VPNalyzer: Researching VPN Vulnerabilities on a Large Scale

Studying the VPN ecosystem and application workflow to prepare VPNalyzer for public release and data analysis.

Anna Ablove (Honors Capstone), Reethika Ramesh, and Roya Ensafi
University of Michigan, Computer Science Engineering Department

ENGINEERING HONORS PROGRAM
UNIVERSITY OF MICHIGAN

Abstract

VPN, or Virtual Private Network, is a tool which aims to allow users to browse the web with enhanced privacy and security by hiding their IP (Internet Protocol) addresses. In theory, this allows for privacy from ISPs (Internet Service Providers) and the bypassing of potential restrictions like government censorship. However, in practice many VPNs are extremely flawed and leak user data — like search queries, traffic, and other app data — to their ISPs. Not only is this a huge violation in consumer trust, but this breakdown of anonymity can be incredibly dangerous for individuals and groups using VPNs for combatting oppressive regimes.

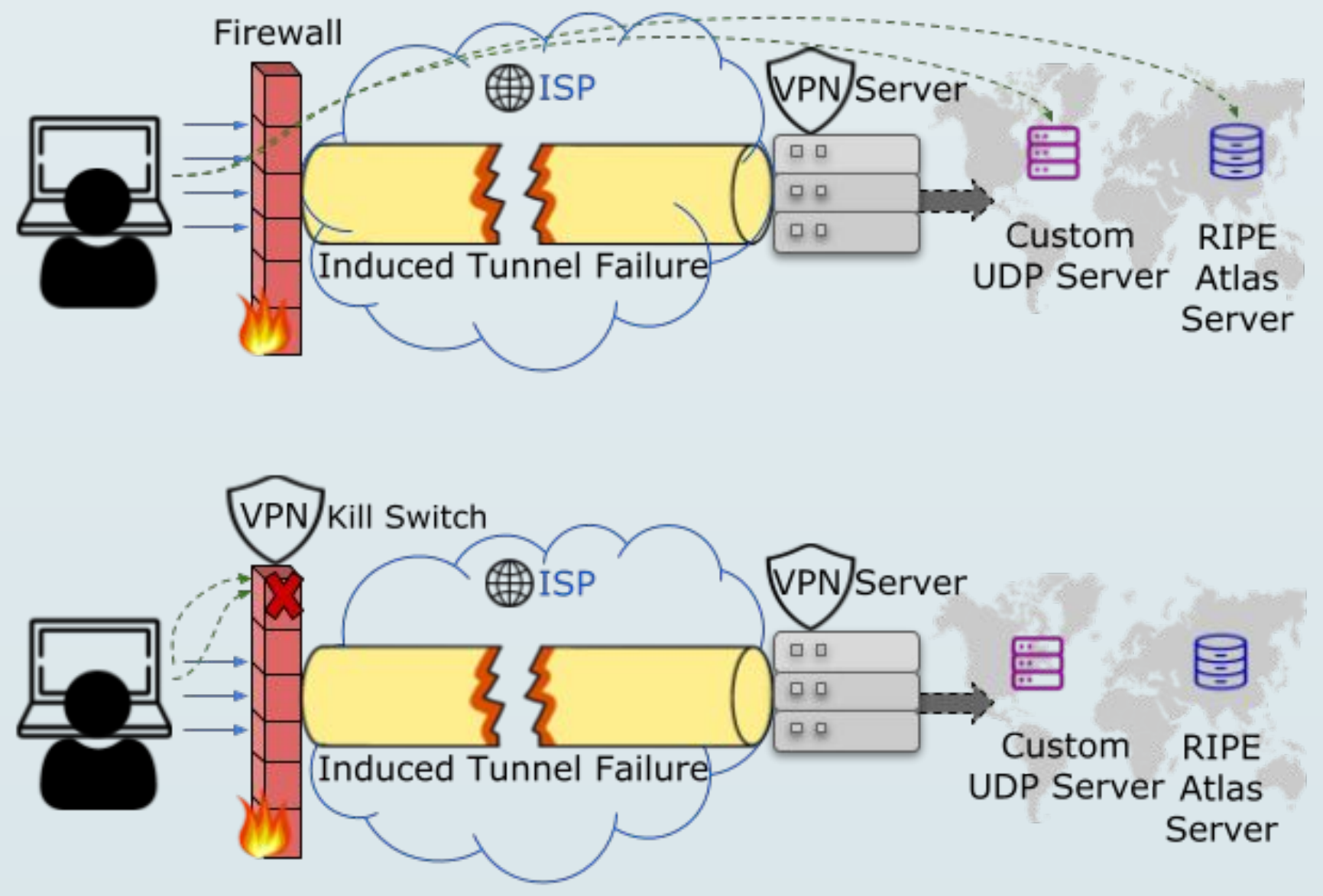
VPNalyzer is an ongoing research project investigating commercial VPN services and seeking to give users the capacity to make informed decisions about different VPN providers. The project has three parallel tracks, quantitative and qualitative user studies, cross-platform one-click install desktop tool for users, and qualitative studies surveying VPN providers. The focus of this capstone is to prepare the tool for public release and plan for the analysis of future data acquisitions

Introduction

- Important to ensure everyone has fair and equal access to the internet
- Specific consideration needs to be taken for activists who live in countries with higher amounts of internet censorship and control and can become government targets if their private information is exposed.

Examples of VPN Fault Points

- Kill Switch
- DNS Leak during Tunnel Failure



Both images show an instance of tunnel failure. The top image depicts an instance without a VPN kill switch, while the bottom image shows the feature enabled.

Guiding Questions

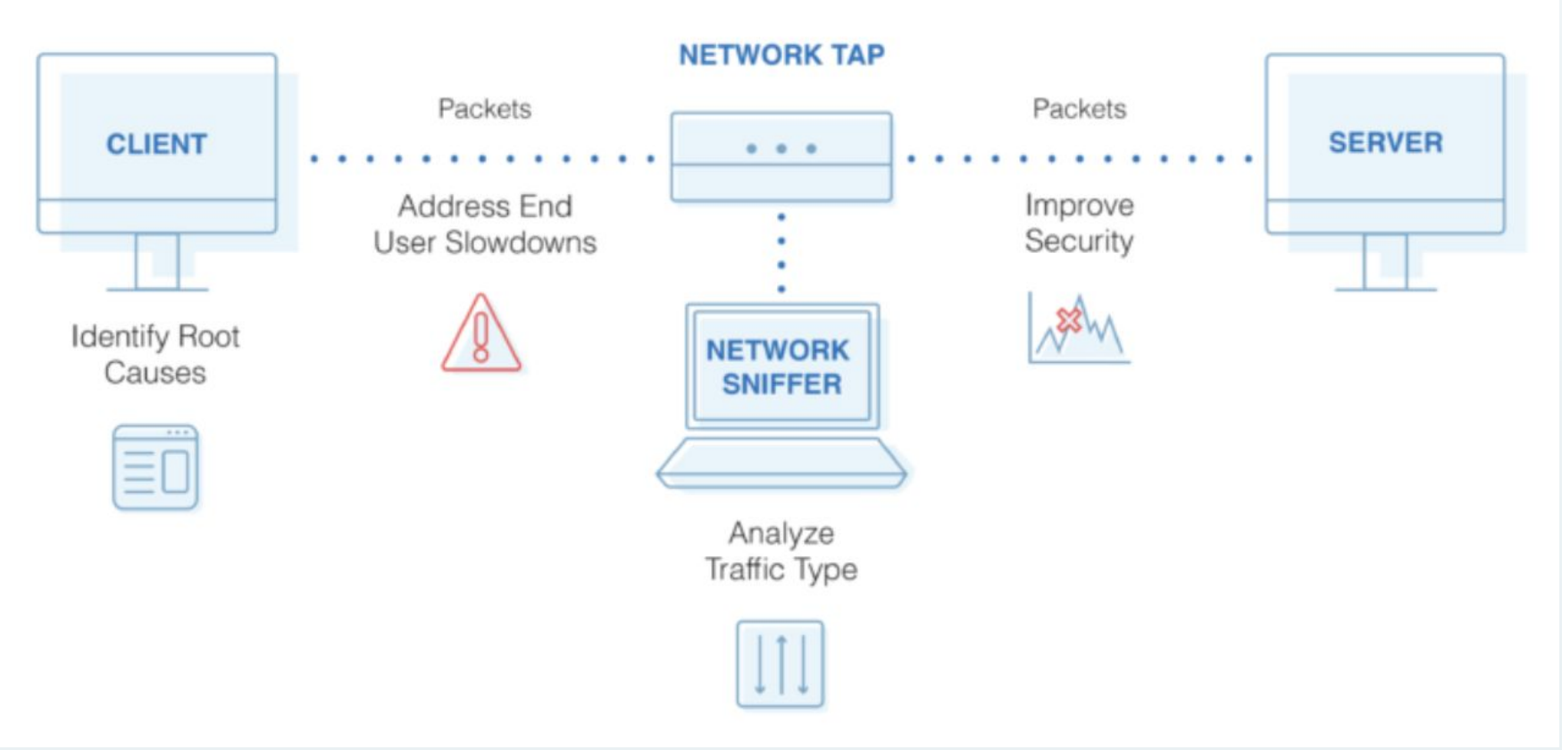
- How secure are commercial VPNs? Where do they fail?
- How can we enforce accountability of VPN providers?
- In what ways can we best empower consumers to find the most trustworthy VPNs?
- How can we analyze/utilize the data from the VPNalyzer tool to answer these questions?

Beta Stage to Public Release

VPNalyzer was developed for three platforms, Windows, Linux, and MacOS. As the tool was in the beta stage at the start of this capstone for all much of the technical scope of the project relates to the finishing touches on the app, specifically the Windows version, such as bundling precompiled binaries and researching and acquiring code signing certificates.

Bundling Precompiled Binaries

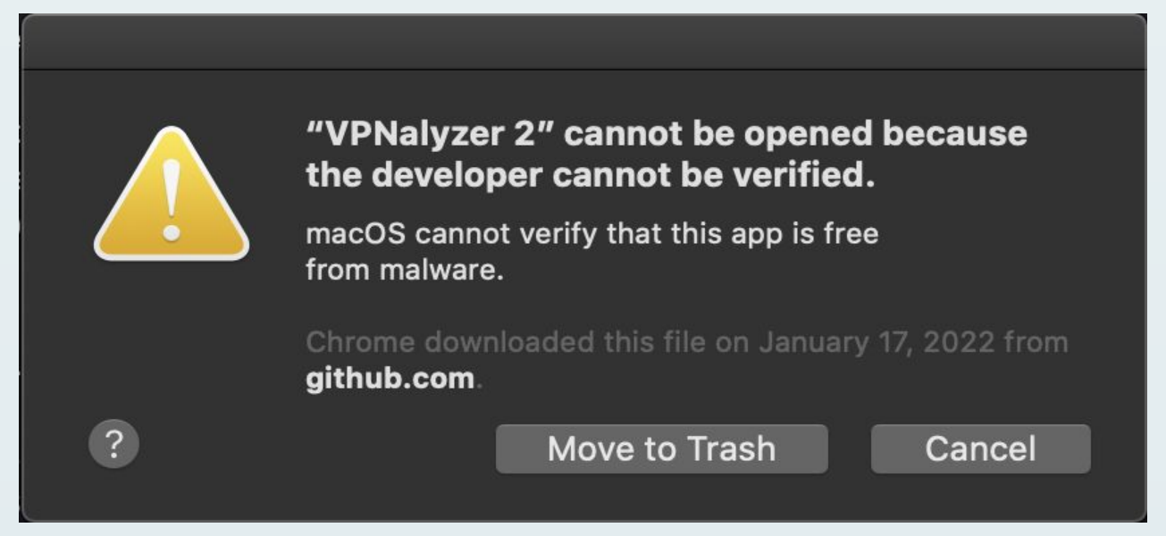
- Npcap Library



Depicted is a top-level view of a packet sniffing system.

Code Signing Certificates

- Need to code-sign the VPNalyzer application to facilitate secure distribution of the tool



"VPNalyzer 2" cannot be opened because the developer cannot be verified.

macOS cannot verify that this app is free from malware.

Chrome downloaded this file on January 17, 2022 from **github.com**.

This is the warning message for an unverified developer on a Mac. The Windows message is essentially the same.

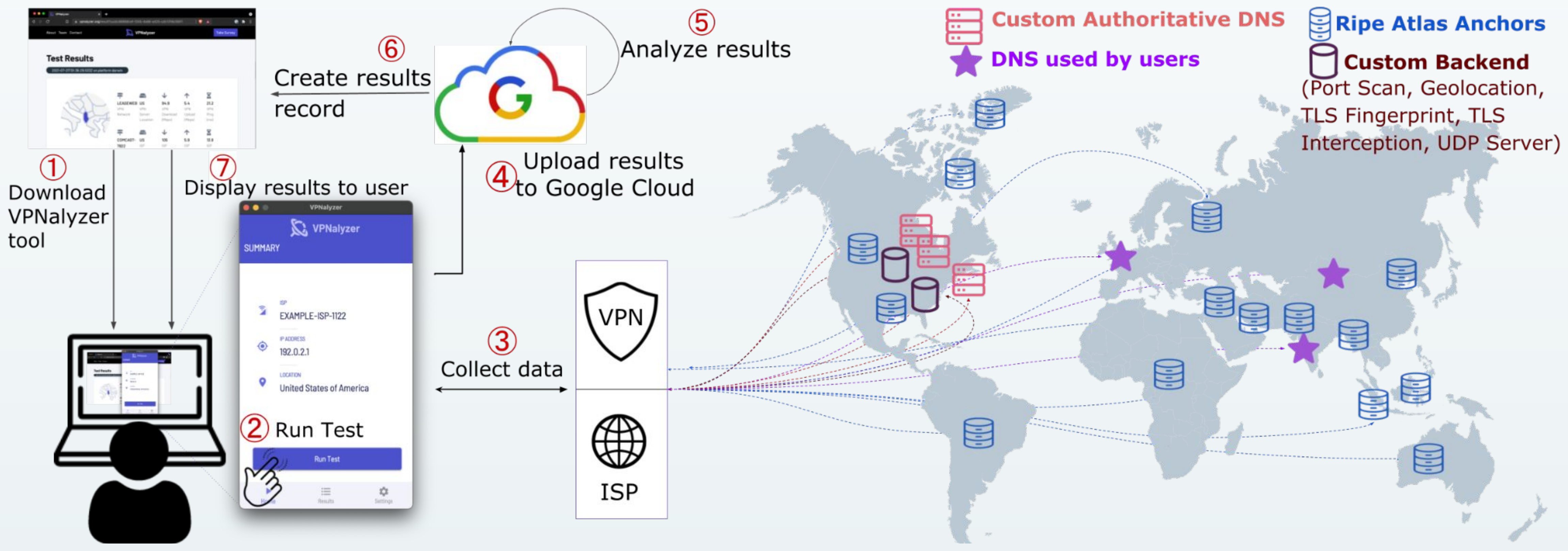
Comparison of Code Signing and EV Code Signing Certificates

	Price	Warning	Physical Signature
Code Signing Cert	$$	Until sufficient downloads	No
EV Code Signing Cert	$$$	No	Yes

Ultimately, we opted for a DigiCert code signing certificate purchased directly from the provider.

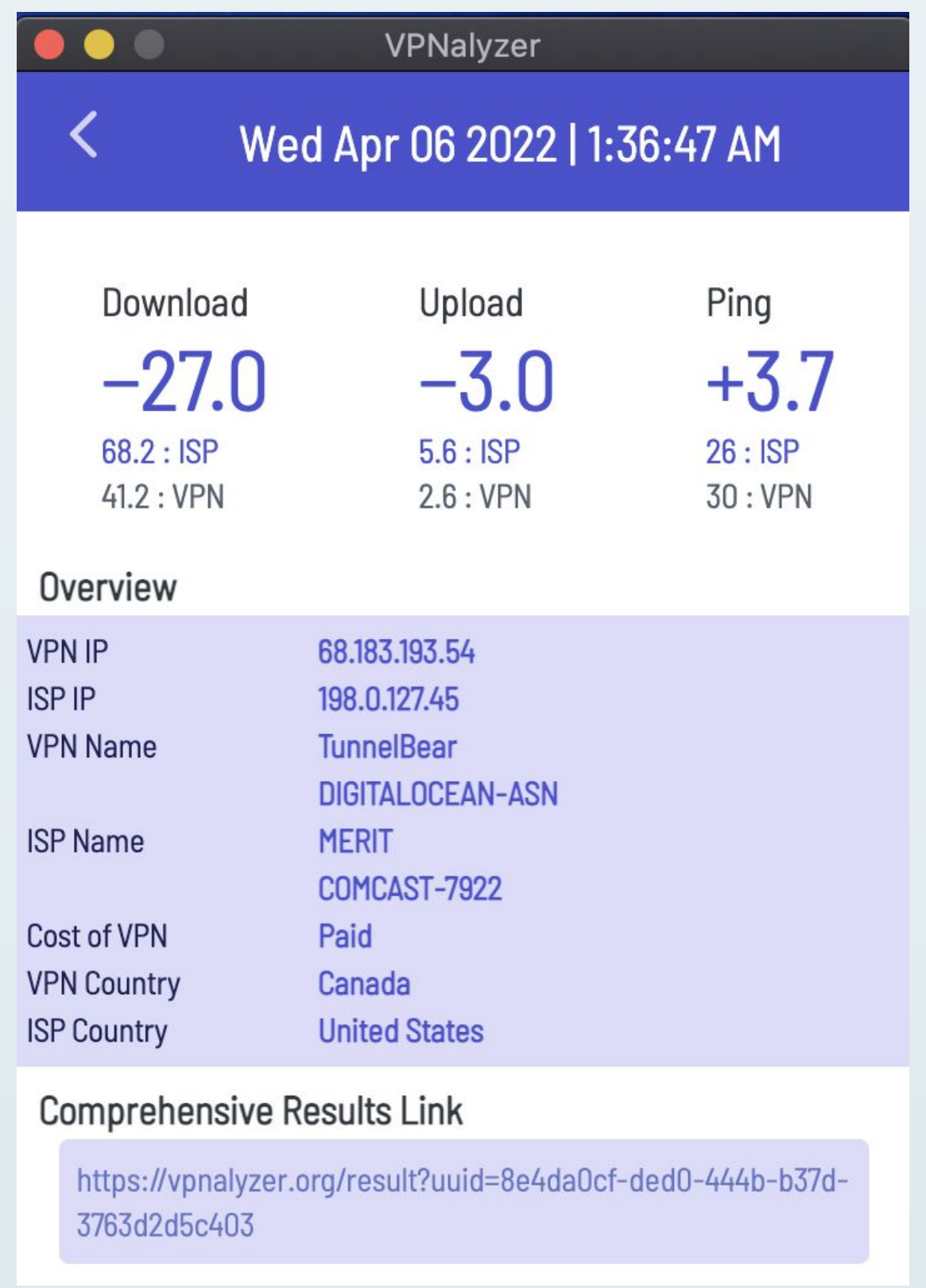
VPNalyzer System Architecture

- VPNalyzer has 14 tests implemented, including the Kill Switch Test, DNSSEC support, IPv6 Leakage, TLS Interception, Geolocation validation, Port Scan, Bandwidth and Latency estimation, and more.
- Along with the tests, the app collects packet capture. The data is uploaded to Google Cloud Storage for analysis. Preliminary results are available in the application and there is also a link to comprehensive results hosted on the website.



VPNalyzer Results Walkthrough

Immediate results as shown on the VPNalyzer tool



VPNalyzer

Wed Apr 06 2022 | 1:36:47 AM

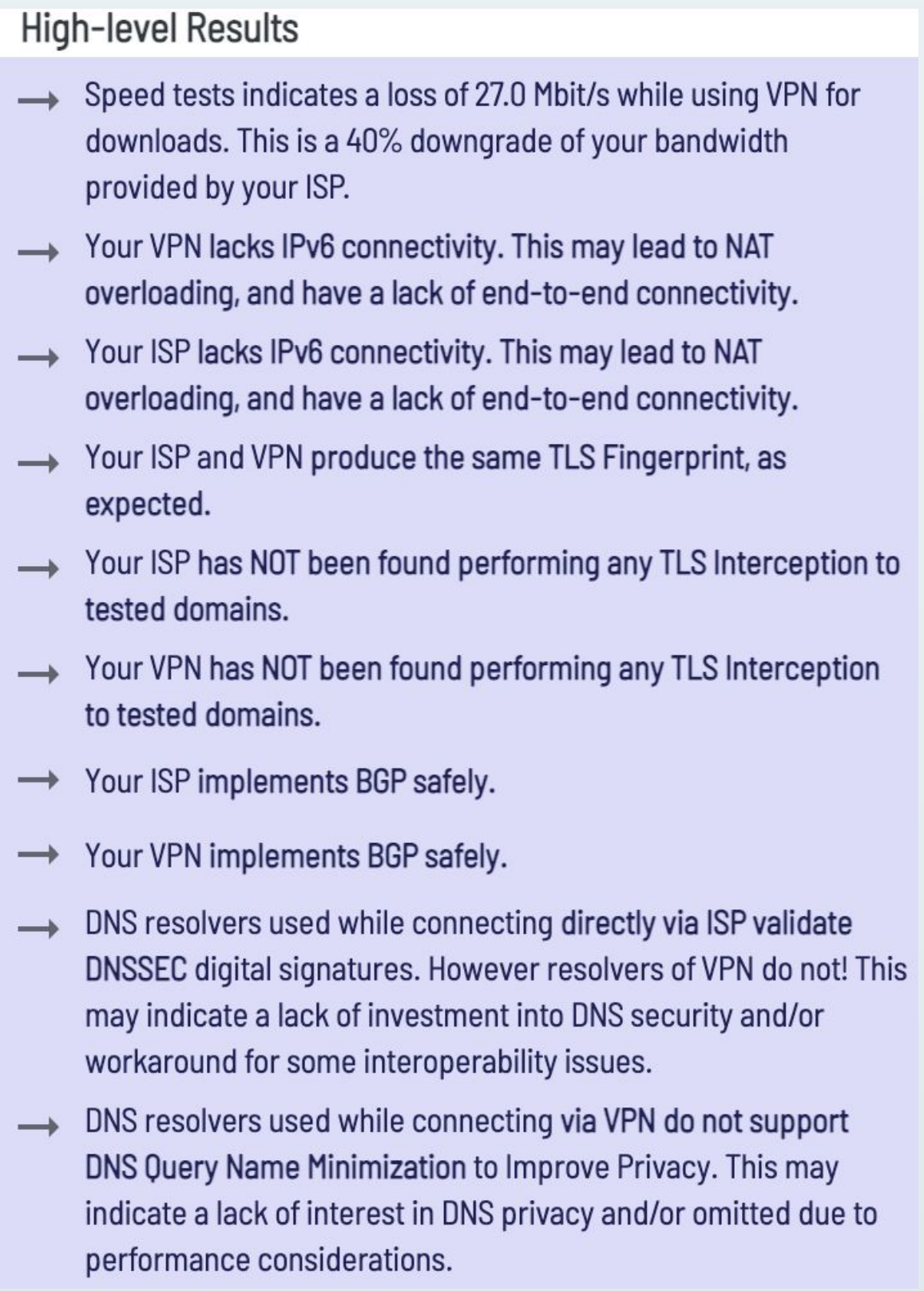
Download	Upload	Ping
–27.0	–3.0	+3.7
68.2 : ISP	5.6 : ISP	26 : ISP
41.2 : VPN	2.6 : VPN	30 : VPN

Overview

VPN IP	68.183.193.54
ISP IP	198.0.127.45
VPN Name	TunnelBear DIGITALOCEAN-ASN
ISP Name	MERIT COMCAST-7922
Cost of VPN	Paid
VPN Country	Canada
ISP Country	United States

Comprehensive Results Link

https://vpnalyzer.org/result?uuid=8e4da0cf-ded0-444b-b37d-3763d2d5c403



High-level Results

→ Speed tests indicates a loss of 27.0 Mbit/s while using VPN for downloads. This is a 40% downgrade of your bandwidth provided by your ISP.

→ Your VPN lacks IPv6 connectivity. This may lead to NAT overloading, and have a lack of end-to-end connectivity.

→ Your ISP lacks IPv6 connectivity. This may lead to NAT overloading, and have a lack of end-to-end connectivity.

→ Your ISP and VPN produce the same TLS Fingerprint, as expected.

→ Your ISP has NOT been found performing any TLS Interception to tested domains.

→ Your VPN has NOT been found performing any TLS Interception to tested domains.

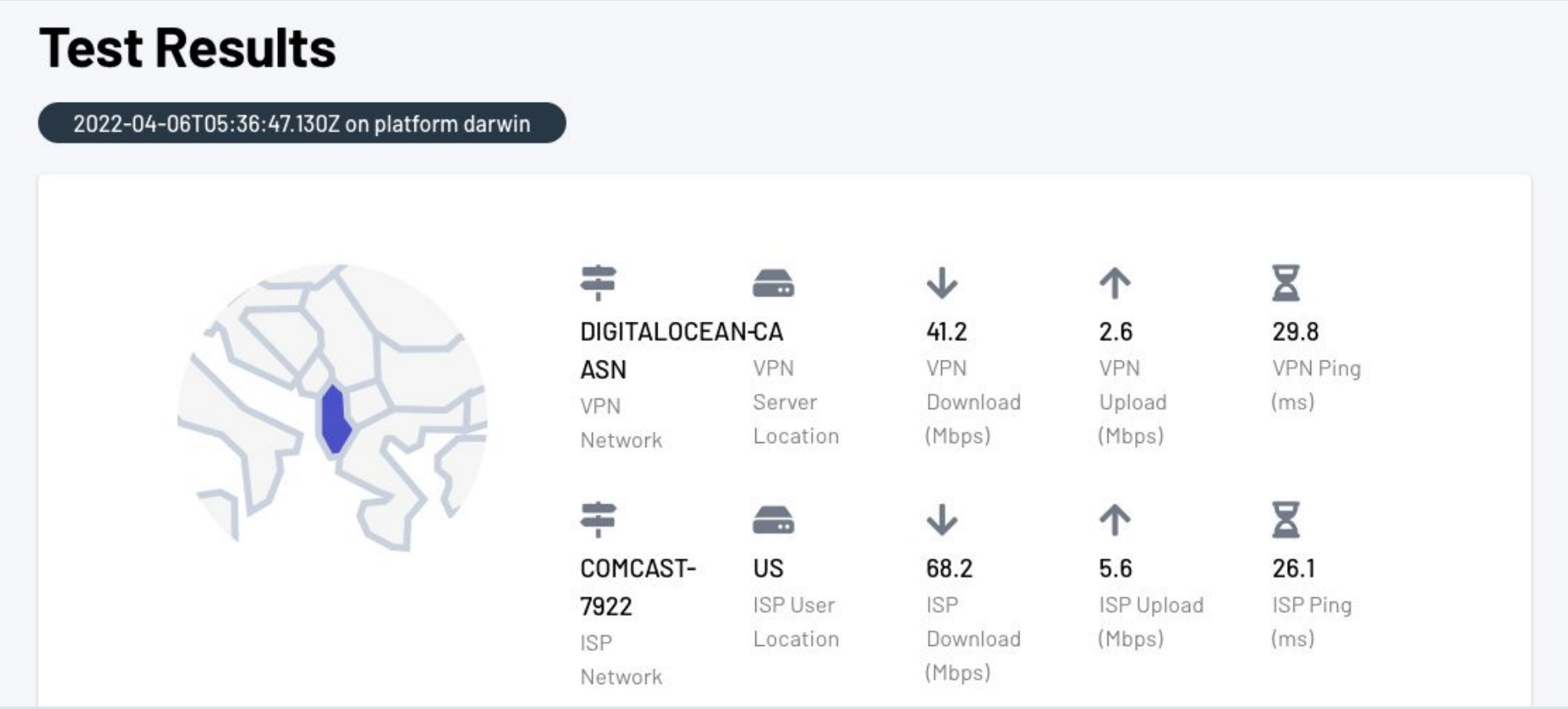
→ Your ISP implements BGP safely.

→ Your VPN implements BGP safely.

→ DNS resolvers used while connecting directly via ISP validate DNSSEC digital signatures. However resolvers of VPN do not! This may indicate a lack of investment into DNS security and/or workaround for some interoperability issues.

→ DNS resolvers used while connecting via VPN do not support DNS Query Name Minimization to Improve Privacy. This may indicate a lack of interest in DNS privacy and/or omitted due to performance considerations.

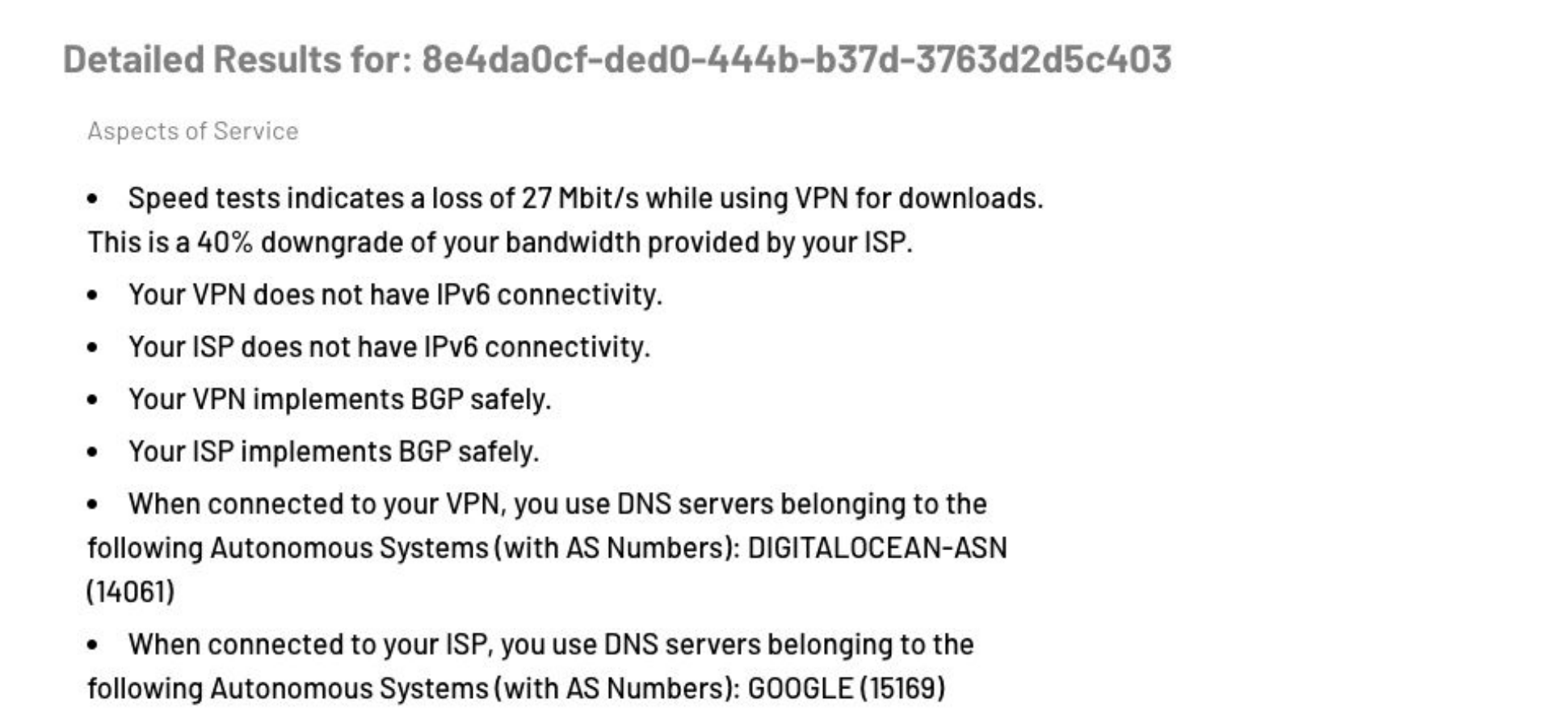
Comprehensive results hosted on the VPNalyzer website



Test Results

2022-04-06T05:36:47.130Z on platform darwin

DIGITALOCEAN-ASN	CA	41.2	2.6	29.8
VPN Network	VPN Server Location	VPN Download (Mbps)	VPN Upload (Mbps)	VPN Ping (ms)
COMCAST-7922	US	68.2	5.6	26.1
ISP Network	ISP User Location	ISP Download (Mbps)	ISP Upload (Mbps)	ISP Ping (ms)



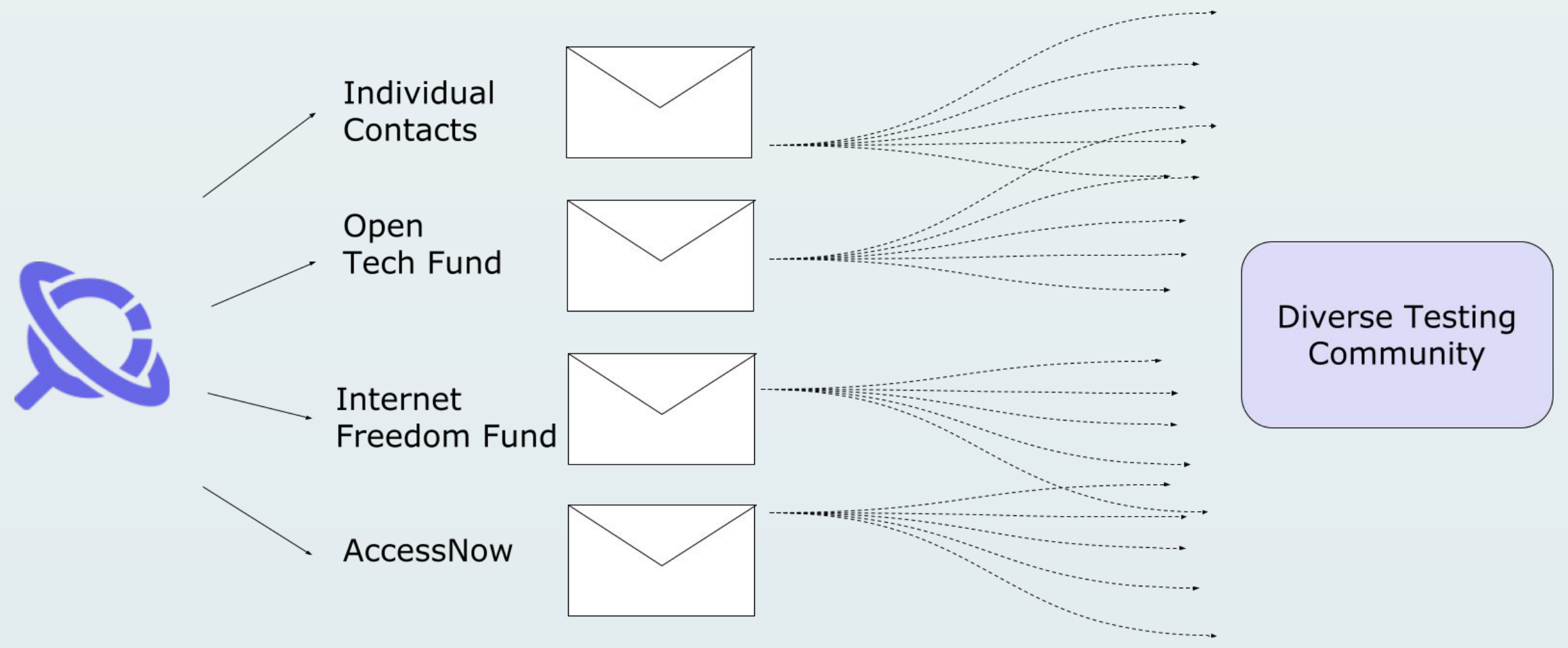
Detailed Results for: 8e4da0cf-ded0-444b-b37d-3763d2d5c403

Aspects of Service

- Speed tests indicates a loss of 27 Mbit/s while using VPN for downloads. This is a 40% downgrade of your bandwidth provided by your ISP.
- Your VPN does not have IPv6 connectivity.
- Your ISP does not have IPv6 connectivity.
- Your VPN implements BGP safely.
- Your ISP implements BGP safely.
- When connected to your VPN, you use DNS servers belonging to the following Autonomous Systems (with AS Numbers): DIGITALOCEAN-ASN (14061)
- When connected to your ISP, you use DNS servers belonging to the following Autonomous Systems (with AS Numbers): GOOGLE (15169)

Data Collection Pipeline

1. Launch tool for public use in April 2022
2. Collect crowdsourced, real-world data from users
3. Reach out to users in other countries



4. Conduct study assuming region-specific VPNs
5. Compare local VPNs from different regions
   a. Analyze security/privacy features and common leaks misconfigurations

Conclusion and Future Plans

In the pursuit of this capstone, I garnered a working knowledge of the fundamentals of VPN technology, as well as the work that was previously done on the VPNalyzer project. Additionally, I reached a working understanding of the current VPN landscape and the common deficiencies that are used to evaluate VPNs.

VPNalyzer is set to go public this summer 2022.

Interested in VPNalyzer? Scan this code to join the mailing list and be informed when the tool is available for public release!