



HAL
open science

Distinguishing Sellers Reported as Scammers on Online Illicit Markets Using Their Language Traces

Clara Degeneve, Julien Longhi, Quentin Rossy

► **To cite this version:**

Clara Degeneve, Julien Longhi, Quentin Rossy. Distinguishing Sellers Reported as Scammers on Online Illicit Markets Using Their Language Traces. *Languages*, 2024, 9 (7), pp.235. 10.3390/languages9070235 . hal-04631257

HAL Id: hal-04631257

<https://hal.science/hal-04631257>

Submitted on 2 Jul 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.




L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Article

Distinguishing Sellers Reported as Scammers on Online Illicit Markets Using Their Language Traces

Clara Degeneve ^{1,*} , Julien Longhi ²  and Quentin Rossy ¹ ¹ École des Sciences Criminelles, University of Lausanne, 1015 Lausanne, Switzerland; quentin.rossy@unil.ch² AGORA Laboratory EA 7392, CY Cergy Paris University, 95000 Cergy, France; julien.longhi@cyu.fr

* Correspondence: clara.degeneve@unil.ch

Abstract: Fraud exists on both legitimate e-commerce platforms and illicit dark web marketplaces, impacting both environments. Detecting fraudulent vendors proves challenging, despite clients' reporting scams to platform administrators and specialised forums. This study introduces a method to differentiate sellers reported as scammers from others by analysing linguistic patterns in their textual traces collected from three distinct cryptomarkets (White House Market, DarkMarket, and Empire Market). It distinguished between potential scammers and reputable sellers based on claims made by Dread forum users. Vendor profiles and product descriptions were then subjected to textometric analysis for raw text and N-gram analysis for pre-processed text. Textual statistics showed no significant differences between profile descriptions and ads, which suggests the need to combine language traces with transactional traces. Textometric indicators, however, were useful in identifying unique ads in which potential scammers used longer, detailed descriptions, including purchase rules and refund policies, to build trust. These indicators aided in choosing relevant documents for qualitative analysis. A pronounced, albeit modest, emphasis on language related to 'Quality and Price', 'Problem Resolution, Communication and Trust', and 'Shipping' was observed. This supports the hypothesis that scammers may more frequently provide details about transactions and delivery issues. Selective scamming and exit scams may explain the results. Consequently, an analysis of the temporal trajectory of vendors that sheds light on the developmental patterns of their profiles up until their recognition as scammers can be envisaged.



Citation: Degeneve, Clara, Julien Longhi, and Quentin Rossy. 2024. Distinguishing Sellers Reported as Scammers on Online Illicit Markets Using Their Language Traces.

Languages 9: 235. <https://doi.org/10.3390/languages9070235>

Academic Editor: Alan Garnham

Received: 15 November 2023

Revised: 13 June 2024

Accepted: 19 June 2024

Published: 28 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: cryptomarket; fraud; scammer; language trace; forensic linguistic

1. Introduction

Illicit markets, like legal markets, have been transformed by the virtual environment, which has altered promotional strategies, sales processes, and the sharing of evaluations between buyers and sellers. Sellers of illicit products and services employ multiple approaches to promote their products to potential customers. Online spaces used for selling illicit products and services can be classified into two main categories. The first is that of dedicated sales sites created on the web in the form of online stores associated with unique domain names and with contents managed by the spaces' administrators. The other category is that of collaborative platforms: online communities that are shared environments in which sellers publish their shops or their ads in a pre-existing convergence setting. Sellers may focus on lawful commerce or the trade of illicit goods and services on specialised forums and cryptomarkets present on the dark web. As Martin (2013) explains, cryptomarkets are digital marketplaces hosted on the dark web that facilitate transactions primarily using cryptocurrencies as the medium of exchange. These marketplaces promote user privacy and anonymity, using a combination of encryption and routing techniques to obfuscate both the identities of the participants and their financial transactions. These markets were initially used to sell drugs but have since diversified into selling many types

of products, such as false identity documents and credit cards, as well as illegal services such as hacking services.

The online activities of sellers and buyers on these platforms leave digital traces that can be exploited to study illicit markets (Rossey and Décarry-Héty 2017). They offer a wealth of information relevant to addressing cross-cutting questions such as ‘What substances are available?’, ‘What is the market volume?’, ‘What are the sellers’ revenues?’, and ‘How is the market structured?’ Regular monitoring of these spaces broadly allows for trend tracking and for considering the use of these traces as a monitoring indicator.

Such analyses, however, require the ability to assess the relevance of the information available on these platforms. Among the validity challenges of these indicators is the presence of fraudsters, who can skew the analyses with sales behaviours that do not match those of genuine sellers. A scam in this case can be described as (Jacquart et al. 2021, p. 410) when ‘a person is interested in an item for sale on a classified ad site, contacts the advertiser, then pays the negotiated amount to the advertiser, but never receives the item’. Within cryptomarkets, the identification of fraudulent sellers can be facilitated in two primary ways: directly by the platform’s administrators or through discussion forums where customers can report dubious activities and alert fellow users (Morselli et al. 2017).

However, can fraudsters be detected by analysing the traces they leave on platforms? Does their sales behaviour differ from that of genuine sellers? This article proposes an approach based on the forensic analysis of language traces left by sellers in their seller profiles and in disseminating their ads. The main hypothesis of this work is that it is possible to distinguish reported scammers from legitimate sellers on cryptomarkets using language traces (Renaut et al. 2017). A language trace can be defined as the remnant of an action that alters the environment (Ribaux 2023; Roux et al. 2022), which is the writing of an illegal or litigious text by an author and which has an informative potential not only for its source but also for the illicit activity itself (Degeneve et al. 2022).

2. Previous Research

2.1. Digital Traces Left by Trust Mechanisms in Online Trade

2.1.1. Deceptive Practices in Cryptomarkets

Most research on the detection of deception, which is a different deviant behaviour from fraud, has focused on the distinction between false and truthful statements, even if both may be considered deceptive activities. Research on the production and detection of deception typically concentrates on individuals, particularly on how they convey lies and the extent to which others can identify those lies (Markowitz et al. 2023). Scams are ‘acts carried out deliberately to enhance one’s gains at the cost of others’ (Christin 2013, p. 241). Deception is used for obtaining illegal financial gain with ‘the deliberate intent to deceive with the promise of goods, services, or other financial benefits that in fact do not exist or that were never intended to be provided’ (Titus et al. 1995, p. 54).

Markowitz et al. (2023) emphasise that the context of a deception behaviour is pivotal, as outlined in their extended Contextual Organization of Language and Deception (COLD) framework. They argue that traditional deception studies often overlook the nuanced interplay between context and communicative behaviour, leading to inconsistent findings across different settings. By integrating three context dimensions—individual differences, situational opportunities for deception, and interpersonal characteristics—Markowitz et al. (2023) enhance the COLD model’s applicability to forensic settings. Their study underscores the complexity of deception, suggesting that both the psychological dynamics of the deceiver and the specificity of the communicative environment significantly influence the effectiveness of deception detection strategies. This holistic approach advocates for a more nuanced consideration of context. As Hancock et al. (2004) note, deception is influenced by communication technologies (e.g., email, instant messaging, and telephone systems). We thus describe here the deception schemes underlying fraud in cryptomarket environments.

Morselli et al. (2017) conducted a study of the management of disputes and violent incidents in the drug segment of cryptomarkets. Drawing on Christin's (2013) observation that a vast majority (95%) of feedback is positive, the researchers explored the phenomenon of scamming. Further, the study agreed with Tzanetakis et al. (2016) in pointing out a tactic employed by some sellers of posting derogatory remarks to tarnish their competitors. The researchers gathered scam-related data from 10 cryptomarkets and a widely visited forum. The main areas of contention they discerned were the non-delivery of goods, lack of communication, and inferior product quality. Qualitative analysis of forums revealed that sellers accused of scamming are occasionally defended by peers, who urge aggrieved buyers to exhibit patience. The inherent design and framework of cryptomarkets aim to curb, if not eradicate, scam incidents.

In a 2020 study, Bancroft et al. (2020) analysed the drug-centric discussion forum PFM, focusing on how reputation is quantified through a 'Karma score' (a form of feedback given by fellow users) and various status indicators. The researchers outlined different manifestations of fraud within this environment. One notable tactic is the 'exit scam', wherein previously trustworthy sellers abruptly decide to deceive buyers. Additionally, Bancroft et al. (2020) highlight the phenomenon of 'selective scamming' (p. 9), in which a seller deliberately fails to dispatch a specific order and retains the payment yet remains undetected by fulfilling all other orders as expected.

The issue of fraudulent activities on cryptomarkets seems to mirror its significance in legal markets. Ineffective administration by market overseers has been identified as a root cause of such deceitful activities (Christin 2013). Many researchers have emphasised the pivotal role of discussion forums as platforms on which users share insights and highlight potential scams. However, the methodologies for identifying potential scammers can diverge.

2.1.2. The Informative Value of Feedback

Feedback is a pivotal element underpinning the concept of trust within online marketplaces. The essence of trust for sellers revolves around expanding their customer base. Feedback mechanisms on digital marketplaces, including cryptomarkets, provide buyers with tools to express their satisfaction or dissatisfaction with a transaction. As Przepiorka et al. (2017) explain, feedback mechanisms play a crucial role in shaping a seller's reputation, since they can directly impact the trajectory of subsequent transactions. Such mechanisms usually encompass two main features: rating systems and commentaries. Rating systems can range from simple thumbs up/down and star ratings to complex scorecards that evaluate different aspects of a transaction, such as product quality, shipping speed, and communication efficacy. Commentaries allow for qualitative feedback, enabling buyers to elaborate on their experiences, highlight specific strengths or concerns, and provide context for their numerical ratings. Hypothetically, the analysis of customer feedback on sales platforms or dedicated forums could aid in detecting a fraudster.

Pavlou and Dimoka (2006) delve into two aspects governing marketplace actors: benevolence and credibility. While benevolence pertains to a seller's genuine goodwill and positive intent towards buyers, credibility revolves around the seller's competency and reliability in fulfilling promises (p. 383). Pavlou and Dimoka analysed 10,000 eBay feedback comments to infer sellers' intentions based on buyers' perceptions. The data came from '1665 completed auctions for 10 distinct products (iPod, n = 512; movie DVD, n = 341; music CD, n = 312; Palm Pilot, n = 138; digital camera, n = 110; camcorder, n = 92; DVD player, n = 84; monitor, n = 76) during May of 2005' (p. 400). The analysis revealed occasional discrepancies between the magnitude of the rating and the sentiments of pronounced comments (especially those using terms like 'abominable' or 'absolutely fabulous'). The subsequent phase involved disseminating a survey to purchasers via email to glean demographic information, with a total of 420 responses received. In the third phase, a content analysis was performed on feedback comments, limiting the scope to the first 25 comments for each seller. This analysis was conducted by a team of three individuals

who categorised comments into five distinct groups. The 25 comments evaluated for each of the 420 sellers revealed that many buyers consult the comments prior to making a purchase. Distinct patterns emerged between benevolence and credibility in the comments, though they are not mutually exclusive. Overall, these comments offer deeper insights into a seller's reputation than mere ratings do. Notably, those categorised as 'ordinary' predominantly carried a positive sentiment.

In their research on Silk Road 1.0, [Przepiora et al. \(2017\)](#) derived data specific to drug transactions. They utilised several key indicators: total ratings received, product pricing, pace of sales, and feedback count per product. Analysing a dataset of 3153 products, they observed that a staggering 95.8% of ratings were perfect 5/5 scores. The researchers subsequently designed a model to assess how fluctuations in an individual seller's reputation, when juxtaposed against their mean reputation, would influence sales dynamics. Their findings underscored a direct correlation: sellers with sterling reputations were inclined to elevate their pricing and expedite sales, and most interestingly, the negative feedback bore a heftier impact than its positive counterpart.

[Tzanetakis et al. \(2016\)](#) draw a parallel between traditional narcotics markets and those operating on cryptomarkets. Street data, both qualitative and quantitative in nature, were sourced from a German project. The research focused on the motivations behind individuals' involvement in drug trafficking, narrowing down the sample to 32 individuals who were primarily driven by monetary incentives. Data from Agora included profiles, feedback, and forum discussions derived from four active sellers, two high-rated and two low-rated. Within these groups, one seller offered multiple drug varieties while the other was limited to one or two. Sales figures revealed three sellers with transaction counts ranging from 200 to 500, and one with transactions between 2000 and 3000. Trust dynamics differed markedly between traditional and cryptomarkets, with the former emphasising safety. On cryptomarkets, trust determinants are intrinsically tied to platform-provided metrics, such as sales volumes, ratings, and general seller information. Ratings predominantly ranged from four to five. Dark web forum interactions substantially foster trust, but some sellers exploit this by leaving negative feedback to tarnish their competitors.

In their recent study, [van Deursen \(2021\)](#) undertook a qualitative examination of feedback on the AlphaBay cryptomarket to investigate the repercussions of the polarity of forum posts on the vendors' sales and pricing. They classified feedback as 'positive', 'neutral', or 'negative' and found that it was often supplemented with descriptive comments. The platform also features an embedded forum. In total, 1655 articles, inclusive of seller details, feedback, and relevant forum content, were gathered. The determination of polarity was achieved through sentiment analysis using a Random Forest algorithm. The findings suggest that positive textual feedback carries more weight than ratings in influencing a seller's market presence. Intriguingly, and contrary to expectations, negative feedback has a beneficial impact on sales and a more pronounced influence on pricing than positive feedback. Among forum comments, positive ones were found to be the most impactful.

Several key observations drawn from previous research informed the direction of our study. First, high feedback scores, though ostensibly indicative of a trustworthy seller, can be misleading. The overwhelmingly positive ratings across various platforms underscore the potential pitfalls of using this metric in isolation to gauge the legitimacy of sellers. Second, forums stand out as crucial platforms where customers exchange insights and raise alarms about dubious actors. The interactive nature of these platforms, coupled with users' collective experiences, often results in a more accurate depiction of a seller's reputation. Nevertheless, the question remains: is it possible to detect a scammer based on their activity within a cryptomarket?

2.1.3. Leveraging Language Traces to Unveil Fraud through Computational Linguistic Analysis

We hypothesise that fraud in online settings—as a particular type of deceptive behaviour like lies, fake news, or rumours—can be detected based on the analysis of language

traces that include deceptive linguistic cues. Language traces are pieces of information used to change people's cognition or beliefs (Addawood et al. 2019). Addawood et al. (2019) explored the linguistic indicators of deception used by political trolls on social media to mislead the audience about their true intentions. They highlight the vulnerability of content-focused social media platforms to such tactics due to their reliance on asynchronous, text-based communication. Through their analysis, they identified key linguistic cues employed by trolls, such as persuasive language, simpler and less specific language, and a higher frequency of hashtags, tweets, and retweets. Despite the challenges of detecting trolls due to their rarity and the resulting imbalance in classification tasks, Addawood et al. note that troll accounts often use fewer nouns and post shorter tweets. They conclude that a simple algorithm could mistakenly classify most accounts as non-trolls with high accuracy but low recall.

Computational linguistics and machine learning experts have also ventured into fraud detection, employing diverse methods to tackle the issue.

Gibbons and Turell (2008) present Egginton's examination of an advanced fee fraud's linguistic framework. Drawing from a spam email he obtained, Egginton undertook discourse analysis to discern tactics for bolstering the potential victim's trust based on that specific spam email. These include specificity in the email's subject and main content, highlighting the situation's urgency, and using complex technical jargon.

Ott et al. (2011) present a comparative approach for detecting fake reviews on Trip Advisor. They compare the results obtained by a panel of three human judges with those of an automated detection algorithm. While the human panel achieved approximately 60% performance in detecting fake reviews, the automated approach reached around 89% performance. Analysing unigrams and bigrams of words proved to be one of the most effective methods (Ott et al. 2011).

Vidros et al. (2017) explored fraudulent online job advertisements. Utilising a corpus of 450 deceptive and 450 genuine ads from an online platform, they applied the bag-of-words model for vectorisation. Subsequently, they trained six distinct classifiers ('ZeroR, OneR, Naive's Bayes, J48 decision trees, random forest and logistic regression' p. 9). The Random Forest algorithm proved the most accurate, with a 91% precision rate. Through a linguistic and contextual analysis, the team determined that deceitful ads were generally shorter, lacked details about job requirements and perks, and exhibited certain keyword patterns such as 'home' (implying 'work from home'). Finally, binary analysis of the corpus showed some characteristics that can help with the distinction: '(a) opportunistic career pages usually do not have a corporate logo; (b) scammers omit adding screening questions; (c) usually mention salary information even in their title to lure candidates; (d) skip designated job attributes (i.e., industry, function, candidate's education level, and experience level) used for jobs board categorisation; (e) prompt defrauded candidates to apply in external websites, bypassing the ATS pipeline; (f) or force them to send their resumes to their personal email addresses directly and (g) address lower educational level' (p. 12).

Jakupov et al. (2022) employed topic modelling to discern deceptive opinion spam among reviews on Trip Advisor, amassing a dataset of 6977 reviews. Utilising the BERTopic module in Python, their methodology effectively identified lexical indicators of deceit within the texts ('Max size of N-gram dictionary: total number of rows in the n-gram dictionary; Rho parameter: prior probability for the sparsity of topic distributions; Alpha parameter: prior probability for the sparsity of topic weights per document; Size of the batch: number of rows processed in chunks; Initial value of iterations used in learning update schedule: learning rates start value, set to 0 in all the experiments; power applied to the iteration during updates: learning stepsize; N-grams: the maximum size of the sequences generated during hashing') (Jakupov et al. 2022, p. 7).

Junger et al. (2023) address the gap in understanding how fraud victims and near-victims recognise deception in real-world scenarios. The researchers analysed responses from a victimisation survey to elucidate effective deception detection strategies used

by individuals exposed to various types of online fraud. They revealed that 69% of near-victims had recognised fraud through their existing knowledge of fraud tactics and warning signs, such as inconsistencies or errors in the fraudsters' communications. Other detection strategies included distrust, adherence to personal security rules, and seeking additional information. Victims and near-victims often cited past experiences and increased awareness from media exposure as factors enhancing their ability to spot fraud. Junger et al. emphasise that knowledge of fraud and proactive information-seeking behaviours are the most effective defences against fraud victimisation.

Research has hinted at the potential of language analysis in discerning deceitful behaviours, as in the studies of deceptive opinion spam and fraudulent listings described above. However, this approach remains largely uncharted when it comes to analysing data from cryptomarkets. Our research seeks to bridge this knowledge gap. By employing a forensic analysis of language traces left by sellers in both their profiles and their advertisements, we developed a methodological approach that harnesses the nuances of language to uncover deceptive patterns. We designed a refined toolset for discerning genuine sellers from reported scammers. The fusion of linguistics and forensic science with the rich data of cryptomarkets could provide an innovative method for vetting the authenticity of sellers, fortifying the integrity of analyses derived from these platforms.

3. Materials and Methods

3.1. Datasets

The data used for this research were collected from three cryptomarkets: DarkMarket, Empire Market, and White House Market (refer to Table 1), which were the major cryptomarkets on the dark web at the time of the study. Initiated in January 2018 on the dark web, Empire Market stepped in to fill the gap created by the mid-2017 closure of AlphaBay Market and quickly rose to prominence, remaining one of the largest dark web markets until August 2020. DarkMarket then rose to become the largest illicit dark web marketplace of its time. It was shut down in January 2021 by an international task force coordinated by Europol. Collection for the White House Market was performed over the period from April 2020 to March 2021. This cryptomarket opened in February 2019 and was closed by its creators in October 2021.

Table 1. Data collected from DarkMarket, Empire Market, and White House Market.

	N of Unique Ads	N of Unique Description	Crawling Period	Nb Crawls
EM	87'543	61'346	2020.06–2020.08	8
DM	88'640	45'432	2020.07–2021.01	17
WHM	83'524	56'739	2020.04–2021.03	30
Total	259'707	163'517		

With the objective of discerning reported scammers within the pool of sellers, our research utilised the Dread forum, as guided by previous scholarly findings. Dread is a dark web forum in operation since 2018.¹ It is structured, similar to Reddit, by threads dealing with different subjects, and users can exchange ideas, create posts, and reply to each other within the same post. In particular, there are threads dedicated to cryptomarkets where buyers and sellers can interact; these threads were collected, as they are also used by users to report fraud.

We methodically retrieved threads pertaining to the trio of cryptomarkets (refer to Table 2) and subsequently applied manual inspection of the posts to capture usernames that were frequently reported as fraudulent by peers.

From the cryptomarket data, we extracted profiles and advertisements corresponding to the identified usernames (for examples of profile and product description, see Appendix A, Figures A1 and A2). Based on the list of usernames, derived as mentioned earlier, vendors were categorised as potential scammers. To respect privacy, no vendor

names have been disseminated, and no other identifying information was used during the study. All the analyses were based on the text, and the results are presented such that no link can be established with the virtual identity of the sellers.

Table 2. Number of posts containing ‘scam’ for every cryptomarket thread on Dread forum.

Thread	Number of Posts Containing ‘Scam’
White House Market	261
Empire Market	1967
DarkMarket	678
Total	2906

3.2. The Choice of a Computational Linguistic Approach

From a forensic perspective, computational linguistics offers objectivity, reproducibility, and accuracy (Juola et al. 2006). Nevertheless, as Fobbe (2020) points out, computational research in forensic authorship attribution lacks theoretical engagement. The assumption that language differences inherently indicate different authors or types of authors based on detectable characteristics should rely on robust methods. Surface structure features dominate studies, yet they fail to capture deeper stylistic nuances. The issue lies not in feature extraction but in the inadequacy of current style theories to explain how feature frequency correlates with individual authorship. Nevertheless, variation in the type of analysis we propose is not aimed at simply increasing the levels of analysis but at combining the analysis of different levels of language within a communicative conception of grammar and expression, as developed by Charaudeau (1992) in particular. We followed a ‘method for decomposing the data into smaller chunks so that a larger set of variables can be used for the discriminant analysis’ (Chaski 2005, p. 11) to fit with the forensic analysis criteria (Roux et al. 2022), and we also took a multi-level approach to linguistics, combining different markers that have in common the enhancement of certain communicative intentions. Juola (2021) has contrasted human and computational analysis in forensic science, noting the difficulty of establishing the validity and reliability of human-based analysis. Juola suggests prioritising objective features like shared vocabulary, word length, N-grams, common words, and punctuation. Longhi (2021) summarizes the tensions between the two approaches: while qualitative stylistic approaches can be seen as too subjective, ‘much of this criticism comes from the United States, where the admissibility of expert evidence is determined in relation to the standards of the Daubert Criteria’ (Wright 2014, p. 19). Thus, computational approaches are ‘considered to be more objective, empirical, replicable, and ultimately more reliable than their stylistic counterparts’, but they can hardly give information about theoretical aspects of linguistic variation.

3.3. Pretreatment

We employed the ‘langdetect’ Python module (accessible at <https://pypi.org/project/langdetect/>, accessed on 6 November 2023) for the task of language identification. We observed that a predominant proportion, 91.45% of genuine profiles and 91.20% of scam profiles, were in English. We opted not to translate the non-English texts into English for several compelling reasons. Firstly, translation inherently introduces alterations in stylistic elements, which could compromise the authenticity and integrity of the original text. Secondly, from a forensic perspective, modifying the original trace of a text through translation is not desirable, as it may obscure or alter linguistic traces pivotal to our analysis. Thirdly, stylometric comparisons across languages can be fraught with challenges. Factors such as sentence complexity and length can vary significantly between languages, making it difficult to draw accurate and consistent conclusions. Additionally, translation might inadvertently introduce translator biases, further complicating the authenticity and interpretation of the results. We deemed it crucial to preserve the original nuances and subtleties of each text to ensure the reliability and robustness of our computational

linguistic methods. Given that most of our sample consisted of English texts, we believed it reasonable to filter out non-English entries to maintain uniformity in the analyses.

All profiles and advertisement descriptions were filtered to retain only the unique texts for each seller on each of the cryptomarkets.

3.4. Analysis

We conducted a preliminary analysis of the number of distinct texts per vendor and per cryptomarket. Then, we subjected the corpus to a comprehensive examination utilising three distinct analytical methods: (1) textometric analysis to quantify text-based characteristics; (2) stylometric analysis, which includes syntax analysis to dissect sentence structures and linguistic patterns; and (3) N-gram analysis to discern overarching topics.

3.4.1. Textometric Analysis of Raw Texts

For the computational assessment of textual data, our study employed the ‘textacy’ Python module, which is accessible at <https://textacy.readthedocs.io/en/latest/> (accessed on 6 November 2023). This tool enabled us to analyse textual statistics, including the number of characters, words, long words, unique words, and sentences. The number of uppercase letters was also calculated. The module also allowed for the evaluation of textual entropy, along with three readability and four diversity indices. The metrics used, along with their detailed definitions and references, are documented online at https://textacy.readthedocs.io/en/latest/api_reference/text_stats.html (accessed on 6 November 2023).

To assign grammatical labels to individual tokens within each corpus, we employed the Part of Speech (POS) Tagging features of the ‘textacy’ package. Subsequently, we computed the mean and median values of the analysed tags across all corpora per vendor.

Features such as the count of uppercase letters, readability scores, diversity indices, and POS tagging are instrumental in stylometric analysis to differentiate and compare authors or distinct bodies of text. These metrics are detailed alongside conventional textometric attributes, as they were derived from the raw text with minimal pre-processing that included only the elimination of return and tab characters. This choice allowed the exploration of textual features directly from unmodified text (i.e., language traces as they were left by writers).

3.4.2. Analysis of the N-Grams

The predominant words, bigrams, and trigrams of words in the lemmatised text were extracted, as proposed by Ott et al. (2011), through the large language model of the ‘spacy’ algorithm integrated into the ‘textacy’ module. This was preceded by a comprehensive pre-processing routine that standardised bullet points, quotation marks, and whitespace while excluding punctuation. The frequency analysis of those N-grams allowed for the identification of recurring topics.

3.4.3. Probabilistic Discrimination

In line with a recent paper on ChatGPT authorship discrimination (Bozza et al. 2023), we compared the use of N-grams between reported scammers and all other vendors using a probabilistic approach (Aitken and Taroni 2005; Taroni et al. 2022). This approach computes the ratio of the probability of occurrence of a particular form if the vendor is labelled as a ‘scammer’ divided by the probability of occurrence of the same form for all other vendors. This likelihood ratio (LR) score signifies the overuse of a form by one group over the other. A value exceeding one supports the hypothesis that the behaviour is more characteristic of the reported scammers over other vendors, while a value less than one indicates a preference for the alternative hypothesis, suggesting that the behaviour is more typical of all other vendors. For instance, an LR of two indicates that it is twice as probable to see the word if the text was written by a reported scammer. Before calculating the LRs, all forms used by less than 1% of vendors were filtered.

4. Results

4.1. Textometric Analysis of Raw Texts

The number of unique descriptions per seller profile over the collection period differed between reported scammers and other sellers (refer to Table 3). On DarkMarket and Empire Market, the average number of distinct profiles increased from 1.0 to 1.6 and from 1.2 to 1.8, respectively. The rise in the White House Market was less pronounced, from 1.6 to 1.9. The analysis of ad descriptions yielded a global ratio of 1.24 distinct texts per ad for those classified as scams, which is notably comparable to the ratio of 1.15 calculated for non-scam advertisements.

Table 3. Number of distinct profiles and ad descriptions for reported scammers and others on each cryptomarket.

	Reported Scammer N Profiles > N Distinct Descriptions	Others N Profiles > N Distinct Descriptions	Reported Scammer N Ads > N Distinct Descriptions	Others N Ads > N Distinct Descriptions
DarkMarket	33 > 52	809 > 813	717 > 906	33'465 > 39'645
Empire Market	83 > 153	804 > 936	2099 > 2537	43'536 > 48'767
White House Market	73 > 142	2036 > 3240	2632 > 3308	42'464 > 49'326
Total	189 > 347	3647 > 4925	5448 > 6751	119'465 > 137'272

The distributions of textual statistics showcased in Figures 1 and 2 fail to differentiate reported scammers from other sellers in terms of their profiles or their ad descriptions.

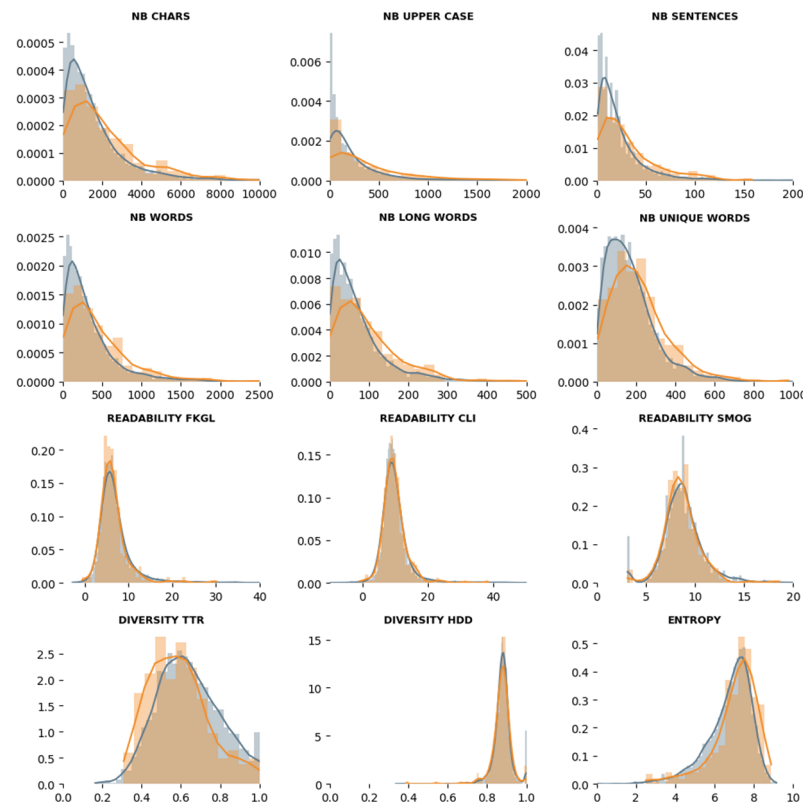


Figure 1. Textometric analysis of profile descriptions. The chart illustrates a comparative analysis with scam-related advertisements depicted in orange at the top, while other advertisements are represented in grey.

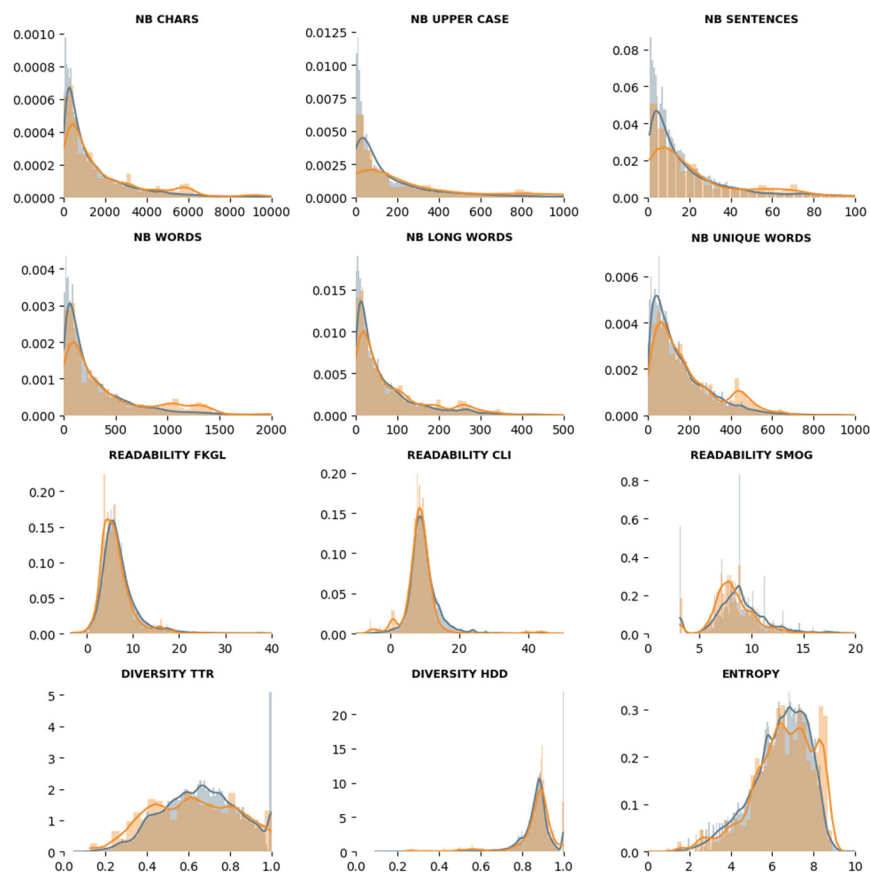


Figure 2. Textometric analysis of product descriptions. The chart illustrates a comparative analysis with scam-related advertisements depicted in orange at the top, while other advertisements are represented in grey.

However, the frequency distribution of word counts used by reported scammers, particularly for unique words, exhibits a notable peak ranging from 1000 to 1500 words and between 400 and 500 unique words which are also associated with high entropy (see Figure 2). Indeed, these texts include lengthy descriptions that incorporate details such as purchase rules, (non-)refund policies, delivery times, and other FAQ-related information. In some cases, the vendor's PGP key is provided within the message so that the buyer can verify the seller's identity through encrypted messaging. Overall, these messages seem to contain a substantial amount of information aimed at maximising buyer trust. They feature phrases like 'we never should SCAM you and we know how it's to get scammed'.

Additionally, a focused analysis was conducted at the peak of texts with low 'readability-cli' scores. These texts primarily contain repetitions of special characters such as '=', '-', '+', '*', '#', and a substantial number of emojis. Indeed, Coleman and Liau's (1975) algorithm relies on the number of characters instead of the number of syllables or words. By filtering these tokens, it was possible to identify types of advertisements that maintain a low-level readability score, which are very brief texts (3–10 words). Within this group, 'custom listing' (Soska and Christin 2015) and 'tip jar' listings were detected. Other texts contain lists of short sentences.

As shown in Figures 3 and 4, the POS-tagging analysis of the listings and profiles did not reveal any significant differences for sellers labelled as scammers. Principal component analysis (PCA) conducted with every available tag revealed that the data is overall inseparable (see Figures 3 and 4). Except for some outliers, PCA does not allow for a clear distinction between specific groups.

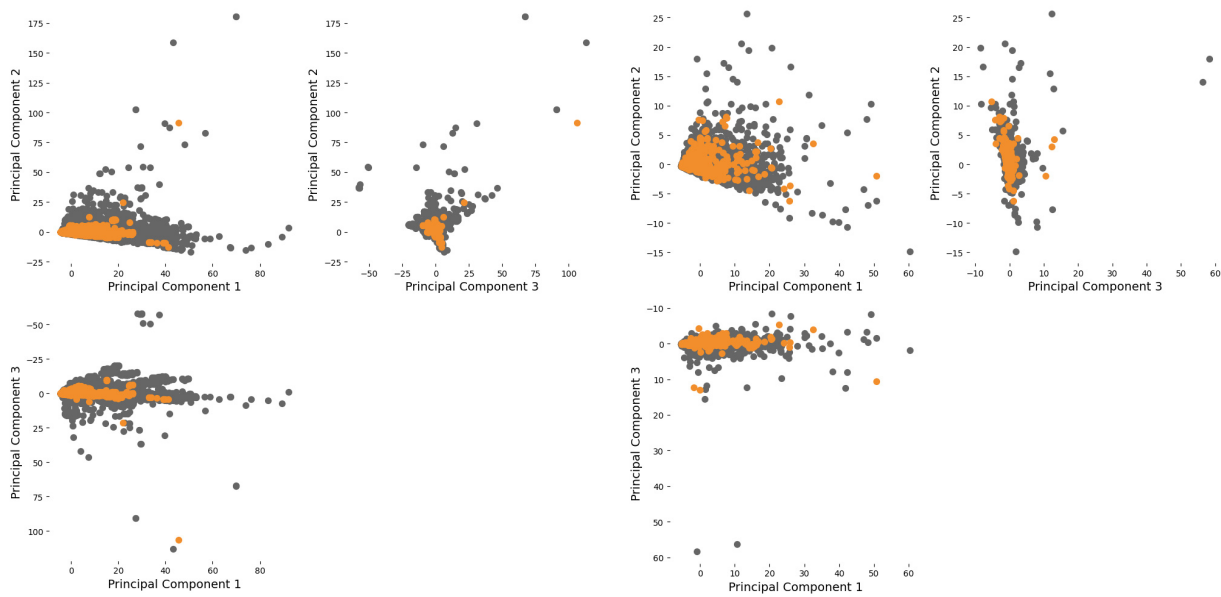


Figure 3. Result of the three-dimensional principal component analysis performed on the 66 POS-tags (listings on the left and profiles on the right). The chart illustrates a comparative analysis with scam-related advertisements depicted in orange at the top, while other advertisements are represented in grey.

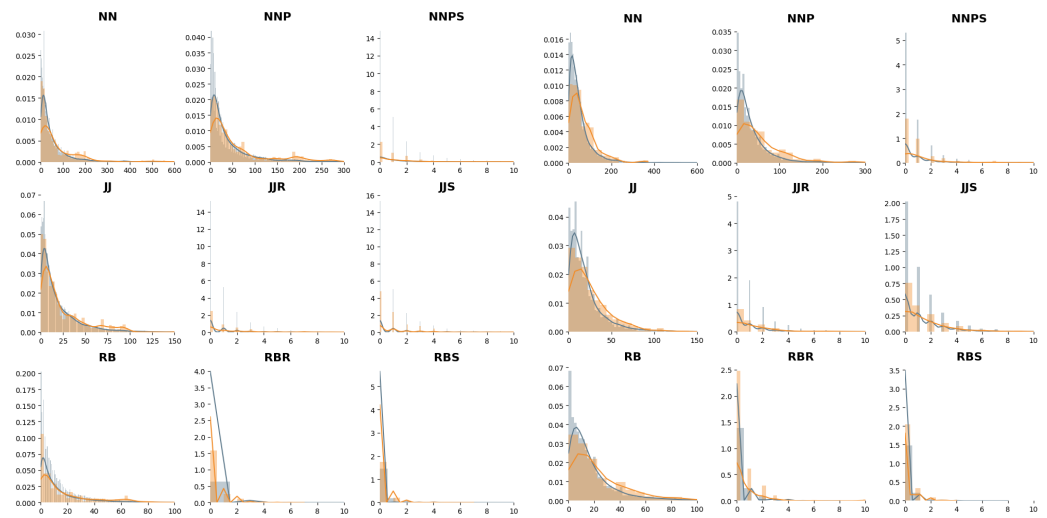


Figure 4. POS-tagging analysis of product descriptions (left) and profiles (right) with eight tags (NN—Noun, singular or mass, NNP—Proper noun, singular, NNPS—Proper noun, plural, JJ—Adjective, JJR—Adjective, comparative, JJS—Adjective, superlative, RB—Adverb, RBR—Adverb, comparative, RBS—Adverb, superlative). The chart illustrates a comparative analysis with scam-related advertisements depicted in orange at the top, while other advertisements are represented in grey.

4.2. Analysis of the N-Grams

Figure 5 illustrates that no N-gram distinctly stands out in differentiating reported scammers from other vendors. Indeed, an N-gram would be inherently discriminatory if it were positioned in the top left for words specific to them and in the bottom right for words specific to other vendors. Indeed, all the words used by more than 30% of reported scammers have a likelihood ratio ranging between 0.9 and 1.9. Therefore, no specific word seems to be discriminatory. Only the bigram ‘high quality’ appears to be relatively frequent, found in 50% of listings as opposed to 37% in those of other vendors.

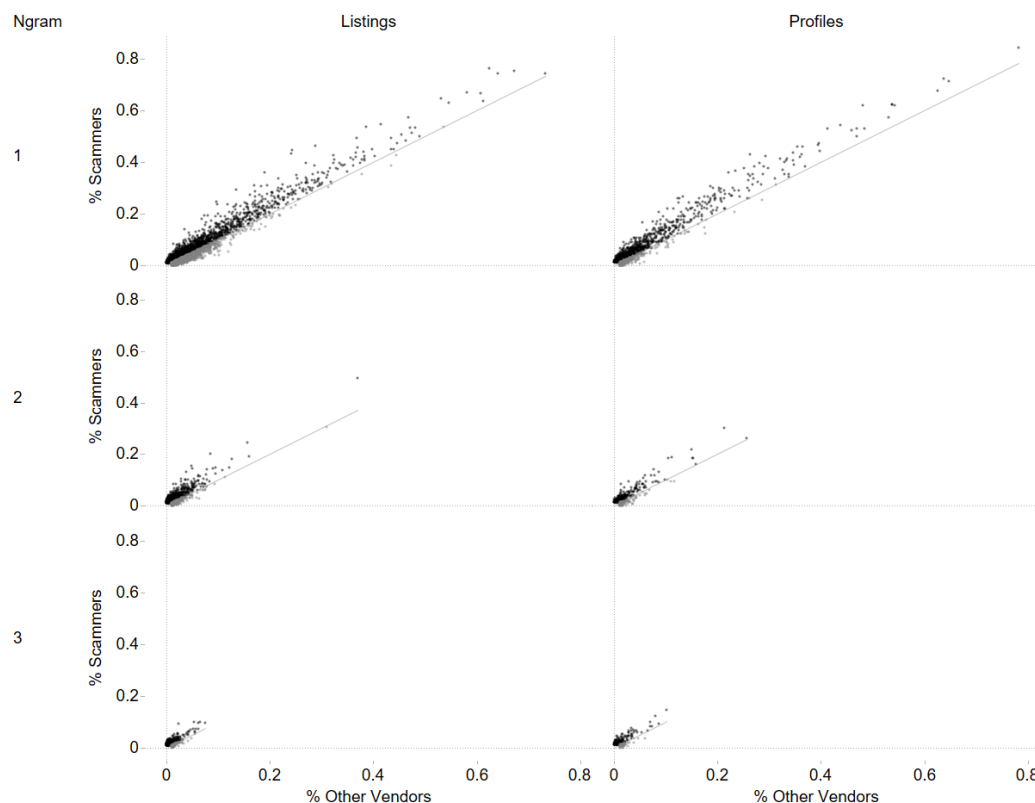


Figure 5. Global overview of the analysis of N-grams. Each point represents a specific N-gram plotted based on its usage frequency by reported scammers (Y-axis) and other vendors (X-axis).

4.2.1. Analysis of the Product's Descriptions

Numerous words and N-grams within the dataset pertain to marketed products (see Figures 6 and 7), while the remaining subset aligns with the lexical domain of sales. Figure 6 focuses on unigrams used by more than 30% of the reported scammers. Terms with the highest LRs are linked to the description of the product type, which is mainly related to drugs. Notably, most terms exhibit an LR falling within the range of 1.1 to 1.3, with none registering below 1. This implies that except for 'address' (LR = 0.9), all unigrams analysed in this context are slightly more prevalent among reported scammers. Most of these terms are in the lexical field of shipping and sales conditions.

Quality and price: The only recurrent bigram is 'high quality', which is employed by almost 50% of reported scammers; its LR of 1.4 indicates that it is only 1.4 times more prevalent among scammers than legitimate vendors. The trigram 'high quality product' is used similarly among both groups and might be a common marketing phrase used to build confidence in the product, regardless of the vendor's legitimacy. The percentage of reported scammers utilising other bigrams is notably low, except for 'lab test' and 'good quality' which are also related to the 'Quality' topic. Additionally, the words 'high dose', 'high purity', and 'high THC', which are grouped in the 'high' category, can also be integrated into the lexical field of product quality.

Problem resolution, communication, and trust: The forms 'reship policy', 'negative feedback', 'refund policy', and 'refund reship' that we decided to regroup with the negation forms 'doesn't' and 'don't' share a commonality in the context of what we called 'problem' (i.e., problem-resolution phrases). They are terms associated with policies, procedures, and customer service aspects, particularly in relation to the handling of disputes, returns, and customer satisfaction. They can be indicative of a seller's approach to handling issues like returns (reship and refund policy), customer complaints (negative feedback), and general terms of service or product guarantees. Communication-related trigrams such as 'question feel free', 'free to contact', and 'let us know' are also quite common. Lastly,

‘term and condition’ is also a common phrase used frequently in scams (6.5%) and other listings (6.4%). This could be because all vendors want to establish a sense of formality and legitimacy to increase trust.

Product-specific terms are mainly linked to drug names like ‘2cb pill’, ‘ketamine s’ (linked to the trigrams ‘ketamine s isomer’ and ‘s isomer ketamine’), ‘og kush’, ‘mg mdma’, and ‘xtc pill’, which is not surprising given that these cryptomarkets are primarily used for drug sales.

Overall, while certain bigrams and trigrams are used more by reported scammers, many are also common in the overall corpus. This indicates the complexity of distinguishing them based solely on N-gram analysis. It suggests the need for more sophisticated methods or additional variables to accurately identify scam listings.

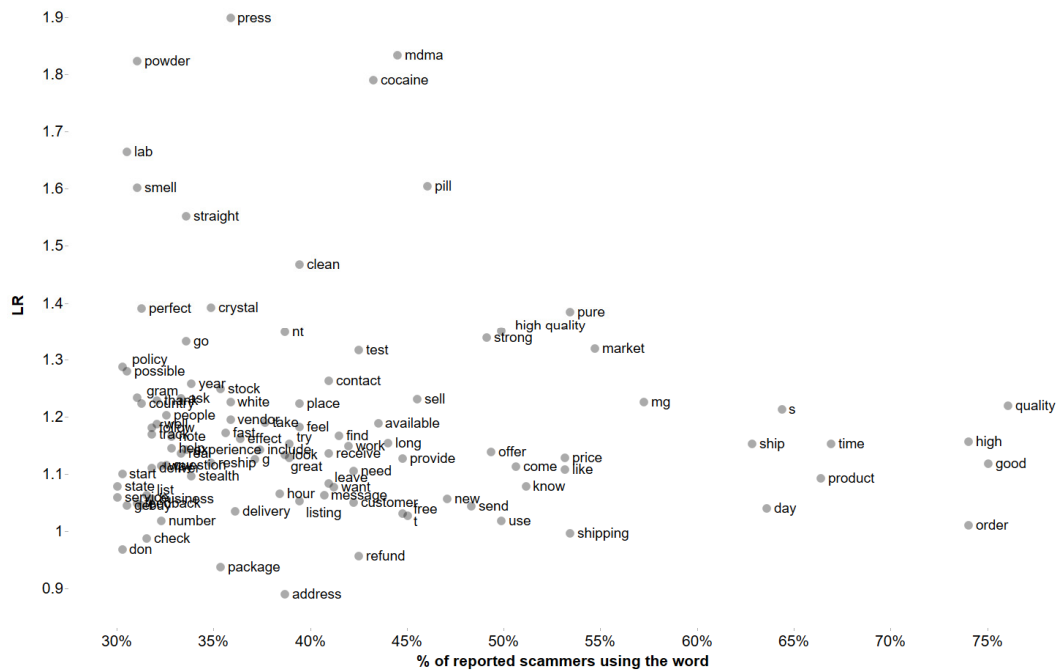


Figure 6. Likelihood ratio of unigrams in the corpus of product descriptions.

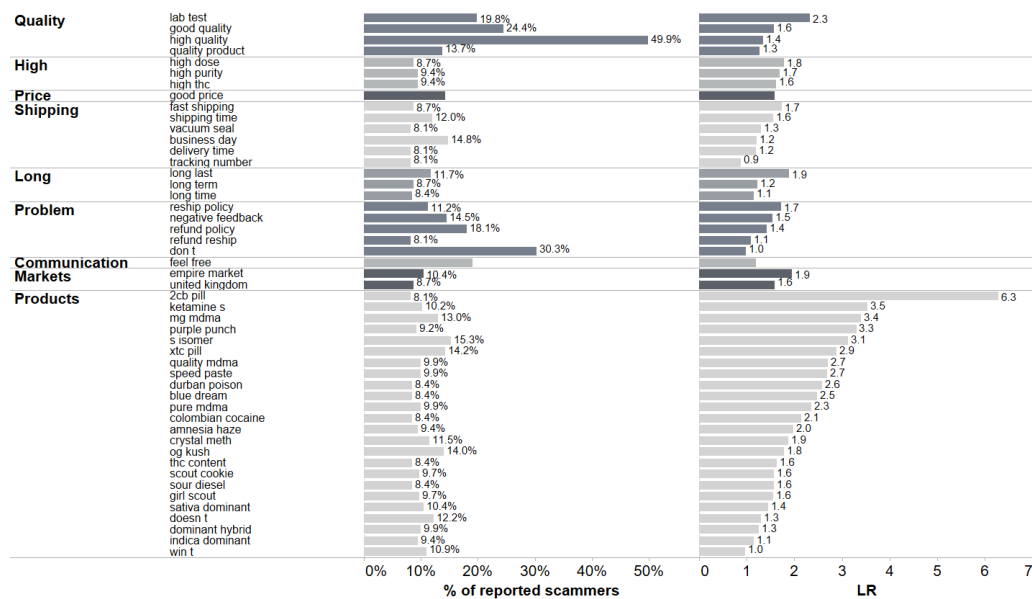


Figure 7. Cont.

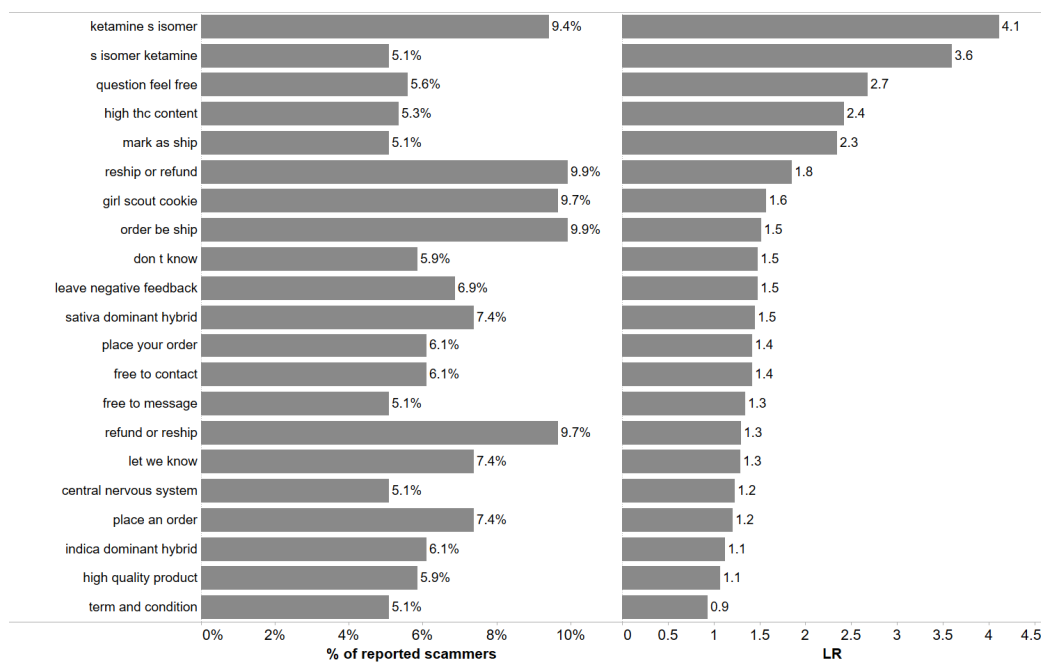


Figure 7. Bigram and trigram analysis of the listing corpus.

4.2.2. Analysis of the Profile Descriptions

This analysis offers insights into the linguistic patterns prevalent in the profile descriptions of reported scammers. The examination of single-word usages is detailed in Figure 8, while the analysis of bigrams and trigrams is delineated in Figure 9. These figures collectively reveal the verbal strategies scammers employ in their profiles.

The lexical domains of shipping and sales persist consistently (see Figure 8). Most unigrams are employed by 30–50% of reported scammers, with LR values between 1 and 1.3. This outcome closely mirrors that obtained from the listing corpus. Notably, the term ‘order’ is used by 84% of reported scammers but with an LR of 1.1, indicating that its usage is not significantly higher among scammers compared to legitimate vendors. It is worth noting that unigrams with the highest LR values (ranging from 1.55 to 1.65) are partially associated with shipping (‘country’, ‘way’, and ‘fast’).

Quality and price: The high incidence of ‘high quality’ in scam listings indicates that reported scammers recurrently advertise the quality of their products. However, like the terms ‘good quality’ and ‘good price’, it is quite common in the overall corpus, potentially diluting its effectiveness as a distinguishing feature.

Problem resolution, communication, and trust: The term ‘customer support’ has a higher likelihood ratio, which indicates it is six times more common in reported scammers’ profiles. This suggests that scammers may prioritise establishing a facade of trust and support to attract and reassure potential customers. The higher occurrence of ‘reship policy’ and ‘refund policy’ in scam listings could be an effort to appear as though they provide customer protection and service, which could lower the perceived risk. Notably, no single trigram is overwhelmingly used, as even the most frequently trigram used by reported scammers (‘refund or reship’) occurs in only 14.7% of listings compared to 10.2% of non-scam listings. This suggests a subtle overlap in the language used by both groups of sellers. Trigrams such as ‘reship or refund’ and ‘leave negative feedback’ are quite common in scammers’ profiles. However, the difference is not stark, with ‘leave negative feedback’ appearing in 10% of scam listings versus 6.9% of clean listings. ‘Feel free’, ‘free to contact’, and ‘customer service’ are common in both scam and other profiles. The data show that reported scammers do not use a drastically distinct set of bigrams and trigrams compared to other vendors.

Shipping and time: Seller profiles contain more information than their listings about shipping times: ‘shipping time’ (18.2%), ‘business day’ (18.2%), and ‘delivery time’ (12.9%). This is probably in part due to the period of the collection, which was during COVID-19. More globally reported scammers frequently use shipping-related terms. Forms like ‘track order’, ‘post office’, ‘po box’, ‘postal code’, and ‘address format’ are associated with the logistics of sending and receiving goods, which might emphasise the need to guide and reassure buyers of the transaction process. Overall, scammers might strategically use shipping-related forms to build credibility and simulate reliability in the delivery process. Nevertheless, these terms relating to standard business operations and logistics are less distinct and may not be reliable indicators on their own.

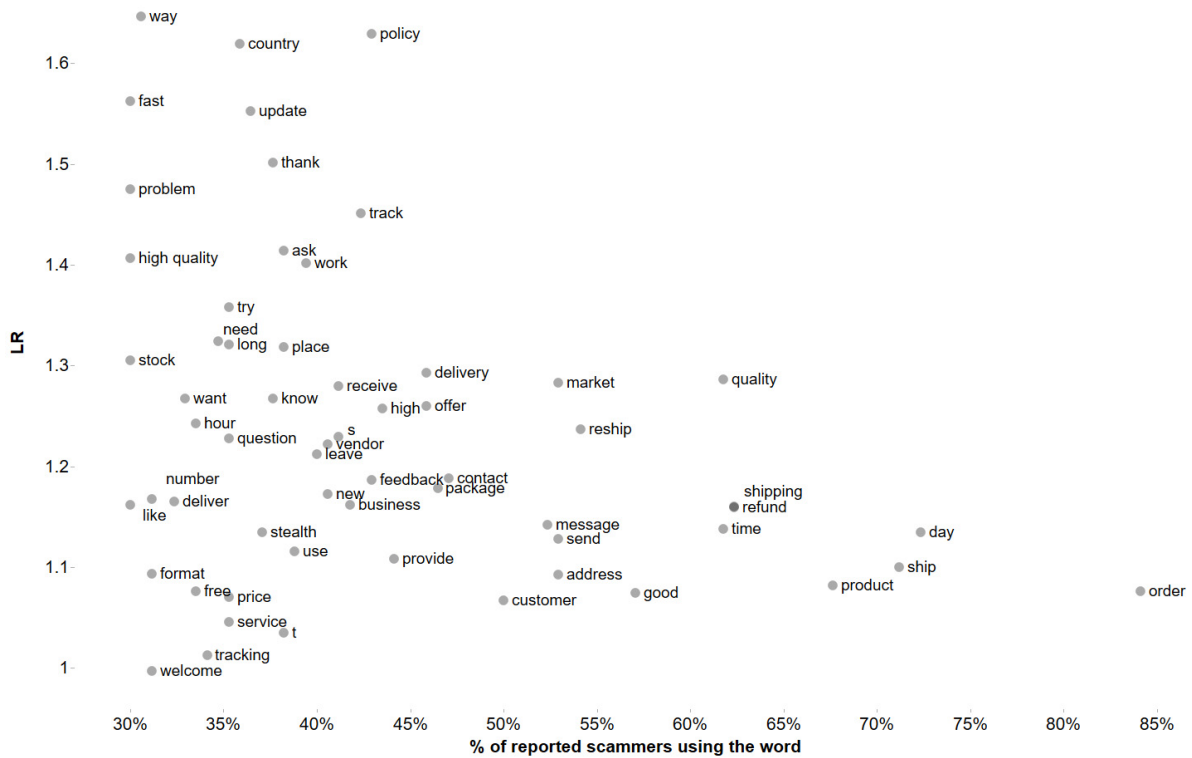


Figure 8. Likelihood ratio of unigrams on the corpus of profiles.

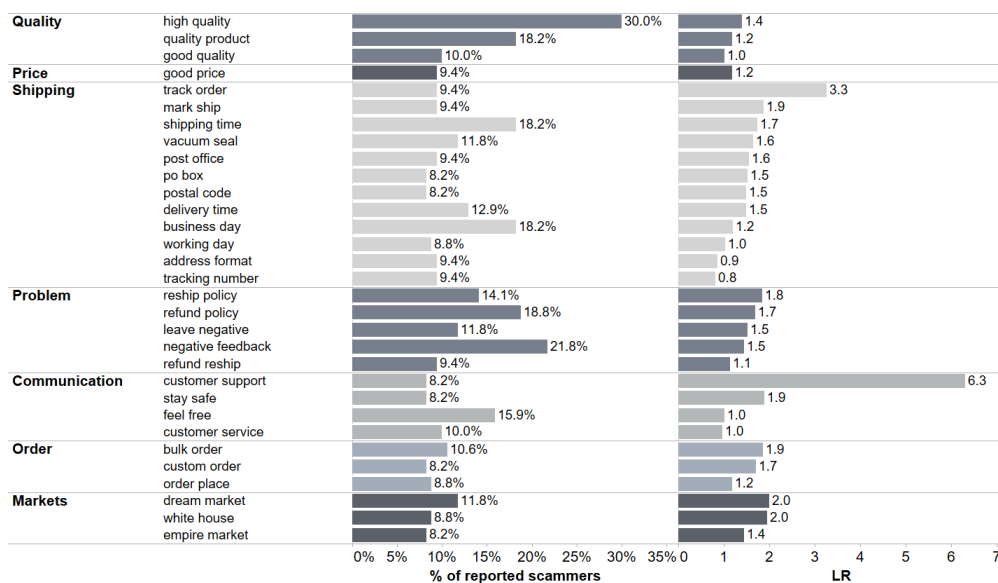


Figure 9. Cont.

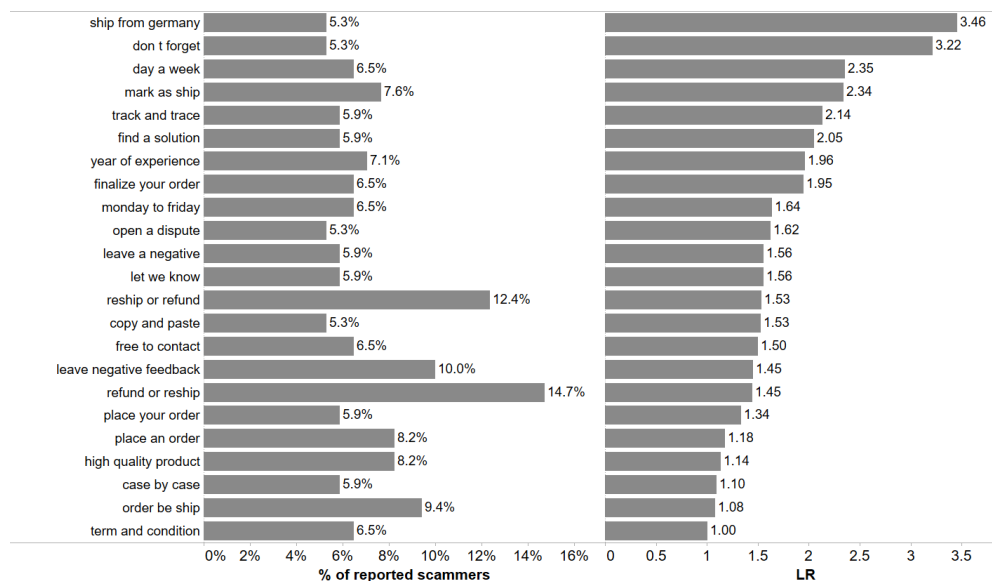


Figure 9. Bigram and trigram analysis of the profile corpus.

Order types: Mentions of ‘bulk order’ and ‘custom order’ in scam listings highlight sellers offering deals that appear more personalised or financially beneficial.

Marketplace names: References to specific markets, such as ‘dream market’, ‘white house’, and ‘empire market’, are used by sellers to link their current profiles with accounts on other marketplaces.

In summary, reported scammers seem to use language that aims to build trust, emphasise the shipping process, and stress the quality of their products to entice potential buyers. While some terms are more prevalent in scam listings, many are also commonly used by all vendors, which presents a challenge for distinguishing between the two based on language alone.

5. Discussion

What really is a scammer? The results obtained in this study might be explained by the fundamental definition of what is referred to as a ‘scammer’ on cryptomarkets. The initial recognition of scammers, leading to the construction of the corpus, was based on self-regulation. The demarcation between scammers and legitimate vendors is contingent upon user-reported allegations on the Dread forum and thus lacks assurance that the sellers accused of perpetrating scams are unequivocally scammers. This reflects a broader issue within online marketplaces, where accusations can be both a reflection of true misconduct and a tactic in competitive sabotage, as noted in studies of online behaviour and marketplace dynamics (Soska and Christin 2015; Morselli et al. 2017).

Furthermore, the taxonomy used for categorising these vendors fails to accommodate the conceptual distinctions inherent in selective scamming and exit scamming (Morselli et al. 2017; Bancroft et al. 2020; Décary-Héту et al. 2018; Morselli et al. 2017). Selective and exit scammer vendors engage in fraudulent activities sporadically, maintaining conventional vending practices for the remainder of their operations. Consequently, their indistinguishability from standard vendors can be attributed to this phenomenon. In the context of selective scamming, vendors conduct most of their transactions legitimately, interspersing them with occasional deceptive practices. In contrast, exit scammers perpetuate a facade of normalcy in their transactions until a strategic juncture at which they abscond with funds and vanish from the platform. Such mixed behaviour is also described by Markowitz (2023), who notes the nuanced dynamics of deception within communication, challenging the traditional binary categorisation of statements as purely false or truthful. This indicates that the embedding of deceptive elements into truthful content is more complex than previously thought, and it calls for a deeper understanding of how deceptive elements

are interwoven into communications. The observation is also underscored by [Hauch et al. \(2015\)](#), who found consistent, albeit small, correlations between specific language patterns and deception.

Consequently, our analysis of textual statistics, including the numbers of characters, words, long words, unique words, and sentences, as well as the syntactic tags, exhibited no statistically significant divergences between the profile descriptions and advertisements. This suggests that textual analysis alone may not be sufficient for scam detection, which indicates a need for multimodal approaches that integrate other indicators such as the number of sales, the number of won and lost disputes, scores, or the quantities of positive and negative feedback. Textometric indicators, however, helped to identify peculiar ads in which sellers created longer descriptions with more details such as purchase rules, (non-)refund policies, and other FAQ-related information to increase trust. These indicators thus support the selection of pertinent documents on which a qualitative analysis can be focused.

The analysis of N-grams in both the listings and the profiles in our corpus revealed only minor differences between reported scammers and all other vendors regarding their content. It is also worth noting the relatively low percentages of those N-grams across the corpus, which indicates that there is not a ‘silver bullet’ bigram or trigram that clearly flags a listing as a scam. This could make it difficult for automatic detection systems to rely solely on these N-grams without a significant number of false positives. Nonetheless, one outcome of the N-gram analysis supports the differentiation: we observed an overuse of the lexicon pertaining to the ‘Quality and Price’, ‘Problem Resolution, Communication, and Trust’ and ‘Shipping’ topics. This suggests that scammers might offer more detailed information about transactions and delivery, potentially alleviating customer concerns. In these environments, where physical goods cannot be inspected before purchase, the trustworthiness and reputation of a seller are paramount. This pattern could indicate a strategic overcompensation, aligning with the deception strategies described in the literature, in which scammers create narratives to build trust ([Button et al. 2014](#); [Rosy and Ribaux 2020](#)).

Additionally, the hypothesis that vendors adapt their descriptions in response to accusations of scamming remains a plausible explanation for the linguistic patterns we observed. In the context of cryptomarkets, when accusations of scamming arise, vendors might modify their language to distance themselves from the behaviours associated with scammers, thereby preserving or rehabilitating their reputations. Vendors accused of scamming may strategically use language that emphasises honesty, reliability, and other trust-building characteristics. They might also avoid certain terms that have become associated with scamming behaviours due to forum discussions or community warnings. This raises the question of how to detect and analyse the absence of language traces. Vendors might also employ counter-allegations or other defensive strategies in their descriptions, directly addressing and refuting scamming accusations, which could change the linguistic patterns observed in their profiles. Such an analysis could improve the understanding of non-violent conflict resolution strategies used by sellers, like negotiation, avoidance, and third-party intervention ([Morselli et al. 2017](#)).

6. Conclusion and Prospects for Subsequent Research

In conclusion, the main hypothesis—that it is possible to distinguish reported scammers from legitimate sellers on cryptomarkets using language traces—is refuted by most of the experimental results. This highlights the challenges of using linguistic analysis alone for scam detection in those virtual settings and suggests the need to combine language traces with transactional traces to effectively distinguish between scammers and legitimate vendors. The difficulty of discerning behaviours based on language traces in cryptomarkets can be regarded as a preventive argument aimed at alerting prospective buyers to these platforms. Globally, we observed a pronounced, albeit modest, emphasis on language related to ‘Quality and Price’, ‘Problem Resolution, Communication and Trust’,

and ‘Shipping’. These findings led us to hypothesise that scammers may frequently provide extensive details about transactions and delivery. This could be a strategic approach to address customers’ potential apprehensions, aiming to establish a semblance of trust and reliability in their operations.

Further investigations are, however, needed. A prospective avenue for subsequent inquiry may entail refining the categorisation of vendors identified as scammers in Dread forum posts. Subsequently, future research efforts could explore the possibility of implementing a more nuanced classification schema for these vendors with the intent of distinguishing various typologies of fraudulent behaviours. It would also be interesting to determine whether it is possible to distinguish genuine reviews from fake ones on the Dread forum based on linguistic traces, in order to enrich the research ground.

Our present analytical methodology encompasses the application of machine learning classification algorithms and topic modelling, enhanced by vectorisation techniques like the tf-idf metric. We have experimented with various classifiers, including multinomial Naive Bayes, support vector machines, and Random Forest. Preliminary findings are revealing intriguing aspects, particularly regarding how vendors establish communication channels with buyers. A notable trend is the encouragement of direct contact through encrypted social media platforms such as Telegram and Wickr. These results, while promising, demand a more thorough analysis. The disparity in the volume of documents between reported scammers and other vendors, coupled with the necessity of categorising different types of scammers more precisely, necessitates a cautious approach before drawing definitive conclusions and publication.

With regard to the pre-processing applied to the texts, we made the choice to eliminate stopwords in order to retain only the main words. However, several studies in the literature have suggested that stopwords can be significant elements, and function words have proved useful in previous authorship attribution studies (Arun et al. 2009). It would therefore be interesting to analyse these stopwords in a future study to determine whether they can discriminate between scammers and legitimate sellers.

Moreover, it was observed that a subset of seventeen profiles bore the singular description ‘banned’. This unequivocally signifies that the respective vendors associated with these profiles have been banished from the platform. The presence of such data provides some form of ground truth regarding the nature of these vendors. Given the longitudinal nature of the data collection, which spanned an extended timeframe, it is feasible to trace the trajectories of these vendors by examining the evolution of their profiles and listings leading up to their expulsion from the platform. Consequently, we envisage an analysis of the trajectory that could shed light on the developmental patterns of these profiles before the vendors’ eventual banishment. Indeed, the adaptive nature of language in vendor descriptions could reflect a complex interplay of reputation management, community interaction, and possibly deceptive strategies. This can be particularly revealing when combined information is extracted from transactional traces, such as the number of sales, the number of won and lost disputes, the score, or the quantities of positive and negative feedback. This information may show a pattern of escalation or changes in behaviour prior to the ban. Future research could benefit from examining these changes over time, potentially applying longitudinal text analysis to capture the evolution of language in response to community feedback and accusations. This would provide a richer understanding of the dynamics at play in cryptomarket ecosystems. It might also be interesting to use a corpus of ads and profiles from legitimate market platforms on the web to see if behaviours, and consequently language traces, differ.

Author Contributions: Conceptualization, C.D., J.L. and Q.R.; Methodology, C.D., J.L. and Q.R.; Validation, J.L. and Q.R.; Formal analysis, C.D. and Q.R.; Investigation, C.D.; Writing—original draft, C.D.; Writing—review & editing, C.D., J.L. and Q.R.; Visualization, C.D. and Q.R.; Supervision, J.L. and Q.R.; Project administration, J.L. All authors have read and agreed to the published version of the manuscript.


Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Navigation tabs: About, Positive Feedback, Negative Feedback, Neutral Feedback, Left Feedback, PGP



Hello and Welcome to our online store where you will find the highest quality of product in the market

Cannazon and Apollon

Please make sure your address is encrypted

Our Inventory:

Weed:

- Kalashnikova
- Hash:
- Morrocan Hash

We aim to ship very quickly

Delivery Schedule:

Cut off timings

- Monday - 3pm
- Tuesday - 3pm
- Wednesday - 3pm
- Thursday - 3pm
- Friday - 3pm

Please message us if the cutoff time has gone and you still need your order dispatched the same day

Figure A1. Example of Vendor Profile on Empire Market.

Description	Feedback	Refund policy
<p>10 Gram *** Das Beste Oder Nix*** 92.0% Reines KOKS ***</p> <p>DEUTSCH</p> <p>Einfach probieren Leute. Das Zeug ist mega. Krümmelt wie Kreide. Keine Razierklinge nötig.</p> <p>DAS BESTE MATERIAL IN DER SCHWEIZ</p> <p>★PROMOTION★ 10 G KOKS AAA+++ HÖCHSTE QUALITÄT</p> <p>FLOCKEN, UNBEHANDELT UND 92.0% REIN ★FULL ESCROW★ ★★</p> <p>★ PROMOTION SALE PRICE</p> <p>★ 10 Gram ★ Bolivianisches Kokaine ★ Flakes Fishscale ★ REINHEITS GRAD 92.0% ★ Straight from the Brick ★ NIEDRIGSTER PRICE/HÖCHSTE QUALITÄT GARANTIERT ★ 99% of orders arrive in 2 days - Shipping = NUR VON UND IN DIE SCHWEIZ ★ SAUBERES UND ANGENEHMES HIGH ★ STEALTH SHIPPING ★ 5 Euro Shipping and handling A-POST (ABSOLUT NO RESHIP) ★ 10 Euro SHIPPING AND HANDLING Option MIT 100% RESHIP ★★ READ THE REFUND & RESHIP POLICY ★★ FOR FURTHER QUESTIONS CONTACT US!!</p> <p>ENGLISH</p> <p>★PROMOTION★ 10 G COCAINE AAA+++ HIGH QUALITY Flakes Fishscale uncut above 92.0% ★FULL ESCROW★ ★★</p> <p>THE BEST COCAINE IN ALL OF SWITZERLAND</p> <p>★ PROMOTION SALE PRICE</p> <p>★ 10 Gram ★ Bolivian Cocaine ★ Flakes Fishscale ★ Purity level above 92.0% ★ Straight from the Brick ★ LOWEST PRICE/HIGHEST QUALITY GUARANTEE ★ 99% of orders arrive in 2 days - Shipping = Only from and to Switzerland ★ Clean and long lasting strong high ★ STEALTH SHIPPING ★ 5 Euro SHIPPING COST A-Post (ABSOLUT NO RESHIP) ★ 10 Euro SHIPPING COST Option WITH 100% RESHIP ★★ READ THE REFUND & RESHIP POLICY ★★ FOR FURTHER QUESTIONS CONTACT US!!</p>		

Figure A2. Example of Product Description on Empire Market. Each seller chooses their own layout to highlight the information they wish to communicate to their customers.

Note

¹ [https://en.wikipedia.org/wiki/Dread_\(forum\)](https://en.wikipedia.org/wiki/Dread_(forum)), accessed 15 November 2022.

References

- Addawood, Aseel, Adam Badawy, Kristina Lerman, and Emilio Ferrara. 2019. Linguistic cues to deception: Identifying political trolls on social media. Paper presented at International AAAI Conference on Web and Social Media, Munich, Germany, June 11–14; pp. 15–25.
- Aitken, Colin, and Franco Taroni. 2005. Statistics and the Evaluation of Evidence for Forensic Scientists. *Significance* 2: 40–43.
- Arun, Rajkumar, Venkatasubramaniyan Suresh, and CE Veni Madhavan. 2009. Stopword graphs and authorship attribution in text corpora. Paper presented at 2009 IEEE International Conference on Semantic Computing, Berkeley, CA, USA, September 14–16; pp. 192–96.
- Bancroft, Angus, Tim Squirrell, Andreas Zaunseder, and Rafanell Irene. 2020. Producing Trust Among Illicit Actors: A Techno-Social Approach to an Online Illicit Market. *Sociological Research Online* 25: 456–72.

- Bozza, Silvia, Claude-Alain Roten, Antoine Jover, Valentina Cammarota, Lionel Pousaz, and Franco Taroni. 2023. A model-independent redundancy measure for human versus ChatGPT authorship discrimination using a Bayesian probabilistic approach. *Scientific Reports* 13: 19217. [CrossRef] [PubMed]
- Button, Mark, Carol McNaughton Nicholls, Jane Kerr, and Rachael Owen. 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47: 391–408.
- Charaudeau, Patrick. 1992. Grammaire du sens et de l'expression. *Hachette, epub ahead of print*.
- Chaski, Carole E. 2005. Who's At The Keyboard? Authorship Attribution in Digital Evidence Investigations. *International Journal of Digital Evidence* 4: 14.
- Christin, Nicolas. 2013. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. Paper presented at 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, May 13; pp. 213–24. Available online: <https://dl.acm.org/doi/10.1145/2488388.2488408> (accessed on 9 November 2023).
- Coleman, Meri, and Ta Lin Liau. 1975. A computer readability formula designed for machine scoring. *Journal of Applied Psychology* 60: 283–84. [CrossRef]
- Degeneve, Clara, Julien Longhi, and Quentin Rossy. 2022. Analysing the digital transformation of the market for fake documents using a computational linguistic approach. *Forensic Science International: Synergy* 5: 100287. [PubMed]
- Décary-Hétu, David, Masarah Paquet-Clouston, Martin Bouchard, and Carlo Morselli. 2018. *Patterns in Cannabis Cryptomarkets in Canada in 2018*. Ottawa: Public Safety Canada.
- Fobbe, Eilika. 2020. Text-Linguistic Analysis in Forensic Authorship Attribution Forensic Linguistics: New Procedures and Standards. *International Journal of Language & Law* 9: 93–114.
- Gibbons, John, and M. Teresa Turell, eds. 2008. *Dimensions of Forensic Linguistics*. AILA applied linguistics series v. 5. Amsterdam and Philadelphia: John Benjamins Pub.
- Hancock, Jeffrey T., Jennifer Thom-Santelli, and Thompson Ritchie. 2004. Deception and design: The impact of communication technology on lying behavior. Paper presented at SIGCHI Conference on Human Factors in Computing Systems, Vienna, Austria, April 24–29; pp. 129–34.
- Hauch, Valerie, Iris Blandón-Gitlin, Jaume Masip, and Siegfried L. Sporer. 2015. Are computers effective lie detectors? A meta-analysis of linguistic cues to deception. *Personality and Social Psychology Review* 19: 307–42. [CrossRef] [PubMed]
- Jacquart, Bérandère, Adrien Schopfer, and Quentin Rossy. 2021. Mules financières: Profils, recrutement et rôles de facilitateur pour les escroqueries aux fausses annonces. *Revue Internationale de Criminologie et de Police Technique et Scientifique* 4/21: 409–26.
- Jakupov, Alibek, Julien Mercadal, Besma Zeddini, and Julien Longhi. 2022. Analyzing Deceptive Opinion Spam Patterns: The Topic Modeling Approach. Paper presented at 2022 IEEE 34th International Conference on Tools with Artificial Intelligence (ICTAI), Macao, China, October 31–November 2; pp. 1251–61. Available online: <https://ieeexplore.ieee.org/document/10097994/> (accessed on 1 May 2023).
- Junger, Marianne, Luka Koning, Pieter Hartel, and Bernard Veldkamp. 2023. In their own words: Deception detection by victims and near victims of fraud. *Frontiers in Psychology* 14: 1135369. [CrossRef]
- Juola, Patrick. 2021. Verifying authorship for forensic purposes: A computational protocol and its validation. *Forensic Science International* 325: 110824. [CrossRef]
- Juola, Patrick, John Sofko, and Patrick Brennan. 2006. A Prototype for Authorship Attribution Studies. *Digital Scholarship in the Humanities* 21: 169–78. [CrossRef]
- Longhi, Julien. 2021. Using digital humanities and linguistics to help with terrorism investigations. *Forensic Science International* 318: 110564. [CrossRef] [PubMed]
- Markowitz, David M. 2023. Deconstructing Deception: Frequency, Communicator Characteristics, and Linguistic Features of Embeddedness. Available online: <https://doi.org/10.31234/osf.io/tm629> (accessed on 9 April 2024).
- Markowitz, David M., Jeffrey T. Hancock, Michael T. Woodworth, and Maxwell Ely. 2023. Contextual considerations for deception production and detection in forensic interviews. *Frontiers in Psychology* 14: 1134052. [CrossRef] [PubMed]
- Martin, James. 2013. Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice* 14: 351–67.
- Morselli, Carlo, David Décary-Hétu, Masarah Paquet-Clouston, and Judith Aldridge. 2017. Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review* 27: 237–54. [CrossRef]
- Ott, Myle, Yejin Choi, Claire Cardie, and Jeffrey T. Hancock. 2011. Finding Deceptive Opinion Spam by Any Stretch of the Imagination. Paper presented at 49th Annual Meeting of the Association for Computational Linguistics, Portland, OR, USA, June 19–24; pp. 309–19.
- Pavlou, Paul A., and Angelika Dimoka. 2006. The Nature and Role of Feedback Text Comments in Online Marketplaces: Implications for Trust Building, Price Premiums, and Seller Differentiation. *Information Systems Research* 17: 392–414. [CrossRef]
- Przepiorka, Wojtek, Lukas Norbutas, and Rense Corten. 2017. Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs. *European Sociological Review* 33: 752–64. [CrossRef]
- Renaut, Laurène, Laura Ascone, and Julien Longhi. 2017. De la trace langagière à l'indice linguistique: Enjeux et précautions d'une linguistique forensique. *Ela. Études de Linguistique Appliquée*, 423–42.
- Ribaux, Olivier. 2023. *De la Police Scientifique à la Tracologie*, 2nd ed. Sciences forensiques. Lausanne: EPFL Press. Available online: <https://www.epflpress.org/produit/672/9782889155446/de-la-police-scientifique-a-la-tracologie> (accessed on 24 October 2023).

- Rossy, Quentin, and David Décary-Héту. 2017. Internet traces and the analysis of online illicit markets. In *The Routledge International Handbook of Forensic Intelligence and Criminology*, 1st ed. Edited by Quentin Rossy, David Décary-Héту, Olivier Delémont and Massimiliano Mulone. London: Routledge, pp. 249–63. Available online: <https://www.taylorfrancis.com/books/9781134888955/chapters/10.4324/97811315541945-21> (accessed on 13 February 2021).
- Rossy, Quentin, and Olivier Ribaux. 2020. Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms. *European Journal on Criminal Policy and Research*, Epub ahead of print. [CrossRef]
- Roux, Claude, Rebecca Bucht, Frank Crispino, Peter De Forest, Chris Lennard, Pierre Margot, Michelle D. Miranda, Niamh NicDaeid, Olivier Ribaux, Alastair Ross, and et al. 2022. The Sydney declaration—Revisiting the essence of forensic science through its fundamental principles. *Forensic Science International* 332: 111182.
- Soska, Kyle, and Nicolas Christin. 2015. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium*, Epub ahead of print.
- Taroni, Franco, Paolo Garbolino, Silvia Bozza, and Colin Aitken. 2022. The Bayes' factor: The coherent measure for hypothesis confirmation. *Law, Probability and Risk* 20: 15–36. [CrossRef]
- Titus, Richard M., Fred Heinzelmann, and John M. Boyle. 1995. Victimization of persons by fraud. *Crime & Delinquency* 41: 54–72.
- Tzanetakis, Meropi, Gerrit Kamphausen, Bernd Werse, and Roger von Laufenberg. 2016. The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy* 35: 58–68. [CrossRef] [PubMed]
- van Deursen, K. 2021. The Effect of Feedback Polarity on the Sales and Prices on Cryptomarket AlphaBay. Bachelor thesis, Utrecht University, Utrecht, The Netherlands.
- Vidros, Sokratis, Constantinos Koliass, Georgios Kambourakis, and Leman Akoglu. 2017. Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset. *Future Internet* 9: 6. [CrossRef]
- Wright, David. 2014. *Stylistics Versus Statistics: A Corpus Linguistic Approach to Combining Techniques in Forensic Authorship Analysis Using Enron Emails*. Leeds: University of Leeds.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.