DNS As An Early Warning System

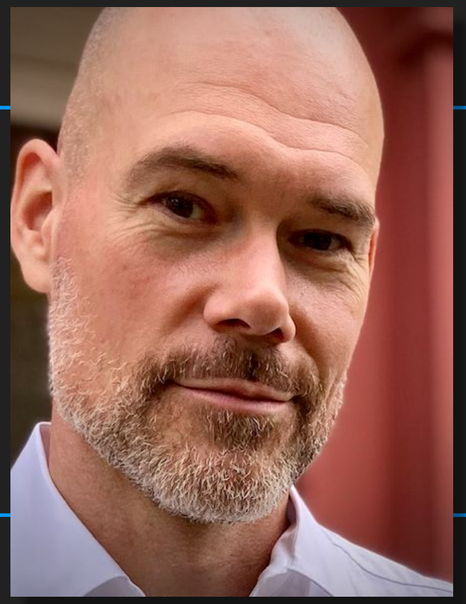
Practical DNS Telemetry For Early Threat Detection and Response

Andreas Taudte
Senior Technical Marketing Manager

efficient iP®

March 2026

Speaker



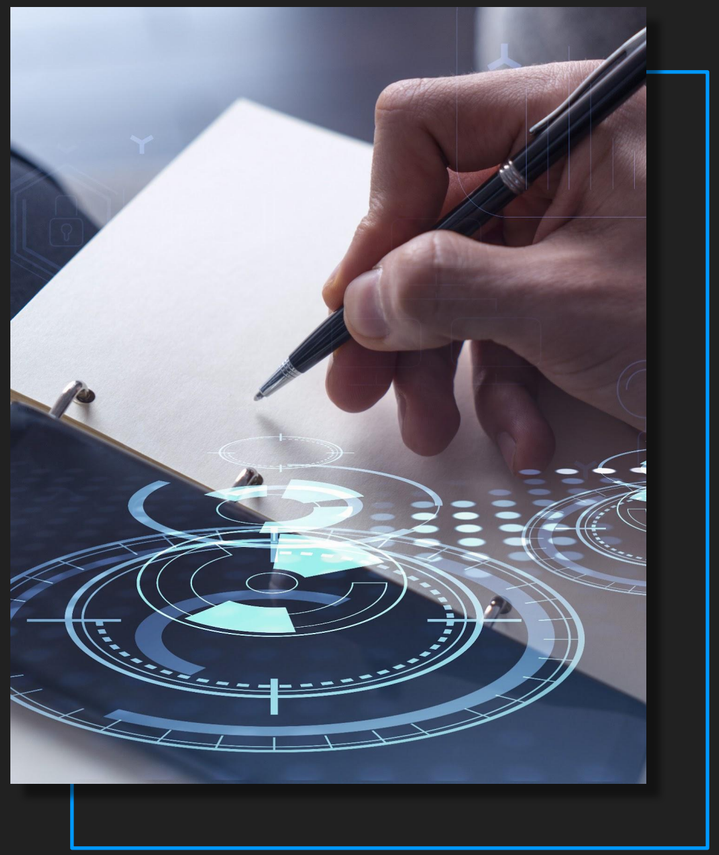
ataudte ataudte ataudte ataudte

Andreas Taudte

Senior Technical Marketing Manager

- 15+ years in DDI across enterprise and public-sector environments
- Delivered architectures, migrations, workshops, and governance models
- Turning complex DDI topics into clear, decision-ready guidance
- Connecting practitioners through the DDI User Group

Agenda



1. Where DNS Becomes A Security Signal
2. Real-Life Signals In DNS Traffic
3. From DNS Signals To Detection And Validation

Where DNS Becomes A Security Signal

efficient iP®

DNS – The Ignored Component

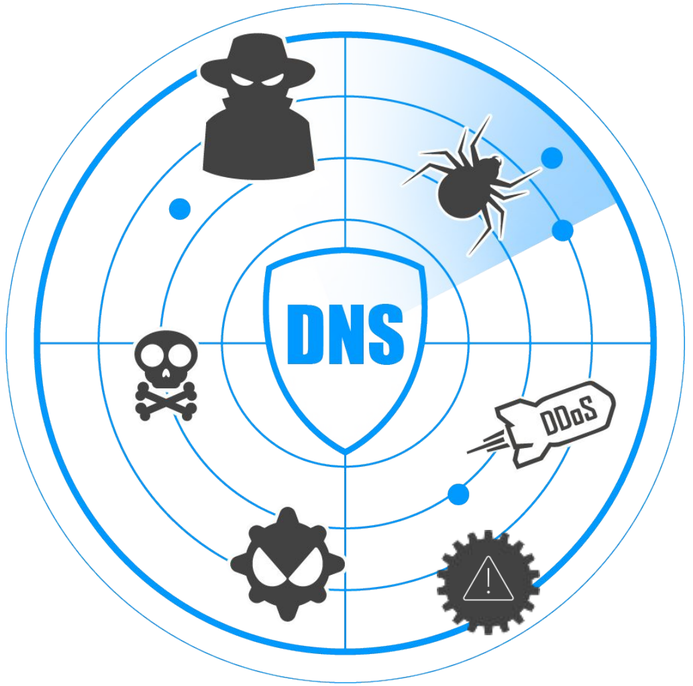
- DNS is foundational but rarely monitored
- Most security tools lack DNS specific visibility
- Logs alone do not create visibility

What Hides In DNS Traffic

- Active threats (exfiltration, C&C, DGA, tunneling, phishing, etc.)
- Early warning signals (reconnaissance, staging, pre-positioning, DGA ramp-up, etc.)
- Volume attacks and stress patterns (floods, spikes, etc.)
- Operational issues (misconfigurations, malfunctions, abnormality, etc.)
- External dependency issues (routing, peering, cloud outages)

Indicators Of Abuse In DNS

- Algorithmically generated domain names
- Oversized labels and deeply nested subdomains
- Spikes in non-existent domain (`NXDOMAIN*`) responses
- Unusual record types
- Query patterns and query volume



*** WPAD, search list, localhost, TTL issues, etc.**

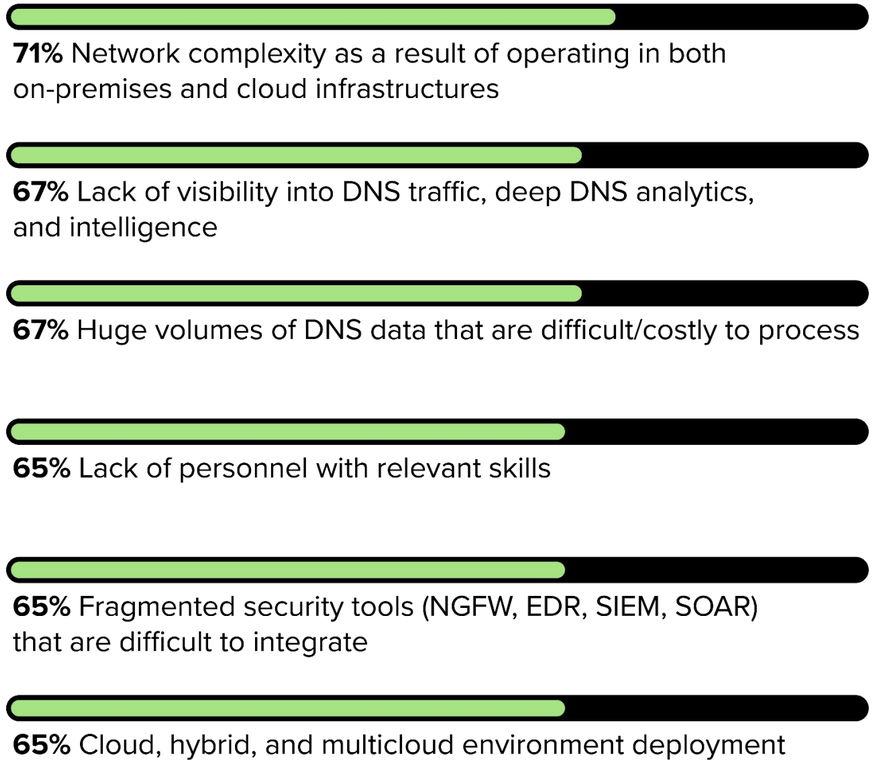
DNS provides early indicators, but not every anomaly is malicious.

The Visibility Gap

- Mixed DNS vendors and servers
- Fragmented visibility
- Inconsistent logs
- Too much DNS data
- Limited skills and staffing

“How challenging are each of the following to your security teams to effectively defend and protect your network?”

(Showing “Highly challenging” and “Challenging”)

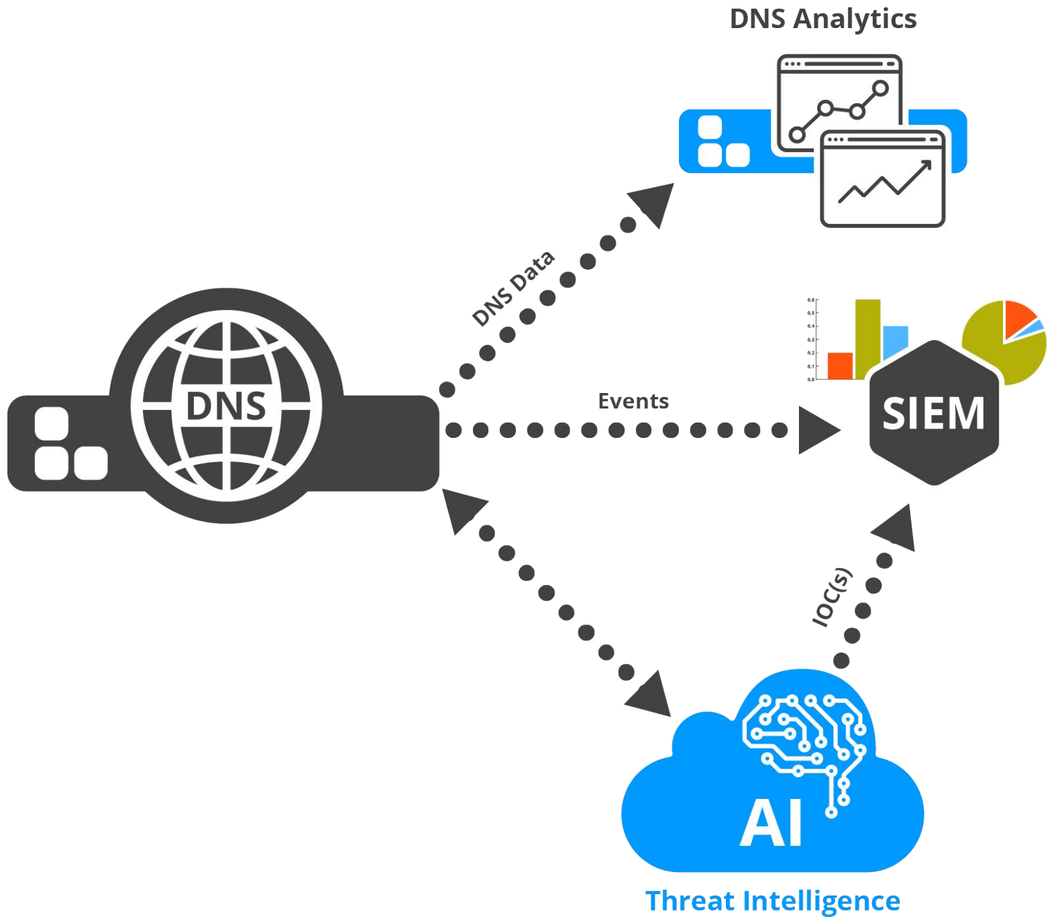


Source: Forrester 2025 Study on DNS Security in a Cloud Era

Base: 218 decision-makers with responsibility for their organization’s security and threat intelligence strategy
Source: Forrester’s Q2 2025 DNS Security Survey [E-62853]

From Logging To Response

- Detection ≠ defense
- DNS signals enable visibility for decisions
- Signals must trigger investigation

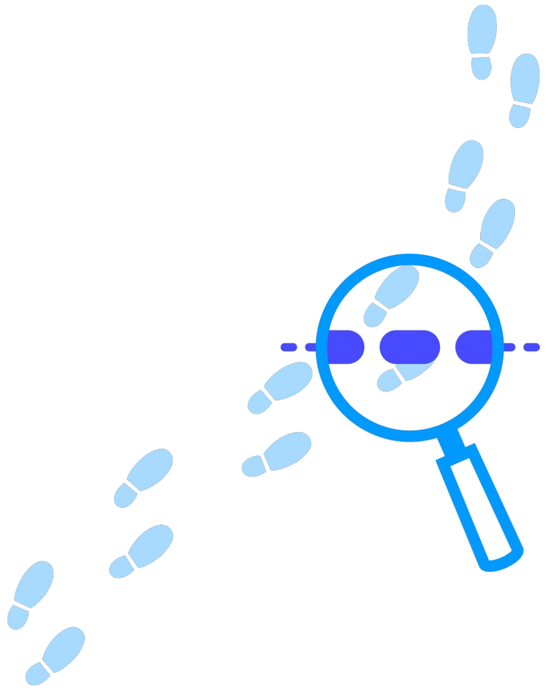


Real-Life Signals In DNS Traffic

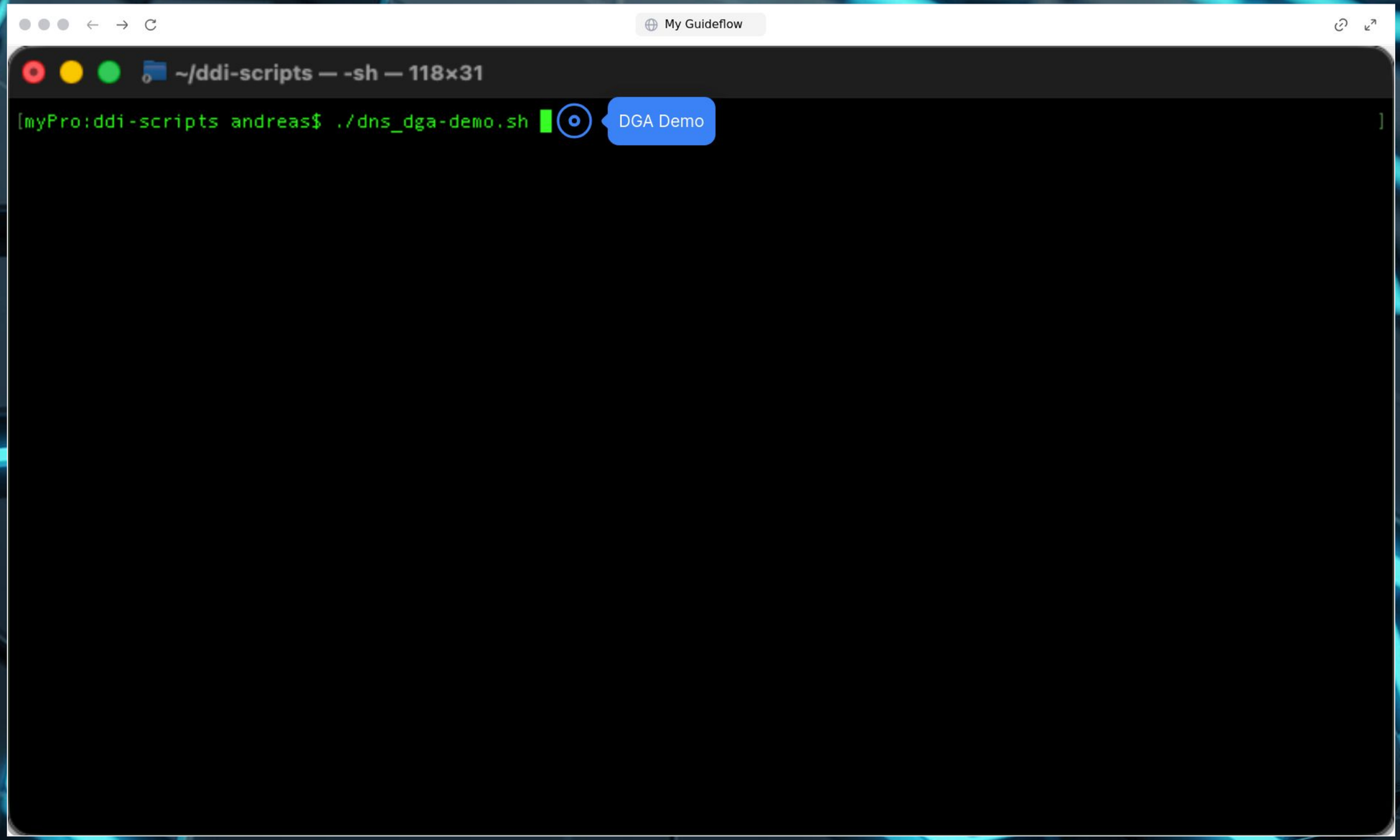
efficient iP®

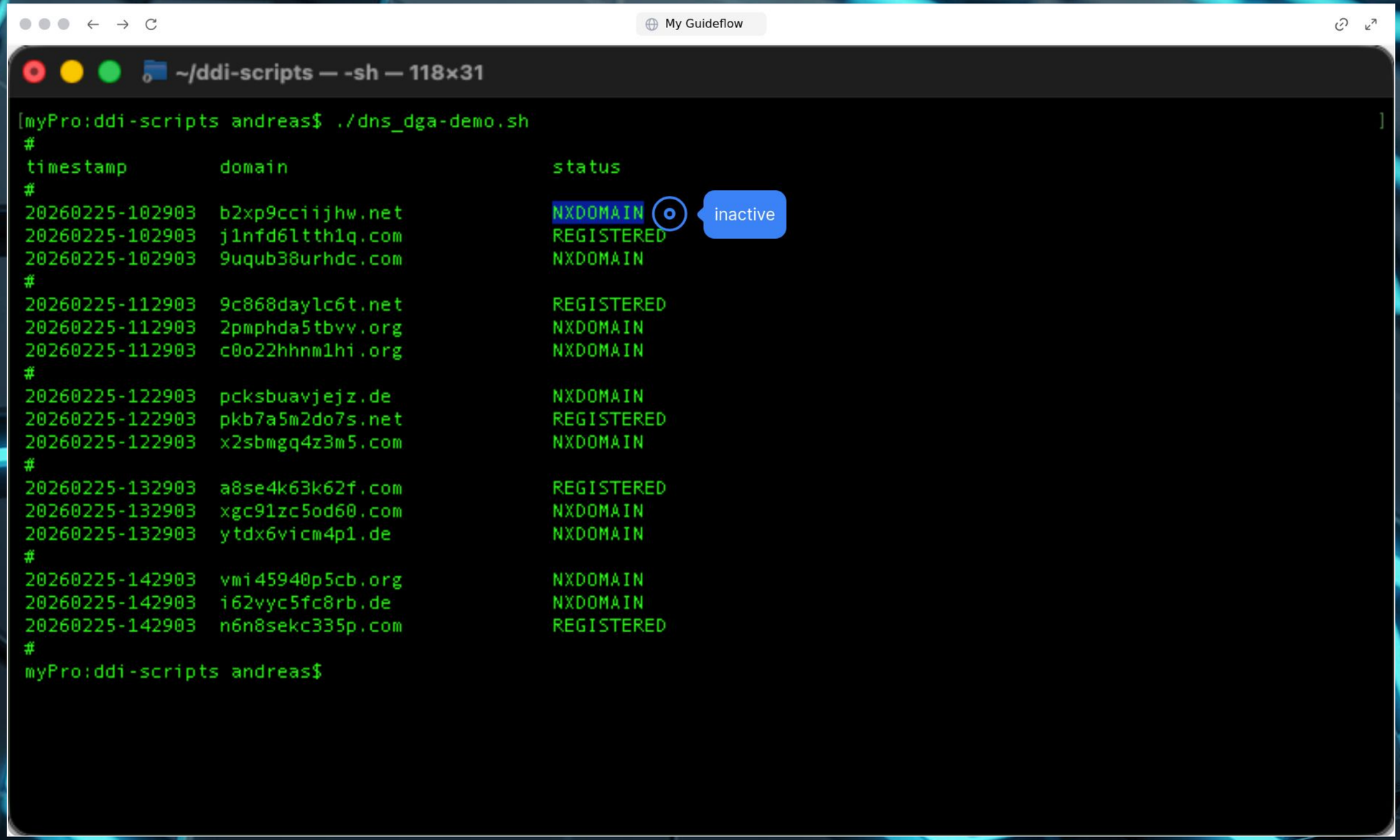
Algorithmic Domain Names

- High entropy labels
- No linguistic structure
- Repetitive querying of non-existent names



Demo: DGA & N-gram



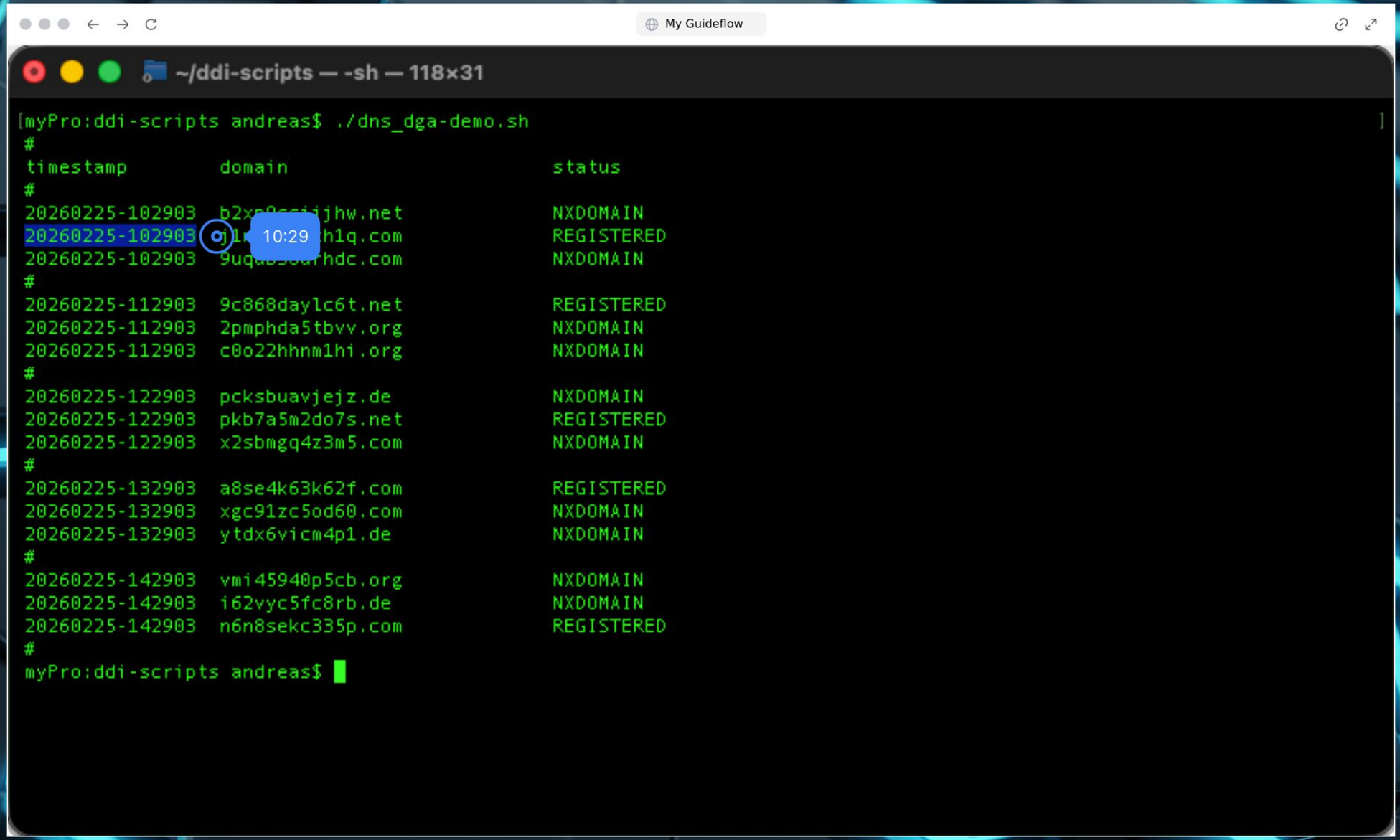


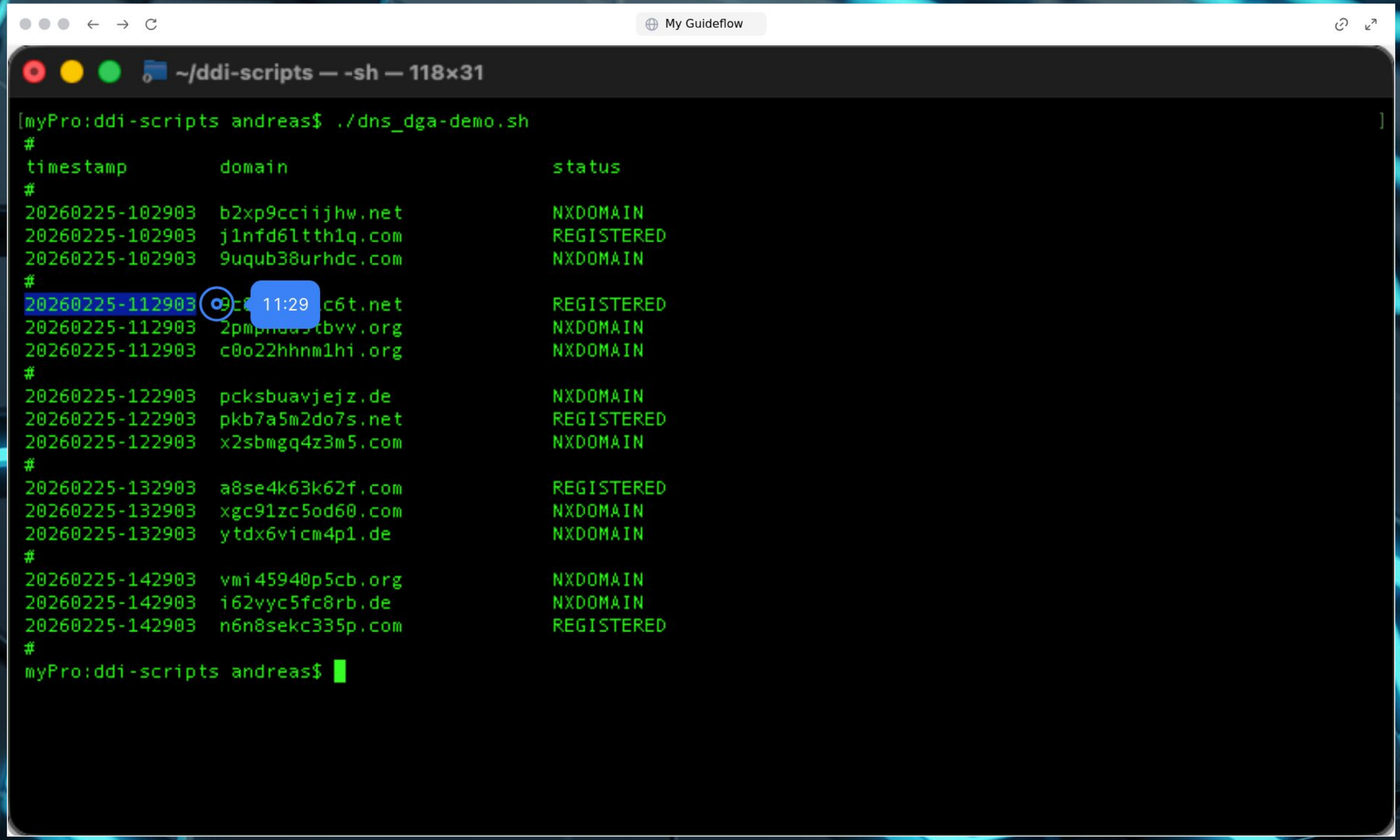
My Guideflow

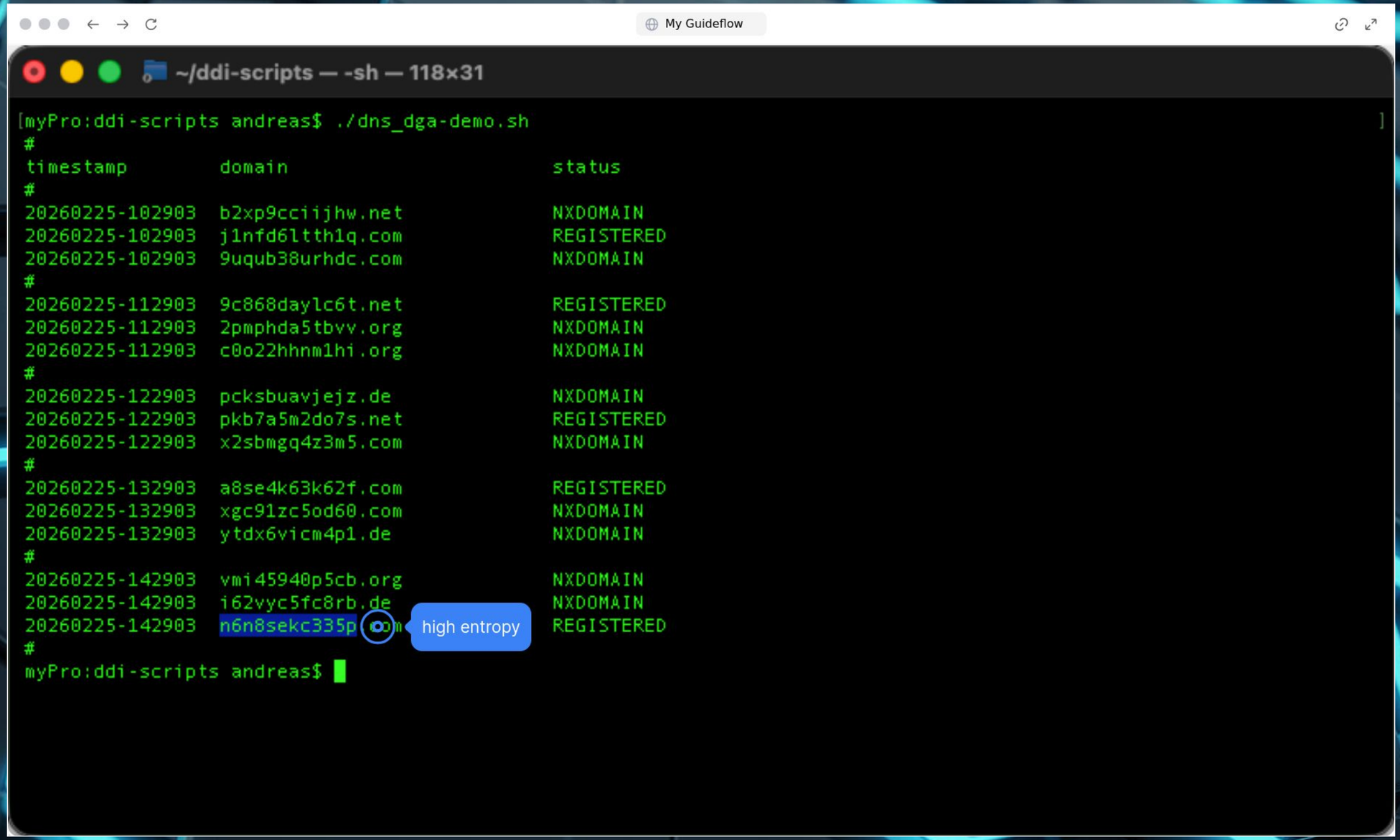
~/ddi-scripts — -sh — 118×31

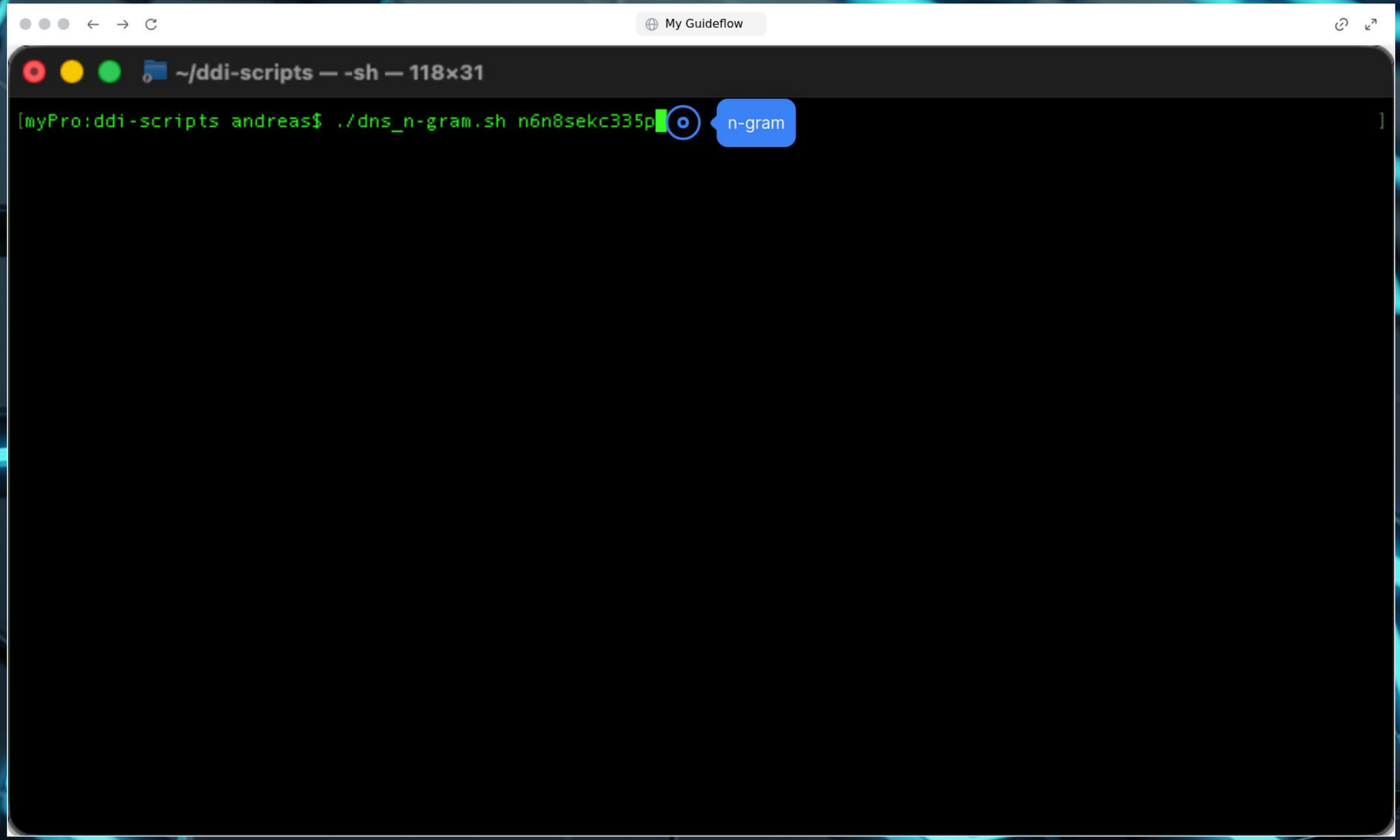
```
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh                                  ]
#
timestamp        domain                    status
#
20260225-102903  b2xp9cciijhw.net          NXDOMAIN
20260225-102903  j1nfd6ltth1q.com         REGISTERED
20260225-102903  9uqub38urhdc.com         NXDOMAIN
#
20260225-112903  9c868daylc6t.net          REGISTERED
20260225-112903  2pmphda5tbvv.org          NXDOMAIN
20260225-112903  c0o22hhnm1hi.org          NXDOMAIN
#
20260225-122903  pcksbuavjejz.de           NXDOMAIN
20260225-122903  pkb7a5m2do7s.net          REGISTERED
20260225-122903  x2sbmgq4z3m5.com          NXDOMAIN
#
20260225-132903  a8se4k63k62f.com          REGISTERED
20260225-132903  xgc91zc5od60.com          NXDOMAIN
20260225-132903  ytdx6vicm4p1.de           NXDOMAIN
#
20260225-142903  vmi45940p5cb.org          NXDOMAIN
20260225-142903  i62vyc5fc8rb.de           NXDOMAIN
20260225-142903  n6n8sekc335p.com          REGISTERED
#
myPro:ddi-scripts andreas$
```

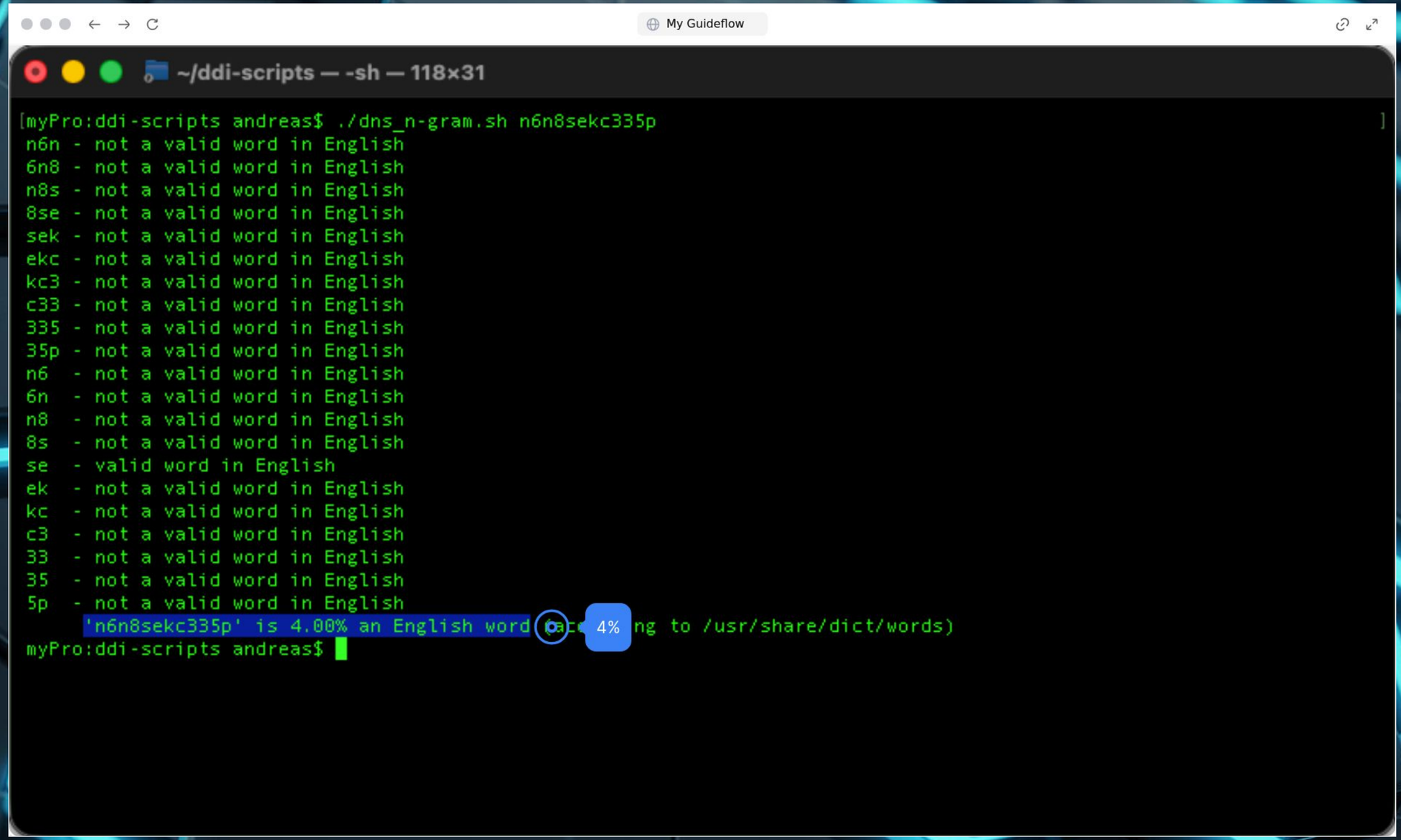
active

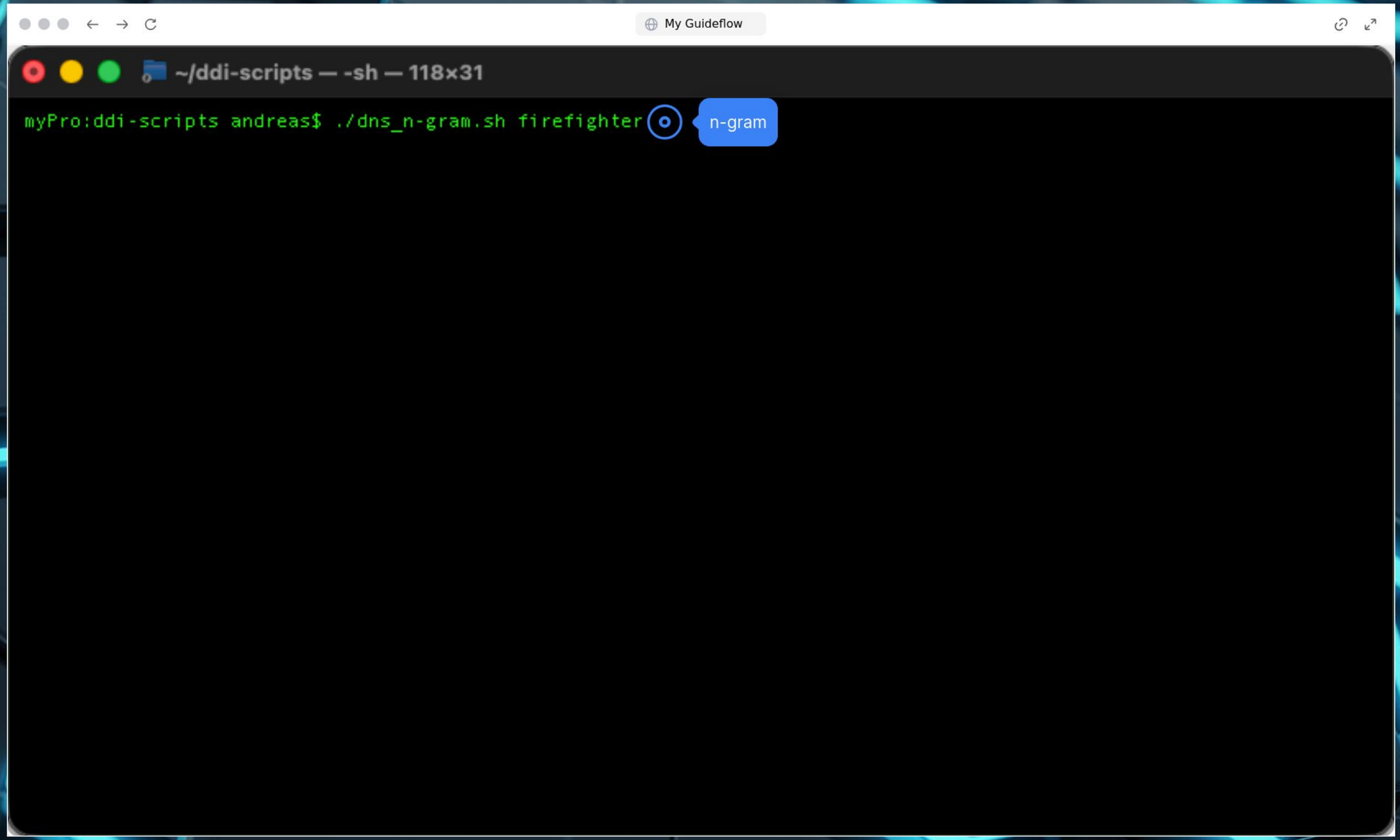


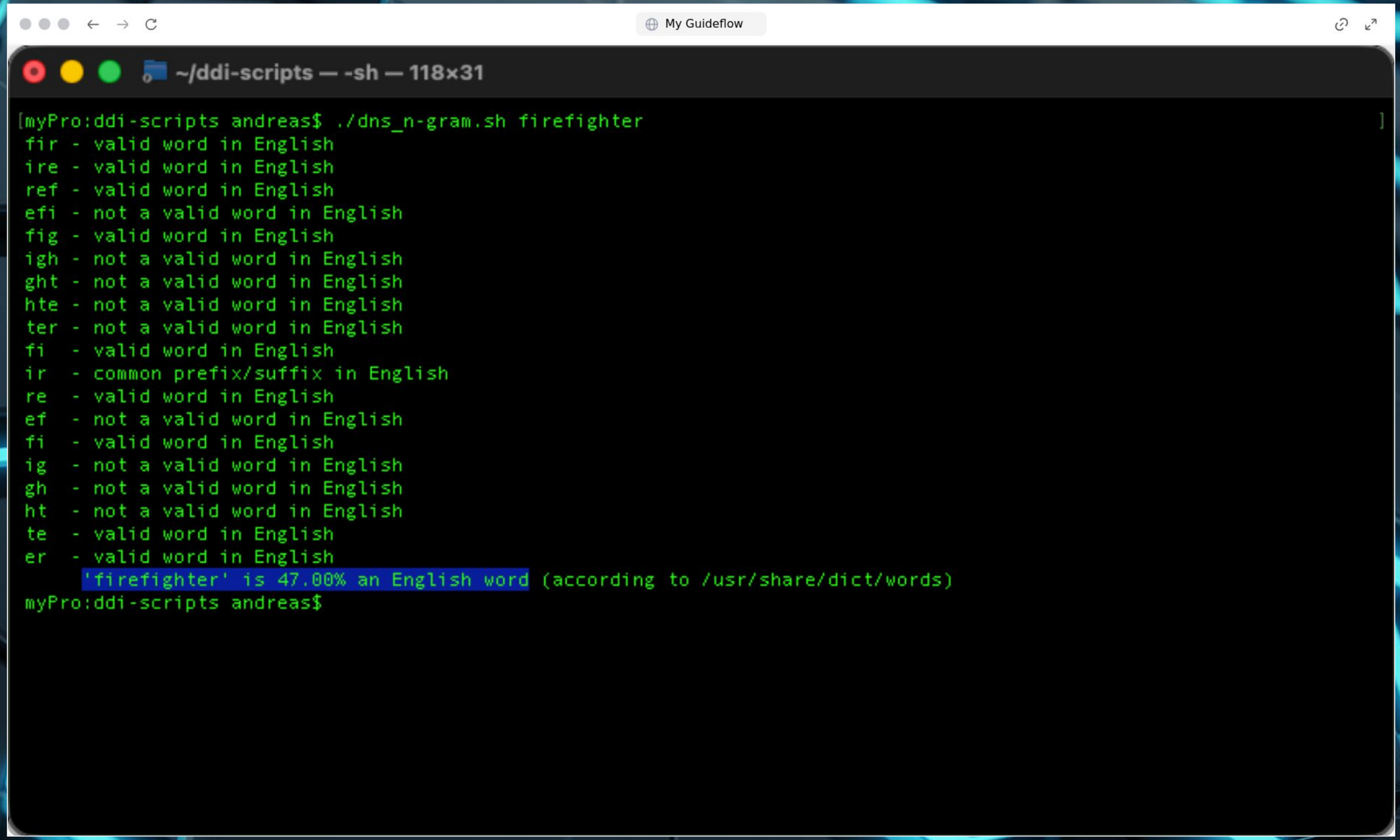






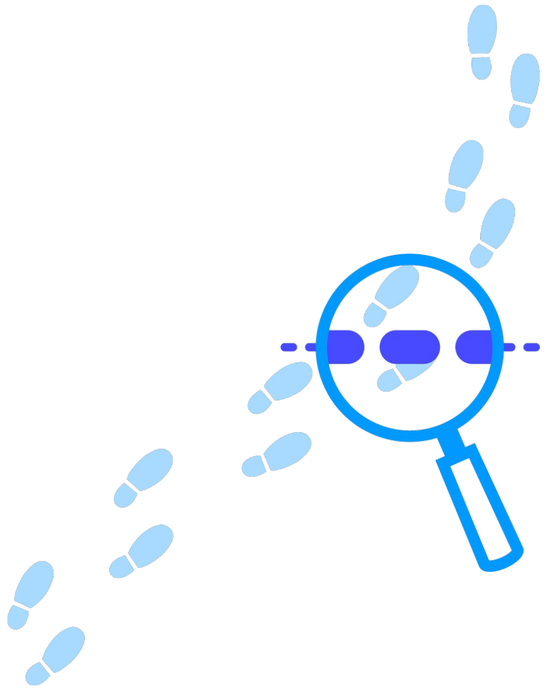




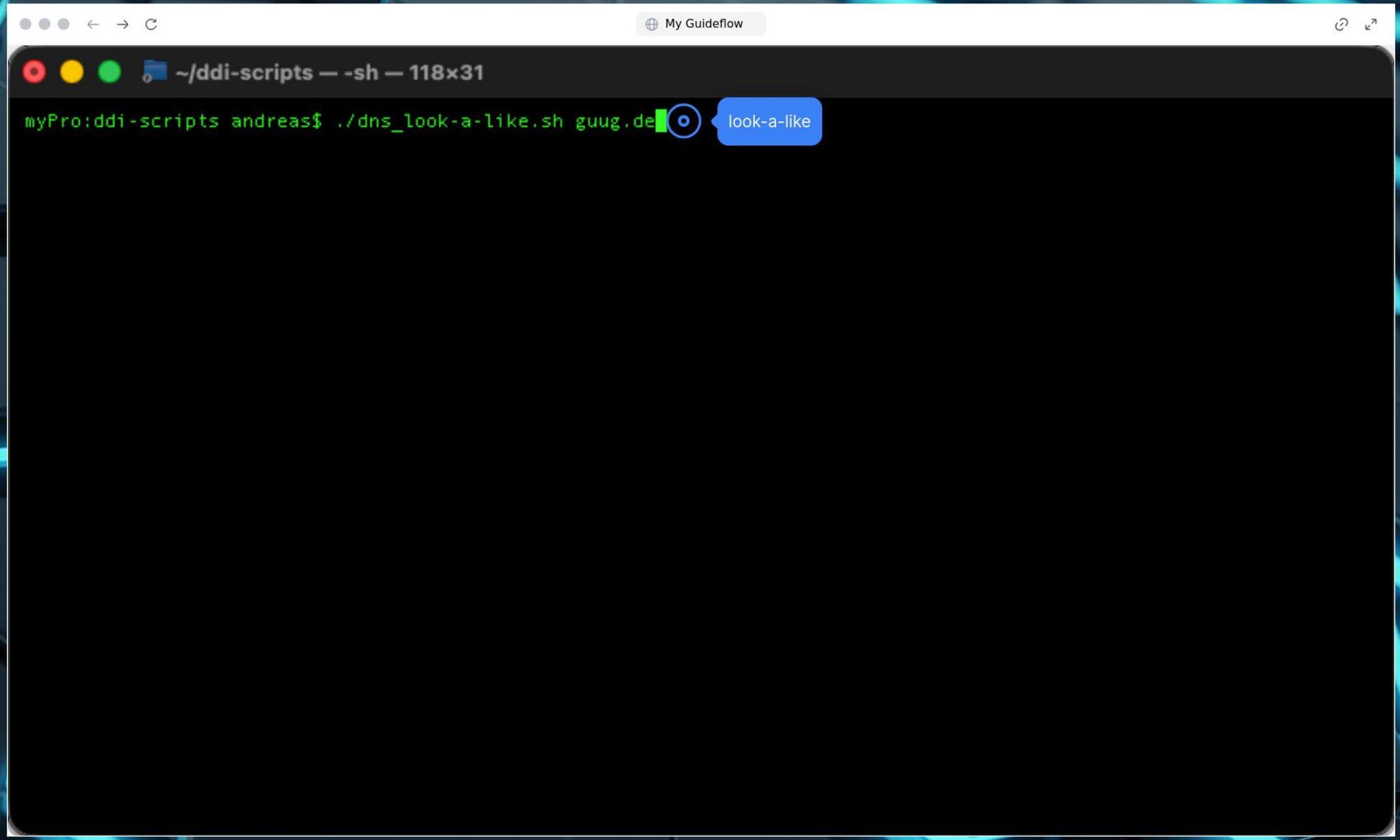


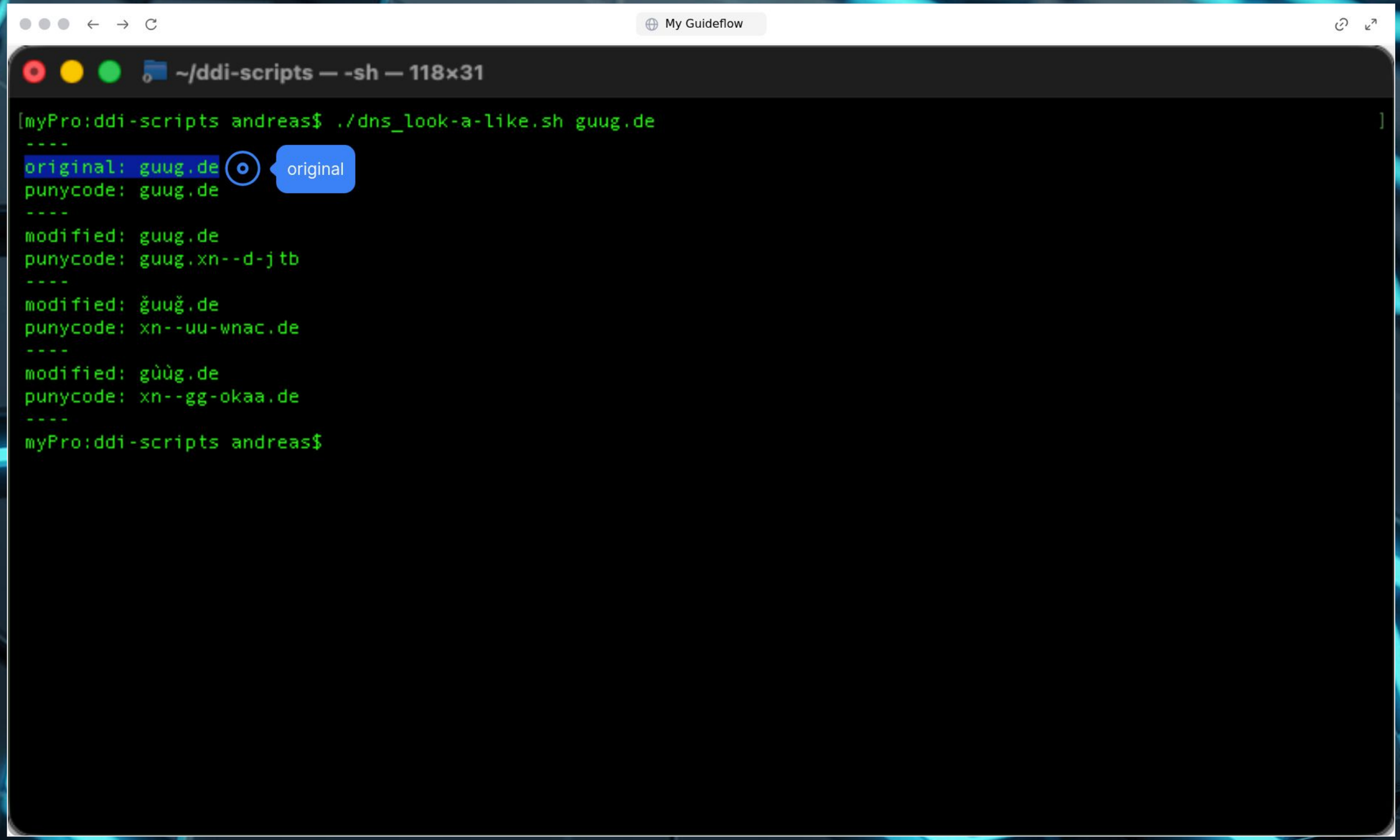
Deceptive But Valid Domains

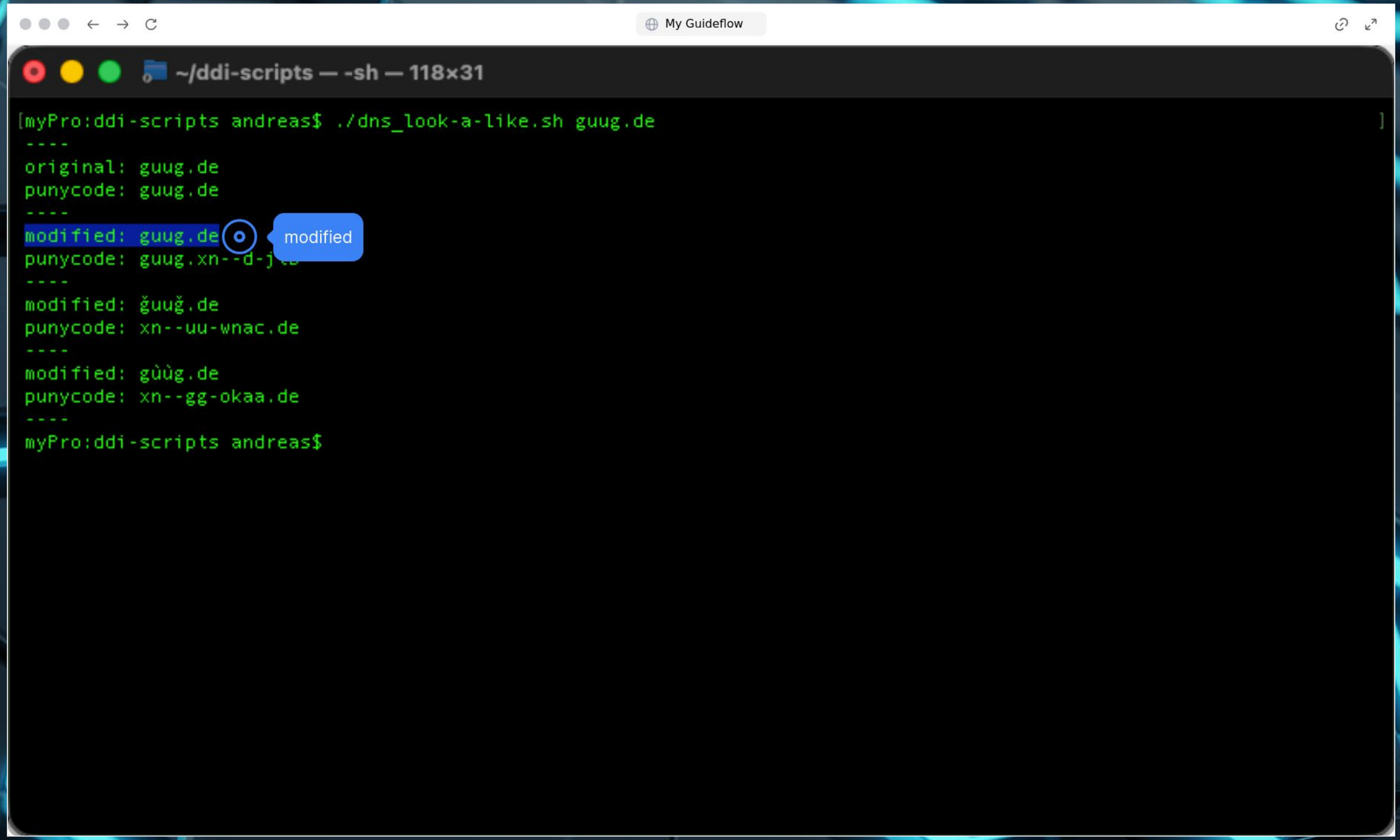
- Visually identical names
- Unexpected punycode
- Legitimate resolution

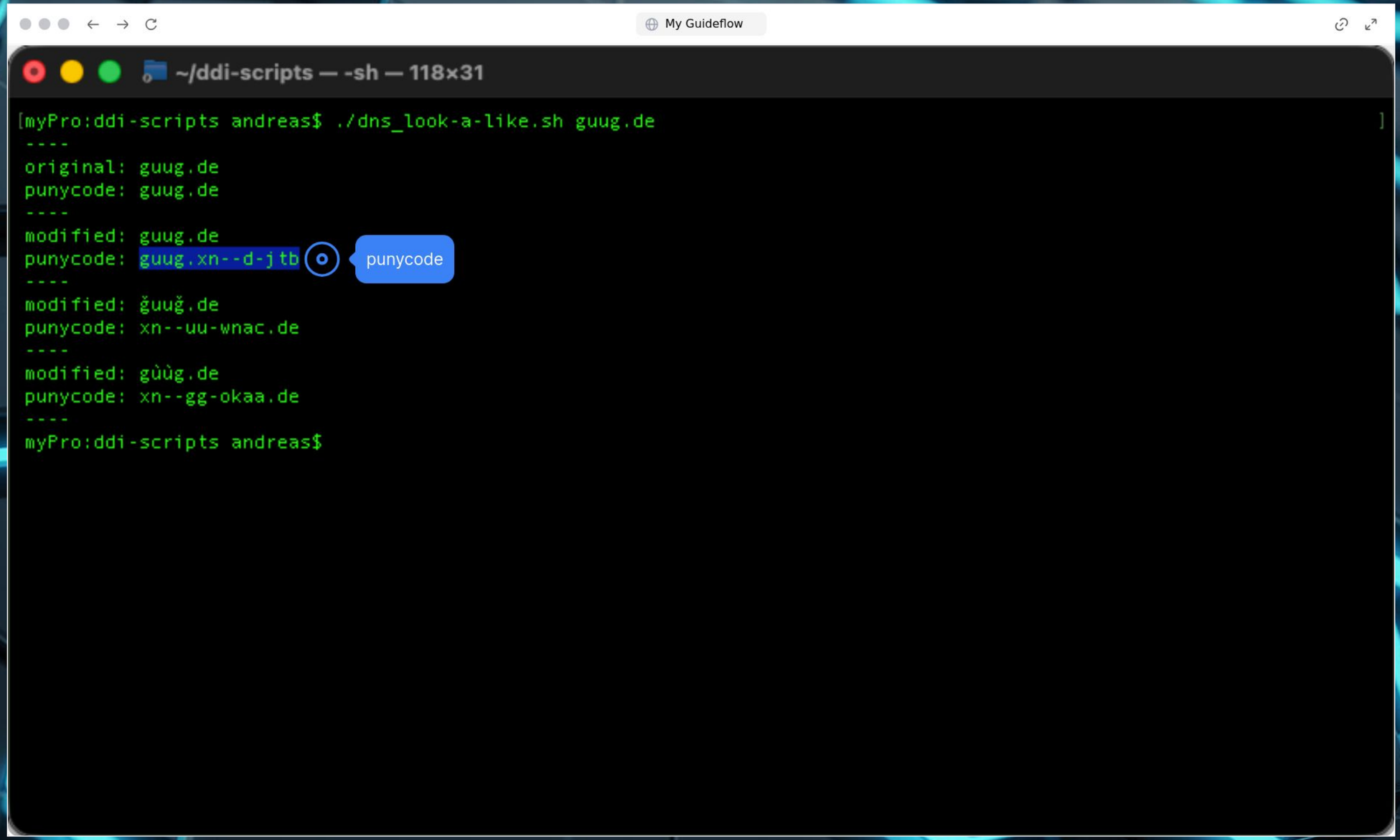


Demo: Look-a-like



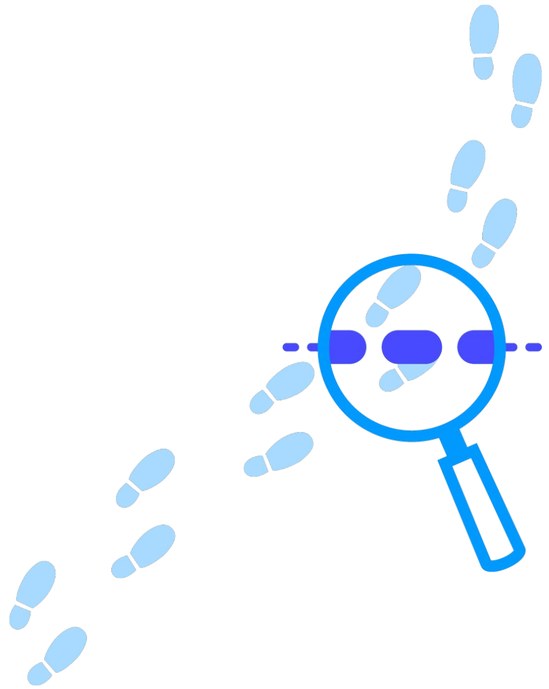




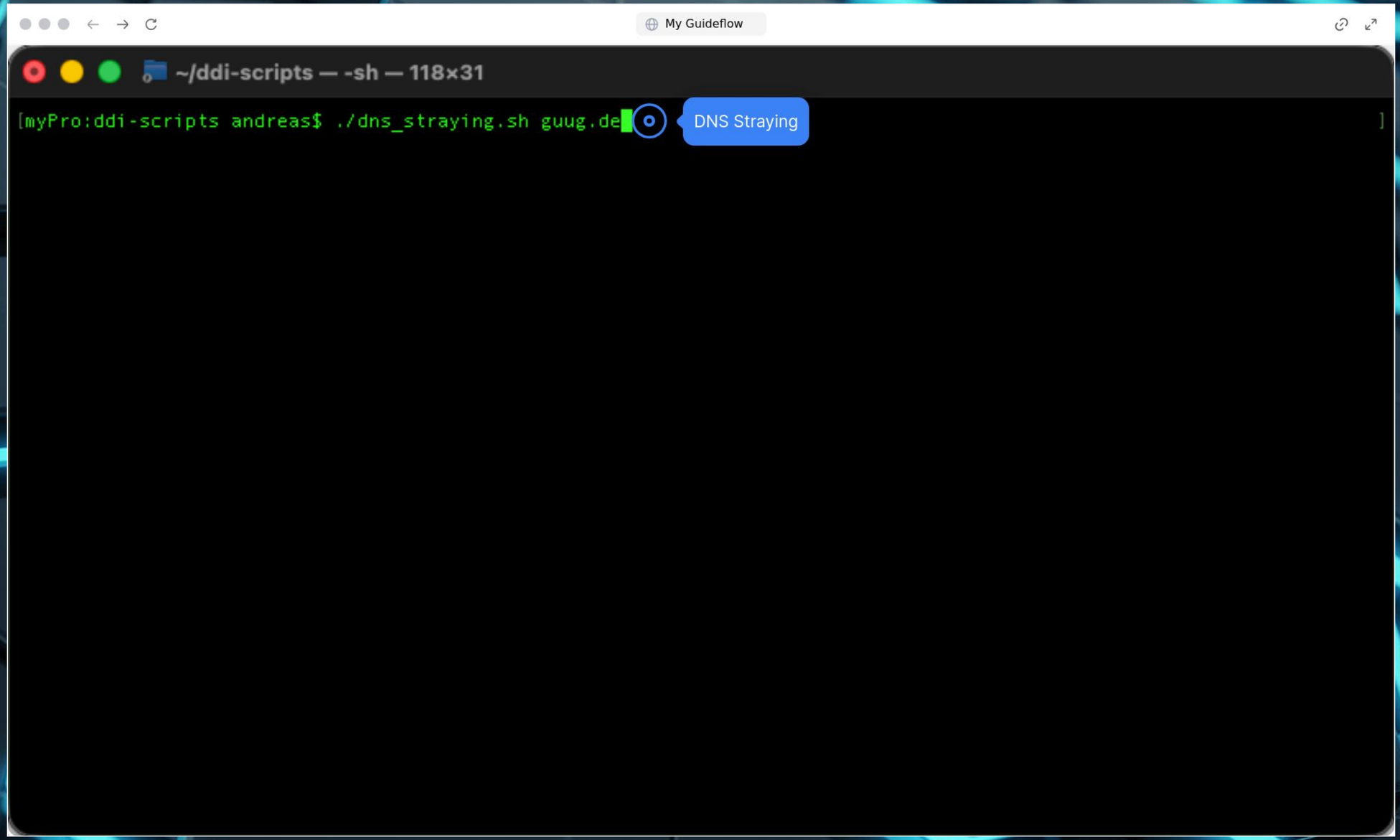


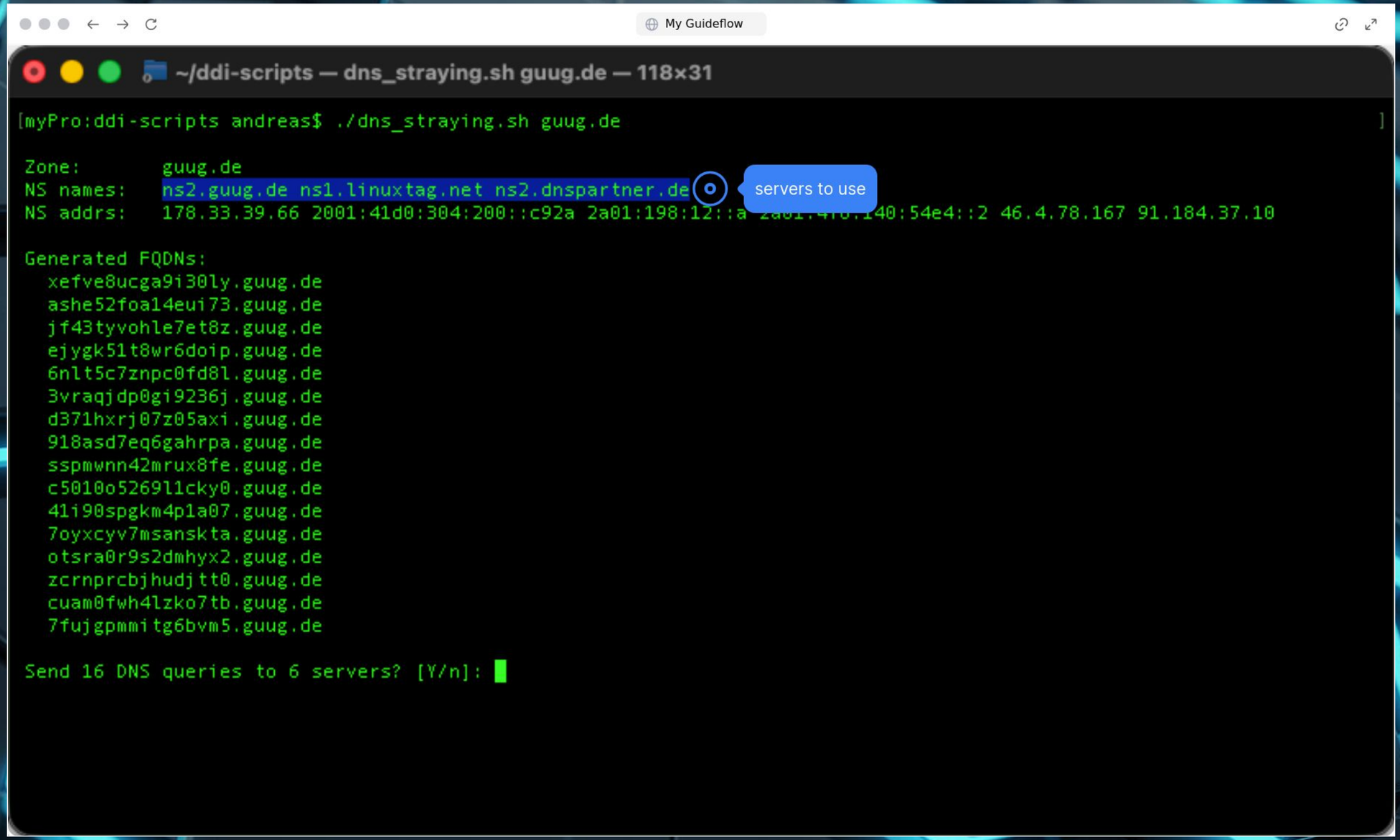
Blending Into DNS Noise

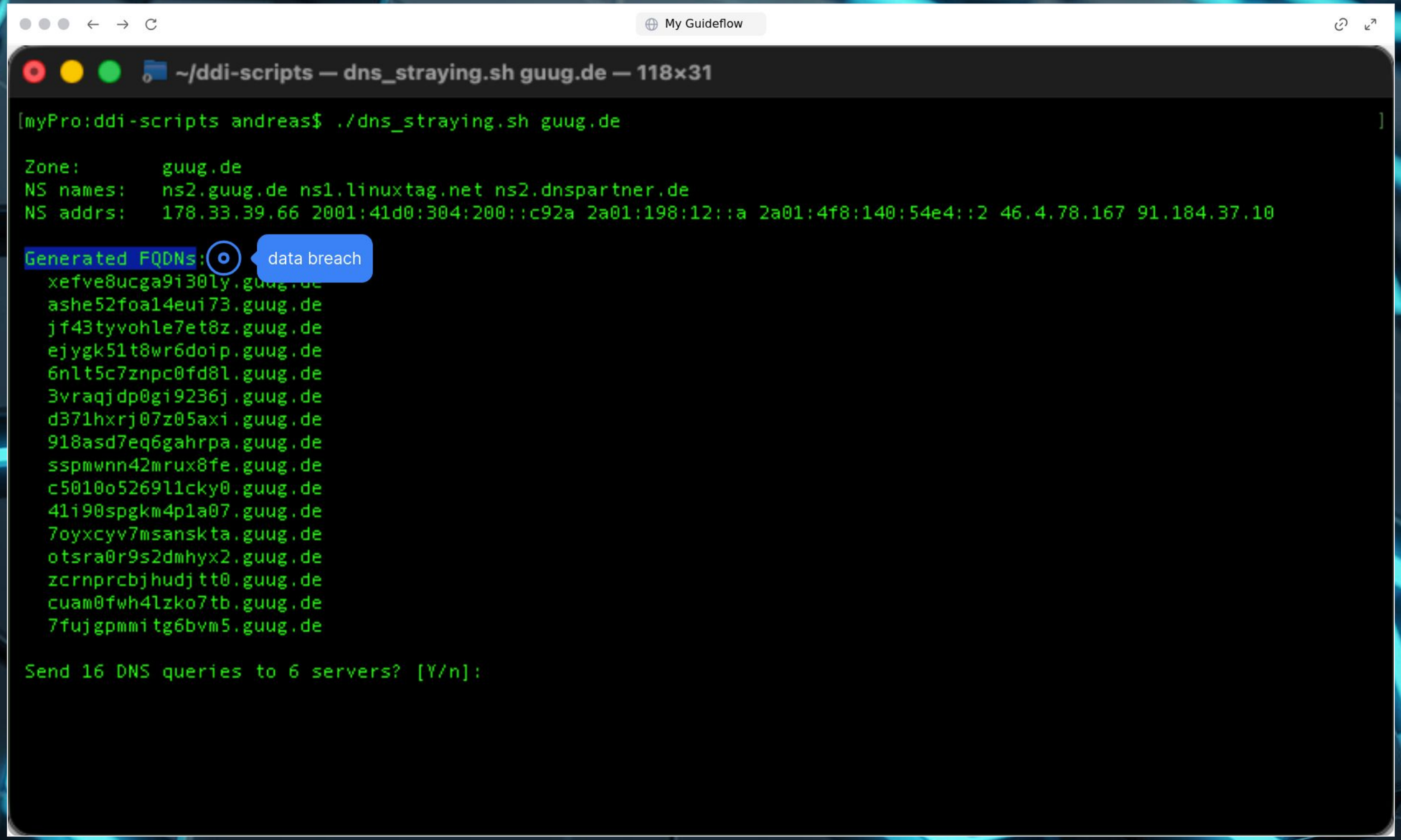
- Random-looking hostnames under real zones
- Persistent NXDOMAIN noise
- Deliberately distributed, low-and-slow patterns

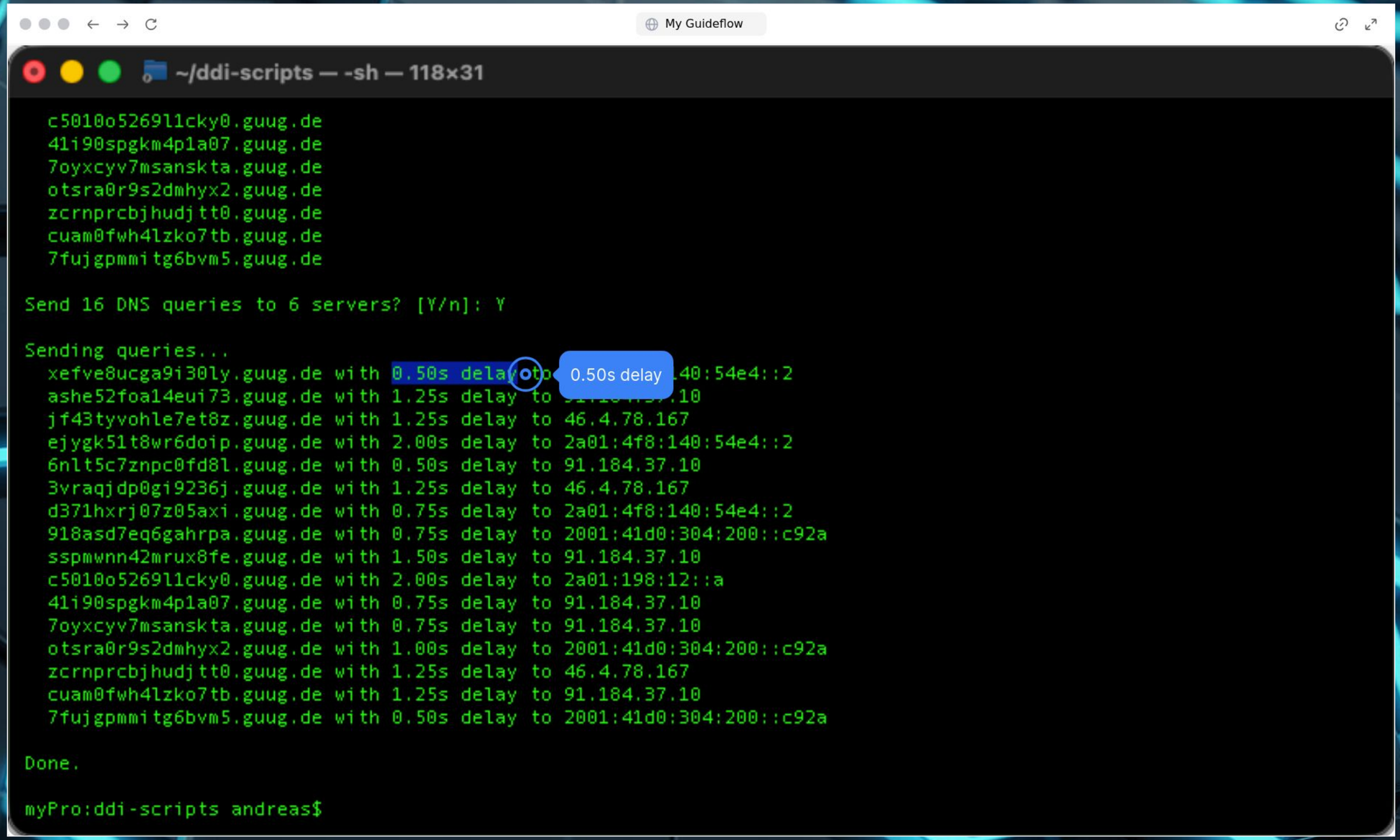


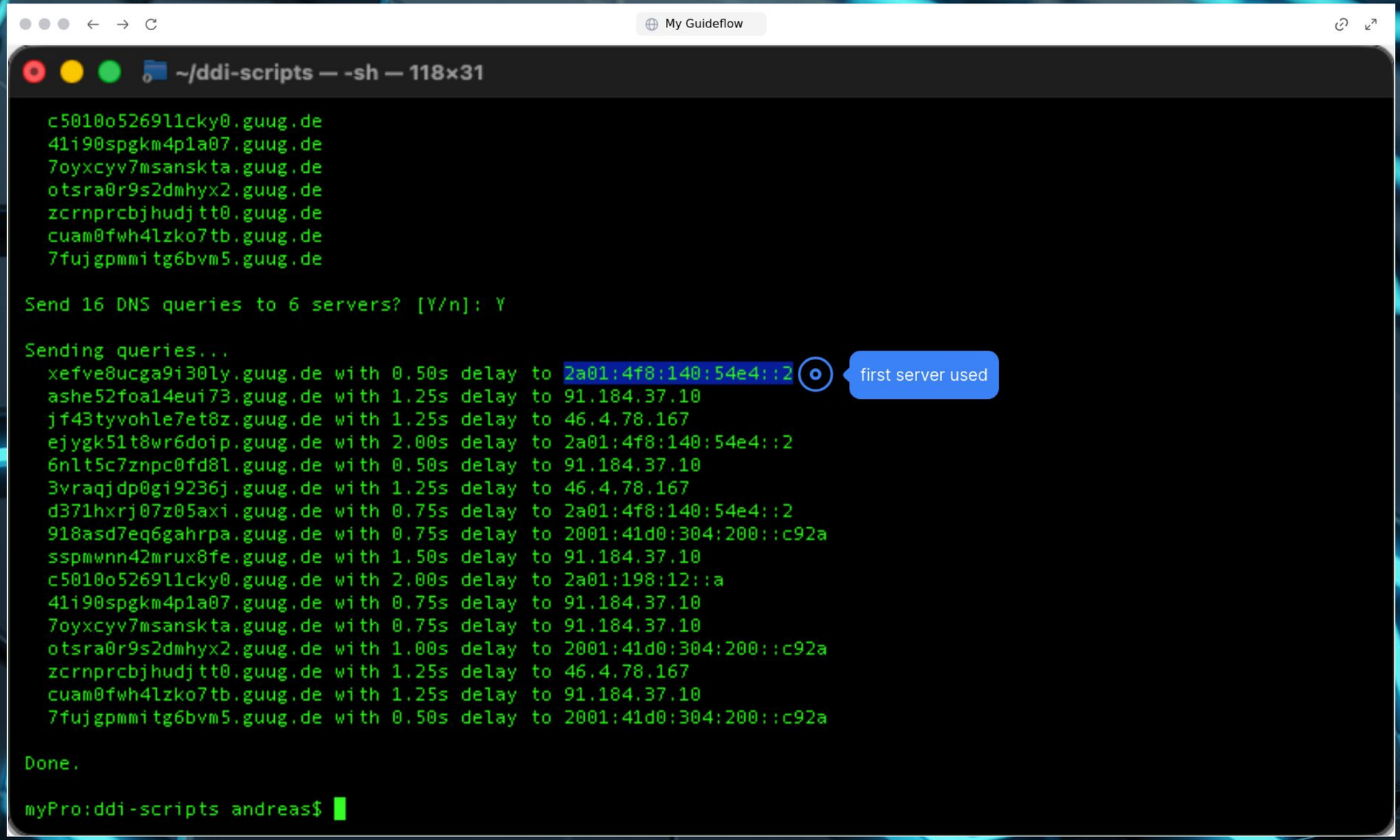
Demo: DNS Straying

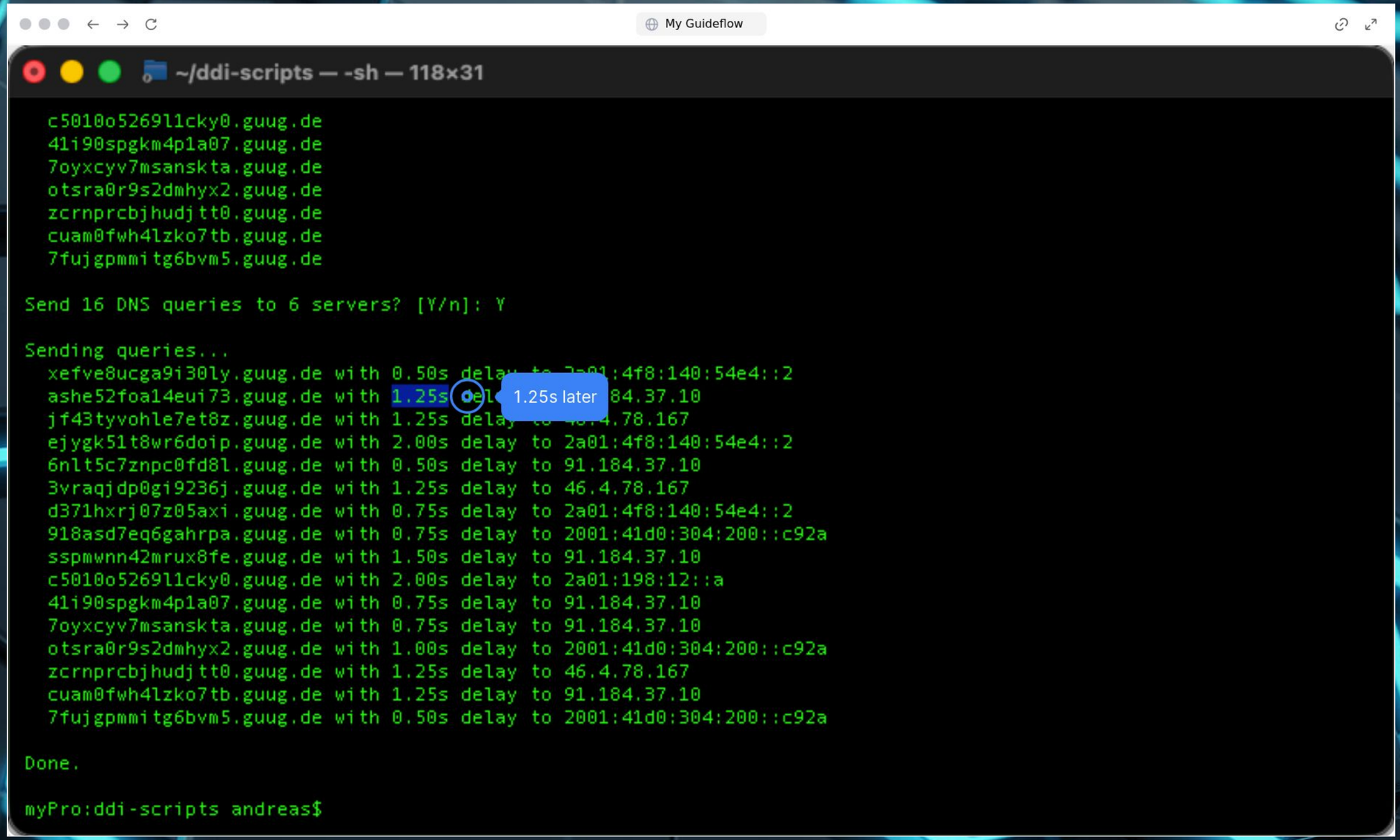


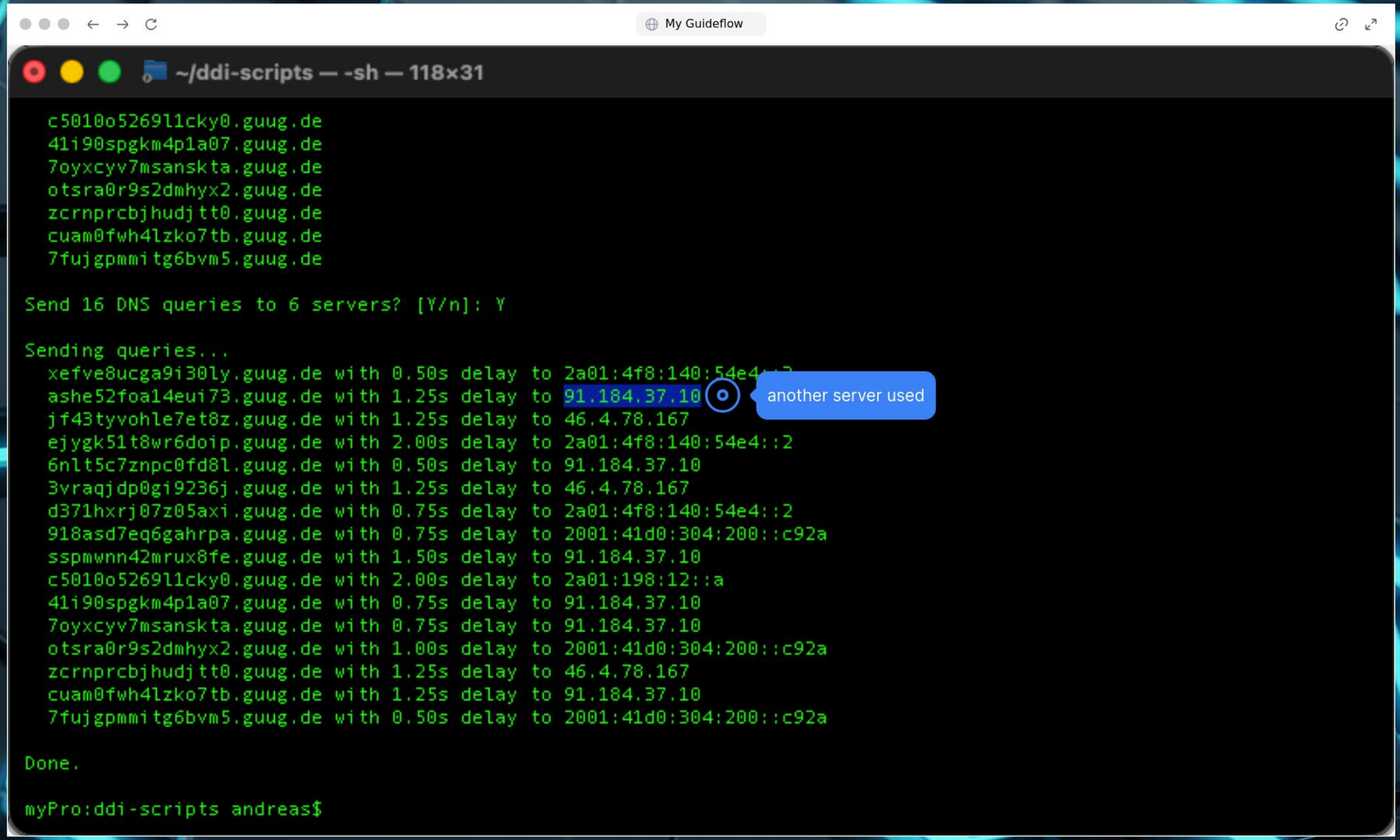






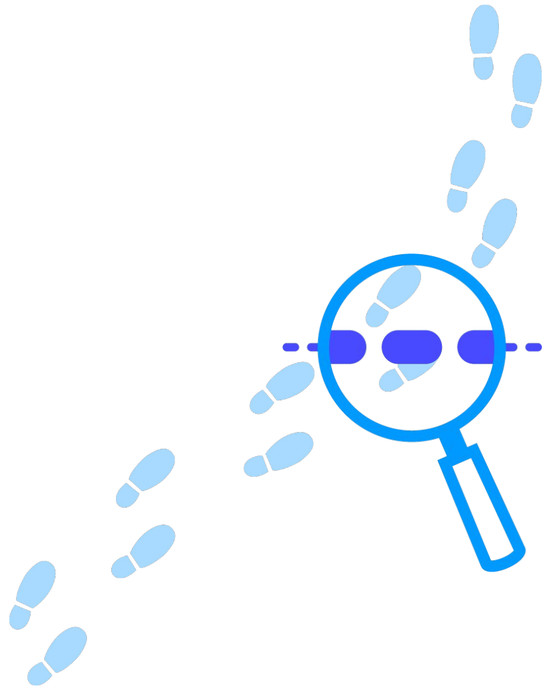




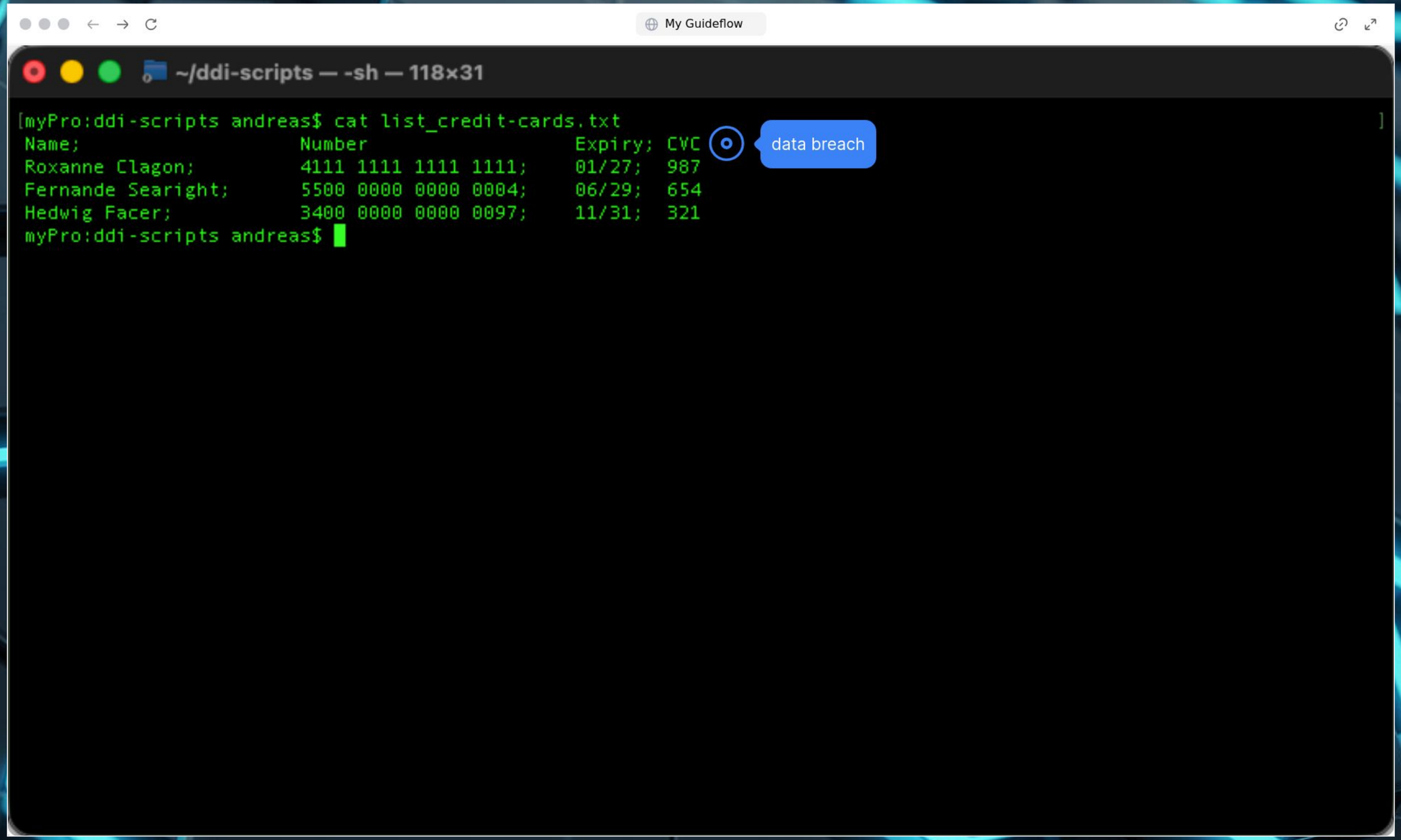


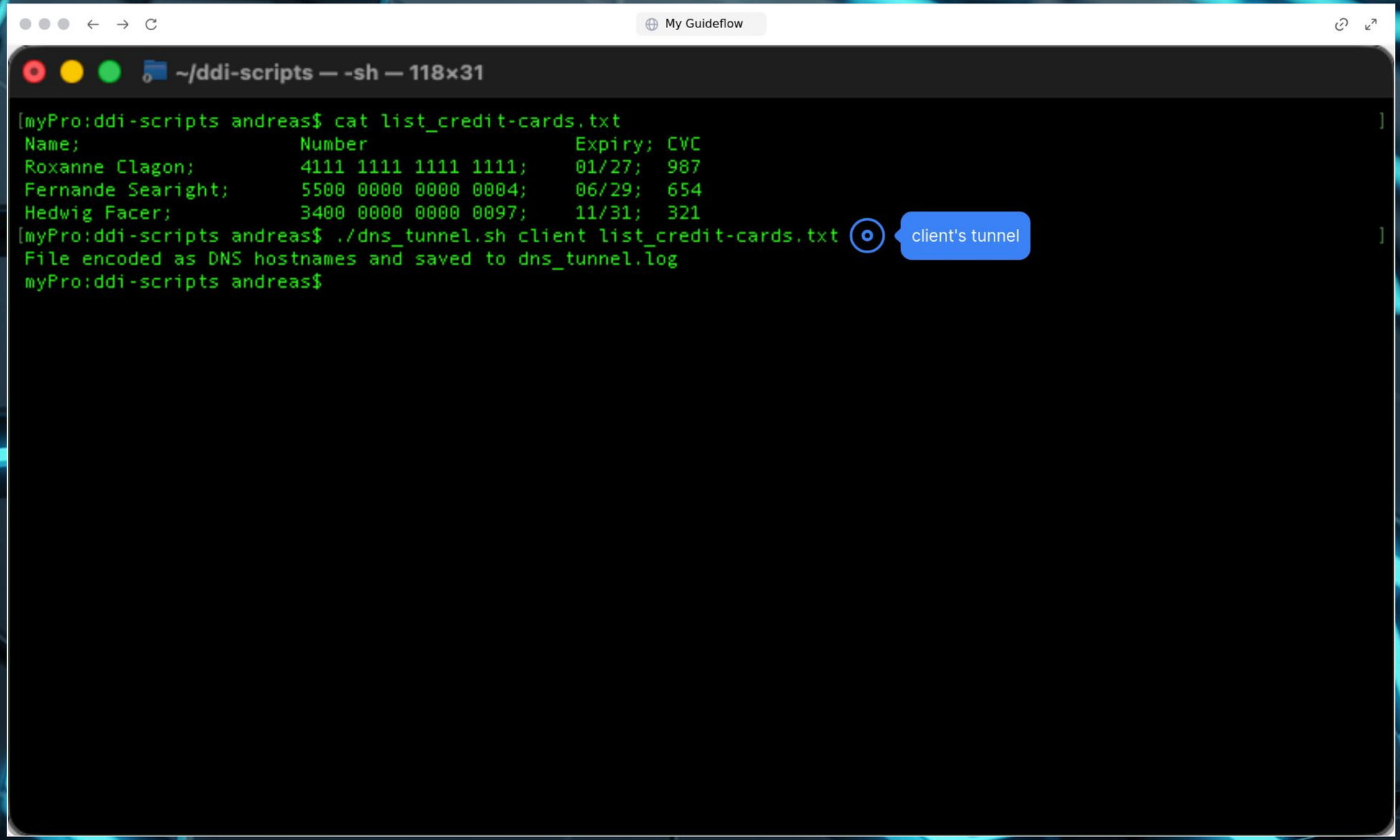
DNS As A Covert Signaling Channel

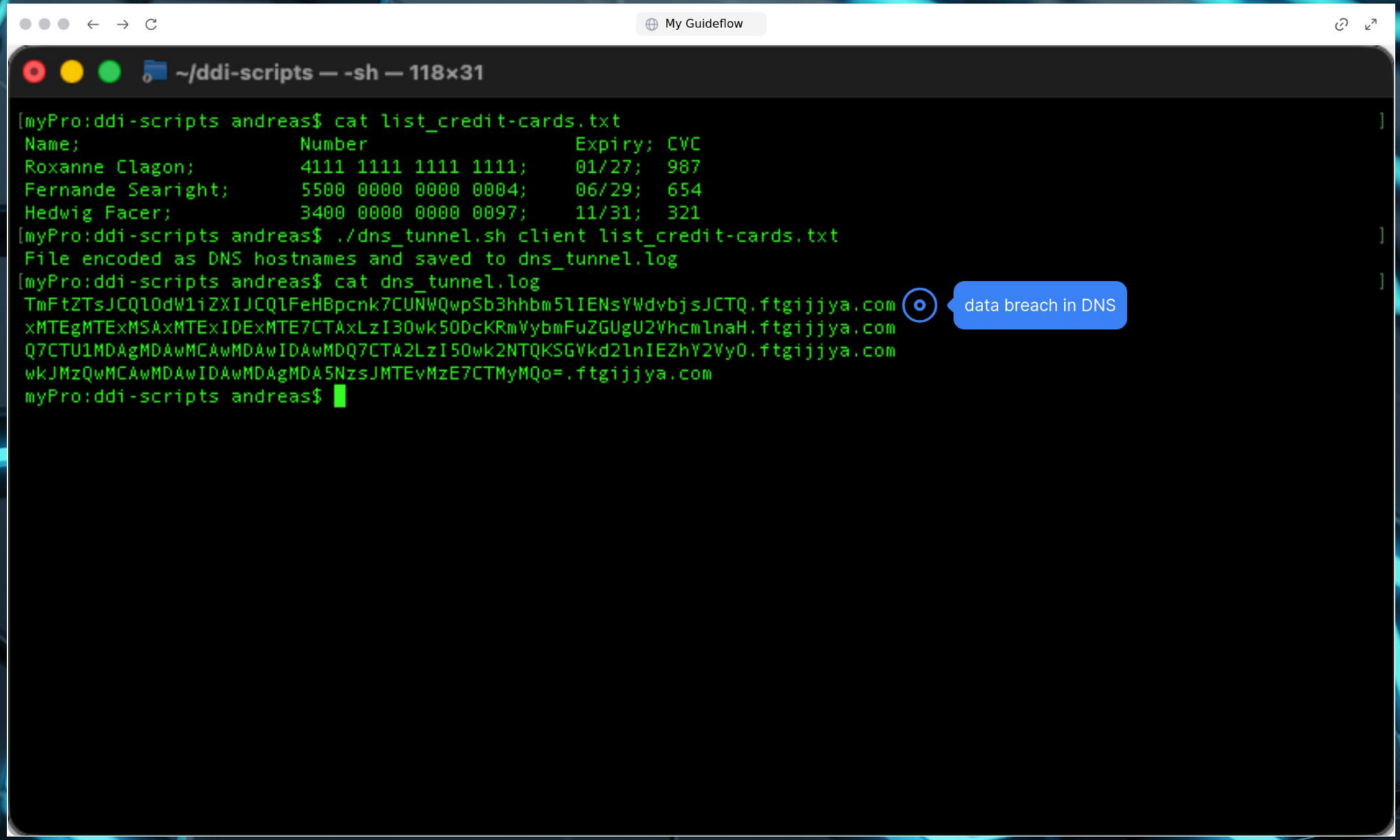
- Data embedded in DNS queries (tunneling)
- Data embedded in DNS metadata (SOA serials)
- RFC-compliant traffic with hidden meaning

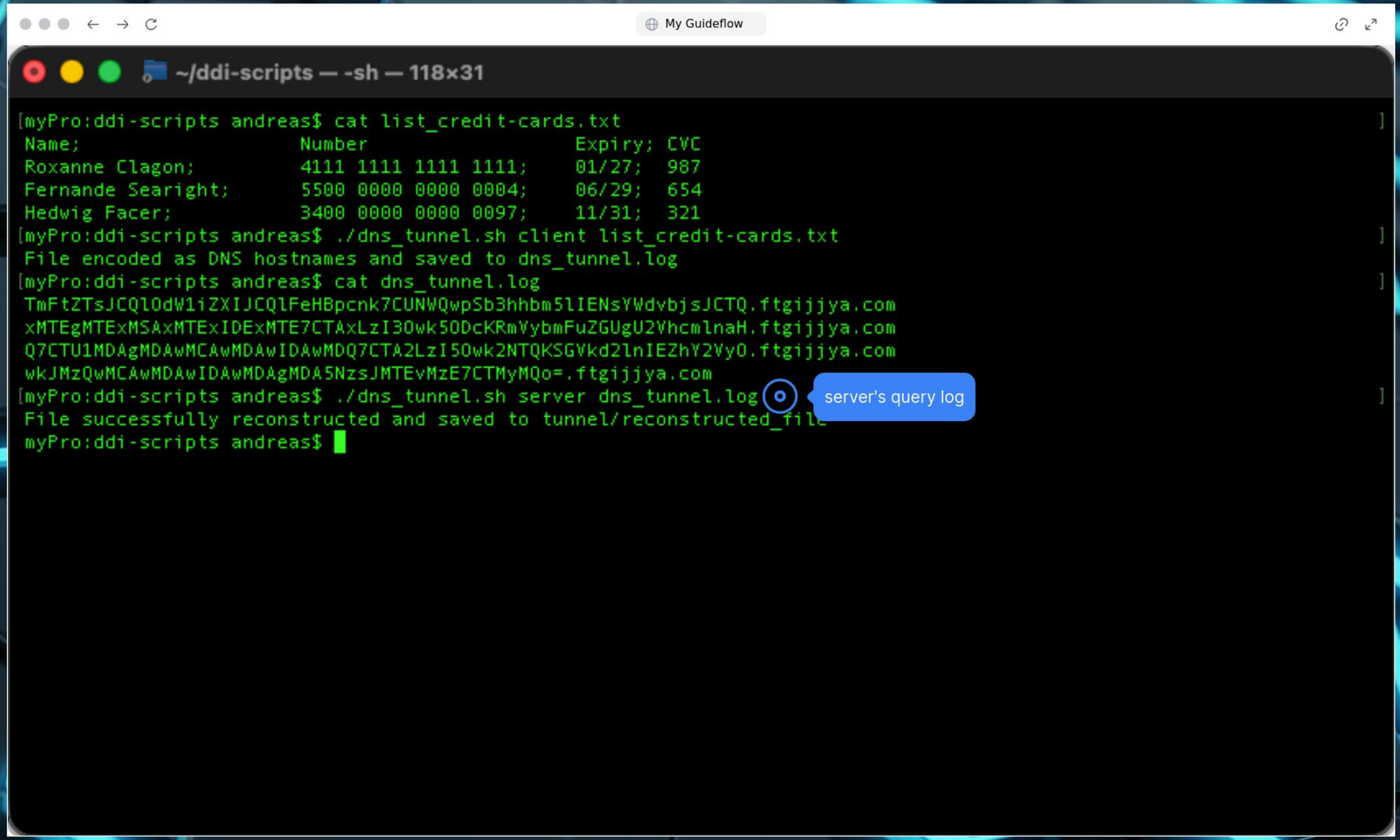


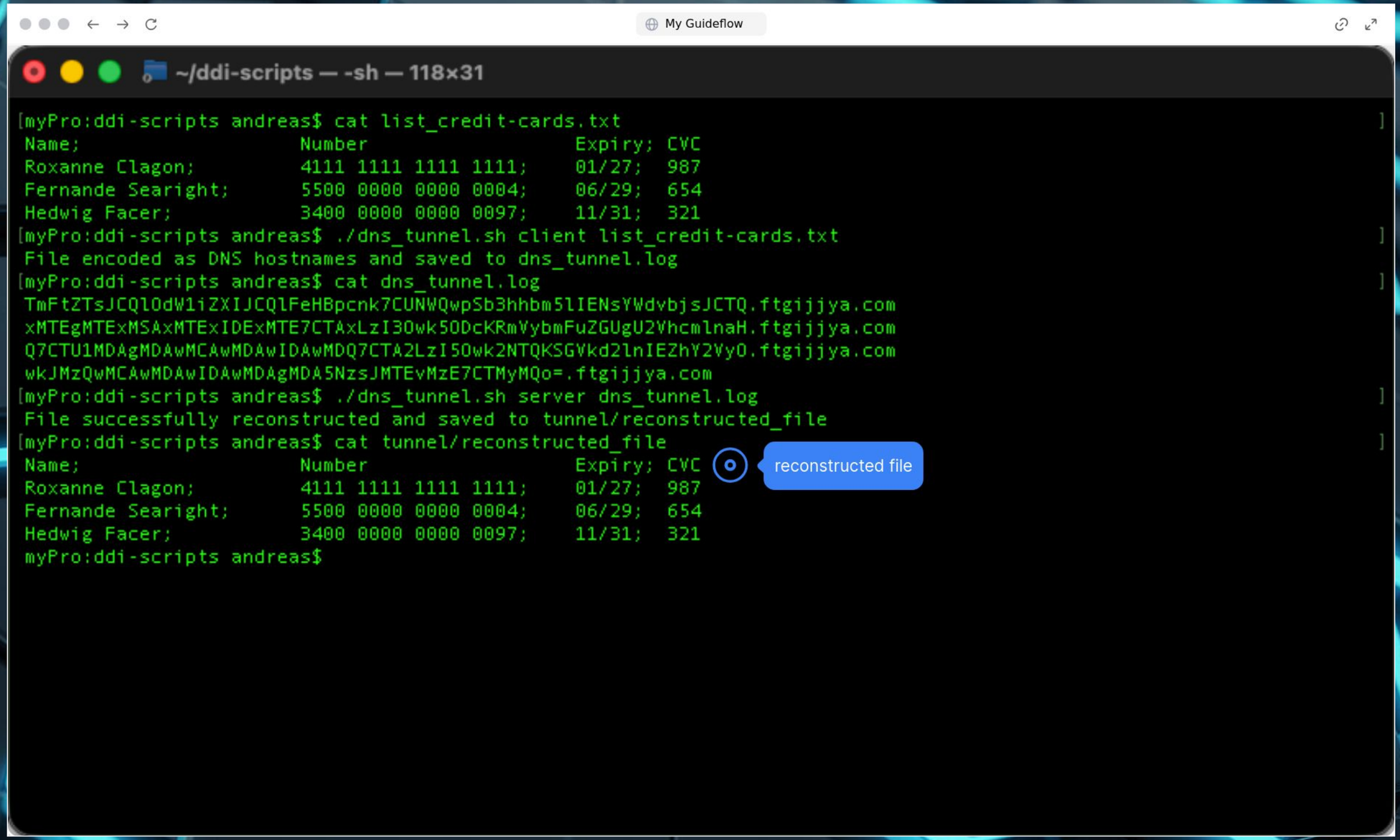
Demo: DNS Tunneling & Serial Numbers

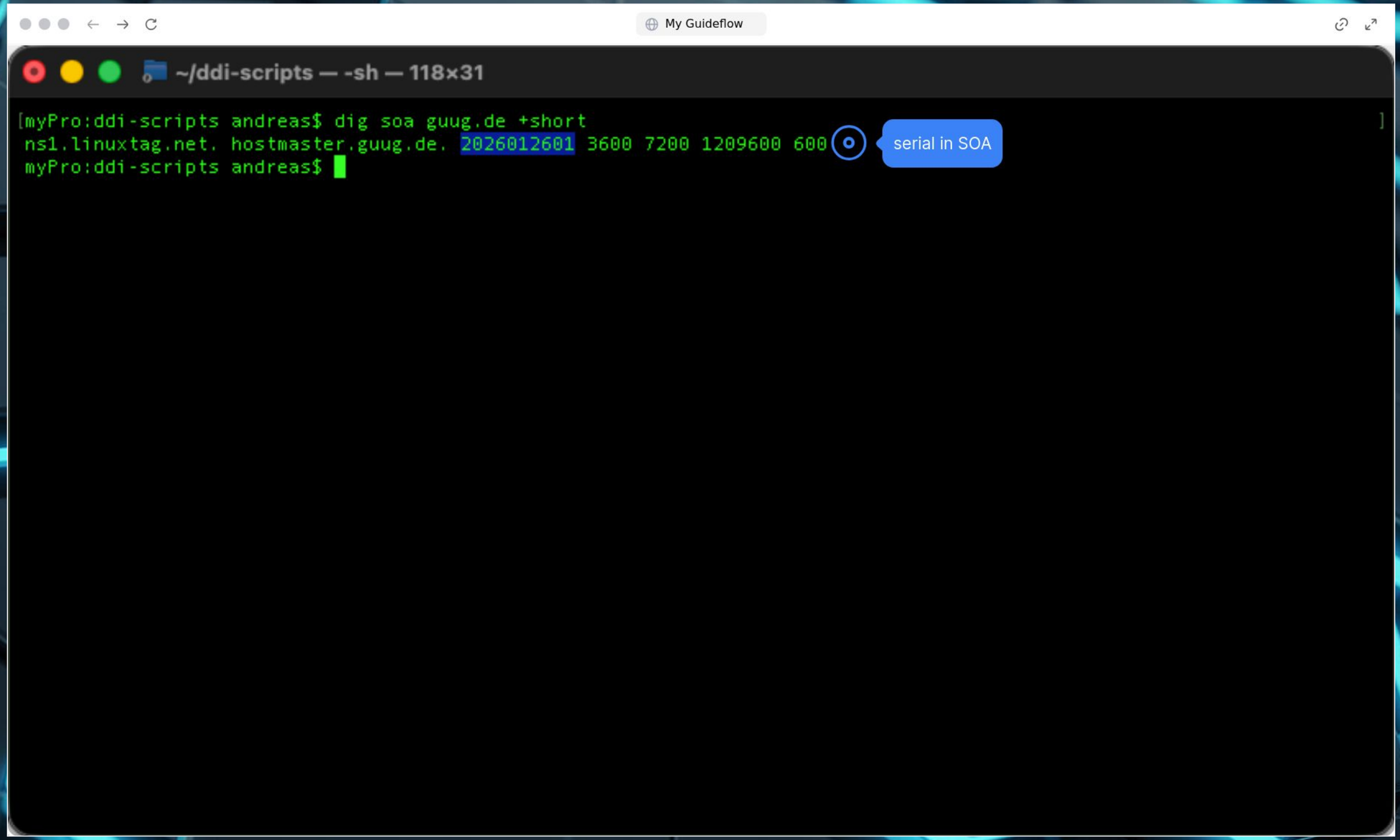


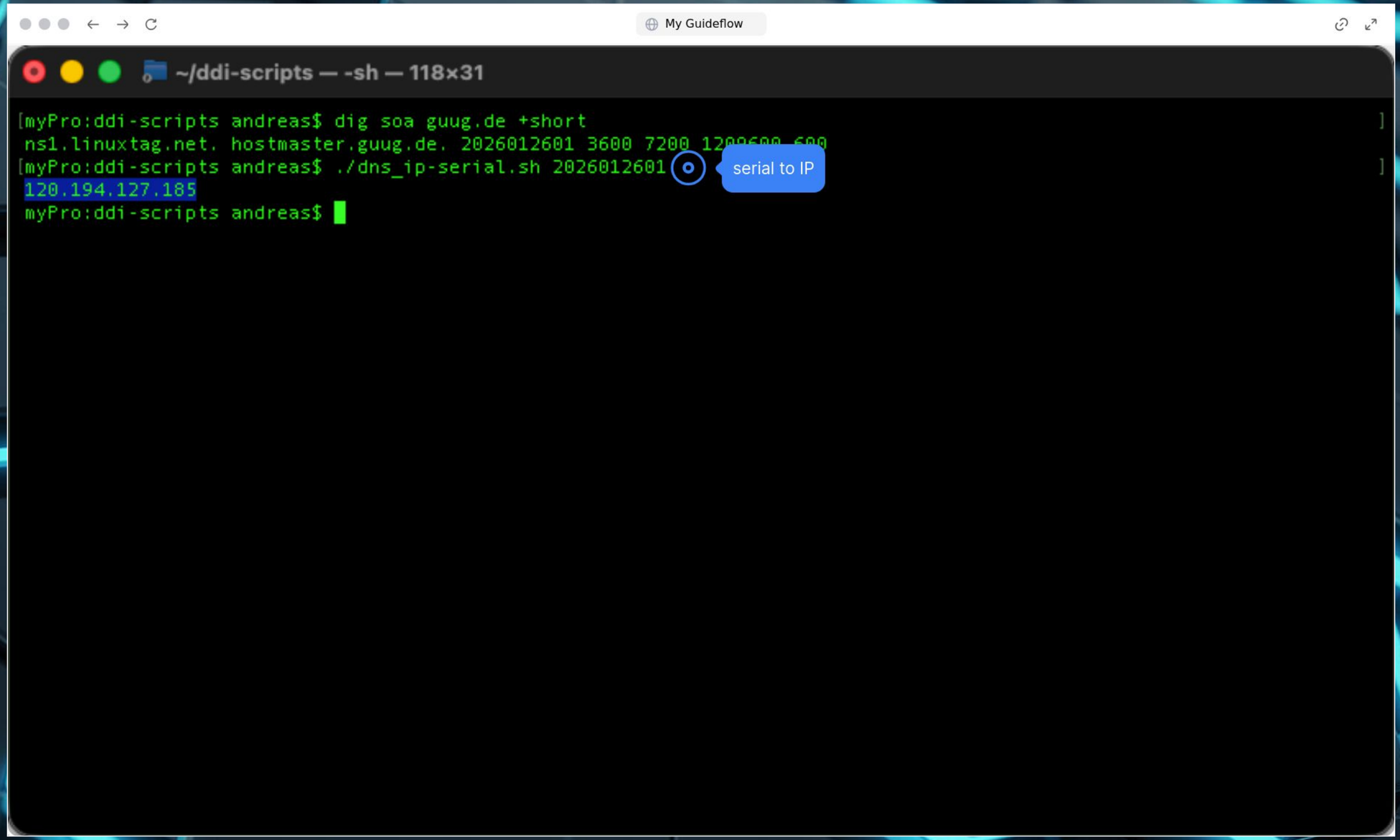








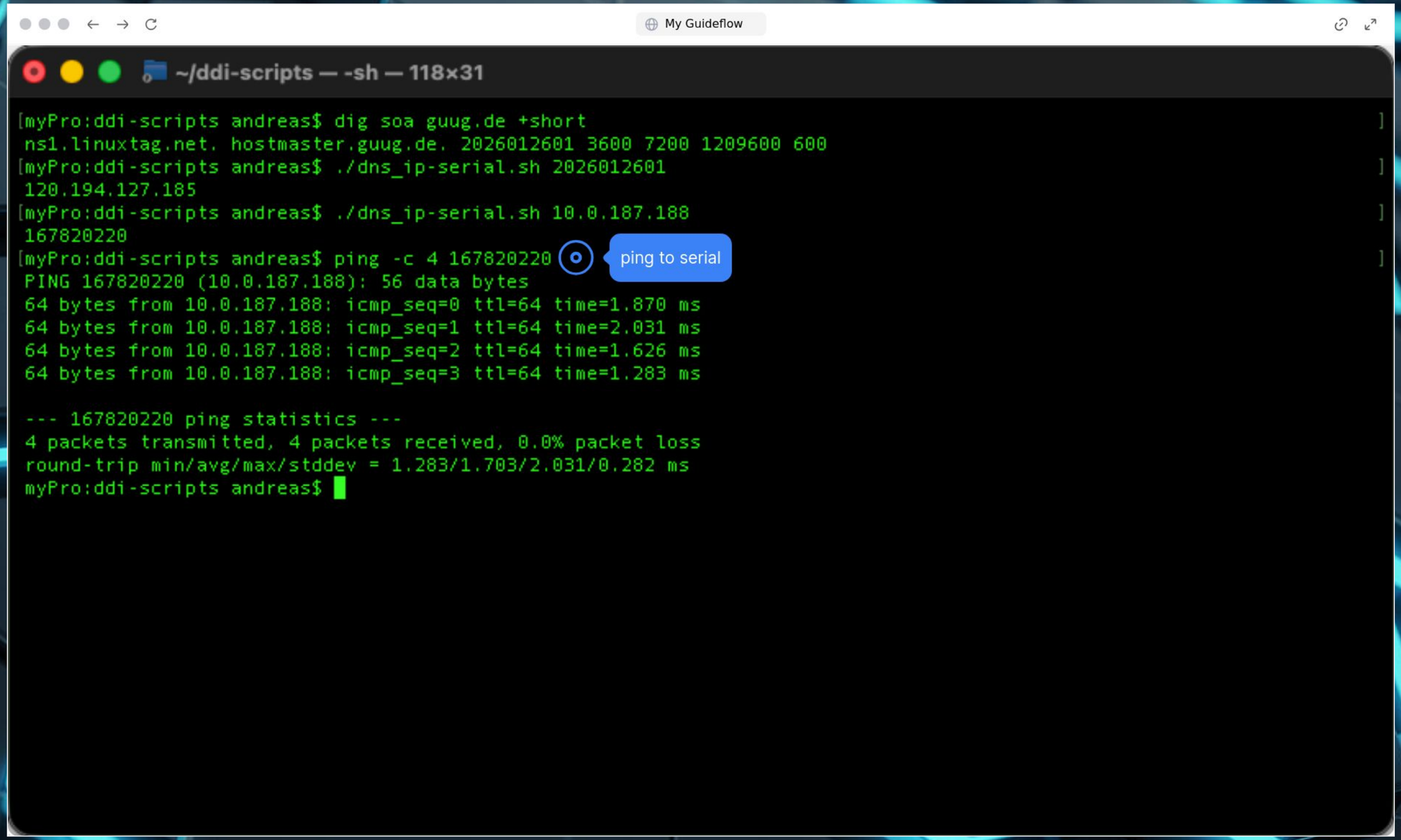




My Guideflow

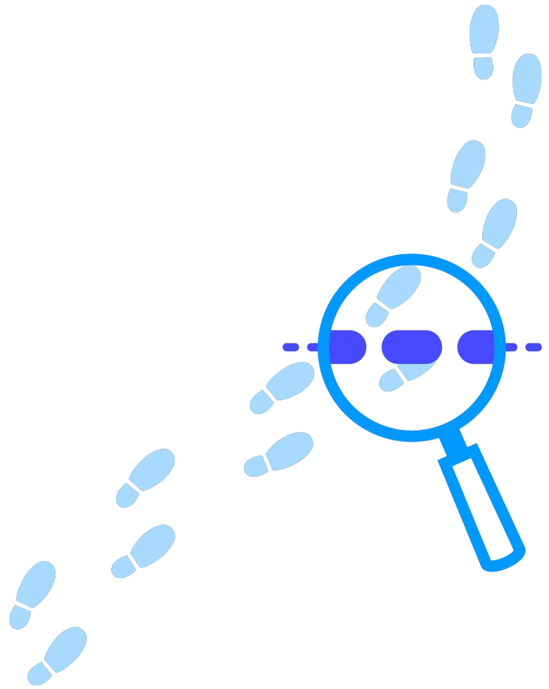
~/ddi-scripts — -sh — 118×31

```
[myPro:ddi-scripts andreas$ dig soa guug.de +short
 ns1.linuxtag.net. hostmaster.guug.de. 2026012601 3600 7200 1209600 600
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 2026012601
 120.194.127.185
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 10.0.187.188
 167820220
 myPro:ddi-scripts andreas$
```



All Of This In Your DNS

- Early warning signals are already in DNS telemetry
- Generic tools often miss DNS specific patterns
- DNS specialized security is needed
- DNS data volume is the challenge



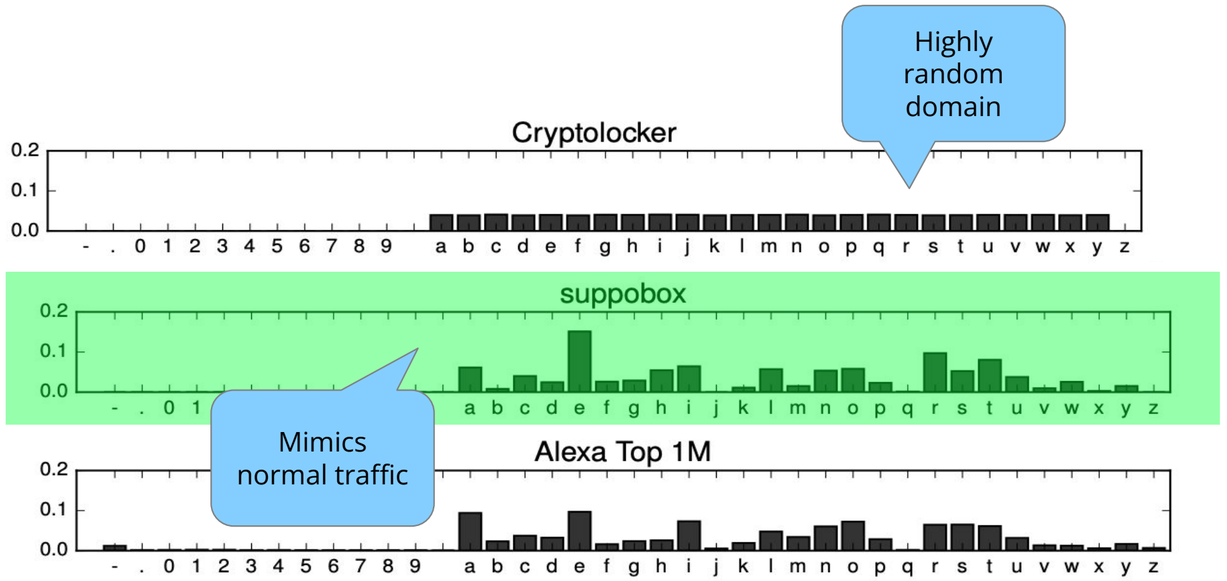
The signals are there. Finding them at scale needs DNS specific detection.

From DNS Signals To Detection And Validation

efficient iP®

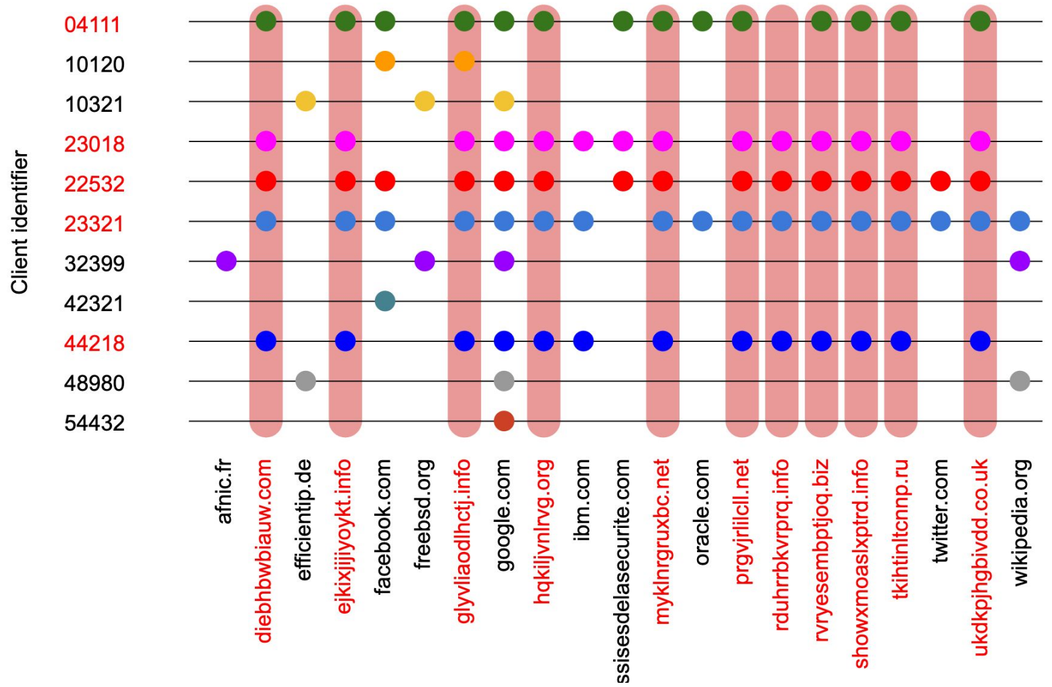
Common DGA Detection

- Analyze domain name syntax only
- Use statistical or ML-based patterns
- High false positives and easy to evade

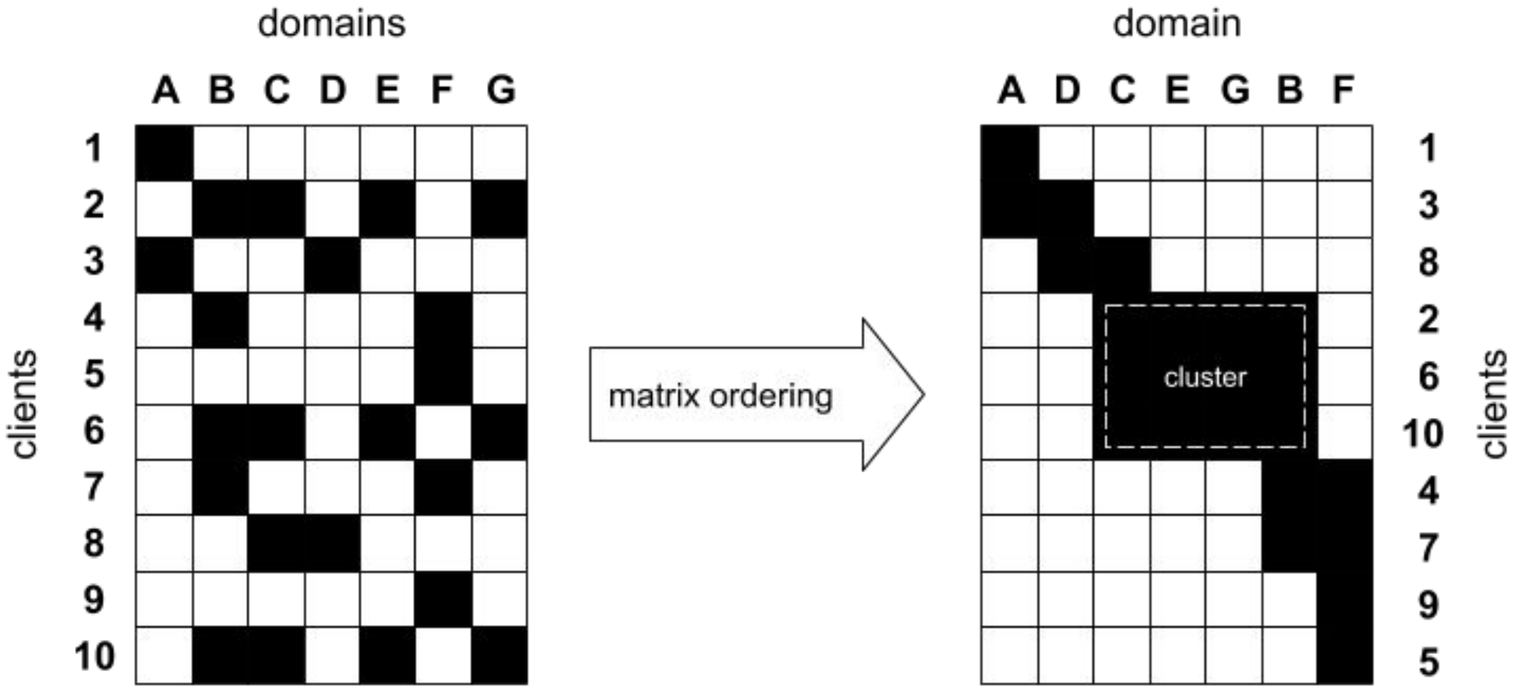


Focus On Clients For DGA Detection

- Analyzes clients instead of domains
- Groups by client and DNS behavior
- Tracks evolution and recruitment dynamics

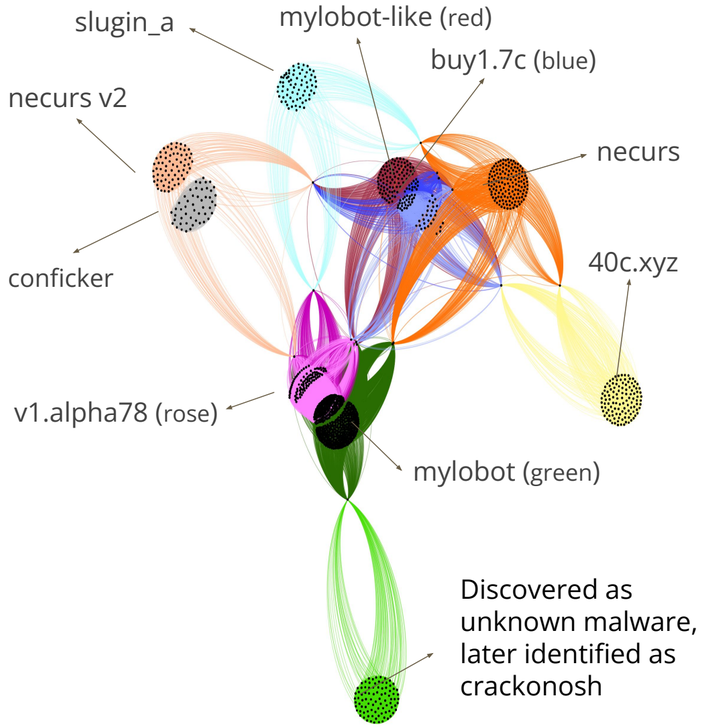


Matrix-Based Validation Of DGA Activity

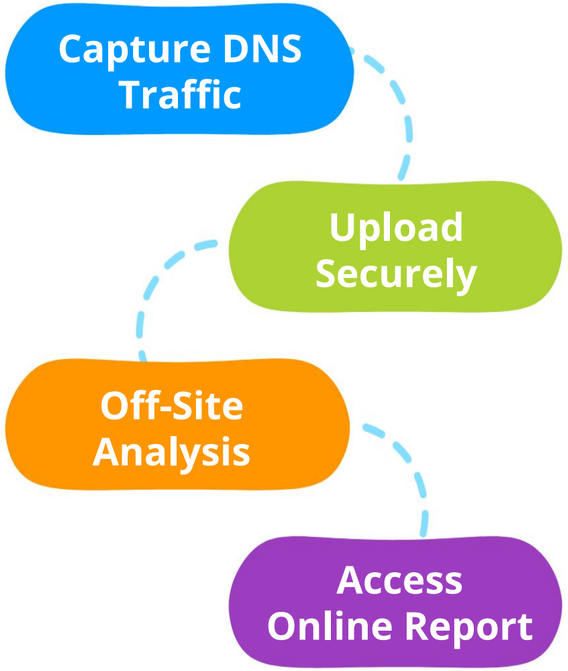


Detecting DGAs Via Tuple Clustering

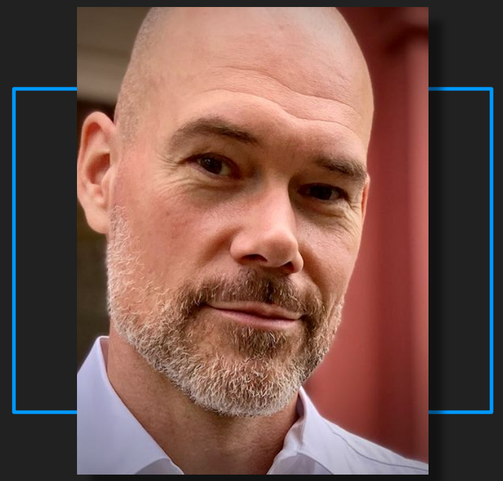
- Project client–domain tuples into a multidimensional space
- Cluster associations using unsupervised analysis
- Clusters indicate potential DGA activity



DNS Risk Assessment



Questions



Andreas Taudte

Senior Technical Marketing Manager

andreas.taudte@efficientip.com

efficient iP®

Thank You

efficient iP®