Shining a Light on AI: Ensuring Vendor Transparency in Data Sourcing and Delivery

Author: Brian P. Mohr, brian@cybermohr.com
Advisor: *Dr. Timothy Proffitt*

Accepted: *December 16th, 2023*

Abstract

Amidst the proliferation of AI solutions, the focus lies in evaluating transparency, undisclosed system modifications, and data exfiltration within the privacy policies of vendors providing desktop applications, browser plug-ins, and browser-only AI solutions. Specifically, the research investigates whether these terms of service provide clear information regarding data collection practices and whether there is any deviation from the documented procedures, focusing on whether excessive data is sent to the AI system. This research expands upon prior work, emphasizing the need to mention spyware in End User License Agreements (EULAs). Doing so offers a broader perspective on data privacy and system transparency in various AI solutions. It contributes to a better understanding of their implications and promotes trust and accountability in the AI ecosystem.

1. Introduction

In recent years, the world has witnessed an unprecedented explosion of AI solutions, marking a profound transformation in how technology interacts with our daily lives. These AI systems, from virtual assistants to predictive analytics, have become integral parts of our digital landscape, shaping how organizations work, communicate, and make decisions. However, with these technologies' immense promise comes a pressing concern: the potential exposure of personal data. Advancements in AI require massive data mining of potentially copyrighted materials such as videos, photos, or texts (Quang, 2022). As AI solutions rely heavily on data for training and operation, fears of data privacy breaches and unauthorized access have surged. This has underscored the critical need to harness the power of AI and safeguard the sensitive information it relies upon. In this context, the quest to balance AI's remarkable capabilities and data protection imperative has become more crucial than ever.

In the ever-evolving landscape of technology, where AI-driven solutions have gained an unprecedented foothold, the research embarks on a critical exploration. The research endeavors to unravel the depths of transparency within the privacy policy governing desktop applications, browser plug-ins, and browser-only AI solutions. Specifically, the hypothesis poses a pivotal question: To what extent is there transparency in the privacy policy for three AI solutions concerning data collection practices and undisclosed system modifications? Furthermore, this work will also scrutinize the pressing concern of whether these agreements encompass instances where an excess of data is funneled to the AI system, surpassing what is deemed necessary or documented. This inquiry delves into the heart of AI ethics and data privacy on a Windows 11 end-point, aiming to shed light on the often-elusive boundary between technological advancement and safeguarding individual privacy.

This research will subject three distinct AI solutions to rigorous evaluation in this research endeavor. The first of these, Dropbox Dash, represents a cutting-edge Windows 11 application currently in private beta testing. It stands out for its capacity to seamlessly search and retrieve data stored both locally on a system and in the cloud, making it a

prime candidate for investigating data collection transparency. The second focus is on the widely used Grammarly, a Chrome plug-in integrated into the Microsoft Edge browser, renowned for its grammar insights. The third, Google Bard, is a purely browser-based solution contingent upon a Google account for access. It harnesses the power of Large Language Models derived from training on internet-wide data. By testing these diverse AI solutions, the research will aim to gain valuable insights into the extent of transparency and data handling across various applications, ranging from local and cloud-based to browser-dependent offerings.

2. Research Method

2.1. Constraints

The assessment of the terms of service for the selected AI solutions revealed a significant gap in providing precise characterizations of the data to be collected. However, the Privacy Policy documentation emerged as a pivotal resource in this research endeavor, offering the essential information needed to establish a benchmark for evaluation. Strikingly, it was noted that the Privacy Policy for each solution remained relatively generic, applicable across the entire spectrum of the vendor's offerings. For example, whether it was a purely web-based solution like Google Bard or standard Google Search, the same policy was applied consistently across all the vendor’s offerings. This uniformity underscores the importance of assessing these policies as a unified source of information in pursuit of transparency and data handling insights.

From a technological standpoint, it is worth noting that all three solutions under scrutiny employ encryption protocols as a security measure when transmitting data for analysis. While encryption is an integral component of data protection and security, it presents a notable challenge from a research perspective. The robust encryption measures, while ensuring the confidentiality of data during transmission, can also make it inherently challenging to analyze the applications' communication pathways. This technological constraint underscores the importance of evaluating the transparency of

data collection practices and understanding the complexities associated with securely transmitting user data in today's digital landscape.

2.2. Research Environment

The system environment for conducting the comprehensive tests was meticulously constructed to ensure uniformity and consistency across all evaluations. It centered on a Windows 11 virtual machine running on VMWare Workstation 17.0.2, build-21581411, which served as the standardized testing ground and is required to support Windows 11 guest operating systems. This virtual machine housed a baseline build that remained constant throughout all three phases of assessments. This approach guaranteed a level playing field for evaluating each AI solution. It also discerned performance variations and data handling practices specific to each solution within a controlled and consistent computing environment.

The Virtual Machine Configuration figure shows the Windows 11 virtual machine configuration used in the research.

Device	Summary
Memory	8 GB
Processors	2
Hard Disk	64 GB
Network Adapter	NAT
Trusted Platform Module	Present

Figure 1 Virtual Machine Configuration

The following Foundational Software Installed for Testing figure dissects the foundational software elements employed in this research study.

Software	Version	Purpose
Windows 11 Pro	10.0.22621 Build 22621	Base Operating System
Microsoft Edge	117.0.245.47	Internet Browser

Microsoft Sysinternals Process Monitor	17.05	Examine process handles and loaded dynamic link libraries (DLLs).
Microsoft Sysinternals Sysmon	15.0	Monitors and records essential system activities through the Windows event log.
IDA Free	8.3.23608	Binary Analysis and Debugging
Burp Suite	Community 2021.10.1.2	Web Application Security and Penetration Testing Tool
Wireshark	4.0.10	Network Traffic Analysis Tool
Postman	10.18	API Testing Tool
Python	3.12.0	Simple computer language for various tasks
FoxyProxy Standard	3.0.7.1	Used by Burp Suite to focus web traffic.
VMWare Tools	12.1.5 Build 20735119	Allows for additional interactions with the guest virtual machine

Figure 2 Foundational Software Installed for Testing

2.3. Testing Approach

In this research, three distinct yet closely aligned methodologies were employed. Each approach was tailored to extract results from systems built identically. The evaluation commenced by scrutinizing the Privacy Policy to discern the data collection

criteria. With this delineation as the sole anticipated outcome, the analysis centered on detecting any additional data elements surreptitiously being extracted from the system. The following Testing Approach figure provides a high-level overview of the testing process for each solution. For an in-depth exploration of the testing outcomes, the findings section of this research delves into the specifics and results of the comprehensive assessment.

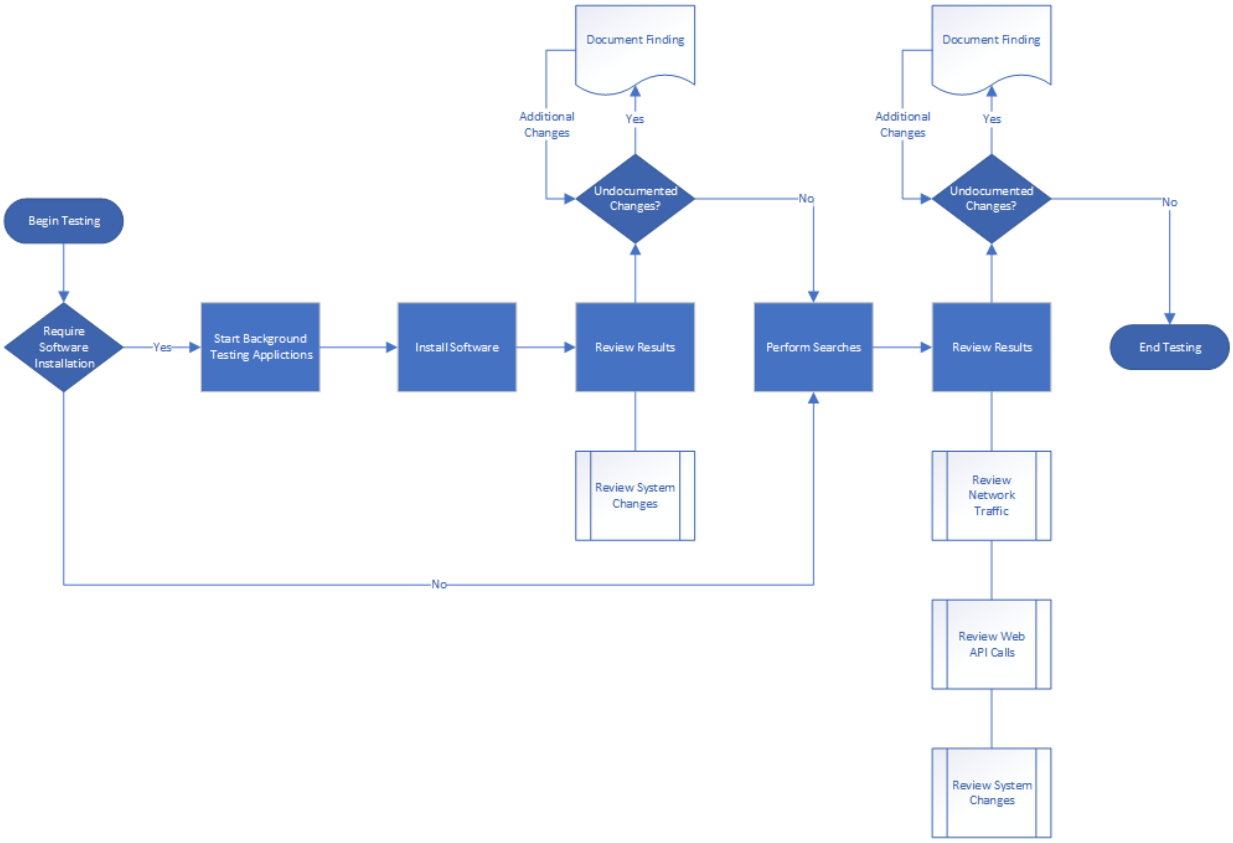

Figure 3 Testing Approach

3. Findings and Discussion

The following comprehensive analysis reviews three cutting-edge AI solutions: Dropbox Dash, Grammarly Plugin, and Google Bard. This scrutiny revolves around a meticulous examination of their respective privacy policies and the practical implications of these policies in real-world application scenarios. The analysis methodically dissects the nature of data collection, storage, and processing as outlined in the privacy policies,

juxtaposing these details with actual system behaviors observed during software installation and usage. The study delves into the nuances of network communication, data encryption, and system modifications by employing a range of diagnostic tools such as Process Monitor, Sysmon, Wireshark, and IDA Free. This evaluation not only aims to unveil the intricacies of user data handling by these applications but also seeks to illuminate any potential discrepancies between the companies' privacy commitments and their operational realities. This investigation provides a comprehensive understanding of how these AI solutions interact with user data and system resources, offering valuable insights into their privacy and security dimensions.

3.1. Dropbox Dash – Desktop AI Solution

3.1.1. Privacy Policy Review

Dropbox's Privacy Policy centers its primary focus on what they term "Your Stuff." Within their policy, "Your Stuff" encompasses a wide array of personal data, including files, documents, photos, comments, messages, and more. It underscores services as a streamlined and personalized platform for users to securely store digital content, collaborate with others, and seamlessly work across various devices and integrated services (Dropbox, 2023). In the analysis of the Privacy Policy, particular attention was directed toward the data collected concerning device information, with a distinct emphasis on understanding the intricacies of this aspect rather than the objects stored within the solution. The following Dropbox Privacy Policy Data Collected figure outlines the findings derived from examining the Privacy Policy, with a dedicated focus on collecting device-related data.

IP Address	Type of browser
Device you use	Web page you visited before coming to their site
Identifiers associated with the device	Location information

Figure 4 Dropbox Privacy Policy Data Collected

3.1.2. Software Installation Findings

A meticulously planned approach was adopted to investigate the system alterations induced by the installation of Dropbox Dash. Two distinct tests were devised, each carefully supported by VMWare Workstation snapshots. This strategic use of snapshots facilitated the ability to install and roll back the system to its previous state for precise testing of the installation impact. The initial step involved transferring the Dropbox Dash Setup Version 2.83.2 Windows executable onto the system. After this, a snapshot was taken, providing a stable reference point for conducting the tests and ensuring the systematic evaluation of the installation's effects on the system environment.

The initial phase of the testing protocol harnesses the power of Microsoft Sysinternals tools, explicitly focusing on Process Monitor, Sysmon, and Wireshark. These tools offer an intricate operating system perspective, enabling a detailed analysis of system alterations, including file and registry modification and network communication during software installation. Process Monitor meticulously records and scrutinizes real-time system activity, shedding light on any changes occurring during installation. Sysmon, on the other hand, provides a comprehensive monitoring and event-logging framework, enriching the understanding of system-level modifications during the installation phase. It is crucial to emphasize that Wireshark, an independent tool, played a vital role in capturing network traffic during the installation, enabling the research to closely examine data exchanges between the system and external sources. This tool trio is invaluable in unraveling the complexities of the installation's impact on the system.

In alignment with the ongoing initial phase of the analysis, the procedure commenced with the configuration of Sysmon to ensure that Process Monitor exclusively captured changes related to the installation. To achieve this, Sysmon and Wireshark were launched with a default configuration, effectively preventing Process Monitor from recording system changes originating from Sysmon itself and concentrating solely on alterations stemming from the installation process. This configuration was initiated through an administrator-level command prompt, employing the command "sysmon -i -accepteula," establishing a controlled environment for capturing and evaluating installation-induced system modifications. It is noteworthy that Microsoft Edge and

Wireshark were launched before Process Monitor to guarantee that it was not inadvertently included in the installation analysis, thus focusing solely on the changes associated with the installed software.

Following the configuration of Sysmon, Wireshark, and Microsoft Edge, the subsequent step involved the initiation of Process Monitor. This was seamlessly executed from the same administrator-level command prompt, utilizing the command "procmon -accepteula." With Process Monitor now active, the current capture was promptly cleared and a new capture was initiated. This meticulous approach ensured that the software installation process was comprehensively monitored and recorded, enabling an in-depth analysis of system-level changes and interactions induced by the installation. The following Dropbox Dash Installation Analysis figure depicts the process for Sysinternals and Wireshark analysis of installation.

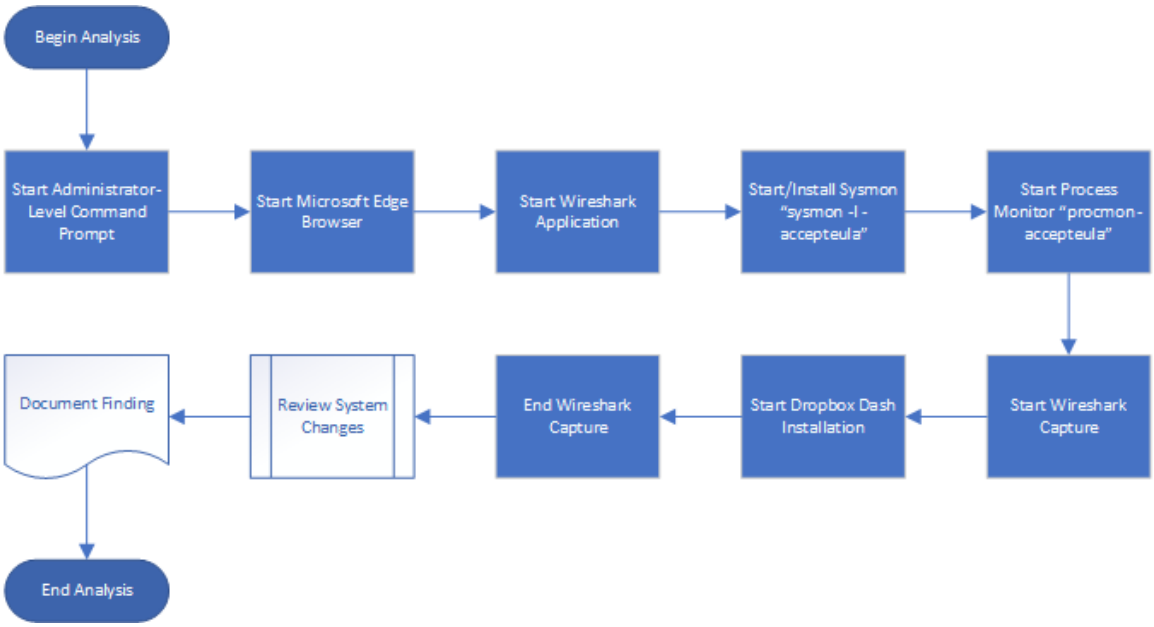

Figure 5 Dropbox Dash Installation Analysis

A meticulous examination of the data generated by Process Monitor, Sysmon, and Wireshark unveiled a few noteworthy insights. During the installation process, it was determined that the software made outbound requests to authenticate my Dropbox account, including identifying the IP address involved in this communication. Furthermore, this communication was conducted over TLS 1.2, ensuring a secure data

exchange. However, due to the robust encryption employed, the specifics of the conversation could not be deciphered, highlighting the adequate security measures in place. This comprehensive analysis, conducted with Wireshark's assistance, confirmed that no abnormal system configurations or unexpected behavior were observed from the operating system's perspective. These findings underscore the software's compatibility with the working environment and its capacity to maintain the integrity of the system configuration. Figure 6 shows the conversation between the installation and Dropbox.

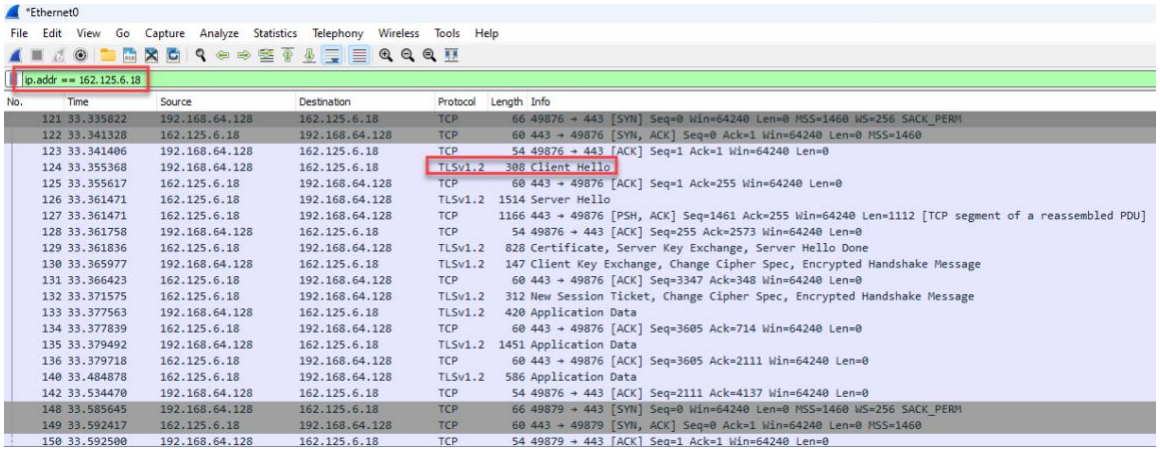

Figure 6 Installation Conversation with Dropbox

The second phase of the installation testing strategy involves utilizing the IDA Free reverse engineering tool. This powerful toolset provides a unique vantage point, enabling the research to delve into the intricacies of the installation process from the application's perspective. IDA's capabilities in reverse engineering empower the dissection of the installation step by step, gaining valuable insights into how the application interacts with the system and any underlying changes it induces. This methodological approach offers a comprehensive understanding of the installation process, complementing the operating system-centric analysis undertaken in the first phase of testing. The following IDA Free Dropbox Dash Setup Executable Analysis figure shows the high-level process of analyzing the Dropbox Dash setup executable.

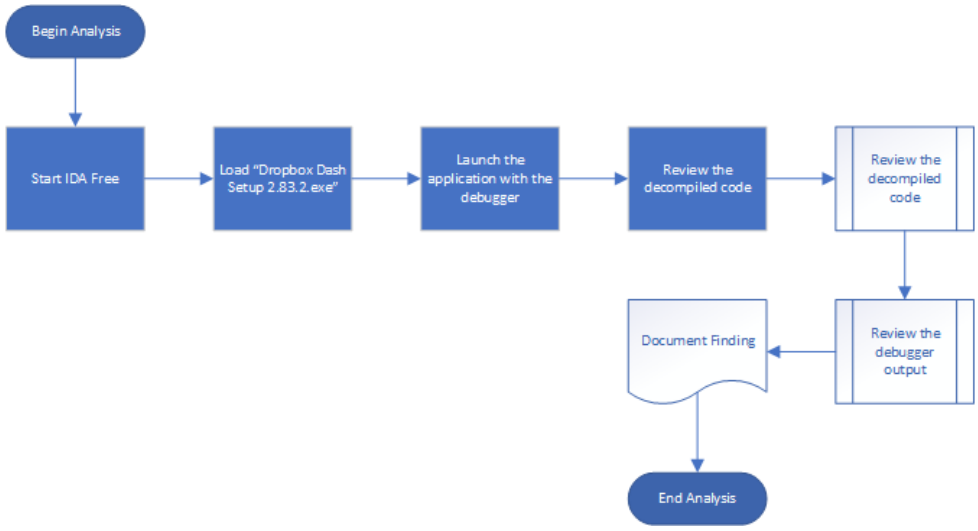

Figure 7 IDA Free Dropbox Dash Setup Executable Analysis

The executable "Dropbox Dash Setup 2.83.2.exe" was initiated and debugged. Subsequently, the decompiled code was meticulously reviewed and the execution process was closely scrutinized. Following this comprehensive analysis, it is noteworthy that no anomalies were detected during the installation phase from a reverse engineering perspective. The following IDA Reverse Engineering Tool Results figure shows the initial and concluding outputs generated by the IDA tool.

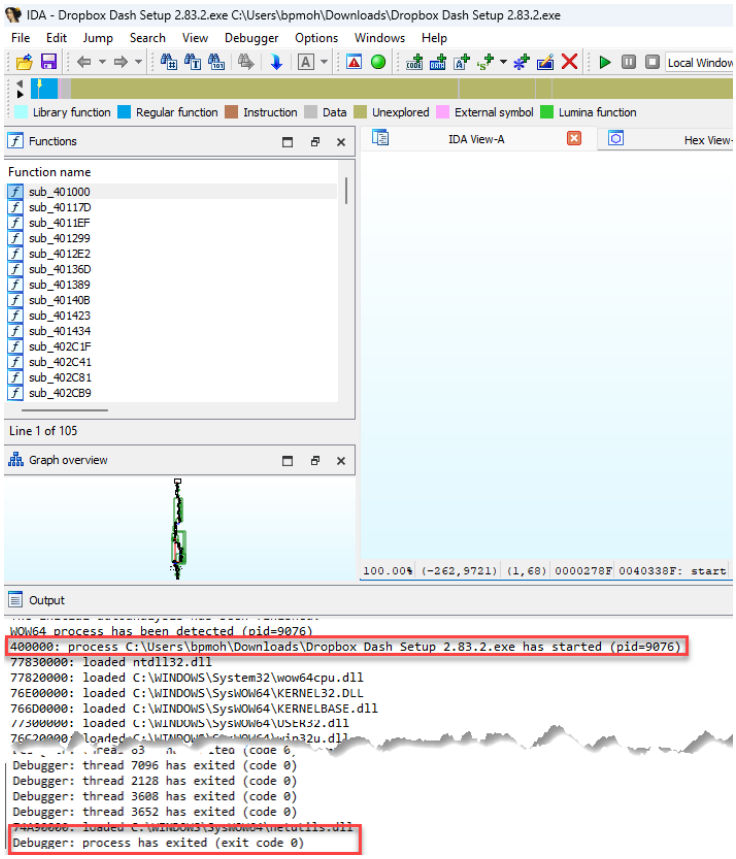

Figure 8 IDA Reverse Engineering Tool Results

3.1.3. Software Usage Findings

The following Dropbox Dash Software Analysis figure shows the high-level steps the research utilized to perform the software usage analysis.

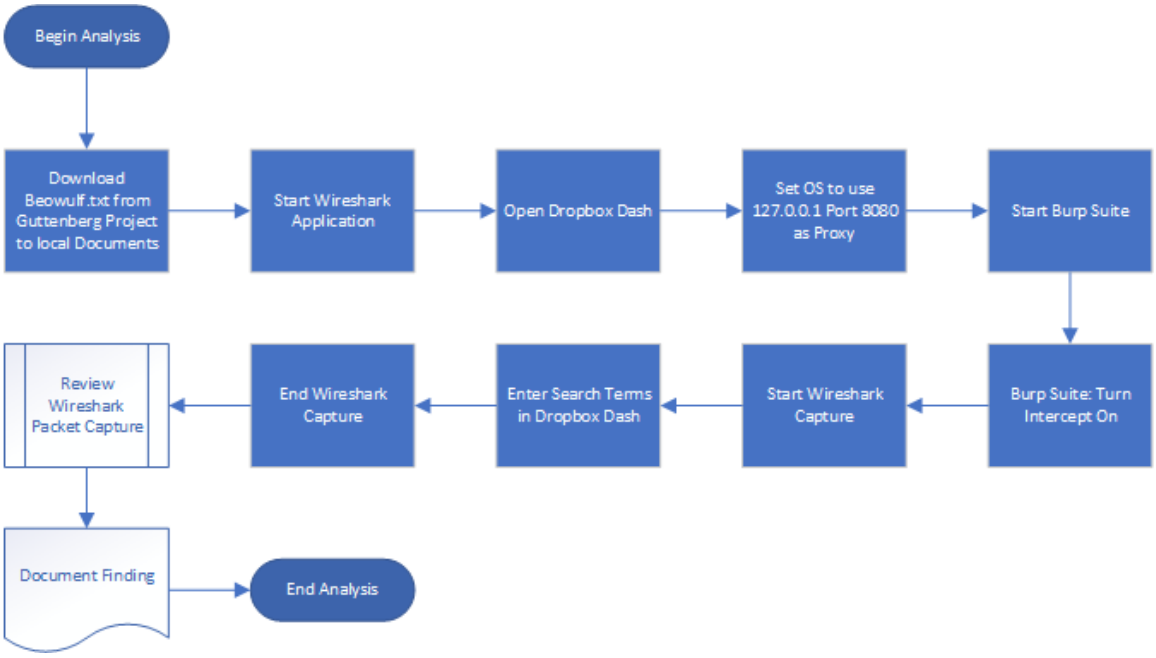

Figure 9 Dropbox Dash Software Analysis

During the testing phase, which aimed to execute searches with Dropbox Dash to locate relevant documents on the local system, the process was initiated by downloading "Beowulf" in Plaintext UTF-8 format from the Gutenberg Project. The document was strategically placed in the “Document” folder, ensuring that it was available for indexing by Dropbox Dash. This meticulously selected document served as the focal point of the search, providing a standardized basis for evaluation. The "Search local files" option in the General settings of Dropbox Dash was enabled to perform the local search effectively. Specifically, the phrase "men may say not where the haunts of these Hell-Runes be," which is contained in Beowulf was searched. The following Dropbox Dash - Enable Search Local Files shows how to enable “Search local files.”

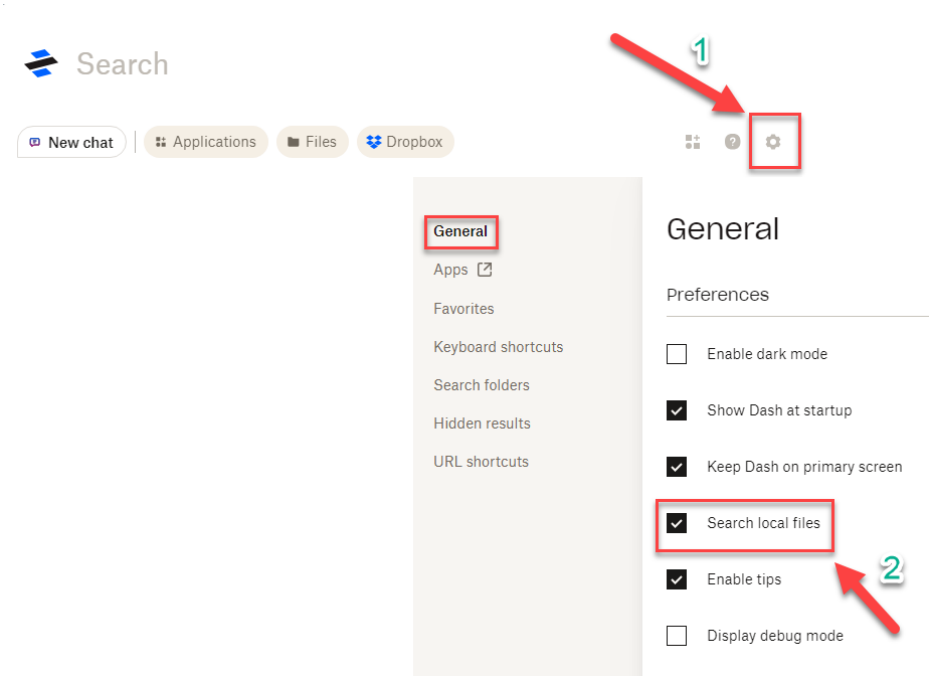

Figure 10 Dropbox Dash - Enable Search Local Files

No results were captured with Burp Suite. This gives the impression that the search stayed on the local box and did not send any information to Dropbox. Upon completion of the search, the Wireshark results were reviewed, which yielded a set of IP address conversations. The research successfully identified the IP addresses 162.125.6.18 and 162.125.6.19 through a thorough analysis. To ascertain their association with Dropbox, a whois search was conducted, ultimately confirming that Dropbox indeed utilized these IP addresses during the search process. Since nothing was seen from Burp Suite and data was seen from Wireshark, it can be concluded that the API was not used to communicate and that the application may have used the Dropbox IP address for keep-alive or update checking.

- 224.0.0.251: Multicast-DNS
- 224.0.0.252: Multicast-DNS
- 3.233.152.251: Amazon AWS Address – Datadog HQ – Cloud Monitoring
- 3.233.152.253: Amazon AWS Address – Datadog HQ – Cloud Monitoring
- 34.120.195.249: Google GCP – ingest.sentry.io – Tracker
- 162.125.6.18: Dropbox
- 162.125.6.19: Dropbox

- 192.168.64.2: Local Router

Ethernet · 5 | IPv4 · 8 | IPv6 · 2 | TCP · 7 | UDP · 10

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.64.1	224.0.0.251	6	420 bytes	6	420 bytes	0	0 bytes	16.120535	2.0116	1670 bits/s	0 bits/s
192.168.64.1	224.0.0.252	4	256 bytes	4	256 bytes	0	0 bytes	16.120535	1.4202	1442 bits/s	0 bits/s
192.168.64.128	3.233.152.251	117	107 kB	25	96 kB	92	11 kB	1.727252	0.8620	892 kbps	99 kbps
192.168.64.128	3.233.152.253	53	34 kB	17	27 kB	36	7 kB	0.006675	0.2448	892 kbps	217 kbps
192.168.64.128	34.120.195.249	1	55 bytes	1	55 bytes	0	0 bytes	17.001643	0.0000		
192.168.64.128	162.125.6.18	36	11 kB	15	6 kB	21	6 kB	4.497240	5.7935	7709 bits/s	7674 bits/s
192.168.64.128	162.125.6.19	45	8 kB	20	6 kB	25	3 kB	4.489696	11.6648	3898 bits/s	1820 bits/s
192.168.64.128	192.168.64.2	21	3 kB	15	2 kB	6	1 kB	0.000000	18.1322	666 bits/s	505 bits/s

Figure 11 Wireshark IP Conversations During Dropbox Dash Search Test

The research followed the TCP conversations for both IP addresses within the Wireshark capture, revealing they were also secured with TLS encryption. Regrettably, this encryption rendered the content of the conversations inaccessible, providing no insights into the specific information that was exchanged during these interactions.

3.1.4. Policy versus Findings

Through the meticulous observations of the installation and usage of Dropbox Dash, the research discerned no alterations to the system beyond what is typically expected during a routine installation process. Regrettably, despite extensive efforts, challenges arose in determining the exact nature of the conversations between the system, the software, and Dropbox's endpoints on the internet for the conversations captured by Wireshark. This challenge stemmed from the robust security measures in place, which, while beneficial for consumer data protection, posed difficulties in validating any potential disparities between Dropbox's Privacy Policy and the actual data transmitted to Dropbox. On the positive side, because Burp Suite showed no communication, it looks like the data searched remained on the system and was not sent to Dropbox.

3.2. Grammarly Plugin – Browser Plug-in AI Solution

3.2.1. Privacy Policy Review

Grammarly's Privacy Policy provides a comprehensive breakdown of the types of data collected, encompassing account information, payment details, user-generated content, cookies, and usage data (Grammarly, 2023). In the analysis, the research honed in on the specifics of log data and device information, recognizing them as pivotal aspects for scrutiny. The primary objective was to gain a detailed understanding of the data collected in these categories rather than focusing on data voluntarily provided by

users, such as account information or the textual content of uploaded data. The following Grammarly Privacy Policy Data Collected figure briefly presents the findings derived from my examination of the Privacy Policy, with a distinct emphasis on collecting log data and device-related information, shedding light on this critical facet of Grammarly's data handling practices.

IP Address	Type of browser
Browser version	Time zone setting
Location	Browser plug-in types
Browser plug-in versions	Operating system
Platform	

Figure 12 Grammarly Privacy Policy Data Collected

3.2.2. Software Installation Findings

When installing a browser extension in Microsoft Edge, one generally expects minimal alterations to the system. The strategy for analyzing the Grammarly browser plug-in closely paralleled the methodology employed for installing Dropbox Dash, with a critical distinction. In this case, the snapshot feature was unnecessary, as a single installation was performed, augmented by including an additional monitoring tool, Burp Suite. The installation analysis was conducted using Microsoft Sysinternals Sysmon, Process Monitor tools, Wireshark, and Burp Suite, with the facilitation of Foxy Proxy. The following Grammarly Plug-in Installation Analysis Process figure illustrates the overarching process employed in this testing regimen.

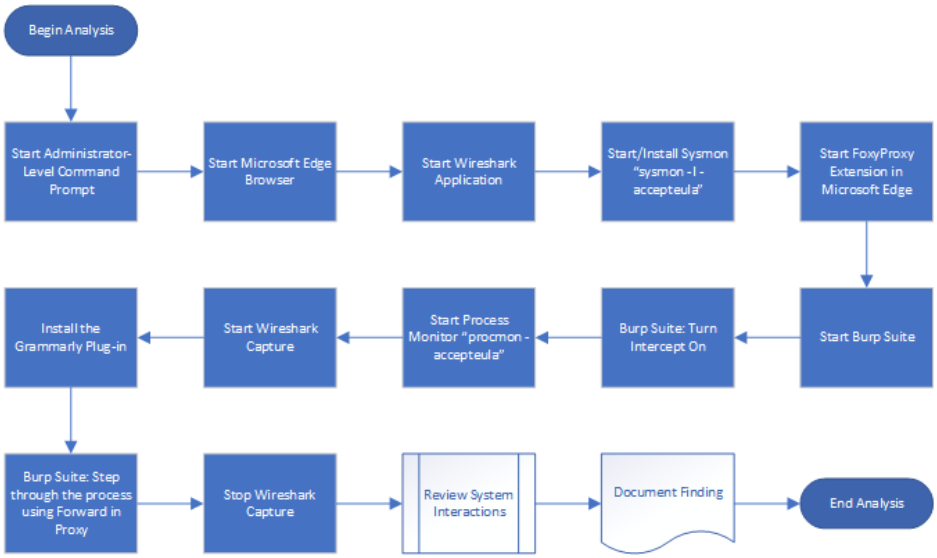

Figure 13 Grammarly Plug-in Installation Analysis Process

At the outset of this endeavor, it became evident that Microsoft Edge extension installation was incompatible with the concurrent use of Foxy Proxy and Burp Suite. Almost immediately, an error surfaced, necessitating the deactivation of Foxy Proxy to proceed with the installation. Once Foxy Proxy was disabled, the installation moved without any hindrances, resulting in a successful installation. The following Grammarly Extension Error with Foxy Proxy Enabled figure visually represents the error message encountered during this phase.

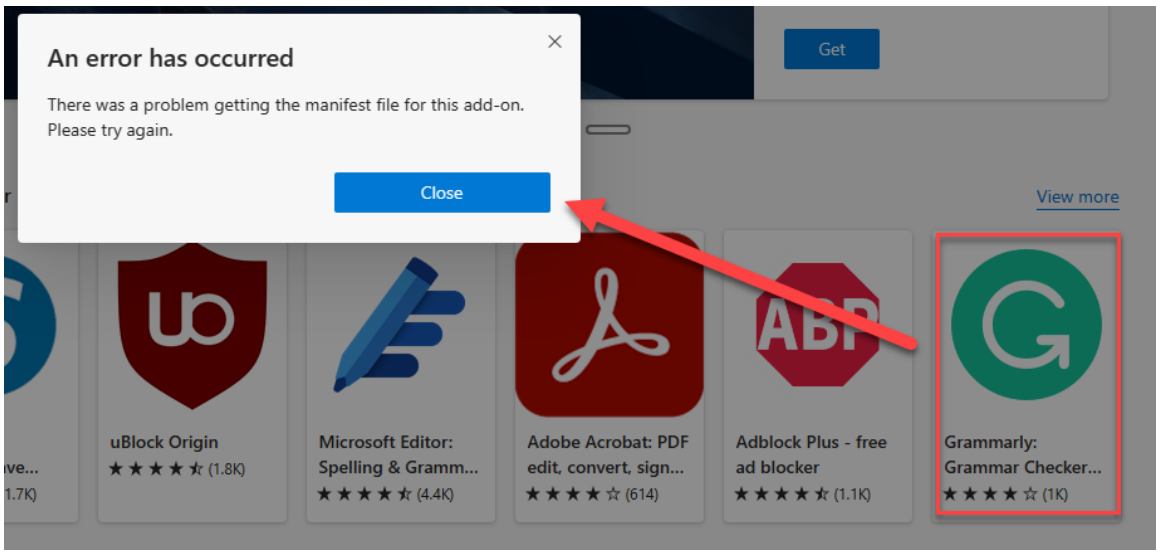

Figure 14 Grammarly Extension Error with Foxy Proxy Enabled

Upon conducting a comprehensive analysis through Wireshark, it was discerned that the communication associated with the Grammarly extension was routed through a Microsoft endpoint identified by the IP address 20.127.250.238. This determination was made employing Whois lookups and an examination of certificates. This communication is visually represented in the following Grammarly Extension IP Communication figure for reference.

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
3.162.112.104	192.168.64.129	12	741 bytes	10	633 bytes	2	108 bytes	0.007161	12.7453	397 bits/s	67 bits/s
3.220.10.1	192.168.64.129	4	299 bytes	2	191 bytes	2	108 bytes	0.000000	0.0008		
20.127.250.238	192.168.64.129	3	292 bytes	2	173 bytes	1	119 bytes	0.435371	0.0015		
192.168.64.129	13.107.6.158	18	9 kB	5	521 bytes	13	9 kB	3.501992	0.0932	44 kbps	753 kbps
192.168.64.129	20.109.122.109	83	57 kB	29	4 kB	54	54 kB	12.475754	0.3375	84 kbps	1275 kbps
192.168.64.129	20.189.173.16	17	6 kB	8	5 kB	9	738 bytes	5.613181	2.3684	17 kbps	2492 bits/s
192.168.64.129	20.253.1.29	46	26 kB	18	7 kB	28	19 kB	5.910517	0.2959	184 kbps	516 kbps
192.168.64.129	23.50.125.163	2	114 bytes	1	54 bytes	1	60 bytes	3.614297	0.0009		
192.168.64.129	23.56.9.154	36	10 kB	14	2 kB	22	8 kB	3.614939	2.1183	8644 bits/s	30 kbps
192.168.64.129	152.195.19.97	2,993	4 MB	288	19 kB	2,705	4 MB	5.835210	0.4933	302 kbps	65 Mbps
192.168.64.129	192.168.64.2	24	4 kB	12	1 kB	12	3 kB	3.602518	8.8728	989 bits/s	2720 bits/s
192.168.64.129	204.79.197.239	76	29 kB	31	11 kB	45	18 kB	5.733212	6.6685	12 kbps	21 kbps

Figure 15 Grammarly Extension IP Communication

A more in-depth examination conducted through Wireshark revealed that all communication occurred over TLS, indicating that the conversations were securely encrypted, precluding the extraction of additional insights. Furthermore, an extensive analysis of Sysmon and Process Monitor failed to uncover any further system modifications of significance resulting from the installation of the Grammarly extension.

3.2.3. Software Usage Findings

To test the functionality of the Grammarly extension, the research employed https://onlinenotepad.org as the testing platform. This choice was made due to the platform's minimal ad presence, ensuring a clear and unobstructed Wireshark packet capture and unadulterated Burp Suite results. To initiate specific functionality tests, the phrase, "The quick brown fox jumped over the lazy dog, Who am I to stop him from jumping" was utilized. This phrase was chosen to deliberately provoke the Grammarly extension to produce grammar correction suggestions. A visual representation of the testing flow for the Grammarly extension, including this specific input, is depicted in the following Grammarly Extension Operation Testing Process figure.

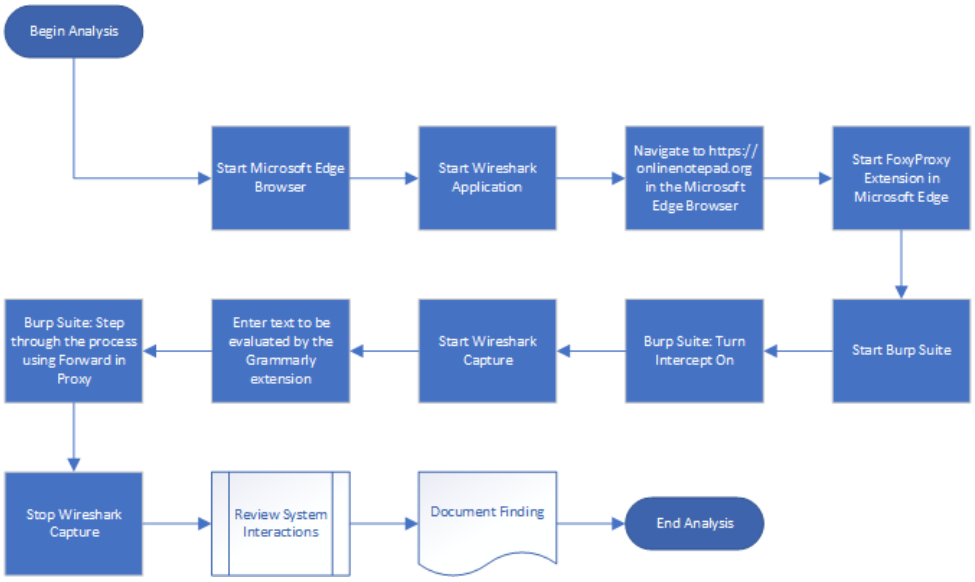

Figure 16 Grammarly Extension Operation Testing Process

Throughout this test, Burp Suite did not capture any calls related to grammar correction. This absence of captured data is attributed to the proxy, which effectively obstructed the extension's interaction without triggering any activity in Burp Suite. Subsequently, upon disabling Foxy Proxy, the grammar correction functionality resumed its flow to the website without impediments. A visual comparison of the results before and after turning off the Foxy Proxy extension is presented in the following figures.

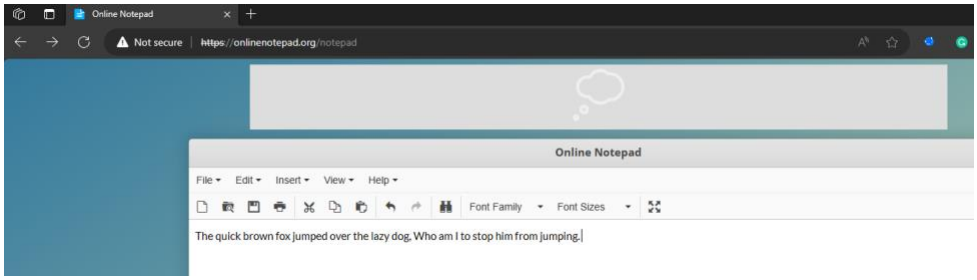

Figure 17 Grammar corrections before Foxy Proxy disabled (no correction)

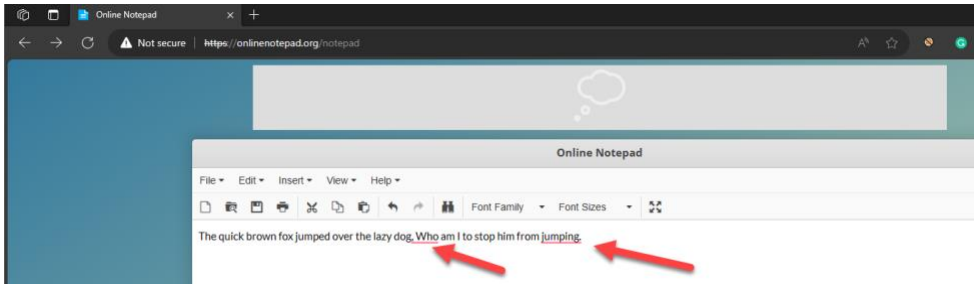

Figure 18 Grammar corrections after Foxy Proxy disable (correction needed)

3.2.4. Policy versus Findings

Through rigorous observation of the Grammarly extension's installation and utilization, the research identified no deviations from the standard system alterations expected during a typical installation process. However, despite extensive investigations, the research encountered difficulties in precisely delineating the interactions between the system, the extension, and Grammarly's online endpoints. These challenges were attributed to the robust security measures, which, while essential for safeguarding consumer data, presented obstacles in verifying potential disparities between Grammarly's Privacy Policy and the data exchanges transpiring with Grammarly's servers.

3.3. Google Bard – Pure Browser AI Solution

3.3.1. Privacy Policy Review

Google's Privacy Policy encompasses a comprehensive overview of data collection, whether users are signed in with a Google Account or not. The analysis primarily examined the scenario involving a Google Account sign-in, which is mandatory for using Google Bard. It is important to note that when signed in, Google collects personal information from data associated with the user's Google Account. However, the specific focus was on the device-related data contained in this context. The analysis deliberately excluded the examination of personal data or information provided as part of the Google Account, instead concentrating on the intricacies of device information. The following Google Privacy Policy Data Collected figure encapsulates the findings obtained through the review of the Privacy Policy, with a dedicated emphasis on collecting device-related data, thereby illuminating this critical aspect of Google's data handling practices (Google, 2023).

Unique identifiers	Type of browser
Browser settings	Device type
Device settings	Operating system

IP address	Crash reports
System activity	Date
Time	Referrer URL
Location	Wi-Fi access points
Cell towers	Bluetooth-enabled devices

Figure 19 Google Privacy Policy Data Collected

3.3.2. Software Installation Findings

The evaluation of Google Bard presented a distinct approach compared to the previous installations. In this case, installation was not a requisite, as the analysis centered on the interactions with Google Bard conducted directly through the Microsoft Edge browser. This methodology bypassed the need for installation-related assessments. Instead, it focused on scrutinizing the application's behavior and data interactions in real-time, thereby providing valuable insights into its functioning and data handling practices without the traditional installation process.

3.3.3. Software Usage Findings

In pursuing software usage insights, the research maintained a consistent methodology, leveraging Microsoft Sysinternals' Sysmon and Process Monitor to monitor system interactions meticulously. This approach ensured that browser interactions with Google Bard remained free from any system modifications while offering a robust operating system perspective that contributed to ongoing system integrity assessment.

Furthermore, to conduct a more direct analysis of usage patterns, Wireshark, a powerful network packet analyzer, and Burp Suite, a versatile web application testing tool, were employed to examine interactions with Google Bard painstakingly. Wireshark allowed for detailed network traffic inspection, providing valuable insights into data exchanges. To facilitate this comprehensive analysis, Foxy Proxy was enlisted to redirect web traffic, empowering Burp Suite to scrutinize and record these interactions thoroughly.

This combined arsenal of tools provided a comprehensive means of assessing software usage and interactions, safeguarding the system's integrity throughout the assessment, and enabling a thorough understanding of the software's behavior and its impact on the system. The following Google Bard Testing Process figure shows the process used to test Google Bard.

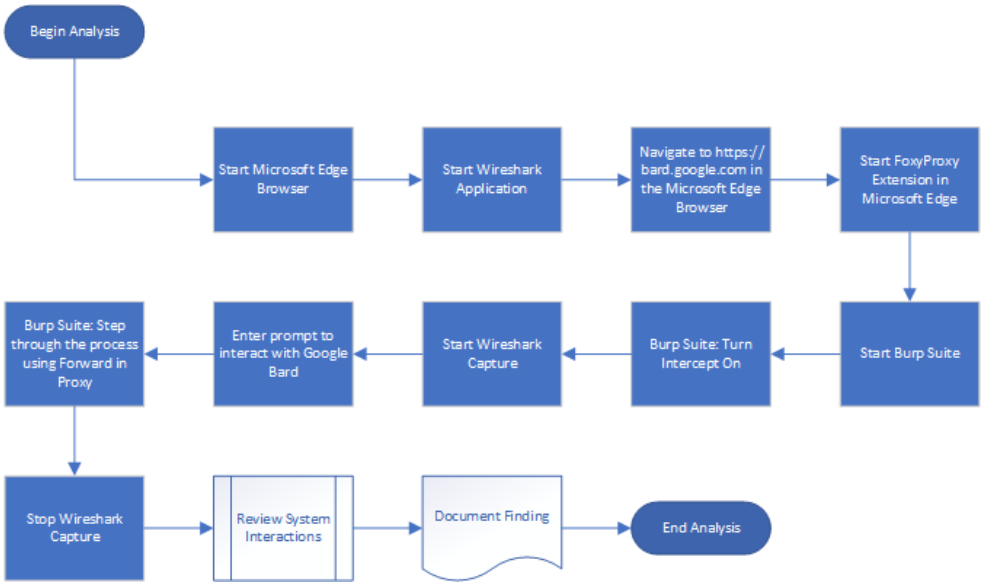

Figure 20 Google Bard Testing Process

Upon commencing the test, the researcher encountered a recurring issue akin to the one experienced while installing the Grammarly extension. With the Foxy Proxy extension enabled, the research faced impediments in carrying out the intended action. The Google Bard website appeared to detect my attempt to intervene in the communication between the Microsoft Edge browser and Google Bard, a behavior akin to a machine-in-the-middle attack. For a visual representation of this issue, please refer to the Google Bard Testing Error figure below, which illustrates the error encountered during this phase.

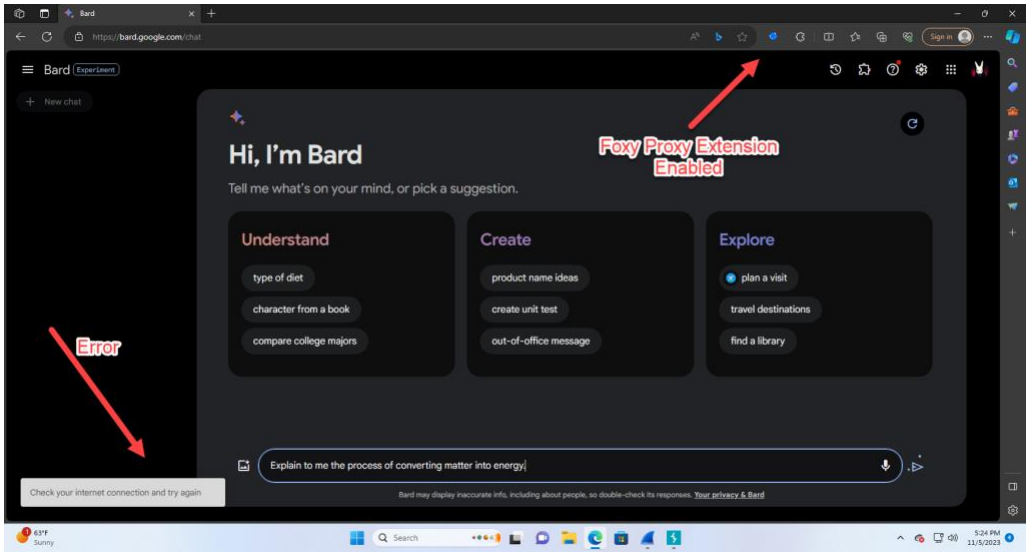

Figure 21 Google Bard Testing Error

This predicament necessitated the deactivation of Foxy Proxy, obliging the research to depend on data gleaned from Wireshark for analysis. As the research delved into evaluating the communication exchange between the system and Google Bard, an obstacle was encountered with encryption through the QUIC protocol. The QUIC protocol, initially developed by Google and equivalent to TLS, introduced encryption that posed challenges in examining the data flow. Nevertheless, the volume of data exchanged during this interaction was minimal, suggesting that both the interaction and its outcomes were entirely encapsulated within Google's endpoints. Given this minimal data exchange, it becomes apparent that no elements originating from the system were included. The subsequent Google Bard Data Exchange figure visually represents this minimal data exchange.

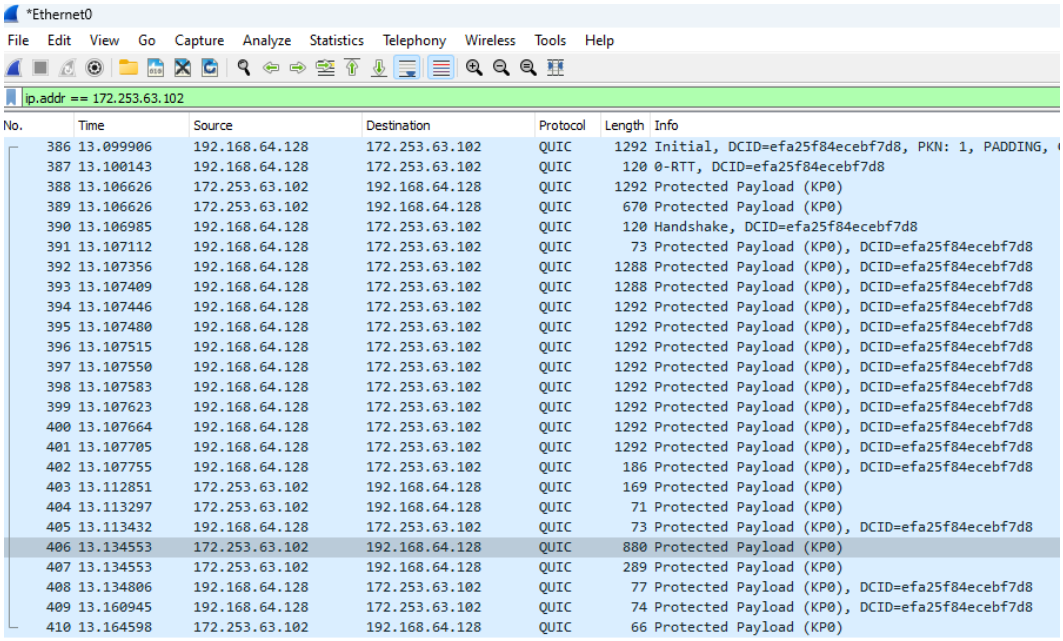

Figure 22 Google Bard Data Exchange

3.3.4. Policy versus Findings

Through meticulous observation of the interactions with the Google Bard website, the research discerned no deviations from the typical system alterations anticipated during such interactions. Nevertheless, despite thorough investigations, the research encountered challenges in accurately characterizing the nature of these interactions, specifically between the system and Google Bard endpoints. These challenges stemmed from the stringent security measures, which, although crucial for safeguarding consumer data, introduced complexities in verifying potential disparities between Google's Privacy Policy and the data exchanges transpiring with the Google Bard AI solution.

4. Recommendations and Implications

It is crucial to acknowledge that this research, despite its rigorous efforts, did not yield substantial insights or findings concerning the evaluation of privacy policies against AI application processes. This limitation primarily stemmed from the pervasive use of encryption in communication, which effectively obscured the transparency of data exchanges. Consequently, the challenge of comprehensively assessing the alignment between privacy policies and actual AI application practices remains unresolved. In light

of this, a pressing need persists to institute thorough evaluations of these AI applications, or even consider a temporary prohibition on their deployment until comprehensive assessments can be conducted. This precautionary approach is imperative to ensure data privacy and security are upheld in an era marked by rapidly evolving AI technologies and intricate data exchange mechanisms.

In the forthcoming section, the research will delve into a series of recommendations to enhance the process of reviewing privacy policies and establish a comprehensive understanding of how the proliferation of AI solutions should be effectively monitored. These recommendations will encompass strategies to navigate the evolving landscape of AI technologies while protecting personal data. Additionally, this research will guide areas that warrant further research, offering a roadmap for continued exploration and refinement in the realm of AI and data privacy.

4.1. Recommendations for Practice

Organizations rely heavily on technology and interconnected systems in today's digitally driven landscape. Safeguarding sensitive data and mitigating cybersecurity risks is paramount. One fundamental step in reducing organizational risk lies in conducting a comprehensive inventory of assets, encompassing hardware and the myriad applications running on those assets, including AI-driven applications. This foundational process serves as the bedrock for effective risk management and cybersecurity.

The inventory of assets and applications is essential for several reasons. Firstly, it provides a clear and accurate view of an organization's digital ecosystem, allowing for better management and oversight. Secondly, it enables organizations to identify and categorize applications not part of the organization's standardized or base build. These outliers can pose unforeseen security risks, as they might not adhere to the organization's security standards and policies. Organizations can mitigate potential vulnerabilities by bringing these applications into the purview of scrutiny and control.

Furthermore, an in-depth analysis of the policies and agreements users must accept to access and use these applications is crucial. Understanding the terms and conditions, privacy policies, and data usage agreements associated with each application

is essential in assessing the potential impact on data privacy and security. It also aids in ensuring that user interactions with these applications align with organizational policies and compliance requirements. Kulkarni and Bedekar's recommendations included introducing or enhancing data privacy education in engineering programs, advocating for better personal data management practices, or suggesting further research into specific areas of concern (2022). This recommendation would serve well to all users in an organization.

Moreover, evaluating how these AI applications interface with the broader system and network is vital. This assessment helps organizations identify potential weaknesses in their network architecture or system configurations that external threats could exploit. It also allows for establishing access controls and monitoring mechanisms to safeguard against unauthorized access or data breaches.

To recap, it is imperative to undertake a comprehensive asset and application inventory while focusing on identifying AI applications that may have slipped from awareness. Evaluating these potentially overlooked AI applications is essential to ascertain whether they pose any risks related to data loss within the organization. In tandem with policy reviews and assessments of application-system interactions, this diligent scrutiny process is a pivotal facet of an organization's proactive risk reduction and cybersecurity strategy. Such proactive measures reinforce data protection and fortify the organization's overarching security stance within the constantly evolving digital landscape.

4.2. Implications for Future Research

Exploring the transparency and communication of AI solutions with the system has unearthed several implications that should guide future research endeavors. While the present study encountered challenges in precisely discerning the intricacies of these interactions, it is essential to acknowledge that the absence of conclusive findings in one study does not negate the potential for insights gleaned by researchers with varying skill sets and specialized tools. This suggests that future research can benefit from more advanced methodologies, potentially shedding light on the nuances of data exchanges

between AI solutions and the system. One such advanced methodology could leverage the "API Message-Driven Regression Testing Framework" proposed by Emine Dumlu Demircioglu and Oya Kalipsiz as a foundation for advancing API testing methodologies across diverse business domains (2023).

Moreover, there is a pressing need for ongoing research in AI solution monitoring and control. As the landscape of AI applications continues to evolve rapidly, organizations must stay vigilant to ensure that these solutions adhere to privacy policies and security standards. The dynamic nature of AI development demands a proactive approach to monitor for new AI solutions introduced into the ecosystem continuously. Future research could develop robust monitoring frameworks and technologies capable of identifying and evaluating the security and privacy implications of emerging AI solutions.

Additionally, exploring effective strategies for controlling the installation and use of AI solutions within organizations is paramount. The capacity to enforce policies and standards for AI solution integration and usage is a crucial aspect of data protection and risk management. Future research can delve into the development of governance frameworks, automated controls, and best practices that facilitate organizations in maintaining oversight and compliance concerning AI solution deployment.

While the present study underscores the complexities of transparency and communication in AI solutions, it also underscores the vast potential for future research to provide enhanced insights, advanced monitoring capabilities, and more effective control mechanisms. As AI continues to play an increasingly pivotal role in our digital landscape, ongoing research efforts are vital in ensuring the responsible and secure integration of these technologies.

5. Conclusion

In conclusion, this research has illuminated the formidable challenge of comprehending the transparency of privacy data exchanges within AI solutions provided by vendors. While efforts revealed valuable insights into the complexity of these

exchanges, the formidable encryption protecting the communication precluded a full understanding of their intricacies. However, it is worth noting that this study underscored the profound significance of monitoring and scrutinizing these interactions.

The profound significance lies in recognizing a critical need for organizations to establish robust monitoring protocols that can effectively navigate the complexities of encrypted AI solution interactions, especially in an era of rapidly evolving AI technologies. These protocols should encompass a spectrum of capabilities, from continuous real-time monitoring of data exchanges to proactive threat detection mechanisms. Additionally, organizations should consider implementing "break and inspect" solutions, which can dissect encrypted traffic for security analysis while preserving the integrity of the encryption.

Furthermore, Cloud Access Security Brokers (CASBs) play a pivotal role in this context, providing organizations with enhanced visibility and control over data exchanges between their networks and cloud-based AI solutions. CASBs can act as a crucial layer of defense by monitoring, securing, and auditing data exchanges, thereby mitigating potential risks associated with AI solution communication.

In essence, the profound significance of this research lies in the imperative for organizations to proactively address the challenges posed by encrypted AI solution interactions. Robust monitoring protocols, advanced "break and inspect" solutions, and integrating CASBs are all essential components of a comprehensive strategy to ensure data privacy and security in an ever-evolving digital landscape. By embracing these measures, organizations can effectively safeguard their data assets and maintain the integrity of their systems, even in the face of encryption barriers.

References

Demircioglu, E. D., & Kalipsiz, O. (2023). API Message-Driven Regression Testing Framework.

Dropbox. (2021, October 1). Dropbox Privacy Policy. Retrieved November 4, 2023, from https://www.dropbox.com/privacy

Google. (2023). Google Privacy Policy. Retrieved November 4, 2023, from https://policies.google.com/privacy

Grammarly, Inc. (2021, October 1). Privacy policy. Grammarly. Retrieved November 4, 2023, from https://www.grammarly.com/privacy-policy

Kulkarni, S., Konde, K., & Bedekar, M. (2022). Analyzing Data Privacy Concerns in Young Adults: Apprehensions of Engineering Students. Grenze International Journal of Engineering and Technology, 8(2.21). Grenze Scientific Society.

Quang, J. (2022). Does training AI violate copyright law? Berkeley Technology Law Journal, 36(1407).