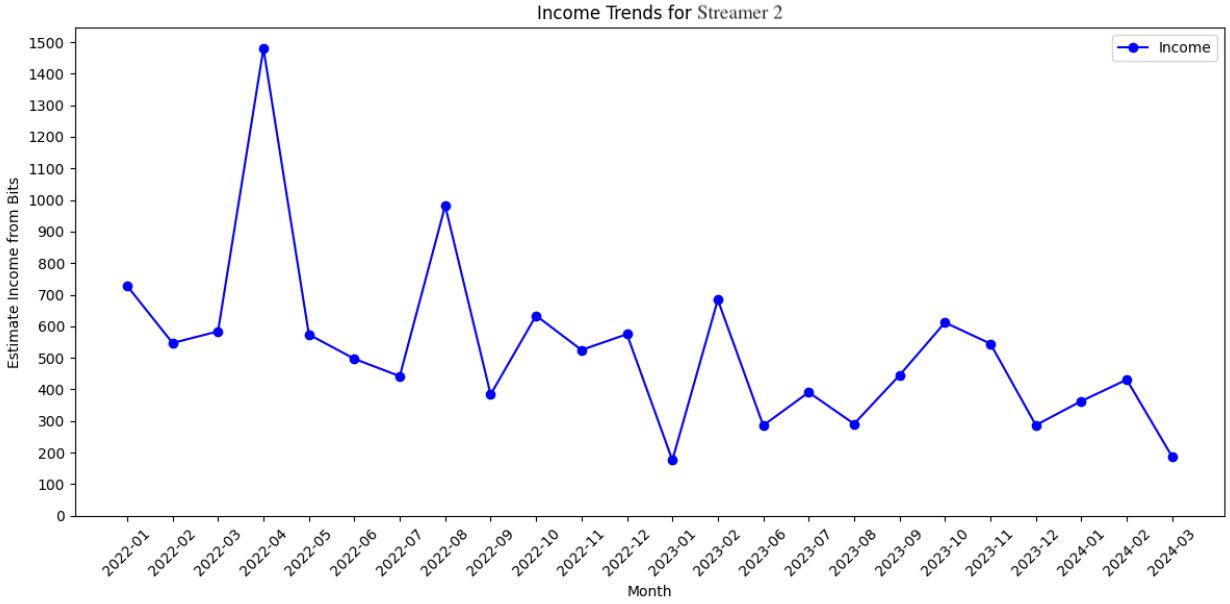

Figure 2: Monthly Income in Bits For The High-Profile Streamer 2

Anomalous Streamers

The anomalous channels display a completely different behavioral pattern. The majority of streamers exist in the lower follower range, with small Bit revenues, until a single month reflects an extreme surge. For example, as seen in Figure 3, Streamer 3 operates with approximately 200 viewers per stream. Bits revenue for Streamer 3 showed minimal activity throughout all months until October and November 2022, when it reached over 10,000 Bits, then rocketed to more than 14,000 Bits before returning to its usual low levels. These two consecutive Bit flows could not be linked to any noticeable channel-based events like tournaments or charity initiatives, making them authentic anomalies.

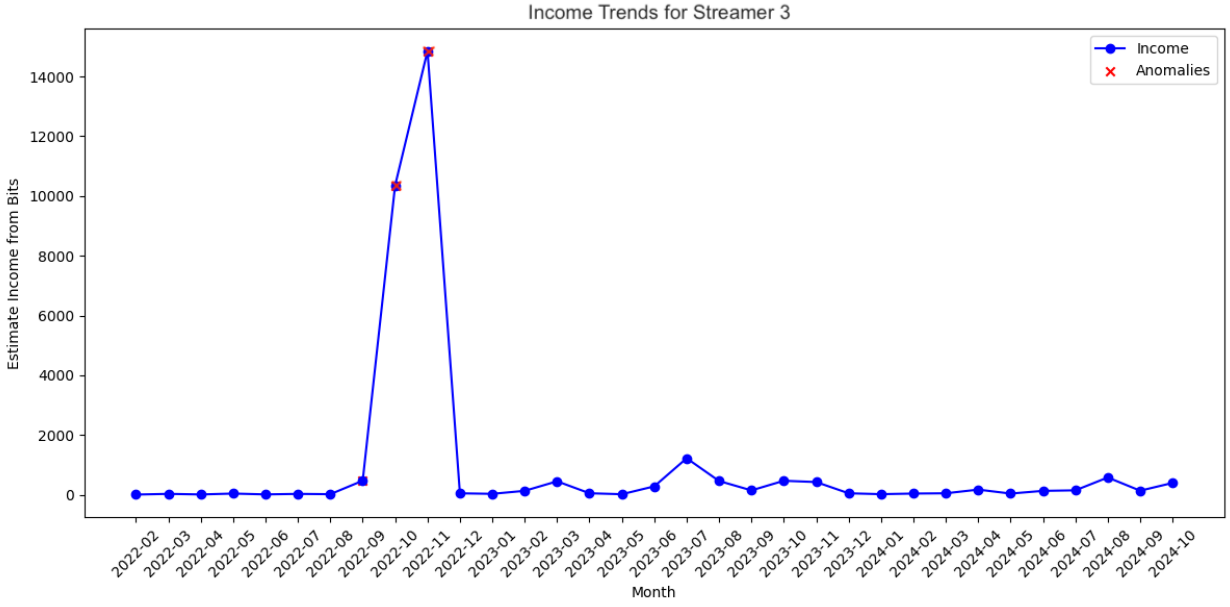

Figure 3: Monthly Income in Bits for The Anomalous Streamer 3.

Another example can be seen in Figure 4, where Streamer 4 earned 13,000 Bits in one month before moving to zero Bits per month. An independent "one-month wonder" increase was one of the typical patterns that emerged from the cases analyzed. The combined action of suspicious actors leads to small streamers instantly receiving substantial amounts of money during these temporary peaks in activity. Normal streamers who do not operate anomalous channels receive Bit donations that match their follower base and audience involvement rates, and their monthly income variations show typical growth patterns or seasonal impacts. Donations for regular users show gradual development with no substantial spikes in amount, unlike what occurs in these anomalous circumstances.

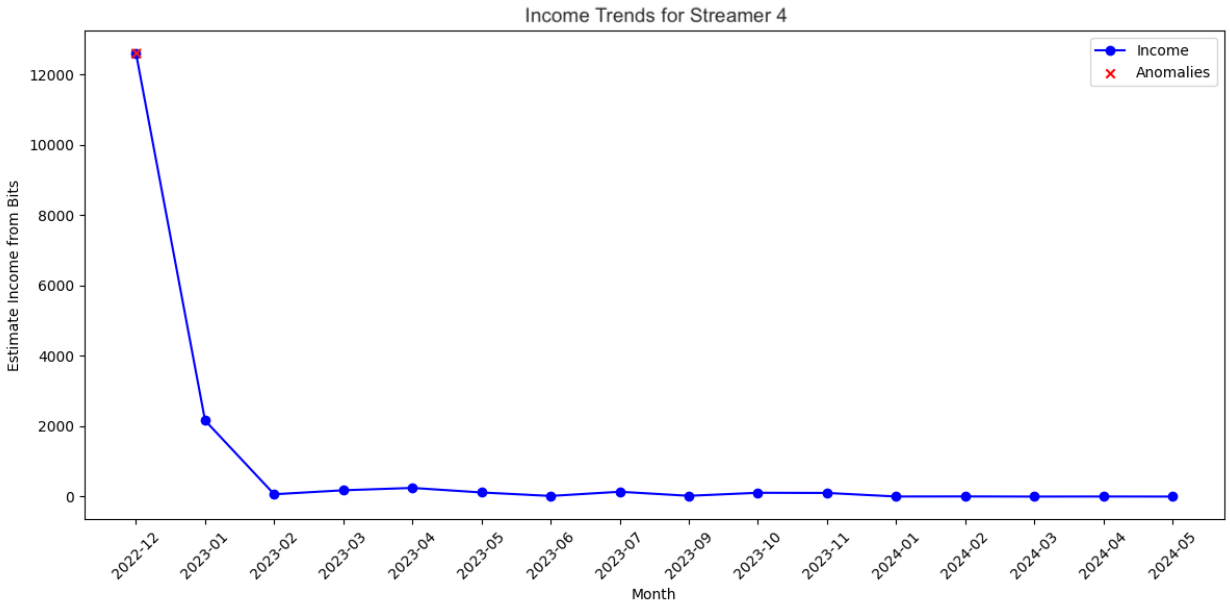

Figure 4: Monthly Income in Bits for The Anomalous Streamer 4

Manual Validation

All cases were manually reviewed using contextual analysis, resulting in the classification of individual anomalies as seen in Figure 5, with red, green, and yellow color designations in a review table. The review scheme uses red labels to indicate unresolved anomalies, green labels for explained anomalies, and yellow labels for mathematically detected but insignificant anomalies. This validation process led to a useful classification of analytical results. Genuine, unexplained outliers made up almost two-thirds of the total 71 anomalies because no accepted external explanation could be found for them, indicating potentially malicious or important deviations. A few anomalies among the total number proved to have valid reasons (indicated by green), since they contained genuine spikes which did not violate the contextual norms. Streamer 5, in Figure 6, serves as an example of a streamer who organizes charity speedruns for fundraising purposes. The channel raised its Bits donation metrics in multiple designated periods (Jan 2022, May 2022, Jan 2023, Jan 2024, and Jul 2024) when hosting fundraising events for charity. These spikes were marked green because they conformed to expected seasonal patterns, driven by positive events rather than irregular behavior.

Streamer	Followers	Subs (Gifted)	Total Avg Viewers	Avgerage Bits	Anomaly 1				Anomaly 2				Banned
					Date	Average Views	Max Views	Bits	Date	Average Views	Max Views	Bits	
1	2,057,380	753 (186)	16,708		Jan, 2022	2,727	19,507	13,600	May, 2022	27,669	93,065	4,650	No
2	82,076	3,032 (0)	143		May, 2022	171	437	1,230	Nov, 2023	78	759	3,000	24/04/2024-26/04/2024
3	93,825	187 (134)	200		Apr, 2022	153	404	1,320	Aug, 2022	336	1,073	1,400	No
4	976,613	777 (52)	2,543		Feb, 2022	2,063	17,192	3,386	Aug, 2024	2,088	7,218	2,790	No
5	15,903	322 (220)	36		Mar, 2024	30	73	1,300	Aug, 2024	483	2,334	2,100	No
6	25,300	2,247 (2126)	107		Jun, 2023	98	235	2,000	Dec, 2023	146	4,559	900	20/12/2024-21/12/2024
7	36,910	260 (50)	102		Dec, 2022	65	158	1,600	Jul, 2023	65	158	1,300	No
8	105,119	74 (50)	229		Sep, 2022	85	166	600	Aug, 2023	97	257	800	No
9	47,658	1224 (1030)	199		Oct, 2022	208	395	10,350	Nov, 2022	242	785	14,850	22/08/2024–29/08/2024

Figure 5: Manual Validation Table

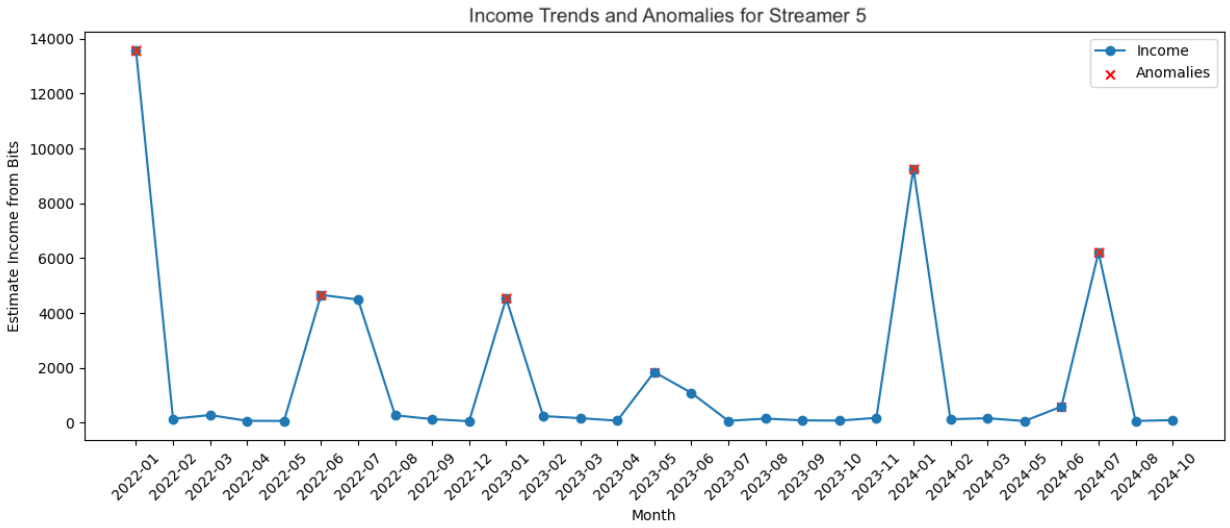

Figure 6: Monthly Income in Bits for The Streamer 5

Discussion

The analysis in this study examined over one million Bit earning records, spanning January 2022 to October 2024, to reveal vital patterns regarding platform-based Bit revenue dynamics. The results show that earnings on the platform present a volatile financial situation with sporadic massive increases in donations. The data examined revealed statistically relevant spikes in revenue, identified as aberrations and marked in red. Some of these red spikes corresponded to legitimate charity fundraisers, although external impacts often trigger such abrupt revenue growth. However, most spikes in viewer donations happened without any observable external triggers, making their sudden rises difficult to explain. In contrast, the earnings of well-known streamers, Streamer 1, Streamer 2, and Streamer 5, consistently followed normal patterns, as their revenues remained within expected ranges driven by standard viewer engagement.

Future Work and Limitations

This analysis provides important insights but also faces several limitations that suggest new directions for future research. Due to a lack of direct access to streamers regarding the flagged anomalies, our analysis was based solely on publicly available information from the content creators, as direct communication was not possible.

The results could be improved by establishing contact with streamers or platforms to obtain additional information or by implementing data collection schedules at shorter intervals to better monitor brief fluctuations. In addition, research effectiveness could be enhanced by expanding the analysis to include subscriber-based revenues and direct donor contributions. This would deliver an enhanced understanding of streamer financial dynamics alongside monetization stream relationships.

Conclusion

The research provides an extensive examination of streamer income trends over 34 months (from January 2022 to October 2024) while focusing on detecting abnormal patterns in Bit revenue data. With regard to revenue reliability, the core research found that top-tier streamers operate in a completely different operational space than less successful streamers. The earnings streams of popular streamers showed a steady and uncomplicated revenue progression each month because their Bit income continued to rise steadily. Mid- and low-profile streamers showed significant volatility in their streamer earnings, experiencing sudden income spikes, which created major deviations from normal patterns. The anomaly detection system identified the sudden revenue spikes because it automatically detected them as genuine outliers occurring in time-series streamer revenue data.

The manual review validated that statistical anomaly alerts monitor genuine audience behavior patterns instead of accidental numerical variations. These additional metrics helped distinguish between widespread community production and donations from select donors who made large contributions. The monitoring system successfully evaluated the complex revenue patterns through its analysis of various data points.

The research findings show that anomaly detection techniques serve as valuable tools for gaining a deeper understanding of streamer revenue patterns. The analytical method produced essential information by identifying distinct abnormal patterns that standard trend measurement methods fail to detect. Using anomaly detection techniques to analyze Bit-based revenue patterns simplifies complex revenue patterns, enabling the extraction of detailed information about streamer economic analysis through outlier identification.

References

Abbasova, A. (2024, April 18). *Luxury on the surface: Social media influencers and financial crime.* https://www.rusi.org/explore-our-research/publications/commentary/luxury-surface-social-media-influencers-and-financial-crime#:~:text=In%202021%2C%20Turkey%20detained%20around,platform's%20integrity%20against%20money%20launderers

Cao, J., Zhang, G., Liu, D., & Shang, M. (2022). Influencing factors of users' shift to buying expensive virtual gifts in live streaming: Empirical evidence from China. *Frontiers in Psychology, 13,* 997651. https://doi.org/10.3389/fpsyg.2022.997651

Cao, Y., Ma, Y., Zhu, Y., & Ting, K. M. (2025). Revisiting streaming anomaly detection: Benchmark and evaluation. *Artificial Intelligence Review, 58*(1), 1–24. http://dx.doi.org/10.1007/s10462-024-10995-w

Carriço, F. (2023, January 26). *A deep look into the unusual activity with Twitch Bits.* https://streamscharts.com/news/unusual-activity-twitch-bits#

Chalk, A. (2021, November 3). *Money-laundering on Twitch triggers call for investigation from Turkish politician*. https://www.pcgamer.com/twitch-money-laundering-scheme-triggers-call-for-investigation-from-turkish-politician/#

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR), 41*(3), 1–58. http://dx.doi.org/10.1145/1541880.1541882

Changalva, R. (2024). Leveraging machine learning for anomaly detection in Oracle Financial Consolidation and Close Cloud Service (FCCS). *Intelligent Systems and Applications in Engineering,* 2186–2198.

Dahari, S., Abdul, M., & Ghapor, A. A. (2025). Robust control chart application in semiconductor manufacturing process. *Journal of Advanced Research in Applied Sciences and Engineering Technology, 43*(2), 203–219. http://dx.doi.org/10.37934/araset.43.2.203219

Davidson, I. (2007). *Anomaly detection, explanation and visualization.* SGI. Tokyo, Japan: Tech. Rep.

Ding, X., Seleznev, N., Kumar, S., Bruss, C. B., & Akoglu, L. (2023). From detection to action: A Human-in-the-loop Toolkit for anomaly reasoning and management. In *Proceedings of the Fourth ACM International Conference on AI in Finance,* 279–287. http://dx.doi.org/10.1145/3604237.3626872

Ekle, O. A., & Eberle, W. (2024). Anomaly detection in dynamic graphs: A comprehensive survey. *ACM Transactions on Knowledge Discovery from Data, 18*(8), 1–44. https://doi.org/10.48550/arXiv.2406.00134

Erdmann, M. (2020, November 4). *Unsupervised anomaly detection in sensor data used for predictive maintenance*. https://epub.ub.uni-muenchen.de/60291/1/Erdmann_Unsupervised_Anomaly_Detection_Sensor_Data.pdf#:~:text=4.1%20The%203σ,rule

Fraud.com International. (2024). *Anomaly detection for fraud prevention: Advanced strategies.* https://www.fraud.com/post/anomaly-detection#:~:text=Anomalies%20refer%20to%20irregularities%20or,early%20and%20preventing%20financial%20losses

Grill, M., Pevný, T., & Rehak, M. (2017). Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences, 83*(1), 43–57. https://doi.org/10.1016/j.jcss.2016.03.007

Hunter, J. S. (1986). The exponentially weighted moving average. *Journal of Quality Technology, 18*(4), 203–210. https://corporatefinanceinstitute.com/resources/career-map/sell-side/capital-markets/exponentially-weighted-moving-average-ewma/

Le, H., Wu, J., Yu, L., & Lynn, M. (2021, November 10). *A study on channel popularity in Twitch*. https://doi.org/10.48550/arXiv.2111.05939

Lee, S. (2025, March 18). *10 step guide to mastering outlier analysis for accurate data.* https://www.numberanalytics.com/blog/10-step-guide-to-mastering-outlier-analysis#:~:text=An%20ideal%20outlier%20detection%20system,false%20positives%20and%20false%20negatives

Musa, T. H., & Bouras, A. (2021). Anomaly detection: A survey. In *Proceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, London, 4,* 391–401. Springer Singapore. http://dx.doi.org/10.1007/978-981-16-2102-4_36

Narassiguin, A., & Garnès, V. (2020). *The influence of COVID-19 on Twitch audience: How lockdown measures affect live streaming usage.* http://upfluence-common.s3.amazonaws.com/Covid19_Twitch.pdf

Nguyen, T. (2021, February 26). *Virtual tips are helping content creators actually make money.* https://www.vox.com/the-goods/22301751/digital-tipping-creators-platforms

O'Donoghue, G. (2024, August 20). *Everything you need to know about Twitch Bits.* https://powder.gg/blog/everything-you-need-to-know-about-twitch-bits/#:~:text=Twitch%20Bits%20are%20a%20form,the%20minimum%20being%201%20cent

Rahm, E., & Do, H. H. (2000). Data cleaning: Problems and current approaches. IEEE Data Engineering Bulletin, 23(4), 3–13.

Siutila, M. (2018). *The gamification of gaming streams. GamiFIN,* 131–140.

Veasey, T. J., & Dodson, S. J. (2014, April). Anomaly detection in application performance monitoring data. *International Journal of Machine Learning and Computing, 4*(2), 120. https://www.ijml.org/papers/398-LC018.pdf

Wang, Q. (2024). Research on the application of machine learning in financial anomaly detection. *iBusiness, 16*(4), 173–183. https://doi.org/10.4236/ib.2024.164012

Weiss, G. (2022, January 06). *Forty arrested in Turkey For Alleged $10 million money laundering scheme on Twitch.* https://www.tubefilter.com/2022/01/06/forty-arrested-turkey-twitch-money-laundering-scheme/#:~:text=Forty%20people%20in%20Turkey%20have,8%20million

Wildwood, L. (2024, December 9). *How much money do Twitch streamers make? (Latest data).* https://bloggingwizard.com/how-much-money-twitch-streamers-make/#:~:text=,per%20live%20viewer%20they%20receive

Yaro, A. S., Maly, F., & Prazak, P. (2023). Outlier detection in time-series receive signal strength observation using Z-score method with S n scale estimator for indoor localization. *Applied Sciences, 13*(6), 3900. https://doi.org/10.3390/app13063900

Zhang, M., Guo, J., Li, X., & Jin, R. (2020). Data-driven anomaly detection approach for time-series streaming data. *Sensors, 20*(19), 5646. http://dx.doi.org/10.3390/s20195646