VOLATILE VAULT – DATA EXFIL IN 2024

[PATRICK EISENSCHMIDT & MORITZ THOMAS]

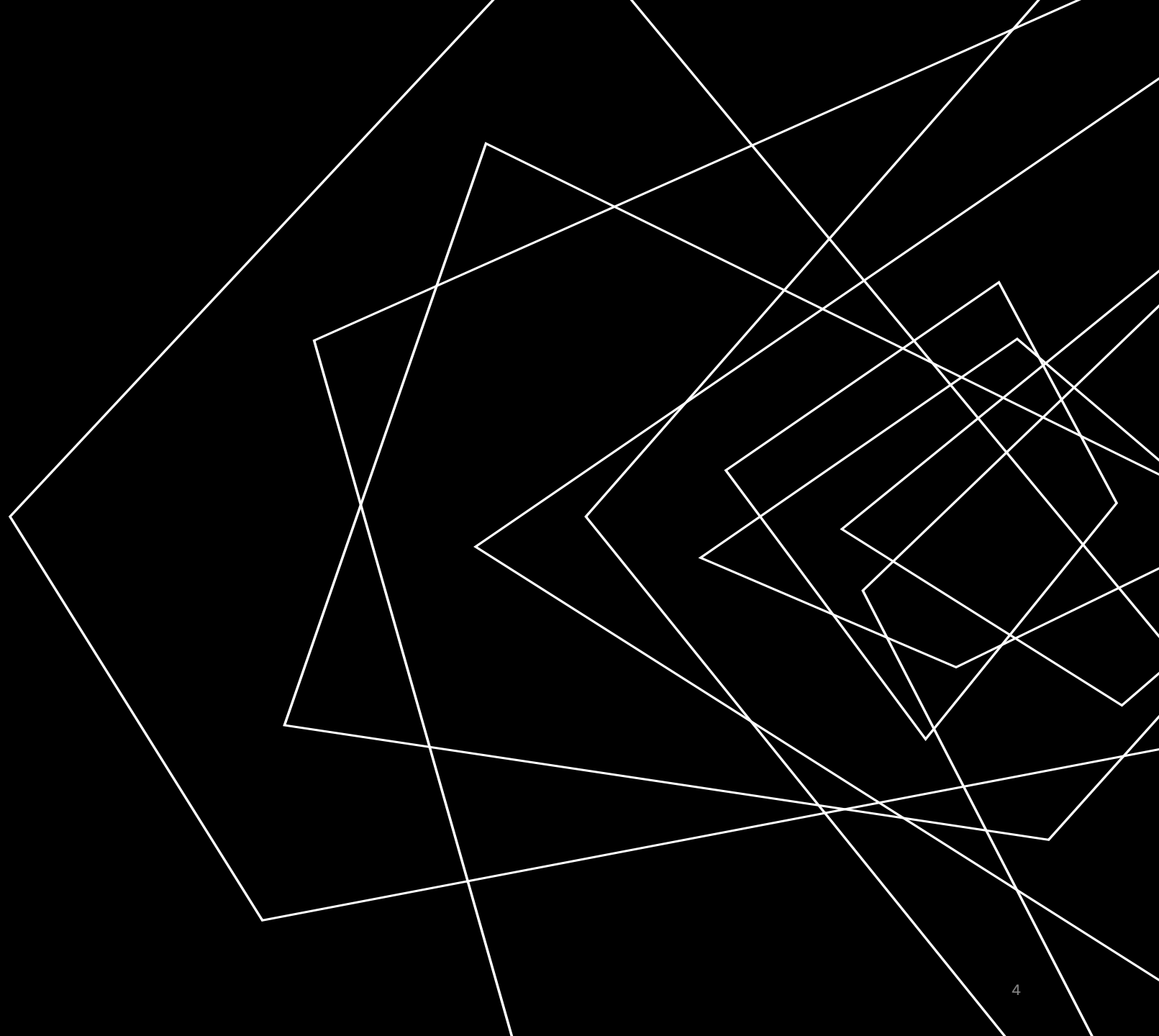
AGENDA

$WHOAMI

Background and Motivation

Detailed Tool Explanation

> Demo



MORITZ THOMAS

@MORITZLTHOMAS

RED TEAM OPERATOR / R&D LEAD
@NVISO SECURITY – ARES

(ADVERSARIAL RISK EMULATION AND SIMULATION)

PATRICK EISENSCHMIDT

@SECDU_DE

RED TEAM MANAGER / LEAD
@NVISO SECURITY - ARES

(ADVERSARIAL RISK EMULATION AND SIMULATION)

NVISO SECURITY

European cybersecurity consulting

Prevent: Pentests, Red Teaming (TLPT/TIBER), ISMS, Awareness, ...

Detect: MDR, SOC, Detection Engineering, ...

Respond: Incident Response, Forensics, ...

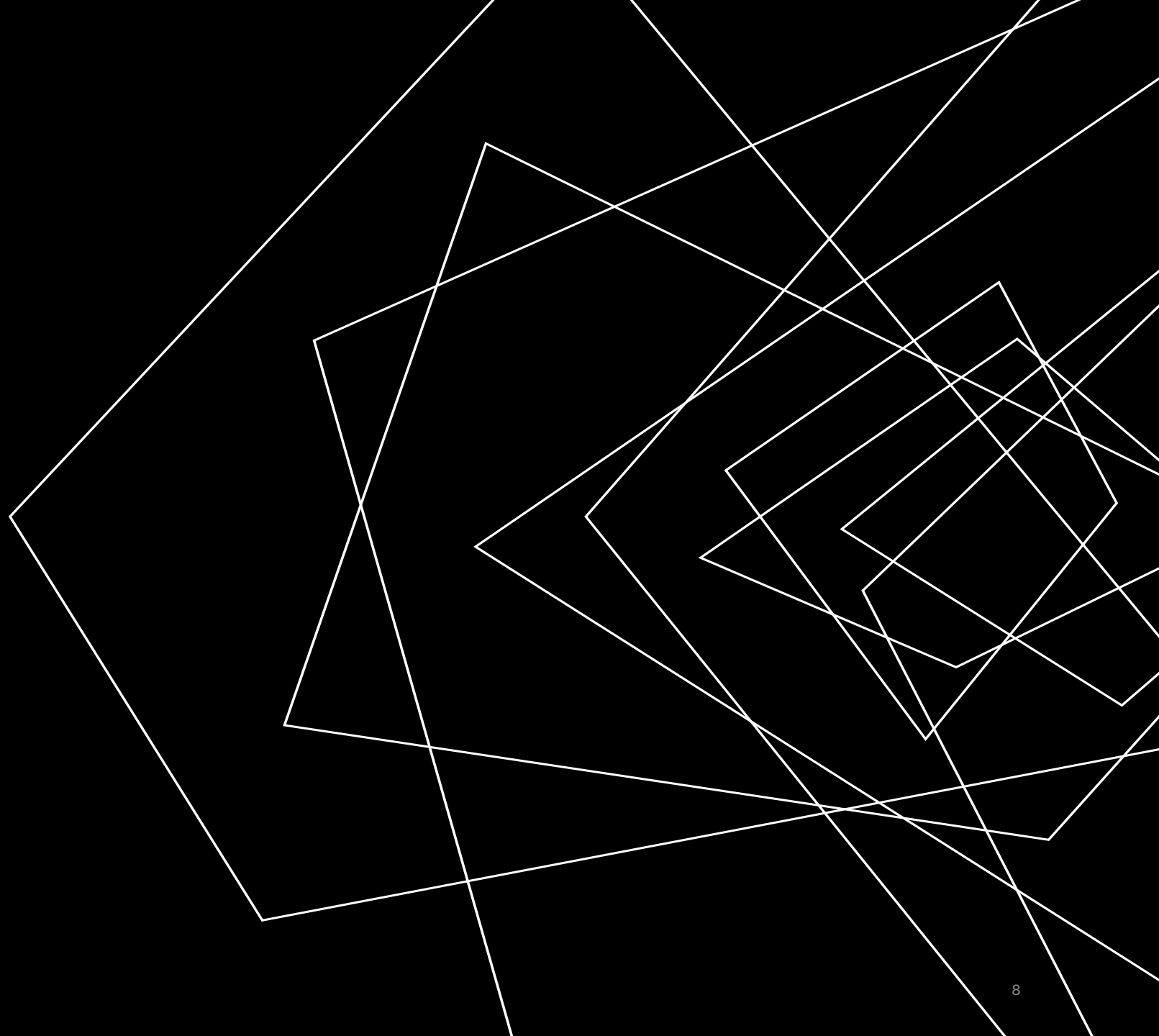
AGENDA

$WHOAMI

Background and Motivation

Detailed Tool Explanation

> Demo



DATA LOSS PREVENTION

Strategies or measures to prevent unauthorized outflow of sensitive data.

> **Protect confidential information** against

Data Extrusion

Insider Threats

Data Exposure

DATA LOSS PREVENTION (DLP)

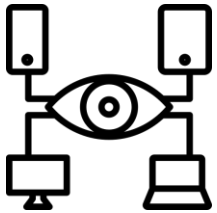
How does it work?

Identification and classification

- Content Inspection
  Scan files, emails, and other data forms for specific patterns, keywords, or metadata to identify sensitive information.
- Contextual Analysis
  Analyze the context in which data is used, such as who is accessing it, where it is being sent, and how it is being handled.
- Data Classification
  Classify data based on predefined categories such as Personally Identifiable Information (PII), financial data, intellectual property, and more.

DATA LOSS PREVENTION (DLP)

Types of DLP solutions?

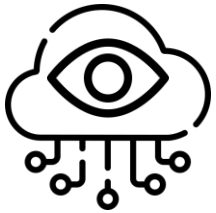


Network Monitoring

Network
ForcePoint DLP
McAfee Total Protection
Zscaler Cloud DLP
E-Mail
MimeCast
Symantec Email Security
Files
Palo Alto
Cisco Umbrella

Endpoint Monitoring

Device Control
Symantec Endpoint DLP
McAfee Endpoint Security
User Activity
CrowdStrike Falcon
Carbon Black



Cloud Monitoring

Data Flow
Netskope
Microsoft Cloud App Security
Microsoft Purview
AWS Macie
Google Cloud DLP

DATA LOSS PREVENTION (DLP)

What does it do?

Protection Capabilities

- Data Encryption
- Access Controls
- Blocking and Quarantine
- Policy Enforcement

MOTIVATION
Red Teaming against DLP

Popular Bypasses

- Renaming file types
- Encrypting / packing data
- Steganography
- DNS
- Certificates
- Chunked HTTP(S) uploads

> Chunked HTTPS uploads but via multiple reputable domains

> Relatively new (unsupported) protocol

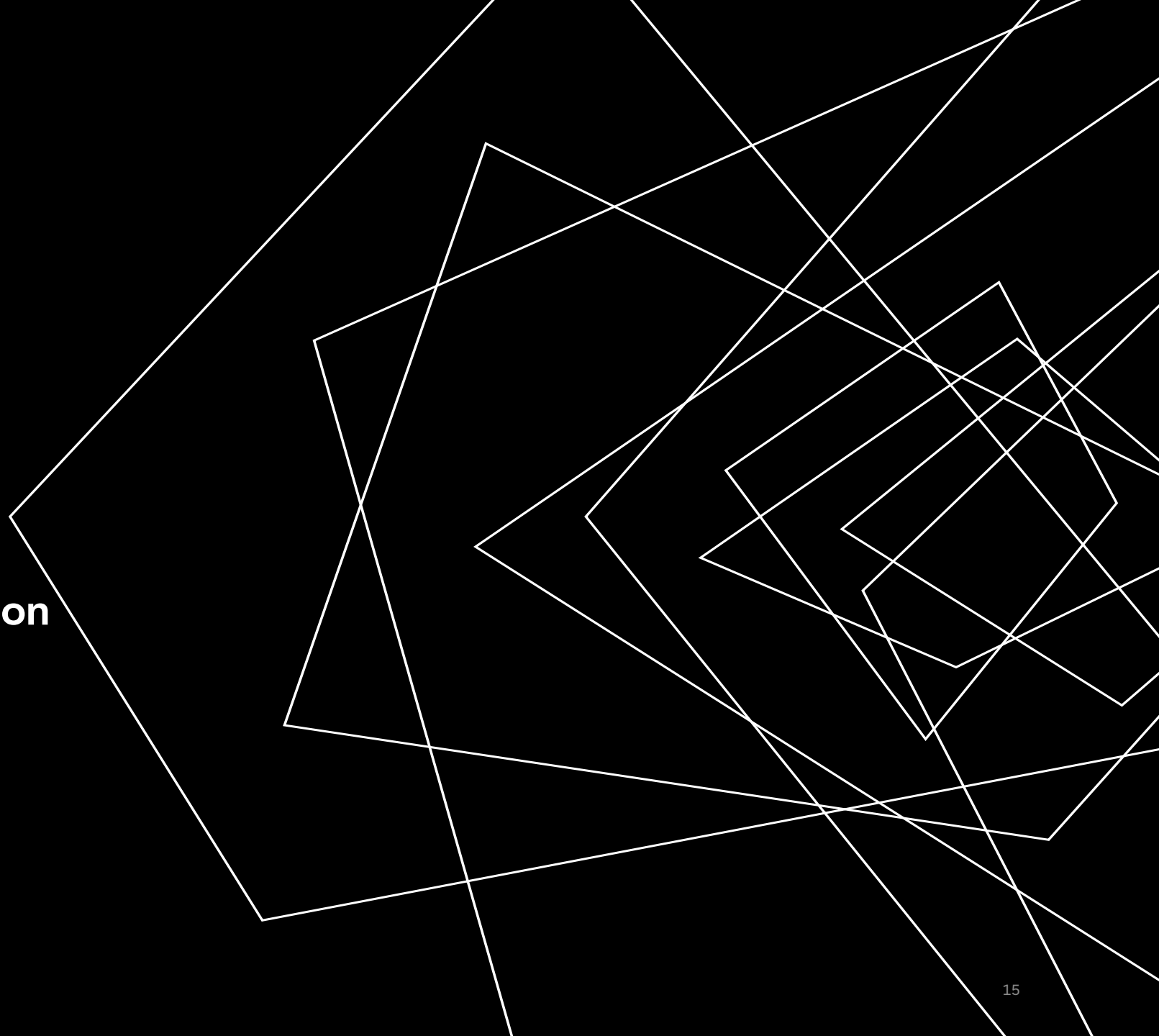
AGENDA

$WHOAMI

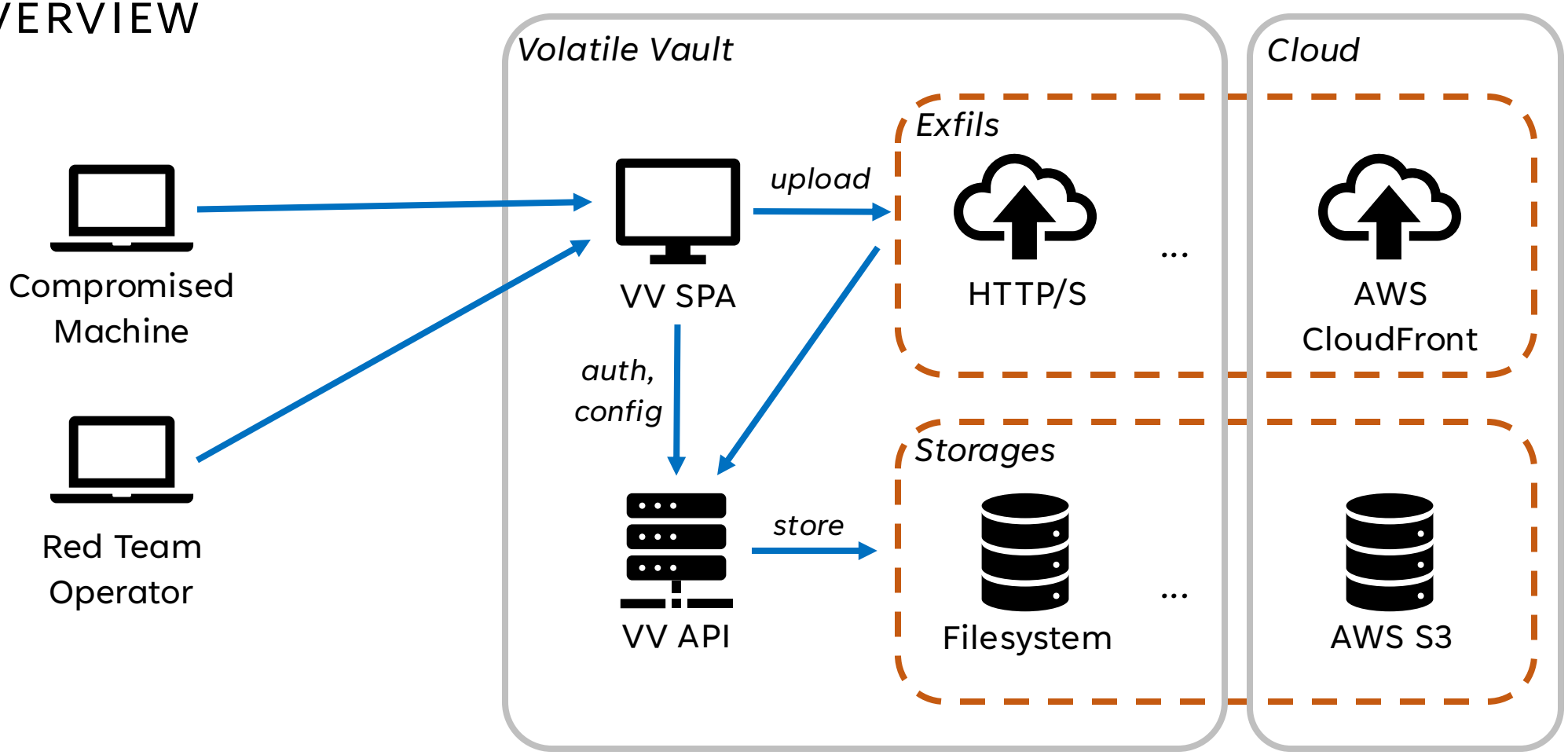
Background and Motivation

Detailed Tool Explanation

> Demo



ARCHITECTURE OVERVIEW



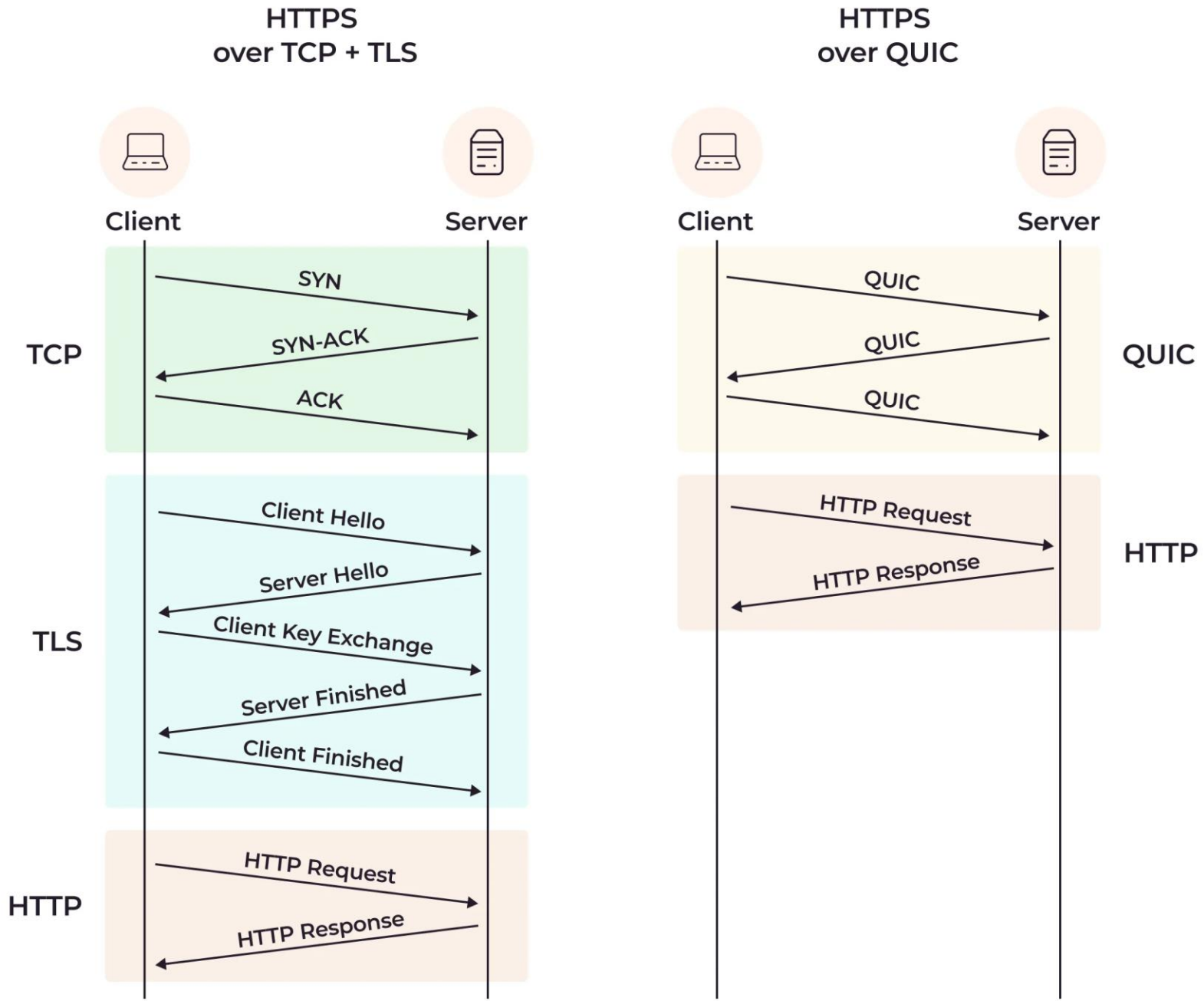
PROTOCOL

HTTP.3 VIA QUIC

HTTP.3 runs on QUIC which uses UDP instead of TCP allows for seamless connection migration, higher security and performance.

QUIC (Quick UDP Internet Connections) is a transport layer network protocol developed by Google in 2012 and was adopted by the IETF in 2013.

see IETF: RFC8999 - RFC9002


HTTPS
over TCP + TLS
Client
Server
TCP
SYN
SYN-ACK
ACK
TLS
Client Hello
Server Hello
Client Key Exchange
Server Finished
Client Finished
HTTP
HTTP Request
HTTP Response
HTTPS
over QUIC
Client
Server
QUIC
QUIC
QUIC
QUIC
HTTP
HTTP Request
HTTP Response

HTTP.3 VIA QUIC - BENEFITS

- Faster Connection Establishment
- Reduced Latency
- Improved Security
- Better Performance on Unstable Networks
- Seamless Connection Migration

> Limited support, relatively new protocol

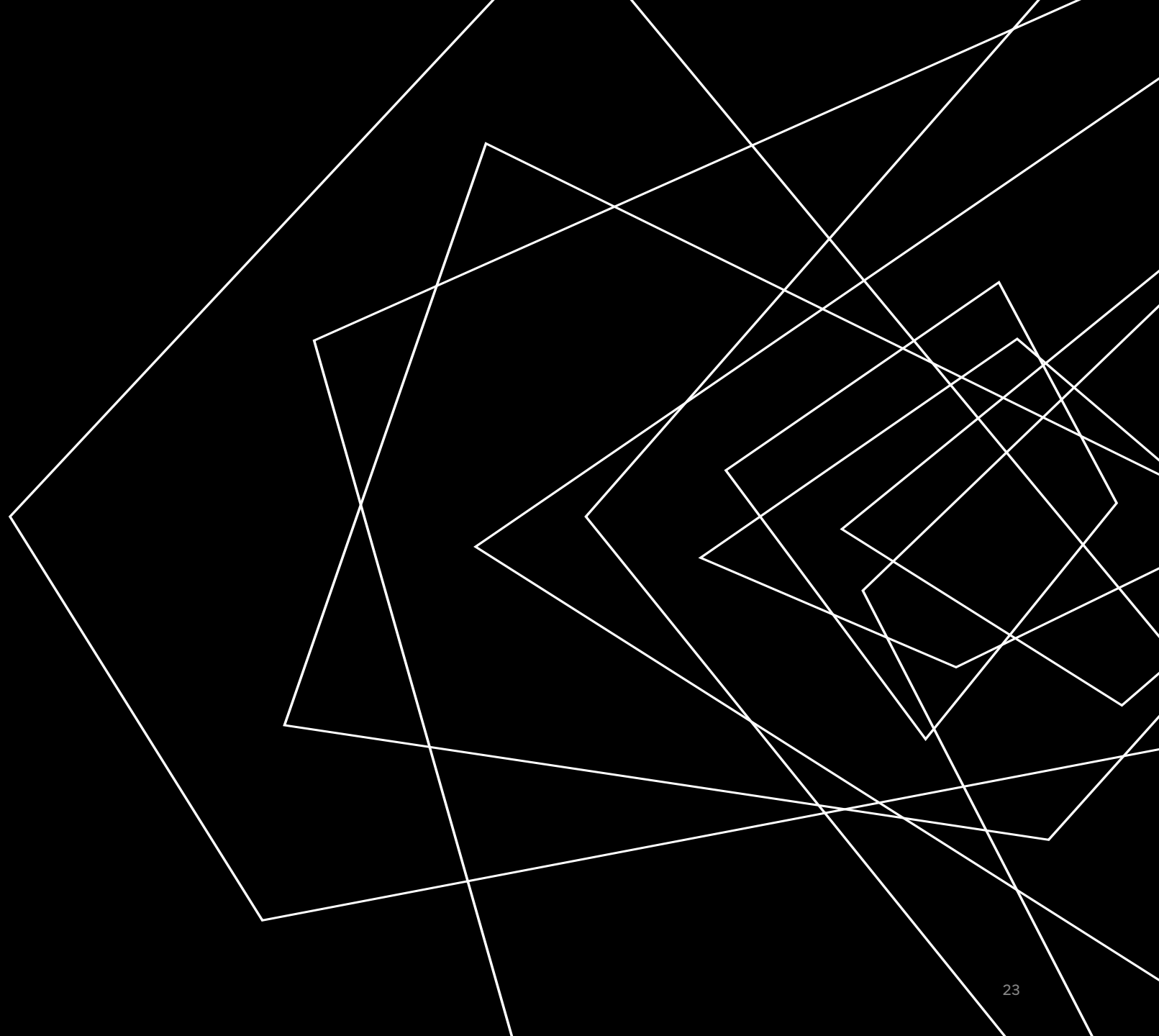
AGENDA

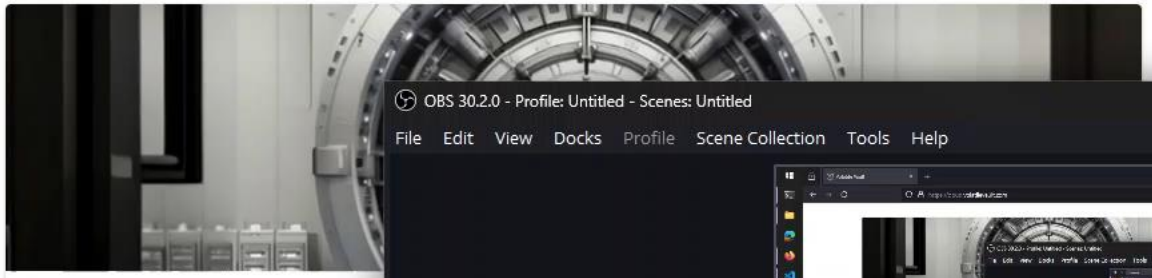
$WHOAMI

Background and Motivation

Detailed Tool Explanation

> Demo





Volatile Vault

Welcome to Volatile Vault. This scree
downloaded and stored. Use the follo

1. Authentication
   - Code
2. What would you like to do?
3. Which transport should be used
4. *No transport selected yet.*
5. *Downloads will determine the sto*
6. *No storage selected.*

OBS 30.2.0 - Profile: Untitled - Scenes: Untitled

File Edit View Docks Profile Scene Collection Tools Help

No source selected | Properties | Filters

Scenes: Scene

Sources: Display Capture

Audio Mixer: Desktop Audio 0.0 dB

Scene Transitions: Fade, Duration 300 ms

Controls: Start Streaming, Stop Recording, Start Virtual Camera, Studio Mode, Settings, Exit

00:00:00 | 00:00:00 | CPU: 0.2% | 60.00 / 60.00 FPS

https://cloud.volatilevault.com

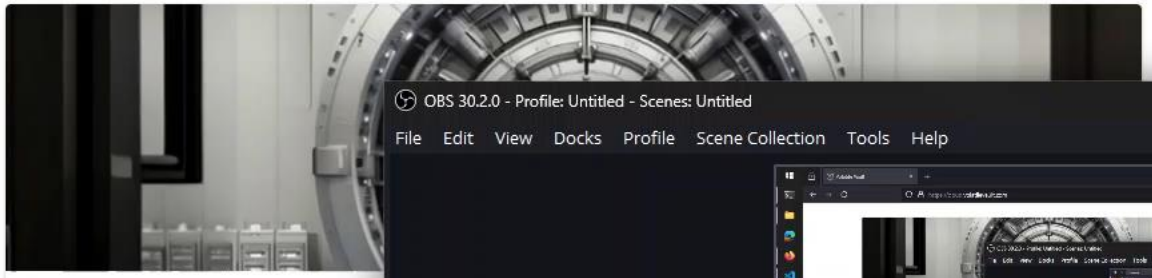
Inspector Console Debugger Network Style Editor Performance

All HTML CSS JS XHR Fonts Images Media WS Other

1 request | 36 B / 423 B transferred | Finish: 4,18 s | DOMContentLoaded: 4,16 s | load: 12,49 s

ENG

01:57
09/08/2024



Volatile Vault

Welcome to Volatile Vault. This scree
downloaded and stored. Use the follo

1. Authentication
   - Code
2. What would you like to do?
3. Which transport should be used
4. *No transport selected yet.*
5. *Downloads will determine the sto*
6. *No storage selected.*

OBS 30.2.0 - Profile: Untitled - Scenes: Untitled

File Edit View Docks Profile Scene Collection Tools Help

No source selected | Properties | Filters

Scenes: Scene

Sources: Display Capture

Audio Mixer: Desktop Audio 0.0 dB

Scene Transitions: Fade, Duration 300 ms

Controls: Start Streaming, Start Recording, Start Virtual Camera, Studio Mode, Settings, Exit

00:00:00 | 00:00:00 | CPU: 0.1% | 60.00 / 60.00 FPS

Volatile Vault — https://cloud.volatilevault.com

Inspector | Console | Debugger | Network | Style Editor | Performance

Filter URLs | Disable Cache | No Throttling

All HTML CSS JS XHR Fonts Images Media WS Other

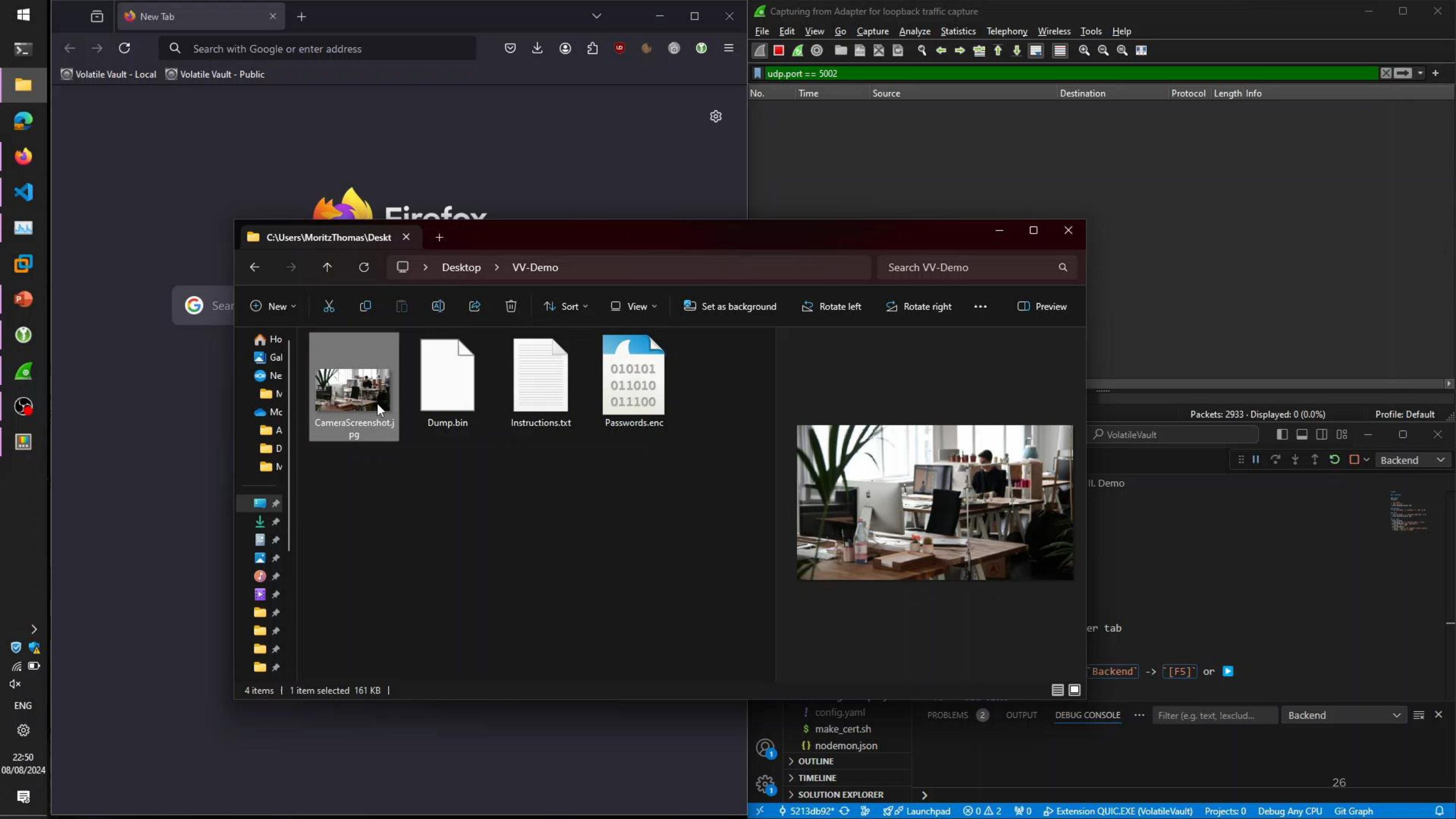
Type | Tr | Size

1 | json | 42 | 36 B

1 request | 36 B / 423 B transferred | Finish: 11,16 s | DOMContentLoaded: 11,10 s | load: 11,10 s

ENG

01:45
09/08/2024


New Tab
Search with Google or enter address
Volatile Vault - Local
Volatile Vault - Public
Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port == 5002
No. Time Source Destination Protocol Length Info
C:\Users\MoritzThomas\Deskt
Desktop › VV-Demo
Search VV-Demo
New Sort View Set as background Rotate left Rotate right Preview
CameraScreenshot.jpg
Dump.bin
Instructions.txt
Passwords.enc
010101
011010
011100
4 items | 1 item selected 161 KB
Packets: 2933 · Displayed: 0 (0.0%)
Profile: Default
VolatileVault
Backend
config.yaml
make_cert.sh
nodemon.json
OUTLINE
TIMELINE
SOLUTION EXPLORER
PROBLEMS 2
OUTPUT
DEBUG CONSOLE
Filter (e.g. text, !exclud...
Backend
ENG
22:50
08/08/2024

KEY TAKEAWAYS

- **Framework for bypassing DLP solutions**
  - **Open Source**
  - **Modular and extensible**
  - **Mix & Match**
- **Two new methods**
  - **Chunked upload with 1 chunk: 1 domain via Cloudfront CDN**
  - **QUIC protocol**
- **Blue Team: DLP Testing Tool**

THANK YOU

Patrick Eisenschmidt

@secdu_de

patrick-eisenschmidt

Moritz Thomas

@moritzlthomas

moritzlthomas

GitHub: https://github.com/molatho/VolatileVault